Cisco GGSN Release 10.1 Configuration Guide

Cisco IOS Release 12.4(24)YE3
Cisco Service and Application Module for IP,
Cisco 7600 Series Internet Router Platform

Last updated February 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number: OL-19936-06

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R))

Copyright © 2010, Cisco Systems, Inc.
All rights reserved

CONTENTS

About This Book 17

CHAPTER 1 **Overview of GPRS and UMTS** 1-1

- Overview 1-1
- Benefits 1-5
- Features Introduced in Cisco IOS Release 12.4(24)YE 1-6
- Features Introduced in Prior Releases 1-6

CHAPTER 2 **Overview of the Single IP Cisco GGSN** 2-1

- Single IP Architecture and the Cisco GGSN 2-1
- Single IP Components and Concepts 2-3
  - Single IP Interface 2-3
    - Single Interface for Configuration 2-3
    - Single Interface for Troubleshooting and Maintaining 2-4
    - Single Interface for Network Management 2-4
  - Session Load Balancing 2-4
  - Address Pool Management 2-5
  - Distributed Endpoints 2-6
  - Distributed Command Line Interface 2-6
    - Distributed Configuration Commands 2-6
    - Distributed Privileged EXEC Commands 2-8
  - Configuration Locking 2-8
  - Redundancy State Sharing 2-9
- Single IP Cisco GGSN Usage Notes 2-9

CHAPTER 3 **Planning to Configure the GGSN** 3-1

Prerequisites 3-1
Before You Begin 3-1
Platform Prerequisites 3-2
Required Hardware and Software 3-2
Required Base Configuration 3-3
Restrictions 3-9
Additional References 3-11
Related Documents 3-11
Standards 3-11
MIBS 3-12
RFCs 3-12
Technical Assistance 3-13

CHAPTER 4 **Configuring GTP Services on the GGSN** 4-1

GTP Overview 4-1
Configuring GGSN Services 4-2
GGSN Services Configuration Task List 4-2
Enabling GGSN Services 4-2
Creating a Loopback Interface 4-3
Creating a Default GTP Virtual Template Interface for the GGSN 4-3
Enabling CEF Switching 4-4
Configuring Echo Timing on a GGSN 4-4
Overview of the Echo Timing on the GGSN 4-5
Overview of the Default Echo Timer 4-5
Overview of the Dynamic Echo Timer 4-7
Echo Timing Configuration Task List 4-10
Customizing the Default Echo Timer 4-10
Configuring the Dynamic Echo Timer 4-11
Disabling the Echo Timer 4-12
Verifying the Echo Timing Configuration 4-12
Verifying Echo Timing Parameters 4-12
Verifying the Dynamic Echo Timer by GTP Path 4-13

Customizing the GGSN Configuration 4-14
Configuring GTP Signaling Options 4-15
Configuring Other GTP Signaling Options 4-15
Configuring the Maximum Number of PDP Contexts on the GGSN 4-16
Configuring the Maximum Number of PDP Contexts When Using DFP with Load Balancing 4-17
Controlling Sessions on the GGSN 4-17
Configuring Session Timers 4-18
Deleting Sessions on the GGSN 4-23
Configuring Flow Control for GTP Error Messages 4-24
Configuring the GGSN to Maintain a History for Deleted SGSN Paths 4-25
Suppressing Echo Requests per SGSN 4-25
Configuring Support for GGSN-Initiated Update PDP Context Requests 4-26
Using the Service-Mode Function 4-27
Configuring Global Maintenance Mode 4-27
Configuring APN Maintenance Mode 4-28
Configuring Charging Maintenance Mode 4-30
Monitoring and Maintaining GTP on the GGSN 4-31
Configuration Examples 4-32
GGSN Configuration Example 4-32
Dynamic Echo Timer Configuration Example 4-34

CHAPTER 5 **Configuring IPv6 PDP Support on the GGSN** 5-35
IPv6 PDPs on the GGSN Overview 5-35
Supported Features 5-38
Restrictions 5-38
Implementing IPv6 PDP Support on the GGSN 5-39
Enabling the Forwarding of IPv6 Traffic on the GGSN 5-39
Configuring an IPv6 Base Virtual Template Interface 5-40
Enabling IPv6 Support on an APN 5-42
Configuring a Local IPv6 Prefix Pool 5-44
Configuring an IPv6 Access Control List 5-45
Configuring Additional IPv6 Support Options 5-47
Monitoring and Maintaining IPv6 PDPs 5-47
Configuration Example 5-48

CHAPTER 6 **Configuring GGSN GTP Session Redundancy** 6-1

GTP-SR Overview 6-1
Prerequisites 6-5
Limitations and Restrictions 6-5
Enabling GTP Session Redundancy 6-6
Configuring the GTP Session Redundancy Interdevice Infrastructure 6-7
Configuring HSRP 6-7
Enabling Interdevice Redundancy 6-12
Configuring the Interdevice Communication Transport 6-12
Configuring Passive Route Suppression on an Interface 6-14
Enabling GTP-SR on the GGSN 6-15
Disabling GTP Session Redundancy 6-15
Configuring Charging-Related Synchronization Parameters 6-16
Monitoring and Maintaining GTP-SR 6-18
Upgrading GGSN Images in a GTP-SR Environment 6-18
Configuration Examples 6-19
Local GTP-SR Examples 6-20
Primary Supervisor Configuration Example 6-20
Primary GGSN Configuration Example 6-22
Secondary GGSN Configuration Example 6-24
Geographical GTP-SR Examples 6-25
GGSN Interface Configuration Examples 6-26
Supervisor Routing Configuration Examples 6-27
GGSN Routing Configuration Examples 6-27

CHAPTER 7 **Configuring Charging on the GGSN** 7-1

Configuring an Interface to the Charging Gateway 7-2
Verifying Interface Configuration to the Charging Gateway 7-2
Configuring the Default Charging Gateway 7-4
Configuring the GGSN to Switchover to the Highest Priority Charging Gateway 7-4
Changing the Default Charging Gateway 7-5
Configuring a Charging Source Interface 7-5
Configuring the GGSN Memory Protection Mode Threshold 7-6
Configuring the Transport Protocol for the Charging Gateway 7-7
Configuring TCP as the Charging Gateway Path Protocol 7-7
Configuring UDP as the Charging Gateway Path Protocol 7-7

Configuring the Charging Release 7-8
Configuring Charging for Roamers 7-9
Configuring PLMN IP Address Ranges 7-10
Enabling Charging for Roamers 7-10
Customizing the Charging Options 7-11
Disabling Charging Processing 7-14
Using Charging Profiles 7-15
Configuring a Charging Profile 7-15
Defining the Charging Characteristics and Triggers of a Charging Profile 7-16
Applying a Default Charging Profile to an APN 7-19
Applying Default Charging Profiles Globally 7-19
Configuring How the GGSN Handles PDPs with Unmatched Charging Profiles 7-20
Configuring G-CDR Backup and Retrieval Using iSCSI 7-20
iSCSI Overview 7-21
Configuring iSCSI Backup and Storage on the GGSN 7-21
Configuring an iSCSI Target Profile 7-23
Associating an iSCSI Target Profile 7-24
Verifying the iSCSI Session 7-24
Monitoring and Maintaining iSCSI CDR Backup and Storage 7-24
Configuring Granular Charging and Storage 7-25
Configuring a Charging Group 7-27
Associating a Charging Group with an Access Point 7-28
Modifying a Charging Group 7-28
Monitoring and Maintaining Granular Charging 7-28
Monitoring and Maintaining the Charging Function on the GGSN 7-29
Configuration Examples 7-29
Global Charging Configuration 7-29
Charging Profile Configuration 7-30
Granular Charging and Storage Configuration 7-31

CHAPTER 8 **Implementing Enhanced Service-Aware Billing** 8-1
Service-Aware GGSN Overview 8-2
Reviewing Limitations and Restrictions 8-3
Enabling Support for Service-Aware Billing 8-3
Configuring Wait Accounting 8-4
Configuring the GGSN to Generate Enhanced G-CDRs 8-4

Configuring Quota Server Support on the Cisco GGSN 8-5
Configuring a Cisco CSG2 Server Group 8-5
Configuring the Quota Server Interface on the GGSN 8-6
Advertising the Next Hop Address For Downlink Traffic 8-9
Configuring the GGSN to Use the Cisco CSG2 as an Authentication and Accounting Proxy 8-9
Configuring a Global RADIUS Server 8-10
Configuring an AAA RADIUS Server Group that includes the Cisco CSG2 8-10
Using Method List to Specify Supported Services 8-10
Specifying Method Lists for an APN 8-11
Monitoring and Maintaining the Quota Server-to-CSG2 Configuration 8-11
Implementing Service-Aware Billing with Diameter/DCCA Support 8-11
Reviewing Service-Aware Billing with DCCA/Diameter 8-12
Supported Features 8-13
Unsupported Features 8-14
Messaging Support 8-14
Service-Aware Billing with DCCA Data Flows 8-15
Configuring the Diameter Base 8-15
Configuring a Diameter Peer 8-16
Enabling Diameter AAA 8-17
Monitoring and Maintaining the Diameter Base 8-20
Configuring the DCCA Client Process on the GGSN 8-20
Enabling Support for Vendor-Specific AVPs in DCCA Messages 8-23
Configuring the Service Aware Billing Parameters in Charging Profiles 8-23
Specifying a Default Rulebase ID 8-24
Specifying a DCCA Profile for Online Billing 8-24
Suppressing CDRs for Prepaid Subscribers 8-25
Configuring Trigger Conditions for Postpaid Subscribers 8-26
Implementing Service-Aware Billing with OCS Address Selection Support 8-27
Service-Aware Billing with OCS Address Selection Data Flows 8-27
Enabling PCC on an APN 8-29
Configuring Standalone GGSN Prepaid Quota Enforcement 8-30
Configuring the Charging Record Type on an APN 8-31
GTP-Session Redundancy for Service-Aware PDPs Overview 8-32
Configuring Per-Service Local Sequence Number Synchronization 8-34
Configuring Enhanced Prepaid Subscriber Features 8-34
Activity-Based Time Billing 8-34
Final Unit Indication Support 8-35
Configuring a Default FUI REDIRECT Filter for an APN 8-37

Configuring Cisco CSG2 Load Balancing 8-37
Configuring Dynamic Cisco CSG2 Load Balancing 8-38
Configuring Static Cisco CSG2 Mapping 8-38
Reviewing Trigger Conditions for Enhance Quota Server Interface Users 8-39
PDP Context Modification 8-39
Tariff Time Change 8-39
Service Flow Reports 8-40
eG-CDR Closure 8-41
Configuration Examples 8-41

CHAPTER 9 **Configuring Network Access to the GGSN** 9-1
Configuring an Interface to the SGSN 9-1
Verifying the Interface Configuration to the SGSN 9-2
Configuring a Route to the SGSN 9-4
Configuring a Static Route to the SGSN 9-4
Configuring OSPF 9-5
Verifying the Route to the SGSN 9-5
Configuring Access Points on the GGSN 9-7
Overview of Access Points 9-8
Description of Access Points in a GPRS/UMTS Network 9-8
Access Point Implementation on the Cisco GGSN 9-9
Basic Access Point Configuration Task List 9-10
Configuring the GPRS Access Point List on the GGSN 9-10
Creating an Access Point and Specifying Its Type on the GGSN 9-10
Configuring Real Access Points on the GGSN 9-11
PDN Access Configuration Task List 9-12
VPN Access Using VRF Configuration Task Lists 9-13
Configuring Additional Real Access Point Options 9-20
Verifying the Real Access Point Configuration 9-27
Configuring Virtual Access Points on the GGSN 9-32
Overview of the Virtual Access Point Feature 9-32
Virtual Access Point Configuration Task List 9-35
Verifying the Virtual Access Point Configuration 9-37
Configuring Access to External Support Servers 9-41

Blocking Access to the GGSN by Foreign Mobile Stations 9-41
Overview of Blocking Foreign Mobile Stations 9-41
Blocking Foreign Mobile Stations Configuration Task List 9-42
Configuring the MCC and MNC Values 9-42
Enabling Blocking of Foreign Mobile Stations on the GGSN 9-43
Verifying the Blocking of Foreign Mobile Stations Configuration 9-43
Controlling Access to the GGSN by MSs with Duplicate IP Addresses 9-44
Configuring Routing Behind the Mobile Station on an APN 9-45
Enabling Routing Behind the Mobile Station 9-45
Verifying the Routing Behind the Mobile Station Configuration 9-46
Configuring Proxy-CSCF Discovery Support on an APN 9-48
Creating P-CSCF Server Groups on the GGSN 9-48
Associating a P-CSCF Server Group with an APN 9-49
Verifying the P-CSCF Discovery Configuration 9-49
Monitoring and Maintaining Access Points on the GGSN 9-50
Configuration Examples 9-50
Static Route to SGSN Example 9-51
Access Point List Configuration Example 9-52
VRF Tunnel Configuration Example 9-53
Virtual APN Configuration Example 9-54
Blocking Access by Foreign Mobile Stations Configuration Example 9-57
Duplicate IP Address Protection Configuration Example 9-58
P-CSCF Discovery Configuration Example 9-58

CHAPTER 10 **Configuring PPP Support on the GGSN** 10-1
Overview of PPP Support on the GGSN 10-1
Configuring GTP-PPP Termination on the GGSN 10-3
Overview of GTP-PPP Termination on the GGSN 10-3
Benefits 10-3
Preparing to Configure PPP over GTP on the GGSN 10-4
GTP-PPP Termination Configuration Task List 10-4
Configuring a Loopback Interface 10-5
Configuring a PPP Virtual Template Interface 10-5
Associating the Virtual Template Interface for PPP on the GGSN 10-7

Configuring GTP-PPP with L2TP on the GGSN 10-7
Overview of GTP-PPP with L2TP on the GGSN 10-7
Benefits 10-8
Restrictions 10-8
GTP-PPP With L2TP Configuration Task List 10-8
Configuring the GGSN as a LAC 10-9
Configuring AAA Services for L2TP Support 10-10
Configuring a Loopback Interface 10-11
Configuring a PPP Virtual Template Interface 10-12
Associating the Virtual Template Interface for PPP on the GGSN 10-13
Configuring GTP-PPP Regeneration on the GGSN 10-14
Overview of GTP-PPP Regeneration on the GGSN 10-14
Restrictions 10-14
GTP-PPP Regeneration Configuration Task List 10-15
Configuring the GGSN as a LAC 10-16
Configuring AAA Services for L2TP Support 10-17
Configuring a PPP Virtual Template Interface 10-18
Associating the Virtual Template Interface for PPP Regeneration on the GGSN 10-20
Configuring PPP Regeneration at an Access Point 10-20
Monitoring and Maintaining PPP on the GGSN 10-21
Configuration Examples 10-22
GTP-PPP Termination on the GGSN Configuration Examples 10-22
GTP-PPP–Over–L2TP Configuration Example 10-24
GTP-PPP Regeneration Configuration Example 10-25
AAA Services for L2TP Configuration Example 10-26

CHAPTER 11 **Configuring QoS on the GGSN** 11-1
Overview of QoS Support on the GGSN 11-1
Configuring UMTS QoS on the GGSN 11-2
Overview of UMTS QoS 11-2
Configuring UMTS QoS Task Lists 11-4
Enabling UMTS QoS Mapping on the GGSN 11-4
Mapping UMTS QoS Traffic Classes to a DiffServ PHB Group 11-4
Assigning a DSCP to a DiffServ PHB Group 11-5
Configuring the DSCP in the Subscriber Datagram 11-7
Configuring the Cisco 7600 Platform GGSN UMTS QoS Requirements 11-8
Verifying the UMTS QoS Configuration 11-11
Configuring the GGSN Default QoS as Requested QoS 11-13

Configuring Call Admission Control on the GGSN 11-13
Configuring Maximum QoS Authorization 11-13
Configuring a CAC Maximum QoS Policy 11-14
Enabling the CAC Maximum QoS Policy Function and Attaching a Policy to an APN 11-15
Configuring Bandwidth Management 11-16
Configuring a CAC Bandwidth Pool 11-16
Enabling the CAC Bandwidth Management Function and Applying a Bandwidth Pool to an APN 11-16
Configuring Per-PDP Policing 11-17
Restrictions 11-18
Per-PDP Policing Configuration Task List 11-18
Creating a Class Map with PDP Flows as the Match Criterion 11-18
Creating a Policy Map and Configuring Traffic Policing 11-19
Attaching the Policy to an APN 11-20
Resetting APN Policing Statistics 11-20
Monitoring and Maintaining QoS on the GGSN 11-20
show Command Summary 11-20
Monitoring UMTS QoS 11-21
Displaying UMTS QoS Status on the GGSN 11-21
Displaying UMTS QoS Information for a PDP Context 11-21
Configuration Examples 11-22
UMTS QoS Configuration Examples 11-22
CAC Configuration Example 11-24
Per-PDP Policing Configuration Example 11-25

CHAPTER 12 **Configuring Security on the GGSN** 12-1
Overview of Security Support on the GGSN 12-2
AAA Server Group Support 12-2
Configuring AAA Security Globally 12-4
Configuring RADIUS Server Communication Globally 12-5
Configuring RADIUS Server Communication at the GGSN Configuration Level 12-6
Configuring Non-Transparent Access Mode 12-6
Specifying an AAA Server Group for All Access Points 12-7
Specifying an AAA Server Group for a Particular Access Point 12-8
Configuring AAA Accounting Services at an Access Point 12-8

Configuring Additional RADIUS Services 12-10
Configuring RADIUS Attributes in Access Requests to the RADIUS Server 12-11
Configuring the CHAP Challenge 12-11
Configuring the MSISDN IE 12-11
Configuring the NAS-Identifier 12-11
Configuring the Charging ID in the Acct-Session-ID Attribute 12-12
Configuring the MSISDN in the User-Name Attribute 12-12
Configuring the Vendor-Specific Attribute in Access Requests to the RADIUS Server 12-13
Suppressing Attributes for RADIUS Authentication 12-14
Suppressing the MSISDN Number for RADIUS Authentication 12-15
Suppressing the 3GPP-IMSI VSA Sub-Attribute for RADIUS Authentication 12-16
Suppressing the 3GPP-GPRS-QoS Profile VSA Sub-Attribute for RADIUS Authentication 12-16
Suppressing the 3GPP-GPRS-SGSN-Address VSA Sub-Attribute for RADIUS Authentication 12-17
Obtaining DNS and NetBIOS Address Information from a RADIUS Server 12-17
Configuring the RADIUS Packet of Disconnect 12-17
Configuring the GGSN to Wait for a RADIUS Response 12-19
Configuring Access to a RADIUS Server Using VRF 12-20
Enabling AAA Globally 12-21
Configuring a VRF-Aware Private RADIUS Server Group 12-22
Configuring Authentication, Authorization, and Accounting Using Named Method Lists 12-23
Configuring a VRF Routing Table 12-23
Configuring VRF on an Interface 12-23
Configuring VRF Under an Access Point for Access to the Private RADIUS Server 12-24
Configuring a Route to the RADIUS Server Using VRF 12-27
Configuring RADIUS Change of Authorization Support 12-29
Securing the GGSN Gn Interface 12-29
Configuring Address Verification 12-30
Configuring Mobile-to-Mobile Traffic Redirection 12-31
Redirecting All Traffic 12-31
Segregating GRX Traffic on GGSN Gn Interface 12-32
Configuring Simultaneous Broadcast and Wait Accounting 12-32
Periodic Accounting Timer 12-34
Configuring a Default GGSN Periodic Accounting Timer 12-35
Configuring an APN-Level Periodic Accounting Timer 12-36

Implementing Lawful Intercept Support on the Cisco GGSN 12-37
Lawful Intercept Overview 12-37
Network Components Used for Lawful Intercept 12-38
Lawful Intercept Processing 12-39
Lawful Intercept MIBs 12-40
Lawful Intercept Topology 12-41
Configuring Lawful Intercept Support 12-41
Prerequisites 12-42
Security Considerations 12-42
Configuration Guidelines and Limitations 12-42
Accessing the Lawful Intercept MIBs 12-43
Configuring SNMPv3 12-44
Creating a Restricted SNMP View of Lawful Intercept MIBs 12-44
Configuring the Cisco GGSN to Send SNMP Notifications for Lawful Intercept 12-46
Disabling SNMP Notifications 12-46
Configuration Examples 12-46
AAA Security Configuration Example 12-47
RADIUS Server Global Configuration Example 12-47
RADIUS Server Group Configuration Example 12-47
RADIUS Response Message Configuration Example 12-49
Address Verification and Mobile-to-Mobile Traffic Redirection Example 12-50
Access to a Private RADIUS Server Using VRF Configuration Example 12-52
Periodic Accounting Timer Example 12-53

CHAPTER 13 **Configuring Dynamic Addressing on the GGSN** 13-1
Overview of Dynamic IP Addressing on the GGSN 13-1
Configuring DHCP on the GGSN 13-2
Configuring DHCP Server Communication Globally 13-3
Configuring DHCP at the GGSN Global Configuration Level 13-4
Configuring a Loopback Interface 13-4
Specifying a DHCP Server for All Access Points 13-5
Specifying a DHCP Server for a Particular Access Point 13-6
Configuring a Local DHCP Server 13-8
Configuration Example 13-8
Configuring MS Addressing via Local Pools on the GGSN 13-10
Configuration Example 13-12

Configuring MS Addressing via RADIUS 13-12
Configuring IP Overlapping Address Pools 13-12
Configuration Examples 13-13
Defining Local Address Pooling as the Global Default 13-14
Configuring Multiple Ranges of IP Addresses into One Pool Example 13-14
Configuring IP Overlapping Address Pools on a GGSN on the Cisco 7600 Platform with Supervisor II / MSFC2 Example 13-14
Configuring the NBNS and DNS Address for an APN 13-16
Using Dynamic IP Address Management on the Cisco GGSN 13-16
Enabling Subnet Management in an eGGSN Environment with Cisco CSG2 13-17
Enabling Subnet Management in a Non eGGSN Environment 13-17

CHAPTER 14 **Configuring Load Balancing on the GGSN** 14-1
Overview of GTP Load Balancing 14-1
Overview of Cisco IOS SLB 14-1
Overview of GTP Load Balancing 14-2
Supported GTP Load Balancing Types 14-3
Cisco IOS SLB Algorithms Supported for GTP Load Balancing 14-4
Dynamic Feedback Protocol for Cisco IOS SLB 14-5
GTP IMSI Sticky Database Support 14-6
GTP APN-Aware Load Balancing 14-7
GTP SLB Restrictions 14-7
Configuring GTP Load Balancing 14-7
GTP Load Balancing Configuration Task List 14-8
Configuration Guidelines 14-8
Configuring the Cisco IOS SLB for GTP Load Balancing 14-9
Configuring a Server Farm and Real Server 14-9
Configuring a Virtual Server 14-11
Configuring a GSN Idle Timer 14-14
Configuring DFP Support 14-14
Configuring GTP APN-Aware Load Balancing 14-15
Verifying the Cisco IOS SLB Configuration 14-18
Configuring the GGSN for GTP Load Balancing 14-19
Configuring a Loopback Interface for GTP SLB 14-19
Configuring DFP Support on the GGSN 14-20
Configuring Messaging from the GGSN to the Cisco IOS SLB 14-21

Monitoring and Maintaining the Cisco IOS SLB Feature 14-25
Configuration Examples 14-26
Cisco IOS SLB Configuration Example 14-26
GGSN1 Configuration Example 14-28

APPENDIX A **Monitoring Notifications** A-1
SNMP Overview A-1
MIB Description A-2
SNMP Notifications A-2
SNMP Versions A-3
SNMPv1 and SNMPv2c A-4
SNMPv3 A-4
SNMP Security Models and Levels A-4
Requests for Comments A-5
Object Identifiers A-5
Related Information and Useful Links A-5
TAC Information and FAQs A-6
SNMP Configuration Information A-6
Configuring MIB Support A-6
Determining MIBs Included for Cisco IOS Releases A-6
Downloading and Compiling MIBs A-7
Considerations for Working with MIBs A-7
Downloading MIBs A-8
Compiling MIBs A-8
Enabling SNMP Support A-9
Enabling and Disabling SNMP Notifications A-9
Enabling and Disabling GGSN Notifications via the CLI A-9
Enabling and Disabling GGSN SNMP Notifications via SNMP A-10
GGSN Notifications A-11
Global Notifications A-12
Service-Aware Billing Notifications A-14
Charging Notifications A-15
Access-Point Notifications A-16

GTP Notification **A-17**
Alarm Notifications **A-17**
cGgsnGlobalErrorNotif **A-19**
cGgsnAccessPointNameNotif **A-20**
cGgsnPacketDataProtocolNotif **A-22**
CgprsCgAlarmNotif **A-24**
cgprsAccPtCfgNotif **A-26**

About This Book

This preface describes who should read the *Cisco GGSN Release 10.1 Configuration Guide, Cisco IOS Release 12.4(24)YE3*, how it is organized, and its document conventions.

Document Revision History

The following table lists the major changes made to this document each release, with the most recent changes listed first.

Revision	Date	Change Summary
OL-19936-06	2/24/2011	Release 10.1, Cisco IOS 12.4(24)YE3. Information for the following features was added: • RADIUS Controlled Redirection • Enhancements to the **show gprs gtp pdp-context msidn** command output.
OL-19936-05	12/07/2010	Release 10.0, Cisco IOS 12.4(24)YE2. Information for the "Overlapping Local IP Address Pools" feature was added.
OL-19936-04	02/25/2010	Release 10.0, Cisco IOS 12.4(24)YE. Information for the following features was added: • Single IP operation and management of the Cisco SAMI • Enhanced prepaid subscriber features • Dynamic IP address management • Cisco Content Services Gateway - 2nd Generation (CSG2) load balancing • Online Charging System (OCS) load balancing
OL-19936-03	12/07/2009	Release 9.2, Cisco IOS 12.4(22)YE2. Enhanced Quota Server Interface feature information was added.

Revision	Date	Change Summary
OL-19936-02	08/04/2009	Release 9.0, Cisco IOS 12.4(22)YE1. Layer 3 Geographical Redundancy and Passive Route Suppression feature information was added.
OL-19936-01	04/15/2009	First publication.

Audience

This publication is designed for network administrators and other people who are responsible for setting up, installing, configuring, and operating the Cisco Gateway GPRS Support Node (GGSN).

Organization

This publication is organized as follows:

Chapter	Description
Chapter 1, “Overview of GPRS and UMTS”	Briefly introduces the 2.5G general packet radio service (GPRS) and the 3G Universal Mobile Telecommunications System (UMTS) technologies, and their implementation in Cisco GGSN software
Chapter 3, “Planning to Configure the GGSN”	This chapter provides information that you should know before configuring a Cisco GGSN.
Chapter 4, “Configuring GTP Services on the GGSN”	Describes how to enable a Cisco GGSN and how to configure GPRS tunneling protocol (GTP) options.
Chapter 5, “Configuring IPv6 PDP Support on the GGSN”	Describes how to configure support for Internet Protocol Version 6 (IPv6) packet data protocol (PDP) contexts on a Cisco GGSN.
Chapter 6, “Configuring GGSN GTP Session Redundancy”	Describes how to configure GTP session redundancy (GTP-SR) between two GGSNs.
Chapter 7, “Configuring Charging on the GGSN”	Describes how to configure the charging function on a gateway GPRS support node (GGSN).
Chapter 8, “Implementing Enhanced Service-Aware Billing”	Describes how to implement the Cisco GGSN as a enhanced service-aware GGSN that is capable of real-time credit-control for prepaid subscribers and service-aware billing for postpaid and prepaid subscribers.
Chapter 9, “Configuring Network Access to the GGSN”	Describes how to configure access from the Cisco GGSN to a serving GPRS support node (SGSN), public data network (PDN), and optionally to a Virtual Private Network (VPN). This chapter also includes information about configuring access points on the GGSN.
Chapter 10, “Configuring PPP Support on the GGSN”	Describes the different methods of Point-to-Point Protocol (PPP) support on the GGSN and how to configure those methods.
Chapter 11, “Configuring QoS on the GGSN”	Describes how to configure Quality of Service (QoS) functions to differentiate traffic flow through the Cisco GGSN.
Chapter 12, “Configuring Security on the GGSN”	Describes how to configure security features on the Cisco GGSN, including Authentication, Authorization, and Accounting (AAA), and Remote Authentication Dial-In User Service (RADIUS).
Chapter 13, “Configuring Dynamic Addressing on the GGSN”	Describes how to configure dynamic IP addressing on the Cisco GGSN.
Chapter 14, “Configuring Load Balancing on the GGSN”	Describes how to configure a Cisco GGSN to support load balancing functions using the Cisco IOS software Server Load Balancing (SLB) feature.
Appendix A, “Monitoring Notifications”	Describes enabling and monitoring Cisco GGSN SNMP notifications in order to manage GPRS/UMTS-related issues.

Conventions

This publication uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information that the system displays are in `screen` font.
`boldface screen` font	Information that you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Tips use the following conventions:

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information.

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

For more detailed installation and configuration information, see the following publications:

- *Release Notes for Cisco GGSN Release 10.0 on the Cisco SAMI*, Cisco IOS Release 12.4(24)YE
- *Cisco Service and Application Module for IP User Guide*
- *Cisco IOS Network Management Configuration Guide*
- *Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers*
- *Cisco 7600 Series Cisco IOS Software Configuration Guide*
- *Cisco 7600 Series Cisco IOS Command Reference*
- *Cisco IOS Quality of Service Solutions Configuration Guide*, Cisco IOS Release 12.4
- For information about MIBs, see:

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
- Cisco IOS Configuration Guides and Command References, Release 12.4

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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, page 1-1
- Benefits, page 1-5
- Features Introduced in Cisco IOS Release 12.4(24)YE3, page 1-6
- Features Introduced in Cisco IOS Release 12.4(24)YE2, page 1-6
- Features Introduced in Cisco IOS Release 12.4(24)YE, page 1-6
- Features Introduced in Prior Releases, page 1-8

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 multimedia 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)

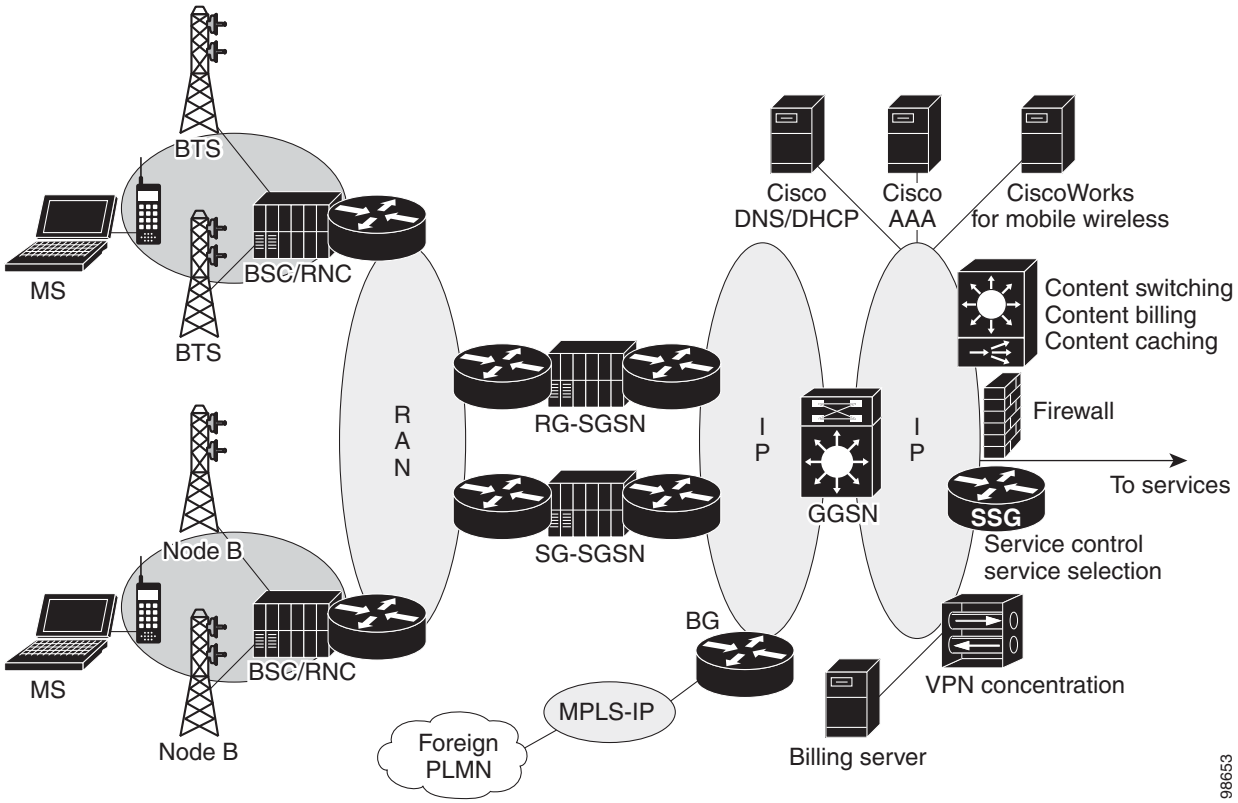
  Connects the radio access network (RAN) to the GPRS/UMTS core. The SGSN:

  - 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 Service and Application Module for IP (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 subscribers. 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.

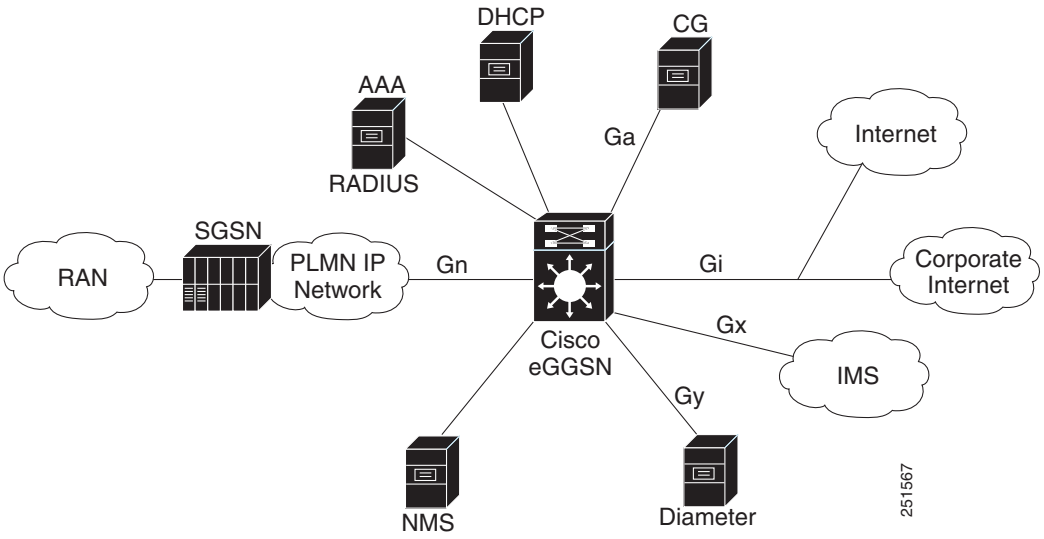
GPRS Interface Reference Model

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 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 and Charging Control (PCC) rules. The Gx interface uses the Diameter protocol.
- AAA Interface—Interface to Authentication, Authorization, and Accounting (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, such as 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 subscriber 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, see the "Configuring Access Points on the GGSN" section on page 9-7.

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. The packet-based air interface 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 in addition to GSM, which is currently widely deployed
- Supports data rates that are faster than rates 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(24)YE3

Cisco GGSN Release 10.1, Cisco IOS Release 12.4(24)YE3 introduces support for RADIUS Controlled Redirection.

The RADIUS Controlled HTTP Redirection feature enables the Cisco GGSN to redirect the HTTP traffic of subscribers to an Advice-of-Charge (AoC) page that notifies them of new tariff changes when they are roaming in a foreign PLMN.

For information about configuring RADIUS controlled HTTP redirection, see "Configuring RADIUS Controlled HTTP Redirection" section on page 8-40.

Features Introduced in Cisco IOS Release 12.4(24)YE2

Support for the following feature is introduced in Cisco GGSN Release 10.0, Cisco IOS Release 12.4(24)YE2:

- Overlapping Local IP Address Pools

  For information about configuring overlapping local IP address pools, see "Configuring Overlapping Local IP Address Pools" section on page 12.

Features Introduced in Cisco IOS Release 12.4(24)YE

Support for the following features is introduced in Cisco GGSN Release 10.0, Cisco IOS Release 12.4(24)YE:

- Single IP operation and management of the Cisco SAMI

  Cisco GGSN Release 10.0 and later supports a Single IP architecture. The Single IP architecture enables a single view of the Cisco GGSN external interfaces (for example, the Gi, Gn, Ga, iSCSI, AAA, Diameter, etc.) and a single point of configuration and operation.

  For information about the Single IP architecture, see Chapter 2, "Overview of the Single IP Cisco GGSN."

- Enhanced prepaid subscriber features
  - Dynamic HTTP redirection and termination with Final Unit Indication (FUI)
  - Activity-based time billing—Activity-based billing, as defined in 3GPP, bills users for only the periods of on the network that activity is occurring, instead of billing them for the entire time they are logged on the network.

  For about configuring these enhanced prepaid subscriber features, see the "Configuring Activity-Based Time Billing for Prepaid Subscribers" section on page 8-36 and the "Configuring FUI-Based HTTP Redirection" section on page 8-37.

- Dynamic IP address management

  With Release 10.0 and later, the Cisco GGSN supports dynamic IP address allocation. Dynamic IP address allocation enables operators to implement a Cisco GGSN without subnetting requirements. The Cisco GGSN supports dynamic IP address allocation from DHCP, RADIUS, and local pools.

  For information about dynamic IP address management, see the "Using Dynamic IP Address Management on the Cisco GGSN" section on page 13-17.

- Cisco CSG2 load balancing

  With the advent of a Single IP architecture of Cisco GGSN Release 10.0 and later, the Cisco GGSN quota server interface supports multiple Cisco CSG2s. Service-aware users from the Cisco GGSN are load-balanced among the Cisco CSG2s.

  For information on Cisco CSG2 load balancing, see the "Configuring Cisco CSG2 Load Balancing" section on page 8-43.

- Online Charging System (OCS) load balancing

  In earlier releases of the Cisco GGSN, you could configure only one DCCA server at a time per APN, however, you could configure different DCCA servers for the same APN on the GGSN instances on the Cisco SAMI.

  With the transition to a single IP architecture in Cisco GGSN Release 10.0, the separate GGSN instances running on the six Cisco SAMI processors function as a single GGSN. To enable an APN to communicate with multiple DCCA servers, with Cisco GGSN Release 10.0 and later, you can configure multiple DCCA profiles under a charging profile that is applied to an APN.

  For information about OCS load balancing, see the "Specifying a DCCA Profile for Online Billing" section on page 8-26.

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
- Multiple APNs per VRF instance
- VPN support
  - Virtual APNs
  - VPN routing and forwarding (VRF) per APN
  - 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
- 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
  - iSCSI
- RADIUS Change of Authorization (CoA) message support for dynamically change session authorizations.
- Downloadable QoS Profile (from an AAA server)
- PPP-Regeneration Scalability and Anonymous User Access for PPP-Regeneration
- Downloadable Pool Name Support
- 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 processes both signaling traffic (to track 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 continues 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 when a prepaid system asks the SGSN to count the traffic flow.

- Granular Charging and Storage
- GRX Traffic Segregation
- Gx Interface Support
- Gy Interface Support
- Lawful Intercept
- Proxy-CSCF Load Balancing
- Standalone GGSN Prepaid Quota Enforcement
- Verbosity and Next Call Conditional Debugging
- HSPA QoS Extensions
- Multiple Subnets Behind the Mobile Station
- Layer 3 Geographical Redundancy
- Passive Route Suppression
- eGCDR Support for Cisco CSG2 Quota Server Configurations

CHAPTER 2

Overview of the Single IP Cisco GGSN

This chapter discusses the concepts related to the Single IP architecture and its implementation with the Cisco GGSN running on the Cisco Service and Application Module for IP (SAMI).

This chapter includes the following sections:

- Single IP Architecture and the Cisco GGSN, page 2-1
- Single IP Components and Concepts, page 2-3
- Single IP Cisco GGSN Usage Notes and Prerequisites, page 2-8

Single IP Architecture and the Cisco GGSN

With the Single IP architecture, the Cisco GGSN Release 10.0 and later on the Cisco SAMI runs on each of the Cisco SAMI PowerPCs (PPCS) like in prior releases, however, the user can configure, manage, and troubleshoot their Cisco GGSN from a single PPC instead of having to establish a session with each of PPCs to configure the Cisco GGSN instance on that PPC.

The Single IP architecture redesigns the functionality of the Cisco SAMI from a model of six independent PPCs, each executing both control and traffic plane functions, to a model where Cisco SAMI PPC3 functions as a Proxy Control Processor (PCOP), and PPCs 4 through 8 function as Traffic and Control Plane processors (TCOPs). The user has to establish only a session with the PCOP to perform all Cisco GGSN related operations.

The Single IP architecture enables a single view of the Cisco GGSN external interfaces (for example, the Gi, Gn, Ga, iSCSI, AAA, Diameter, etc.) and a single point for the following:

- Configuring the Cisco GGSN
- Managing the Cisco GGSN
- Troubleshooting and debugging the Cisco GGSN

Although transparent from the user perspective, to achieve a view of a single GGSN across six different PPCs, the SingleIP architecture incorporates enhancements, or in some cases new functionality, in the following areas:

- Load balancing of sessions across available traffic-handling PPCs.
- Distribution of address pools across available traffic-handling PPCs.

- Distributed application/protocol and interface endpoints across PPCs.
  - UDP—Gn, Ga (charging gateway), Cisco Content Services Gateway - 2nd Generation (CSG2), DNS, DHCP
  - TCP—Ga (charging gateway), Gy (Diameter), Internet Small Computer System Interface (iSCSI)
  - SCTP—Redundancy
- Redundancy state sharing and session state synchronization across PPCs.

Figure 2-1 is a high level representation of the Single IP Cisco GGSN.

Figure 2-1 High Level Representation of Single IP GGSN

In Figure 2-1, using Interprocessor Communication Protocol (IPC), the PCOP distributes configuration information to and aggregates the data received from the TCOPs. When requested, the TCOPs send counter updates to the PCOP.

Note As perceived by external systems, the Cisco GGSN does not change. The Single IP Cisco GGSN looks and feels the same as a non-single IP implementation of the Cisco GGSN executing on a single processor. Additionally, the configuration tasks of the Cisco GGSN do not change from the operator perspective.

Single IP Components and Concepts

The following sections provide an overview of some Single IP components and concepts:

- Single IP Interface, page 2-3
- Session Load Balancing, page 2-4
- Address Pool Management, page 2-4
- Distributed Endpoints, page 2-5
- Distributed Command Line Interface, page 2-5
- Redundancy State Sharing, page 2-8

Single IP Interface

A Single IP architecture enables the support of a single IP address across the Cisco GGSN instances running on the Cisco SAMI PPCs for each the following interfaces:

- Authentication, Authorization, and Accounting (AAA)
- Dynamic Host Configuration Protocol (DHCP)/Domain Name System (DNS)
- Internet Small Computer System Interface (iSCSI)
- Failover
- Charging gateway (Ga)
- Internet/Corporate (Gi)
- Policy Control (Gy)
- Cisco CSG2 (Gx)

In addition the support of a single IP address configuration for the interfaces listed above, Single IP architectures enables the following:

- Single Interface for Configuration, page 2-3
- Single Interface for Troubleshooting and Maintaining, page 2-4
- Single Interface for Network Management, page 2-4

Single Interface for Configuration

The Single IP Cisco GGSN provides a single point from which a user can configure the Cisco GGSN.

From PPC3, a user can configure the Cisco GGSN features across the Cisco SAMI PPCs with a single execution of each command required for a feature. A *distributed CLI agent* propagates the configuration to the TCOPs (PPCs 4 through 8) without the user having to perform any additional configuration tasks.

Configuration information is propagated to the TCOPs by the distributed CLI agent using IPC messaging between the PCOP and the TCOPs.

By default, all of the Cisco GGSN configuration tasks and associated commands that the user executes from the PCOP are propagated to, and take effect on, all of the TCOPs, except for commands that configure functionality on a TCOP that should be configured only on the PCOP.

For a list of the specific tasks, and their associated commands, that are not propagated to the TCOPs, and are only configured on the PCOP, see "Distributed Configuration Commands" section on page 2-5.

Single Interface for Troubleshooting and Maintaining

The Single IP Cisco GGSN provides a single point from which the user can troubleshoot and maintain the Cisco GGSN. From a session with PPC3, the user can troubleshoot, debug, and maintain the Cisco GGSN using **show**, **debug**, and **clear** commands.

When using **show** and **debug** commands:

- **show** commands for which command output is identical from all the PPCs, the execution of the command is limited to the PCOP. These commands do not require information to be collected from the TCOPs and/or aggregated at the PCOP. The output for these **show** commands is unchanged from non-single IP versions of the Cisco GGSN.
- For commands that require additional information from a TCOP, the TCOP is identified and the command propagated to the specific TCOP.
- For **show** commands that display global statistics, the statistics are collected from all of he TCOPs, and combined into a single output display by PCOP. The output for these **show** commands is unchanged from non-single IP versions of the Cisco GGSN.

By default, all of the Cisco GGSN **debug** commands are executed on the TCOPs and the trace is displayed on the PCOP. The PCOP does not perform any aggregation for distributed **debug**.

Single Interface for Network Management

The Single IP Cisco GGSN supports a single IP address as the target address for Simple Network Management Protocol (SNMP) operations. When the user configures the IP address for SNMP operations on the Cisco GGSN, all MIBs on the Cisco SAMI that are related to the Cisco GGSN functionality are accessible through the IP address.

Single IP GGSN supports distributed SNMP MIB support. Information required from Cisco SAMI PPCs other than PPC3 is either pushed to or pulled from the PPCs, depending on the MIB target.

For more information about SNMP and the Cisco GGSN, see Appendix A, “Monitoring Notifications.”

Session Load Balancing

Using the *session manager* function, PPC3 load balances and determines to which TCOP to assign the new session.

The PPC3 only chooses a TCOP for a session. The session manager session load balancing function maintains information about the TCOP selected to host a user in a *user session table*. Once the user session is established on a TCOP, all data plane packets from that same mobile subscriber are directed to the same TCOP.

Address Pool Management

Although local-pool addresses are configured on the PPC3, the same address pools are available at each TCOP. The Cisco GGSN utilizes a client-server approach with address caching at the TCOP.

Note For IPv4 address pool management support on the Cisco GGSN Release 10.0 and later, configure the Cisco SAMI **sami addr-pool cache** command.

Distributed Endpoints

Applications which use UDP for communication are assigned the source port ranges to identify the right TCOP. This port range can be configured on the PCOP and the PCOP equally distributes to the TCOPs.

To configure the port range on the PCOP, use the Cisco SAMI **sami balance port** command. For information about the **sami balance port** command, see *Cisco Service and Application Module for IP User Guide*.

The PCOP propagates RADIUS related configuration to the TCOPs, and the source port range is allocated to each TCOP during start up. The TCOPs use the source port from the given range for sending Authentication and Accounting messages so that the responses are forwarded to the correct TCOP.

To enable 200 ports in the range from 21645 to 21844 that will be propagated to the TCOPs to be used as the source ports for sending out RADIUS requests, use the **radius-server source-ports extended** command in global configuration mode.

Distributed Command Line Interface

The Single IP Cisco GGSN utilizes a *distributed CLI agent* at PPC3 to distribute configuration information to and retrieve information from the TCOPs using IPC.

The distributed CLI applies to the following types of commands:

- Distributed Configuration Commands, page 2-5
- Distributed Privileged EXEC Commands, page 2-7

Note When using the Single IP Cisco GGSN, if the user attempts to establish a session to a PPC other than the PCOP (PPC3), an EXEC banner displays that warns them to be aware that all “normal” maintenance activities should be run from the PCOP.

Distributed Configuration Commands

By default, the distributed CLI agent propagates all configuration commands to the TCOPs, except for commands that might configure some functionality on the TCOP that belongs only on the PCOP.

The following commands, listed below by their associated task, are only executed on PPC3:

- Configuring a Local IPv6 Prefix Pool
  - **ipv6 local pool** (global configuration)—Configures a local IPv6 prefix pool.
- Enabling HSRP and Configuring an HSRP Primary Group
  - **standby version 2** (interface configuration)—Changes the HSRP version to HSRP Version 2.
  - **standby ip** (interface configuration)—Enables HSRP on the interface
  - **standby priority** (interface configuration)—Set the Hot Standby priority used in choosing the active router. The priority value range is from 1 to 255, where 1 denotes the lowest priority and 255 denotes the highest priority. Specify that, if the local router has priority over the current active router, the local router should attempt to take its place as the active router.
  - **standby name** (interface configuration)—Specifies the name of the standby group.
  - **standby use-bia** (interface configuration)—Configures HSRP to use the burned-in address of an interface as its virtual MAC address instead of the preassigned MAC address.

- Configuring HSRP Follow Groups
  - **standby follow** (interface configuration)—Specifies the number of the follow group and the name of the primary group to follow and share status.
  - **standby ip** (interface configuration)—Specifies the group number and virtual IP address of the follow group.
- Configuring OSPF
  - **router ospf process id** (global configuration)—Enables OSPF routing, and enters router configuration mode, where process-id specifies an internally used identification parameter for an OSPF routing process.
  - **network** (ospf configuration)—Defines an interface on which OSPF runs and defines the area ID for that interface
- Configuring MS Addressing via Local Pools on the Cisco GGSN
  - **ip local pool** (global configuration)—Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface,
- Configuring the Cisco GGSN as a Dynamic Feedback Protocol (DFP) Agent
  - **ip dfp agent gprs** (global configuration)—Identifies a DFP agent subsystem and initiates DFP agent configuration mode.
  - **interval** (dfp agent configuration)—Identifies a DFP agent subsystem and initiates DFP agent configuration mode.
  - **password** (dfp agent configuration)—(Optional) Configures a DFP agent password for MD5 authentication.
  - **port** (dfp agent configuration)—Defines the port number to be used by the DFP manager to connect to the DFP agent.
  - **inservice** (dfp agent configuration)—Enables the DFP agent for communication with a DFP manager.
- Configuring CAC Failure Notification Support when the Cisco IOS SLB is in Directed Server NAT Mode
  - **gprs slb mode directed** (global configuration)—Defines directed server NAT as the Cisco IOS SLB operation mode for GGSN-IOS SLB messaging.
  - **gprs slb vserver** (global configuration)—Configures the Cisco IOS SLB virtual server(s) to be notified by a GGSN when the condition defined using the gprs slb notify command occurs.
- Configuring Support for GGSN-Cisco IOS SLB Messaging Delete NOtification (GTP' IMSI Sticky Database)
  - **gprs slb notify session-deletion** (global configuration)—Configures the GGSN to send a delete notification message to the Cisco IOS SLB when the last PDP context associated with an IMSI is deleted.
  - **gprs slb vservers** (global configuration)—Configures the Cisco IOS SLB virtual server(s) to be notified by a GGSN when the condition defined using the gprs slb notify command occurs.

Distributed Privileged EXEC Commands

The Single IP Cisco GGSN uses the Cisco SAMI Remote Console and Logging (RCaL) interface from PPC3 to collect and display **show** and **debug** command output from the TCOPs.

To use the RCAL interface to issue **show** and **debug** commands, use the following command in global configuration mode from the PPC3:

Command	Purpose
`Router(config)# execute-on {{cpu_number [,cpu_num] | all} command}}`	Executes commands remotely when RCAL is enabled, where: •*cpu_num*—Specifies the TCOP from which the user wants to collect and display command output. Valid values 4 through 8. • **all**—Executes the command on all TCOPs (PPCs 4 through 8). • *command*—Specifies the **show** or **debug** command to execute on the TCOPs.

The following sections discuss the following types of distributed privileged EXEC commands:

- Distributed show Commands, page 2-7
- Distributed debug Commands, page 2-7
- Distributed clear Commands, page 2-7

Distributed show Commands

By default, not all **show** commands are propagated to the TCOP. For **show** commands for which the output is the same for all PPCs, the execution is restricted to the PCOP.

For **show** commands that display statistics that are local to a TCOP, the information is retrieved from the TCOP and displayed. For commands that display global statistics from all of the TCOPs, by default, the information is retrieved from all the TCOPs and aggregated at PPC3.

Distributed debug Commands

By default, all Cisco GGSN **debug** commands are propagated to the TCOPs. PPC does not aggregate any of the distributed **debug** commands.

Distributed clear Commands

By default, all Cisco GGSN **clear** commands are propagated to the TCOPs, except for the **clear gprs slb statistics** command, which is executed only on PPC3. The **clear gprs slb statistics** command clears Cisco IOS Server Load Balancing (SLB) statistics.

Redundancy State Sharing

With the Single IP Cisco GGSN, PPC3 negotiates the Hot Standby Routing Protocol (HSRP) states and the five TCOPs on their respective cards follow the events generated by the HSRP module. This enables the six PPCs on the Cisco SAMI to function as a single unit.

The TCOPs function as Cisco IOS Redundancy Framework (RF) redundant pairs. Stream Control Transmission Protocol (SCTP) endpoint connections are extended by reserving 12-contiguous ports. In the following example, ports ranging from 5000 to 5011 are reserved by RF for interdevice redundancy for creating SCTP endpoints fro RF and Check-point Facility (CF) on all six Cisco SAMI PPCs.

```
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.1.1.61
   remote-port 5000
    remote-ip 10.1.1.88
```

For information about configuring GTP Session Redundancy, see Chapter 6, "Configuring GGSN GTP Session Redundancy."

Single IP Cisco GGSN Usage Notes and Prerequisites

The following usage notes and prerequisites apply to the implementation of a Single IP GGSN:

- Single IP and IPC support must be configured on the Cisco SAMI. For information about configuring Single IP support on the Cisco SAMI, see *Cisco Service and Application Module for IP User Guide*.
- To support the Single IP architecture, the following features have been introduced:
  - Using Dynamic IP Address Management on the Cisco GGSN, page 4
  - Configuring Cisco CSG2 Load Balancing on the Cisco GGSN, page 7
  - Configuring OCS Load Balancing, page 9

The following changes exist between the non-Single IP Cisco GGSN and the Single IP Cisco GGSN:

- Configuration

  The configuration of a Single IP GGSN does not differ from a non-single IP GGSN. All configurations must be performed on the PCOP, which are then propagated to all TCOPs. Failure of the command in any of the TCOPs causes a rollback of the configuration on the PCOP and other TCOPs.

  A few values configured on the PCOP, for example the maximum number of PDP contexts, are distributed to the TCOPs as seen in the following example:

```
sup-06-3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
PPC3(config)#gprs maximum-pdp-context-allowed ?
  <5-4294967295>  Max PDP context allowed
PPC3(config)#gprs maximum-pdp-context-allowed 10000
PPC3(config)#end
PPC3#
PPC3#show run| i maximum-pdp-context-allowed
gprs maximum-pdp-context-allowed 10000
PPC3#execute-on all sh run | i maximum-pdp-context-allowed
```

```
gprs maximum-pdp-context-allowed 2000
gprs maximum-pdp-context-allowed 2000
gprs maximum-pdp-context-allowed 2000
gprs maximum-pdp-context-allowed 2000
gprs maximum-pdp-context-allowed 2000
PPC3#
```

- **show** Command Displays

  The display of most **show** commands are aggregated to display consolidated outputs of all the TCOPs. However, a few **show** commands display the outputs from each TCOP.

  For example, the **show ip iscsi session** command displays output from all TCOPs:

```
PPC3#show ip iscsi session
----------- Slot 6/CPU 3, show ip iscsi session -------------

ID        TARGET             STATE                CONNECTIONS
-----------------------------------------------------------------
8         LINUX              Logged In            1
----------- Slot 6/CPU 4, show ip iscsi session -------------

ID        TARGET             STATE                CONNECTIONS
-----------------------------------------------------------------
7         LINUX              Logged In            1
----------- Slot 6/CPU 5, show ip iscsi session -------------

ID        TARGET             STATE                CONNECTIONS
-----------------------------------------------------------------
7         LINUX              Logged In            1
----------- Slot 6/CPU 6, show ip iscsi session -------------

ID        TARGET             STATE                CONNECTIONS
-----------------------------------------------------------------
7         LINUX              Logged In            1
----------- Slot 6/CPU 7, show ip iscsi session -------------

ID        TARGET             STATE                CONNECTIONS
-----------------------------------------------------------------
7         LINUX              Logged In            1
----------- Slot 6/CPU 8, show ip iscsi session -------------

ID        TARGET             STATE                CONNECTIONS
-----------------------------------------------------------------
7         LINUX              Logged In            1
PPC3#
```

  Whereas, the **show gprs iscsi statistics** command aggregates the output from all TCOPs as seen in the following example:

```
PPC3#show gprs iscsi statistics
GPRS iSCSI statistics for iSCSI Profile LINUX:
    Profile Name: LINUX
    Open Requests  = 5       ,    Failed Open Attempts  = 0
    Write Requests = 0       ,    Failed Write Requests = 0
    Read Requests  = 5       ,    Failed Read Requests  = 5
    Close Requests = 0       ,    Failed Close Requests = 0
    Number of DTRs in Write Queue = 0
    Number of DTRs in Read Queue = 0
PPC3#
```

- RADIUS

  For RADIUS responses to reach the correct TCOP, the following configuration on the Cisco GGSN is mandatory:

```
PPC3(config)#radius-server source-ports extended
```

- iSCSI

  a. The file systems for ISCSI storage are not visible on the PCOP. To view the file systems, execute the command on all TCOPs using the **execute-on all sh file systems** command:

```
PPC3#show file systems
File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
             -             -   network     rw   snmp:
             -             -    opaque     rw   null:
             -             -   network     rw   tftp:
*     27740160      27736064     flash     rw   bootflash:
       131072        128947     nvram     rw   nvram:
             -             -    opaque     wo   syslog:
             -             -   network     rw   rcp:
             -             -   network     rw   ftp:
             -             -   network     rw   http:
             -             -   network     rw   scp:
             -             -    opaque     ro   tar:
             -             -   network     rw   https:
             -             -    opaque     ro   cns:

PPC3#execute-on all show file systems
----------- Slot 6/CPU 4, show  file systems-------------

File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
             -             -   network     rw   snmp:
             -             -    opaque     rw   null:
             -             -   network     rw   tftp:
*     27740160      27736064     flash     rw   bootflash:
       131072        129996     nvram     rw   nvram:
             -             -    opaque     wo   syslog:
             -             -   network     rw   rcp:
             -             -   network     rw   ftp:
             -             -   network     rw   http:
             -             -   network     rw   scp:
             -             -    opaque     ro   tar:
             -             -   network     rw   https:
             -             -    opaque     ro   cns:
    3217522688    3217506304      disk     rw   sda0:#


----------- Slot 6/CPU 5, show  file systems-------------

File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   archive:
```

```
                -             -    opaque     rw   system:
                -             -    opaque     rw   tmpsys:
                -             -   network     rw   snmp:
                -             -    opaque     rw   null:
                -             -   network     rw   tftp:
*      27740160      27736064     flash     rw   bootflash:
         131072        129996     nvram     rw   nvram:
                -             -    opaque     wo   syslog:
                -             -   network     rw   rcp:
                -             -   network     rw   ftp:
                -             -   network     rw   http:
                -             -   network     rw   scp:
                -             -    opaque     ro   tar:
                -             -   network     rw   https:
                -             -    opaque     ro   cns:
     3217522688    3217506304      disk     rw   sda1:#


----------- Slot 6/CPU 6, show  file systems-------------

File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
                -             -    opaque     rw   archive:
                -             -    opaque     rw   system:
                -             -    opaque     rw   tmpsys:
                -             -   network     rw   snmp:
                -             -    opaque     rw   null:
                -             -   network     rw   tftp:
*      27740160      27736064     flash     rw   bootflash:
         131072        129996     nvram     rw   nvram:
                -             -    opaque     wo   syslog:
                -             -   network     rw   rcp:
                -             -   network     rw   ftp:
                -             -   network     rw   http:
                -             -   network     rw   scp:
                -             -    opaque     ro   tar:
                -             -   network     rw   https:
                -             -    opaque     ro   cns:
     3217522688    3217506304      disk     rw   sda2:#


----------- Slot 6/CPU 7, show  file systems-------------

File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
                -             -    opaque     rw   archive:
                -             -    opaque     rw   system:
                -             -    opaque     rw   tmpsys:
                -             -   network     rw   snmp:
                -             -    opaque     rw   null:
                -             -   network     rw   tftp:
*      27740160      27736064     flash     rw   bootflash:
         131072        129996     nvram     rw   nvram:
                -             -    opaque     wo   syslog:
                -             -   network     rw   rcp:
                -             -   network     rw   ftp:
                -             -   network     rw   http:
                -             -   network     rw   scp:
                -             -    opaque     ro   tar:
                -             -   network     rw   https:
                -             -    opaque     ro   cns:
     3217522688    3217506304      disk     rw   sda3:#
```

```
----------- Slot 6/CPU 8, show  file systems-------------

File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
             -             -   network     rw   snmp:
             -             -    opaque     rw   null:
             -             -   network     rw   tftp:
*     27740160      27736064     flash     rw   bootflash:
        131072        129996     nvram     rw   nvram:
             -             -    opaque     wo   syslog:
             -             -   network     rw   rcp:
             -             -   network     rw   ftp:
             -             -   network     rw   http:
             -             -   network     rw   scp:
             -             -    opaque     ro   tar:
             -             -   network     rw   https:
             -             -    opaque     ro   cns:
    3217522688    3217506304      disk     rw   sda4:#

PPC3#
```

b. To format iSCSI disks from the Cisco GGSN, establish a session with the TCOP and execute the **format** command:

```
sup#session slot 6 proc 4
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.64 ... Open

    ************************************************************
    **                   !!! WARNING !!!                      **
    **                                                        **
    **  You are accessing the Traffic Processor on this       **
    **  system. It is strongly advised to use the Control     **
    **  Processor (processor 3) for any activity.             **
    **                                                        **
    **  Please contact your Cisco Technical Support           **
    **  personnel for any support in using this interface.    **
    **                                                        **
    ************************************************************

06-3-4>en
06-3-4#
06-3-4#show sda0:
-#- --length-- -----date/time------ path
1            0 Feb 08 2010 16:50:54 root
2           64 Feb 08 2010 16:50:58 root/master.dat
3            0 Feb 08 2010 16:50:56 salvage

3217506304 bytes available (16384 bytes used)

06-3-4#format sda0:
Format operation may take a while. Continue?
Format operation will destroy all data in "sda0:".  Continue? Writing Monlib
sectors..
Monlib write complete

Format: All system sectors written. OK...
```

```
Format: Total sectors in formatted partition: 6296544
Format: Total bytes in formatted partition: 3223830528
Format: Operation completed successfully.

Format of sda0: complete
06-3-4#
SAMI 6/4: Feb 24 06:36:07.129: %RSM-3-WARNING: Warning: iSCSI target in profile
LINUX cannot be used for storing/retrieving CDRs. Disk is formatted. Please
disconnect and connect to the Target.
```

- Address Pool Management

  To support IPv4 address management, the following Cisco SAMI command must be configured on the PCOP:

  ```
  PPC3(config)#sami addr-pool cache 1-300
  ```

- Configuration locking

  If any debug error messages such as “Configuration in progress. Dropping the create PDP req. Please try later!” or “APN in config lock and disallows new create” is observed, verify the configure-related PDP creation blocking using the following command in privilege EXEC mode:

  ```
  Router#show gprs configuration-lock counte

   system level lock counter: 0
   access point 1 apn1 counter:0
   access point 2 apn2 counter:0
  ```

  This command displays GGSN configuration locking counters. There are two kinds of configuration locking counters, system level locking counters and access-point locking counters. If the system level locking counter is non-zero, any create PDP context requests are blocked. If one access-point locking counter is non-zero, any create PDP context requests referred to that access point are blocked. Typically these counters are zero and a non-zero state is transient. However, if a user observes a configuration-lock counter remains in a non-zero state, use the following command to reset all of the configuration lock counters to zero.

  ```
  Router# clear gprs configuration-lock counter
  ```

  A warning message displays if there is non-zero counter.

CHAPTER 3

Planning to Configure the GGSN

This chapter provides information that you should know before configuring a gateway GPRS support node (GGSN).

This chapter includes the following sections:

- Prerequisites, page 3-1
- Restrictions, page 3-9
- Additional References, page 3-11

Prerequisites

Depending on the platform on which you are implementing a GGSN, the prerequisites vary. The sections below provide general guidelines to follow before configuring a GGSN in your network:

- Before You Begin, page 3-1
- Platform Prerequisites, page 3-2

Before You Begin

The Cisco GGSN is supported on the Cisco Service and Application Module for IP (SAMI) for the Cisco 7600 series router platform.

Before you begin to configure a GGSN, you should know which networks your mobile users will be allowed to access using the GGSN. After you identify the networks, you can plan the interfaces to configure for the networks, and plan the associated access points to those networks and configure them on the GGSN.

For example, you might want to provide user access to the Internet through a public data network (PDN), plus access to two private corporate intranets. In this case, you need to set up three access points—one to enable user access to the PDN, and one for each of the two private intranets.

Platform Prerequisites

When configuring GGSNs on the Cisco 7600 series router platform, ensure that requirements outlined in the following sections are met:

- Required Hardware and Software, page 3-2
- Required Base Configuration, page 3-3

Required Hardware and Software

Implementing the Cisco GGSN Release 9.2 on the Cisco 7600 series Internet router platform requires the following hardware and software.

- Any module that has ports to connect to the network.
- A Cisco 7600 series router and one of the following supervisor engines running Cisco IOS Release 12.2(33)SRC or later:
  - Cisco 7600 Series Supervisor Engine 720 with a Multiplayer Switch Feature Card 3 (WS-SUP720)
  - Cisco 7600 Series Supervisor Engine 720 with a Multilayer Switch Feature Card 3 and Policy Feature Card 3B (WS-SUP720-3B)
  - Cisco 7600 Series Supervisor Engine 720 with a Multilayer Switch Feature Card 3 and Policy Feature Card 3BXL (WS-SUP720-3BXL)
  - Cisco 7600 Series Supervisor Engine 32 with a Multiplayer Switch Feature Card (WS-SUP32-GE-3B) with LCP ROMMON Version 12.2(121) or later on the Cisco SAMI.
  - Cisco 7600 Series Supervisor Engine 32 with a Mutlilayer Switch Feature Card and 10 Gigabit Ethernet Uplinks (WS-SUP32-10GE-3B) with LCP ROMMON Version 12.2[121] or later on the Cisco SAMI.

  Or, one of the following Cisco 7600 series route switch processors running Cisco IOS Release 12.2(33)SRE or later
  - Cisco 7600 Series Route Switch Processor 720 with Distributed Forwarding Card 3C (RSP720-3C-GE)
  - Cisco 7600 Series Route Switch Processor 720 with Distributed Forwarding Card 3CXL (RSP720-3CXL-GE)

  For details on upgrading the Cisco IOS release running on the supervisor engine, see the "Upgrading to a New Software Release" section in the Release Notes for Cisco IOS Release 12.2SR. For information about verifying and upgrading the LCP ROMMON image on the Cisco SAMI, see *Cisco Service and Application Module for IP User Guide*.

  Note The Cisco IOS software required on the supervisor engine is dependent on the supervisor engine being used and the Cisco mobile wireless application running on the Cisco SAMI processors.

- Cisco Service and Application Module for IP (Cisco Product Number: WS-SVC-SAMI-BB-K9). The SAMI processors must be running Cisco IOS Release 12.4(24)T3a or later.

Note The Cisco GGSN software application ships preloaded on the Cisco SAMI and automatically loads onto each processor during an image upgrade. The Cisco GGSN software application supports both the Cisco SAMI 1 GB memory default and the 2 GB memory option (Cisco Product Number: MEM-SAMI-6P-2GB[=]).

- IPSec VPN Services Module (for security)

Note Certain Cisco GGSN features, such as enhanced service-aware billing and GTP-session redundancy, require additional hardware and software.

GTP-Session Redundancy

In addition to the required hardware and software above, implementing GTP-Session Redundancy (GTP-SR) requires at minimum:

- In a one-router implementation, two Cisco SAMIs in the Cisco 7600 Series Router, or
- In a two-router implementation, one Cisco SAMI in each of the Cisco 7600 Series Routers.

Enhanced Service-Aware Billing

In addition to the required hardware and software, implementing enhanced service-aware billing requires an additional Cisco SAMI running the Cisco Content Services Gateway - 2nd Generation software in each Cisco 7600 Series Router.

Required Base Configuration

After establishing connectivity from the switch to the various elements in your network, complete the following base configuration before implementing and customizing GGSNs on the Cisco SAMI.

Supervisor Engine Configuration

On the supervisor engine, ensure that the following tasks are completed:

1. A Layer 3–routed VLAN for each GGSN interface is created. For example, create a VLAN for the following interfaces:
   - Gn VLAN—Interconnects the Gn interfaces.
   - Ga VLAN—Interconnects the Ga interfaces.
   - AAA/OAM/DHCP VLAN—Interconnects the GGSN interfaces used for Authentication, Authorization, and Accounting (AAA), Operation, Administration, and Maintenance (OAM), and DHCP functions.
   - One VLAN per APN Gi interface

   You can configure the VLANs from VLAN database mode or global configuration mode. You cannot configure extended-range VLANs in VLAN database mode. You can configure extended-range VLANs only in global configuration mode.

   Note RPR+ redundancy does not support configurations entered in VLAN database mode. If you have a high-availability configuration with redundant Supervisor modules using RPR(+), configure the VLANs in global configuration mode, not in VLAN database mode; otherwise, the VLAN information will not be synchronized to the redundant Supervisor module.

To configure a VLAN from global configuration mode:

```
Sup#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Sup(config)#vlan 222
Sup(config-vlan)#end
Sup#
```

In the preceding example, VLAN 222 is a Layer 2–switched VLAN. The subnet associated with it is not known by the supervisor engine routing table. To configure VLAN 222 as a Layer 3–switched VLAN (or routed VLAN), configure a VLAN 222 interface on the supervisor engine and assign an IP address to the interface:

```
Sup# configure terminal
Sup(config)# interface vlan222
Sup(config-if)# ip address n.n.n.n mask
Sup(config-if)# no ip redirects
```

The following is an example of the VLAN configuration on the supervisor engine:

```
Sup# show running-config
!
. . .
vlan 103,110,160,200,300-301,310
!
!
interface Vlan103
 description Gn VLAN
 ip address 10.20.21.1 255.255.255.0
 no ip redirects
!
interface Vlan110
 description OAM/AAA/DHCP VLAN
 ip address 10.20.50.1 255.255.255.0
 no ip redirects
!
interface Vlan200
 description Ga Charging VLAN
 no ip address
 no ip redirects
!
interface Vlan310
 description VLAN for APN Internet
 ip address 10.20.51.1 255.255.255.0
```

For detailed information on configuring VLANs, see *Cisco 7600 Series Cisco IOS Software Configuration Guide*.

2. The Cisco IOS Software server load balancing (SLB) feature is installed and configured for GTP load balancing. For more information, see the *IOS Server Load Balancing* feature module and Chapter 14, “Configuring Load Balancing on the GGSN.”

3. Traffic is permitted to the Cisco SAMI by enabling multiple switch virtual interfaces (SVIs), assigning the VLANs to a VLAN group, and then assigning the VLAN groups to the Cisco SAMI using the following commands:

```
!
...
!
svclc multiple-vlan-interfaces
svclc module 7 vlan-group 71, 73
svclc vlan-group 71, 71
svclc vlan-group 73, 95, 100, 101
!
```

```
...
!
```

Note VLAN IDs must be consistent be the same in the supervisor engine and Cisco SAMI configurations. For more information about configuring the Cisco SAMI, refer the *Cisco Service and Application Module for IP User Guide.*

4. A static route is configured to the GGSN on PPC3:

```
...
!
ip route 10.20.30.1 255.255.255.255 10.20.21.20
!
...
```

GGSN Configuration

On the GGSN on the Cisco SAMI PPC3, ensure that:

1. A static route is configured to the supervisor engine.

```
...
!
ip route 0.0.0.0 0.0.0.0 10.20.21.1
!
...
```

2. A subinterface, on which 802.1Q encapsulation is enabled, is configured to each VLAN that you created on the supervisor engine.

   The following is an example of a Gn subinterface configuration on the GGSN to VLAN 103 configured on the supervisor engine:

```
!
...
interface GigabitEthernet0/0.2
 description Gn Interface
 encapsulation dot1Q 101
 ip address 10.1.1.72 255.255.255.0
 no cdp enable
...
!
```

   For detailed information on configuring, see the following:

   - Ga subinterfaces—"Configuring an Interface to the Charging Gateway" section on page 7-2.
   - Gn subinterfaces—"Configuring an Interface to the SGSN" section on page 9-1.
   - Gi subinterfaces— "Configuring an Interface to a PDN" section on page 9-12.

Configuration Examples

The following are base configuration examples for the supervisor engine and the Cisco GGSN.

Supervisor Engine

```
hostname 7600-a
!
boot system flash
boot device module 7 cf:4
!
svclc multiple-vlan-interfaces
```

```
svclc module 7 vlan-group 71, 73
svclc vlan-group 71, 71
svclc vlan-group 73, 95, 100, 101
vtp mode transparent
redundancy
 mode rpr-plus
 main-cpu
  auto-sync running-config
  auto-sync standard
!
power redundancy-mode combined
!
!
vlan 1
 vlan1 1002
 vlan2 1003
!
vlan 2
 name SNIFFER
!
vlan 71,95
!
vlan 100
 name Internal_Gi_for_GGSN-SAMI
!
vlan 101
 name Internal_Gn/Ga
!
vlan 165
!
vlan 302
 name Gn_1
!
vlan 303
 name Ga_1
!
vlan 1002
 vlan1 1
 vlan2 1003
!
vlan 1003
 vlan1 1
 vlan2 1002
 parent 1005
 backupcrf enable
!
vlan 1004
 bridge 1
 stp type ibm
!
vlan 1005
 bridge 1
!
interface FastEthernet8/22
 description To SGSN
 no ip address
 switchport
 switchport access vlan 302
!
interface FastEthernet8/23
 description To CGF
 no ip address
 switchport
 switchport access vlan 302
```

```
!
interface FastEthernet8/26
 description To DHCP/RADIUS Servers
 no ip address
 switchport
 switchport access vlan 95
!
interface FastEthernet8/31
 description To BackBone
 no ip address
 switchport
 switchport access vlan 71
!
interface FastEthernet9/32
 description To CORPA
 no ip address
 switchport
 switchport access vlan 165
 no cdp enable
!
!interface Vlan1
 no ip address
 shutdown
!
interface Vlan71
 description VLAN to tftpserver
 ip address 1.7.46.65 255.255.0.0
!
interface Vlan95
 description VLAN for RADIUS and DHCP
 ip address 10.2.25.1 255.255.255.0
!
interface Vlan100
 description Internal VLAN SUP-to-SAMI Gi
 ip address 10.1.2.1 255.255.255.0
!
interface Vlan101
 description VLAN to GGSN for GA/GN
 ip address 10.1.1.1 255.255.255.0
!
interface Vlan165
 description VLAN to CORPA
 ip address 165.1.1.1 255.255.0.0
!
interface Vlan302
 ip address 40.0.2.1 255.255.255.0
!
interface Vlan303
 ip address 40.0.3.1 255.255.255.0
!
router ospf 300
 log-adjacency-changes
 summary-address 9.9.9.0 255.255.255.0
 redistribute static subnets route-map GGSN-routes
 network 40.0.2.0 0.0.0.255 area 300
 network 40.0.3.0 0.0.0.255 area 300
!
ip classless
ip route 9.9.9.72 255.255.255.255 10.1.1.72
ip route 9.9.9.73 255.255.255.255 10.1.1.73
ip route 9.9.9.74 255.255.255.255 10.1.1.74
ip route 9.9.9.75 255.255.255.255 10.1.1.75
ip route 9.9.9.76 255.255.255.255 10.1.1.76
ip route 110.72.0.0 255.255.0.0 10.1.1.72
```

```
ip route 110.73.0.0 255.255.0.0 10.1.1.73
ip route 110.74.0.0 255.255.0.0 10.1.1.74
ip route 110.75.0.0 255.255.0.0 10.1.1.75
ip route 110.76.0.0 255.255.0.0 10.1.1.76
!
access-list 1 permit 9.9.9.0 0.0.0.255
!
route-map GGSN-routes permit 10
 match ip address 1
!
```

GGSN on the Cisco SAMI PPC3

```
service gprs ggsn
!
hostname 7600-7-2
!
ip cef
!
interface Loopback0
 description USED FOR DHCP gateway
 ip address 110.72.0.2 255.255.255.255
!
interface Loopback100
 description GPRS GTP V-TEMPLATE IP ADDRESS
 ip address 9.9.9.72 255.255.255.0
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.1
 description Gi
 encapsulation dot1Q 100
 ip address 10.1.2.72 255.255.255.0
!
interface GigabitEthernet0/0.2
 description Ga/Gn Interface
 encapsulation dot1Q 101
 ip address 10.1.1.72 255.255.255.0
 no cdp enable
!
interface GigabitEthernet0/0.71
 description TFTP or Backbone
 encapsulation dot1Q 71
 ip address 1.7.46.72 255.255.0.0
!
interface GigabitEthernet0/0.95
 description CNR and CAR
 encapsulation dot1Q 95
 ip address 10.2.25.72 255.255.255.0
!
interface Virtual-Template1
 description GTP v-access
 ip unnumbered Loopback100
 encapsulation gtp
 gprs access-point-list gprs
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.2.1
ip route 40.1.2.1 255.255.255.255 10.1.1.1
ip route 40.1.3.10 255.255.255.255 10.1.1.1
ip route 40.2.2.1 255.255.255.255 10.1.1.1
ip route 40.2.3.10 255.255.255.255 10.1.1.1
```

```
ip route 40.3.2.3 255.255.255.255 10.1.1.1
ip route 40.4.2.3 255.255.255.255 10.1.1.1
!
gprs access-point-list gprs
  access-point 1
   access-point-name CORPA.com
   ip-address-pool dhcp-proxy-client
   aggregate auto
   dhcp-server 10.2.25.90
   dhcp-gateway-address 110.72.0.2
!
```

Restrictions

When configuring a Cisco GGSN:

- The Cisco GGSN does not support the Cisco Express Forwarding (CEF) neighbor resolution optimization feature, which is enabled by default. Therefore, to avoid the possibility of incomplete adjacency on VLAN interfaces for the redirected destination IP address and an impact to the upstream traffic flow for PDP sessions upon startup, ensure that you configure the **no ip cef optimize neighbor resolution** command.
- The number of PDP contexts supported on a GGSN is dependent on the memory and platform in use and the GGSN configuration (for example, whether or not a method of Point to Point Protocol [PPP] is configured to forward packets beyond the terminal equipment and mobile termination, whether Dynamic Feedback Protocol [DFP] is being used or the memory protection feature is enabled, and what rate of PDP context creation will be supported).

Note DFP weighs PPP PDPs against IP PDPs. One PPP PDP is equal to eight IP PDPs, and one IPv6 PDP equals 8 IPv4 PDPs.

Table 1 lists the maximum number of PDP contexts the Cisco SAMI with the 1 GB memory option can support. Table 2 lists the maximum number the Cisco SAMI with the 2 GB memory option can support.:

Table 1 Number of PDPs Supported in 1 GB SAMI

PDP Type	Maximum Number per SAMI
IPv4	384,000
IPv6	48,000
PPP Regeneration	96,000
PPP	48,000

Table 2 Number of PDPs Supported in 2 GB SAMI

PDP Type	Maximum Number per SAMI
IPv4	816,000
IPv6	96,000

Table 2 Number of PDPs Supported in 2 GB SAMI

PDP Type	Maximum Number per SAMI
PPP Regeneration	192,000
PPP	96,000

- To avoid issues with high CPU usage, we recommend the following configurations:
  - To reduce the CPU usage during startup, disable logging to the console terminal by configuring the **no logging console** command in global configuration mode.
  - To ensure that the HSRP interface does not declare itself active until it is ready to process a peer's Hello packets, configure the delay period before the initialization of HSRP groups with the **standby delay minimum 100 reload 100 interface** configuration command under the HRSP interface.
  - To minimize issues with high CPU usage for additional reasons, such as periods of high PPP PDP processing (creating and deleting), use the **no logging event link-status** interface command to disable the notification of interface data link status changes on all virtual template interfaces of the GGSN.

```
!
interface Virtual-Template1
description GGSN-VT
ip unnumbered Loopback0
encapsulation gtp
no logging event link-status
gprs access-point-list gprs
end
```

For implementation of a service-aware GGSN, the following additional important notes, limitations, and restrictions apply:

- RADIUS accounting is enabled between the CSG2 and GGSN to populate the Cisco CSG2 User Table entries with the PDP context user information.
- CSG2 must be configured with the quota server address of the GGSN.
- Service IDs on the CSG2 are configured as numeric strings that match the category IDs on the Diameter Credit Control Application (DCCA) server.
- If RADIUS is not being used, the Cisco CSG2 is configured as a RADIUS endpoint on the GGSN.
- On the SGSN, the values configured for the number GTP N3 requests and T3 retransmissions must be larger than the sum of all possible server timers (RADIUS, DCCA, and CSG2).

  Specifically the SGSN N3*T3 must be greater than:

  2 x RADIUS timeout + *N* x DCCA timeout + CSG2 timeout

  where:
  - 2 is for both authentication and accounting.
  - *N* is for the number of Diameter servers configured in the server group.

Note Configuring a N3* T3 lower than the default might impact slow TCP-based charging paths.

Additional References

For additional information related to implementing basic connectivity, see the following sections:

- Related Documents, page 3-12
- Standards, page 3-12
- MIBS, page 3-12
- RFCs, page 3-14
- Technical Assistance, page 3-14

Related Documents

- *Release Notes for Cisco GGSN Release 10.0 on the Cisco SAMI, Cisco IOS Release 12.4(24)YE*
- *Cisco Service and Application Module for IP User Guide*
- *Cisco IOS Network Management Configuration Guide*
- *Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers*
- *Cisco 7600 Series Cisco IOS Software Configuration Guide*
- *Cisco 7600 Series Cisco IOS Command Reference*
- *Cisco IOS Quality of Service Solutions Configuration Guide*, Cisco IOS Release 12.4
- Cisco IOS Configuration Guides and Command References, Release 12.4

Standards

Cisco GGSN Release 10.0 supports the following Third Generation Partnership Program (3GPP) standards and is backward compatible with prior 3GPP Technical Specifications (TS):

Table 3-3 Third Generation Partnership Program (3GPP) Standards Supported by Cisco GGSN Release 10.0

3G TS#	Title	Release	GGSN Release 10.0
29.060	GTP across Gn and Gp	7	8.1.0
29.061	Interworking with PDN	7	7.5.0
32.015	Charging	99	3.12.0
32.215	Charging	5	5.9.0
32.251	Charging	7	7.5.1

Note Cisco GGSN Release 10.0 provides limited support on some sections of the TSs listed above.

The GGSN interfaces comply with the following SMG (Special Mobile Group) standards:

- Ga interface—SMG#28 R99
- Gn interface—SMG#31 R98

MIBS

Platform-Related MIBs

- BGP4-MIB
- CISCO-AAA-SERVER-MIB
- CISCO-BULK-FILE-MIB
- CISCO-CDP-MIB
- CISCO-CLASS-BASED-QOS-MIB
- CISCO-CONFIG-COPY-MIB

- CISCO-CONFIG-MAN-MIB
- CISCO-ENTITY-ASSET-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-FLASH-MIB
- CISCO-FTP-CLIENT-MIB
- CISCO-HSRP-EXT-MIB
- CISCO-HSRP-MIB
- CISCO-IMAGE-MIB
- CISCO-IP-LOCAL-POOL-MIB
- CISCO-IP-STAT-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-NBAR-PROTOCOL-DISCOVERY-MIB
- CISCO-PING-MIB
- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB
- CISCO-QUEUE-MIB
- CISCO-RTTMON-MIB
- CISCO-STACK-MIB
- CISCO-SYSLOG-MIB
- CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB
- CISCO-VPDN-MGMT-EXT-MIB
- CISCO-VPDN-MGMT-MIB
- ENTITY-MIB
- ETHERLIKE-MIB
- EVENT-MIB
- EXPRESSION-MIB
- IF-MIB
- NOTIFICATION-LOG-MIB
- RMON-MIB
- RSVP-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB
- TCP-MIB
- UDP-MIB

Application-Related MIBs

- CISCO-GGSN-EXT-MIB
- CISCO-GGSN-GEO-MIB
- CISCO-GGSN-MIB
- CISCO-GGSN-QOS-MIB
- CISCO-GGSN-SERVICE-AWARE-MIB
- CISCO-GPRS-ACC-PT-MIB
- CISCO-GPRS-CHARGING-MIB
- CISCO-GTP-MIB
- CISCO-IP-LOCAL-POOL-MIB
- CISCO-ISCSI-MIB

For information about MIBs, see:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

- RFC 1518, *An Architecture for IP Address Allocation with CIDR*
- RFC 1519, *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*
- RFC 1661, *The Point-to-Point Protocol (PPP)*
- RFC 2461, *Neighbor Discovery for IP Version 6 (IPv6)*
- RFC 2462, *IPv6 Stateless Address Autoconfiguration*
- RFC 2475, *An Architecture for Differentiated Services*
- RFC 3162, *RADIUS and IPv6*
- RFC 3588, *Diameter Base Protocol*
- RFC 3720, *Internet Small Computer Systems Interface (iSCSI)*
- RFC 4006 *Diameter Credit-Control Application*

Technical Assistance

The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.

http://www.cisco.com/techsupport

CHAPTER 4

Configuring GTP Services on the GGSN

This chapter describes how to configure a gateway GPRS service node (GGSN) and how to configure GPRS tunneling protocol (GTP) options.

For complete description of the GGSN commands in this chapter, see *Cisco GGSN Command Reference* for the Cisco GGSN release you are using.

To locate documentation of other commands that appear in this chapter, use the command reference master index or search online. See the "Related Documents" section on page 3-12 for a list of the other Cisco IOS Software documentation that might be helpful while configuring the GGSN.

This chapter includes the following sections:

- GTP Overview, page 4-1
- Configuring GGSN Services, page 4-2
- Configuring Echo Timing on a GGSN, page 4-4
- Customizing the GGSN Configuration, page 4-14
- Using the Service-Mode Function, page 4-27
- Monitoring and Maintaining GTP on the GGSN, page 4-31
- Configuration Examples, page 4-32

GTP Overview

GTP is the protocol used to tunnel multi-protocol packets through the general packet radio service/Universal Mobile Telecommunication System (GPRS/UMTS) network. It is defined on the Gn interface as the protocol between GSNs in the GPRS/UMTS backbone network.

The Cisco GGSN simultaneously supports both GTP Version 0 (GTP v0) and GTP Version 1 (GTP v1). GPRS R97/R98 uses GTP Version 0, and UMTS R99 uses GTP v1.

The GGSN automatically selects the GTP version to use according to the capabilities of the SGSN.

Configuring GGSN Services

The Cisco GGSN software uses a logical interface called a *virtual template interface* to configure an instance of Cisco IOS software running on a Cisco Service and Application Module for IP (SAMI) processor as a GGSN.

This section describes the primary tasks you need to complete when configuring for GGSN services. The subsequent configuration tasks describe how to establish connectivity from the GGSN to the serving GPRS support node (SGSN) and public data networks (PDNs) once the Cisco IOS instance on the Cisco SAMI processor is configured as a GGSN.

The following requirements must be met when configuring a GGSN:

- Configure only a single GGSN entity per instance of Cisco IOS software, using the **service gprs ggsn** command in global configuration mode. Up to six GGSNs can be configured on one Cisco SAMI—one GGSN per processor.
- On each GGSN, configure a single default virtual template interface (as virtual template number 1) with GTP encapsulation. This default virtual template interface should never be unconfigured as long as **gprs service ggsn** is enabled. (Additional virtual template interfaces with GTP encapsulation can be configured for segregating GRX traffic. For more information about segregating GRX traffic, see "Segregating GRX Traffic on GGSN Gn Interface" section on page 12-31.)
- Ensure that the memory protection threshold is configured appropriately, according to the router and memory size. For information on configuring the memory protection threshold, see "Configuring the GGSN Memory Protection Mode Threshold" section on page 7-6.

GGSN Services Configuration Task List

To configure a Cisco SAMI processor that is running an instance of Cisco IOS GGSN software for GGSN services, perform the following tasks:

- Enabling GGSN Services, page 4-2
- Creating a Loopback Interface, page 4-3
- Creating a Default GTP Virtual Template Interface for the GGSN, page 4-3
- Enabling CEF Switching, page 4-4

Enabling GGSN Services

Using the **service gprs ggsn** command in global configuration mode, configure only a single GGSN entity per Cisco SAMI processor.

To enable GGSN services, use the following command in global configuration mode:

Command	Purpose
`Router(config)# service gprs ggsn`	Specifies that the Cisco IOS software instance functions as a GGSN.

Creating a Loopback Interface

Rather than directly configuring an IP address on the virtual template, we recommend that you create a loopback interface and then associate the loopback interface IP address to the virtual template used for GTP encapsulation using the **ip unnumbered loopback** command in interface configuration mode.

Note If the IP address of the loopback interface is not assigned to the virtual template interface using the **ip unnumbered loopback** command, packets will not be CEF-switched and performance will be affected.

A loopback interface is a software-only interface that emulates an interface that is always up. It is a virtual interface that is supported on all platforms. The interface number is the number of the loopback interface that you want to create or configure. There is no limit to the number of loopback interfaces that you can create. A GGSN uses loopback interfaces to support the configuration of several different features.

To create a loopback interface, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface loopback number`	Creates a loopback interface. A loopback interface is a virtual interface that is always up.
Step 2	`Router(config-if)# ip address ip-address mask`	Assigns an IP address to the loopback interface.

Creating a Default GTP Virtual Template Interface for the GGSN

Configure only a single default GTP virtual template interface (as virtual template number 1) with GTP encapsulation on a GGSN. The default GTP virtual template must be configured, and never unconfigured as long as s**ervice gprs ggsn** is configured.

Note The default GTP virtual template (Virtual-Template 1) must have a valid IP address associated with it using either the **ip address** or **ip unnumbered** command.

To create a default GTP virtual template interface for GGSN, use the following command, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface virtual-template 1`	Creates a virtual template interface, where *number* identifies the virtual template interface. This command takes you to interface configuration mode.
Step 2	`Router(config-if)# description description`	Description of the interface.
Step 3	`Router(config-if)# ip unnumber loopback number`	Assigns the previously defined loopback IP address to the virtual template interface.

	Command	Purpose
Step 4	`Router(config-if)# encapsulation gtp`	Specifies GTP as the encapsulation type for packets transmitted over the virtual template interface.
Step 5	`Router(config-if)# gprs access-point-list gprs`	Specifies a name for a new access point list, or references the name of the existing access point list, and enters access-point list configuration mode.

Enabling CEF Switching

CEF switching uses a forwarding information base (FIB) table and an adjacency table to accomplish packet switching. The adjacency table is indexed by Layer 3 network addresses and contains the corresponding Layer 2 information to forward a packet.

CEF switching eliminates the use of the route-cache table, and the overhead that is required in aging out its table entries and repopulating the table. The FIB table mirrors the entire contents of the IP routing table, which eliminates the need for a route-cache table.

For more information about switching paths, see *Cisco IOS Switching Services Configuration Guide*.

When you enable CEF switching globally on the GGSN, all interfaces on the GGSN are automatically enabled for CEF switching.

Note To ensure that CEF switching functions properly, wait a short period of time before enabling CEF switching after it is disabled using the **no ip cef** command.

To enable CEF switching on the GGSN, use the following commands beginning in global configuration mode:

Command	Purpose
`Router(config)# ip cef`	Enables CEF on the GGSN.

Configuring Echo Timing on a GGSN

GGSN uses echo timing to determine whether an SGSN or external charging gateway is active.

For a GTP path to be active, the SGSN must be active. To determine that an SGSN is active, the GGSN and SGSN exchange echo messages. Although the GGSN supports different methods of echo message timing, the basic echo flow begins when the GGSN sends an echo request message to the SGSN. The SGSN sends a corresponding echo response message back to the GGSN.

If the GGSN does not receive a response after a certain number of retries (a configurable value), the GGSN assumes that the SGSN is not active. This indicates a GTP path failure, and the GGSN clears all PDP context requests associated with that path.

This section describes the different methods of echo timing that are supported on the GGSN and how to configure them. It includes the following topics:

- Overview of the Echo Timing on the GGSN, page 4-5
- Echo Timing Configuration Task List, page 4-10
- Verifying the Echo Timing Configuration, page 4-12
- Dynamic Echo Timer Configuration Example, page 4-34

Overview of the Echo Timing on the GGSN

The GGSN supports two different means of echo timing—the default echo timer and the dynamic echo timer. Only a single timer can be in use at any time on the GGSN. The following sections describe these two timers:

- Overview of the Default Echo Timer, page 4-5
- Overview of the Dynamic Echo Timer, page 4-7

Note For simplicity, this document describes the operation of echo timing between the GGSN and an SGSN. If an external charging gateway is in use in the GPRS/UMTS network, the GGSN uses the same type of echo timers to maintain the charging gateway path.

Overview of the Default Echo Timer

The default echo timer is enabled on the GGSN automatically. However, you can choose to enable the dynamic echo timing method as an alternative.

When you are using the default echo timer on the GGSN, the following commands apply:

- **gprs gtp n3-requests**—Specifies the maximum number of times that the GGSN attempts to send an echo-request message. The default is 5 times.
- **gprs gtp path-echo-interval**—Specifies the number of seconds that the GGSN waits for a response from an SGSN or external charging gateway, and, after receiving a response, the number of seconds the GGSN waits before sending the next echo-request message. The default is 60 seconds.
- **gprs gtp t3-response**—Specifies the initial number of seconds that the GGSN waits before resending a signaling request message when a response to a request has not been received. This time is doubled for every retry. The default is 1 second.

Figure 4-1 shows the default echo request sequence when a response is successfully received within the specified path echo interval. If the GGSN receives the echo response within the path echo interval (as specified in the **gprs gtp path-echo-interval** command; the default is 60 seconds), it sends another echo request message after 60 seconds (or whatever time was configured in the **gprs gtp path-echo-interval** command). This message flow continues as long as the GGSN receives an echo response message from the SGSN within the specified path echo interval.

Figure 4-1 Default GTP Path Echo Interval Request Sequence in Path Success Mode

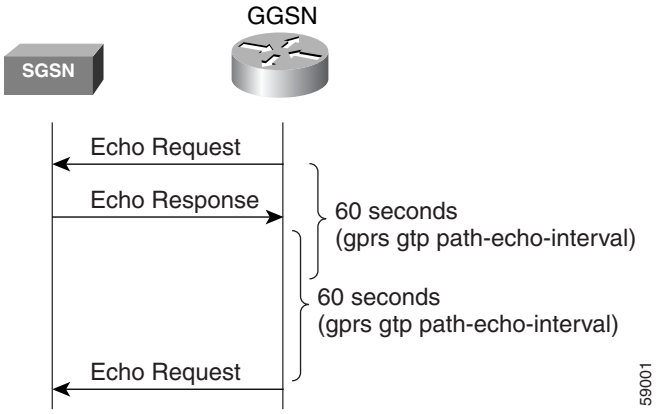
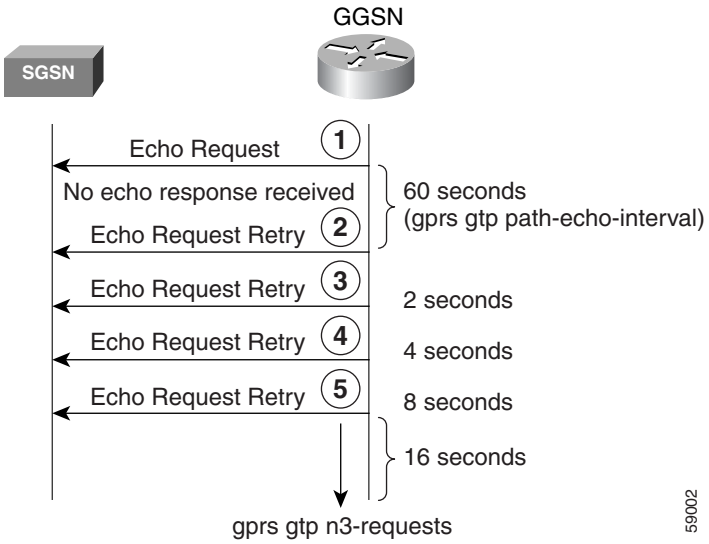


Figure 4-2 shows the default echo request sequence when the GGSN fails to receive a response to its echo request within the specified path echo interval. If the GGSN fails to receive an echo response message from the SGSN within the path echo interval, it resends echo request messages until the N3-requests counter is reached (as specified by the **gprs gtp n3-requests** command; the default is 5). Because the initial request message is included in the N3-requests counter, the total number of retries is N3 - 1. The T3 timer increases by a factor of 2 for each retry (the factor value is not configurable).

Figure 4-2 Default Echo Timing Request Sequence in Path Failure Mode



For example, if N3 is set to the default of 5, and T3 is set to the default of 1 second, the GGSN will resend 4 echo request messages (the initial request + 4 retries= 5). If the GGSN does not receive an echo response from the SGSN during the 60-second path echo interval, then the GGSN immediately sends the first echo request retry message upon expiration of the path echo interval. The T3 time increases for each additional echo request, by a factor of 2 seconds, as long as the GGSN does not receive an echo response. So, the GGSN resends another message in 2 seconds, 4 seconds, and 8 seconds. After the 5th message, the GGSN waits for a final period of 16 seconds for an echo response.

If the GGSN fails to receive an echo response message from the SGSN within the time period of the N3-requests counter, it deletes all of the PDP contexts and clears the GTP path. For this example, the total elapsed time from when the first request message is sent to when PDP contexts are cleared is

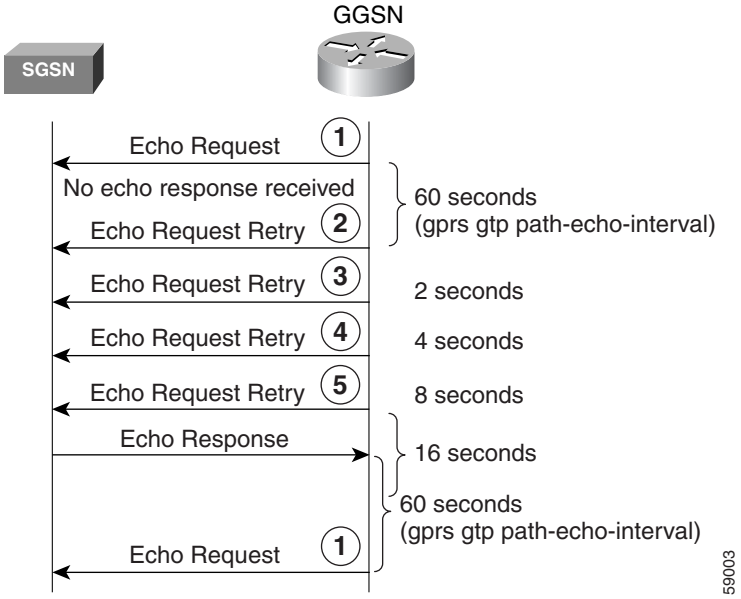
60 + 2 + 4 + 8 + 16 = 90 seconds

where 60 is the initial value of the path echo interval, and the remaining 4 time periods are the increments of the T3 timer for the subsequent retries. The path is cleared after another 60-second period, or 150 seconds.

If the GGSN receives an echo response within the N3 x T3 transmission period, it goes back to success mode for its echo request sequences.

Figure 4-3 shows the GGSN receiving an echo response message within N3 x T3 retransmissions of an echo request. In this scenario, the GGSN sent an initial echo request followed by 4 retries for a total of 5 requests, according to the default setting of 5 N3 requests. The GGSN receives the echo response after the 5th and final retry, within the remaining 16 seconds. Now the GGSN is back in success mode, and it waits 60 seconds (the value of the **gprs gtp path-echo-interval** command) before sending the next echo request message.

Figure 4-3 Default Echo Timing with Echo Response Received Within N3 x T3 Retransmissions



Overview of the Dynamic Echo Timer

Because the GGSN's default echo timer cannot be configured to accommodate network congestion, the GTP path could be cleared prematurely. The dynamic echo timer feature enables the GGSN to better manage the GTP path during periods of network congestion. Use the **gprs gtp echo-timer dynamic enable** command to enable the GGSN to perform dynamic echo timing.

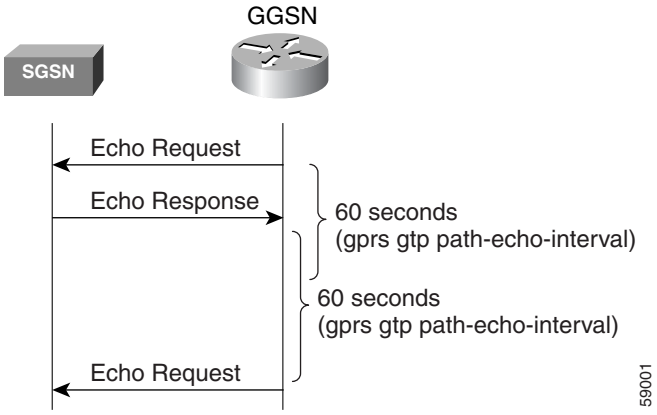
The dynamic echo timer is different from the default echo timer because it uses a calculated round-trip time (RTT), and a configurable factor or multiplier to be applied to the RTT statistic. Different paths can each have a different RTT, so the dynamic echo timer can vary for different paths.

When you are using the dynamic echo timer on the GGSN, the following commands apply:

- **gprs gtp echo-timer dynamic enable**—Enables the dynamic echo timer on the GGSN.
- **gprs gtp echo-timer dynamic minimum**—Specifies the minimum time period (in seconds) for the dynamic echo timer. If the RTT multiplied by the smooth factor is less than this value, the GGSN uses the value set in this command. The default is 5 seconds.
- **gprs gtp echo-timer dynamic smooth-factor**—Specifies the multiplier that the dynamic echo timer uses when calculating the time to wait to send retries, when it has not received a response from the SGSN within the path echo interval. The default is 2.
- **gprs gtp n3-requests**—Specifies the maximum number of times the GGSN attempts to send an echo-request message. The default is 5 times.
- **gprs gtp path-echo-interval**—Specifies the number of seconds that the GGSN waits, after receiving a response from an SGSN or external charging gateway, before sending the next echo-request message. The default is 60 seconds.

Figure 4-4 shows the dynamic echo request sequence when a response is successfully received within the specified path echo interval. Just as in the default echo timing method, if the GGSN receives the echo response within the path echo interval (as specified in the **gprs gtp path-echo-interval** command; the default is 60 seconds), it sends another echo request message after 60 seconds (or whatever time was configured in the **gprs gtp path-echo-interval** command). This message flow continues as long as the GGSN receives an echo response message from the SGSN within the specified path echo interval.

Figure 4-4 Dynamic GTP Path Echo Interval Request Sequence in Path Success Mode



The GGSN calculates the RTT statistic for use by the dynamic echo timer. The RTT is the amount of time between sending a particular echo request message and receiving the corresponding echo response message. RTT is calculated for the first echo response received (see Figure 4-5); the GGSN records this statistic. Because the RTT value might be a very small number, there is a minimum time for the dynamic echo timer to use. This value is configured using the **gprs gtp echo-timer dynamic minimum** command.

Figure 4-5 Dynamic Echo Timing Request Sequence RTT Calculation

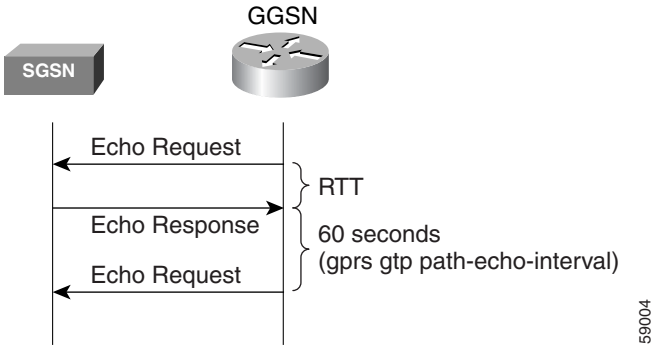
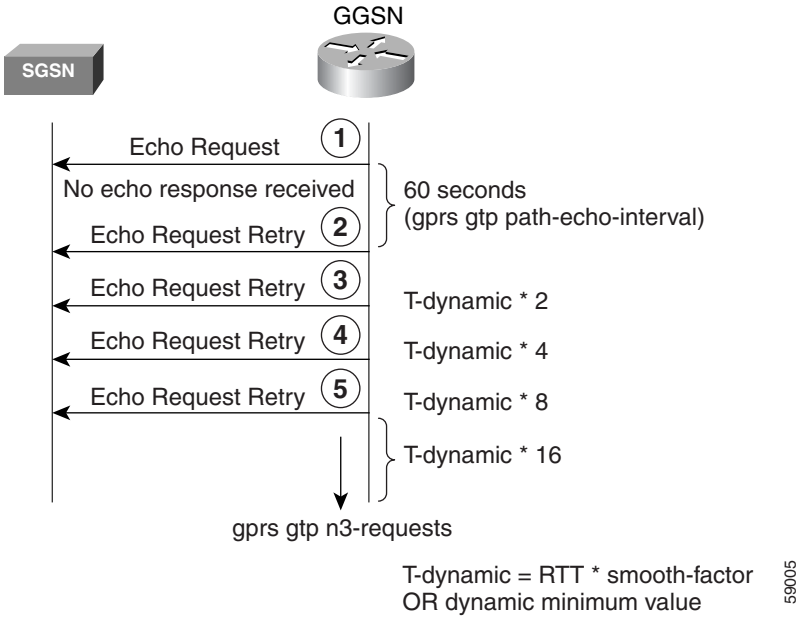


Figure 4-6 shows the dynamic echo timing request sequence in path failure mode. If the GGSN fails to receive an echo response message from the SGSN within the path echo interval, it goes into retransmission, or path failure mode. During path failure mode, the GGSN uses a value referred to as the *T-dynamic*. The T-dynamic is the greater of either the dynamic minimum, or the RTT statistic multiplied by the smooth factor.

Figure 4-6 Dynamic Echo Timing Request Sequence in Path Failure Mode



The T-dynamic essentially replaces the use of the **gprs gtp t3-response** command, which is used in the default echo timer method on the GGSN. The T-dynamic timer increases by a factor of 2 for each retry (again, this factor is not configurable), until the N3-requests counter is reached (the N3-requests counter includes the initial request message).

For example, if the RTT is 6 seconds, the dynamic minimum is 5 seconds, N3 is set to 5, and the smooth factor is set to 3, then the GGSN will resend up to 4 echo request messages (initial request + 4 retries = 5) in path failure mode. If the GGSN does not receive an echo response from the SGSN during the 60-second path echo interval, then the GGSN immediately sends the first echo request retry message upon expiration of the path echo interval. The RTT x smooth factor equals 18 seconds (6 x 3), which is greater than the dynamic minimum of 5 seconds, so the dynamic minimum value is not used. The

T-dynamic value is 18 (RTT x smooth factor), so the GGSN sends another retry echo request message in 36 seconds (18 x 2), 72 seconds (18 x 4), and 144 seconds (18 x 8). After the fifth message, the GGSN waits for a final period of 288 seconds (18 x 16) for an echo response.

If the GGSN fails to receive an echo response message from the SGSN in this time period, it clears the GTP path and deletes all PDP contexts. The total elapsed time, from when the first request message is sent, to when the PDP contexts are cleared, is

60 + 36 + 72 + 144 + 288 = 600 seconds

where 60 is the initial value of the path echo interval, and the remaining 4 time periods are the increments of the T-dynamic for the subsequent retries. The path is cleared after another 60-second period, or 660 seconds.

If the GGSN receives an echo response within the N3 x T-dynamic transmission period, it goes back to success mode for its echo request sequences. In success mode, the GGSN begins echo requests and awaits responses according to the specified path echo interval as shown in Figure 4-4.

Sequence Numbering for Retransmissions

The GGSN does not increment the sequence number of an echo request message during retransmissions. Therefore, during the period when an echo response has not been received by the GGSN, the GGSN continues to use the same sequence number for all echo request retries until the N3 requests limit is reached, or until a response is received. When a response is received, the sequence number of the next echo request message is incremented by 1.

If the GGSN has sent an echo request message with a higher sequence number, but still receives echo responses for sequence numbers lower than the current echo request message, the response is ignored.

Echo Timing Configuration Task List

This section describes the tasks required to customize the default echo timing method, or to enable and configure the dynamic echo timing method on the GGSN. By default, the GGSN activates the default echo timing method.

To configure echo timing on the GGSN, perform the following tasks:

- Customizing the Default Echo Timer, page 4-10 (Recommended, if used)
- Configuring the Dynamic Echo Timer, page 4-11 (Optional)
- Disabling the Echo Timer, page 4-12 (Optional)

Customizing the Default Echo Timer

The default echo timing method is enabled automatically on the GGSN. If you want to use the default echo timer, Cisco recommends that you modify the following commands to optimize your network as necessary.

To customize the default echo timing method on the GGSN, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs gtp n3-requests requests`	(Optional) Specifies the maximum number of times that the GGSN attempts to send a signaling request to an SGSN. The default is 5.
Step 2	`Router(config)# gprs gtp path-echo-interval interval`	(Optional) Specifies the number of seconds that the GGSN waits, after receiving a response from an SGSN or external charging gateway, before sending the next echo-request message. The default is 60 seconds.
Step 3	`Router(config)# gprs gtp t3-response response-interval`	(Optional) Specifies the initial time that the GGSN waits before resending a signaling request message when a response to a request has not been received. This time is doubled for every retry. The default is 1 second.

Configuring the Dynamic Echo Timer

To activate the dynamic echo timing method on the GGSN, you must enable the dynamic echo timer. After you activate the dynamic echo timer, you can modify the corresponding options to optimize the timing parameters for your network.

To configure the dynamic echo timing method on the GGSN, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs gtp echo-timer dynamic enable`	Enables the dynamic echo timer on the GGSN.
Step 2	`Router(config)# gprs gtp echo-timer dynamic minimum number`	(Optional) Specifies the minimum time period used by the dynamic echo timer. The default is 5 seconds.
Step 3	`Router(config)# gprs gtp echo-timer dynamic smooth-factor number`	(Optional) Specifies the multiplier that the GGSN uses to calculate the time to wait to send retries of the dynamic echo timer. The default is 2.
Step 4	`Router(config)# gprs gtp n3-requests requests`	(Optional) Specifies the maximum number of times that the GGSN attempts to send a signaling request to an SGSN. The default is 5.
Step 5	`Router(config)# gprs gtp path-echo-interval interval`	(Optional) Specifies the number of seconds that the GGSN waits, after receiving a response from an SGSN or external charging gateway, before sending the next echo-request message. The default is 60 seconds.

Disabling the Echo Timer

If for some reason you need to disable the GGSN from performing echo processing with an SGSN or external charging gateway, you can specify 0 seconds for the path echo interval.

To disable the echo timer, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs gtp path-echo-interval 0`	(Optional) Specifies a path interval of 0 seconds, which disables the GGSN from performing echo processing.

Verifying the Echo Timing Configuration

This section describes how to verify the echo timing method on the GGSN. It includes the following topics:

- Verifying Echo Timing Parameters, page 4-12
- Verifying the Dynamic Echo Timer by GTP Path, page 4-13

Verifying Echo Timing Parameters

To verify the parameters in use by the GGSN for echo timing, you can use the **show gprs gtp parameters** or **show running-config** privileged EXEC command.

The GGSN automatically sets default values for the parameters applicable to the dynamic echo timer, even when the dynamic echo timer is not enabled. Therefore, the **show gprs gtp parameters** command does not indicate which echo timing method is currently activated.

Verifying Default Echo Timing Parameters

To verify the parameters in use by the default echo timer, use the **show gprs gtp parameters** privileged EXEC command, and observe the following parameters shown in bold text below:

```
Router# show gprs gtp parameters
    GTP path echo interval                      = 60
    GTP signal max wait time T3_response        = 1
    GTP max retry N3_request                    = 5
    GTP dynamic echo-timer minimum              = 5
    GTP dynamic echo-timer smooth factor        = 2
    GTP buffer size for receiving N3_buffer     = 8192
    GTP max pdp context                         = 45000
```

Verifying Dynamic Echo Timing Parameters

To verify the parameters in use by the dynamic echo timer, use the **show gprs gtp parameters** privileged EXEC command, and observe the parameters shown in bold text below:

```
Router# show gprs gtp parameters
    GTP path echo interval                          = 60
    GTP signal max wait time T3_response            = 1
    GTP max retry N3_request                        = 5
    GTP dynamic echo-timer minimum                  = 5
    GTP dynamic echo-timer smooth factor            = 2
    GTP buffer size for receiving N3_buffer         = 8192
    GTP max pdp context                             = 45000
```

Verifying the Dynamic Echo Timer by GTP Path

You can use the **show running-config** privileged EXEC command to verify whether the dynamic echo timer is enabled.

The value of the dynamic echo timer varies for each GTP path on the GGSN. To verify whether the dynamic echo timer is enabled on the GGSN, and to verify the value (in seconds) of the dynamic echo timer (T-dynamic), use the **show gprs gtp path** privileged EXEC command.

If the dynamic echo timer is not activated, the word “Disabled” appears beside the corresponding path in the dynamic echo timer output field.

Step 1 To verify that the dynamic echo timer is enabled, use the **show running-config** command, and verify that the **gprs gtp dynamic echo-timer enable** command appears as shown in bold text toward the end of the following sample output:

```
Router# show running-config

Current configuration : 6769 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service gprs ggsn
!
ip cef
!
. . .
!

interface loopback 1
 ip address 10.41.41.1 255.255.255.0
!
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list gprs
!
. . .
!
gprs access-point-list gprs
  access-point 1
   access-point-name gprs.cisco.com
   exit
```

```
   !
  access-point 2
   access-point-name gprt.cisco.com
   access-mode non-transparent
   aaa-group authentication test2
   aaa-group accounting test2
   ip-address-pool dhcp-proxy-client
   dhcp-server 10.65.0.1
   dhcp-gateway-address 10.65.0.1
   exit
   !
!
gprs ms-address exclude-range 10.21.1.0 10.21.1.5
gprs gtp echo-timer dynamic enable
gprs gtp echo-timer dynamic smooth-factor 5
gprs gtp echo-timer dynamic minimum 10
gprs gtp response-message wait-accounting
!
. . .
!
end
```

Step 2 To verify the T-dynamic values for the corresponding GTP paths, use the **show gprs gtp path all** privileged EXEC command.

The following example indicates that the dynamic echo timer is enabled on the GGSN and that the T-dynamic values of 5 seconds and 2 seconds are in use for the corresponding paths:

```
Router# show gprs gtp path all
         Total number of path : 2

Local address           Remote address          GTP version    Dynamic echo timer
10.41.41.1(3386)        10.18.18.200(3386)      0              5
10.10.10.1(2123)        10.10.10.4(2123)        1              2
```

Customizing the GGSN Configuration

This section describes some of the options that you can configure on the GGSN to further customize the default configuration.

For information about configuring GPRS/UMTS charging options, see the "Customizing the Charging Options" section on page 7-11.

This section includes the following topics:

- Configuring GTP Signaling Options, page 4-15
- Configuring the Maximum Number of PDP Contexts on the GGSN, page 4-16
- Controlling Sessions on the GGSN, page 4-17
- Configuring Flow Control for GTP Error Messages, page 4-24
- Configuring the GGSN to Maintain a History for Deleted SGSN Paths, page 4-24
- Suppressing Echo Requests per SGSN, page 4-24

Configuring GTP Signaling Options

In addition to the commands used to configure the instance of Cisco IOS software for GGSN support, the GGSN feature supports several optional commands that you can use to customize your GTP configuration.

For certain GTP processing options, the default values represent recommended values. Other optional commands also are set to default values, but Cisco recommends modifying these commands to optimize your network as necessary, or according to your hardware. This section describes some of the commands that you should consider using to optimize GTP signaling.

To optimize your GTP signaling configuration, use the following commands, beginning in global configuration mode:

Command	Purpose
`Router(config)# gprs gtp n3-requests requests`	(Optional) Specifies the maximum number of times that the GGSN attempts to send a signaling request. The default is 5.
`Router(config)# gprs gtp path-echo-interval interval`	(Optional) Specifies the number of seconds that the GGSN waits before sending an echo-request message to check for GTP path failure. The default is 60 seconds.
`Router(config)# gprs gtp t3-response response_interval`	(Optional) Specifies the the initial number of seconds that the GGSN waits before resending a signaling request message when a response to a request has not been received. This time is doubled for every retry. The default is 1 second.

Note These GTP signaling commands are also used to support echo timing on the GGSN. For more information about echo timing on the GGSN, see the "Configuring Echo Timing on a GGSN" section on page 4-4.

Configuring Other GTP Signaling Options

This section describes some other GTP signaling options that you can modify as needed to support your network needs.

To configure other GTP signaling options, use the following commands, beginning in global configuration mode:

Command	Purpose
`Router(config)# gprs gtp map signalling tos tos-value`	(Optional) Specifies an IP ToS mapping for GTP signaling packets. The default is 5.
`Router(config)# gprs gtp n3-buffer-size bytes`	(Optional) Specifies the size of the receive buffer that the GGSN uses to receive GTP signaling messages and packets sent through the tunneling protocol. The default is 8192 bytes.

Command	Purpose
`Router(config)# gprs gtp response-message pco ipcp nack`	(Optional) Specifies for the GGSN to return an IPCP Conf-Nack (Code 03) in the GTP PCO IE of a Create PDP Context response when returning IP Control Protocol (IPCP) options for which the granted values (non-zero) differ from those requested (IPCP Conf-Reject [Code 04] for those options for which the returned address values are zero). By default, the GGSN sends an IPCP Conf-Ack (Code 2) in the PCO IE of the Create PDP Context response for all the requested IPCP address options supported by the GGSN (the values returned may be the same as or differ from those values requested, or be even zero.)
`Router(config)# gprs gtp response-message pco ipcp message-length`	Configures an extra field that indicates the message length to be added to the header in the PCO IE of the Create PDP Context response when returning IPCP options.

Configuring the Maximum Number of PDP Contexts on the GGSN

The practical upper limit for the maximum number of PDP contexts supported on a GGSN depends on the memory and platform in use and on the GGSN configuration (for example, whether a method of PPP is configured to forward packets beyond the terminal equipment and mobile termination, whether Dynamic Feedback Protocol [DFP] is being used or the memory protection feature is enabled, and the rate of PDP context creation to be supported).

Note DFP weighs PPP PDPs against IP PDPs, with one PPP PDP equal to eight IPv4 PDPs. One IPv6 PDP equals eight IPv4 PDPs.

Table 1 lists the maximum number of PDP contexts the Cisco SAMI with the 1-GB memory option can support. Table 2 lists the maximum number of PDPs the Cisco SAMI with the 2-GB memory option can support:

Table 1 Number of PDPs Supported in 1-GB SAMI

PDP Type	Maximum Number per SAMI
IPv4	384,000
IPv6	48,000
PPP Regeneration	96,000
PPP	48,000

Table 2 Number of PDPs Supported in 2-GB SAMI

PDP Type	Maximum Number per SAMI
IPv4	816,000
IPv6	96,000

Table 2 Number of PDPs Supported in 2-GB SAMI

PDP Type	Maximum Number per SAMI
PPP Regeneration	192,000
PPP	96,000

Note When the maximum allowable number of PDP contexts is reached, the GGSN refuses new PDP contexts until sessions are available.

To configure the maximum number of PDP contexts on the GGSN, use the following command, beginning in global configuration mode:

Command	Purpose
`Router(config)# gprs maximum-pdp-context-allowed pdp-contexts`	Specifies the maximum number of PDP contexts that can be activated on the GGSN.

Configuring the Maximum Number of PDP Contexts When Using DFP with Load Balancing

If you use DFP with GPRS/UMTS load balancing, also specify the maximum number of PDP contexts for each GGSN. Do not accept the default value of 10000 PDP contexts; a value of 45000 is recommended. Significantly lower values can affect performance in a GPRS/UMTS load-balancing environment.

Note For more information about configuring GPRS/UMTS load balancing, see the *IOS Server Load Balancing*, 12.1(9)E documentation located at Cisco.com at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e9/index.htm

To configure the maximum number of PDP contexts on the GGSN for DFP, use the following command, beginning in global configuration mode:

Command	Purpose
`Router(config)# gprs maximum-pdp-context-allowed 45000`	Specifies 45000 as the maximum number of PDP contexts that can be activated on the GGSN.

Controlling Sessions on the GGSN

GPRS/UMTS provides always-on services for mobile subscribers. The GGSN can support only a certain number of PDP contexts. The number of PDP contexts supported depends upon the configuration and memory resources of the platform.

Sessions can be established with the GGSN that provide network connectivity, even though no activity may be occurring over that session. After a PDP context is established on the GGSN, whether there is activity over the session or not, the GGSN is using resources. Therefore, you may want to configure a session timer that controls the amount of time that a session can remain established on the GGSN before the PDP context (or contexts) is cleared.

In addition, when performing certain maintenance functions (for example, modifying an APN configuration), you can manually delete PDP contexts.

This section includes the following topics:

- Configuring Session Timers, page 4-18
- Deleting Sessions on the GGSN, page 4-23

Configuring Session Timers

This section describes how you can configure the session idle time and absolute session time on the GGSN to control when the GGSN deletes a session. The section includes the following topics:

- Overview of the Session Idle Timer and the Absolute Session Timer on the GGSN, page 4-18
- Configuring the Session Idle Timer, page 4-19 (Optional)
- Configuring the Absolute Session Timer, page 4-21 (Optional)
- Disabling the Session Idle Timer on the GGSN, page 4-20
- Verifying the Timer Configuration, page 4-22

Overview of the Session Idle Timer and the Absolute Session Timer on the GGSN

The GGSN allows you to control the clearing of PDP contexts by configuring durations for a session idle timer (RADIUS attribute 28) and an absolute session timer (RADIUS attribute 27). The session idle timer and absolute session timer specify the amount of time that the GGSN waits before purging a mobile session.

The duration specified for the session idle time is the same for all of the PDP contexts belonging to a session (a GTPv1 mobile session can have multiple PDP contexts), but an individual timer is started for each PDP context of that session. Therefore, the session idle timer is per-PDP, but the timer duration is per-session. The absolute session timer is session-based and controls the absolute duration of a session (active or inactive). When the absolute session timer is exceeded, the GGSN deletes all PDP contexts of the session (those with the same mobile subscriber identity (IMSI) or mobile station address).

Note The session idle timeout (RADIUS Attribute 28) support applies to IP PDPs, PPP PDPs terminated at the GGSN, and PPP regenerated PDPs (not PPP L2TP PDPs). The absolute session timeout (Attribute 27) support applies to IP PDPs and PPP PDPs terminated at the GGSN (not PPP Regen or PPP L2TP PDPs). If configured, a session idle timer is started on every PDP context; an absolute session timer is started on the session.

You can configure the timers globally on the GGSN for sessions occurring on all access points, and you can configure timers for a particular access point. In addition to the session idle timer and the absolute session timer that you can configure on the GGSN, RADIUS servers can also specify session timeout attributes.

The following list gives the order in which the GGSN implements the timers:

1. RADIUS server—If the access point is configured for non-transparent access mode and the RADIUS server returns a timeout attribute, then the GGSN sets the timeout value based on the attribute sent from the RADIUS server. The RADIUS server timeout attribute is given in seconds. If the value returned by the RADIUS server is less than 30 seconds, the GGSN sets the timeout value to 30 seconds. If the value is greater than 30 seconds, the GGSN sets the timeout value to the same value returned by the RADIUS server.
2. Access-point—If the access point is configured for transparent access mode, or is in non-transparent access mode and the RADIUS server does not return a timeout value, then the GGSN uses the value that you specified for the **gtp pdp-context timeout session** or **gtp pdp-context timeout idle** commands.
3. Global timer—If the GGSN does not receive a timeout value from the RADIUS server or the access point, then it uses the value that you specified for the **gprs gtp pdp-context timeout session** or **gprs gtp pdp-context timeout idle** commands.

In summary, the timeout values from the RADIUS server take precedence over the timer configurations on the GGSN, and the timers for a particular access point takes precedence over the globally configured timers.

The values for the **gtp pdp-context timeout session** and **gtp pdp-context timeout idle** commands override the values for the **gprs gtp pdp-context timeout session** or **gprs gtp pdp-context timeout idle** commands.

Note When you enable a session timer (idle or absolute), any gateway GPRS support node-call detail records (G-CDRs) triggered for the termination of a PDP context because a timer expires will have a cause value of “managementIntervention.”

Configuring the Session Idle Timer

GGSN supports the RADIUS Idle-Timeout (Attribute 28) field. The GGSN stores the attribute 28 value if it is present in the access request packets sent by the AAA server. When a PDP context is idle for an amount of time that exceeds the duration specified with this command, the GGSN terminates the context.

The duration specified for the timer applies to all PDP contexts of a session, however, a timer is started for each PDP context.

The session idle timer can be configured globally and at the APN. The values configured at the APN level override those configured globally.

Note The session idle timer started for a PDP context is reset by TPDU traffic and GTP signaling messages for that PDP context. For example, if an Update PDP Context request is received, the session idle timer is reset for that PDP context.

Configuring the Session Idle Timer Globally on the GGSN

To configure the amount of time that the GGSN allows a PDP context to remain idle on any access point before purging the context, use the following command, beginning in global configuration mode:

Command	Purpose
`Router(config)# gprs gtp pdp-context timeout idle` *seconds* [**uplink**]	Specifies the time, in seconds, that the GGSN allows a PDP context to remain idle on any access point before purging the context. The valid range is between 30 and 429467. The default is 259200 seconds (72 hours). Optionally, specify the **uplink** keyword option to enable the session idle timer in the uplink direction only. When the **uplink** keyword option is not specified, the session idle timer is enabled in both directions (uplink and downlink).

Note As an alternative, you can configure the session idle timer globally using the **gprs idle-pdp-context purge-timer** *hours* command in global configuration mode, however, the two methods cannot be configured at the same time.

Configuring the Session Idle Timer on an Access Point on the GGSN

To configure the amount of time that the GGSN allows a PDP context to remain idle for a particular access point before purging the context, use the following command, beginning in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# gtp pdp-context timeout idle` *seconds* [**uplink**]	Specifies the time, in seconds, that the GGSN allows a PDP context to remain idle for a particular access point before purging the context. The valid range is between 30 and 429467. The default is 259200 seconds (72 hours). Optionally, specify the **uplink** keyword option to enable the session idle timer in the uplink direction only. When the **uplink** keyword option is not specified, the session idle timer is enabled in both directions (uplink and downlink).

Note As an alternative, you can configure the session idle timer on an access point using the **session idle-time** *hours* access-point configuration command; however, the two methods cannot be configured at the same time.

Disabling the Session Idle Timer on the GGSN

By default, for all access points, the GGSN purges the idle PDP contexts of a session after 72 hours. If you want to allow PDP contexts to remain idle for an indefinite period of time, you can disable the timer for a particular user by configuring 0 as the session idle time duration in the user profile on the RADIUS server. If the user is not authenticated by RADIUS, the session idle timer cannot be disabled.

Configuring the Absolute Session Timer

GGSN supports the RADIUS Session-Timeout (Attribute 27) field. When you enable the absolute session timer, the GGSN stores the attribute 27 value if it is present in the access request packets sent by the AAA server. When the duration of a session exceeds the value specified with this command, the GGSN terminates all PDP contexts belonging to the session (those with the same IMSI or MS address).

The absolute session timer can be configured globally and at the APN. The values configured at the APN level override those configured globally.

By default, the absolute session timer is disabled.

Note The GGSN absolute session timer requires that you have enabled the GGSN to include the Session-Timeout (Attribute 27) in RADIUS requests using the **gprs radius attribute session-timeout** command in global configuration mode.

Configuring the Absolute Session Timer Globally on the GGSN

To configure the amount of time that the GGSN allows a session to exist for any access point before ending the session and purging all PDP contexts belonging to the session, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs gtp pdp-context timeout session` *seconds*	Specifies the amount of time, in seconds, that the GGSN allows a session to exist on any access point before ending the session and purging all PDP contexts with the same IMSI or MS address. The valid range is between 30 and 4294967 seconds.

Configuring the Absolute Session Timer on an Access Point on the GGSN

To configure the amount of time that the GGSN allows a session to exist on a particular access point before ending the session and purging all PDP contexts belonging to the session, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# gtp pdp-context timeout session` *seconds*	Specifies the amount of time, in seconds, that the GGSN allows a session to exist on a particularly access point before ending the session and purging all PDP contexts with the same IMSI or MS address. The valid range is between 30 and 4294967 seconds.

Disabling the Absolute Session Timer on the GGSN

By default, the absolute session timer is disabled on the GGSN. To return to the default configuration after enabling the absolute session timer, use the **no** form of the global or access-point configuration commands (**no gprs gtp pdp-context timeout session** or **no gtp pdp-context timeout session**).

Verifying the Timer Configuration

To display timer information for a particular PDP context, you can use the **show gprs gtp pdp-context** command, using the **tid** or **imsi** keywords. The following example shows sample output for the **show gprs gtp pdp-context tid** command for a PDP context with an session idle timer set at the value of 200 hours (720000 seconds) and an absolute session timer set at 24 hours (86400 seconds). The timer values are displayed in the **session timeout** and **idle timeout** fields shown in bold:

```
Router#show gprs gtp pdp-context tid 1234000000000014
TID              MS Addr                   Source  SGSN Addr       APN
1234000000000014 1.2.3.18                  Static  4.4.4.10        gtpv1.com

    current time :Feb 15 2010 04:11:17
    user_name (IMSI): 214300000000004    MS address: 1.2.3.18
    MS International PSTN/ISDN Number (MSISDN): 112000000000004
    sgsn_addr_signal: 4.4.4.10           sgsn_addr_data:   4.4.4.10
    control teid local:  0x0210001F
    control teid remote: 0x00000041
    data teid local:     0x02100020
    data teid remote:    0x00000042
    primary pdp: Y           nsapi: 1
    signal_sequence:  1                  seq_tpdu_up:      0
    seq_tpdu_down:    0
    upstream_signal_flow:   0            upstream_data_flow:   0
    downstream_signal_flow: 0            downstream_data_flow: 0
    RAupdate_flow:          0
    pdp_create_time:   Feb 15 2010 04:07:59
    last_access_time:  Feb 15 2010 04:07:59
    mnrgflag:          0               tos mask map: B8
    session timeout: 86400
    idle timeout: 720000
    umts qos_req: 0911012901010111050101
    umts qos_neg: 0911012901010111050101
    QoS class: conversational
    rcv_pkt_count:       10026         rcv_byte_count:    1824732
    send_pkt_count:      5380          send_byte_count:   4207160
    cef_up_pkt:        0             cef_up_byte:      0
    cef_down_pkt:      0             cef_down_byte:    0
    cef_drop:          0             out-sequence pkt: 0
    charging_id:         42194519
    visitor: No          roamer: Unknown
    charging characteristics:          1
    charging characteristics received: 0
    csg: csggroup1, address: 75.75.75.1
    pdp reference count: 2
    primary dns:         0.0.0.0
    secondary dns:       0.0.0.0
    primary nbns:        0.0.0.0
    secondary nbns:      0.0.0.0
    ntwk_init_pdp:       0
    single pdp-session: Disabled

    absolute session start time:   NOT SET
    Accounting Session ID: 161616010283D657
    Periodic accounting interval: NOT SET
    AAA Unique ID: 16 (0x10)
    Interim Update statistics:
        records sent 0, records failed 0
    Direct Tunnel: Disabled
    Eggsn mode: 0x06 (QS: disabled, EGCDR: enabled, SVC-MESG: enabled)
    PDP internal flags: 7C0001
    MCB internal flags: 0
```

Deleting Sessions on the GGSN

If necessary, you can manually delete PDP contexts using the **clear gprs gtp pdp-context** privileged EXEC command.

You can delete PDP contexts by TID, IMSI value, or by access point (by IP version or all active PDPs on that access-point).

As defined by 3GPP standards, by default, the GGSN sends a Delete PDP Context request to the SGSN, and waits for a response from the SGSN before deleting the PDP context. Also, only a certain number of PDP contexts can be deleted at one time when multiple PDP contexts are being deleted.

If an SGSN is not responding to the GGSN's Delete PDP Context requests, a long delay might occur before the task is completed. You can use the Fast PDP Delete feature (the **no-wait-sgsn** and **local-delete** access point keyword options) to eliminate this delay. The Fast PDP Delete feature enables you to delete PDP contexts within an APN without the GGSN waiting for a response from the SGSN, or delete PDP contexts locally without the GGSN sending a Delete PDP Context request to the SGSN at all.

When using the Fast PDP Delete feature:

- The Fast PDP Delete feature can be used only when an APN or the GGSN is in maintenance mode. Therefore, the **no-wait-sgsn** and **local-delete** keyword options are available only when the APN or GGSN is in maintenance mode.
- When the **no-wait-sgsn** and **local-delete** keyword options are specified, and the command entered, the GGSN prompts you with the following caution:

  ```
  Deleting all PDPs without successful acknowledgements from the SGSN will result in the
  SGSN and GGSN going out of sync. Do you want to proceed ? [n]:
  ```

  The default is **no**. To cancel the delete, type **n** and press enter. To proceed with the delete, type **y** and press enter.
- When processing service-aware PDPs, while the GGSN does not wait for a response from the SGSN when the Fast PDP Delete feature is used, the GGSN must wait for a response from the Cisco CSG and Diameter server. Therefore, the Fast PDP Delete feature is not as useful for service-aware PDPs.
- If a Delete PDP Context requests is lost, the SGSN will not be able to delete the PDP context. This condition might result in inconsistent CDRs generated by the GGSN and the SGSN.
- When the **no-wait-sgsn** keyword option is specified, the GGSN does not throttle the Delete PDP Context requests to the SGSN, and therefore, the GGSN might flood the SGSN with Delete PDP Context requests.
- The Fast PDP Delete feature applies only to PDP deletion initiated by the **clear gprs gtp-context** privileged EXEC command. PDP deletion due to other circumstances, such as PDP deletion during a failure condition, is not impacted.

To manually delete PDP contexts, use the following command in privileged EXEC mode:

Command	Purpose
Router(config-access-point)# **clear gprs gtp pdp-context** {**tid** *tunnel-id* | **imsi** *imsi_value* | **path** *ip-address* [*remote_port_num*] | **access-point** *access-point-index* [**no-wait-sgsn** | **local-delete**] | pdp-type {**ipv6** | **ipv4**} | **all**}	Clears one or more packet data protocol (PDP) contexts (mobile sessions) by TID, IMSI value, path, or by access point (by IP version or all active PDPs). **Note** The **no-wait-sgsn** and **local-delete** keyword options are available only when an APN is in maintenance mode (using **service-mode maintenance** command).

For more information about placing an APN in maintenance mode, see "Configuring APN Maintenance Mode" section on page 4-28.

Configuring Flow Control for GTP Error Messages

GTP error indication messages are sent by the GGSN to the SGSN when the SGSN sends data for PDP context the GGSN cannot locate. The error indication message informs the SGSN that the PDP context cannot be located so that the SGSN can clean up the PDP context on its end.

By default, the GGSN disables flow control for GTP error messages.

You can enable flow control for transmission of GTP error messages by using the **gprs gtp error-indication-throttle** command in global configuration mode. This command sets the initial value of a counter which is decremented each time an error indication message is sent. When the counter reaches zero, the GGSN stops transmitting error indication messages. The GGSN resets this counter to the configured throttle value after one second.

To configure flow control for GTP error messages, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs gtp error-indication-throttle window-size` *size*	Specifies the maximum number of error indication messages that the GGSN sends out in one second, where size is an integer between 0 and 256. There is no default value.

Configuring the GGSN to Maintain a History for Deleted SGSN Paths

The Cisco GGSN can be configured to store statistics collected for deleted SGSN paths.

To configure the maximum number of deleted SGSN paths entries for which you want the GGSN to store a history of statistics, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs gtp path history` *number*	Configures the maximum number of deleted SGSN path entries for which the GGSN will store a history of statistics. A valid value is between 1 and 1000. The default is 100.

Note If the number of entries is changed to a lower value, the older values are deleted.

Suppressing Echo Requests per SGSN

Using the **gprs gtp path sgsn** command in global configuration mode, operators can selectively disable echo requests for GSNs that might not have the capability to respond to echo requests from the GGSN while keeping the echo requests intact for the other SGSNs. In addition, echo requests can be disabled for a specific port of a GSN.

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 using the **gprs gtp path** command. 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.

You can disable echo requests for a range of IP addresses, or a single IP address, with an optional port number.

To suppress echo requests, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs gtp path sgsn` *start-ip-address* `[`*end-ip-address*`] [`*UDP port*`] echo 0`	Specifies that the path created for all SGSNs in the range *start-ip-address* and *end-ip-address*, and corresponding to the UDP port configured, has an echo request interval of 0 (disabled).

The following example disables echo requests for one SGSN:

```
Router(config)# gprs gtp path sgsn 10.10.10.10 echo 0
```

The following example disables echo request for one SGSN for port 4000 only:

```
Router(config)# gprs gtp path sgsn 10.10.10.10 4000 echo 0
```

Configuring Support for GGSN-Initiated Update PDP Context Requests

Note GGSN-initiated Update PDP Context Requests are supported for GTPv1 PDP contexts.

With Cisco GGSN Release 8.0 and later, 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.

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

The GGSN includes the following Information Elements (IEs) in the Update PDP Context Request:

- Recovery
- NSAPI
- QoS profile
- Direct tunnel flags, if the update request is initiated due to a direct tunnel error indication received from the RNC.

Once the QoS is renegotiated, the SGSN returns an Update PDP Context Response to the GGSN to complete the process. If the Cause value in the Update PDP Context Response from the SGSN is "Request Accepted," one of the following actions will occur:

- If the Update PDP Context Request was initiated by an error indication message from the RNC, the PDP context is preserved.
- If the Update PDP Context Request was initiated by a CoA containing new QoS, then an Interim-Acct-Update message is sent to communicate the new QoS (the QoS values supplied in the Update PDP Context Request might have been negotiated downwards by the SGSN). The GGSN will inform the same in an Acct-Update message.

If the Cause value in the Update PDP Context Response is anything other than "Request Accepted," then one of the following actions will occur:

- If the Update PDP Context Request was initiated due to an error indication from the RNC, the PDP is locally deleted.
- If the Update PDP Context Request was initiated by a CoAcommand in global configuration mode, then:
  - If the **gprs gtp update qos-fail delete** command in global configuration mode or the **gtp update qos-fail delete** command in access-point configuration mode are configured, the GGSN will delete the PDP context and send notification of the update failure in an Acct-Stop message.
  - If the **gprs gtp update qos-fail delete** command in global configuration mode or the **gtp update qos-fail delete** command in access-point configuration mode are not configured, the GGSN will retain the PDP context and generate an accounting interim record with the negotiated QoS value.
  - In all cases of failure, an error message is logged to indicate the failure.

Note There is no error message syslog generated for direct tunnel Update PDP Context request failure.

To enable GGSN-initiated Update PDP Context Requests globally, issue the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs gtp update qos-fail delete`	Configures the GGSN to delete a PDP context if a GGSN-initiated QoS update fails, and no GGSN-initiated Update PDP Context Request failure action is configured under the APN using the **gtp update qos-fail** command in access point configuration mode.

To enable GGSN-initiated Update PDP Context Requests under an APN, issue the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# gtp update qos-fail delete`	Configures the GGSN to delete a PDP context if a GGSN-initiated QoS update fails.

Using the Service-Mode Function

The GGSN service-mode function enables you to make configuration changes and test calls without affecting all active sessions on a GGSN. You can configure the service-mode state globally, on an access point, and for the GGSN charging function. There are two service-mode states: operational and maintenance. The default mode is operational.

Configuring Global Maintenance Mode

When a GGSN is placed in global maintenance mode, it rejects all new Create PDP Context requests. Therefore, no new PDP contexts are activated for an entire GGSN while it is in global maintenance mode.

The following sections provide examples of how to use global maintenance mode:

Adding a New GGSN

1. Enable GGSN services and place the GGSN in maintenance mode

```
Router(config)# service ggsn
Router(config)# gprs service-mode maintenance
```

2. Configure the GGSN for your network.
3. Place the GGSN in operational mode.

```
Router(config)# gprs service-mode operational
```

Modifying a GGSN

1. Place the GGSN in maintenance mode.

   ```
   Router(config)# gprs service-mode maintenance
   ```

   Wait for existing PDPs for all APNs to be released normally (average session time is approximately 1 hour) and for buffered CDRs to be sent to the charging gateway. If it is not possible for CDRs to be sent to the charging gateway because there is not an active charging gateway, manually clear the CDRs by placing the charging function in maintenance mode using the **gprs charging service-mode** command and issuing the **clear gprs charging cdr all no-transfer** command. For more information on placing the charging function in maintenance mode, see the "Configuring Charging Maintenance Mode" section on page 4-30.

2. Modify the GGSN configuration as desired.

3. Return the GGSN to operational mode.

   ```
   Router(config)# gprs service-mode operational
   ```

Deactivating a GGSN

1. Place the GGSN in maintenance mode.

   ```
   Router(config)# gprs service-mode maintenance
   ```

   Wait for existing PDPs for all APNs to be released normally (average session time is approximately 1 hour) and for buffered CDRs to be sent to the charging gateway. If it is not possible for CDRs to be sent to the charging gateway because there is not an active charging gateway, manually clear the CDRs by placing the charging function in maintenance mode using the **gprs charging service-mode** command and issuing the **clear gprs charging cdr all no-transfer** command. For more information on placing the charging function in maintenance mode, see the "Configuring Charging Maintenance Mode" section on page 4-30.

2. Remove the GGSN from service.

   ```
   Router(config)# no service gprs ggsn
   ```

To configure the global service-mode state of the GGSN, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs service-mode [operational | maintenance]`	Configures the global service-mode state. The default is operational.

Note When the GGSN is in global maintenance mode, all APNs are placed in maintenance mode as well.

Configuring APN Maintenance Mode

The service-mode state of an APN can be configured to enable you to add a new APN or modify an existing APN without affecting sessions for other APNs in the GGSN.

When an APN is in maintenance mode, it does not accept Create PDP Context requests. Once active PDP contexts are released (or manually cleared using the **clear gprs gtp pdp-context access-point** command), all APN-related parameters can be configured or modified and the APN set to operational mode.

In addition, once you have added and configured an APN, you can verify the configuration using the **gprs service-mode test imsi** command in global configuration mode to set up a test user (one per GGSN) and performing a PDP context creation.

Note The GGSN must be in operational mode (**gprs service-mode operational** command) to test a PDP context creation from a test user using the **gprs service-mode test imsi** command.

To delete an APN, change the APN service-mode state to maintenance mode, wait for all existing PDPs to be released, and then remove the APN using the **no access-point-name** command.

To configure the service-mode state of an APN, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# service-mode [operational | maintenance]`	Configures service-mode state of an APN.

The following sections provide examples of how to use APN maintenance mode:

Adding a new APN

1. Add a new APN and place it in maintenance mode (by default, an APN is in operational mode).

   ```
   Router(config-access-point)# access-point-name apn-num
   Router(config-access-point)# service-mode maintenance
   ```

2. Configure the APN.
3. Create a PDP context for testing the APN configuration.

   ```
   Router(config)# gprs service-mode test imsi imsi-value
   ```

4. Place the APN in operational mode.

   ```
   Router(config-access-point)# service-mode operational
   ```

Modifying an APN

1. Place the APN in maintenance mode.

   ```
   Router(config-access-point)# service-mode maintenance
   ```

   Wait for PDP contexts to be released or clear them manually by using the **clear gprs gtp pdp-contexts access-point** command.

2. Modify the APN.
3. Create a PDP context for testing the APN configuration.

   ```
   Router(config)# gprs service-mode test imsi imsi-value
   ```

4. Place the APN in operational mode.

   ```
   Router(config-access-point)# service-mode operational
   ```

Deleting an APN:

1. Place the APN in maintenance mode.

   ```
   Router(config-access-point)# service-mode maintenance
   ```

   Wait for PDP contexts to be released or clear them manually by using the **clear gprs gtp pdp-contexts access-point** command.

2. Delete the APN.

   ```
   Router(config-access-point)# no access-point-name apn-num
   ```

Configuring Charging Maintenance Mode

The charging function of a GGSN primarily consists of collecting call detail records (CDRs) and transmitting CDRs to charging gateways. The service mode state of the GGSN charging function does not impact the collection of CDRs. However, when the charging function is placed in maintenance service-mode state, CDRs are not transmitted to the charging gateway.

When the charging function is in maintenance mode, you can add, delete, or modify charging gateways (for example, change the IP address of the charging gateways, their priority, and number). If a new primary charging gateway is configured while the charging function is in maintenance mode, when the charging function of the GGSN is placed back in operational mode, all accumulated CDRs are sent to the new charging gateway.

When in maintenance mode, all collected CDRs, and those in the pending queue, are stored on the GGSN. If desired, these stored CDRs can be cleared using the **clear gprs charging cdr all no-transfer** command. When cleared, they will not be transmitted to the charging gateway when the charging function is returned to operational mode.

The following charging function configuration commands require the charging function to be in maintenance mode:

- **gprs charging path-protocol**
- **gprs charging header short**
- **gprs charging map data tos**
- **gprs charging message transfer-request command-ie**
- **gprs charging message transfer-response number-responded**
- **gprs charging port**
- **gprs default charging-gateway**
- **gprs charging send-buffer**

By default the charging function is in operational mode. To configure the service-mode state of the charging function, use the following command in global configuration mode:

Command	Purpose
`Router(config)#` **`gprs charging service-mode`** [**`operational`** | **`maintenance`**]	Configures the service-mode state of a GGSN's charging function.

The following section provide example of how to use charging maintenance mode:

Modifying a Charging Gateway

1. Place the GGSN charging function in maintenance mode.

   ```
   Router(config)# gprs charging service-mode maintenance
   ```

   CDRs are collected but not transmitted. All collected and buffered CDRs are stored until the charging function is returned to operational mode. At that time, they are sent to the charging gateway.

2. Modify the charging configuration (number of gateways, path protocol, order, etc.).
3. If desired, clear all stored and pending CDRs so that they will not be sent to the charging gateway once the charging function is returned to operational mode.

   ```
   Router(config)# clear gprs charging cdr all no-transfer
   ```

4. Return the charging function to operational mode.

   ```
   Router(config)# gprs charging service-mode operational
   ```

To manually clear all CDRs stored on the GGSN, including those in the pending queue, use the following command in global configuration mode:

Command	Purpose
`Router(config)#` **`clear gprs charging cdr all no-transfer`**	Clears stored CDRs, including those in the pending queue, when a the charging function is in maintenance mode.

Note To clear CDRs, the GGSN must be in global maintenance mode (using the **gprs service-mode maintenance** command) and charging maintenance mode (using the **gprs charging service-mode maintenance** command.

Note When the GGSN is in charging and global maintenance modes, the GGSN no longer creates CDRs for existing PDPs.

Monitoring and Maintaining GTP on the GGSN

This section provides a summary list of the **show** commands that you can use to monitor GTP on the GGSN.

The following privileged EXEC commands are used to monitor and maintain GTP on the GGSN:

Command	Purpose
`Router#` **`show gprs access-point`**	Displays information about access points on the GGSN.
`Router#` **`show gprs access-point statistics`**	Displays data volume and PDP activation and deactivation statistics for access points on the GGSN.

Command	Purpose
Router# **show gprs gtp ms** {**imsi** *imsi* | **access-point** *access-point-index* | **all**}	Displays a list of the currently active mobile stations (MSs) on the GGSN.
Router# **show gprs gtp parameters**	Displays information about the current GTP configuration on the GGSN.
Router# **show gprs gtp path** {**remote-address** *ip-address* [*remote-port-num*] | **version** *gtp-version* | **all**}	Displays information about one or more GTP paths between the GGSN and other GPRS/UMTS devices.
Router# **show gprs gtp path statistics history** *number*	Displays statistics for GTP path entries stored in history.
Router# **show gprs gtp path statistics remote-address** *ip-address* [**remote-port** *port-num*]	Displays statistics for a specific path.
Router# **show gprs gtp pdp-context** {**tid** *tunnel_id* [**service** [**all** | **id** *id_string*]] | **ms-address** *ip_address* [**access-point** *access-point-index*] | **imsi** *imsi* [**nsapi** *nsapi* [**tft**]] | **path** *ip-address* [*remote-port-num*] | **access-point** *access-point-index* | **pdp-type** {**ip** | **ppp**} | **qos-umts-class** {**background** | **conversational** | **interactive** | **streaming**} | **qos-precedence** {**low** | **normal** | **high**} | **qos-delay** {**class1** | **class2** | **class3** | **classbesteffort**} | **version** *gtp-version*} | **msisdn** [*msisdn*] **detail** | **ms-ipv6-addr** *ipv6-address* | **all**}	Displays a list of the currently active PDP contexts. **Note** The **show gprs gtp pdp-context** command options vary, depending on the type of QoS method that is enabled on the GGSN.
Router# **show gprs gtp statistics**	Displays the current GTP statistics for the GGSN (such as information element (IE), GTP signaling, and GTP PDU statistics).
Router# **show gprs gtp status**	Displays information about the current status of GTP on the GGSN.
Router# **show gprs service-mode**	Displays the current service mode of the GGSN and the last time the service mode was changed.

Configuration Examples

This section includes the following examples:

- GGSN Configuration Example, page 4-32
- Dynamic Echo Timer Configuration Example, page 4-34

GGSN Configuration Example

The following example shows part of a sample GGSN configuration with some of the commands that you use to configure basic GGSN GTP services:

```
Router# show running-config

Current configuration : 3521 bytes
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
! Enables GGSN services
```

```
!
service gprs ggsn
!
ip cef
!
! Configures a loopback interface
!
interface loopback 1
 ip address 10.40.40.3 255.255.255.0
!
! Defines the virtual-template interface
! with GTP encapsulation
!
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list gprs
!
. . .
!
gprs access-point-list gprs
!
  access-point 1
   access-point-name gprs.cisco.com
   exit
!
  access-point 2
   access-point-name gprt.cisco.com
   exit
   !
  access-point 3
   access-point-name gpru.cisco.com
   access-mode non-transparent
   aaa-group authentication abc
   exit
!
! Configures GTP parameters
!
gprs maximum-pdp-context-allowed 90000
gprs gtp path-echo-interval 0
gprs default charging-gateway 10.15.15.1
!
! Enables the memory protection feature to become active if the memory threshold falls
! below 50 MB
!
gprs memory threshold 512
!
. . .

. . .
!
end
```

Dynamic Echo Timer Configuration Example

The following example shows part of a sample GGSN configuration for the dynamic echo timer. In this example, the dynamic echo timer is enabled, the smooth factor is changed from the default value of 2 to the value 5, and the dynamic minimum value is changed from the default value of 5 seconds to the value 10 seconds:

```
Router# show running-config

Current configuration : 6769 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service gprs ggsn
!
ip cef
!
. . .
!
interface loopback 1
 ip address 10.41.41.1 255.255.255.0
!
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list gprs
!
. . .
!
gprs access-point-list gprs
  access-point 1
   access-point-name gprs.cisco.com
   exit
   !
  access-point 2
   access-point-name gprt.cisco.com
   access-mode non-transparent
   aaa-group authentication test2
   aaa-group accounting test2
   ip-address-pool dhcp-proxy-client
   dhcp-server 10.65.0.1
   dhcp-gateway-address 10.65.0.1
   exit
!
! Enables the dynamic echo timer
!
gprs gtp echo-timer dynamic enable
!
! Configures a smooth factor of 5
!
gprs gtp echo-timer dynamic smooth-factor 5
!
! Configures the dynamic minimum as 10 seconds
!
gprs gtp echo-timer dynamic minimum 10
gprs gtp response-message wait-accounting
!
end
```

CHAPTER 5

Configuring IPv6 PDP Support on the GGSN

This chapter describes how to configure support for Internet Protocol Version 6 (IPv6) packet data protocol (PDP) contexts on a Cisco Gateway GPRS Support Node (GGSN).

For complete descriptions of the GGSN commands in this chapter, see *Cisco GGSN Command Reference* for the Cisco GGSN release you are using.

To locate documentation for other commands that appear in this chapter, use the command reference master index or search online. See the "Related Documents" section on page 3-12 for a list of other Cisco IOS Software documentation that could be helpful while configuring the GGSN.

This chapter includes the following sections:

- IPv6 PDPs on the GGSN Overview, page 5-35
- Implementing IPv6 PDP Support on the GGSN, page 5-39
- Monitoring and Maintaining IPv6 PDPs, page 5-47
- Configuration Example, page 5-48

IPv6 PDPs on the GGSN Overview

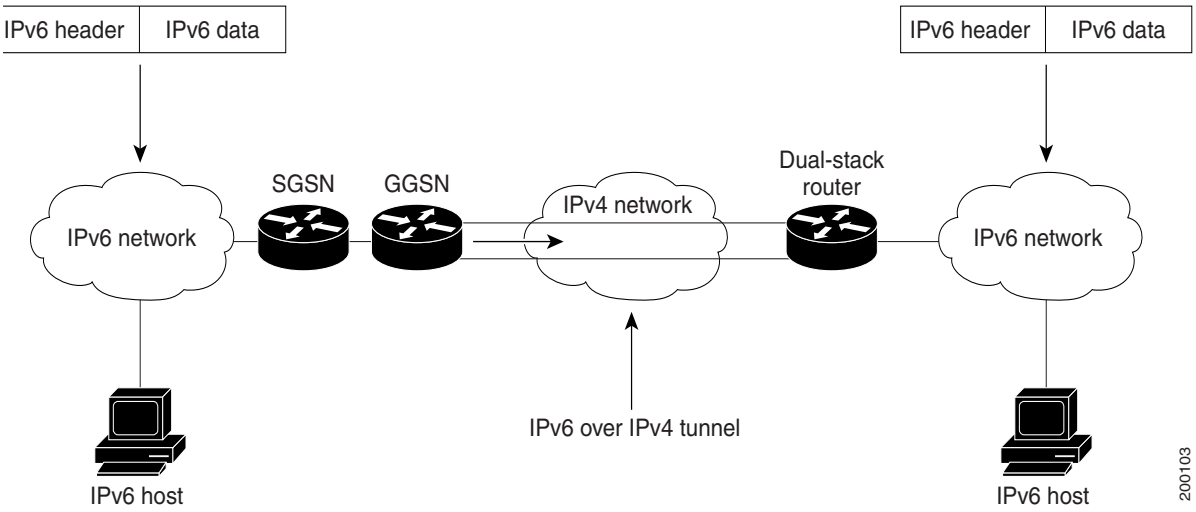
This section provides a brief overview of IPv6 PDP support for the Cisco GGSN. For detailed information about the implementation of IPv6 in Cisco IOS Software, including IPv6 address formats and addressing schemes, see *Cisco IOS IPv6 Configuration Guide*.

The Cisco GGSN supports IPv6 primary PDP context activation, and serving GPRS support node (SGSN)-initiated modification and deactivation procedures via IPv6 stateless autoconfiguration (as specified by RFC 2461 and RFC 2462). An IPv6-over-IPv4 tunnel configured on the Cisco 7600 Series Router supervisor engine module establishes connectivity between isolated or remote IPv6 networks over an existing IPv4 infrastructure.

Note Tunnels must be configured from the supervisor engine. Tunneling from the GGSN is not supported.

Figure 5-1 shows the IPv6 over IPv4 tunnel configuration.

Figure 5-1 IPv6 over IPv4 Tunnel Configuration



IPv6 Stateless Autoconfiguration

Interfaces on an IPv6 node must have a link-local address, which is typically automatically configured from the identifier for an interface and the link-local prefix FE80::/10. A link-local address enables a node to communicate with other nodes on the link, and it can be used to further configure the node.

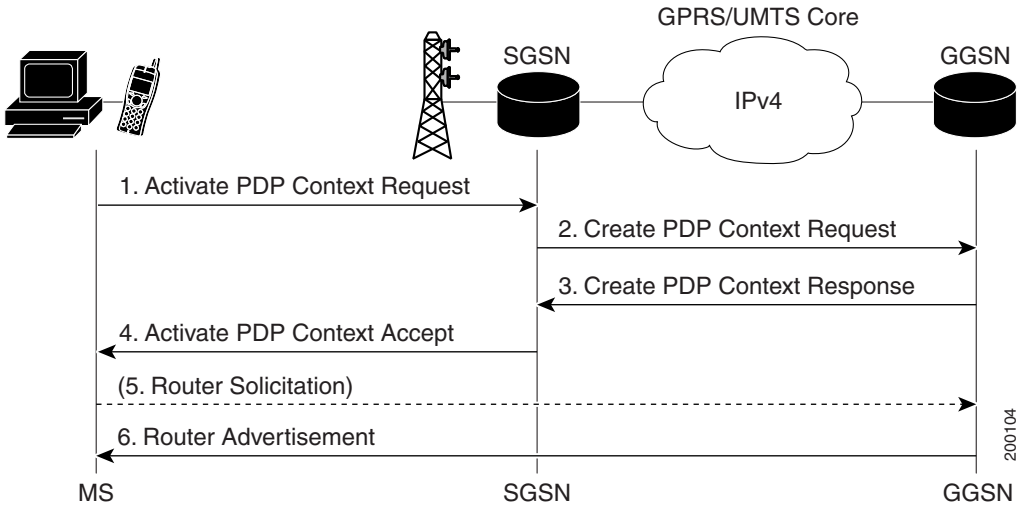
Nodes can connect to a network and automatically generate site-local and global IPv6 addresses without the need for manual configuration or help of a server, such as a RADIUS. With IPv6, a Cisco GGSN advertises any site-local and global prefixes, and advertises its willingness to function as a default router for the link in router advertisements (RAs). RAs are sent periodically, and are sent in response to router solicitation messages, which hosts send at system startup.

The Cisco GGSN assigns an interface ID to the IPv6 mobile station (MS) in the Create PDP Context response, or the MS can automatically configure a site-local and global IPv6 address by appending its interface identifier (64 bits) to the prefix (64 bits) included in an RA.

The resulting 128-bit IPv6 address configured by the node is then subjected to Duplicate Address Detection to ensure its uniqueness on the link. If the prefix advertised in the RA is globally unique, then the IPv6 address configured by the node is also guaranteed to be globally unique. Hosts send router solicitation messages, which have a value of 133 in the Type field of the Internet Control Message Protocol (ICMP) packet header, at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled RA.

Figure 5-2 depicts the creation of an IPv6 PDP context via IPv6 stateless autoconfiguration.

Figure 5-2 IPv6 PDP Context Creation on the Cisco GGSN Using IPv6 Stateless Autoconfiguration



In the steps of the call flow shown in Figure 5-2, the following occurs:

1. Activate PDP Context Request—The MS sends the SGSN an Activate PDP Context request.
2. Create PDP Context Request—The SGSN sends a Create PDP Context request to the GGSN.

   Upon receiving the Create PDP Context request from the SGSN, the GGSN generates an IPv6 address composed of the prefix allocated to the PDP context and an interface identifier generated by the GGSN.
3. Create PDP Context Response—The GGSN returns an address in its Create PDP Context response to the SGSN.

   Since the MS is considered to be alone on its link toward the GGSN, the interface identifier does not need to be unique across all PDPs. The MS extracts and stores the interface identifier from the address received and uses it to build its link-local address and its complete IPv6 address.
4. Activate PDP Context Accept—The SGSN sends an Activate PDP Context accept to the MS, and the context is established.
5. Router Solicitations—The MS can or cannot send router solicitations to the GGSN.
6. Router Advertisements—The GGSN sends RAs periodically.

   In the RAs, the GGSN sends a 64-bit prefix, which is the same prefix as the one it provided in Step 3. After the MS receives the RA, it constructs its complete IPv6 address by concatenating the interface ID received in Step 3, or a locally generated interface ID, and the prefix provided in the RA. If the RA contains more than one prefix option, the MS considers only the first one, and discards the rest.

   Because any prefix the GGSN advertises in a Create PDP Context response is unique within the scope of the prefix, the MS does not have to perform Duplicate Address Detection. Therefore, the GGSN can discard the neighbor solicitations the MS can send to detect a duplicate address.

Supported Features

For IPv6 PDP contexts, the Cisco GGSN supports the following features:

- IPv6 GTPv0 and GTPv1 PDP establishment via IPv6 stateless autoconfiguration.
- IPv6 prefix allocation from a locally configured 64-bit prefix pool.
- GGSN sending of RAs and answering of router solicitation messages from MSs.
- IPv6 gateway GPRS support node-call detail record (G-CDR) generation.
- Dual-stack APN (both IPv4 and IPv6 PDPs supported simultaneously).
- IPv6 DNS address configuration per APN for IPv6 DNS address allocation if requested.
- RADIUS authentication, accounting, and IPv6 address allocation from RADIUS server.
- Per-APN RA timers. These timers include the RA interval and lifetime intervals, and the initial interval before sending the first RA.
- Standard and extended ACL support for IPv6 APNs.
- GPRS-specific security features (address verification and mobile-to-mobile traffic redirection features).
- QoS (marking and Call Admission Control).
- Proxy Call Session Control Function (Proxy-CSCF) support for IPv6 servers.

Restrictions

The following limitations and restrictions apply to IPv6 PDP context support on the GGSN:

- The following features are not supported for IPv6 PDP contexts:
  - Secondary PDP contexts
  - Per-PDP policing
  - Stateful address autoconfiguration with DHCPv6
  - DHCPv6 relay or proxy-client
  - Stateful IPv6 autoconfiguration
  - GTP session redundancy (GTP-SR)
  - Enhanced service-aware billing
  - PPP PDP and PPP regeneration
  - Virtual routing and forwarding (VRF)

    (If a dual-stack APN is configured, and VRF is enabled on the APN, IPv4 PDP contexts go into the VRF, but IPv6 PDP contexts stay in the global routing table.)
  - Route probe, routing behind the mobile, and single PDP session, and configuring a primary and back NetBIOS Name Service.

Note Fro a complete list of APN configurations supported or not supported for IPv6 PDP contexts, see Chapter 9, “Configuring Network Access to the GGSN.”

- IP CEF and IPv6 CEF must be enabled. (IPv6 CEF requires IP CEF to be enabled.)
- All infrastructure nodes in the public land mobile network (PLMN), the SGSN, GGSN, and charging gateway, are assumed to be IPv4 nodes.
- IPv6 must be implemented on the supervisor engine module.
- IPv6 over IPv4 tunnels must be configured from the supervisor engine module. Tunneling from the GGSN is not supported.
- RADIUS must be implemented as an infrastructure node in the PLMN.
- The the **no virtual-template snmp** command must be configured.
- The **no virtual-template subinterface** must not be configured.
- The following commands must not be configured on the IPv6 base virtual template:
  - **snmp if-index persists**
  - **ntp disable**

Implementing IPv6 PDP Support on the GGSN

To configure IPv6 support on the GGSN, complete the tasks listed in the following sections:

- Enabling the Forwarding of IPv6 Traffic on the GGSN, page 5-39 (Required)
- Configuring an IPv6 Base Virtual Template Interface, page 5-40 (Required)
- Enabling IPv6 Support under an APN, page 5-42 (Required)
- Configuring a Local IPv6 Prefix Pool, page 5-44 (Required)
- Monitoring and Maintaining IPv6 PDPs, page 5-47 (Optional)

Enabling the Forwarding of IPv6 Traffic on the GGSN

The forwarding of IPv6 traffic on the GGSN requires that Cisco Express Forwarding (CEF) and IPv6 CEF are enabled globally on the GGSN. In addition, to forward IPv6 traffic using CEF, configure the forwarding of IPv6 unicast datagrams globally on the GGSN by using the **ipv6 unicast-routing** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef**
4. **ipv6 unicast-routing**
5. **ipv6 cef**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip cef** **Example:** `Router# configure terminal`	Enables Cisco Express Forwarding for IPv4 globally on the router.
Step 4	**ipv6 unicast-routing** **Example:** `Router(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams.
Step 5	**ipv6 cef** **Example:** `Router(config)# ipv6 cef`	Enables CEF for IPv6 globally on the router.

Configuring an IPv6 Base Virtual Template Interface

A virtual-access subinterface is created for each IPv6 PDP context established on the GGSN. The configurations for virtual access, such as RA timers, are cloned from an IPv6 base virtual template interface that is assigned to the APN. The commands configured under the IPv6 base virtual template define the behavior of the IPv6 protocol.

You can configure multiple base virtual templates, each with a different configuration. Multiple APNs can share a base virtual template, however, only one base virtual template can be assigned to an APN (using the **ipv6 base-vtemplate** command) at a time.

When a Create PDP Context request is received, a virtual subinterface is cloned from the base virtual template that is assigned to the APN, and an IPv6 address is allocated as configured under the APN after the IPv6 virtual-access subinterface is created. The Create PDP Context response is returned after the virtual-access subinterface is created, and authentication and address allocation are successfully completed.

Caution To avoid severe performance issues, ensure that the **no ipv6 nd ra suppress** command *is* configured and that the **no-virtual-template subinterface** commands *is not* configured under the IPv6 base virtual template interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **ipv6 enable**
5. **no ipv6 nd ra suppress**
6. **ipv6 nd ra interval** {*maximum-secs* [*minimum-secs*] | *msec maximum-msecs* [*minimum-msecs*]}
7. **ipv6 nd ra lifetime** *seconds*
8. **ipv6 nd ra initial** [**exponential**] *InitialAdvertInterval InitialAdvertisements*
9. **ipv6 nd prefix default** *infinite infinite* **off-link**
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template number`	Creates a virtual template interface, where number identifies the virtual template interface.
Step 4	**ipv6 enable** **Example:** `Router(config-if)# ipv6 enable`	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address. **Note** This command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing.
Step 5	**no ipv6 nd ra suppress** **Example:** `Router(config-if)# no ipv6 nd ra suppress`	Enables the sending of IPv6 router advertisement transmissions on non-LAN interface types (for example, serial or tunnel interfaces).
Step 6	**ipv6 nd ra interval** {*maximum-secs* [*minimum-secs*] | *msec maximum-msecs* [*minimum-msecs*]} **Example:** `Router(config-if)# ipv6 nd ra interval 21600`	Configures the interval between IPv6 RA transmissions on an interface.
Step 7	**ipv6 nd ra lifetime** *seconds* **Example:** `Router(config-if)# ipv6 nd ra lifetime 21600`	Configures the router lifetime value, in seconds, in IPv6 router advertisements on an interface.

	Command or Action	Purpose
Step 8	**ipv6 nd ra initial** [**exponential**] *InitialAdvertInterval InitialAdvertisements* **Example:** `Router(config-if)# ipv6 nd ra initial 3 3`	Configure the interval, in seconds, between IPv6 router advertisement transmissions, and the number of RAs sent during the initial phase on an interface. Optionally, specify the **exponential** keyword option to configure the value specified for the *InitialAdvertInterval* be used as the initial timer value and double on each subsequent transmission.
Step 9	**ipv6 nd prefix default infinite infinite off-link** **Example:** `Router(config-if)# ipv6 nd prefix default infinite infinted off-link` **ipv6 nd prefix** {*ipv6-prefix/prefix-length* | **default**} [**no-advertise** | [*valid-lifetime preferred-lifetime* [**off-link** | **no-rtr-address** | **no-autoconfig**]] | [**at valid-date** | *preferred-date* [**off-link** | **no-rtr-address** | **no-autoconfig**]]	Configures which IPv6 prefixes are included in IPv6 router advertisements.
Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.

Enabling IPv6 Support under an APN

The commands configured under an APN define the behavior of the IPv6 PDP contexts processed by that APN (such as the method of IPv6 address allocation to use), and also define GTP IPv6 elements (such as the IPv6 addresses of the primary and backup DNS).

For a complete list of APN-configuration options that are supported for IPv6 PDP contexts, see Chapter 9, “Configuring Network Access to the GGSN.”

To enable IPv6 support under an APN, complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-point** *access-point-index*
4. **access-point-name** *apn-name*
5. **ipv6 dns primary** *ipv6-address* [**secondary** *ipv6-address*]
6. **ipv6** [**enable** | **exclusive**]
7. **ipv6 ipv6-address-pool** {**local** *pool-name* | **radius-client**}
8. **ipv6 ipv6-access-group** *ACL-name* [**up** | **down**]
9. **ipv6 base-vtemplate** *number*
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**access-point** *access-point-index* **Example:** `Router(config)# access-point 2`	Specifies an access point number and enters access-point configuration mode.
Step 4	**access-point-name** *apn-name* **Example:** `Router(config-access-point)# access-point-name ipv6_apn1.com`	Specifies the network (or domain) name for a PDN that subscribers can access from the GGSN at a defined access point.
Step 5	**ipv6** [**enable** | **exclusive**] **Example:** `Router(config-access-point) ipv6 enable`	Configures an access point to allow IPv6 PDP contexts. • enable—Configures support for both IPv4 and IPv6 PDP contexts on the APN. • exclusive—Configures support for only IPv6 PDP contexts on the APN. By default, only IPv4 PDP contexts are supported on an APN.
Step 6	**ipv6 dns primary** *ipv6-address* [**secondary** *ipv6-address*] **Example:** `Router(config-access-point) ipv6 dns primary 2001:999::9`	Specifies the address of a primary (and backup) IPv6 DNS sent in IPv6 Create PDP Context response, if requested.
Step 7	**ipv6 ipv6-address-pool** {**local** pool-name | **radius-client**} **Example:** `Router(config-access-point) ipv6 ipv6-address-pool local localv6`	Configures a dynamic IPv6 prefix allocation method for an access-point. **Note** This release of the Cisco GGSN supports IPv6 prefix allocation via locally configured pools.
Step 8	**ipv6 ipv6-access-group** *ACL-name* [**up** | **down**] **Example:** `Router(config-access-point) ipv6 ipv6-access-group ipv6filter down`	Applies an access-control list (ACL) configuration to uplink or downlink payload packets.

	Command or Action	Purpose
Step 9	**ipv6 base-vtemplate** *number* **Example:** `Router(config-access-point) ipv6 base-vtemplate 10`	Specifies the base virtual template interface from which the APN copies IPv6 RA parameters when creating virtual subinterfaces for IPv6 PDP contexts.
Step 10	**exit** **Example:** `Router(config-access-point)# exit`	Exits interface configuration mode.

Configuring a Local IPv6 Prefix Pool

The function of prefix pools in IPv6 is similar to that of address pools in IPv4. The main difference is that IPv6 assigns prefixes rather than single addresses.

As for IPv4, an IP address can be obtained from a locally configured pool, or it can be retrieved from an AAA server. The Cisco GGSN supports prefix allocation via local pools.

When configuring a local IPv6 prefix pool, overlapping membership between pools is not permitted. Once a pool is configured, it cannot be changed. If you change the pool configuration, the pool is removed and re-created and all prefixes previously allocated are freed.

For detailed information on configuring local IPv6 prefix pools using the following commands, see *Cisco IOS IPv6 Configuration Guide*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 local pool** *poolname prefix/prefix-length assigned-length* [**shared**] [**cache-size** *size*]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

Step 3	**ipv6 local pool** *poolname prefix/prefix-length assigned-length* [**shared**] [**cache-size** *size*]
	
	Example:
	`Router(config)# ipv6 local pool pool1 2001:0DB8::/48 64`
	
	`Router# show ipv6 local pool`
	
	`Pool Prefix Free In use`
	
	`pool1 2001:0DB8::/48 65516 20`
		Configures a local IPv6 prefix pool.
		
		Note The value 64 must be configured as the assigned length. The minimum prefix length accepted by the GGSN is /48.

Step 4	**exit** **Example:** `Router(config)# exit`	Exits interface configuration mode.

Configuring an IPv6 Access Control List

IPv6 access control lists restrict IPv6-related traffic, based on the configured IPv6 filters. A filter contains the rules for matching an IP packet; if a packet matches, the rule also stipulates whether the packet are permitted or denied.

An IPv6 access control filter is applied to an APN by using the **ipv6 ipv6-access-group** command in access-point configuration mode.

For detailed information on configuring IPv6 Access Control Lists using the following commands, see *Cisco IOS IPv6 Configuration Guide*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **deny** *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [**operator** [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [**operator** [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number]* [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]
5. **permit** *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address}* [**operator** [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | *host destination-ipv6-address*} [**operator** [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | **mh-type**]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 access-list** *access-list-name* **Example:** `Router(config)# ipv6 access-list ipv6filter`	Defines an IPv6 access list name and places the GGSN in IPv6 access list configuration mode.
Step 4	**deny** *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [**operator** [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [**operator** [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**] **Example:** `Router(config-ipv6-acl)# deny ipv6 any 2001:200::/64`	Sets deny conditions for an IPv6 access list.
Step 5	**permit** *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [**operator** [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | *host destination-ipv6-address*} [**operator** [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | **mh-type**]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] **Example:** `Router(config-ipv6-acl)# permit ipv6 any any`	Sets permit conditions for an IPv6 access list.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits interface configuration mode.

Configuring Additional IPv6 Support Options

This section summarizes some other IPv6-specific options that you can configure on an access point.

Additional details about configuring several of these options are provided in other chapters of this book. These options apply to IPv6 PDP contexts only. A summary of all APN IPv6 configuration options is provided in Chapter 9, "Configuring Network Access to the GGSN."

To configure additional IPv6-specific options for a GGSN access point, use any of the following commands, beginning in access-point list configuration mode.

	Command	Purpose
Step 1	`Router(config-access-point)# ipv6 ipv6-access-group` *ACL-name* `[up | down]`	(Optional) Applies an access control list (ACL) configuration to uplink or downlink payload packets.
Step 2	`Router(config-access-point)# ipv6 redirect [all | intermobile]` *ipv6-address*	(Optional) Configures the GGSN to redirect IPv6 traffic to an external IPv6 device. The available options are: • **all—**Redirects all IPv6 traffic to an external IPv6 device for an APN. • **intermobile—**Redirects mobile-to-mobile IPv6 traffic to an external IPv6 device. • *ipv6-address*—IP address of the IPv6 external device to which you want to redirect IPv6 traffic.
Step 3	`Router(config-access-point)# ipv6 security verify source`	(Optional) Enables the GGSN to verify the IPv6 source address of an upstream Transport Protocol Data Unit (TPDU) against the address previously assigned to an MS.

Monitoring and Maintaining IPv6 PDPs

The following privileged EXEC **show** commands can be used to monitor the IPv6 configuration and IPv6 PDPs on the GGSN.

Command	Purpose
`Router# show gprs access-point`	Displays information about access points on the GGSN.
`Router# show gprs access-point statistics`	Displays data volume and PDP activation and deactivation statistics for access point on the GGSN.
`Router# show gprs access-point status`	Displays the number of active PDPs on an access point and how many of those PDPs are IPv4 PDPs, and an how many are IPv6 PDPs.
`Router# show gprs gtp pdp-context`	Displays a list of the currently active PDP contexts.
`Router# show gprs gtp status`	Displays information about the status of the GTP on the GGSN.
`Router# show gprs pcscf`	Displays a summary of the P-CSCF server group or groups configured on the GGSN for P-CSCF Discovery.

Configuration Example

The following example shows IPv6 support configured on a GGSN. The IPv6 related configuration statements appear in bold text:

```
ip cef
!
ipv6 unicast-routing
ipv6 cef
!
interface Virtual-Template10
  ipv6 enable
  no ipv6 nd ra suppress
  ipv6 nd ra interval 21600
  ipv6 nd ra lifetime 21600
  ipv6 nd ra initial 3 3
  ipv6 nd prefix default infinite infinite off-link
!
access-point 2
 access-point-name ipv6_test.com
  ipv6 dns primary 2001:999::9
  ipv6 enable
  ipv6 ipv6-address-pool local localv6
  ipv6 base-vtemplate 10
!
ipv6 local pool localv6 2001:234::/48 64
!
!
```

CHAPTER 6

Configuring GGSN GTP Session Redundancy

This chapter describes how to configure GPRS Tunneling Protocol session redundancy (GTP-SR) between two Cisco Gateway GPRS Support Nodes (GGSNs).

Note The Cisco GGSN supports GTP-SR for IPv4 Packet Data Protocol (PDP) contexts only.

For complete descriptions of the GGSN commands in this chapter, see *Cisco GGSN Command Reference*.

To locate documentation of other commands that appear in this chapter, use the command reference master index or search online. See the "Related Documents" section on page 3-12 for a list of other Cisco IOS software documentation that might be helpful when configuring the GGSN.

This chapter includes the following sections:

- GTP-SR Overview, page 6-1
- Enabling GTP Session Redundancy, page 6-6
- Disabling GTP Session Redundancy, page 6-15
- Configuring Charging-Related Synchronization Parameters, page 6-16
- Monitoring and Maintaining GTP-SR, page 6-18
- Upgrading GGSN Images in a GTP-SR Environment, page 6-18
- Configuration Examples, page 6-19

GTP-SR Overview

The GTP-SR supported by the Cisco GGSN enables two GGSNs configured on separate Cisco Service and Application Module for IP (SAMI) modules to appear as one network entity. If one of the GGSNs in a redundant configuration fails, GTP-SR ensures that continuous service is provided to mobile subscribers.

In a GTP-SR configuration, the active GGSN establishes and terminates PDP sessions, and sends the required stateful data to the standby GGSN. To stay current on the states of active PDP sessions, the standby GGSN receives the stateful data sent by the active GGSN. When the standby GGSN detects that the active GGSN has failed, it becomes active, and assumes the responsibilities of the active GGSN.

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.

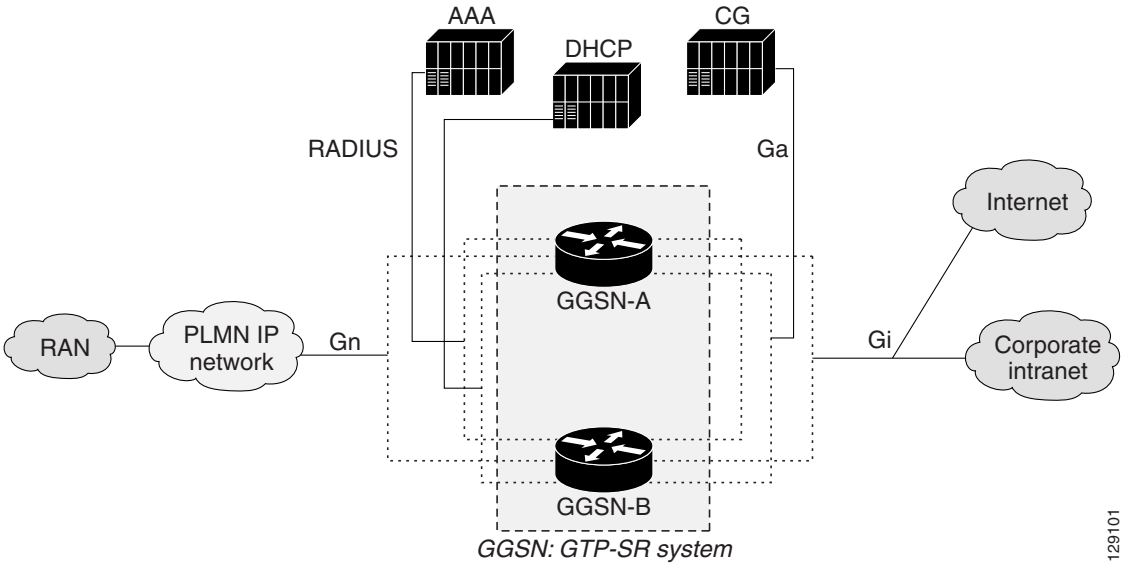
Note Before GTP-SR can be enabled on redundant GGSNs, a GTP-SR interdevice infrastructure must be configured between the GGSNs. For information on configuring the GTP-SR interdevice infrastructure, see the "Configuring the GTP Session Redundancy Interdevice Infrastructure" section on page 6-7.

In the GTP-SR configuration examples (Figure 6-1 and Figure 6-2):

- The components of GTP-SR are active and standby operation modes, stateful session synchronization, and switchover event detection and recovery.
- Active and standby operation
  - The GGSN is active or standby based on configuration.
  - For geographical redundancy implementations, the active GGSN receives packets based on route advertisement via a routing protocol. For local redundancy implementations, the active GGSN receives packets based on MAC address insertion.
  - The active GGSN processes control messages and tunnels subscriber data traffic.
  - The standby GGSN maintains session states and forwarding entries to minimize data loss.
- Stateful session sychronization
  - Session persistence is maintained for switchover
  - 1-to-1 stateful session synchronization is supported
  - The active GGSN downloads all sessions to standby GGSN
  - For maximum network bandwidth efficiency, only the changed states and bundling events are delivered in messages.
  - Reliable transport is used for sychnronization

Figure 6-1 illustrates a local GTP-SR implementation.

Figure 6-1 Local GTP-SR Implementation

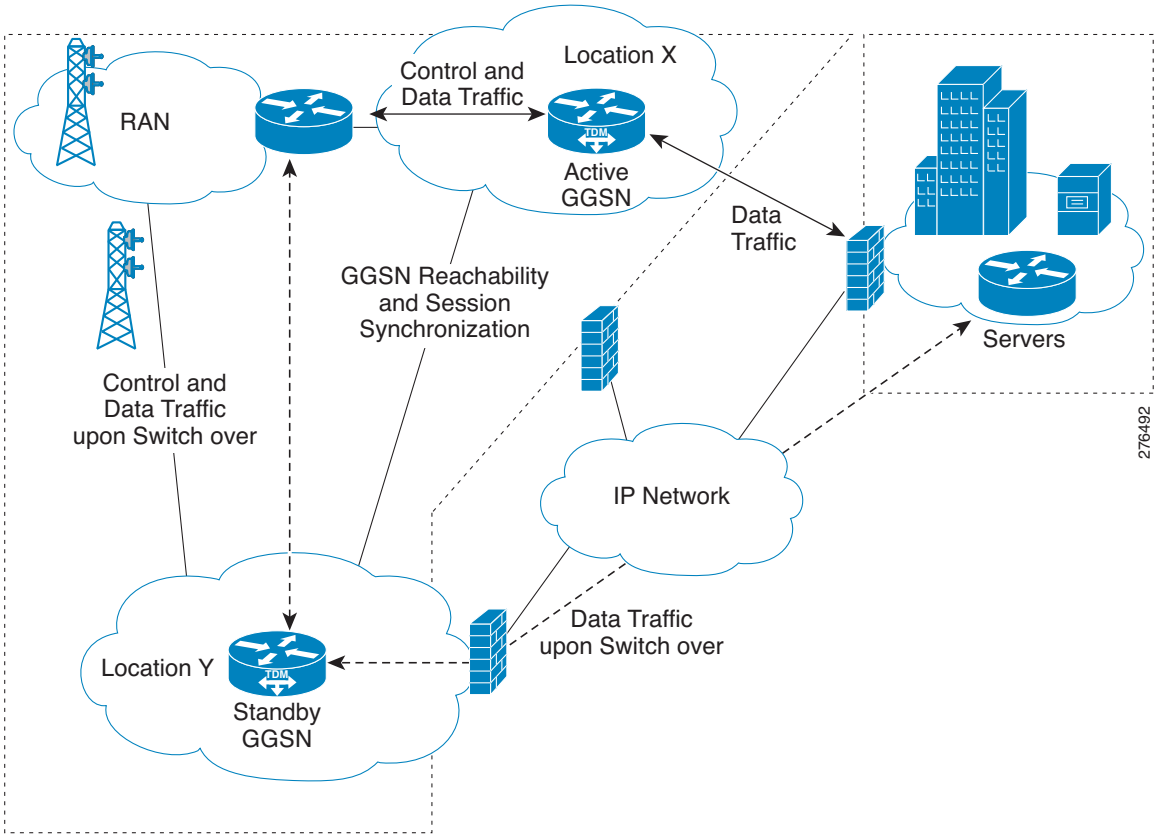


Local GTP-SR Notes

- L2 HSRP provides local GTP-SR support.
- Active GGSN and standby GGSN are located in the same local site (on the same LAN).
- Active and standby GGSNs are configured to participate in the same local HSRP group.
- HSRP transport is L2-based multicasting.

Figure 6-2 illustrates a geographical GTP-SR implementation.

Figure 6-2 Geographical GTP-SR Implementation



Geographical GTP-SR Notes

- L3 HSRP provides geographical GTP-SR support.
- Active GGSN and standby GGSN are located in geographically separate locations that are connected over a WAN.
- Active and standby GGSNs are configured to participate in the same geographical HSRP group.
- HSRP transport is IP unicast routing. This requires that the unicasting IP addresses be routable between the two locations.
- L2 and L3 HSRP are mutually exclusive, therefore, when L3 HSRP is enabled, L2 HSRP is automatically disabled.
- Only an active GGSN should advertises routes using the Open Shortest Path First (OSPF) as the Interior Gateway Protocol (IGP), therefore, GGSN interfaces must be configured not to form OSPF adjacency when functioning as a standby GGSN.

Prerequisites

GTP-SR on the Cisco GGSN requires the following:

- Two Cisco 7600 series routers in which a Cisco Supervisor Engine 720 (Sup720) and RSP, with a Multilayer Switch Feature Card (Cisco Product ID: SUP720-MSFC3-BXL) is installed.

  For local redundancy, the Sup720 must be running Cisco IOS Release 12.2(33)SRB1 or later. For geograhpical redundancy, the Sup720 must be running Cisco IOS Release 12.2(33)SRC or later.
- Two Cisco SAMIs in each of the Cisco 7600 series routers. The Cisco SAMI processors must be running the same Cisco GGSN release; Cisco IOS Release 12.4(15)XQ or later for local redundancy, or Cisco IOS Release 12.4(22)YE1 for geographical redundancy.
- HSRP Version 2.
- Except for certain protocol-related configurations that need to be distinct, such as the IP addresses of the HSRP-enabled interfaces and the remote IP addresses in the SCTP configuration, the active GGSN and the standby GGSNs must have the same configuration. Each configuration must be completed in the same order on both GGSNs in the GTP-SR configuration.
- When loading or upgrading a new Cisco GGSN image, both GGSNs must be loaded (virtually) together.
- On the serving GPRS support node (SGSN), the values configured for the number of GTP N3 requests and T3 retransmissions must be larger than the value or the switchover timer. This configuration enables requests sent during a switchover to be serviced by the newly active GGSN rather than dropped.
- Using the **ip radius source-interface** command in global configuration mode, RADIUS must be configured to use the IP address of a specified interface for all outgoing RADIUS packets.

Limitations and Restrictions

The the following limitations and restrictions apply to GTP-SR:

- PDP Contexts —Redundancy is not supported for the following types of PDP contexts. With a switchover, these PDP contexts require reestablishment on the newly active GGSN.
  - IPv6 PDPs
  - PPP type PDPs
  - PPP regeneration / L2TP access PDPs
  - Network initiated PDPs
- Timers—Except for the session timer, GGSN timers are not synchronized with the standby GGSN. When a switchover occurs, the timers on the newly active GGSN are incrementally restarted. Incrementally restarting the timers prevents them from expiring simultaneously.

  When a PDP context is re-created on the standby GGSN, the session timer is restarted with the elapsed time subtracted from the value of the initial session timer. Once the session expires on the standby GGSN, the PDP context is deleted.
- Counters—If a switchover occurs, status counters such as "cgprsAccPtSuccMsActivatedPdps," and some statistics counters have a non-zero value that is the value of the counter when the switchover occurred. All other counters are reset to zero.

  If a GGSN reload occurs, all counters are set back to zero.

- Sequence numbers related to GTP signaling and data are not synchronized between the active GGSN and the standby GGSN.
- Charging—All pertinent information for establishing charging on the standby GGSN for a PDP context is synchronized; however, the user data related charging information for a PDP context is not sychronized. Therefore, all CDRs in the previously active GGSN that were not sent to the charging gateway are lost when a switchover occurs.
- Once a GTP-SR configuration is established between two GGSNs, modifying the configuration of one of the GGSNs might cause the GGSN to reload before the changes can be saved. To ensure that configuration changes are not lost, disable GTP-SR before modifying the configuration of a GGSN. For information on disabling GTP-SR, see the "Disabling GTP Session Redundancy" section on page 6-15.
- In a GTP session redundancy (GTP-SR) environment, *do not* use the **clear gprs gtp pdp-context** command on the standby GGSN. If you issue this command on the standby GGSN, you are prompted to confirm before the command is processed. To determine if the redundancy state of a GGSN is active or standby, use the **show gprs redundancy** command.
- When configuring geographical redundancy:
  - L2 and L3 HSRP are mutually exclusive.
  - Migrating from L2 to an L3 HSRP configuration requires a system reload.
  - If using Cisco GGSN Release 10.0 or later, OSPF cannot be used on the Cisco SAMI for learning routes to any of the external nodes such as the RADIUS server, SGSN, etc. However, OSPF like routing protocols can be run on the supervisor with static or default routes configured on the Cisco SAMI pointing to the supervisor.
  - When using L3 HSRP, the Cisco Content Services Gateway - 2nd Generation does not switch over when the Cisco GGSN switches over, therefore, the user might be overcharged.
  - Cisco IOS Release 12.2(33)SRC has a per-chassis limitation of 1000 Border Gateway Protocol (BGP) peers or 1000 OSPF neighbors, therefore, per GGSN on a Cisco SAMI PPC, 160 BGP peers or 160 OSPF neighbors.
  - The source interfaces (RADIUS, charging, Diameter, etc.) must be configured with the same IP address on both the active and standby GGSNs, and be distributed through the OSPF routing protocol .

Enabling GTP Session Redundancy

To configure GTP-SR, complete the tasks, in the order in which they are presented, in the following sections:

- Configuring the GTP Session Redundancy Interdevice Infrastructure, page 6-7
- Configuring Passive Route Suppression on an Interface, page 6-14
- Enabling GTP-SR on the GGSN, page 6-15

Configuring the GTP Session Redundancy Interdevice Infrastructure

The GTP-SR feature uses the Cisco IOS CF to send stateful data over SCTP to a redundantly configured GGSN. In addition, the Cisco GGSN uses the Cisco IOS RF in conjunction with Cisco IOS HSRP to monitor and report transitions on active GGSNs and standby GGSNs.

To configure the GTP-SR interdevice infrastructure before enabling GTP-SR on redundant GGSNs, complete the tasks in the following sections

- Configuring HSRP, page 6-7
- Enabling Interdevice Redundancy, page 6-12
- Configuring the Interdevice Communication Transport, page 6-12

Configuring HSRP

The HSRP is a protocol typically used for redundancy. The HSRP provides high network availability because it routes IP traffic from hosts on networks without relying on the availability of any single router.

In a group of routers, the HSRP is used for selecting an active router and a standby router. The HSRP monitors both the inside and outside interfaces so that if any interface goes down, the whole device is deemed to be down. When a device is deemed to be down, the standby device becomes active and takes over the responsibilities of an active device.

Specifically, the HSRP provides the following:

- Dynamic active and standby role selection
- Heartbeat for failure detection
- Method to receive packets only on the active GGSN

To support Layer 3 geographical redundancy, the HSRP has enhanced these three functions as follows:

- Role selection is based on IP unicast routing instead of link-local multicast
- Heartbeat is also an IP unicast message between peers instead of link-local multicast, and triggers active GGSN to advertise routes
- Routes for GGSN IP address and subscriber networks are advertised (by active GGSN) instead of listening to a virtual MAC address for directing traffic to the active GGSN.

Note In HSRP, the virtual IP address and MAC address are used for receiving packets. These addresses are unnecessary when routing is used for L3 geographical redundancy. Therefore, when implementing L3 geographical redundancy, the virtual IP address in the HSRP group is set to zero.

Restrictions and Recommendations

When configuring HSRP, the following recommendation and restrictions apply:

- At minimum, HSRP must be enabled and an HSRP *primary* group defined on one interface per GGSN. Each additional HSRP interface on the GGSN with its own separate VLAN can be configured as a *client* group.

  The client group feature enables all interfaces configured as a client group to share the HSRP parameters of the primary group. This facilitates HSRP group setup and maintenance in environments that contain numerous GGSN interfaces and HSRP groups. The primary group and associated client groups share the same group track states and have the same priority.

Typically, HSRP groups are needed on the following interfaces. One group is configured as the primary group and the rest as client groups. Each interface must be configured on a different VLAN.

  - Gn interface—primary group
  - Ga interface—client group
  - DHCP (can be shared with the Gi interface)—client group
  - Gi APN (per VRF)—client group
  - RADIUS—client group
  - Diameter—client group
  - Quota Server—client group

  To configure additional interfaces as a HSRP client group, use the **standby** command in interface configuration mode and specify the **follow** keyword option with the same group number as the primary group.

- Use the same group number that is used for the primary group for each client group. Using the same group number for the primary group and client groups facilitates HSRP group setup and maintenance in an environment that contains numerous GGSN interfaces and HSRP groups.
- The same HSRP group cannot be used on another active/standby GGSN pair mapped to the same physical VLAN.
- When HSRP is configured on an interface, a preemption delay can be configured using the **standby preempt** command in interface configuration mode; however, in a GTP-SR configuration, we recommend not configuring a preemption delay unless absolutely necessary. Not configuring a preemption delay prevents any unnecessary switchovers. If a preemption delay must be configured, ensure that a sufficient delay is specified so that bulk synchronization can complete before preemption takes effect.
- When implementing local redundancy, when the **standby use-bia** command is not used to allow bridges and gateways to learn the virtual MAC address, for optimization purposes, configure the **standby mac-refresh** command to a value greater than the default. By default, hello messages are sent every 3 seconds under the main interface (gig 0/0). Once configured, all HSRP groups (primary and follow) will send hello messages only if the node is in active mode.

Note A GGSN reloads if additional HSRP configurations are added after the initial HSRP setup is configured.

For complete information on configuring Cisco IOS HSRP, see the "Configuring the Hot Standby Router Protocol" section of the *Cisco IOS IP Configuration Guide*, Release 12.3.

Enabling L2 HSRP and Configuring a Local HSRP Primary Group on an Interface

L2 HSRP is the default HSRP. L2 HSRP supports local redundancy (redundancy between two Cisco GGSNs on the same LAN).

To enable L2 HSRP on an interface and configure the primary group, use the following commands in interface configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface GigabitEthernet0/number`	Configures 1000-Mbps Ethernet interface and enters interface configuration mode.
Step 2	`Router(config-if)# encapsulation dot1Q vlan_id`	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN).
Step 3	`Router(config-if)# ip address ip address ip-address mask`	Sets a primary IP address for an interface.
Step 4	`Router(config-if)# standby version 2`	Enables HSRP Version 2.
Step 5	`Router(config-if)# standby [group-number] ip [ip-address [secondary]]`	Enables the HSRP on the interface.
Step 6	`Router(config-if)# standby [group-number] priority priority`	(Optional) Sets the hot standby priority used in choosing the active router. The priority value range is from 1 to 255. The value of 1 denotes the lowest priority and 255 denotes the highest priority. For example, if the local router has priority over the current active router, the local router will attempt to take its place as the active router.
Step 7	`Router(config-if)# standby [group-number] name name`	Specifies the name of the standby group.
Step 8	`Router(config-if)# standby use-bia [scope interface]`	(Optional) Configures HSRP to use the burned-in address (BIA) of an interface as its virtual MAC address instead of using the preassigned MAC address.

The following is an example of a L2 HSRP configuration:

```
interface GigabitEthernet0/0.7
 encapsulation dot1Q 21
 ip address 172.2.2.1 255.255.0.0
 standby 1 ip 172.2.2.10
 standby 1 name local
```

Enabling L3 HSRP and Configuring a Geographical HSRP Primary Group on an Interface

L3 HSRP supports geographical redundancy. Geographical redundancy is redundancy between two Cisco GGSNs located in geographically separate locations, connected by a WAN.

In a geographical redundancy implementation, only the active device needs to send routing updates. Therefore, when configuring an L3 HSRP group, you must also configure the interfaces to not send routing updates when the GGSN is the standby GGSN. For information on enabling passive route suppression see "Configuring Passive Route Suppression on an Interface" section on page 6-14.

To enable L3HSRP on an interface and configure the primary group, use the following commands in interface configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface GigabitEthernet0/number`	Configures 1000-Mbps Ethernet interface and enters interface configuration mode.
Step 2	`Router(config-if)# encapsulation dot1Q vlan_id`	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN).
Step 3	`Router(config-if)# ip address ip address ip-address mask`	Sets a primary IP address for an interface.
Step 4	`Router(config-if)# standby version 2`	Changes the HSRP version to HSRP Version 2.
Step 5	`Router(config-if)# standby [group-number] ip none`	Enables the HSRP on the interface and disables Virtual IP (VIP) learning from HSRP messages. VIP learning is not used for L3 HSRP.
Step 6	`Router(config-if)# standby [group-number] priority priority`	(Optional) Sets the hot standby priority used in choosing the active router. The priority value range is from 1 to 255. The value of 1 denotes the lowest priority and 255 denotes the highest priority. For example, if the local router has priority over the current active router, the local router will attempt to take its place as the active router.
Step 7	`Router(config-if)# standby [group-number] name name`	Specifies the name of the standby group.
Step 8	`Router(config-if)# standby group-number unicast destination destination-ip [source source-ip]`	Configures the HSRP group to use IP unicast routing, and sets the destination and source addresses of the peer devices. Up to four destinations can be defined. Configuring the standby **unicast command** sets the Virtual IP (VIP) to 0.0.0.0 and the virtual MAC address to that of the interface. Once unicast transport is enabled, the original L2-based multicast transport is automatically disabled. The **source** *ip-address* keyword option, if specified, is the source IP address of the HSRP packet. If not specified, the source IP address is taken from the corresponding interface configuration.

The following is an example of an L3 HSRP configuration:

Primary GGSN

```
interface GigabitEthernet0/0.7
 encapsulation dot1Q 21
 ip address 10.0.0.3 255.255.0.0
 standby 1 ip none
 standby 1 name geo
 standby 1 unicast destination 172.0.0.1
```

Standby GGSN

```
interface GigabitEthernet0/0.8
 encapsulation dot1Q 21
 ip address 172.0.0.1 255.255.0.0
 standby 1 ip none
 standby 1 name geo
 standby 1 unicast destination 10.0.0.3
```

Configuring HSRP Client Groups

Once HSRP is enabled and the primary group is configured on a GGSN interface, additional GGSN interfaces can be configured to share the HSRP parameters of the primary group by configuring those interfaces as HSRP client groups.

To configure a GGSN interface as an client group, use the **standby** command and specify the **follow** keyword option using the same group number and name as the primary group.

Interfaces that share a group track states together and have the same priority.

Note HSRP group parameters such as priority, name, tracking, and timers are configured under the primary group only. Do not configure these parameters under client groups because the groups inherit them from the primary group.

To configure an interface to follow a primary group, use the following commands in interface configuration mode:

	Command	Purpose
Step 1	`Router(config-if)# standby` *group-number* **ip** [*virtual-ip-address* | **none**]	Specifies the group number and: • *virtual-ip-address*—For L2 HSRP, specifies the virtual IP address of the client group. (The group number specified must be the same as the primary group number.) • **none**—For L3 HSRP, disables Virtual IP (VIP) learning from HSRP messages.
Step 1	`Router(config-if)# standby` *group-number* **follow** *group-name*	Specifies the number and name of the primary group for the client group to follow and share status. **Note** The group number specified must be the same as the primary group number.

Enabling Interdevice Redundancy

The HSRP primary group is associated with Cisco IOS RF to enable session redundancy between two GGSNs.

To enable interdevice redundancy, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# redundancy inter-device`	Configures redundancy and enters interdevice configuration mode. To remove all interdevice configuration, use the **no** form of the command.
Step 2	`Router(config-red-interdevice)# scheme standby` *standby-group-name*	Defines the redundancy scheme to use. Currently, "standby" is the only supported scheme. • *standby-group-name*—Must match the standby name specified by the **standby name** command (see the "Configuring HSRP" section on page 6-7). Also, the standby name should be the same on both GGSNs in a redundant configuration.
Step 3	`Router(config-red-interdevice)# exit`	Returns to global configuration mode.

Configuring the Interdevice Communication Transport

Interdevice redundancy requires a transport for communication between the redundant GGSNs. This transport is configured using Interprocess Communication (IPC) commands.

To configure the interdevice communication transport between the two GGSNs, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ipc zone default`	Configures the Interdevice Communication Protocol (IPC) and enters IPC zone configuration mode. Use this command to initiate the communication link between the active GGSN and the standby GGSN.
Step 2	`Router(config-ipczone)# association 1`	Configures an association between two GGSNs and enters IPC association configuration mode. In IPC association configuration mode, you configure the details of the association. These details include the transport protocol, local port and local IP addresses, and the remote port and remote IP addresses. The valid association IDs range from 1 to 255. There is no default value.

	Command	Purpose
Step 3	`Router(config-ipczone)# no shutdown`	Restarts a disabled association and its associated transport protocol. **Note** Shutdown of the association is required for any changes to the transport protocol parameters.
Step 4	`Router(config-ipczone-assoc)# protocol sctp`	Configures SCTP as the transport protocol for this association and enables SCTP protocol configuration mode.
Step 5	`Router(config-ipc-protocol-sctp)# local-port` *local_port_num*	Defines the local SCTP port number and enables IPC Transport-SCTP local configuration mode. The local SCTP port is used to communicate with the redundant peer. The valid port number range is from 1 to 65535. There is no default. **Note** The local port number should be the same as the remote port number on the peer router.
Step 6	`Router(config-ipc-local-sctp)# local ip` *ip_addr*	Defines the local IP address that is used to communicate with the redundant peer. The local IP address must match the remote IP address on the peer router.
Step 7	`Router(config-ipc-local-sctp)# keepalive` [*period* [*retries*]]	(Optional) Enables keepalive packets. Optionally, specifies the number of times the Cisco IOS software attempts to send keepalive packets without a response before bringing down the interface or tunnel protocol for a specific interface. The valid value for *period* is an integer value in seconds great than 0. The default is 10. The valid value for *retries* is an integer value greater than one and less than 355. The default is the previously used value or 5 if there was no value previously specified.
Step 8	`Router(config-ipc-local-sctp)# retransmit-timeout` *interval*	(Optional) Configures the message retransmission time. The valid range is from 300 to 60000 milliseconds. The default is minimum 300 and maximum 600.
Step 9	`Router(config-ipc-local-sctp)# path-retransmit` *number*	(Optional) Configures the maximum number of keepalive retries before the corresponding destination address is marked inactive. The valid range is from 2 to 10. The default is 4.
Step 10	`Router(config-ipc-local-sctp)# assoc-retransmit` *number*	(Optional) Defines the maximum retransmissions over all destination addresses before an association is declared failed. The valid range is from 2 to 20. The default is 4.

	Command	Purpose
Step 11	`Router(config-ipc-local-sctp)# max-inbound-streams max-streams`	(Optional) Configures the maximum number of inbound streams allowed for the local port. The valid range is from 2 to 25. The default is 17 streams.
Step 12	`Router(config-ipc-local-sctp)# init-timeout msec`	(Optional) Configures the maximum interval for the init packet retransmission time-out value. The valid range is from 1000 to 60000 milliseconds. The default is 1000 milliseconds.
Step 13	`Router(config-ipc-local-sctp)# exit`	Exits IPC transport - SCTP local configuration mode.
Step 14	`Router(config-ipc-protocol-sctp)# remote-port port_nun`	Defines the remote SCTP port number and enables IPC Transport-SCTP remote configuration mode. The remote SCTP port is used to communicate with the redundant GGSN. The valid port numbers range is from 1 to 65535. There is no default. **Note** The remote port number should be the same as the local port number on the peer GGSN.
Step 15	`Router(config-ipc-remote-sctp)# remote-ip ip_addr`	Defines the remote IP address of the redundant GGSN that is used to communicate with the local device. All remote IP addresses must refer to the same GGSN.

To remove an association, use the **no** form of the command.

Configuring Passive Route Suppression on an Interface

In a geographical redundancy implementation, only the active GGSN advertises routes. Therefore, interfaces must be configured to stop redistributing routes when the GGSN become a standby GGSN.

To configure passive route suppression on an interface, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# passive-interface [default] interface-type interface-number [on-standby]`	Configures the suppression of routing updates on an interface (OSPF adjacency is not formed with a neighbor on the supervisor). Optionally, specify the **on-standby** keyword option to configure the suppression of routing updates on an interface only when in standby mode.

In the following example, two GigabitEthernet interfaces are configured to suppress routing updates when the GGSN is the standby GGSN:

```
router ospf 100
 router-id 30.30.30.30
 no log-adjacency-changes
 redistribute static subnets
 passive-interface GigabitEthernet0/0.100 on-standby
 network 10.0.0.0 0.0.0.255 area 0
 network 1.1.1.10.0.0.0 area 0
!
router ospf 200 vrf Gi-VRF
 no log-adjacency-changes
 redistribute static route-map xxx
 passive-interface GigabitEthernet0/0.200 on-standby
 network 11.0.0.0 0.0.0.255 area 1
```

Enabling GTP-SR on the GGSN

To enable GTP-SR, use the following command in global configuration mode on each of the redundant GGSNs:

Command	Purpose
`Router(config)# gprs redundancy`	Enables GTP-SR on the GGSN.

Disabling GTP Session Redundancy

To disable GTP-SR (at both the GGSN application level and the interdevice infrastructure level), complete the following tasks in the order in which they are listed. Ensure that the GGSN is in standby mode when you start these tasks.

1. Verify that the GGSN is in standby mode and disable the GGSN application-level redundancy.

   ```
   Router(config)# show gprs redundancy
   ...
   Router(config)# no gprs redundancy
   ```

   The GGSN becomes a standalone active GGSN.

2. Remove the standby scheme configured under interdevice configuration mode.

   ```
   Router(config)# redundancy inter-device
   Router(config-red-interdevice)# no scheme standby HSRP-Gn
   ```

3. Save the configuration changes to memory.

   ```
   Router(config)# write memory
   ```

4. Reload the router.

   ```
   Router# reload
   ```

   Once the GGSN comes back up, additional configuration changes can be made and saved without the GGSN reloading.

5. Disable SCTP by disabling the association between the two devices and deconfiguring SCTP.

   ```
   Router(config)# ip zone default
   ```

```
Router(config-ipczone)# association 1
Router(config-ipczone-assoc)# shutdown
...
Router(config-ipczone-assoc)# no protocol sctp
```

6. To remove the HSRP configuration associated with an interface, use the **no** forms of the relevant HSRP commands. Remove the HSRP group configuration for the client groups first.

```
Router(config)# interface GigabitEthernet0/0.56001
Router(config-if)# no standby 52 ip 172.90.1.52
Router(config-if)# no standby 52 follow HSRP-Gn
Router(config-if)# no standby version 2
Router(config-if)# exit

Router(config)# interface GigabitEthernet0/0.401
Router(config-if)# no standby 52 ip 192.1268.1.52
Router(config-if)# no standby 52 name HSRP-Gn
Router(config-if)# no standby version 2
Router(config-if)# exit
```

7. Save configuration changes to memory:

```
Router(config)# write memory
```

Configuring Charging-Related Synchronization Parameters

Charging-related data necessary to establish charging for a PDP context is synchronized with the standby GGSN. This data includes:

- Charging Identity (CID) associated with a PDP context
- Local sequence number
- Record sequence number
- GTP' sequence number
- Per service local sequence number

Note For geographical redundancy, you must configure the charging source interface with the same IP address on boththe active and standby GGSNs, and the address should be distributed via the OSPF routing protocol.

Charging Identity (CID) and Local Record Sequence Number

When an established PDP context is synchronized, the CID assigned to the PDP context's call detail record (CDR) is also synchronized with the standby GGSN. When the standby GGSN receives the synchronized data for the PDP context, if the CID value provided is greater than the current value of the global CID counter, the standby GGSN writes the value to the global CID counter. If a switchover occurs, the newly active GGSN starts from the latest CID value that was written, plus a window/offset for all new PDP contexts created on the newly active GGSN.

When the CID timer of the active GGSN expires, and the active GGSN writes the global CID counter value to memory, the CID value and local record sequence (if configured) are synchronized with the standby GGSN, and the standby GGSN writes the information to memory. If the local sequence number is also configured, when the write timer associated with the local sequence number expires, both the CID

and the local sequence number are synchronized with the standby GGSN. When the standby GGSN becomes active, it uses the local record sequence number, plus the latest CID value written to memory, plus a window/offset for subsequent PDP contexts created on the newly active GGSN.

Record Sequence Number

The charging gateway uses the record sequence number to detect duplicate CDRs associated with a PDP context.

To minimize the amount of data being synchronized with the standby GGSN, the record sequence number is not synchronized each time a CDR is closed. Instead, a window threshold for the record sequence number is synchronized each time a CDR closes.

The current value of the record sequence number and the record number last synchronized for a PDP context are checked. If the difference in their values is the value configured for the window size, the current record sequence number is synchronized with the standby GGSN. When a standby GGSN becomes the active GGSN, it starts from the last value synchronized plus the window size.

To configure the window size that determines when the CDR record sequence number is synchronized with the standby GGSN, use the following command in global configuration mode:

Command	Purpose
`Router# gprs redundancy charging sync-window cdr rec-seqnum size`	Configures the window size used to determine when the CDR record sequence number is synchronized. The valid range is from 1 to 20. The default is 10.

GTP' Sequence Number

The charging gateway uses the GTP' sequence number to prevent the duplication of packets. The GGSN sends encoded CDRs associated with a PDP context in a GTP packet to the charging gateway. If the charging gateway acknowledges the GTP packet, it removes the packet from memory. If it is not acknowledged, it is retransmitted. The charging gateway cannot acknowledge GTP packets if the sequence number repeats.

To minimize the amount of data being synchronized with the standby GGSN, the GTP' sequence number is not synchronized each time a CDR is closed. Instead, a window threshold for the GTP' sequence number is synchronized each time a CDR message is sent. The current value of the GTP' sequence number and the GTPP sequence number last synchronized for a PDP context are checked. If the difference in their values is the value configured for the window size, the GTP prime sequence number is synchronized with the standby GGSN. When a standby GGSN becomes the active GGSN, it starts from the last value synchronized plus the window size.

To configure the window size that determines when the GTP' sequence number is synchronized with the standby GGSN, use the following command in global configuration mode:

Command	Purpose
`Router# gprs redundancy charging sync-window gtpp seqnum size`	Configures the window size that determines when the GTP' sequence number is synchronized. The valid range is from 5 to 65535. The default is 10000. **Note** A GGSN can transmit 128 GTP packets without any acknowledgement. Therefore, we recommend that you configure the window size to be greater than 128.

Per Service Local Sequence Number

The charging gateway uses the per service local sequence number to detect duplicate service containers associated with a PDP context.

To minimize the amount of data being synchronized to the standby GGSN, the per service local sequence number is not synchronized each time a gateway GPRS support node-call detail record (G-CDR) is closed. Instead, the current value of the local sequence number and the local sequence number last synchronized for a PDP context is checked, and if the difference is more than the configured window size, the current local sequence number is synchronized with the standby GGSN. When a standby GGSN becomes the active GGSN, it starts from the last value synchronized, plus the window size.

To configure the window size that determines when the per service local sequence number is synchronized with the standby GGSN, use the following command in global configuration mode:

Command	Purpose
`Router# gprs redundancy charging sync-window svc-seqnum size`	Configures the window size that determines when the per service local sequence number is synchronized with the standby GGSN. A valid value is a number between 1 and 200. The default is 50.

Monitoring and Maintaining GTP-SR

The following privileged EXEC **show** commands can be used to monitor the different elements of the GTP-SR configuration.

Command	Purpose
`Router# show gprs redundancy`	Displays statistics related to GTP-SR.
`Router# show redundancy [clients | counters | events | history | states | switchovers]`	Displays current or historical status and related information on planned or logged handovers.
`Router# show standby`	Displays HSRP information.

Upgrading GGSN Images in a GTP-SR Environment

To upgrade to a new Cisco GGSN image on the Cisco SAMI, complete the following tasks:

1. Identify all application entities (GGSN images) on the SAMI by using the **show version** command on the LCP (PPC0) console.
2. Using the Cisco IOS SLB **no inservice** command, remove all GGSNs on the Cisco SAMI processors from the GTP server load balancing (SLB) list on the supervisor. This prevents a GGSN from receiving new Create PDP Context requests, but allows it to continue servicing existing PDP contexts.
3. Wait until all PDP contexts are cleared or manually clear PDP contexts by using the **clear gprs gtp pdp-context** command.
4. Load the new images onto the SAMI, and reset the SAMI as described in the *Cisco Service and Application Module for IP User Guide*.

5. Once the images have been reloaded, return the GGSNs to the GTP SLB list by using the Cisco IOS SLB **inservice** command on the supervisor.

For complete information on upgrading application images on the Cisco SAMI, see *Cisco Service and Application Module for IP User Guide.*

Configuration Examples

This section provides the following configuration examples:

- Local GTP-SR Examples, page 6-20
- Geographical GTP-SR Examples, page 6-25

Note The following configurations examples are just samples of configurations. Actual configurations vary based on network design.

Local GTP-SR Examples

This section contains the following configuration examples from a local GTP-SR implementation:

- Primary Supervisor Configuration Example, page 6-20
- Primary GGSN Configuration Example, page 6-22
- Secondary GGSN Configuration Example, page 6-24

Primary Supervisor Configuration Example

The following example shows part of a sample configuration on the Primary Supervisor. Some commands that you use to configure GTP-SR are highlighted in bold text.

```
sup-primary# show running-config
Building configuration...

Current configuration : 7144 bytes
!
! Last configuration change at 12:28:26 UTC Tue Oct 21 2003
! NVRAM config last updated at 13:32:08 UTC Thu Oct 16 2003
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname sup-primary
!
...
!
svclc multiple-vlan-interfaces
svclc module 7 vlan-group 71,73
svclc vlan-group 71 71 svclc vlan-group 73 95,100,101
ip subnet-zero
!
no ip domain-lookup
!
interface GigabitEthernet2/1
 description "VLAN for Inter-dev SCTP"
 no ip address
 switchport
 switchport access vlan 498
 switchport mode access
 no cdp enable
!
...
!
interface FastEthernet3/25
 description "VLAN for Gn"
 no ip address
 duplex full
 switchport
 switchport access vlan 410
 switchport mode access
 no cdp enable
!
interface FastEthernet3/26
 description "VLAN for Gi"
 no ip address
 duplex full
```

```
 switchport
 switchport access vlan 420
 switchport mode access
!
...
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan410
 description "Virtual LAN for Gn interface for all GGSNs on an SAMI"
 ip address 10.20.21.1 255.255.255.0
 no ip redirects
!
interface Vlan420
 description "One Gi Vlan all GGSN images of mwmam"
 ip address 10.20.51.1 255.255.255.0
 no ip redirects
!
interface Vlan498
 description "VLAN for Inter-dev_SCTP"
 ip address 10.70.71.1 255.255.255.0
!
router ospf 1
 router-id 10.20.1.2
 log-adjacency-changes
 summary-address 10.20.30.0 255.255.255.0
 redistribute static subnets route-map GGSN-routes
 network 10.20.1.0 0.0.0.255 area 1
!
ip classless
ip route 0.0.0.0 0.0.0.0 128.107.234.100
ip route 1.8.0.0 255.255.0.0 1.8.0.1
ip route 1.12.0.0 255.255.0.0 1.12.0.1
ip route 10.2.5.0 255.255.255.0 10.2.15.1
ip route 10.20.30.11 255.255.255.255 10.20.21.81
ip route 10.20.30.12 255.255.255.255 10.20.21.82
ip route 10.20.30.13 255.255.255.255 10.20.21.83
ip route 10.20.30.14 255.255.255.255 10.20.21.84
ip route 10.20.30.15 255.255.255.255 10.20.21.85
ip route 110.1.0.0 255.255.0.0 10.20.51.91
ip route 120.1.0.0 255.255.0.0 10.20.51.92
ip route 128.107.241.185 255.255.255.255 128.107.234.161
ip route 130.1.0.0 255.255.0.0 10.20.51.93
ip route 140.1.0.0 255.255.0.0 10.20.51.94
ip route 150.1.0.0 255.255.0.0 10.20.51.95
ip route 172.19.23.55 255.255.255.255 172.19.24.1
ip route 223.0.0.0 255.0.0.0 1.8.0.1
ip route 223.0.0.0 255.0.0.0 1.12.0.1
no ip http server
no ip http secure-server
ip pim bidir-enable
!
!
access-list 1 permit 10.20.30.0 0.0.0.255
access-list 101 permit ip 128.107.234.160 0.0.0.31 any
access-list 102 permit ip any 128.107.234.160 0.0.0.31
arp 127.0.0.22 0000.2200.0000 ARPA
!
route-map GGSN-routes permit 10
 match ip address 1
!
!
```

```
line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 exec-timeout 0 0
 password abc
 logging synchronous
 transport input lat pad mop telnet rlogin udptn nasi
line vty 5 15
 exec-timeout 0 0
 password abc
 logging synchronous
!
ntp master
end

sup-primary#
```

Primary GGSN Configuration Example

```
Active_GGSN# show running-config
Building configuration...

Current configuration : 2942 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service gprs ggsn
no service dhcp
!
hostname Act_GGSN
!
...
!
redundancy inter-device
 scheme standby Gn
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.70.71.5
    keepalive 3000
    retransmit-timeout 300 10000
    path-retransmit 10
    assoc-retransmit 20
   remote-port 5000
    remote-ip 10.70.71.9
!
no aaa new-model
ip subnet-zero
!
!
no ip cef
no ip domain lookup
!
!
interface Loopback1
 description VT address of processor3:GGSN"
```

```
 ip address 10.20.30.12 255.255.255.255
!
interface Loopback2
 description "Loopback of GTP-SLB for dispatch mode"
 ip address 10.20.30.91 255.255.255.255
!
interface GigabitEthernet0/0
 no ip address
 standby use-bia
!
interface GigabitEthernet0/0.3
 description "VLAN for Gn interface of UMTS"
 encapsulation dot1Q 410
 ip address 10.20.21.52 255.255.255.0
 no ip mroute-cache
 no keepalive
 no cdp enable
 standby version 2
 standby 7 ip 10.20.21.82
 standby 7 priority 190
 standby 7 name Gn
!
interface GigabitEthernet0/0.31
 description "VLAN for Gi interface of UMTS"
 encapsulation dot1Q 420
 ip vrf forwarding internet
 ip address 10.30.21.52 255.255.255.0
 standby 7 follow Gn
 standby 7 ip 10.30.21.82
!
interface GigabitEthernet0/0.71
 description "VLAN for inter-dev_SCTP"
 encapsulation dot1Q 498
 ip address 10.70.71.5 255.255.255.0
!
interface Virtual-Template1
 ip unnumbered Loopback1
 no ip redirects
 encapsulation gtp
 gprs access-point-list gprs
!
ip local pool APN1 110.1.0.1 110.1.10.255
ip classless
no ip http server
!
gprs access-point-list gprs
  access-point 1
   access-point-name apn1
   ip-address-pool local APN1
!
gprs gtp path-echo-interval 0
!
gprs charging disable
gprs redundancy
!
!
...
!
!
end

Active_GGSN-3#
```

Secondary GGSN Configuration Example

```
Standby_GGSN# show running config
Building configuration...

Current configuration : 2823 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Stby_GGSN
!
service gprs ggsn
!
...
!
redundancy inter-device
 scheme standby Gn
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.70.71.9
    keepalive 3000
    retransmit-timeout 300 10000
    path-retransmit 10
    assoc-retransmit 20
   remote-port 5000
    remote-ip 10.70.71.5
!
no aaa new-model
ip subnet-zero
!
!
no ip cef
!!
interface Loopback1
 description VT address of processor3:GGSN"
 ip address 10.20.30.12 255.255.255.255
!
interface Loopback2
 description "Loopback of GTP-SLB for dispatch mode"
 ip address 10.20.30.91 255.255.255.255
!
interface GigabitEthernet0/0
 no ip address
 standby use-bia
!
interface GigabitEthernet0/0.3
 description "VLAN for Gn interface of UMTS"
 encapsulation dot1Q 410
 ip address 10.20.21.62 255.255.255.0
 no ip mroute-cache
 no keepalive
 no cdp enable
 standby version 2
 standby 7 ip 10.20.21.82
 standby 7 priority 160
 standby 7 name Gn
```

```
!
interface GigabitEthernet0/0.31
 description "VLAN for Gi interface of UMTS"
 encapsulation dot1Q 420
 ip vrf forwarding internet
 ip address 10.30.21.62 255.255.255.0
 standby 7 follow Gn
 standby 7 ip 10.30.21.82
!
interface GigabitEthernet0/0.71
 description "VLAN for inter-dev_SCTP"
 encapsulation dot1Q 498
 ip address 10.70.71.9 255.255.255.0
!
interface Virtual-Template1
 ip unnumbered Loopback1
 no ip redirects
 encapsulation gtp
 gprs access-point-list gprs
!
ip local pool APN1 110.1.0.1 110.1.10.255
ip classless
no ip http server
!
!
gprs access-point-list gprs
  access-point 1
   access-point-name apn1
   ip-address-pool local APN1
   !
  !
!
!
gprs charging disable
gprs redundancy
!
!
...
!
!
end

Stby_GGSN-3#
```

Geographical GTP-SR Examples

This section contains the following configuration examples from a geographical GTP-SR implementation:

- GGSN Interface Configuration Examples, page 6-26
- Secondary GGSN Interface Configuration Example, page 6-26
- Supervisor Routing Configuration Examples, page 6-27
- GGSN Routing Configuration Examples, page 6-27

GGSN Interface Configuration Examples

Primary GGSN Interface Configuration Example

```
!
interface Loopback1
 description GGSN Loopback i/f
 ip address 1.1.1.1 255.255.255.255
!
interface GigabitEthernet0/0.100
 description Gn VLAN
 encapsulation dot1Q 100
 ip address 10.0.0.1 255.255.255.0
 standby 1 ip none
 standby 1 name geo
 standby 1 unicast destination 20.0.0.2
!
interface GigabitEthernet0/0.200
 description Gi VLAN
 encapsulation dot1Q 200
 ip vrf forwarding Gi-VRF
 ip address 11.0.0.1 255.255.255.0
 standby 1 ip none
 standby 1 follow geo
!
interface Virtual-Template1
 ip unnumbered Loopback1
 encapsulation gtp
 gprs access-point-list APLIST
!
```

Secondary GGSN Interface Configuration Example

```
!
interface Loopback1
 description GGSN Loopback i/f
 ip address 2.2.2.2 255.255.255.255
!
interface GigabitEthernet0/0.300
 description Gn VLAN
 encapsulation dot1Q 300
 ip address 20.0.0.2 255.255.255.0
 standby 1 ip none
 standby 1 name geo
 standby 1 unicast destination 10.0.0.1
!
interface GigabitEthernet0/0.400
 description Gi VLAN
 encapsulation dot1Q 400
 ip vrf forwarding Gi-VRF
 ip address 21.0.0.2 255.255.255.0
 standby 1 ip none
 standby 1 follow geo
!
interface Virtual-Template1
 ip unnumbered Loopback1
 encapsulation gtp
gprs access-point-list APLIST
!
```

Supervisor Routing Configuration Examples

Primary Supervisor Configuration Example

```
ip vrf Gi-VRF
rd 200:1
!
interface Vlan200
description Gi-VRF
ip vrf forwarding Gi-VRF
ip address 11.0.0.10 255.255.255.0
end
!
router ospf 200 vrf Gi-VRF
log-adjacency-changes
network 11.0.0.0 0.0.0.255 area 1
```

Secondary Supervisor Routing Configuration Example

```
ip vrf Gi-VRF
rd 200:1
!
interface Vlan400
description Gi-VRF
ip vrf forwarding Gi-VRF
ip address 21.0.0.20 255.255.255.0
end
!
router ospf 400 vrf Gi-VRF
log-adjacency-changes
network 21.0.0.0 0.0.0.255 area 3
!
```

GGSN Routing Configuration Examples

Primary GGSN Routing Configuration Example

```
router ospf 10
router-id 30.30.30.30
no log-adjacency-changes
redistribute static subnets
passive-interface GigabitEthernet0/0.10 on-standby
network 10.0.0.0 0.0.0.255 area 0
network 1.1.1.1 0.0.0.0 area 0
!
router ospf 20 vrf Gi-VRF
no log-adjacency-changes
redistribute static route-map xxx
passive-interface GigabitEthernet0/0.20 on-standby
network 11.0.0.0 0.0.0.255 area 1
!
```

Secondary GGSN Routing Configuration Example

```
router ospf 30
router-id 40.40.40.40
no log-adjacency-changes
redistribute static subnets
passive-interface GigabitEthernet0/0.30 on-standby
network 20.0.0.0 0.0.0.255 area 2
network 2.2.2.2 0.0.0.0 area 2
!
router ospf 40 vrf Gi-VRF
```

```
no log-adjacency-changes
redistribute static route-map xxx
passive-interface GigabitEthernet0/0.40 on-standby
network 21.0.0.0 0.0.0.255 area 3
!
```

CHAPTER 7

Configuring Charging on the GGSN

This chapter describes how to configure the charging function on a gateway GPRS support node (GGSN).

If at minimum, one charging gateway is defined on the Cisco GGSN, by default, charging processing is enabled on the GGSN.

There are several ways to customize communication with a charging gateway. Many of the default values for the charging options should provide a satisfactory configuration until you become more familiar with your network and decide to customize the charging interface.

Note The global configuration charging commands described in this chapter apply to and affect all charging groups configured on a GGSN, unless specified otherwise in the command description.

For complete descriptions of the GGSN commands in this chapter, see *Cisco GGSN Command Reference* for the Cisco GGSN release you are using. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

This chapter includes the following sections:

- Configuring an Interface to the Charging Gateway, page 7-2 (Required)
- Configuring the Default Charging Gateway, page 7-4 (Required)
- Configuring a Charging Source Interface, page 7-5 (Optional)
- Configuring the GGSN Memory Protection Mode Threshold, page 7-6 (Optional)
- Configuring the Transport Protocol for the Charging Gateway, page 7-7 (Optional)
- Configuring the Charging Release, page 7-8 (Optional)
- Configuring Charging for Roamers, page 7-9 (Optional)
- Customizing the Charging Options, page 7-11 (Optional)
- Disabling Charging Processing, page 7-14 (Optional)
- Using Charging Profiles, page 7-15 (Optional)
- Configuring G-CDR Backup and Retrieval Using iSCSI, page 7-21 (Optional)
- Configuring Granular Charging and Storage, page 7-26 (Optional)
- Monitoring and Maintaining the Charging Function on the GGSN, page 7-30
- Configuration Examples, page 7-30

Configuring an Interface to the Charging Gateway

To establish access to an external charging gateway in the general packet radio service/Universal Mobile Telecommunication System (GPRS/UMTS) network, you must configure an interface on the GGSN to connect to the network of the charging gateway. In GPRS/UMTS, the interface between the GGSN and the charging gateway is referred to as the *Ga interface*. The Cisco GGSN supports both a 2.5G Ga interface and a 3G Ga interface.

On the Cisco 7600 series router platform, the Ga interface is a logical one to a Layer-3 routed Ga VLAN configured on the supervisor engine. IEEE 802.1Q-encapsulation must be configured on the logical interface.

For more information about the Ga VLAN on the supervisor engine, see the "Platform Prerequisites" section on page 3-2. For more information about configuring interfaces, see *Cisco IOS Interface Configuration Guide* and *Cisco IOS Interface Command Reference*.

To configure a subinterface to the Ga VLAN on the supervisor engine, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface gigabitethernet slot/port.subinterface-number`	Configures the subinterface.
Step 2	`Router(config-if)# encapsulation dot1q vlanid`	Defines the encapsulation format as IEEE 802.1Q (dot1q), and specifies the VLAN identifier.
Step 3	`Router(config-if)# ip address ip-address mask`	Sets a primary IP address for an interface.

Verifying Interface Configuration to the Charging Gateway

To verify the interface to the charging gateway, you can first verify your GGSN configuration and then verify that the interface is available.

Step 1 To verify that you have properly configured a Ga VLAN on the supervisor engine, use the **show running-config** command. The following example is a portion of the output from the command showing the GigabitEthernet 8/22 physical interface configuration as the Ga interface to a charging gateway and the Ga VLAN configuration:

```
Sup# show running-config
Building configuration...

Current configuration :12672 bytes
!
version 12.2
...
!
interface GigabitEthernet8/22
 no ip address
 switchport
 switchport access vlan 302
!
interface Vlan302
 description Vlan to GGSN for Ga
 ip address 40.40.40.100 255.255.255.0
```

To verify that the physical interface and the Ga VLAN are available, use the **show interface** command on the supervisor engine. The following example shows that the GigabitEthernet8/22 physical interface to the charging gateway is up, and the Ga VLAN, VLAN 101:

```
Sup# show ip interface brief GigabitEthernet8/22
Interface                  IP Address      OK? Method Status                Protocol
GigabitEthernet8/22        unassigned      YES unset  up                    up

Sup# show ip interface brief Vlan302
Interface                  IP-Address      OK? Method Status                Protocol
Vlan302                    40.40.40.100    YES TFTP   up                    up

Sup#
```

Step 2 To verify the Ga VLAN configuration and availability, use the **show vlan name** command on the supervisor engine. The following example shows the Gn VLAN Gn_1:

```
Sup# show vlan name Ga_1

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
302  Ga_1                             active    Gi4/1, Gi4/2, Gi4/3, Gi7/1
                                                Gi7/2, Gi7/3, Fa8/22, Fa8/26

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
302  enet  100302     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Step 3 On the GGSN, to verify that you have properly configured a Ga subinterface to the Ga VLAN on the supervisor, use the **show running-config** command. The following example is a portion of the output from the command which shows a GigabitEthernet0/0.2 subinterface configuration as the Ga interface to the charging gateway:

```
GGSN# show running-config
Building configuration...

Current configuration : 5499 bytes
!
! Last configuration change at 20:38:31 PST Tue Oct 13 2009
!
version 12.4
!
.....
!
interface GigabitEthernet0/0.2
 description Ga Interface
 encapsulation dot1Q 302
 ip address 40.40.40.41 255.255.0.0
 no cdp enable
!
.....
ip route 40.1.2.1 255.255.255.255 10.1.1.1
```

Step 4 To verify that the subinterface is available, use the **show ip interface brief** command. The following example shows that the Gigabit Ethernet 0/0.2 subinterface to the Ga VLAN is in *up* status and the protocol is also *up*:

```
GGSN# show ip interface brief GigabitEthernet0/0.2
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0.2       40.40.40.41     YES NVRAM  up                    up
```

Configuring the Default Charging Gateway

You can configure a charging gateway that the GGSN uses, by default, to communicate charging information. In addition, you can specify secondary and tertiary charging gateway as backup charging gateways. All charging gateways share the same global charging parameters.

Note With the introduction of the Granular Charging feature in Cisco GGSN Release 9.0 and later, this set of default charging gateways are identified as *charging group 0*, the default charging group.

To configure a default charging gateway for a GGSN, use the following command in global configuration mode:

Command	Purpose
Router(config)# **gprs default charging-gateway** {*ip-address* | *name*} [{*ip-address* | *name*}] [{*ip-address* | *name*}] [{*ip-address* | *name*}]	Specifies a primary charging gateway and optionally, the secondary and tertiary backup charging gateways, where: • *ip-address*—Specifies the IP address of a charging gateway. The second and third *ip-address* arguments specify the IP address of the backup charging gateways. • *name*—Specifies the hostname of a charging gateway. The second and third *name* arguments specify the hostname of the backup charging gateways.

Configuring the GGSN to Switchover to the Highest Priority Charging Gateway

When priority switchover is configured on the GGSN using the **gprs charging switchover priority** command, regardless of the state of the current active charging gateway, when a gateway of higher priority comes up, the GGSN switches to and sends gateway GPRS support node-call detail records (G-CDRs) to that charging gateway.

Note This command applies to only the globally defined charging gateways that are a part of the default charging group (charging group 0). To configure the switchover priority for charging groups 1 through 29, use the **switchover priority** command in charging group configuration mode.

To configure priority switchover on the GGSN for the default charging group, use the following command in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs charging switchover priority`	Configures the GGSN to switch to the gateway of higher priority when that gateway becomes active.

Changing the Default Charging Gateway

To change the default charging gateway of a GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs default charging-gateway 10.9.0.2`	Specifies a primary charging gateway at IP address 10.9.0.2.
Step 2	`Router(config)# no gprs default charging-gateway 10.9.0.2`	Removes the primary charging gateway at IP address 10.9.0.2.
Step 3	`Router(config)# gprs default charging-gateway 10.9.0.3`	Specifies the new default primary charging gateway at IP address 10.9.0.3.

Configuring a Charging Source Interface

By default, the global GTP virtual template interface is used for all charging messages. With Cisco GGSN Release 8.0 and later, you can configure a charging source interface for charging messages.

The *charging source interface* is a loopback interface that the GGSN is configured to use for charging traffic by using the **gprs charging interface source loopback** command. Once a loopback interface is configured as the charging source interface, all charging messages use the IP address of that loopback interface as their source address.

The charging source interface feature enables you to separate charging traffic. Optionally, a VPN Routing and Forwarding (VRF) instance can be configured on the loopback interface to separate charging traffic onto a private VLAN.

When configuring a charging source interface:

- Once configured, the loopback interface cannot not be modified without removing the charging source interface configuration. All charging messages will use the new end points from the path structure.
- A charging source interface cannot be unconfigured while there are active packet data protocol (PDP) contexts or call detail records (CDRs).

To configure a charging source interface, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface loopback` *number*	Creates a loopback interface. A loopback interface is a virtual interface that is always up.
Step 2	`Router(config-if)# ip address` *ip-address mask*	Assigns an IP address to the loopback interface.
Step 3	`Router(cfg-acct-mlist)# exit`	Exits from interface configuration mode.

To configure the GGSN to use the loopback interface for charging traffic, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs charging interface source loopback` *number*	Specifies the loopback interface for the GGSN to use for charging messages. **Note** The charging source interface must be a loopback interface, and the interface must be configured using a valid IP address. Optionally, a VRF instance can be configured on the interface to separate charging traffic onto a private VLAN.

Configuring the GGSN Memory Protection Mode Threshold

The GGSN memory protection feature prevents processor memory from being drained during periods of abnormal conditions, such as when all charging gateways are down and the GGSN is buffering call detail records (CDRs) into memory.

When the memory threshold is enabled, by default the memory threshold is 10 percent of the total memory available when GGSN services are enabled by the **gprs ggsn service** command.

You can use the **gprs memory threshold** command to configure the threshold according to the router memory and size, that when exceeded, activates the memory protection mode on the GGSN.

When the amount of memory remaining on the system reaches the defined threshold, the memory protection feature activates, and the GGSN performs the following actions to keep the processor memory from falling below the threshold:

- Rejects new Create PDP Context requests with a *No Resource* cause value.
- Drops any existing PDPs for which an Update PDP Context is received with a *Management Intervention* cause value.
- Drops any PDPs for which a volume trigger has occurred.

Note While the memory protection feature is active, byte counts are tracked and reported when the GGSN recovers. However, because some change conditions are not handled when the GGSN is in memory protection mode, some counts (for example, QoS and tariff conditions) do not reflect the accurate charging condition.

To configure the memory threshold that activates the memory protection feature on the GGSN when reached, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs memory threshold threshold`	Configures the threshold on the GGSN that when reached activates the memory protection feature. The valid range is from 0 to 1024 MB. The default is 10% of the total memory available when GGSN services are enabled.

Configuring the Transport Protocol for the Charging Gateway

You can configure a GGSN to support either Transport Control Protocol (TCP) or User Datagram Protocol (UDP) as the transport path protocol for communication with the charging gateway.

The GGSN default transport path protocol is *UDP*, a connectionless protocol that is considered an unreliable transport method but can yield greater performance.

Configuring TCP as the Charging Gateway Path Protocol

TCP is a connection-based protocol that provides reliable transmission through packet acknowledgment.

To specify TCP as the transport path protocol, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs charging cg-path-requests 1`	Specifies the number of minutes that the GGSN waits before trying to establish the TCP path to the charging gateway when TCP is the specified path protocol. The default is 0 minutes, which disables the timer.
Step 2	`Router(config)# gprs charging path-protocol tcp`	Specifies that the GGSN uses the TCP networking protocol to transmit and receive charging data.

Configuring UDP as the Charging Gateway Path Protocol

By default, the Cisco GGSN uses UDP as the transport path protocol to the charging gateway. If you need to reconfigure the charging gateway for UDP transport, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs charging path-protocol udp`	Specifies that the GGSN uses UDP networking protocol to transmit and receive charging data. The default value is UDP.

Configuring the Charging Release

The Cisco GGSN supports both 2.5G and 3G Ga interfaces, and GPRS (R97/R98) and UMTS (R99) Quality of Service (QoS) profile formats. The Cisco GGSN can be configured to comply with 3GPP TS 32.215 Release 4, Release 5, or Release 7.

When specifying the **99** or **98** keywords, the following actions take place:

- If the GGSN is configured to present R97/R98 CDRs (**gprs charging release 98** is configured):
  - If the PDP context is R98, the GGSN presents an R97/R98 G-CDR.
  - If the PDP context is R99, the GGSN converts the R99 QoS profile to an R97/R98 QoS profile, and presents an R97/R98 G-CDR.
- If the GGSN is configured to present R99 CDRs (**gprs charging release 99** is configured):
  - If the PDP context is R99, the GGSN presents an R99 G-CDR.
  - If the PDP context is R98, the GGSN converts the QoS profile and presents an R99 CDR.

Note With Cisco GGSN Release 9.2 and later, the generation of enhanced G-CDRs (eG-CDRs) requires that charging release 7 has been configured on the GGSN. For information about configuring the GGSN to generate eG-CDRs, see the "Configuring the GGSN to Generate Enhanced G-CDRs" section on page 8-4.

To configure the charging release with which the GGSN complies when presenting G-CDRs, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs charging release {99 | 98 | 4 | 5 | 7}`	Configures the format presented by the GGSN in CDRs. • **99**—R97, R98, and R99 QoS profile formats are presented. • **98**—R97/R98 QoS profile format is presented. • **4**—GGSN complies with 3GPP TS 32.215 Release 4. • **5**—GGSN complies with 3GPP TS 32.215 Release 5. • **7**—GGSN complies with 3GPP TS 32.215 Release 7. The default value is 99. **Note** When 99 is configured, the Charging Characteristics parameter is included in G-CDRs. When **4**, **5**, or **7** is configured, the Charging Characteristics Selection Mode information element (IE) is included.

To verify charging release configuration, use the **show gprs charging parameters** command.

Configuring Charging for Roamers

The Charging for Roamers feature enables you to configure the Cisco GGSN to generate G-CDRs for roaming mobile subscribers.

When the Cisco GGSN receives a Create PDP Context request, and the charging for roamers feature is enabled on the GGSN, the GGSN checks the Routing Area Identity (RAI) IE to see if the GGSN and the SGSN public land mobile network (PLMN) IDs are present and match. If both of the PLMN IDs are not present, or if they are present, but do not match, the GGSN matches the IE containing the SGSN Signaling Address field against a list of PLMN IP address ranges that have been defined using the **gprs plmn ip address** command with the **sgsn** keyword option specified.

If the GGSN determines that the SGSN that sent the Create PDP Context request is not located within the same PLMN as it is, the GGSN generates the G-CDR. If the GGSN determines that the SGSN is located in the same PLMN, it does not generate a CDR until it receives notification that the SGSN has changed location to another PLMN.

Before enabling the charging for roamer feature:

- To use the RAI IE in Create PDP Context requests to detect roamers, a valid home PLMN must be configured on the GGSN using the **gprs mcc mn** command in global configuration mode.

  When a valid home PLMN is configured, or a valid trusted PLMN, a G-CDR is not generated if the RAI matches the configured home or trusted PLMN. A G-CDR is created for all PDPs with RAIs that do not match the home or trusted PLMN.

- If the RAI field is not present in a Create PDP Context request, and an address range has not been configured using the **gprs plmn ip address** command with the **sgsn** keyword option specified, the PDP is classified as *unknown* and treated as a roamer.

- Before enabling the charging for roamers feature using the **gprs charging roamers** command, you must first define a set of IP address ranges for a PLMN using the **gprs plmn ip address** command.

  Ensure that you configure the **gprs plmn ip address** and **gprs charging roamers** commands in the proper order:

  a. Configure the IP address range for a PLMN by using the **gprs plmn ip address** command. You can change an IP address range by reissuing the **gprs plmn ip address** command.

  b. Enable the charging for roamers feature on the GGSN using the **gprs charging roamers** command.

To enable the charging for roamers feature on the GGSN, complete the following tasks:

- Configuring PLMN IP Address Ranges, page 7-10
- Enabling Charging for Roamers, page 7-10

To verify your configuration, use the **show gprs charging parameters** command. To verify your PLMN IP address ranges, use the **show gprs plmn ip address** command.

Configuring PLMN IP Address Ranges

Depending on how the PLMN IP address ranges are configured, the charging for roamers feature operates as follows:

- If no PLMN IP address ranges have been configured using the **gprs plmn ip address** *start_ip end_ip* [**sgsn**] command, the GGSN generates G-CDRs for all initiated PDP contexts regardless of whether the GGSN and SGSN are located within the same PLMN.
- If a list of PLMN IP address ranges is configured using the **gprs plmn ip address** *start_ip end_ip* [**sgsn**] command, and one or more of those ranges have been defined with the **sgsn** keyword specified, the GGSN uses the ranges defined with the **sgsn** keyword specified to determine whether an SGSN is located within the same PLMN.

  With this configuration, the following scenarios describe how the charging for roamers feature functions:

  - MS1 is subscribed to PLMN1 and attaches to an SGSN in PLMN2. From PLMN2, MS1 initiates a PDP context with the GGSN in PLMN1. In this scenario, MS1 is a roamer, and the GGSN generates a CDR because it determines that the SGSN is located in a different PLMN.
  - MS1 is subscribed to PLMN1 and attaches to an SGSN in PLMN2. From PLMN2, MS1 initiates a PDP context with the GGSN in PLMN2. In this scenario, MS1 is not a roamer, and the GGSN does not generate a G-CDR because it determines that it is in the same PLMN as the SGSN.

To configure PLMN IP address ranges, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs plmn ip address start_ip end_ip [sgsn]`	Specifies the IP address range of a PLMN. Optionally, specifies that only PLMN IP address ranges defined with the **sgsn** keyword specified be used to determine if an SGSN is located in a PLMN other than the GGSN.

Enabling Charging for Roamers

To enable the charging for roamers feature on the GGSN, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs charging roamers`	Enables charging for roamers on a GGSN.

Customizing the Charging Options

For the GGSN charging options, the default values represent recommended values. Other optional commands are also set to default values; however, we recommend modifying these commands to optimize your network as necessary, or according to your hardware.

The GGSN uses echo timing to maintain the path between SGSNs and external charging gateways. However, the GGSN can implement only a single method of echo timing for all the paths that it needs to maintain. To learn more about echo timing on the GGSN, or to modify the echo timing feature, see the "Configuring Echo Timing on a GGSN" section on page 4-4 in the "Configuring GTP Services on the GGSN" chapter.

Note The following charging options can be used by both G-CDRs or eG-CDRs, and the GGSN generates an eG-CDR or G-CDR depending upon its charging configuration. Therefore, when describing the GGSN charging options, the reference to G-CDRs can apply to either a G-CDR or eG-CDR.

Use the following commands in global configuration mode to fine-tune charging processing on the GGSN:

Command	Purpose
`Router(config)# gprs charging cdr-aggregation-limit` *CDR_limit*	Specifies the maximum number of CDRs that a GGSN aggregates in a charging data transfer message to a charging gateway. The default is 255 CDRs.
`Router(config)# gprs charging cdr-option apn [virtual]`	Specifies to include the access point name (APN) IE in G-CDRs. Optionally, specify the **virtual** keyword to include the virtual APN in G-CDRs, accounting records, and credit control requests (CCRs).
`Router(config)# gprs charging cdr-option apn-selection-mode`	Enables the GGSN to provide the reason code for access point name (APN) selection in G-CDRs.
`Router(config)# gprs charging cdr-option camel-charge-info`	Specifies to include a copy of the tag and length of the Customized Application for Mobile Enhanced Logic (CAMEL) from the SGSN's CDR in G-CDRs.
`Router(config)# gprs charging cdr-option chch-selection-mode`	Specifies to include the charging characteristics selection mode parameter in G-CDRs.
`Router(config)# gprs charging cdr-option dynamic-address`	Specifies to include the dynamic address flag IE in G-CDRs.
`Router(config)# gprs charging cdr-option imeisv`	Specifies to include the International Mobile Equipment Identity IMEI software version (IMEISV) IE in G-CDRs. The IMEISV identifies the mobile equipment used by the subscriber.
`Router(config)# gprs charging cdr-option local-record-sequence-number`	Enables the GGSN to use the local record sequence number IE in G-CDRs.
`Router(config)# gprs charging cdr-option ms-time-zone`	Specifies to include the MS Time Zone (MSTZ) IE in G-CDRs. The MSTZ IE indicates the offset between universal time and local time. A change of the MSTZ in an update request results in a CDR closure and the opening of a new CDR (as specified in R7 32.251). Additionally, an interim accounting record is generated when the MSTZ change occurs in an update request.

Command	Purpose
`Router(config)# gprs charging cdr-option nip`	Specifies to include the Network-Initiated PDP IE in G-CDRs.
`Router(config)# gprs charging cdr-option no-partial-cdr-generation [all]`	Disables the GGSN from creating fully qualified partial G-CDRs. Optionally, specify the **all** keyword option to configure the GGSN to copy the SGSN list for charging releases before Release 4 when an SGSN change limit trigger is configured as well. The default is fully qualified partial G-CDR creation is enabled. **Note** Enable this feature only when there are no active PDP contexts. Enabling this feature will affect all subsequent PDP contexts.
`Router(config)# gprs charging cdr-option node-id`	Enables the GGSN to specify the node that generated the CDR in the node ID field in G-CDRs.
`Router(config)# gprs charging cdr-option packet-count`	Enables the GGSN to provide uplink and downlink packet counts in the optional record extension field in G-CDRs.
`Router(config)# gprs charging cdr-option pdp-address`	Specifies to include the PDP address IE in G-CDRs.
`Router(config)# gprs charging cdr-option pdp-type`	Specifies to include the PDP type IE in G-CDRs.
`Router(config)# gprs charging cdr-option rat-type`	Specifies to include the radio access technology (RAT) IE in G-CDRs. The RAT indicates whether the SGSN serves the user equipment (UE) by Universal Terrestrial Radio Access Network (UTRAN) or GSM/EDGE RAN (GERAN). A change of the RAT in an Update PDP Context request results in a CDR closure and the opening of a new CDR (as specified in R7 32.251). Additionally, an interim accounting record is generated when the RAT change occurs in an update request.
`Router(config)# gprs charging cdr-option served-msisdn`	Enables the GGSN to provide the mobile station ISDN (MSISDN) number from the Create PDP Context request in G-CDRs.
`Router(config)# gprs charging cdr-option service-record` [*value*]	Enables the GGSN to generate per-service records. Optionally, the maximum number of services records in a CDR can be specified. When the limit is reached, the current G-CDR is closed and a new partial CDR is opened. If a maximum number is not specified, the default (5) is used.
`Router(config)# gprs charging cdr-option sgsn-plmn`	Configures the GGSN to include the SGSN PLMN ID in G-CDRs. **Note** When configured, the SGSN PLMN ID appears only if the optional RAI IE is received from the SGSN in the Create or Update PDP Context Request.
`Router(config)# gprs charging cdr-option user-loc-info`	Specifies to include the user location information (ULI) IE in G-CDRs. The ULI provides the cell global identity (CGI) and service area identity (SAI) of the subscriber location.
`Router(config)# gprs charging cg-path-requests` *minutes*	Specifies the number of minutes that the GGSN waits before trying to establish the path to the charging gateway when TCP is the specified path protocol. The default is 0 minutes, which disables the timer.

Command	Purpose
`Router(config)# gprs charging container change-limit number`	Specifies the maximum number of charging containers within each G-CDR from the GGSN. A valid value is a number between 1 and 100. The default is 5.
`Router(config)# gprs charging container sgsn-change-limit number`	Specifies the maximum number of SGSN changes that can occur before closing a G-CDR for a particular PDP context. A valid value is a number between 0 and 15. The default is 0, which disables the timer.
`Router(config)# gprs charging container time-trigger number`	Specifies a global time limit that causes the GGSN to close and update the G-CDR for a particular PDP context when exceeded by that PDP context. A valid value is a number, in minutes, between 5 and 429467295. The default is 0, which disables the timer.
`Router(config)# gprs charging container volume-threshold threshold_value`	Specifies the maximum number of bytes that the GGSN maintains in a user's charging container before closing it and updating the G-CDR. A valid value is a number between 1 and 4264967295. The default is 1,048,576 bytes (1 MB).
`Router(config)# gprs charging flow-control private-echo`	Implements an echo request with private extensions for maintaining flow control on packets transmitted to the charging gateway.
`Router(config)# gprs charging header short`	Enables the GGSN to use the GPRS tunneling protocol (GTP) short header (6-byte header) instead of the GTP long header.
`Router(config)# gprs charging map data tos tos_value`	Specifies an IP type of service (ToS) mapping for GPRS charging packets. The default is 3.
`Router(config)# gprs charging message transfer-request command-ie`	Specifies for the GGSN to include the Packet Transfer Command IE in Data Record Transfer Request messages
`Router(config)# gprs charging message transfer-request possibly-duplicate`	Specifies for the GGSN to retransmit Data Record Transfer Request messages (sent to a previously active charging gateway) with the value of the Packet Transfer Request IE set to 2 (Send Possibly Duplicate Data Record Packet).
`Router(config)# gprs charging message transfer-response number-responded`	Specifies for the GGSN to use the Number of Requests Responded field instead of the Length field in the Requests Responded IE of Data Record Transfer Response messages.
`Router(config)# gprs charging packet-queue-size queue_size`	Specifies the maximum number of unacknowledged charging data transfer requests that the GGSN maintains in its queue. The default is 128 packets.
`Router(config)# gprs charging path-protocol {udp | tcp}`	Specifies the protocol that the GGSN uses to transmit and receive charging data. The default is UDP.
`Router(config)# gprs charging port port-num`	Configures the destination port of the charging gateway. The default is 3386.
`Router(config)# gprs charging send-buffer bytes`	Configures the size of the buffer that contains the GTP PDU and signaling messages on the GGSN. The default is 1460 bytes.
`Router(config)# gprs charging server-switch-timer seconds`	Specifies a timeout value that determines when the GGSN attempts to find an alternate charging gateway after a destination charging gateway cannot be located or becomes unusable. The default is 60 seconds.

Command	Purpose
`Router(config)# gprs charging tariff-time time`	Specifies a time of day when GPRS/UMTS charging tariffs change. There is no default tariff time. **Note** If the system software clock is manually set using the **clock set** privileged EXEC command at the supervisor console prompt, the time a tariff change will occur must be reconfigured.
`Router(config)# gprs charging message transfer-request command-ie`	Specifies for the GGSN to include the Packet Transfer Command information element (IE) in Data Record Transfer Response messages. **Note** Even though the Cisco GGSN supports the Packet Transfer Command IE, only the "Send Data Record Packet" value is used, even though the packet might be duplicated. The Cisco GGSN does not support the "Send Possibly Duplicated Data Record Packet," "Cancel Data Record Packet," or "Release Data Record Packet" values. Therefore, the charging gateway or billing servers must have the ability to eliminate duplicate CDRs.
`Router(config)# gprs charging message transfer-response number-responded`	Configures the GGSN to use the Number of Requests Responded field instead of the Length field in the Requests Responded IE of Data Record Transfer Response messages.
`Router(config)# gprs charging reconnect minutes`	Configures the GGSN to periodically attempt to reconnect to a charging gateway that is unreachable to determine when the link is back up. **Note** Configuring the GGSN to automatically attempt to reconnect to a unreachable charging gateway is necessary only when UDP is used as the charging transport protocol and the charging gateway does not support echo requests.
`Router(config)# gprs charging transfer interval seconds`	Specifies the number of seconds that the GGSN waits before it transfers charging data to the charging gateway. The default is 105 seconds.

For information about configuring GGSN GTP options, see the "Customizing the GGSN Configuration" section on page 4-14 in the "Configuring GTP Services on the GGSN" chapter.

Disabling Charging Processing

Caution The **gprs charging disable** command removes charging data processing on a GGSN, which means that the data required to bill customers for network usage is not being collected by the GGSN or being sent to the charging gateway. We recommend that you avoid using this command in production GPRS/UMTS network environments. When it is necessary to use this command, use it with extreme care and reserve its usage only under nonproduction network conditions.

You can disable charging on the GGSN only after all the open CDRs have been processed and sent to the charging gateway. To clear the current GGSN CDRs, use the **clear gprs charging cdr** command in privileged EXEC mode.

To disable charging processing on a GGSN, use the following command, beginning in global configuration mode:

Command	Purpose
`Router(config)# gprs charging disable`	Disables charging transactions on the GGSN.

Using Charging Profiles

Using charging profiles that you create, customize, and specify as the default charging method for a specific type of user at a global and/or APN level, you can apply different charging methods on a per-PDP basis. Charging profiles provide the ability to offer flexible services that are customized to subscriber preferences.

When using charging profiles, note that you must configure the GGSN to:

- Include the charging characteristics selection mode parameter in CDRs by configuring the **gprs charging cdr-option chch-selection-mode** command.
- Receive the charging characteristics selection mode IE in CDRs by configuring the **gprs charging release** command

To apply different charging methods on a per-PDP basis using GGSN charging profiles, you must complete the tasks outline in the following sections:

- Configuring a Charging Profile, page 7-15
- Defining the Charging Characteristics and Triggers of a Charging Profile, page 7-17
- Applying a Default Charging Profile to an APN, page 7-20
- Applying Default Charging Profiles Globally, page 7-20
- Configuring How the GGSN Handles PDPs with Unmatched Charging Profiles, page 7-21

Configuring a Charging Profile

Charging profiles define a charging method to apply to a specific type of subscriber (home, roamer, visitor).

You can apply a charging profile at an APN level or global level as the default charging method for a specified subscriber type.

The GGSN supports up to 256 charging profiles, numbered 0 to 255. Profile 0 is a set profile that always exists on the GGSN. It is the global default charging profile. You do not create profile 0, however, you can modify it using the charging-related global configuration commands. Profiles 1 to 255 are user-defined and customized using the Cisco GGSN charging profile configuration commands.

When a Create PDP Context request is received by the GGSN, the GGSN selects the appropriate charging profile based on the following sources of input:

- Serving GPRS support node (SGSN)/home location registere (HLR) via the Charging Characteristics Selection Mode.
- Local defaults.
- Charging profile index Authentication, Authorization and Accounting (AAA) attribute.

Note The charging profile index received from AAA takes effect only if service-aware billing is enabled globally on the GGSN, using the **gprs service-aware** command in global configuration mode, and at the APN level, using the **service-aware** command in access-point configuration mode.

For information on configuring a service-aware GGSN, see Chapter 8, "Implementing Enhanced Service-Aware Billing."

The order in which the GGSN selects a charging profile for a PDP context, is as follows:

1. Charging profile index in the override rule on the APN—If a default charging profile is configured at both the APN and the global level to override the SGSN specification, the APN default charging profile is used first.
2. Charging profile index in the override rule on the box—If there is no default charging profile default configured at the APN, the default charging profile configured globally is use.
3. Charging profile index from AAA.
4. Charging profile index from SGSN/HLR.
5. Charging profile index from the non-override rule on the APN.
6. Charging profile index from non-override rule on the box.

If none of the above applies, the PDP context is rejected if the **gprs charging characteristics reject** command in global configuration mode is configured and the Create PDP Context request is GTP v1. If the **gprs charging characteristics reject** command is not configured, the GTPv1 PDP context is created using charging profile 0.

Note The global default charging profile, charging profile 0, is not supported for service-aware PDPs. Create PDP Context requests for service-aware PDPs are rejected with error code 199.

Note Charging profiles cannot be removed, and the DCCA profile under the charging profile cannot be modified (using the **content dcca profile** charging profile command) if the profile is being used by PDP contexts or rules. If the profile is being used by rules, it must be disassociated with the APN before making such configuration changes.

To create or modify a charging profile, and enter charging profile configuration mode, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs charging profile` *profile-num*	Creates a new charging profile or modifies an existing one, and enters charging profile configuration mode. The valid values are 1 to 255.

Defining the Charging Characteristics and Triggers of a Charging Profile

Note With Cisco GGSN Release 9.2 and later, when an enhanced quota server interface is configured, the Cisco GGSN does not function as a quota server for service-aware postpaid users. Therefore, with Cisco IOS Release 12.2(22)YE2 and later, the **content** command in charging profile configuration mode are ignored as well as the charging profile configuration commands that configure trigger conditions for postpaid users not using an enhanced quota server interface.

For more information about configuring enhanced service-aware billing, see *Cisco GGSN Configuration Guide*.

To configure the charging characteristics and triggers of a charging profile, use the following commands in charging profile configuration mode:

Command	Purpose
`Router(ch-prof-conf)# category {hot | flat | prepaid | normal}`	Identifies the category of subscriber to which a charging profile applies.
`Router(ch-prof-conf)# cdr suppression`	Specifies that CDRs be suppressed.
`Router(ch-prof-conf)# cdr suppression prepaid`	Specifies that CDRs be suppressed for prepaid subscribers.
`Router(ch-prof-conf)# content dcca profile profile-name`	Specifies the Diameter Credit Control Application (DCCA) profile to communicate with a DCCA server. **Note** Presence of this configuration in a charging profile indicates that online charging should be applied. A DCCA profile defines the DCCA server group. If the DCCA profile is defined in a charging profile, any PDP using the charging profile has to contact the DCCA server first to determine if online charging should be used. If a charging profile does not contain a **content dcca profile** configuration, users using the charging profile will be treated as postpaid (offline billing). **Note** This command cannot be modified if the profile is being used by PDP contexts or rules. If the profile is being used by rules, it must be disassociated with the APN before making such configuration changes.

Command	Purpose
`Router(ch-prof-conf)# content postpaid {plmn-change | qos-change | rat-change | sgsn-change | user-loc-info-change}`	Configures a condition in a charging profile for postpaid subscribers that, when the condition occurs, triggers the GGSN to request quota reauthorization for a PDP context. • **plmn-change**—Public land mobile network (PLMN) change triggers a quota reauthorization request. • **qos-change**—Quality of Service (QoS) change triggers a quota reauthorization request. • **rat-change**—Radio access technology (RAT) change triggers a quota reauthorization request. • **sgsn-change**—SGSN change triggers a quota reauthorization request. • **user-loc-info-change**—User location information change triggers a quota reauthorization. **Note** The **plmn-change**, **rat-change**, and **user-loc-info-change** keyword options require that the GGSN is configured to include these fields in the service-record IE in CDRs using the **gprs charging service record include** command in global configuration mode.
`Router(ch-prof-conf)# content postpaid time` *number*	Configures for postpaid subscribers when service-aware billing is enabled, the time duration limit that when exceeded, causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
`Router(ch-prof-conf)# content postpaid validity` *seconds*	Configures for postpaid subscribers when service-aware billing is enabled, the amount of time quota granted to a user is valid.
`Router(ch-prof-conf)# content postpaid volume` *threshold*	Configures for postpaid subscribers when service aware billing is enabled, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
`Router(ch-prof-conf)# content rulebase` *id*	Defines a default rulebase ID to apply to PDP contexts.
`Router(ch-prof-conf)# description`	Specifies the name or a brief description of a charging profile.
`Router(ch-prof-conf)# limit duration` *number* `[reset]`	Configures the time duration limit (in minutes) that causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context when exceeded. If the **reset** keyword option is configured, the time trigger is restarted if the CDR is closed by any other trigger. If the **reset** keyword is not specified (which is the default), the time trigger is not restarted when the volume trigger expires (**limit volume** command), but is restarted when any other trigger expires.

Command	Purpose
`Router(ch-prof-conf)# limit volume` *number* [**reset**]	Configures the maximum number of bytes that can be reported in each CDR from an active PDP context before the GGSN closes and updates the CDR, and opens a partial CDR for the PDP context while it remains in session on the GGSN. If the **reset** keyword option is configured, the volume trigger is started if the CDR is closed by any other trigger. If the **reset** keyword is not specified, the volume trigger is not restarted when the time trigger expires (**limit duration** command), but is restarted when any other trigger expires.
`Router(ch-prof-conf)# limit sgsn-change`	Specifies that a charging profile use the global tariff changes configured using the **gprs charging tariff-time** command.
`Router(ch-prof-conf)# tariff-time`	Specifies that a charging profile use the global tariff change time configured using the **gprs charging tariff-time** command.

Applying a Default Charging Profile to an APN

To configure a default charging profile for a specific type of user at an APN, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# charging profile {home | roaming | visiting | any} [trusted] profile_num [override]`	Configures a default charging profile for a specific type of user to use at an APN, if no charging characteristics are received from the SGSN, where: • **home**—Specifies that the charging profile applies to home users. • **roaming**—Specifies that the charging profile applies to roaming users (users whose serving GPRS support node [SGSN] public land mobile network [PLMN] ID differs from the gateway GPRS support node's [GGSN's]). • **visiting**—Specifies that the charging profile applies to visiting users (users whose International Mobile Subscriber Identity [IMSI] contains a foreign PLMN ID). • **any**—Specifies that the charging profile will apply to all types of users. • **trusted**—(Optional) Specifies that the charging profile applies if the user is a visiting or roaming user (depending on whether **roaming** or **visiting** is specified) whose PLMN ID is a trusted one (as configured by the **gprs mcc mnc** command). • *profile-number*—Number of the charging profile that is being associated with the access point. Valid values are 0 to 15. If 0 is specified, charging behavior is defined by global charging characteristics (those not defined in a charging profile). • **overide**—(Optional) Specifies that the charging characteristic value received from the SGSN in the Create PDP Context request be ignored and the APN default used instead.

Applying Default Charging Profiles Globally

Default charging profiles applied at the global level are used when a default charging profile has not been specified for an APN.

To configure a default charging profile for a specific type of user globally, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs charging profile default {home | roaming | visiting | any} [trusted] chp_num [override]`	Applies a default charging profile globally for a specific type of user.

Configuring How the GGSN Handles PDPs with Unmatched Charging Profiles

You can configure the GGSN to reject or accept GTPv1 Create PDP Context requests for which a profile cannot be matched. If the GGSN is configured to accept these PDP context requests, the charging method defined by charging profile 0 is applied. By default, the GGSN accepts Create PDP Context requests and applies the charging method defined in charging profile 0.

The following restrictions apply to charging profiles selected for service-aware PDPs:

- All PDP s belonging to the same user must use the same charging profile as that of the primary PDP.
- The global default charging profile, charging profile 0, is not supported for service-aware PDPs. Create PDP Context requests for service-aware PDPs are rejected with error code 199.

To configure a GGSN to reject Create PDP Context requests for which a charging profile cannot be matched, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs charging characteristics reject`	Configures the GGSN to reject GTPv1 Create PDP Context requests for which a charging profile cannot be selected.

Configuring G-CDR Backup and Retrieval Using iSCSI

Cisco GGSN Release 8.0 and later utilizes the Cisco IOS software Small Computer Systems Interface over IP (iSCSI) support, as defined in RFC 3720, to enable CDR storage and retrieval from storage target on a Storage Area Network (SAN).

This section contains the following topics on iSCSI support on the GGSN:

- iSCSI Overview, page 7-22
- Configuring iSCSI Backup and Storage on the GGSN, page 7-22
- Monitoring and Maintaining iSCSI CDR Backup and Storage, page 7-25

iSCSI Overview

The iSCSI transport protocol operates over TCP/IP, enabling mobile operators and service providers to use their SAN connected to an iSCSI interface to save complete data transfer record (DTR) messages containing closed CDRs.

SAN technology, which enables customers to build scalable storage solutions, is comprised of the following primary elements:

- **SCSI**—An interface standard which enables multiple devices to be installed on a system, attached to cable to form a chain of devices. Each device is assigned a unique ID, which is expressed as a number, that identifies that device on the bus. SCSI IDs can be broken into Logical Unit Numbers (LUNs), enabling a number of devices to share a single SCSI ID. Devices from which I/O requests originate are called initiators, and devices from which responses originate are called targets.
- **SAN**—Technology that involves moving network storage to a separate network of its own. Disk, tape, and optical storage can then be attached to the storage network that is based on a fabric of switches and hubs that connects storage devices to a heterogeneous set of servers.

  A SAN system provides block-level access to data residing on shared storage arrays through dedicated storage networks.
- **iSCSI**—Transport protocol that maps SCSI requests and responses over TCP and provides block-level data transfer between the SCSI initiator (the Cisco GGSN is this example), and the target (the storage device on the SAN). The initiator sends I/O requests and the target sends I/O responses.

A SAN topology is distinguished by the following features:

- Storage is not directly connected to network clients.
- Storage is not directly connected to servers.
- Storage devices are interconnected.
- Multiple servers can share multiple storage devices.

Configuring iSCSI Backup and Storage on the GGSN

In a SCSI environment, the GGSN functions as an iSCSI initiator.

To enable G-CDR backup storage on an iSCSI device, complete the following:

1. On the GGSN, configure an iSCSI target profile that includes the name and IP address of the target, and the TCP port on which to *listen* for iSCSI traffic.
2. Configure the GGSN to use the interface for record storage when a charging gateway is not available.

With Cisco GGSN Release 9.0 and later, you can configure and associate up to 30 iSCSI target profiles with a set of unique charging gateways within a charging group.

As an alternative, you can configure an iSCSI target profile as the primary storage for CDRs by configuring only an iSCSI target profile and no charging gateway at the global level (default charging group 0), or at the APN level by defining only an iSCSI target in the charging group associated with an APN (charging groups 1 to 29).

The I/O requests sent by the GGSN are converted into SCSI requests and transported over TCP/IP to the remote storage target.

Choosing the Record Format when Writing to iSCSI

By default, when writing DTRs to iSCSI, the format for storing records is *GTP*, wherein the complete DTR is written to the iSCSI target. As an alternative, you can configure the iSCSI record format as ASN.1 by using the **gprs charging iscsi rec-format** command in global configuration mode and specifying the **asn.1** keyword option. When you configure ASN.1 as the record format, the GGSN writes only the raw ASN1-encoded CDRs into iSCSI without embedding the DTR information element into the records. The ASN.1 format is useful when the records are retrieved from iSCSI using FTP.

To configure the record format, use the **gprs charging iscsi rec-format** command in global configuration mode.

Note The records in ASN.1 format are generated when **gprs auto-retrieve** is disabled on the GGSN, which is the default behavior. Use the ASN.1 format only when the iSCSI target is used as the primary storage for charging records (no charging gateways are configured).

Writing DTRs when iSCSI is used as Backup Storage

- Once iSCSI backup storage configuration is in place, when a charging gateway is not reachable, the writing toward the iSCSI is initiated. The complete DTR message is sent to the iSCSI target defined in the target profile.
- The recommended iSCSI record format when using iSCSI as backup is GTP (the default format). If the iSCSI auto-retrieval (the **gprs auto-retrieve** command in global configuration mode) is enabled, the record format must be configured as GTP.
- When iSCSI auto-retrieval is enabled, along with sending the complete DTR message, the GGSN adds a 12-byte header in front of the message before storing it to SAN. This header is used when the DTRs are retrieved and sent to the charging gateway. (In addition, the RSM-layer adds a 12-byte header and 4-byte trailer to the message before it is stored).

Note If the DTRs are retrieved directly from the SAN through other means such as FTP, then each record must skip the 10-byte header to get to the actual DTR containing encoded CDRs.

Writing DTRs when iSCSI is used as Primary Storage

- When there are no charging gateways configured, and only an iSCSI target profile is defined at the global charging level (charging group 0), or granular charging level (charging groups 1 to 29), the iSCSI is the primary storage for writing charging records.
- Although you can use any iSCSI record format, the ASN.1 iSCSI record format enables the storage of store raw ASN.1 encoded CDRs into iSCSI without any additional headers.

Reading CDRs

- Once the iSCSI backup storage configuration is in place, when a charging gateway comes up, the iSCSI initiator (GGSN) requests for any iSCSI records to be received from the iSCSI target.
- Once the GGSN receives a record, the 12-byte header added by the GGSN when the write process is removed and the complete DTR are sent to the charging gateway.

  If the DTRs are to be marked for possible duplication before sending to the charging gateway, you must configure the GGSN with the following charging configuration commands.

  - **gprs charging message transfer-request command-ie**
  - **gprs charging message transfer-request possibly-duplicate**

iSCSI Restrictions

When configuring iSCSI CDR backup and storage on the GGSN Release 10.0 or later:

- Number of TCP connections per iSCSI session is limited to one.
- iSCSI targets cannot be dynamically discovered.
- iSCSI target device should be preformatted with five virtual disks; one disk for each Cisco GGSN TCOP (PPC4 through PPC8).
- Each LUN must have only five FAT32 partition. Maximum of size of a LUN must not be more than 2TB, which is the maximum disk size supported by a FAT32 file system.

When configuring iSCSI CDR Backup and Storage on the GGSN, complete the tasks in the following sections:

- Configuring an iSCSI Target Profile, page 7-24
- Associating an iSCSI Target Profile, page 7-25
- Verifying the iSCSI Session, page 7-25

Configuring an iSCSI Target Profile

Note You can configure up to 30 iSCSI profiles on the GGSN, however, you can define only one target per profile, and associate only one profile with the GGSN to use the iSCSI interface at a time by using the **gprs iscsi** command in global configuration mode.

To configure the iSCSI target profile on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ip iscsi target-profile target_profile_name`	Creates an iSCSI target profile for the target and enters iSCSI interface configuration mode on the GGSN.
Step 2	`Router(config-iscsi)# name target name`	(Required) Name of the iSCSI target.
Step 3	`Router(config-iscsi)# ip ip_address`	(Required) IP address of the iSCSI target.
Step 4	`Router(config-iscsi-target)# record-store file-size size`	(Optional) Size, in bytes, that when reached closes a file and data is written to a new file.
Step 5	`Router(config-iscsi-target)# record-store file-closure-interval minutes`	(Optional) The interval, in minutes, at which files are closed and data is written to a new file.
Step 6	`Router(config-iscsi)# source-interface loopback_interface_number`	(Optional) Number of the loopback interface if iSCSI traffic is to use a different source interface.
Step 7	`Router(config-iscsi)# vrf vrf_name`	(Optional) Name of the VPN Routing and Forwarding (VRF) instance if iSCSI traffic needs a virtual private network (VPN).
Step 8	`Router(config-iscsi)# exit`	Exits from iSCSI interface configuration mode.

Note The **name**, **ip**, and **port** iSCSI interface subconfigurations are required. For a complete list of optional configurations that you can configure under a target profile, issue the "**?**" command in iSCSI interface configuration mode or see the **ip iscsi target-profile** command description in the *Cisco GGSN Command Reference*.

Associating an iSCSI Target Profile

To configure the GGSN to use a iSCSI interface for CDR storage when no charging gateway is available, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs iscsi target_profile_name`	Configures the GGSN to use a iSCSI profile for record storage. **Note** Only one profile can be defined at a time. **Note** The profile name specified must be the same as the one configured using the **ip iscsi target-profile** command.

Verifying the iSCSI Session

To verify that the iSCSI session is up, use the following command in privileged EXEC mode:

Command	Purpose
`Router# show ip iscsi session`	Displays the status of iSCSI session.

Monitoring and Maintaining iSCSI CDR Backup and Storage

You can use the following is a list of commands to monitor and maintain the iSCSI backup and storage functions on the GGSN:

Command	Purpose
`Router# clear gprs iscsi statistics`	Clears GGSN iSCSI processing statistics.
`Router# clear ip iscsi statistics`	Clears iSCSI processing statistics.
`Router# clear record-storage-module`	Clears record storage module statistics.
`Router# show ip iscsi name`	Displays the name of the iSCSI initiator.
`Router# show ip iscsi session`	Displays the status of an iSCSI session.
`Router# show ip iscsi stats`	Displays the iSCSI and SCSI layer statistics.
`Router# show ip iscsi target`	Displays the details of the iSCSI target.
`Router# show record-storage-module stats`	Displays record storage module statistics.
`Router# show record-storage-module target-info [all | target-profile profile_name]`	Displays all disks available and their status, or the disk defined by a target profile.

Configuring Granular Charging and Storage

The Cisco GGSN supports an access-point level charging configuration (granular charging) in addition to the default global charging configuration.

With granular charging, you can configure up to 30 *charging groups* per GGSN. In each charging group you can define a unique primary, secondary, and tertiary charging gateway, and iSCSI target, and assign the charging group to an APN. Charging groups enable you to send charging records belonging to different APNs to different destinations.

If you do not assign a charging group with an APN, the default charging group (the primary, secondary, and tertiary charging gateways, iSCSI target, switchover priority, etc., configured at the global level) is used.

Charging group 0 is the default charging group defined at the global level. You can configure and associate charging groups 1 to 29.

Usage Notes

When configuring granular charging and storage:

- You can configure up to 30 charging groups per GGSN and assign them to APNs. The 0 value is reserved for the default global charging group that contains the global charging gateway and global iSCSI target, if configured. You can use values 1 to 29 to define other charging groups.
- By default, all APNs use the default global charging group 0 unless a charging group (charging group 1 to 29) is assigned to the APN.
- You can assign the same charging group to multiple APNs, but you can assign only one charging group per APN.
- You can assign a charging gateway to only a single charging group. A charging gateway cannot be shared across groups regardless of whether it is defined as the primary, secondary, or tertiary gateway.
- You can assign an iSCSI target to only a single charging group. An iSCSI cannot be shared across groups.
- The charging gateway switchover inside one charging group retains the same precedence as the global configuration (charging group 0)—primary charging gateway, to secondary charging gateway, to tertiary charging gateway, to iSCSI target.
- Once you have assigned a charging group to an APN, the APN only switches over inside the charging group. The APN will not fall back to the globally configured charging gateways or iSCSI target.
- If you assign an empty charging group (a group to which you have not defined a charging gateway or an iSCSI target) to an APN, CDRs for that APN are not generated unless you place the charging group in maintenance mode by using the **service-mode maintenance** command in charging group configuration mode.
- If you define only an iSCSI target in a charging group, there is no fallback to the globally configured iSCSI target.
- If you assign a charging group in which an iSCSI target has not been defined to an APN, that APN cannot fallback to the globally configured iSCSI profile. Therefore, to enable iSCSI backup and storage for an APN, ensure that the iSCSI target has been defined in the charging group assigned to the APN.
- To use an iSCSI target as the primary storage device for charging records for an APN, and not just as a backup device, define only an iSCSI target in the charging group associated with the APN.

- Auto-retrieval (the **gprs auto-retrieve** command in global configuration mode) is supported only at the global level (default charging group 0). Auto-retrieval is not supported at the APN charging group level (groups 1 to 29).
- The set iSCSI record format applies to all charging groups.
- You can individually place each charging group in maintenance mode or operational mode. Before modifying a charging group (adding or deleting charging gateways or the iSCSI target), place the group in maintenance mode by using the **service-mode** command in charging group configuration mode.
- When a charging group is in maintenance mode, pending DTRs from the group are moved to the group's charging maintenance queue. When the charging group is returned to operational mode, pending messages present in the group maintenance queue, or open CDRs present for the APNs using the charging group, are moved to the charging path or iSCSI queue based on the following sequence:
  - If charging gateways are defined in the charging group, pending messages and open CDRs are moved to the path of the charging gateway with the highest priority.
  - If no charging gateways are defined, but an iSCSI target is, pending messages and open CDRs are moved to the iSCSI write queue.
  - If neither a charging gateway or an iSCSI target are defined in the charging group, the group cannot be moved to operational mode if there are any pending messages or open CDRs for the group.

Note CDRs are not generated for a charging group when the group is empty and in operational mode

To configure granular charging, complete the tasks in the following sections:

- Configuring a Charging Group, page 7-28
- Associating a Charging Group with an Access Point, page 7-29
- Modifying a Charging Group, page 7-29
- Monitoring and Maintaining Granular Charging, page 7-29

To configure granular charging and storage, complete the tasks in the following sections:

- Configuring a Charging Group, page 7-28
- Associating a Charging Group with an Access Point, page 7-29
- Modifying a Charging Group, page 7-29

Configuring a Charging Group

To configure a charging group, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs charging group group-number`	Defines or modifies a charging group, where *group-number* is a value between 1 and 29. **Note** The value of 0 is reserved for the default charging group that contains the global charging gateway and global iSCSI target, if defined. You can use values 1 to 29 to define other charging groups.
Step 2	`Router(config-chrg-group)# description description`	Charging gateway group definition.
Step 3	`Router(config-chrg-group)# primary {ip-address | name}`	Specifies the primary charging gateway for the group, where: • *ip-address*—Specifies the IP address of the primary charging gateway. • *name*—Specifies the hostname of the primary charging gateway.
Step 4	`Router(config-chrg-group)# secondary {ip-address | name}`	Specifies the secondary charging gateway for the group, where: • *ip-address*—Specifies the IP address of the secondary charging gateway. • *name*—Specifies the hostname of the secondary charging gateway.
Step 5	`Router(config-chrg-group)# tertiary {ip-address | name}`	Specifies the tertiary charging gateway for the group, where: • *ip-address*—Specifies the IP address of the tertiary charging gateway. • *name*—Specifies the hostname of the tertiary charging gateway.
Step 6	`Router(config-chrg-group)# switchover priority`	Configures the GGSN to switch to the gateway of higher priority in the charging group when that gateway becomes active.
Step 7	`Router(config-chrg-group)# iscsi iscsi-profile-name`	Specifies an iSCSI target for CDR backup when all charging gateways are down.
Step 8	`Router(config-chrg-group)# service-mode [maintenance | operational]`	Places the charging group into maintenance mode or operational mode. The default is operational.
Step 9	`Router(config-chrg-group)# exit`	Exits charging group configuration mode.

Associating a Charging Group with an Access Point

Once you have configured the charging group, assign it to an APN.

To assign a charging group to an APN, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# charging group chrg-group-number`	Assigns an existing charging group to an APN, where *group-number* is a number 1 through 29.

Modifying a Charging Group

Before modifying a charging group, place the charging group in maintenance mode.

To place a charging group in maintenance mode, use the following command in charging group configuration mode:

Command	Purpose
`Router(config-chrg-group)# service-mode maintenance`	Places the charging group in maintenance mode.

To return the charging group to operational mode after modifying it, use the following command in charging group configuration mode:

Command	Purpose
`Router(config-chrg-group)# service-mode operational`	Places the charging group in operational mode.

Monitoring and Maintaining Granular Charging

The following is a list of commands that you can use to monitor and maintain granular charging on the GGSN:

Command	Purpose
`Router# clear gprs charging cdr charging-group`	Clears CDRs.
`Router# clear gprs iscsi statistics`	Clears the current GPRS-related iSCSI statistics.
`Router# show gprs access-point`	Displays information about access points on the GGSN.
`Router# show gprs charging parameters charging-group`	Displays cumulative charging statistics for the GGSN.
`Router# show gprs charging statistics`	Displays current charging statistics for the GGSN.
`Router# show gprs charging status`	Displays current charging statistics for the GGSN.
`Router# show gprs charging summary`	Displays a summary of all charging groups defined on the GGSN.

Note Many of the **clear** and **show** commands above have been enhanced with a **charging-group** keyword option for clearing and showing information specific to a charging group.

Monitoring and Maintaining the Charging Function on the GGSN

This section provides a summary list of the **show** commands that you can use to monitor charging functions on the GGSN.

The following privileged EXEC commands are used to monitor and maintain charging on the GGSN:

Command	Purpose
`Router# show gprs charging parameters`	Displays information about the current GGSN charging configuration.
`Router# show gprs service-mode`	Displays the current global service mode state of the GGSN and the last time it was changed.
`Router# show gprs charging statistics`	Displays cumulative statistics about the transfer of charging packets between the GGSN and charging gateways.

Configuration Examples

The following are examples of charging configurations implemented on the GGSN.

Global Charging Configuration

GGSN Configuration

```
Router# show running-config
Building configuration...

Current configuration :7390 bytes
!
! Last configuration change at 16:56:05 UTC Wed Jun 25 2003
! NVRAM config last updated at 23:40:27 UTC Fri Jun 13 2003
!
version 12.3
.....
interface GigabitEthernet0/0.2
 description Ga/Gn Interface
 encapsulation dot1Q 101
 ip address 10.1.1.72 255.255.255.0
 no cdp enable
!
.....
ip route 40.1.2.1 255.255.255.255 10.1.1.1
!
gprs access-point-list gprs
  access-point 1
   access-point-name auth-accounting
   access-mode non-transparent
   aaa-group authentication first
   aaa-group accounting second
   ip-address-pool dhcp-proxy-client
   dhcp-server 10.60.0.1
   dhcp-gateway-address 10.60.0.1
   exit
   !
. . .
```

```
!
gprs default charging-gateway 10.9.0.2
gprs charging send-buffer 1000
gprs charging container volume-threshold 500000
gprs charging container change-limit 3
gprs charging cdr-aggregation-limit 10
gprs charging cdr-option apn-selection-mode
gprs charging cdr-option served-msisdn
!
gprs memory threshold 512
!
. . .
!
end
```

Supervisor Engine Configuration

```
Sup# show running-config
Building configuration...

Current configuration :12672 bytes
!
version 12.2
...
interface FastEthernet8/22
 no ip address
 switchport
 switchport access vlan 302
!
interface Vlan101
 description Vlan to GGSN for GA/GN
 ip address 10.1.1.1 255.255.255.0
!
interface Vlan302
 ip address 40.0.2.1 255.255.255.0
```

Charging Profile Configuration

The following partial configuration example shows two charging profiles (charging profile 1 and charging profile 2) configured on the GGSN, with charging profile 1 being configured as the global default charging profile to be used for *any* type of user if a charging profile is not specified at the APN:

```
Router# show running-config
Building configuration...

Current configuration :7390 bytes
!
! Last configuration change at 16:56:05 UTC Wed Jun 25 2003
! NVRAM config last updated at 23:40:27 UTC Fri Jun 13 2003
!
version 12.3
.....
interface GigabitEthernet0/0.2
 description Ga/Gn Interface
 encapsulation dot1Q 101
 ip address 10.1.1.72 255.255.255.0
 no cdp enable
!
.....
ip route 40.1.2.1 255.255.255.255 10.1.1.1
!
```

```
!
. . .
!
gprs charging profile default any 1

gprs charging profile 1
 description "roamer_profile"
 limit volume 500000 reset
 limit duration 30 reset
!
gprs charging profile 2
 description "any_unmatched"
 limit volume 1000000 reset
 limit duration 60 reset
. . .
!
. . .
!
end
```

Granular Charging and Storage Configuration

The following partial configuration example shows two charging groups (charging group 1 and charging group 2) configured on the GGSN, with an iSCSI target defined in charging group 1. Charging group 1 is associated with access point 4 and access point 5:

```
Router# show running-config
Building configuration...

Current configuration :7390 bytes
.....
!
gprs access-point-list gprs
access-point 4
access-point-name test2
charging group 1
!
access-point 5
access-point-name pppregen
charging group 1
ppp-regeneration
!
!
!
gprs charging group 2
primary 66.66.66.1
secondary 66.66.66.2
tertiary 66.66.66.3
!
gprs charging group 1
primary 55.55.55.1
secondary 55.55.55.2
tertiary 55.55.55.3
iscsi ISCSI_TARGET1
switchover priority
!
gprs iscsi TARGET_LINUX
```

CHAPTER 8

Implementing Enhanced Service-Aware Billing

This chapter describes how to implement the Cisco Gateway GPRS Support Node (GGSN) as a service-aware GGSN. A service-aware GGSN is capable of real-time credit-control for prepaid subscribers and service-aware billing for postpaid and prepaid subscribers.

Note Service-aware GGSN functionality is supported for IPv4 packet data protocol (PDP) contexts only.

For complete descriptions of the GGSN commands in this chapter, see *Cisco GGSN Command Reference* for the Cisco GGSN release you are using. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

This chapter includes the following sections:

- Service-Aware GGSN Overview, page 8-2
- Reviewing Limitations and Restrictions, page 8-3
- Enabling Support for Service-Aware Billing, page 8-3
- Configuring Wait Accounting, page 8-4
- Configuring the GGSN to Generate Enhanced G-CDRs, page 8-4
- Configuring Quota Server Support on the Cisco GGSN, page 8-5
- Implementing Service-Aware Billing with Diameter/DCCA Support, page 8-12
- Implementing Service-Aware Billing with OCS Address Selection Support, page 8-29
- Enabling PCC under an APN, page 8-31
- Configuring Standalone GGSN Prepaid Quota Enforcement, page 8-32
- Configuring the Charging Record Type under an APN, page 8-34
- GTP-Session Redundancy for Service-Aware PDPs Overview, page 8-35
- Configuring Per-Service Local Sequence Number Synchronization, page 8-36
- Configuring Activity-Based Time Billing for Prepaid Subscribers, page 8-36
- Configuring HTTP Redirection, page 8-37
- Configuring Cisco CSG2 Load Balancing, page 8-43
- Reviewing Trigger Conditions for Enhance Quota Server Interface Users, page 8-45
- Configuration Examples, page 8-47

Service-Aware GGSN Overview

Implemented together, Cisco GGSN and Cisco Content Services Gateway - 2nd Generation (CSG2) function as a service-aware GGSN, also known as an enhanced GGSN (eGGSN).

There are two methods of implementing a service-aware GGSN:

1. Using the Cisco GGSN and Cisco CSG2 configuration with Cisco IOS Diameter protocol/Diameter Credit Control Application (DCCA) support on the GGSN
2. Using Cisco GGSN and Cisco CSG2 configuration with Online Charging System (OCS) address support on the GGSN.

In a service-aware GGSN implementation, Cisco CSG2 and GGSN provide the following functions:

- Cisco CSG2:
  - Inspects packets and categorizes traffic.
  - Requests quota and reports usage.
  - Provides billing plans, service names, and content definitions.
  - Acts as a RADIUS proxy for non-DCCA traffic.
  - Functions in prepaid mode for each service-flow charge recording.

  For detailed information about configuring Cisco CSG2, see *Cisco Content Services Gateway - 2nd Generation Release 3.5 Installation and Configuration Guide*.
- When implemented with Diameter/DCCA, the GGSN:
  - Functions as a quota server to Cisco CSG2.
  - Provides the Diameter interface to the DCCA server for quota requests and returns.
  - Manages the quota requested by Cisco CSG2 and received from the DCCA server.
  - Maps DCCA server rulebases to Cisco CSG2 billing plans.
  - Maps DCCA server category quota to Cisco CSG2 service quota.
- When implemented with OCS address selection support, the GGSN functions as a quota server for postpaid subscribers only. OCS address selection support enables an external OCS to which Cisco CSG2 has a direct connection to provide online credit control for prepaid subscribers.

To implement a service-aware GGSN, complete the tasks in the following sections:

- Reviewing Limitations and Restrictions, page 8-3
- Enabling Support for Service-Aware Billing, page 8-3 (Required)
- Configuring Wait Accounting, page 8-4 (Required if support for service-aware billing is enabled on an access point name [APN])
- Configuring the GGSN to Generate Enhanced G-CDRs, page 8-4 (Required)
- Configuring Quota Server Support on the Cisco GGSN, page 8-5 (Required)
- Implementing Service-Aware Billing with Diameter/DCCA Support, page 8-12 (Required if OCS Address Selection Support is not enabled)
- Implementing Service-Aware Billing with OCS Address Selection Support, page 8-29 (Required if Diameter/DCCA Support is not configured)
- Configuring the Service Aware Billing Parameters in Charging Profiles, page 8-25 (Required)

Reviewing Limitations and Restrictions

The following limitations and restrictions apply to enhanced service-aware billing:

- If session redundancy is required, GGSN supports a maximum of 21 categories per user.
- To populate the Cisco CSG2 User Table entries with the PDP context user information, enable RADIUS accounting between the Cisco CSG2 and Cisco GGSN.
- Configure the quota server address of the Cisco GGSN on the Cisco CSG2.
- If using DCCA, configure the service IDs on Cisco CSG2 as numeric strings that match the category IDs on the DCCA server.
- If you are not using RADIUS, configure the Cisco CSG2 as a RADIUS proxy on the GGSN.
- On the SGSN, the values you configure for the number GTP N3 requests and T3 retransmissions must be larger than the sum of all possible server timers (RADIUS, DCCA, and Cisco CSG2).

  Specifically the SGSN N3*T3 must be greater than:

  2 x RADIUS timeout + *N* x DCCA timeout + Cisco CSG2 timeout

  where:

  - 2 is for both authentication and accounting.
  - *N* is for the number of Diameter servers configured in the server group.
- If you enable support for service-aware billing on an access point name (APN), configure the GGSN to wait for a RADIUS accounting response before sending a Create PDP Context response to the SGSN.

Enabling Support for Service-Aware Billing

Support for enhanced service-aware billing must be enabled on the GGSN before you can implement service-aware billing features on the Cisco GGSN.

To enable service-aware billing support on the GGSN, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs service-aware`	Enables the GGSN to support service-aware billing.

To enable service-aware billing support on a particular access-point, use the following command in access-point configuration mode:

Command	Purpose
`Router(access-point-config)# service-aware`	Enables an APN to support service-aware billing.

Note If you enable support for service-aware billing under an APN, you must configure the GGSN to wait for a RADIUS accounting response before it sends a Create PDP Context response to the SGSN. For information about configuring the GGSN to wait for a RADIUS accounting response, see the "Configuring Wait Accounting" section on page 8-4.

Configuring Wait Accounting

If service-aware billing is enabled under an APN, you must configure wait accounting on the GGSN. When wait accounting is configured on the GGSN, the waits for a RADIUS accounting response before it sends a Create PDP Context response to the SGSN

To enable wait accounting on the GGSN, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs gtp response-message wait-accounting`	Configures the GGSN to wait for a RADIUS accounting response before sending a Create PDP Context response to the SGSN.

Note Wait accounting is required for an enhanced GGSN (eGGSN) implementation, but is optional for a Standalone GGSN Quota Enforcement.

Configuring the GGSN to Generate Enhanced G-CDRs

Gateway GPRS support node-call detail records (G-CDRs) contain information for the entire duration of, or part of, a PDP context. The G-CDR includes information such as the subscriber (mobile station ISDN [MSISDN] number, mobile subscriber identity [IMSI]), APN used, Quality of Service (QoS) applied, SGSN ID (as the mobile access location), a time stamp and duration, the data volume recorded separately for the upstream and downstream direction, and volume thresholds for intermediate CDR generation and tariff time switches.

In addition, enhanced G-CDRs (eG-CDRs) also contain a service-record information element (IE) that contains the usage data of each service flow used by a PDP session, specified by category ID. For example, the upstream and downstream volume, and the duration are recorded per service flow.

By default, the GGSN does not include the service records in G-CDRs. To support a service-aware GGSN implementation, you must configure the GGSN to generate eG-CDRs by configuring it to include service records in G-CDRs.

Note With Cisco GGSN Release 9.2 and later, the generation of enhanced G-CDRs (eG-CDRs) requires that charging release 7 has been configured on the GGSN by using the **gprs charging release 7** command in global configuration mode.

To configure the GGSN to include the service records in G-CDRs, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs charging cdr-option service-record [1-100]`	Configures the GGSN to include the service-record IE in G-CDRs and specifies the maximum service records an G-CDR can contain before the G-CDR is closed and a partial G-CDR is opened. A valid value is a number between 1 and 100. The default is 5.

To configure the GGSN to include the public land mobile network (PLMN) ID, radio access technology (RAT), or User Location Info fields in the service-record IE in eG-CDRs, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs charging service-record include [plmn-id | rat | user-loc-info-change]`	Configures the GGSN to include certain fields in the service-record IE in eG-CDRs, where: • **plmn-id**—Configures the GGSN to include the PLMN-ID field. • **rat**—Configures the GGSN to include the RAT field. The RAT indicates whether the SGSN serves the user equipment (UE) UMTS or GSM/EDGE RAN (GERAN). • **user-loc-info-change**—Configures the GGSN to include the User-Location-Info field.

Configuring Quota Server Support on the Cisco GGSN

To configure quota server support on the GGSN, complete the tasks in the following sections:

- Configuring a Cisco CSG2 Server Group, page 8-6 (Required)
- Configuring the Quota Server Interface on the GGSN, page 8-7 (Required)
- Advertising the Next Hop Address For Downlink Traffic, page 8-10
- Configuring the GGSN to Use the Cisco CSG2 as a RADIUS Authentication and Accounting Proxy, page 8-10 (Required, if RADIUS is not being used.)
- Monitoring and Maintaining the Quota Server-to-CSG2 Configuration, page 8-12

Configuring a Cisco CSG2 Server Group

We recommend that you configure two Cisco CSG2s (one active, the other standby) to function as one when interacting with the quota server process on the GGSN.

When configuring the Cisco CSG2 group that the GGSN quota server interface uses to communicate with the Cisco CSG2, you must specify a virtual IP address along with the real IP addresses of each of the Cisco CSG2s that make up the redundant pair. The quota server process on the GGSN communicates with the virtual address and the active Cisco CSG2 listens to the virtual IP address.

To configure a Cisco CSG2 group on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ggsn csg csg-group-name`	Specifies a name for the Cisco CSG2 server group and enters Cisco CSG2 group configuration mode.
Step 2	`Router(config-csg-group)# virtual-address ip-address`	Specifies the virtual IP address of the Cisco CSG2 group. This is the IP address that the quota server process on the GGSN uses to communicate with the Cisco CSG2.
Step 3	`Router(config-csg-group)# port port-number`	(Optional) Configures the port on which the Cisco CSG2 listens for communications from the quota server. The default is 3386. **Note** The Cisco CSG2 always sends messages to the quota server on port 3386.
Step 4	`Router(config-csg-group)# real-address ip-address`	Configures the IP address of a real Cisco CSG2 for source checking of inbound messages from a Cisco CSG2. Configure a real IP address for each of the Cisco CSG2s that make up the redundant pair.
Step 5	`Router(config-csg-group)# aaa-group accounting server-group`	Configures the Cisco CSG2 RADIUS interface for accounting services.

Configuring the Quota Server Interface on the GGSN

In releases before Cisco GGSN Release 9.2, the GGSN uses the quota server interface to the Cisco CSG2 to obtain usage information to generate eG-CDRs for the following types of users:

- Service-aware prepaid (Gy) and service-aware postpaid (QS) users

  For prepaid subscribers or for postpaid subscribers configured as prepaid on the CSG2, the GGSN functions as the quota server and adds service containers to the eG-CDRs whenever it receives usage from the CSG2 over the quota server interface.

With Cisco GGSN Release 9.2 and later, you can specify the **service-msg** keyword option of the **ggsn quota-server** command to configure an enhanced quota server interface between the GGSN and Cisco CSG2. An *enhanced* quota server interface supports the exchange of service control messages that contain service usage information and enable the GGSN to generate eG-CDRs for the following additional types of users:

- Service-aware prepaid (GTP') users

  In a service-aware GGSN implemented with OCS address selection, the GGSN does not function as a quota server for prepaid users. OCS address selection support enables the Cisco CSG2 to obtain quota from an external OCS to which it has a direct GTP' connection. The GGSN generates eG-CDRs by obtaining the service usage via the enhanced quota server interface.

- Service-aware postpaid users

  The GGSN does not function as the quota server for service-aware postpaid users. The GGSN uses the enhanced quota server interface to obtain usage from the Cisco CSG2 and adds the usage to the eG-CDRs.

- Policy and Charging Control (PCC)-enabled (Gx) users

  When Gx-enabled users are also prepaid (Gy) users, support for eG-CDR generation is as present in releases before Cisco IOS Release 12.4(22)YE2 and the service containers are added to eG-CDRs based on the usage received in quota server messages.

  When a Gx user is also a prepaid user in an implementation in which the CSG2 has a direct OCS interface, or a postpaid user (either service-aware or nonservice-aware), the GGSN obtains usage from the CSG2 via the enhanced quota server interface and add the usage to the eG-CDRs.

Note With Cisco IOS Release 12.4(22)YE2 and later, when an enhanced quota server interface is enabled on the GGSN, the GGSN does not function as the quota server for service aware postpaid users or Gx postpaid users; therefore, these uses must be configured as postpaid on the Cisco CSG2. For information about configuring the Cisco CSG2, see *Cisco Content Services Gateway 2nd Generation - Release 3.5 Installation and Configuration Guide.*

Quota Server Interface

The quota server interface on the GGSN provides support of the following:

- Attributes in RADIUS Accounting Start messages to the Cisco CSG2
  - Billing plan ID—Corresponds with the rulebase ID received from a DCCA server. The quota server process on the GGSN maps the rulebase ID to the billing plan ID.
  - Quota server address and port—IP address and port of the quota server that the Cisco CSG2 should use for a user.
  - By default, this is the IP address of the GGSN unless OCS address selection support is enabled on the GGSN. For information about enabling OCS address selection support on the GGSN, see the "Implementing Service-Aware Billing with OCS Address Selection Support" section on page 8-29.
  - Downlink next hop address—Next hop address (user address) for downlink traffic (Cisco CSG2-to-GGSN).
- Threshold Limit Values (TLVs):
  - Quota Consumption Timer (QCT). The QCT is assumed to be zero.
  - Quota Holding Timer (QHT)
  - Quota Threshold

For more information on the quota server interface, billing plans, and the QCT and QHT, see *Cisco Content Services Gateway 2nd Generation - Release 3.5 Installation and Configuration Guide*.

Enhanced Quota Server Interface

The enhanced quota server interface provides the additional support the following:

- Service control messages
  - Service Control Request (SCR)
  - Service Control Request Ack
  - Service Control Usage (SCU)
  - Service Control Usage Ack
- Attributes in RADIUS Accounting and Stop messages to the Cisco CSG2
  - Quota server mode—Specifies the capability of the enhanced quota server interface; whether online charging is enabled or offline charging is enabled.
  - eG-CDR correlator ID—Identifier that the GGSN uses to match Service Control Usage with the Service Control Request

When configuring an enhance quota server interface:

- An APN must be enabled for service-aware billing support (**service-aware** command) or PCC-enabled (**pcc** command) to trigger service control messages.
- GPRS Charging Release 7 must be configured as described in the "Configuring the Charging Release" section on page 7-8.
- Configure a charging record type for participating APNs as described in the "Configuring the Charging Record Type under an APN" section on page 8-34.

- Configure the sychronization for per -service local sequence number as described in the "Configuring Per-Service Local Sequence Number Synchronization" section on page 8-36.
- You can configure one quota server interface per GGSN. Configuring more than one quota server interface overwrites the existing interface.

To configure the quota server interface on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ggsn quota-server server-name [service-msg]`	Enables the quota server process on the GGSN and enters quota server configuration mode. Optionally, specify the **service-msg** keyword option to enable the quota server process to exchange service control messages.
Step 2	`Router(config-quota-server)# interface interface-name`	Specifies the logical interface, by name, for the quota server to use. We recommend that you use a loopback interface as the quota server interface. **Note** The quota server must use a different address than the GTP virtual template address.
Step 3	`Router(config-quota-server)# echo-interval [ 0 | 60-65535]`	Specifies the number of seconds that the quota server waits before sending an echo request message to the Cisco CSG. The valid values are 0 (echo messages are disabled) or a value between 60 and 65535. The default is 60.
Step 4	`Router(config-quota-server)# n3-requests number`	Specifies the maximum number of times that the quota server attempts to send a signaling request to the Cisco CSG. The valid value is a number between 2 and 65535. The default is 5.
Step 5	`Router(config-quota-server)# t3-response number`	Specifies the initial time that the quota server waits before resending a signaling request message when a response to a request has not been received. The valid value is a number between 2 and 65535. The default is 1.
Step 6	`Router(config-quota-server)# csg group csg-group-name`	Specifies the Cisco CSG2 group that the quota server process uses to communicate with a Cisco CSG2. **Note** The quota server process supports only one path to a Cisco CSG2, therefore, you can specify only one Cisco CSG2 group at a time. **Note** The the **csg group** quota server configuration command and the **csg-group** access point configuration command are mutually exclusive. You cannot define a CSG group under the quota server interface if one has already been configured under an APN.

	Command	Purpose
Step 7	`Router(config-quota-server)# scu-timeout` *csg-group-name*	Specifies the time, in seconds, that the GGSN waits to receive the SCU from the Cisco CSG2 before discarding the SCR. A valid value is a number between 1 and 1000. The default is 30.
Step 8	`Router(config-quota-server)# exit`	Exits quota server configuration mode.

Advertising the Next Hop Address For Downlink Traffic

To configure the next hop address (the user address) for downlink traffic (Cisco CSG2-to-GGSN) to be advertised in Accounting Start requests to the RADIUS endpoint, use the following command in access-point configuration mode:

Command	Purpose
`GGSN(access-point-config)# advertise downlink next-hop` *ip-address*	Configures the next hop address, to which downlink traffic destined for the GGSN is routed, to be advertised in Accounting Start requests.

Configuring the GGSN to Use the Cisco CSG2 as a RADIUS Authentication and Accounting Proxy

If you are not using RADIUS, you must configure the Cisco CSG2 as a RADIUS proxy.

To configure the GGSN to use the Cisco CSG2 as a RADIUS proxy, complete the following tasks:

- Configuring a Global RADIUS Server, page 8-11
- Configuring an AAA RADIUS Server Group that includes the Cisco CSG2, page 8-11
- Using Method List to Specify Supported Services, page 8-11
- Specifying Method Lists for an APN, page 8-12

Configuring a Global RADIUS Server

To configure a RADIUS server globally, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number]`	Specifies a RADIUS server host.
Step 2	`Router(config)# radius-server key {0 string | 7 string | string}`	Sets the authentication and encryption key for all RADIUS communications between the GGSN and the RADIUS daemon.

Configuring an AAA RADIUS Server Group that includes the Cisco CSG2

To define an Authentication, Authorization and Accounting (AAA) RADIUS server group, and include the Cisco CSG2 as a server in the server group, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa group server radius group-name`	Specifies an AAA RADIUS server group and assigns the selected server group for authentication services.
Step 2	`Router(config-sg-radius)# server ip_address [auth-port port-number] [acct-port port-number]`	Configures the IP address of the RADIUS endpoint in the server group.
Step 3	`Router(config-sg-radius)# exit`	Exits server group configuration mode.

Using Method List to Specify Supported Services

To use AAA method lists to specify the types of services the group supports, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa authentication ppp list-name group group-name`	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.
Step 2	`Router(config)# aaa authorization network list-name group group-name`	Sets parameters that restrict network access to a user.
Step 3	`Router(config)# aaa accounting network list-name start-stop group group-name`	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS.

Specifying Method Lists for an APN

To reference method lists for the APNs that use the Cisco CSG2 as a RADIUS proxy, use the following commands in access-point configuration mode:

	Command	Purpose
Step 1	`Router(access-point-config)# aaa-group authentication` *server-name*	Specifies an AAA server group and assigns the selected server group for authentication services on the access point.
Step 2	`Router(access-point-config)# aaa-group accounting` *server-name*	Specifies the logical interface, by name, for the quota server to use.

Monitoring and Maintaining the Quota Server-to-CSG2 Configuration

To monitor and maintain the quota server-to-Cisco CSG2 configuration, use the following commands in privileged EXEC mode.

Command	Purpose
`Router# clear ggsn quota-server statistics`	Clears quota server-related statistics (messages and error counts).
`Router# show ggsn quota-server [parameters | statistics]`	Displays quota server parameters or statistics about quota server messages and error counts.
`Router# show ggsn csg [parameters | statistics]`	Displays the parameters used by the Cisco CSG2 group or the number of path and quota management messages sent and received by the quota server.

Implementing Service-Aware Billing with Diameter/DCCA Support

To implement a service-aware GGSN with Diameter/DCCA support, complete the tasks in the following sections:

- Reviewing Service-Aware Billing with DCCA/Diameter, page 8-13
- Configuring the Diameter Base, page 8-16
- Configuring the DCCA Client Process on the GGSN, page 8-21
- Enabling Support for Vendor-Specific AVPs in DCCA Messages, page 8-24
- Configuring the Service Aware Billing Parameters in Charging Profiles, page 8-25

Reviewing Service-Aware Billing with DCCA/Diameter

In a service-aware GGSN implementation with DCCA, the Cisco CSG2 categorizes traffic, reports usage, and manages quota. The GGSN functions as a DCCA client to communicate with a DCCA server to provide the following functions:

- Diameter interface (Gy) to the DCCA server via which the Cisco CSG2 requests quota and reports usage.
- Quota negotiation by sending quota requests from the Cisco CSG2 to the DCCA server and pushing quota returns from the DCCA server to the Cisco CSG2.
- DCCA server rulebases to Cisco CSG2 billing plans mapping.
- DCCA server category quota to Cisco CSG2 service quota mapping.
- PDP maintenance and determining if a PDP is prepaid or postpaid.

If prepaid service-based charging or postpaid service-based charging is required, entries are created on the Cisco CSG2. The Cisco CSG2 inspects the service categories and reports usage to the GGSN. If the user is to be treated as a postpaid subscriber (offline charging), the GGSN records the usage information that is reported by the Cisco CSG2 in an eG-CDR. If the user is to be treated as a prepaid subscriber (online charging), the GGSN records the reported usage information in an eG-CDRs, and translates and sends the information to a DCCA server.

The GGSN also handles Gn-side triggers for quota reauthorization and server-initiated reauthorization or termination requests. The Cisco CSG2 sends the authorization requests, quota reports, and service stops to the GGSN,. The GGSN translates what the Cisco CSG2 sends into DCCA messages for transport over the Diameter interface. When the DCCA server responds with additional quota, the GGSN pushes the quota to the Cisco CSG2.

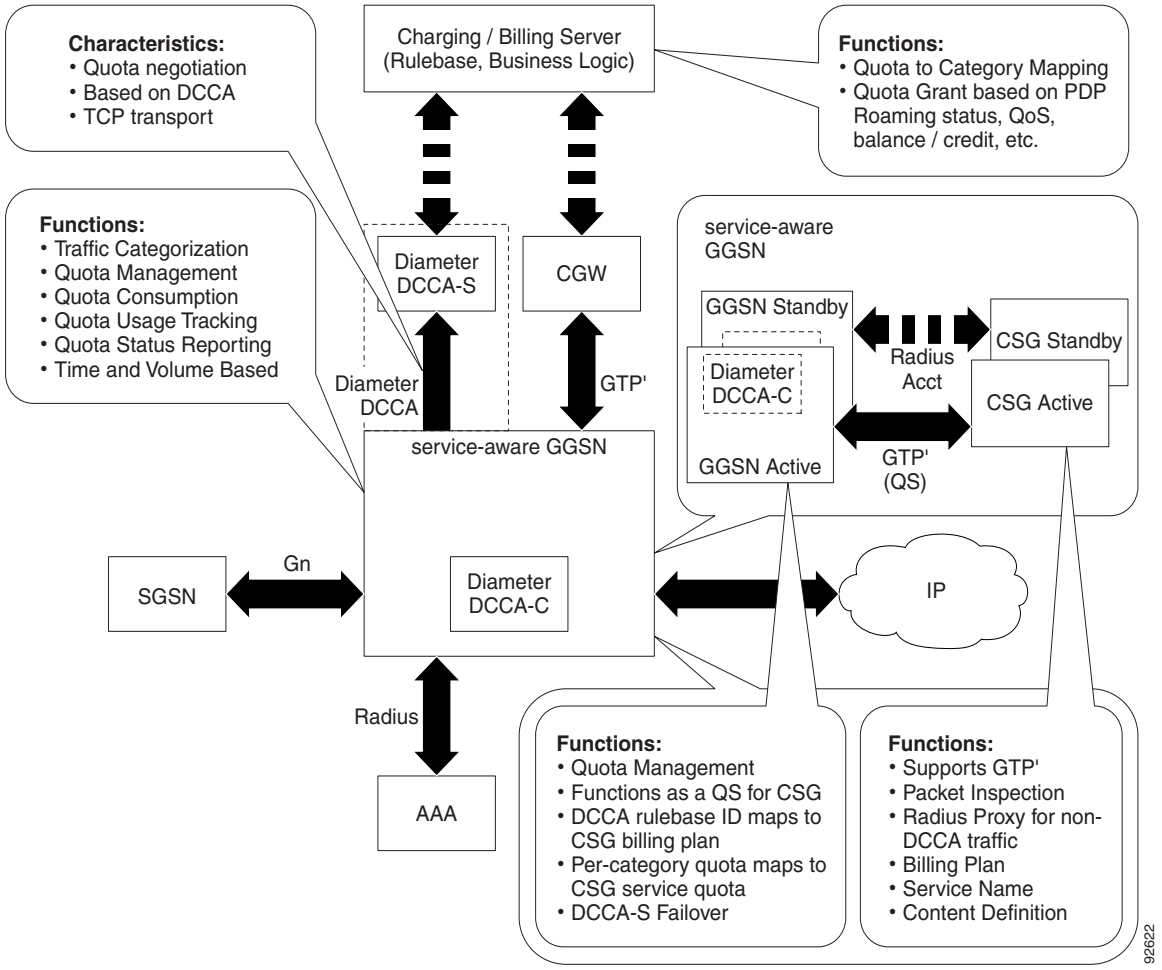
Note If RADIUS is not being used, you must configure the Cisco CSG2 as a RADIUS proxy.

This section contains the following overview information about service-aware billing with DCCA/Diameter:

- Supported Features, page 8-14
- Unsupported Features, page 8-15
- Messaging Support, page 8-15
- Service-Aware Billing with DCCA Data Flows, page 8-16

Figure 8-1 shows the functions and characteristics of a service-aware GGSN implemented with DCCA support.

Figure 8-1 High-Level Overview of Service-Aware GGSN Functions When Implemented with DCCA Support



Supported Features

To enable the implementation of a service-aware GGSN with DCCA, the Cisco GGSN supports the following features:

- Diameter/DCCA client interface support for online/real-time credit control for prepaid subscribers (IP PDP contexts only)
- Quota server functionality and interface to Cisco CSG2 for per-service billing
- Enhanced G-CDRs for service-based CDRs for prepaid and postpaid subscribers
- AAA authentication interface—DCCA rulebase support and charging profile selection
- AAA accounting interface—Cisco CSG2 User Table population and Cisco CSG-based proxies
- Enhanced Ga interface for offline charging

Unsupported Features

The following features are not supported by a service-aware GGSN implementation with DCCA:

- Charging differentiation for secondary PDP contexts
- PPP PDP contexts
- PPP regeneration
- Network management
- Cell identity
- PDP contexts for both online DCCA exchange and offline service-based usage
- Dynamic configuration for blocking/forwarding traffic while waiting for quota reauthorization
- Diameter proxy, relay, or redirection
- Diameter transport layer security
- SCTP transport
- No dual quota support (for receiving volume and time quota)

Messaging Support

To support credit control via Diameter, the DCCA client process on the GGSN and the DCCA server exchange the following messages:

- Credit Control Request (CCR)—Initial, Update, and Final
- Credit Control Answer (CCA)—Initial, Update, and Final

In addition, the GGSN Diameter interface supports the following base Diameter messages:

- Capability Exchange Request (CER) and Capability Exchange Answer (CEA)—The GGSN advertises DCCA support in CER messages. In addition, the GGSN can be configured to advertise support for vendor-specific attribute value pairs (AVPs) using the **diameter vendor support** command in global configuration mode.
- Disconnect Peer Request (DPR) and Disconnect Peer Answer (DPA)—The GGSN sends a DPR message when the CER with a Diameter peer fails or there is no Diameter server configured.
- Device Watchdog Request (DWR) and Device Watchdog Answer (DWA)—The GGSN uses DWR and DWA messages to detect transport failures with a Diameter peer. A watchdog timer can be configured for each Diameter peer using the **timer watchdog** command in Diameter peer configuration mode.
- Re-auth Request (RAR) and Re-auth Answer (RAA)
- Abort Session Request (ASR) / Abort Session Answer (ASA)—No Failed-AVP is sent in an ASA when an incorrect ASR is sent from the DCCA server.

As a DCCA client, the GGSN also receives the following notifications from Cisco IOS AAA:

- CCA message receipts
- Asynchronous session termination requests
- Server-initiated RARs

Service-Aware Billing with DCCA Data Flows

The following is a high-level overview of the flow of traffic during the creation of a PDP context for a prepaid subscriber in an enhanced service-aware billing implementation using DCCA.

PDP Context Creation Data Flow for Prepaid Subscribers

1. SGSN sends a Create PDP Context request to the service-aware GGSN.
2. GGSN sends an Access-Request message to the RADIUS (server or Cisco CSG2 configured as a RADIUS proxy).
3. RADIUS returns an Access-Accept response. From the Access-Accept response, the GGSN obtains a default rulebase ID, or if the response does not contain a default rulebase ID, the GGSN obtains the rulebase ID from a locally configured value in the charging profile selected for the Create PDP Context request.
4. Service-aware GGSN sends a Diameter Credit Control Request (CCR) to the DCCA server.
5. DCCA server returns a Credit Control Answer (CCA) to the GGSN. This CCA might contain a rulebase and quota request.
6. If the CCA contains a rulebase, the GGSN sends an Accounting-Start request with the selected rulebase to the RADIUS.
7. RADIUS receives the Accounting-Start request from the GGSN and creates a Cisco CSG2 User Table entry for the user.
8. RADIUS sends an Accounting-Start response to the GGSN.
9. If the DCCA server sends a quota request in a CCA to the GGSN, the GGSN pushes the quota request to the Cisco CSG2.
10. When the GGSN receives a quota push response from the Cisco CSG2, it sends the Create PDP Context response to the SGSN, and the context is established.

PDP Context Creation Data Flow for Postpaid Subscribers

1. SGSN sends a Create PDP Context request to the service-aware GGSN.
2. GGSN sends an Accounting-Start request containing the selected rulebase to the RADIUS (server or the Cisco CSG2 configured as a RADIUS proxy).
3. RADIUS proxy receives the Accounting-Start request and creates a Cisco CSG2 User Table entry for the user.
4. RADIUS proxy sends an Accounting-Start response to the GGSN.
5. When the GGSN receives the Accounting-Start response from the RADIUS proxy, it sends a Create PDP Context response to the SGSN, and the context is established.

Configuring the Diameter Base

To configure the Diameter protocol base, complete the tasks in the following sections:

- Configuring a Diameter Peer, page 8-17
- Enabling Diameter AAA, page 8-18
- Configuring Diameter Protocol Parameters Globally, page 8-19
- Monitoring and Maintaining the Diameter Base, page 8-21

Configuring a Diameter Peer

To configure a Diameter peer, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# diameter peer name`	Configures a device as a Diameter protocol peer and enters Diameter peer configuration mode.
Step 2	`Router(config-dia-peer)# address ipv4 ip-address`	Defines a route to the host of the Diameter peer using IPv4.
Step 3	`Router(config-dia-peer)# transport {tcp | sctp} port port-num`	Configures the transport protocol for connecting to the Diameter peer. **Note** The Cisco GGSN supports TCP.
Step 4	`Router(config-dia-peer)# security ipsec`	Configures IPSec as the security protocol for the Diameter peer-to-peer connection.
Step 5	`Router(config-dia-peer)# source interface interface`	Configures the interface to connect to the Diameter peer.
Step 6	`Router(config-dia-peer)# timer {connection | transaction | watchdog} value`	Configures Diameter base protocol timers for peer-to-peer communication. The valid range, in seconds, is from 0 to 1000. The default is 30. • **connection**—Maximum amount of time the GGSN attempts to reconnect to a Diameter peer after a connection to the peer is brought down due to a transport failure. A value of 0 configures the GGSN to not try to reconnect. • **transaction**—Maximum amount of time the GGSN waits for a Diameter peer response before trying another peer. • **watchdog**—Maximum amount of time the GGSN waits for a Diameter peer response to a watchdog packet. When the watchdog timer expires, a DWR is sent to the Diameter peer and the watchdog timer is reset. If a DWA is not received before the next expiration of the watchdog timer, a transport failure to the Diameter peer has occurred. When configuring timers, the value for the transaction timer, should be larger than the TX-timeout value, and, on the SGSN, the values configured for the number GTP N3 requests and T3 retransmissions must be larger than the sum of all possible server timers (RADIUS, DCCA, and Cisco CSG2). Specifically, the SGSN N3*T3 must be greater than 2 x RADIUS timeout + *N* x DCCA timeout + Cisco CSG2 timeout where: • 2 is for both authentication and accounting. • *N* is for the number of Diameter servers configured in the server group.

	Command	Purpose
Step 7	`Router(config-dia-peer)# destination host string`	Configures the Fully Qualified Domain Name (FQDN) of a Diameter peer.
Step 8	`Router(config-dia-peer)# destination realm string`	Configures the destination realm (part of the domain "@*realm*") of a Diameter peer. The realm might be added by the AAA client when sending a request to AAA. However, if the client does not add the attribute, then the value you configure in Diameter peer configuration mode is used when sending messages to the destination Diameter peer. If you do not configure a value in Diameter peer configuration mode, the value you configure globally by using the **diameter destination realm** command is used.
Step 9	`Router(config-dia-peer)# ip vrf forwarding name`	Associates a Virtual Routing and Forwarding (VRF) instance with a Diameter peer. **Note** If a VRF name is not configure for a Diameter server, the global routing table is used.

Enabling Diameter AAA

To enable Diameter AAA, complete the tasks in the following sections:

- Defining the Diameter AAA Server Group, page 8-18
- Defining an Authorization Method List for Prepaid Subscribers, page 8-19

Defining the Diameter AAA Server Group

For redundancy, configure Diameter servers as Diameter AAA server groups that consist of a primary and secondary server.

To define a Diameter AAA server group, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa new-model`	Enables AAA.

	Command	Purpose
Step 2	`Router(config)# aaa group server diameter group-name`	Groups different Diameter server hosts into distinct lists and methods. Configuring AAA server groups allows different servers to be used for each element of AAA. It also defines a redundant set of servers for each element.
Step 3	`Router(config-sg-diameter)# server name auth-port 1645 acct-port 1646`	Configures the name of the Diameter server for the group server. The name specified for this command should match the name of a Diameter peer defined using the **diameter peer** command. **Note** The port numbers 1645 and 1646 are defaults for authorization and accounting, respectively. Explicit port numbers are required only if non-default ports are used.

Defining an Authorization Method List for Prepaid Subscribers

To apply parameters that restrict access to a network for prepaid subscribers, use the following command in global configuration mode:

Command	Purpose
`Router(config)# aaa authorization prepaid method_list group server_group [group server_group]`	Defines an authorization method list for prepaid subscribers and defines the Diameter AAA groups to send records.

Configuring Diameter Protocol Parameters Globally

The GGSN uses global Diameter protocol parameters if you have not defined Diameter parameters at the Diameter peer level.

To configure global Diameter parameters, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# diameter timer {connection | transaction | watchdog} value`	Configures Diameter base protocol timers to use if none have been configured at the Diameter peer level. The valid range, in seconds, is 0 to 1000. The default is 30. • **connection**—Maximum amount of time the GGSN attempts to reconnect to a Diameter peer after being disconnected due to a transport failure. A value of 0 configures the GGSN to not try to reconnect. • **transaction**—Maximum amount of time the GGSN waits for a Diameter peer response before trying another peer. • **watchdog**—Maximum amount of time the GGSN waits for a Diameter peer response to a watchdog packet. When the watchdog timer expires, a DWR is sent to the Diameter peer and the watchdog timer is reset. If a DWA is not received before the next expiration of the watchdog timer, a transport failure to the Diameter peer has occurred. When configuring timers, the value for the transaction timers, should be larger than the value for the TX timer, and, on the SGSN, the values configured for the number GTP N3 requests and T3 retransmissions must be larger than the sum of all possible server timers (RADIUS, DCCA, and Cisco CSG2). Specifically, the SGSN N3*T3 must be greater than 2 x RADIUS timeout + *N* x DCCA timeout + Cisco CSG2 timeout where: • 2 is for both authentication and accounting. • *N* is for the number of Diameter servers configured in the server group.
Step 2	`Router(config)# diameter redundancy`	Enables the Diameter node to be a Cisco IOS Redundancy Facility (RF) client and track session states. The Diameter base does not initiate a connection to a Diameter peer that is in standby mode. Upon a standby-to-active mode transition, a connection to the newly active peer is established. **Note** This command is required for Service-aware PDP session redundancy. For more information about service-aware PDP session redundancy, see the "GTP-Session Redundancy for Service-Aware PDPs Overview" section on page 8-35.
Step 3	`Router(config)# diameter origin realm string`	Configures the realm of origin (part of the domain "@*realm*") in which this Diameter node is located. Origin realm information is sent in requests to a Diameter peer.
Step 4	`Router(config)# diameter origin host string`	Configures the Fully Qualified Domain Name (FQDN) of the host of this Diameter node. The origin host information is sent in requests to a Diameter peer.

	Command	Purpose
Step 5	`Router(config)# diameter vendor support {Cisco | 3gpp | Vodafone}`	Configures this Diameter node to advertise the vendor AVPs it supports in capability exchange messages with Diameter peers. Multiple instances of this command can be configured if the vendor IDs differ.

Monitoring and Maintaining the Diameter Base

To monitor and maintain Diameter peer configurations, use the following command in privileged EXEC mode.

Command	Purpose
`Router# show diameter peer`	Displays Diameter peer-related information.

Configuring the DCCA Client Process on the GGSN

The GGSN functions as a DCCA client when interacting with the DCCA server to obtain and request quota. As a DCCA client, the GGSN sends CCR messages to and receives CCAs from the DCCA server for credit control sessions (one credit control session per PDP session). In addition, the defaults you configure in the DCCA client profile dictate how the GGSN handles credit control sessions if a server switchover should occur and no instructions are sent by the server.

Failure Handling Defaults on the DCCA Client

The following two AVPs determine how the credit-control (CC) sessions are handled if a switchover occurs:

- CC-Session-Failover AVP—Indicates that a CC session should fail over to the alternate Diameter server. You set this AVP by using the **session-failover** command in DCCA client profile configuration mode.
- Credit-Control-Failure-Handling (CCFH) AVP—Determines how the GGSN behaves if a failure does occur. You set this AVP by using the **ccfh** command in DCCA client profile configuration mode.

You can configure defaults for these AVPs in the DCCA client profile for failure handling, however, the values received from the DCCA server override the defaults you configure on the GGSN.

The CCFH AVP determines the action the DCCA client takes on a session when the following fault conditions occur:

- Tx timeout expires.
- CCA message containing protocol error (Result-Code 3xxx) is received.
- CCA fails (for example, a CCA with a permanent failure notification [Result-Code 5xxx]) is received.
- Failure-to-send condition exists. (The DCCA client is not able to communicate with the desired destination.)
- An invalid answer is received.

To configure a DCCA client profile, in which you configure the characteristics of a DCCA client process, and reference to from the charging profile, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs dcca profile` *name*	Defines the DCCA client process on the GGSN and enters DCCA client profile configuration mode.
Step 2	`Router(config-dcca-profile)# authorization` *method_list_name*	Defines the method list that is used to specify the Diameter AAA server groups.
Step 3	`Router(config-dcca-profile)# tx-timeout` *seconds*	Configures a TX timeout value, in seconds, that the DCCA client uses to monitor the communication of CCRs with a Diameter server. The valid range is from 1 to 1000 seconds. The default is 10. When configuring timers, the value for the transaction timer, should be larger than the TX-timeout value, and, on the SGSN, the values configured for the number GTP N3 requests and T3 retransmissions must be larger than the sum of all possible server timers (RADIUS, DCCA, and Cisco CSG2). Specifically, the SGSN N3*T3 must be greater than 2 x RADIUS timeout + *N* x DCCA timeout + Cisco CSG2 timeout where: • 2 is for both authentication and accounting. • *N* is for the number of Diameter servers configured in the server group.
Step 4	`Router(config-dcca-profile)# ccfh {continue | terminate | retry_terminate}`	Configures the default Credit Control Failure Handling (CCFH) action to take on PDP contexts when a fault condition occurs. • **continue**—Allows the PDP context and user traffic for the relevant category or categories to continue, regardless of the interruption. Quota management of other categories is not affected. • **terminate**—Terminates the PDP context and the CC session. • **retry_terminate**—Allows the PDP context and user traffic for the relevant category or categories to continue. Hard-coded quota (1 GB) is passed to the CSG2 when the first DCCA server is unavailable. The DCCA client retries to send the CRR to an alternate server and if a failure-to-send condition occurs with the alternate server, the PDP context is terminated. The default is to terminate. A value from the DCCA server in a CCA overrides this default.

	Command	Purpose
Step 5	`Router(config-dcca-profile)# session-failover`	Specifies that a session should switchover to the alternate DCCA server Configures Credit Control Session Failover (CCSF) AVP support when a CCA message from a DCCA server does not contain a value for the CCSF AVP. By default, session switchover is not supported.
Step 6	`Router(config-dcca-profile)# destination-realm` *string*	Specifies the destination realm to be sent in CCR initial requests to the DCCA server. For subsequent CCRs, the Origin-Realm AVP received in the last CCA is used as the Destination-Realm.
Step 7	`Router(config-dcca-profile)# trigger {plmn-change | qos-change | rat-change | sgsn-change | user-loc-info-change}`	Configures a change that when it occurs, triggers the GGSN (functioning as a DCCA client) to request quota-reauthorization and generate an eG-CDR. • **plmn-id**—PLMN ID change triggers a quota reauthorization request. • **qos-change**—QoS change triggers a quota reauthorization request. • **rat**—RAT change triggers a quota reauthorization request. The RAT indicates whether the SGSN serves the user equipment (UE) UMTS or GSM/EDGE RAN (GERAN). • **sgsn-change**—SGSN change triggers a quota reauthorization request. • **user-loc-info-change**—User location change triggers a quota-reauthorization request. Modifying this command does not affect existing PDP contexts using a DCCA client profile. The **plmn-change**, **rat-change**, and **user-loc-info-change** keyword options require that the GGSN is configured to include these fields in the service-record IE in CDRs using the **gprs charging service record include** command. When configuring triggers: • This command is supported by the generic DCCA client and 3GPP Gy-DCCA only. • Explicitly enable all triggers for both prepaid and postpaid users. • Configured prepaid triggers apply to all of the services that flow through the PDP context. The triggers received for a given service from the OCS server take precedence over the ones configure using the **trigger** command.

Enabling Support for Vendor-Specific AVPs in DCCA Messages

The Cisco GGSN supports the following DCCA implementations:

- VF_CLCI (Vodafone)
- 3GPP Gy-compliant (3GPP)

Note With Cisco GGSN Release 9.0 and later, neither of these implemenations are supported by default. A DCCA implementation must be explicitly enabled using the **gprs dcca 3gpp** command or the **gprs dcca clci** command.

The Gy-compliant implementation supports some additional 3GPP Vendor Specific Attributes (VSAs) in addition to the standard DCCA attributes. The VF_CLCI compliant implementation supports Vodafone specific VSAs, 3GPP VSAs where necessary, and the standard DCCA attributes.

The Cisco GGSN advertises the support of only DCCA application (Auth-Application-Id of 4) in CER messages. In addition, it advertises the support of the following Vendor Ids (for recognizing the vendor specific AVPs).

- Cisco (vendor id = 9)
- 3GPP (vendor id = 10415)
- Vodafone (vendor id = 12645)

To enable the Cisco GGSN to send 3GPP VSAs in DCCA messages to the DCCA server, complete the following task while in global configuration mode.

Command	Purpose
`Router(config)# gprs dcca 3gpp`	Configures the GGSN to send 3GPP VSAs in DCCA messages to the server.

To enable the GGSN to send Vodafone VSAs in DCCA messages to the DCCA server, in addition to the standard DCCA attributes and 3GPP VSAs, complete the following task while in global configuration mode.

Command	Purpose
`Router(config)# gprs dcca clci`	Configures the GGSN to send Vodafone vendor-specific AVPs in DCCA messages to the server.

For a list of supported AVPs in respect to the Gy-based and VF-CLCI, refer to the *Diameter Credit Control Application on the Cisco GGSN* technical whitepaper.

Configuring the Service Aware Billing Parameters in Charging Profiles

The GGSN supports up to 256 charging profiles, numbered 0 to 255. Profile 0 is a set profile that always exists on the GGSN. It is the global default charging profile. You do not create profile 0, however, you can modify it using the charging-related global configuration commands. Profiles 1 to 255 are user-defined and customized using the Cisco GGSN charging profile configuration commands.

To support service-aware billing, you can configure a charging profile to allow eG-CDRs and suppress G-CDRs for all or only online charging.

You can also configure the following service-aware billing characteristics in a charging profile:

- Default rulebase-ID to apply to a user
- Default charging type (to be used primarily for a prepaid or postpaid subscriber)
- DCCA servers to contact for quota requests (presence indicates online charging)

To configure service-aware billing characteristics in a charging profile, complete the tasks in the following sections:

- Specifying a Default Rulebase ID, page 8-25
- Specifying a DCCA Profile for Online Billing, page 8-26
- Suppressing CDRs for Prepaid Subscribers, page 8-27
- Configuring Trigger Conditions for Postpaid Subscribers, page 8-27

Specifying a Default Rulebase ID

In a service-aware implementation with Diameter/DCCA (see the "Implementing Service-Aware Billing with Diameter/DCCA Support" section on page 8-12), rulebases contain the rules for defining categories of traffic; categories on which decisions such as whether to allow or disallow traffic, and how to measure traffic, are based. The GGSN maps Diameter rulebase IDs to Cisco CSG2 billing plans.

To configure a default rulebase ID to apply to PDP contexts using a particular charging profile, use the following command in charging profile configuration mode:

Command	Purpose
`Router(ch-prof-conf)# content rulebase id`	Defines a default rulebase ID to apply to PDP contexts using this charging profile.

Note The rulebase value presented in a RADIUS Access Accept message overrides the default rulebase ID configured in a charging profile. A rulebase ID received in a CCA initial message from a DCCA server overrides the rulebase ID received from the RADIUS server and the default rulebase ID configured in a charging profile.

For Gy:DCCA prepaid solution, the Rulebase ID cannot be received in a DCCA and the Rulebase ID does not apply to the standalone prepaid solution.

Specifying a DCCA Profile for Online Billing

When the primary PDP context is created, the charging profile is selected.

If you define a DCCA profile in the charging profile, online billing is indicated for that PDP. Therefore, regardless of whether or not a user is prepaid or postpaid, the GGSN contacts the DCCA server if the **content dcca profile** configuration is present.

Note This charging profile configuration requires that service-aware billing has been implemented with Diameter/DCCA (see "Implementing Service-Aware Billing with Diameter/DCCA Support" section on page 8-12.)

If the user is to be treated as a postpaid subscriber, the DCCA server returns a CAA with a result-code of CREDIT_CONTROL_NOT_APPLICABLE (4011) and the user is treated as a postpaid subscriber.

If a charging profile does not contain a DCCA profile configuration, users are treated as postpaid (offline billing).

To specify the DCCA client profile to communicate with a DCCA server, use the following command in charging profile configuration mode:

Command	Purpose
`Router(ch-prof-conf)# content dcca profile profile-name [weight max-weight]`	Specifies the profile to communicate with a DCCA server and optionally, assigns a weight to the charging profile for weighted round robin load balancing. A valid weight is a number from 1 to 255. The default is 1.

OCS Load Balancing

In earlier releases of the Cisco GGSN (before Release 10.0), each Cisco SAMI PPC ran a Cisco GGSN instance. The APNs of each GGSN instance were mapped to only one DCCA profile (OCS server), however, the same APN across the Cisco GGSN instances on the Cisco SAMI PPCs could be mapped to different DCCA profiles. Therefore, an APN on a Cisco SAMI hosting six GGSN instances could communicate with one or more OCSs.

With the transition to a Single IP architecture in Cisco GGSN Release 10.0 and later, the separate GGSN instances running on the six Cisco SAMI processors function as a single GGSN instance, therefore, an APN must be able to communicate with multiple DCCA servers.

For efficient OCS utilization, subscribers are load balanced among the OCSs using a weighted round-robin selection of DCCA profiles defined under the charging profile that is applied to an APN. This means that the next DCCA profile defined in a charging profile is used whenever a new primary PDP context uses the charging profile. If you associate a weight to a DCCA profile (using the **weight** keyword option), that profile is used for the corresponding weight before the next DCCA profile is used. The GGSN uses the same OCS/DCCA for the duration of the primary and all secondary PDPs.

Suppressing CDRs for Prepaid Subscribers

In a service-aware implementation with Diameter/DCCA (see "Implementing Service-Aware Billing with Diameter/DCCA Support" section on page 8-12), charging for prepaid subscribers is handled by the DCCA client; therefore, eG-CDRs do not need to be generated for prepaid subscribers.

To configure the GGSN to suppress eG-CDRs for users with an active connection to a DCCA server, use the following command in charging profile configuration mode:

Command	Purpose
`Router(ch-prof-conf)# cdr suppression prepaid`	Specifies that CDRs be suppressed for prepaid subscribers.

Note When G-CDRs suppression is enabled, if a Diameter server error occurs while a session is active, the user is reverted to postpaid status, but CDRs for the PDP context are not generated.

Configuring Trigger Conditions for Postpaid Subscribers

If a user is a prepaid subscriber not using an enhanced quota server interface, all the credit control is performed by the DCCA server. If the user is a postpaid subscriber not using an enhanced quota server interface, and service-aware billing is enabled, the default values configured in a charging profile define the conditions that control how often usages should be reported.

Note Triggers must be explicitly enabled for both prepaid and postpaid subscribers.

To define the trigger conditions in a charging profile for postpaid subscribers, use the following commands in charging profile configuration mode:

	Command	Purpose
Step 1	`Router(ch-prof-conf)# content postpaid {qos-change | sgsn-change | plmn-change | rat-change}`	Configures the condition that, when it occurs, causes the GGSN to request quota reauthorization for a PDP context. • **qos-change**—Quality of Service (QoS) change triggers a quota reauthorization request. • **sgsn-change**—SGSN change triggers a quota reauthorization request. • **plmn-change**—Public land mobile network (PLMN) change triggers a quota reauthorization request. • **rat-change**—Radio access technology (RAT) change triggers a quota reauthorization request. **Note** The **plmn-change** and **rat-change** keyword options require that the GGSN is configured to include the RAT and/or PLMN ID fields in the service-record IE in CDRs using the **gprs charging service record include** command. **Note** Explicitly enable triggers for both prepaid and postpaid subscribers.
Step 2	`Router(ch-prof-conf)# content postpaid time value`	Specifies the time duration limit, in seconds, that causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context when exceeded. The valid value is between 300 and 4294967295 seconds. The default is 1048576.
Step 1	`Router(ch-prof-conf)# content postpaid validity seconds`	Specifies the amount of time, in seconds, that quota granted for a postpaid subscriber is valid. The valid range is from 900 to 4294967295 seconds. The default is no validity timer is configured.
Step 2	`Router(ch-prof-conf)# content postpaid volume value`	Specifies the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR. The valid value is between 1 and 4294967295. The default is 1,048,576 bytes (1 MB).

Implementing Service-Aware Billing with OCS Address Selection Support

As an alternative to the GGSN with DCCA online charging solution, you can configure the GGSN to support OCS address selection. OCS address selection enables online credit control for prepaid subscribers to be provided by an external OCS to which the Cisco CSG2 has a direct GTP' interface. When you configure the GGSN to support OCS address selection, the GGSN functions as a quota server for postpaid subscribers only. The GGSN does not generate enhanced G-CDRs (eG-CDRs) for prepaid subscribers.

By default, the GGSN sends its IP address in Accounting-Start messages to the Cisco CSG2 (functioning as a RADIUS proxy) to establish itself as the quota server for postpaid and prepaid subscribers. When OCS address selection support is configured, if the IP address of an OCS is returned in the "csg:quota_server" attribute in an Access-Accept message from the AAA server, the GGSN forwards that address in the same attribute in an Accounting-Start message to the Cisco CSG2. This notifies the Cisco CSG2 to use the external OCS as the quota server for this PDP context. In a service-aware GGSN implementation using OCS address selection, the GGSN functions as the quota server for postpaid subscribers only.

Service-Aware Billing with OCS Address Selection Data Flows

The following is a high-level overview of the flow of traffic during the creation of a PDP context for a prepaid subscriber in an enhanced service-aware billing implementation using OCS address selection.

1. SGSN sends a Create PDP Context request to the service-aware GGSN.
2. GGSN sends an Access-Request message to the RADIUS endpoint (server or the Cisco CSG2 configured as a RADIUS proxy).
3. RADIUS endpoint determines if the user is prepaid, and if so, responds to the Access-Request message with an Access-Accept message that includes the "csg:quota_server" attribute containing the IP address and port of an external OCS.

4. If the APN is configured as service-aware, and the GGSN is configured to generate eG-CDRs, the GGSN receives the Access-Accept from the RADIUS endpoint, and because the "csg_quota_server" attribute is present and includes the IP address of an OCS, the GGSN determines that the user is a prepaid subscriber, and returns an Accounting-Start request that includes the following attributes:
   - csg:billing_plan
   - csg:quota_server attribute—The "csg:quota_server" attribute contains the OCS IP address and port to the Cisco CSG2. If it does not, the GGSN forwards its own IP address in the "csg:quota_server" field.)
   - csg:eggsn_qs—IP address and port number of the enhanced quota server interface.
   - csg:eggsn_qs_mode—Indicates whether the enhanced quota server interface is enabled to exchange service control messages with the CSG2.
5. Upon receiving the Accounting-Start Request, the RADIUS endpoint performs the following:
   a. Creates a Cisco CSG2 User Table entry.
   b. Identifies that the GGSN generates the eG-CDRs, and disables service level CDR generation for the user.
   c. Identifies that the user is a prepaid user based on the billing plan received.
   d. Enables the quota server message exchange with the specified OCS address.
   e. Enables service control message exchange with the GGSN.
   f. Sends an Accounting-Start Response to the GGSN.
6. GGSN sends a Create PDP Context response to the SGSN, and the context is established.
7. When trigger conditions occur, Service Control Requests (SCRs) and Service Control Usage (SCU) messages are exchanged between the GGSN and CSG2 to add service containers to eG-CDRs, or close eG-CDRs.
8. GGSN generates eG-CDRs and sends them to the charging gateway.

Note When an external OCS is used as the quota server for prepaid subscribers, the GGSN receives service-level usage reports from the Cisco CSG2 for postpaid subscribers and generates eG-CDRs accordingly. The GGSN does not generate eG-CDRs for prepaid subscribers unless an enhanced quota interface has been configured as described in "Configuring the Quota Server Interface on the GGSN" section on page 8-7.

OCS address selection support on the GGSN requires that the following conditions are met:

- Support for service-aware billing is enabled globally and at the APN level (see the "Enabling Support for Service-Aware Billing" section on page 8-3).
- Wait accounting is enabled (using the "Configuring Wait Accounting" section on page 8-4).
- GGSN is configured to communicate with the Cisco CSG2 (see the "Configuring Quota Server Support on the Cisco GGSN" section on page 8-5).
- The GGSN is configured to generate eG-CDRs (see the "Configuring the GGSN to Generate Enhanced G-CDRs" section on page 8-4).
- The correct configuration exists on the AAA server.

To enable OCS address selection support on the GGSN, use the following command in global configuration mode:

	Command	Purpose
Step 1	`Router(conf)# gprs radius attribute quota-server ocs-address`	Configures the GGSN to send the OCS IP address received in an Access-Accept response from a RADIUS server in the csg:quota server attribute in Accounting-Start messages to the Cisco CSG2.

Enabling PCC under an APN

The Gx interface is a reference point between the Policy and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF). It is used for provisioning and removal of Policy and Charging Control (PCC) files from PCRF to PCEF.

When a Create PDP Context request is received from an SGSN on a PCC-enabled APN:

1. After authentication, the GGSN sends an Accounting Start messages to the CSG2 that contains the following Cisco AVPs (in addition to the other standard 3GPP attributes):
   - pcc_enabled—Indicates whether a subscriber is a Gx user. If enabled, the CSG2 marks the subscriber as a Gx user and communicates with the PCRF for this subscribers session. (If not enabled, the CSG2 marks the subscriber as a non-Gx subscriber and does not communicate with the PCRF.)
   - coa_flags—Indicates whether the GGSN supports Gx updates via RADIUS CoA messaging. If enabled, the GGSN supports Gx updates via RADIUS CoA messaging. (If not enabled, indicates MS-initiated QoS updates.)
2. If the GGSN is configured to generate eG-CDRs, in the Accounting Start message, the GGSN includes the following additional attributes:
   - csg:eggsn_qs—IP address and port number of the enhanced quota server interface.
   - csg:eggsn_qs_mode—Indicates whether the enhanced quota server interface is enabled to exchange service control messages with the CSG2.
3. Upon receiving the Accounting-Start Request, the CSG2 performs the following:
   a. Creates a Cisco CSG2 User Table entry.
   b. Identifies that it is a Gx user based on the attributes received.
   c. Identifies that GGSN generates the eG-CDRs, and disables service level CDR generation for the user.
   d. Enables the exchange of service control messages with the enhanced quota server interface defined in the “csg:eggsn_qs” attribute in the Accounting Start message.
4. The CSG2 communicates with the PCRF to provision charging rules and the authorized QoS attributes.
5. The CSG2 sends a CoA request to the GGSN that notifies the GGSN of the authorization status and authorized QoS attributes, and sends an Accounting Start response to the GGSN.
6. The Cisco GGSN receives the CoA request, and based on the authorization status, sends the Create PDP Context response to the SGSN and the PDP context is created.

7. When trigger conditions occur, Service Control Requests (SCRs) and Service Control Usage (SCU) messages are exchanged between the GGSN and CSG2 to add service containers to eG-CDRs, and/or close eG-CDRs.
8. The GGSN generates eG-CDRs and sends them to the charging gateway.

Note If an APN is PCC-enabled, configure the GGSN to wait for a RADIUS accounting start response before sending a Create PDP Context response to the SGSN. For information about configuring wait accounting, see the "Configuring Wait Accounting" section on page 8-4.

To configure an APN as a PCC-enabled APN, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# pcc`	Configures the APN as a PCC-enabled APN.

Configuring Standalone GGSN Prepaid Quota Enforcement

You can implement prepaid quota enforcement using a service-aware GGSN, the Cisco GGSN and Cisco CSG2 implemented together to provide enhanced billing services, or you can implement prepaid quota enforcement using a Cisco GGSN operating in standalone mode.

When you implement the prepaid feature using a Cisco GGSN operating in standalone mode, the GGSN monitors data packets on volume basis, time basis, or both, for each prepaid subscriber. If you have configured the GGSN for both volume and time quota, the GGSN inspects both usages, and requests additional quota as soon as either usage meets its threshold or expires.

When configuring standalone GGSN prepaid quota enforcement:

- Support for service-aware billing must be enabled on the GGSN using the **gprs service-aware** command.
- The measurement of time starts as soon as the session is established.
- The GGSN monitors on a per-user basis, not on a per-service basis.
- In a redundant configuration, the active GGSN synchronizes quota allocated information with the standby GGSN when event triggers occur, such as at the time of each quota grant. Periodic synchronization of quota usage information is not performed. To ensure a user is not overcharged, the standby and active GGSNs maintain synchronization of the CC-Request-Number along with each quota grant.
- The GGSN monitors quota on a per-user basis, therefore, when the standalone GGSN requests quota, only one service is expected in the Multiple-Service-Credit-Control [MSCC] AVP. If the CCA contains multiple services, or no service in the MSCC AVP, the CCA is considered an invalid answer, and the CCFH determines the action.
- Only single service is supported. If multiple services are configured, the CCFH determines whether the GGSN rejects the PDP or converts it to postpaid.
- With a dual quota, the Quota Holding Timer (QHT) starts after the Quota Consumption Timer (QCT). Even though the QCT does not apply to volume quota, this behavior is due to time quota. With time quota, the QHT starts after the quota consumption ceases, which occurs after the QCT.
- If a DCCA profile is not configured under the charging profile, the PDP is rejected.

- Once a PDP is converted to postpaid, enhanced G-CDRs are no longer generated, only G-CDRs.
- In a redundant configuration, all timers (QHT, QCT, time threshold, etc.) except for the Quota Validity Timer (QVT) are restarted once the standby GGSN becomes active. The QVT timestamp is synchronized, and when a standby GGSN becomes active, the newly active GGSN waits for the remaining time to elapse instead of restarting the timer.

To configure the GGSN to perform quota enforcement for prepaid subscribers in standalone mode, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs prepaid stand-alone`	Configures the GGSN to perform prepaid quota enforcement in standalone mode.

To configure the maximum limit on the volume/time quota threshold in terms of percentage of the volume/time quota received, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs prepaid quota threshold` *percentage*	Sets the maximum limit on the volume/time quota threshold, as a percentage of the volume/time quota grant received from the DCCA server on the threshold received. The valid value is 0 to 100 percent. The default is 80.

When you configure the prepaid quota threshold, the threshold value used on the GGSN is the lower value between the:

- Threshold value, in percentage, received in a CCA
- Configured percentage of the quota grant

To monitor standalone quota enforcement, use the following commands in privileged EXEC mode:

Command	Purpose
`Router# clear gprs prepaid quota sanity`	Clears sanity statistics of the GPRS quota grant parameters.
`Router# clear gprs prepaid statistics`	Clears GGSN quota-manager statistics.
`Router# show gprs prepaid quota sanity`	Displays sanity statistics of the GPRS quota grant parameters.
`Router# show gprs prepaid statistics`	Displays GGSN quota-manager statistics.

Configuring the Charging Record Type under an APN

With Cisco GGSN Release 9.2, and later, you can configure the charging record type for an APN. This command is supported when one of the following conditions exists:

- You have configured the APN to be service-aware (see the "Enabling Support for Service-Aware Billing" section on page 8-3) or PCC-enabled (see the "Enabling PCC under an APN" section on page 8-31).
- You have configured the quota server interface to support the exchange service control messages (see the "Configuring the Quota Server Interface on the GGSN" section on page 8-7).
- You have configured GPRS Charging Release 7 (see the "Configuring the Charging Release" section on page 7-8).

To configure the charging record type for an APN, use the following command in access-point configuration mode:

Command	Purpose
`Router(access-point-config)# charging record type [gcdr | egcdr | none]`	Configures the charging record type for an APN, where: • **gcdr**—G-CDRs are generated. • **egcdr**—eG-CDRs are generated. • **none**—No records are generated. By default, G-CDR generation is enabled, however, it can be disabled by using the **cdr suppression** command in access-point configuration mode.

You can configure the charging record type in the following modes:

- Global configuration
- Charging profile configuration
- Access-point configuration

When configuring the charging record type at the APN level, note that the charging profile configuration overrides the global configuration, and the APN level configuration overrides the charging profile configuration.

For example, you can enable eG-CDR generation globally by using the **gprs charging cdr-option service-record** command, and then configure the **charging record type gcdr** command under an APN to restrict the user of that APN to generate G-CDRs. The remaining service aware users generates eG-CDRs.

If the charging record type command is not configured at the APN level, the default behavior is based on the existing eG-CDR generation global configuration set by using the **gprs charging cdr-option service-record** command.

GTP-Session Redundancy for Service-Aware PDPs Overview

GTP-Session Redundancy (GTP-SR) ensures that when an active GGSN fails, a standby GGSN has all the necessary information about a PDP context to continue service without interruption. In an enhanced service-aware billing environment, this means service-related information must also be synchronized from the active to standby service-aware GGSN. Therefore, with GGSN Release 5.2 and later, service-aware data necessary to establish charging for service-aware PDP sessions is synchronized with the standby GGSN.

The service-aware data synchronized with the standby GGSN includes the following:

- Per-PDP context services—Rulebase ID and DCCA failure handling settings (CCSF and CCSH AVPs).
- Per-category information—Category ID, Cisco CSG2 session, and category state and event triggers. Many category states are intermediate states; therefore, they are not synchronized to the standby service-aware GGSN. The following category states are synchronized: “blacklist,” “idle,” and “authorized.”

  All event triggers are recorded. At the end of the processing of an event on the active GGSN, the clearing of the event’s trigger is synchronized to the standby GGSN. If a switchover occurs, if an event trigger is found present on a category, the newly active GGSN re-initiates the event.
- Path states—The quota server process on the active GGSN synchronizes the state of the path to a Cisco CSG2 to the quota server process on the standby GGSN. The path echo timer on the standby quota server is not started unless the standby quota server becomes active. Path sequence numbers are not synchronized. After a switchover occurs, the newly active quota server starts from 0.

Note Category usage data is not synchronized from an active GGSN to the standby GGSN. This prevents over-reporting of usage if a switchover occurs.

GTP-SR for Service-Aware PDP Sessions Guidelines

In addition to the prerequisites listed in Chapter 6, “Configuring GGSN GTP Session Redundancy,” to achieve session redundancy for service-aware PDP sessions, ensure that the following configurations exist on the redundantly configured service-aware GGSN:

- GTP-SR is enabled on the GGSN using the **gprs redundancy** command in global configuration mode. Also, if the GGSN is functioning as a Diameter node, ensure that it is enabled to track session states by using the **diameter redundancy** command in global configuration mode. See the “Configuring the Diameter Base” section on page 8-16 for information on configuring Diameter redundancy.
- The quota server process is configured the same on both the active GGSN and the standby GGSN. Specifically, on each active/standby pair, the quota server address is the same. To ensure that the Cisco CSG2 only talks to the active quota server process, configure it to always route messages for the quota server through the virtual HSRP address for the Gi interface. In reverse, the virtual Cisco CSG2 address is used by the GGSN to deliver messages to the active Cisco CSG2 of a redundant pair. See the “Configuring a Cisco CSG2 Server Group” section on page 8-6 for more information about configuring a virtual Cisco CSG2 address.
- If using Diameter, configure a DCCA client source address on both the active GGSN and the standby GGSN. The DCCA client source address is the local address used in the TCP connection to the DCCA server. We recommend that you use a logical interface that is routable via a virtual HRSP address between the active GGSN and the standby GGSN.

For information on configuring Cisco IOS HRSP, see *Configuring the Hot Standby Router Protocol* section of the *Cisco IOS IP Configuration Guide, Release 12.3*. For detailed information on GTP-SR, see Chapter 6, "Configuring GGSN GTP Session Redundancy."

For information about fault-tolerance on the Cisco CSG2, see *Cisco Content Services Gateway - 2nd Generation Release 3.5 Installation and Configuration Guide*.

Configuring Per-Service Local Sequence Number Synchronization

The charging gateway uses the per service local sequence number to detect duplicate service containers associated with a PDP context.

To minimize the amount of data being synchronized to the standby GGSN, the per service local sequence number is not synchronized each time an eG-CDR is closed. Instead, the current value of the local sequence number and the local sequence number last synchronized for a PDP context is checked, and if the difference is more than the configured window size, the current local sequence number is synchronized with the standby GGSN. When a standby GGSN becomes the active GGSN, it starts from the last value synchronized, plus the window size.

To configure the window size that determines when the per service local sequence number is synchronized with the standby GGSN, use the following command in global configuration mode:

Command	Purpose
`Router# gprs redundancy charging sync-window svc-seqnum` *size*	Configures the window size that determines when the per service local sequence number is synchronized with the standby GGSN. The valid value is a number between 1 and 200. The default is 50.

Configuring Activity-Based Time Billing for Prepaid Subscribers

Cisco GGSN Release 10.0 supports activity-based time billing is an enhancement to the standard duration-based billing.

Activity-based billing, as defined by 3GPP standards, bills subscribers for only the time they are active on the network instead of the entire time they are logged on to the network. This feature enables you to eliminate charging for periods of inactivity between packets.

To support activity-based time billing, in an eGGSN implementation, the Cisco GGSN receives the quota consumption time (QCT) AVP and the quota holding time (QHT) AVP in the CCA for each of the services (i.e. MSCC) from the OCS. In a Service Authorization Response, a Service Reauthorization Response, or a Quota Push message, the Cisco GGSN forwards the QCT and QHT values to the Cisco CSG2.

Note The QCT and QHT values sent from the OCS, and forwarded to the Cisco CSG2 by the Cisco GGSN, take precedence over the values configured on the Cisco CSG2. If the GGSN does not receive the QCT or QHT AVP from the OCS, the Cisco CSG2 uses locally configured QCT and QHT values.

The QCT is the maximum time a user can be charged during periods of inactivity. The QHT corresponds to the service idle timeout configured on the Cisco CSG2. The Cisco GGSN quota server QHT overrides the service idle timeout configured on the Cisco CSG2, as well as any prior quota server QHTs.

For information about activity-based time billing on the Cisco CSG2, see *Cisco Content Services Gateway - 2nd Generation Release 4 Installation and Configuration Guide, Cisco IOS Release 12.4(24)MD*.

There are no new or modified Cisco GGSN commands for Activity-Based Time Billing support.

Configuring HTTP Redirection

The Cisco GGSN supports Final Unit Indication (FUI) HTTP redirection and termination (introduced in Cisco IOS Release 12.4(24)YE) and RADIUS controlled HTTP redirection (introduced in Cisco IOS Release 12.4(24)YE3). Both methods of redirection can be configured under an APN at the same time.

This section contains information on the following:

- Configuring FUI-Based HTTP Redirection, page 8-37
- Configuring RADIUS Controlled HTTP Redirection, page 8-40

Configuring FUI-Based HTTP Redirection

With Cisco GGSN Release 10.0, Cisco IOS 12.4(24) YE and later, an OCS can ask the GGSN to take final action when the account of a subscriber no longer has an adequate number of credits, and the last packet cannot go through because the quota has been exhausted. When this condition occurs, the OCS sends a Final Unit Indication (FUI) attribute value pair (AVP) in a CCA.

The OCS sends the FUI AVP in a CCA at the service (Multiple-Service-Credit-Control[MSCC]) level. The FUI sent by the OCS contains a grant of quota that represents the final units of quota for a service, and contains an action that the GGSN must take once the subscriber to that service uses the final units of quota.

Note The Cisco GGSN supports the FUI in Standalone Mode as well as in an eGGSN implementation. In an eGGSN implementation, the Cisco GGSN uses the Cisco CSG2 as an enforcement point to implement the FUI action. The Cisco GGSN sends the FUI TLV in a Service Authorization Responses or Quota Push Messages to the Cisco CSG2 to communicate the action for the Cisco CSG2 to take.

The possible FUI actions supported by the Cisco GGSN are TERMINATE or REDIRECT final actions.

FUI REDIRECT

Note FUI redirect filters are applied to all uplink and downlink traffic. The filter names can come from the OCS, or you can configure FUI filters under an APN using the **redirect http rule** command in access-point configuration mode.

- If the CCA does not contain a redirect server address, the Cisco GGSN ignores the message and allows service to continue.
- If the CCA contains a redirect server address and granted service units (GSU) with final units for the service, the Cisco GGSN performs the following actions, depending on whether it is operating in standalone mode or in an eGGSN implementation:
  - In standalone mode, after the final units of quota are consumed, the Cisco GGSN returns the quota to the OCS, indicating that the redirect action has started and the subscriber should be redirected to the redirect server. (The OCS provided redirection takes precedence over any existing redirect configuration.) Downlink packets that are allowed by weight 0 filter continue to flow to the subscriber. Once the subscriber replenishes their account, the OCS allows the subscriber to continue the service by reauthorizing the service. After a successful reauthorization, the original uplink user plane is restored. If the subscriber does not replenish the account with more quota, the service is terminated after the validity time.
  - In an eGGSN implementation, in response to a service authorization request, the FUI is sent to the Cisco CSG2 with the redirection action set. After the final units of quota are consumed, the Cisco CSG2 returns the quota to the GGSN (GGSN returns to OCS) indicating that the redirect action has started, and redirect the subscriber to the redirect server. If the subscriber does not replenish the account with more quota, the service might be terminated by indication from the OCS (CCA after the validity time).
  - In an eGGSN implementation, the Cisco GGSN sends the GSU, FUI with redirection action set, and a redirect server address to the Cisco CSG2. When the final quota is spent, the Cisco CSG2 returns the quota to the GGSN (GGSN returns to the OCS) indicating the service is being redirected. If the subscriber does not replenish their account with more quota, the service might be terminated by the OCS (CCA after the validity time).

    Note If the GGSN does not provide a dynamic URL, the Cisco CSG2 uses the redirect URL configured on the **ip csg redirect** command in global configuration mode.

    For more information about the **ip csg redirect** command, see *Cisco Content Services Gateway - 2nd Generation Release 4 Installation and Configuration Guide, Cisco IOS Release 12.4(24)MD*.
- If a CCA does not contain GSU, in both standalone mode and in an eGGSN implementation, the service is immediately redirected, and after redirection, if the subscriber does not replenish the account in a timely manner, the PDP is terminated.

FUI-Action TERMINATE

- If the group AVP in the CCA has any other AVP in it, such as a Redirect-Server_address, the Cisco GGSN terminates the category as follows:
  - In standalone mode, once the final units for the service are consumed, the Cisco GGSN sends the CCR(final) to the OCS and the PDP context is deleted.
  - In an eGGSN implementation, in response to a service authorization request, the FUI TLV is sent to the Cisco CSG2 with the termination action set. Once the final units for the service are consumed, the Cisco CSG2 sends a Service STOP to the Cisco GGSN, and the Cisco GGSN sends a CCR(update) or CCR(final) and terminates the service. If it is the last service, the PDP context is deleted.
- If the CCA also contains the GSU AVP with final units for the service, the following actions occur:
  - In standalone mode, the Cisco GGSN sends the CCR(final) to the OCS and the PDP context is deleted after the final units are consumed.
  - In an eGGSN implementation, the Cisco GGSN sends a CCR(update) or CCR(final) and terminates the service. If it is the final service, the PDP context is deleted.

Note In an eGGSN implementation, if the OCS sends both the FUI-action REDIRECT and FUI-action RESTRICT in the same CCA, the GGSN forwards both actions and their associated TLVs to the Cisco CSG2. When both are received, the Cisco CSG2 ignores the FUI-action RESTRICT and processes the FUI-action REDIRECT.

Configuring a Default FUI Redirection Rule and Local Filters

Note The Cisco GGSN supports the FUI redirection filter configuration when in standalone prepaid mode.

The OCS should return Filter IDs in the FUI group TLV. If the OCS server does not include the Filter IDs in the FUI TLV, the Cisco GGSN FUI-based HTTP redirection configures the GGSN to look for a preconfigured ACL for the FUI REDIRECT action. If an APN does not have a redirect filter defined, and the OCS server does not include a filter ID, all packets are dropped and redirection does not occur.

To configure a rule and FUI filter to apply under an APN if a filter ID is not received in the FUI TLV from the OCS, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# redirect http rule` *acl-number* [**filter-id** *acl-number-in acl-number-out*]	Configures a default FUI rule under an APN if a filter ID is not received in the FUL TLV from the OCS. Optionally, specify the **filter-id** keyword option to apply an FUI redirection filter to a packet before it is dropped to verify if the packet is TCP, and if so, initiate HTTP redirection.

Example 1

In the following Filter ID/ACL configuration example, the redirect server cluster is allowed 172.168.0.1 - 172.168.0.6 for both uplink and downlink traffic.

```
ip access-list extended redirect-example-out
  permit tcp any 172.168.0.1 0.0.0.248 eq www
  permit icmp any any
  permit udp any any eq domain

ip access-list extended redirect-example-in
  permit tcp 172.168.0.1 0.0.0.248 any eq www
  permit icmp any any
  permit udp any any eq domain
```

Example 2

The following ACL is used when a packet is about to be dropped to verify if the packet is TCP. If it is TCP ACK, the GGSN initiates an HTTP redirection from the GGSN.

```
access-list 100 permit tcp any any eq www
```

Example 3: Configuring a Default FUI Filter at an APN

The following example applies a FUI-based redirect HTTP filter to an APN:

```
GGSN(config-access-point)# redirect http rule 100 filter-id redirect-example-in
redirect-example-out
```

Configuring RADIUS Controlled HTTP Redirection

With Cisco GGSN Release 10.1, Cisco IOS Release 12.4(24)YE3 and later, the RADIUS Controlled HTTP Redirection feature enables the Cisco GGSN to redirect the HTTP traffic of subscribers to an Advice-of-Charge (AoC) page that notifies them of new tariff changes when they are roaming in a foreign PLMN.

Cisco GGSN Release 10.1 supports the following new AVPs in RADIUS Access-Accept messages to implement the RADIUS Controlled Redirection feature:

- Address-Type (IP or URL)
- Redirect-Address (IP or URL)
- Filter-ID (preventing access for both downlink (DL) and uplink (UL) traffic to other L3/L4 destinations)
- Redirect-Time (the time after which the redirection or filter-ids are removed)

During the create PDP context request process, AAA sends, at minimum, the mandatory attributes (Address-Type and the Redirect-Address) to the GGSN in an Access-Accept message. When the Cisco GGSN receives these attributes, it applies the RADIUS controlled redirection attributes and sends a create PDP response to the SGSN.

Note The Cisco GGSN downloads five attributes from AAA. These attributes include the two mandatory attributes (Address-type and Redirect-Address). The other attributes (DL and UL Filter-IDs and Redirect-Time) are optional from AAA. If these options are not downoaded from AAA, an operator must configure them under the APN for RADIUS Controlled HTTP Redirection to work.

Note In an eGGSN implementation, the wait accounting feature must be enabled using the **gprs gtp response-message wait-accounting** global configuration command.

With RADIUS-controlled HTTP redirection, note the following:

- If DL/UL filters or values for the redirect interval are not downloaded from AAA, then the values configured under APN using the **redirect radius-controlled** command are used. Also, the **redirect radius-controlled rule** *acl-number* command configures the ACL to use when a packet is about to be dropped, to verify if the packet is TCP, and if TCP ACK, to punt the packet to the process path and initiated an HTTP redirect packet from the GGSN.

  Note The **redirect radius-controlled rule** *acl-number* command is mandatory, regardless of whether the RADIUS Controlled Redirection attributes are downloaded from AAA or are configured locally.

- If the redirect server type and redirect server address are not found in the Access-Accept message from AAA, the GGSN processes the create PDP context request as a normal subscriber who does not need RADIUS controlled HTTP redirection.
- The RADIUS configuration takes precedence over the APN configuration.
- If a redirect interval (Redirect-Time AVP) is not found in the Access-Accept message or a value is not configured locally, the Cisco GGSN uses a default interval of 60 seconds.
- Both FUI-based and RADIUS-controlled redirection can exist at the same time under an APN.

Configuring a Default RADIUS Controlled Redirection Rule and Local Filters

The Cisco GGSN should receive two Filter-IDs from AAA and a Redirect-Time in an Access-Accept message. If the Access-Accept message does not include the filter-ids and redirect time, the GGSN uses values that are configured locally.

Note Values received from AAA take precedence over the locally configured values.

To configure a default RADIUS controlled redirection rule, and local filter IDs and a redirect time, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# redirect radius-controlled rule` *acl-number* `[filter-id` *acl-number-in acl-number-out*`] [interval` *seconds*`]`	Configures a default RADIUS-controlled rule under APN, where the required *acl-number* variable is the number of the access control list (ACL) to apply. Optionally, • Specify the **filter-id** keyword option to specify the filter to apply to a packet to check the weight of traffic destined for the redirect server IP or URL. • Specify the **interval** keyword option to specify, in seconds, the time after which the redirection or filter-ids are removed. The default value is 60.

Note The bare minimum configuration to enable RADIUS-Controlled HTTP Redirection is **redirect radius-controlled rule** *acl-rule*. This configuration will define an ACL rule and a default interval of 60 seconds.

Example 1

In the following Filter ID/ACL configuration example, the redirect server cluster is allowed 172.168.0.1 - 172.168.0.6 for uplink TCP traffic and permit any TCP traffic for downstream:

```
ip access-list extended redirect-example-out
        permit tcp any 172.168.0.1 0.0.0.248 eq www
        permit icmp any any
        permit udp any any eq domain
ip access-list extended redirect-example-in
        permit tcp any any
        permit icmp any any
        permit udp any any eq domain
```

Example 2

The following ACL is used when a packet is about to be dropped to verify if the packet is TCP. If it is TCP ACK, the GGSN initiates an HTTP redirection from the GGSN.

```
access-list 100 permit tcp any any eq www
```

Note The **access-list** command is mandatory, regardless of whether RADIUS controlled redirection attributes are downloaded from AAA or configured locally.

Example 3

The following example applies a RADIUS controlled redirect HTTP filter to an APN:

```
GGSN(config-access-point)# redirect radius-controlled rule 100 filter-id
redirect-example-in redirect-example-out interval 30
```

Verifying the RADIUS Redirection Information

To view the RADIUS controlled redirection related information, use the **show gprs gtp pdp-context** command and specify the **tid** keyword option. The RADIUS controlled redirection information appears in bold.

```
GGSN_Active#show gprs gtp pdp-context tid 2222222222000010
TID MS Addr Source SGSN Addr APN
2222222222000010 172.2.3.4 Static 1.0.0.1 csg.cisco.com

current time :Nov 29 2010 17:57:37
user_name (IMSI): 222222222200000 MS address: 172.2.3.4
MS International PSTN/ISDN Number (MSISDN): 44444444444
sgsn_addr_signal: 1.0.0.1 sgsn_addr_data: 1.0.0.1
control teid local: 0x02100003
control teid remote: 0x10001441
data teid local: 0x02100004
data teid remote: 0x10001442
primary pdp: Y nsapi: 1
signal_sequence: 0 seq_tpdu_up: 9
seq_tpdu_down: 10
upstream_signal_flow: 0 upstream_data_flow: 0
downstream_signal_flow: 0 downstream_data_flow: 0
RAupdate_flow: 0
pdp_create_time: Nov 29 2010 17:55:28
last_access_time: Nov 29 2010 17:57:17
mnrgflag: 0 tos mask map: B8
session timeout: 0
idle timeout: 580

Radius redirection info
----------------------
Radius redirect server: 70.0.0.48
Radius IN filter-id : inacl
Radius OUT filter-id : outacl
Redirection Interval:00:05:00 (300)
Remaining Interval: 169

umts qos_req: 0911012901010111050101
umts qos_neg: 0911012901010111050101
QoS class: conversational
rcv_pkt_count: 10 rcv_byte_count: 1000
send_pkt_count: 10 send_byte_count: 1000
cef_up_pkt: 5 cef_up_byte: 500
cef_down_pkt: 5 cef_down_byte: 500
cef_drop: 0 out-sequence pkt: 0
charging_id: 46514448
visitor: No roamer: Unknown
charging characteristics: 1
charging characteristics received: 0
pdp reference count: 1
primary dns: 0.0.0.0
secondary dns: 0.0.0.0
primary nbns: 0.0.0.0
```

Configuring Cisco CSG2 Load Balancing

With Cisco GGSN Release 10.0 and later, in a service-aware GGSN implementation, the Single IP Cisco GGSN quota server interface can communicate with multiple Cisco CSGs.

To efficiently utilize the Cisco CSGs, subscribers are load balanced among the Cisco CSG2s, and once a Cisco CSG2 has been selected for a particular subscriber, all interfaces communicate with that Cisco CSG2.

Support for Cisco CSG2 load balancing involves the following:

- Support for the configuration of multiple Cisco CSG2 groups per APN.
- Selection of a Cisco CSG2 via dynamic subnet mapping or static subnet mapping.

Note To enable downlink traffic to reach the correct Cisco CSG2, routes need to be present on the supervisor either through static routes or dynamic routes advertised by a Cisco CSG2 via OSPF.

Note The Cisco GGSN gives priority to static mapping configurations over dynamic subnet creation.

Configuring Dynamic Cisco CSG2 Load Balancing

With dynamic load balancing, the subscriber-to-Cisco CSG2 mapping is dynamically determined during the create PDP context process.

The Cisco CSG2 selection is based on the IP address allocated to the subscriber, and the subnet formed by the Cisco GGSN subnet manager under the APN. Once a Cisco CSG2 has been chosen for a subscriber, the same Cisco CSG2 is chosen for the same subnet for different TCOPs and Cisco GGSNs in the same administrative domain.

Note Before configuring a Cisco CSG2 group, ensure that a RADIUS interface for accounting services has been configured for the CSG group using the **aaa-group accounting** command in CSG group configuration mode (see Configuring a Cisco CSG2 Server Group, page 8-6).

To configure a dynamic subnet-to-Cisco CSG2 group mapping, use the following commands in access-point configuration mode:

	Command	Purpose
Step 1	`Router(config-access-point)# aggregate 0.0.0.0 sub-mask`	Configures a default subnet mask for subnet management and enables dynamic subnet creation. **Note** The load balancer function selects a Cisco CSG2 based on the subnet.
Step 2	`Router(config-access-point)# csg-group csg-group-name`	Configures one or more Cisco Content Services Gateway - 2nd Generation (CSG2) group under the APN.

Note The **csg-group** access point configuration command and the **csg group** quota server configuration command are mutually exclusive. You cannot define a CSG group under an APN if one is already configured under the quota server interface.

Configuring Static Cisco CSG2 Mapping

Static load balancing supports an eGGSN implementation for which an external load balancing is being used for RADIUS and data traffic. In this configuration, operators can configure a static subnet-to-Cisco CSG2 mapping under the an APN.

To configure a static subnet-to-Cisco CSG2 group mapping, use the following commands in access-point configuration mode:

	Command	Purpose
Step 1	`Router(config-access-point)# csg-group csg-group-name`	Configures one or more Cisco Content Services Gateway - 2nd Generation (CSG2) group under the APN.
Step 2	`Router(config-access-point)# aggregate subnet-addr subnet-mask csg-group-name`	Configures a static subnet-to-Cisco CSG2 group mapping.

Note The **csg-group** access point configuration command and the **csg group** quota server configuration command are mutually exclusive. You cannot define a CSG group under an APN if one is already configured under the quota server interface.

Reviewing Trigger Conditions for Enhance Quota Server Interface Users

The Cisco GGSN generates eG-CDRs when the following types of trigger conditions occur when the Cisco CSG2 has a direct interface to an OCS, when a subscriber is a Gx user, or when a user is postpaid:

- PDP Context Modification, page 8-46
- Tariff Time Change, page 8-46
- Service Flow Reports, page 8-46
- eG-CDR Closure, page 8-47

Note The following trigger conditions do not require any special configuration on the GGSN. Volume and duration, and service flow triggers must be configured on the Cisco CSG2. For information about configuring the Cisco CSG2, see *Cisco Content Services Gateway 2nd Generation - Release 3.5 Installation and Configuration Guide.*

PDP Context Modification

When one of the following PDP context modification triggers occurs, the GGSN performs the following actions:

- RAT type, PLMN change, or MS time zone change
  - Adds a volume container followed by the list of service containers.
  - Closes the eG-CDR.
  - If a SVC record limit is reached, closes the eG-CDR, opens a partial CDR, and adds the remaining SVC records to the new eG-CDR.
- QoS change or user location change
  - Adds a volume container followed by a list of service containers.
  - If the maximum change condition limit is reached, closes the eG-CDR.
  - If a SVC record limit is reached, closes the eG-CDR, opens a partial CDR, and adds the remaining SVC records to the new eG-CDR.
- SGSN change
  - Adds a volume container followed by a list of service containers.
  - If the maximum SGSN limit is reached, closes the eG-CDR.
  - If the maximum change condition limit is reached, closes the eG-CDR.
  - If there an SVC record limit is reached, closes the eG-CDR, opens a partial CDR, and adds the remaining SVC records to the new eG-CDR.

Tariff Time Change

When a tariff time change occurs, the GGSN performs the following actions:

- Adds a volume container.
- If the maximum change limit is reached, closes the eG-CDR.
- For a prepaid GTP' user, the Cisco CSG2 might send a service usage message and the GGSN would then add it to the eG-CDR.

Service Flow Reports

When the following service flow trigger conditions occur, the GGSN generates service containers for each service:

- Time limit expiration
- Volume limit expiration
- Service flow termination

Volume and duration, and service flow triggers must be configured on the Cisco CSG2. For information about configuring volume and duration triggers, and service flow triggers on the Cisco CSG2, see *Cisco Content Services Gateway 2nd Generation - Release 3.5 Installation and Configuration Guide*.

Additionally, for prepaid GTP' users, the GGSN generates service containers for the following trigger conditions when the same triggers are configured on the Cisco CSG2:

- Time threshold reached
- Volume threshold reached
- Time quota exhausted
- Volume quota exhausted
- Service data flow termination or when service idles out

eG-CDR Closure

When the following eG-CDR closure trigger conditions occur, the GGSN adds the volume containers followed by service containers, except for when CDRs are manually cleared:

- End of PDP context
- Partial record reason
  - Data volume limit
  - Time limit
  - Maximum number of charging condition changes (QoS, tariff time, user-location-info change)
  - Management intervention
  - MS time zone change
  - Inter-PLMN SGSN change
  - RAT change

Configuration Examples

The following is an example of enhanced service-aware billing support configured on the GGSN.

```
Current configuration :3537 bytes
!
! Last configuration change at 15:26:45 UTC Fri Jan 7 2005
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service gprs ggsn
!
hostname sup-samiA
!
boot-start-marker
boot-end-marker
!
enable password abc
!
aaa new-model
!
!
!Configures the CSG2 RADIUS server group
!
aaa group server radius CSG-group
```

```
server 10.10.65.100 auth-port 1812 acct-port 1813
!
!Configures the Diameter server group
!
aaa group server diameter DCCA
server name DCCA
!
!
!Assigns AAA services to the CSG2 RADIUS and Diameter server groups
!
aaa authentication ppp CSG-list group CSG-group
aaa authorization prepaid DCCA group DCCA
aaa authorization network CSG-list group CSG
aaa accounting network CSG-list start-stop group CSG-group
aaa session-id common
ip subnet-zero
!
!
ip cef
!
!
...
!
!
gprs access-point-list gprs
!
...
!
!
!Enables service-aware billing on the GGSN
!
gprs service-aware
!
gprs access-point-list gprs
 access-point 10
  access-point-name cisco.com
  access-mode non-transparent
  aaa-group authentication CSG-list
  aaa-group accounting CSG-list
  gtp response-message wait-accounting
  charging profile any 1 override
  service-aware
  advertise downlink next-hop 10.10.150.2
  !
 access-point 20
  access-point-name yahoo.com
  access-mode non-transparent
  aaa-group authentication CSG
  aaa-group accounting CSG
  gtp response-message wait-accounting
  charging profile any 1 override
  service-aware
  !
 !
!
!Configures a DCCA client profile
!
gprs dcca profile 1
  ccfh continue
  authorization CSG-list
  destination-realm cisco.com
  trigger sgsn-change
  trigger qos-change
!
```

```
gprs charging profile 1
  limit volume 64000
  limit duration 64000
  content rulebase PREPAID
  content dcca profile 1
  content postpaid volume 64000
  content postpaid time 1200
  content postpaid qos-change
  content postpaid sgsn-change
!
!Congigures the quota server
!
ggsn quota-server qs
 interface Loopback2
 csg group csg_1
 !
!
!Configures a CSG2 group
!
ggsn csg-group csg_1
 virtual-address 10.10.65.10
 port 4386
 real-address 10.10.65.2
 !
tftp-server abcbar
!
radius-server host 10.10.65.100 auth-port 1812 acct-port 1813
radius-server host 10.20.154.201 auth-port 1812 acct-port 1813
radius-server key abc
radius-server vsa send accounting
radius-server vsa send accounting 3gpp2
!
!configures Diameter global parameters
!
diameter origin realm corporationA.com
diameter origin host sup-sami42.corporationA.com
diameter vendor supported cisco
!
!configures Diameter peer
!
diameter peer DCCA
 address ipv4 172.18.43.59
 transport tcp port 4100
 timer connection 20
 timer watchdog 25
 destination realm corporationA.com
!
!
...
!
end
```

CHAPTER 9

Configuring Network Access to the GGSN

This chapter describes how to configure access from the gateway GPRS support node (GGSN) to a serving GPRS support node (SGSN), public data network (PDN), and optionally to a Virtual Private Network (VPN). It also includes information about configuring access points on the GGSN.

For complete descriptions of the GGSN commands in this chapter, see *Cisco GGSN Command Reference* for the Cisco GGSN release you are using. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

This chapter includes the following sections:

- Configuring an Interface to the SGSN, page 9-1 (Required)
- Configuring a Route to the SGSN, page 9-4 (Required)
- Configuring Access Points on the GGSN, page 9-7 (Required)
- Configuring Access to External Support Servers, page 9-43 (Optional)
- Blocking Access to the GGSN by Foreign Mobile Stations, page 9-43 (Optional)
- Controlling Access to the GGSN by MSs with Duplicate IP Addresses, page 9-46 (Optional)
- Configuring Routing Behind the Mobile Station under an APN, page 9-47 (Optional)
- Configuring Proxy-CSCF Discovery Support under an APN, page 9-50(Optional)
- Monitoring and Maintaining Access Points on the GGSN, page 9-52
- Configuration Examples, page 9-52

Configuring an Interface to the SGSN

To establish access to an SGSN, you must configure an interface to the SGSN. In general packet radio service/Universal Mobile Telecommunication System (GPRS/UMTS), the interface between the GGSN and the SGSN is referred to as the *Gn interface*. The Cisco GGSN supports both a 2.5G and 3G Gn interface.

On the Cisco 7600 series router platform, the Gninterface is a logical one to a Layer-3 routed Gn VLAN configured on the supervisor engine. IEEE 802.1Q-encapsulation must be configured on the logical interface.

For more information about the Gn VLAN on the supervisor engine, see Platform Prerequisites, page 3-2. For more information about configuring interfaces, see *Cisco IOS Interface Configuration Guide* and the *Cisco IOS Interface Command Reference*.

To configure a subinterface to the Gn VLAN on the supervisor engine, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface gigabitethernet slot/port.subinterface-number`	Specifies the subinterface on which IEEE 802.1Q will be used.
Step 2	`Router(config-if)# encapsulation dot1q vlanid`	Defines the encapsulation format as IEEE 802.1Q (dot1q), and specifies the VLAN identifier.
Step 3	`Router(config-if)# ip address ip-address mask`	Sets a primary IP address for an interface.

Verifying the Interface Configuration to the SGSN

Step 1 To verify that you have properly configured a Gn VLAN on the supervisor engine, use the **show running-config** command. The following example is a portion of the output from the command showing the GigabitEthernet 8/22 physical interface configuration as the Gn interface to SGSN and the Gn VLAN configuration:

```
Sup# show running-config
Building configuration...

Current configuration :12672 bytes
!
version 12.x
...
interface GigabitEthernet8/22
 no ip address
 switchport
 switchport access vlan 302
!
interface Vlan101
 description Vlan to GGSN for GA/GN
 ip address 10.1.1.1 255.255.255.0
!
interface Vlan302
 ip address 40.0.2.1 255.255.255.0
```

Step 2 To verify that the physical interface and the Gn VLAN are available, use the **show interface** command on the supervisor engine. The following example shows that the GigabitEthernet8/22 physical interface to the SGSN is up, as is the Gn VLAN, VLAN 101.

```
Sup# show ip interface brief GigabitEthernet8/22
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet8/22        unassigned      YES unset  up                    up

Sup# show ip interface brief Vlan302
Interface                  IP-Address      OK? Method Status                Protocol
Vlan302                    40.0.2.1        YES TFTP   up                    up

Sup#
```

Step 3 To verify the Gn VLAN configuration and availability, use the **show vlan name** command on the supervisor engine. The following example shows the Gn VLAN Gn_1:

```
Sup# show vlan name Gn_1

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
302  Gn_1                             active    Gi4/1, Gi4/2, Gi4/3, Gi7/1
                                                Gi7/2, Gi7/3, Fa8/22, Fa8/26

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
302  enet  100302     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Step 4 On the GGSN, to verify that you have properly configured a Gn subinterface to the Gn VLAN, use the **show running-config** command. The following example is a portion of the output from the command showing a Gigabit Ethernet 0/0.2 physical interface configuration as the Gn interface to the charging gateway:

```
GGSN# show running-config
Building configuration...

Current configuration :7390 bytes
!
! Last configuration change at 16:56:05 UTC Wed Jun 25 2003
! NVRAM config last updated at 23:40:27 UTC Fri Jun 13 2003
!
version 12.3
.....
interface GigabitEthernet0/0.2
 description Ga/Gn Interface
 encapsulation dot1Q 101
 ip address 10.1.1.72 255.255.255.0
 no cdp enable
!
.....
ip route 40.1.2.1 255.255.255.255 10.1.1.1
```

Step 5 To verify that the subinterface is available, use the **show ip interface brief** command. The following example shows that the Gigabit Ethernet 0/0.2 subinterface to the Gn VLAN is in “up” status and that the protocol is also “up”:

```
GGSN# show ip interface brief GigabitEthernet0/0.2
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0.2       10.1.1.72       YES NVRAM  up                    up
```

Configuring a Route to the SGSN

To communicate with the SGSN, you can use static routes or a routing protocol, such as Open Shortest Path First (OSPF).

Note For the SGSN to communicate successfully with the GGSN, the SGSN must also configure a static route, or be able to dynamically route to the IP address of the GGSN *virtual template,* not the IP address of a GGSN interface.

The following sections provide some basic commands that you can use to configure a static route or enable OSPF routing on the GGSN. For more information about configuring IP routes, see *Cisco IOS IP Configuration Guide* and *Cisco IOS IP Command References*.

The following topics are included in this section:

- Configuring a Static Route to the SGSN, page 9-4
- Configuring OSPF, page 9-5
- Verifying the Route to the SGSN, page 9-5

Configuring a Static Route to the SGSN

A static route establishes a fixed route to the SGSN that is stored in the routing table. If you are not implementing a routing protocol, such as OSPF, then you can configure a static route to the SGSN, to establish the path between network devices.

To configure a static route from an interface to the SGSN, use the following commands, beginning in global configuration mode:

Command	Purpose
`Router(config)# ip route prefix mask {ip-address | interface-type interface-number} [distance] [tag tag] [permanent]`	Configures a static IP route, where: • *prefix*—Specifies the IP route prefix for the destination. (This is the IP address of the SGSN.) • *mask*—Specifies the prefix mask for the destination. (This is the subnet mask of the SGSN network.) • *ip-address*—Specifies the IP address of the next hop that can be used to reach the destination network. • *interface-type interface-number*—Specifies the network interface type and interface number that can be used to reach the destination network. (This is an interface on the GGSN for the Gn interface.) • *distance*—Specifies an administrative distance for the route. • **tag** *tag*—Specifies a tag value that can be used as a "match" value for controlling redistribution via route maps. • **permanent**—Specifies that the route will not be removed, even if the interface shuts down.

Configuring OSPF

As with other routing protocols, enabling OSPF requires that you create an OSPF routing process, specify the range of IP addresses to be associated with the routing process, and assign area IDs to be associated with that range of IP addresses.

Note On the Cisco 7600 series router platform, the OSPF routing process is configured on the supervisor engine to advertise only the GPRS tunneling protocol (GTP) server load balancing (SLB) virtual server and the GGSN virtual template addresses.

To configure OSPF, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# router ospf process-id`	Enables OSPF routing, and enters router configuration mode, where *process-id* specifies an internally used identification parameter for an OSPF routing process. The *process-id* is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.
Step 2	`Router(config-router)# network ip-address wildcard-mask area area-id`	Defines an interface on which OSPF runs and defines the area ID for that interface, where: • *ip-address*—Specifies the IP address to be associated with the OSPF network area. • *wildcard-mask*—Specifies the IP address mask that includes “don't care” bits for the OSPF network area. • *area-id*—Specifies the area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address. If you intend to associate areas with IP subnets, you can specify a subnet address as the area ID.

Verifying the Route to the SGSN

To verify the route to the SGSN, you can first verify your GGSN configuration and then verify that a route is established.

Step 1 To verify the supervisor engine configuration, use the **show running-config** command and verify the route that you configured to the SGSN. The following example shows a partial configuration of a configuration to the SGSN:

```
Sup# show running-config
Building configuration...

Current configuration :3642 bytes
!
version 12.3
...
ip slb vserver V0-GGSN
 virtual 10.10.10.10 udp 3386 service gtp
```

```
!
vlan 101
 name Internal_Gn/Ga
!
vlan 302
 name Gn_1
!
vlan 303
 name Ga_1
!
interface FastEthernet8/22
 no ip address
 switchport
 switchport access vlan 302
!
interface FastEthernet8/23
 no ip address
 switchport
 switchport access vlan 302
!
interface FastEthernet8/24
 no ip address
 switchport
 switchport access vlan 303
!
interface Vlan101
 description Vlan to GGSN for GA/GN
 ip address 10.1.1.1 255.255.255.0
!
interface Vlan302
 ip address 40.0.2.1 255.255.255.0
!
interface Vlan303
 ip address 40.0.3.1 255.255.255.0
!
router ospf 300
 log-adjacency-changes
 summary-address 9.9.9.0 255.255.255.0
 redistribute static subnets route-map GGSN-routes
 network 40.0.2.0 0.0.0.255 area 300
 network 40.0.3.0 0.0.0.255 area 300
!
ip route 9.9.9.42 255.255.255.255 10.1.1.42
ip route 9.9.9.43 255.255.255.255 10.1.1.43
ip route 9.9.9.44 255.255.255.255 10.1.1.44
ip route 9.9.9.45 255.255.255.255 10.1.1.45
ip route 9.9.9.46 255.255.255.255 10.1.1.46
ip route 9.9.9.72 255.255.255.255 10.1.1.72
ip route 9.9.9.73 255.255.255.255 10.1.1.73
ip route 9.9.9.74 255.255.255.255 10.1.1.74
ip route 9.9.9.75 255.255.255.255 10.1.1.75
ip route 9.9.9.76 255.255.255.255 10.1.1.76
!
access-list 1 permit 9.9.9.0 0.0.0.255
!
route-map GGSN-routes permit 10
 match ip address 1
```

Step 2 To verify the GGSN configuration, use the **show running-config** command. The following example shows a partial configuration of a configuration to the SGSN:

```
Sup# show running-config
Building configuration...

Current configuration :3642 bytes
!
version 12.3
!
...

interface GigabitEthernet0/0
 no ip address
!

interface GigabitEthernet0/0.2
 description Ga/Gn Interface
 encapsulation dot1Q 101
 ip address 10.1.1.72 255.255.255.0
 no cdp enable
!
ip route 40.1.2.1 255.255.255.255 10.1.1.1
ip route 40.2.2.1 255.255.255.255 10.1.1.1
ip route 40.1.3.10 255.255.255.255 10.1.1.1
ip route 40.2.3.10 255.255.255.255 10.1.1.1
```

Step 3 To verify that the supervisor engine has established a route to the SGSN, use the **show ip route** command as shown in bold in the following examples:

```
Sup# show ip route ospf 300
9.0.0.0/8 is variably subnetted, 12 subnets, 2 masks
O       9.9.9.0/24 is a summary, 1w1d, Null0
!

Sup# show ip route 9.9.9.72
Routing entry for 9.9.9.72/32
  Known via "static", distance 1, metric 0
  Redistributing via ospf 300
  Routing Descriptor Blocks:
  * 10.1.1.72
      Route metric is 0, traffic share count is 1
!
```

Configuring Access Points on the GGSN

Successful configuration of access points on the GGSN requires careful consideration and planning to establish the appropriate access for mobile sessions to external PDNs and private networks.

The following topics are included in this section:

- Overview of Access Points, page 9-8
- Basic Access Point Configuration Task List, page 9-10
- Configuring Real Access Points on the GGSN, page 9-11 (Required)
- Configuring Virtual Access Points on the GGSN, page 9-33 (Optional)

Configuration of access points on the GGSN also requires properly establishing communication with any supporting DHCP and RADIUS servers that you might be using to provide dynamic IP addressing and user authentication functions at the access point.

Details about configuring other services such as DHCP and RADIUS on an access point are discussed in the "Configuring Dynamic Addressing on the GGSN" and "Configuring Security on the GGSN" chapters.

Overview of Access Points

This section includes the following topics:

- Description of Access Points in a GPRS/UMTS Network, page 9-8
- Access Point Implementation on the Cisco GGSN, page 9-9

Description of Access Points in a GPRS/UMTS Network

The GPRS and UMTS standards define a network identity called an access point name (APN). An APN identifies the part of the network where a user session is established. In the GPRS/UMTS backbone, the APN serves as a reference to a GGSN. An APN is configured on and accessible from a GGSN in a GPRS/UMTS network.

An APN can provide access to a public data network (PDN), or a private or corporate network. An APN also can be associated with certain types of services such as Internet access or a Wireless Application Protocol (WAP) service.

The APN is provided by either the mobile station (MS) or by the SGSN to the GGSN in a Create PDP Context request message when a user requests a session to be established.

To identify an APN, a logical name is defined that consists of two parts:

- Network ID—A mandatory part of the APN that identifies the external network to which a GGSN is connected. The network ID can be a maximum of 63 bytes and must contain at least one label. A network ID of more than one label is interpreted as an Internet domain name. An example of a network ID might be "corporate.com."
- Operator ID—An optional part of the APN that identifies the public land mobile network (PLMN) in which a GGSN is located. The operator ID contains three decimal-separated labels; the last label must be "gprs." An example of an operator ID might be "mnc10.mcc200.gprs."

  When the operator ID exists, it is placed after the network ID, and it corresponds to the Domain Name System (DNS) name of a GGSN. The maximum length of an APN is 100 bytes. When the operator ID does not exist, a default operator ID is derived from the mobile network code (MNC) and mobile country code (MCC) information contained in the international mobile subscriber identity (IMSI).

Access Point Implementation on the Cisco GGSN

Configuring access points is one of the central configuration tasks on the Cisco GGSN. Proper configuration of access points is essential to successful implementation of the GGSN in the GPRS/UMTS network.

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

- Access point list—Logical interface that is associated with the virtual template of the Cisco GGSN. The access point list contains one or more access points.
- Access point—Defines an APN and its associated access characteristics, including security and method of dynamic addressing. An access point on the Cisco GGSN can be a virtual or real access point.
- Access point index number—Integer assigned to an APN that identifies the APN within the GGSN configuration. Several GGSN configuration commands use the index number to reference an APN.
- Access group—An additional level of router security on the router 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.

Access Point Types on the GGSN

Cisco IOS GGSN Release 3.0 and later support the following access point types:

- Real—Uses real access point types to configure the GGSN for direct access to a particular target network through an interface. The GGSN always uses real access points to reach an external network.

  For information on configuring real access points on the GGSN, see the "Configuring Real Access Points on the GGSN" section on page 9-11.

- Virtual—Uses virtual access point types to consolidate access to multiple target networks through a virtual APN access point at the GGSN. Because the GGSN always uses real access points to reach an external network, virtual access points should be used in combination with real access points on the GGSN.

  For information on configuring virtual access points on the GGSN, see the "Configuring Virtual Access Points on the GGSN" section on page 9-33.

Note GGSN Release 1.4 and earlier only support real access points. To address provisioning issues in the PLMN, GGSN Release 3.0 and later support virtual access point types. In addition, with GGSN Release 6.0, Cisco IOS Release 12.3(14)YU and later, you can configure virtual APNs to be dynamically mapped, per user, to the target APN during a "pre-authentication" phase. For more information, see the "Configuring Virtual Access Points on the GGSN" section on page 9-33.

Basic Access Point Configuration Task List

This section describes the basic tasks required to configure an access point on the GGSN. Detailed information about configuring access points for specialized functions such as for virtual APN access are described in separate sections of this chapter.

To configure an access point on the GGSN, perform the following basic tasks:

- Configuring the GPRS Access Point List on the GGSN, page 9-10 (Required)
- Creating an Access Point and Specifying Its Type on the GGSN, page 9-10 (Required)

Configuring the GPRS Access Point List on the GGSN

The GGSN software requires that you configure an entity called an *access point list*. You configure the GPRS access point list to define a collection of virtual and real access points on the GGSN.

When you configure the access point list in global configuration mode, the GGSN software automatically associates the access point list with the virtual template interface of the GGSN. Therefore, the GGSN supports only a single access point list.

Note Be careful to observe that the GPRS/UMTS access point list and an IP access list are different entities in the Cisco IOS software. A GPRS/UMTS access point list defines access points and their associated characteristics, and an IP access list controls the allowable access on the router by IP address. You can define permissions to an access point by configuring both an IP access list in global configuration and configuring the **ip-access-group** command in your access point configuration.

To configure the GPRS/UMTS access point list and configure access points within it, use the following command, beginning in global configuration mode:

Command	Purpose
`Router(config)# gprs access-point-list list-name`	Specifies a name for a new access point list, or references the name of the existing access point list, and enters access-point list configuration mode.

Creating an Access Point and Specifying Its Type on the GGSN

You need to define access points within an access point list on the GGSN. Therefore, before you can create an access point, you must define a new access point list or specify the existing access point list on the GGSN to enter access-point list configuration mode.

When you create an access point, you must assign an index number to the access point, specify the domain name (network ID) of the access point, and specify the type of access point (virtual or real). Other options that you can configure on an access point are summarized in the "Configuring Additional Real Access Point Options" section on page 9-20.

To create an access point and specify its type, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs access-point-list list-name`	Specifies a name for a new access point list, or references the name of the existing access point list, and enters access-point list configuration mode.
Step 2	`Router(config-ap-list)# access-point access-point-index`	Specifies an index number for a new access point definition, or references an existing access point definition, and enters access point configuration mode.
Step 3	`Router(config-access-point)# access-point-name apn-name`	Specifies the network (or domain) name for a PDN that users can access from the GGSN at a defined access point. **Note** The *apn-name* must match the APN that is provisioned at the MS, home location register (HLR), and DNS server.
Step 4	`Router (config-access-point)# access-type {virtual [pre-authenticate [default-apn apn-name]]| real}`	(Optional) Specifies the type of access point. The available options are: • **virtual**—APN type that is not associated with any specific physical target network on the GGSN. Optionally, can be configured to be dynamically mapped, per user, to a target APN. • **real**—APN type that corresponds to an interface to an external network on the GGSN. This is the default value. **Note** The default access-type is real. Therefore, you only need to configure this command if the APN is a virtual access point.

Configuring Real Access Points on the GGSN

The GGSN uses real access points to communicate to PDNs or private networks that are available over a Gi interface on the GGSN. Use real access point types to configure the GGSN for direct access to a particular target network through an interface.

If you have configured a virtual access point, you must also configure real access points to reach the target networks.

The GGSN supports configuration of access points to public data networks and to private networks. The following sections describe how to configure different types of real access points:

- PDN Access Configuration Task List, page 9-12
- VPN Access Using VRF Configuration Task Lists, page 9-13

PDN Access Configuration Task List

Configuring a connection to a public PDN includes the following tasks:

- Configuring an Interface to a PDN (Gi interface) (Required)
- Configuring an Access Point for a PDN (Required)

Configuring an Interface to a PDN

To establish access to a PDN in the GPRS/UMTS network, you must configure an interface on the GGSN to connect to the PDN. This interface is referred to as the *Gi interface*.

On the Cisco 7600 series router platform, this interface is a logical one (on which IEEE 802.1Q encapsulation is configured) to a Layer 3 routed Gi VLAN configured on the supervisor engine.

For more information about the Gi VLAN on the supervisor engine, see "Platform Prerequisites" section on page 3-2.

For more information about configuring interfaces, see *Cisco IOS Interface Configuration Guide* and the *Cisco IOS Interface Command Reference*.

Note If you are using VPN routing and forwarding (VRF) for VPN access, you must enable Cisco Express Forwarding (CEF) switching on the GGSN. If you enable CEF switching at the global configuration level, then it is automatically enabled for each interface unless it is specifically disabled at the interface.

Configuring 802.1Q-Encapsulated Subinterfaces

To configure a subinterface that supports IEEE 802.1Q encapsulation to the Gi VLAN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface gigabitethernet slot/port.subinterface-number`	Specifies the subinterface on which IEEE 802.1Q will be used.
Step 2	`Router(config-if)# encapsulation dot1q vlanid`	Defines the encapsulation format as IEEE 802.1Q (dot1q), and specifies the VLAN identifier.
Step 3	`Router(config-if)# ip address ip-address mask`	Sets a primary IP address for an interface.

Configuring an Access Point for a PDN

To configure an access point for a PDN, you must define a real access point in the GPRS access point list.

To configure a real access point on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs access-point-list list-name`	Specifies a name for a new access-point list, or references the name of an existing access-point list, and enters access-point list configuration mode.
Step 2	`Router(config-ap-list)# access-point access-point-index`	Specifies an index number for a new access point definition, or references an existing access point definition, and enters access point configuration mode.
Step 3	`Router(config-access-point)# access-point-name apn-name`	Specifies the network (or domain) name for a PDN that users can access from the GGSN at a defined access point. **Note** The *apn-name* must match the APN that is provisioned at the MS, HLR, and DNS server.
Step 4	`Router(config-access-point)# access-type real`	Specifies an APN type that corresponds to an interface to an external network on the GGSN. Real is the default value.

For an example of a GPRS access point configuration, see the "Access Point List Configuration Example" section on page 9-54.

VPN Access Using VRF Configuration Task Lists

The Cisco IOS GGSN software supports connectivity to a VPN using VPN routing and forwarding (VRF).

Note VRF is not supported for IPv6 PDPs. Therefore, if the **ipv6** command is configured under an APN on which VRF is enabled, the IPv4 PDPs are routed in VRF, but the IPv6 PDPs are routed in the global routing table.

The GGSN software provides a couple of ways that you can configure access to a VPN, depending on your platform, network configuration over the Gi interface between the GGSN and your PDNs, and the VPN that you want to access.

To configure VPN access using VRF on the GGSN, perform the following tasks:

- Enabling CEF Switching, page 9-14 (Required)
- Configuring a VRF Routing Table on the GGSN, page 9-14 (Required)
- Configuring a Route to the VPN Using VRF, page 9-14 (Required)
- Configuring an Interface to a PDN Using VRF, page 9-16 (Required)
- Configuring Access to a VPN, page 9-17 (Required)

For sample configurations, see the "VRF Tunnel Configuration Example" section on page 9-55.

Enabling CEF Switching

When you enable CEF switching globally on the GGSN, all interfaces on the GGSN are automatically enabled for CEF switching.

Note To ensure that CEF switching functions properly, wait a short time before enabling CEF switching after it is disabled using the **no ip cef** command.

To enable CEF switching for all interfaces on the GGSN, use the following commands, beginning in global configuration mode:

Command	Purpose
`Router(config)# ip cef`	Enables CEF on the processor.

Configuring a VRF Routing Table on the GGSN

To configure a VRF routing table on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ip vrf` *vrf-name*	Configures a VRF routing table, and enters VRF configuration mode.
Step 2	`Router(config-vrf)# rd` *route-distinguisher*	Creates routing and forwarding tables for a VRF and specifies the default route distinguisher for a VPN.

Configuring a Route to the VPN Using VRF

Be sure that a route exists between the GGSN and the private network that you want to access. You can verify connectivity by using the **ping** command from the GGSN to the private network address. To configure a route, you can use a static route or a routing protocol.

Configuring a Static Route Using VRF

To configure a static route using VRF, use the following command, beginning in global configuration mode:

Command	Purpose
`Router(config)# ip route vrf vrf-name prefix mask [next-hop-address] [interface {interface-number}] [global] [distance] [permanent] [tag tag]`	Configures a static IP route, where: • *vrf-name*—Specifies the name of the VPN routing/forwarding instance (VRF) for the static route. • *prefix*—Specifies the IP route prefix for the destination. • *mask*—Specifies the prefix mask for the destination. • *next-hop-address*—Specifies the IP address of the next hop that can be used to reach the destination network. • *interface interface-number*—Specifies the network interface type and interface number that can be used to reach the destination network. • **global**—Specifies that the given next hop address is in the non-VRF routing table. • *distance*—Specifies an administrative distance for the route. • **permanent**—Specifies that the route will not be removed, even if the interface shuts down. • **tag** *tag*—Specifies a tag value that can be used as a "match" value for controlling redistribution via route maps.

Verifying a Static Route Using VRF

To verify that the GGSN has established the static VRF route that you configured, use the **show ip route vrf** privileged EXEC command as shown in the following example:

```
GGSN# show ip route vrf vpn1 static
     172.16.0.0/32 is subnetted, 1 subnets
U       172.16.0.1 [1/0] via 0.0.0.0, Virtual-Access2
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
S       10.100.0.3/32 [1/0] via 10.110.0.13
```

Configuring an OSPF Route Using VRF

To configure an OSPF route using VRF, use the following command, beginning in global configuration mode:

Command	Purpose
`Router(config)# router ospf process-id [vrf vrf-name]`	Enables OSPF routing, and enters router configuration mode, where, • *process-id*—Specifies an internally used identification parameter for an OSPF routing process. The *process-id* is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process. • **vrf** *vrf-name*—Specifies the name of the VPN routing/forwarding instance.

Configuring an Interface to a PDN Using VRF

To establish access to a PDN, an interface on the GGSN to connect to the PDN. This interface is referred to as the Gi interface.

On the Cisco 7600 series router platform, this interface is a logical one (on which IEEE 802.1Q encapsulation is configured) to a Layer 3 routed Gi VLAN configured on the supervisor engine.

For more information about the Gi VLAN on the supervisor engine, see "Platform Prerequisites" section on page 3-2.

For more information about configuring interfaces, see *Cisco IOS Interface Configuration Guide* and the *Cisco IOS Interface Command Reference*.

Note If you are using VRF for VPN access, you must enable CEF switching on the GGSN. If you enable CEF switching at the global configuration level, then it is automatically enabled for each interface unless it is specifically disabled at the interface.

Configuring 802.1Q-Encapsulated Subinterfaces

To configure a subinterface that supports IEEE 802.1Q encapsulation to the Gi VLAN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface gigabitethernet slot/port.subinterface-number`	Specifies the subinterface on which IEEE 802.1Q will be used.
Step 2	`Router(config-if)# encapsulation dot1q vlanid`	Defines the encapsulation format as IEEE 802.1Q (dot1q), and specifies the VLAN identifier.
Step 3	`Router(config-if)# ip address ip-address mask`	Sets a primary IP address for an interface.

Configuring Access to a VPN

After you have completed the prerequisite configuration tasks, you can configure access to a VPN with a tunnel or without a tunnel.

The following sections describe the different methods you can use to configure access to a VPN:

Configuring Access to a VPN Without a Tunnel

Configuring Access to a VPN With a Tunnel

Note With GGSN Release 5.0 and later, you can assign multiple APNs to the same VRF.

Configuring Access to a VPN Without a Tunnel

If you configure more than one Gi interface to different PDNs, and need to access a VPN off one of those PDNs, then you can configure access to that VPN without configuring an IP tunnel. To configure access to the VPN in this case, you need to configure the **vrf** command in access point configuration mode.

To configure access to a VPN in the GPRS access point list, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs access-point-list list-name`	Specifies a name for a new access point list, or references the name of the existing access point list, and enters access-point list configuration mode.
Step 2	`Router(config-ap-list)# access-point access-point-index`	Specifies an index number for a new access point definition, or references an existing access point definition, and enters access point configuration mode.
Step 3	`Router(config-access-point)# access-point-name apn-name`	Specifies the network (or domain) name for a PDN that users can access from the GGSN at a defined access point. **Note** The *apn-name* must match the APN that is provisioned at the MS, HLR, and Domain Name System (DNS) server.
Step 4	`Router(config-access-point)# access-type real`	Specifies an APN type that corresponds to an interface to an external network on the GGSN. Real is the default value.
Step 5	`Router(config-access-point)# vrf vrf-name`	Configures VRF at a GGSN access point and associates the access point with a particular VRF instance.
Step 6	`Router(config-access-point)# exit`	Exits access point configuration mode.

For information about the other access point configuration options, see the "Configuring Additional Real Access Point Options" section on page 9-20.

Configuring Access to a VPN With a Tunnel

If you have only a single Gi interface to a PDN from which you need to access one or more VPNs, you can configure an IP tunnel to access those private networks.

To configure access to the VPN using a tunnel, perform the following tasks:

- Configuring the VPN Access Point (Required)
- Configuring the IP Tunnel (Required)

Configuring the VPN Access Point

To configure access to a VPN in the GPRS access point list, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs access-point-list` *list-name*	Specifies a name for a new access point list, or references the name of the existing access point list, and enters access-point list configuration mode.
Step 2	`Router(config-ap-list)# access-point` *access-point-index*	Specifies an index number for a new access point definition, or references an existing access point definition, and enters access point configuration mode.
Step 3	`Router(config-access-point)# access-point name` *apn-name*	Specifies the access point network ID, which is commonly an Internet domain name. **Note** The *apn-name* must match the APN that is provisioned at the MS, HLR, and DNS server.
Step 4	`Router(config-access-point)# access-mode {transparent | non-transparent}`	(Optional) Specifies whether the GGSN requests user authentication at the access point to a PDN. The available options are: • **transparent**—No security authorization or authentication is requested by the GGSN for this access point. This is the default value. • **non-transparent**—GGSN acts as a proxy for authenticating.
Step 5	`Router(config-access-point)# access-type real`	Specifies an APN type that corresponds to an interface to an external network on the GGSN. Real is the default value.

	Command	Purpose
Step 6	`Router(config-access-point)# ip-address-pool {dhcp-proxy-client | radius-client | local pool-name | disable}`	(Optional) Specifies a dynamic address allocation method using IP address pools for the current access point. The available options are: • **dhcp-proxy-client**—DHCP server provides the IP address pool. • **radius-client**—RADIUS server provides the IP address pool. • **local**—Specifies that a local pool provides the IP address. This option requires configuration of a local pool using the **ip local pool** command in global configuration mode. • **disable**—Turns off dynamic address allocation. **Note** If you are using a dynamic address allocation method, then you must configure this command according to the appropriate IP address pool source. **Note** When the **radius-client** keyword option is specified, 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 pool name, and the IP address is used instead of an address being allocated from the pool.
Step 7	`Router(config-access-point)# vrf vrf-name`	Configures VPN routing and forwarding at a GGSN access point and associates the access point with a particular VRF instance.
Step 8	`Router(config-access-point)# exit`	Exits access point configuration mode.

For information about the other access point configuration options, see the "Configuring Additional Real Access Point Options" section on page 9-20.

Configuring the IP Tunnel

When you configure a tunnel, you might consider using loopback interfaces as the tunnel endpoints instead of real interfaces because loopback interfaces are always up.

To configure an IP tunnel to a private network, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface tunnel number`	Configures a logical tunnel interface number.
Step 2	`Router(config-if)# ip vrf forwarding vrf-name`	Associates a VRF instance with the interface.

	Command	Purpose
Step 3	`Router(config-if)# ip address ip-address mask [secondary]`	Specifies an IP address for the tunnel interface. **Note** This IP address is not used in any other part of the GGSN configuration.
Step 4	`Router(config-if)# tunnel source {ip-address | type number}`	Specifies the IP address (or interface type and port or card number) of the Gi interface to the PDN or a loopback interface.
Step 5	`Router(config-if)# tunnel destination {hostname | ip-address}`	Specifies IP address (or hostname) of the private network that you can access from this tunnel.

Configuring Additional Real Access Point Options

This section summarizes the configuration options that you can specify for a GGSN access point.

Some of these options are used in combination with other global router settings to configure the GGSN. Further details about configuring several of these options are discussed in other topics in this chapter and other chapters of this book.

Note Although the Cisco IOS software allows you to configure other access point options on a virtual access point, only the **access-point-name** and **access-type** commands are applicable to a virtual access point. Other access point configuration commands, if configured, will be ignored.

To configure options for a GGSN access point, use any of the following commands, beginning in access-point list configuration mode:

	Command	Purpose
Step 1	`Router(config-access-point)# aaa-accounting {enable | disable}`	Enables or disables accounting for a particular access point on the GGSN. **Note** If you have configured a transparent access APN and you want to provide accounting at that APN, you need to configure the **aaa-accounting enable** command at the APN.
Step 2	`Router(config-access-point)# aaa-group {authentication | accounting} server-group`	Specifies a default authentication, authorization, and accounting (AAA) server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN, where: • **authentication**—Assigns the selected server group for authentication services on the APN. • **accounting**—Assigns the selected server group for accounting services on the APN. • *server-group*—Specifies the name of an AAA server group to be used for AAA services on the APN. **Note** The name of the AAA server group that you specify must correspond to a server group that you configure using the **aaa group server** command.
Step 3	`Router(config-access-point)# access-mode {transparent | non-transparent}`	(Optional) Specifies whether the GGSN requests user authentication at the access point to a PDN. The available options are: • **transparent**—No security authorization or authentication is requested by the GGSN for this access point. This is the default value. • **non-transparent**—GGSN acts as a proxy for authenticating.
Step 1	`Router(config-ap-list)# access-point access-point-index`	Specifies an index number for a new access point definition, or references an existing access point definition, and enters access point configuration mode.
Step 2	`Router(config-access-point)# access-point-name apn-name`	Specifies the network (or domain) name for a PDN that users can access from the GGSN at a defined access point. **Note** The *apn-name* must match the APN that is provisioned at the MS, HLR, and DNS server.

	Command	Purpose
Step 3	`Router(config-access-point)# access-type {virtual | real}`	(Optional) Specifies the type of access point. The available options are: • **virtual**—APN type that is not associated with any specific physical target network. • **real**—APN type that corresponds to an interface to an external network on the GGSN. This is the default value. **Note** The default access-type is real. Therefore, you only need to configure this command if the APN is a virtual access point.
Step 4	`Router(config-access-point)# access-violation deactivate-pdp-context}`	(Optional) Specifies that a user's session be ended and the user packets discarded when a user attempts unauthorized access to a PDN through an access point.
Step 5	`Router(config-access-point)# aggregate {auto | ip-network-prefix{/mask-bit-length | subnet-mask}} [csg-group-name]`	(Optional) Configures the GGSN to create an aggregate route in its IP routing table when receiving PDP requests from MSs on the specified network through a particular access point on the GGSN. **Note** The **aggregate auto** command will not aggregate routes when using local IP address pools. **Note** This configuration applies to IPv4 PDP contexts. **Note** To configure a default subnet mask for subnet management and enable dynamic subnet creation in an eGGSN implementation with Cisco CSG2, specify **0.0.0.0** *subnet-mask.*
Step 6	`Router(config-access-point)# anonymous user username [password]`	(Optional) Configures anonymous user access at an access point.
Step 7	`Router(config-access-point)# block-foreign-ms`	(Optional) Restricts GGSN access at a particular access point based on the mobile user's home PLMN.
Step 8	`Router(config-access-point)# cac-policy`	(Optional) Enables the maximum QoS policy function of the Call Admission Control (CAC) feature and applies a policy to an access point.
Step 9	`Router(config-access-point)# charging group chrg-group-number`	Associates an existing charging group with an APN, where *group-number* is a number 1 through 29.

	Command	Purpose
Step 10	`Router(config-access-point)# csg-group chrg-group-number`	(Optional) Configures one or more Cisco Content Services Gateway - 2nd Generation (CSG2) groups under an APN to use for quota server-to-CSG communication for that APN when service-aware billing is enabled. **Note** The **csg-group** command in access point configuration mode and the **csg group** command in quota server configuration mode are mutually exclusive. You cannot define a CSG group under an APN if one is already configured under the quota server interface.
Step 11	`Router(config-access-point)# dhcp-gateway-address ip-address`	(Optional) Specifies a DHCP gateway to handle DHCP requests for mobile station (MS) users entering a particular PDN access point. **Note** This configuration applies to IPv4 PDP contexts.
Step 12	`Router(config-access-point)# dhcp-server {ip-address} [ip-address] [vrf]`	(Optional) Specifies a primary (and backup) DHCP server to allocate IP addresses to MS users entering a particular PDN access point. **Note** This configuration applies to IPv4 PDP contexts.
Step 13	`Router(config-access-point)# dns primary ip-address secondary ip-address`	(Optional) Specifies a primary (and backup) DNS to be sent in Create PDP Context responses at the access point. **Note** This configuration applies to IPv4 PDP contexts.

	Command	Purpose
Step 14	`Router(config-access-point)# gtp pdp-context single pdp-session [mandatory]`	(Optional) Configures the GGSN to delete the primary PDP context, and any associated secondary PDP contexts, of a *hanging* PDP session upon receiving a new create request from the same MS that shares the same IP address of the hanging PDP context. A hanging PDP context is a PDP context on the GGSN whose corresponding PDP context on the SGSN has already been deleted for some reason. When a hanging PDP session occurs and the **gtp pdp-context single pdp-session** command is not configured, if the same MS (on the same APN) sends a new Create PDP Context request that has a different NSAPI but is assigned the same IP address used by the hanging PDP session, the GGSN rejects the new Create PDP Context request. When configure without the **mandatory** keyword specified, this feature applies only to those users for whom the Cisco vendor-specific attribute (VSA) "gtp-pdp-session=single-session" is defined in their RADIUS user profile. To enable this feature and apply it to all users under an APN regardless of their RADIUS user profiles, specify the **mandatory** keyword option. **Note** If this feature is used with GTP load balancing, it might not function properly. **Note** This configuration applies to IPv4 PDP contexts.
Step 15	`Router(config-access-point)# gtp response-message wait-accounting`	(Optional) Configures the GGSN to wait for a RADIUS accounting response before sending a Create PDP Context response to the SGSN.
Step 16	`Router(config-access-point)# gtp pdp-context timeout idle` *interval* `[uplink]`	(Optional) Specifies the time, in seconds, that a GGSN allows a session to be idle at a particular access point before terminating the session.
Step 17	`Router(config-access-point)# gtp pdp-context timeout session` *interval* `[uplink]`	(Optional) Specifies the time, in seconds, that the GGSN allows a session to exist at any access point before terminating the session.

	Command	Purpose
Step 18	`Router(config-access-point)# ip-access-group` *access-list-number* {**in** | **out**}	(Optional) Specifies access permissions between an MS and a PDN through the GGSN at a particular access point, where *access-list-number* specifies the IP access list definition to use at the access point. The available options are: • **in**—Applies the IP access list definition from the PDN to the MS. • **out**—Applies the IP access list definition from the MS to the PDN. **Note** To disable the sending of ICMP messages, ensure that the **no ip unreachable** command in interface configuration mode is configured on the virtual template interface. **Note** This configuration applies to IPv4 PDP contexts.
Step 19	`Router(config-access-point)# ip-address-pool` {**dhcp-proxy-client** | **radius-client** [**no-redistribute**] | **local** *pool-name* | **disable**}	(Optional) Specifies a dynamic address allocation method using IP address pools for the current access point. The available options are: • **dhcp-proxy-client**—DHCP server provides the IP address pool. • **radius-client**—RADIUS server provides the IP address pool.Optionally, specify the **no-redistribute** keyword option to disable route propagation from the Cisco GGSN to the supervisor. • **local**—Specifies that a local pool provides the IP address. This option requires that a local pool is configured using the **ip local pool** command in global configuration mode. • **disable**—Turns off dynamic address allocation. **Note** If you are using a dynamic address allocation method, then you must configure this command according to the appropriate IP address pool source. **Note** This configuration applies to IPv4 PDP contexts.
Step 20	`Router(config-access-point)# ip probe path` *ip_address* **protocol udp** [**port** *port* **ttl** *ttl*]	(Optional) Enables the GGSN to send a probe packet to a specific destination for each PDP context that is successfully established under an APN. **Note** This configuration applies to IPv4 PDP contexts.
Step 21	`Router(config-access-point)# ipv6 ipv6-access-group` *ACL-name* [**up** | **down**]	(Optional) Applies an access-control list (ACL) configuration to uplink or downlink IPv6 payload packets.

	Command	Purpose
Step 22	`Router(config-access-point)# ipv6 ipv6-address-pool {local pool-name | radius-client}`	(Optional) Configures a dynamic IPv6 prefix allocation method on an access-point.
Step 23	`Router(config-access-point)# ipv6 base-vtemplate number`	(Optional) Specifies the virtual template interface, containing IPv6 routing advertisements (RA) parameters, for an APN to copy to create virtual subinterfaces for IPv6 PDP contexts.
Step 24	`Router(config-access-point)# ipv6 dns primary ipv6-address [secondary ipv6-address]`	(Optional) Specifies the address of a primary (and backup) IPv6 DNS to be sent in IPv6 Create PDP Context responses on an access point.
Step 25	`Router(config-access-point)# ipv6 [enable | exclusive]`	(Optional) Configures an access point to allow both IPv6 and IPv4 PDP contexts, or to just allow IPv6 PDP contexts.
Step 26	`Router(config-access-point)# ipv6 redirect [all | intermobile] ipv6-address`	(Optional) Configures the GGSN to redirects IPv6 traffic to an external IPv6 device. The available options are: • **all—**Redirects all IPv6 traffic to an external IPv6 device for an APN. • **intermobile—**Redirects mobile-to-mobile IPv6 traffic to an external IPv6 device. • *ipv6-address*—IP address of the IPv6 external device to which you want to redirect IPv6 traffic.
Step 27	`Router(config-access-point)# ipv6 security verify source`	(Optional) Enables the GGSN to verify the IPv6 source address of an upstream TPDU against the address previously assigned to an MS.
Step 28	`Router(config-access-point)# msisdn suppression [value]`	(Optional) Specifies that the GGSN overrides the mobile station ISDN (MSISDN) number with a pre-configured value in its authentication requests to a RADIUS server.
Step 29	`Router(config-access-point)# nbns primary ip-address secondary ip-address`	(Optional) Specifies a primary (and backup) NetBIOS Name Service (NBNS) to be sent in the Create PDP Context responses to at the access-point. **Note** This configuration applies to IPv4 PDP contexts.
Step 30	`Router(config-access-point)# network-behind-mobile`	Enables an access point to support routing behind the mobile station (MS). **Note** This configuration applies to IPv4 PDP contexts.
Step 31	`Router(config-access-point)# pcc`	Configures the APN as a PCC-enabled APN.

	Command	Purpose
Step 32	`Router(config-access-point)# ppp-regeneration [max-session number | setup-time seconds | verify-domain | fixed-domain | allow-duplicate]`	(Optional) Enables an access point to support PPP regeneration, where: • **max-session** *number*—Specifies the maximum number of PPP regenerated sessions allowed at the access point. The default value is device dependent and is determined by the maximum IDBs that can be supported by the router. • **setup-time** *seconds*—Specifies the maximum amount of time (between 1 and 65535 seconds) within which a PPP regenerated session must be established. The default value is 60 seconds. • **verify-domain**—Configures the GGSN to verify the domain sent in the protocol configuration option (PCO) IE sent in a Create PDP Context request against the APN sent out by the user when PPP-regeneration is being used. If a mismatch occurs, the Create PDP Context request is rejected with the cause code "Service not supported." • **fixed-domain**—Configures the GGSN to use the access point name as the domain name with which it initiates an L2TP tunnel to the user when PPP-regeneration is being used. The **ppp-regeneration fixed-domain** and **ppp-regeneration verify-domain** command configurations are mutually exclusive. When the **ppp-regeneration fixed-domain** command is configured, domain verification cannot be performed. • **allow-duplicate**—Configures the GGSN to not check for duplicate IP addresses for PPP regenerated PDP contexts. **Note** This configuration applies to IPv4 PDP contexts.
Step 33	`Router(config-access-point)# radius attribute acct-session-id charging-id`	(Optional) Specifies that the charging ID in the Acct-Session-ID (attribute 44) is included in access requests.
Step 34	`Router(config-access-point)# radius attribute nas-id format`	(Optional) Specifies that the GGSN sends the NAS-Identifier in access requests at the APN where *format* is a string sent in attribute 32 containing an IP address (%i), a hostname (%h), and a domain name (%d).

	Command	Purpose
Step 35	`Router(config-access-point)# radius attribute suppress [imsi | qos | sgsn-address]`	(Optional) Specifies that the GGSN suppress the following in its authentication and accounting requests to a RADIUS server: • **imsi**—Suppresses the 3GPP-IMSI number. • **qos**—Suppresses the 3GPP-GPRS-Qos Profile. • **sgsn-address**—Suppresses the 3GPP-GPRS-SGSN-Address
Step 36	`Router(config-access-point)# radius attribute user-name msisdn`	(Optional) Specifies that the MSISDN is included in the User-Name (attribute 1) field in access requests.
Step 37	`Router(config-access-point) redirect all ip ip address`	(Optional) Configures the GGSN to redirect all traffic to an external device. **Note** This configuration applies to IPv4 PDP contexts.
Step 38	`Router(config-access-point) redirect intermobile ip ip address`	(Optional) Configures the GGSN to redirect mobile-to-mobile traffic to an external device. **Note** This configuration applies to IPv4 PDP contexts.
Step 39	`Router(config-access-point) security verify {source | destination}`	Specifies that the GGSN verify the source or destination address in Transport Protocol Data Units (TPDUs) received from a Gn interface. **Note** This configuration applies to IPv4 PDP contexts.
Step 40	`Router(config-access-point)# session idle-timer number`	(Optional) Specifies the time (between 1 and 168 hours) that the GGSN waits before purging idle mobile sessions for the current access point.
Step 41	`Router(config-access-point)# subscription-required`	(Optional) Specifies that the GGSN checks the value of the selection mode in a PDP context request to determine if a subscription is required to access a PDN through the access point.
Step 42	`Router(config-access-point)# vrf vrf-name`	(Optional) Configures VPN routing and forwarding at a GGSN access point and associates the access point with a particular VRF instance. **Note** This configuration applies to IPv4 PDP contexts.

Verifying the Real Access Point Configuration

This section describes how to verify that you have successfully configured access points on the GGSN, and includes the following tasks:

- Verifying the GGSN Configuration, page 9-29
- Verifying Reachability of the Network Through the Access Point, page 9-31

Verifying the GGSN Configuration

To verify that you have properly configured access points on the GGSN, use the **show running-config** command and the **show gprs access-point** commands.

Note The **gprs access-point-list** command first appears in the output of the **show running-config** command under the virtual template interface, which indicates that the GPRS access point list is configured and is associated with the virtual template. To verify your configuration of specific access points within the GPRS access point list, look further down in the **show** command output where the **gprs access-point-list** command appears again, followed by the individual access point configurations.

Step 1 From global configuration mode, use the **show running-config** command as shown in the following example. Verify that the **gprs access-point-list** command appears under the virtual template interface, and verify the individual access point configurations within the **gprs access-point-list** section of the output as shown in bold:

```
Router# show running-config
Building configuration...

Current configuration : 3521 bytes
!
version 12.x
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service gprs ggsn
!
hostname ggsn
!
ip cef
!
...
!
interface loopback 1
 ip address 10.40.40.3 255.255.255.0
!
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list gprs
!
. . .
!
gprs access-point-list gprs
!
  access-point 1
   access-point-name gprs.cisco.com
   access-mode non-transparent
   aaa-group authentication abc
   network-request-activation
   exit
!
  access-point 2
   access-point-name gprt.cisco.com
   exit
!
  access-point 3
   access-point-name gpru.cisco.com
```

```
   ip-address-pool radius-client
   access-mode non-transparent
   aaa-group authentication abc
   exit
!
gprs maximum-pdp-context-allowed 90000
gprs gtp path-echo-interval 0
gprs default charging-gateway 10.15.15.1
!
gprs memory threshold 512
!
...
radius-server host 172.18.43.7 auth-port 1645 acct-port 1646 non-standard
radius-server retransmit 3
radius-server key 7 12150415
call rsvp-sync
!
no mgcp timer receive-rtcp
!
mgcp profile default
!
gatekeeper
 shutdown
end
```

Step 2 To view the configuration of a specific access point on the GGSN in further detail, use the **show gprs access-point** command and specify the index number of the access point, as shown in the following example:

```
Router# show gprs access-point 2
    apn_index 2          apn_name = gprt.cisco.com
    apn_mode: transparent
    apn-type: Real
    accounting: Disable
    wait_accounting: Disable
    dynamic_address_pool: not configured
    apn_dhcp_server: 0.0.0.0
    apn_dhcp_gateway_addr: 0.0.0.0
    apn_authentication_server_group:
    apn_accounting_server_group:
    apn_username: , apn_password:
    subscribe_required: No
    deactivate_pdp_context_on violation: No
    network_activation_allowed: No
    Block Foreign-MS Mode: Disable
    VPN: Disable
    GPRS vaccess interface: Virtual-Access1
    number of ip_address_allocated 0

    Total number of PDP in this APN :1

    aggregate:
    In APN:    Disable

    In Global: Disable
```

Step 3 To view a summary of every access point that is configured on the GGSN, use the **show gprs access-point all** command as shown in the following example:

```
Router# show gprs access-point all

There are 3 Access-Points configured

Index   Mode            Access-type    AccessPointName      VRF Name
-------------------------------------------------------------------------
1       non-transparent    Real       gprs.cisco.com
-------------------------------------------------------------------------
2       transparent        Real       gprt.cisco.com
-------------------------------------------------------------------------
3       non-transparent    Real       gpru.cisco.com
-------------------------------------------------------------------------
```

Verifying Reachability of the Network Through the Access Point

The following procedure provides a basic methodology for verifying reachability from the MS to the destination network.

Note Many factors can affect whether you can successfully reach the destination network. Although this procedure does not attempt to fully address those factors, it is important for you to be aware that your particular configuration of the APN, IP routing, and physical connectivity of the GGSN, can affect end-to-end connectivity between a host and an MS.

To verify that you can reach the network from the MS, perform the following steps:

Step 1 From the MS (for example, using a handset), create a PDP context with the GGSN by specifying the APN to which you want to connect. In this example, you specify the APN *gprt.cisco.com*.

Step 2 From global configuration mode on the GGSN, use the **show gprs access-point** command and verify the number of created network PDP contexts (in the Total number of PDP in this APN output field).

The following example shows one successful PDP context request:

```
Router# show gprs access-point 2
    apn_index 2          apn_name = gprt.cisco.com
    apn_mode: transparent
    apn-type: Real
    accounting: Disable
    wait_accounting: Disable
    dynamic_address_pool: not configured
    apn_dhcp_server: 0.0.0.0
    apn_dhcp_gateway_addr: 0.0.0.0
    apn_authentication_server_group:
    apn_accounting_server_group:
    apn_username: , apn_password:
    subscribe_required: No
    deactivate_pdp_context_on violation: Yes
    network_activation_allowed: No
    Block Foreign-MS Mode: Disable
```

```
VPN: Disable
GPRS vaccess interface: Virtual-Access1
number of ip_address_allocated 0

Total number of PDP in this APN :1

aggregate:
In APN:    Disable

In Global: Disable
```

Step 3 To test further, generate traffic to the network. To do this, use the **ping** command from a handset, or from a laptop connected to the handset, to a host on the destination network, as shown in the following example:

```
ping 192.168.12.5
```

Note To avoid possible DNS configuration issues, use the IP address (rather than the hostname) of a host that you expect to be reachable within the destination network. For this test to work, the IP address of the host that you select must be able to be properly routed by the GGSN.

In addition, the APN configuration and physical connectivity to the destination network through a Gi interface must be established. For example, if the host to be reached is in a VPN, the APN must be properly configured to provide access to the VPN.

Step 4 After you have begun to generate traffic over the PDP context, use the **show gprs gtp pdp-context** command to see detailed statistics including send and receive byte and packet counts.

Tip To find the Terminal Identifier (TID) for a particular PDP context on an APN, use the **show gprs gtp pdp-context access-point** command.

The following example shows sample output for a PDP context for TID 81726354453647FA:

```
Router#show gprs gtp pdp-context tid 81726354453647FA
TID              MS Addr                   Source  SGSN Addr       APN
81726354453647FA 1.2.3.18                  Static  4.4.4.10        gtpv1.com

    current time :Feb 15 2010 04:11:17
    user_name (IMSI): 214300000000004    MS address: 1.2.3.18
    MS International PSTN/ISDN Number (MSISDN): 112000000000004
    sgsn_addr_signal: 4.4.4.10           sgsn_addr_data:   4.4.4.10
    control teid local:  0x0210001F
    control teid remote: 0x00000041
    data teid local:     0x02100020
    data teid remote:    0x00000042
    primary pdp: Y           nsapi: 1
    signal_sequence:  1                  seq_tpdu_up:      0
    seq_tpdu_down:    0
    upstream_signal_flow:   0            upstream_data_flow:   0
    downstream_signal_flow: 0            downstream_data_flow: 0
    RAupdate_flow:          0
    pdp_create_time:   Feb 15 2010 04:07:59
    last_access_time:  Feb 15 2010 04:07:59
    mnrgflag:          0                tos mask map: B8
    session timeout: 86400
    idle timeout: 720000
    umts qos_req: 0911012901010111050101
    umts qos_neg: 0911012901010111050101
```

```
QoS class: conversational
rcv_pkt_count:       10026          rcv_byte_count:     1824732
send_pkt_count:      5380           send_byte_count:    4207160
cef_up_pkt:          0              cef_up_byte:        0
cef_down_pkt:        0              cef_down_byte:      0
cef_drop:            0              out-sequence pkt:   0
charging_id:         42194519
visitor: No          roamer: Unknown
charging characteristics:          1
charging characteristics received: 0
csg: csggroup1, address: 75.75.75.1
pdp reference count: 2
primary dns:         0.0.0.0
secondary dns:       0.0.0.0
primary nbns:        0.0.0.0
secondary nbns:      0.0.0.0
ntwk_init_pdp:       0
single pdp-session: Disabled

absolute session start time:   NOT SET
Accounting Session ID: 161616010283D657
Periodic accounting interval: NOT SET
AAA Unique ID: 16 (0x10)
Interim Update statistics:
    records sent 0, records failed 0
Direct Tunnel: Disabled
Eggsn mode: 0x06 (QS: disabled, EGCDR: enabled, SVC-MESG: enabled)
PDP internal flags: 7C0001
MCB internal flags: 0
```

Configuring Virtual Access Points on the GGSN

This section includes the following topics:

- Overview of the Virtual Access Point Feature, page 9-33
- Virtual Access Point Configuration Task List, page 9-37
- Verifying the Virtual Access Point Configuration, page 9-39

For a sample configuration, see the "Virtual APN Configuration Example" section on page 9-56.

Overview of the Virtual Access Point Feature

GGSN Release 3.0 and later support virtual APN access from the PLMN using the virtual access point type on the GGSN. The virtual APN feature on the GGSN allows multiple users to access different physical target networks through a shared APN access point on the GGSN.

In a GPRS/UMTS network, the user APN information must be configured at several of the GPRS/UMTS network entities, such as the home location register (HLR) and DNS server. In the HLR, the user subscription data associates the IMSI (unique per user) with each APN that the IMSI is allowed to access. At the DNS server, APNs are correlated to the GGSN IP address. If DHCP or RADIUS servers are in use, the APN configuration can also extend to those servers.

The virtual APN feature reduces the amount of APN provisioning required by consolidating access to all real APNs through a single virtual APN at the GGSN. Therefore, only the virtual APN is provisioned at the HLR and DNS server, instead of each of the real APNs to be reached. The GGSN also must be configured for the virtual APN.

Note On the Cisco 7600 series router platform, identical virtual APN configurations must exist on each GGSN that is load-balanced by means of a virtual server.

Benefits of the Virtual APN Feature

The virtual APN feature provides the following benefits:

- Simplifies provisioning of APN information
- Improves scalability for support of large numbers of corporate networks, ISPs, and services
- Increases flexibility of access point selection
- Eases deployment of new APNs and services
- By setting the APN from the AAA server (pre-authentication-based virtual APN), operators can work with any APN from the handset, including the wildcard APN (*) because the target APN the user is not connected to is base on the user provisioning.

General Restrictions of the Virtual APN Feature

The virtual APN feature has the following restrictions:

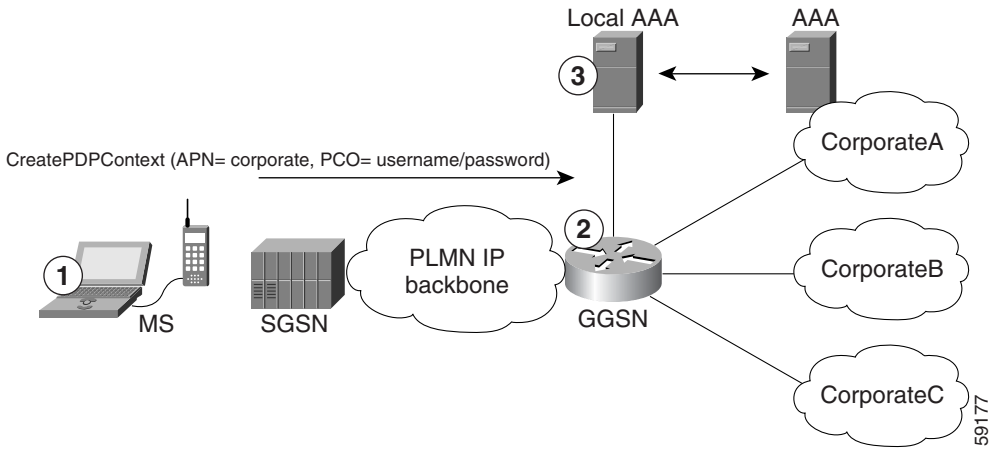
- CDRs do not include domain information because for virtual APNs, the domain information is removed from the username attribute. By default, the associated real APN name is used in CDRs and authentication requests to a virtual APN. However, the GGSN can be configured to send the virtual APN in CDRs using the **gprs charging cdr-option** command with the **apn virtual** keyword options specified.
- Although the Cisco IOS software allows you to configure other access point options on a virtual access point, no other access point options are applicable if they are configured.

Domain-based Virtual Access Point s

By default, the GGSN determines the ultimate target network for a session by receiving the Create PDP Context request at the virtual access point and extracting the domain name to direct the packet to the appropriate real APN. The real APN is the actual destination network. Domain-based APN resolution is the default.

Figure 9-1 shows how the GGSN, by default, supports a Create PDP Context request from an MS processed through a virtual APN on the GGSN.

Figure 9-1 Default Virtual APN PDP Context Activation on the GGSN



1. At the MS, the user connects to the network with a username in the form of login@domain, such as ciscouser@CorporateA.com. The SGSN sends a Create PDP Context request to the GGSN, using the virtual APN of "corporate." The Create PDP Context request also includes the username in login@domain format in the protocol configuration option (PCO) information element.
2. The GGSN extracts the domain from the information in the PCO, which corresponds to the real target network on the GGSN. In this example, the GGSN finds CorporateA.com as the domain and directs the session to the appropriate real APN for the target network. In this case, the real APN is corporateA.com. The GGSN uses the complete username to do authentication.
3. The local or corporate AAA server is selected based on the domain part of the username, which is CorporateA.com in this case.

Pre-authentication-based Virtual Access Points

The pre-authentication-based virtual APN feature utilizes AAA servers to provide dynamic, per-user mapping of a virtual APN to a target (real) APN.

When the **pre-authenticate** keyword option is specified when configuring a virtual APN, a pre-authentication phase is applied to Create PDP Context requests received that include a virtual APN in the APN information element.

Pre-authentication-based virtual APN requires that the AAA server be configured to provision user profiles to include the target APN. The AAA maps a user to the target using user identifications such as the IMSI, user name, or MSISDN, etc. In addition, the target APN must be locally configured on the GGSN.

The following is the typical call flow with regard to external AAA servers when a virtual APN is involve:

1. The GGSN receives a Create PDP Context Request that includes a virtual APN. It locates the virtual APN and starts a pre-authentication phase for the PDP context by sending an Access-Request message to an AAA server.
2. The AAA server does a lookup based on the user identification (username, MSISDN, IMSI, etc.) included in the Access-Request message, and determines the target-APN for the user from the user profile. The target APN is returned as a Radius attribute in the Access-Accept message to the GGSN.
3. The GGSN checks for a locally-configured APN that matches the APN name in the target APN attribute in the Access-Accept message.
   - I f a match is found, the virtual APN is resolved and the Create PDP Context Request is redirected to the target APN and is further processed using the target APN (just as if the target APN was included in the original Create PDP Context request). If the real APN is non-transparent, another Access-Request is sent out. Typically, the AAA server should be different.
   - If a match is not found, the Create PDP Context Request is rejected.
   - If there is no target APN included in the RADIUS attribute in the access-accept message to the GGSN, or if the target APN is not locally configured, the Create PDP Context Request is rejected.
4. GGSN receives an access-accept from the AAA server for the second round of authentication.

Restrictions of the Pre-authentication-based Virtual APN Feature

In addition to the restrictions listed in the "General Restrictions of the Virtual APN Feature" section on page 9-34, when configuring pre-authentication-based virtual APN functionality:

- If a user profile on the AAA server is configured to include a target APN, then the target APN should be a real APN, and it should be configured on the GGSN.
- An APN can only be configured for domain-based virtual APN functionality or pre-authentication-based APN functionality, not both.
- The target APN returned from AAA must be a real APN, and if more than one APN is returned, the first one is used and the rest ignored.
- Configure anonymous user access under the virtual APN (using the **anonymous user** command in access-point configuration mode) to mobile stations (MS) to access without supplying the username and password (the GGSN uses the common password configured on the APN).
- At minimum, an AAA access-method must be configured under the virtual APN, or globally. If a method is not configured, the create PDP request will be rejected.

Virtual Access Point Configuration Task List

To configure the GGSN to support virtual APN access, you must configure one or more virtual access points. You also need to configure the real access points that provide the information required for connecting to the physical networks of the external PDNs or VPNs.

In addition to the configuring the GGSN, you must also ensure proper provisioning of other GPRS/UMTS network entities as appropriate to successfully implement the virtual APN feature on the GPRS/UMTS network.

To configure virtual APN access on the GGSN, perform the following tasks:

- Configuring Virtual Access Points on the GGSN, page 9-37 (Required)
- Configuring Real Access Points on the GGSN, page 9-11 (Required)
  - PDN Access Configuration Task List, page 9-12
  - VPN Access Using VRF Configuration Task Lists, page 9-13
- Configuring Other GPRS/UMTS Network Entities With the Virtual APN, page 9-38 (Optional)

For a sample configuration, see the "Virtual APN Configuration Example" section on page 9-56.

Configuring Virtual Access Points on the GGSN

Use virtual access point types to consolidate access to multiple real target networks on the GGSN. Because the GGSN always uses real access points to reach an external network, virtual access points are used in combination with real access points on the GGSN.

You can configure multiple virtual access points on the GGSN. Multiple virtual access points can be used to access the same real networks. One virtual access point can be used to access different real networks.

Note Be sure that you provision the HLR and configure the DNS server to properly correspond to the virtual APN domains that you have configured on the GGSN. For more information, see the "Configuring Other GPRS/UMTS Network Entities With the Virtual APN" section on page 9-38.

To configure a virtual access point on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs access-point-list` *list-name*	Specifies a name for a new access-point list, or references the name of the existing access-point list, and enters access-point list configuration mode.
Step 2	`Router(config-ap-list)# access-point` *access-point-index*	Specifies an index number for a new access point definition, or references an existing access point definition, and enters access point configuration mode.
Step 3	`Router(config-access-point)# access-point-name` *apn-name*	Specifies the network (or domain) name for a PDN that users can access from the GGSN at a defined access point. **Note** The *apn-name* must match the APN that is provisioned at the MS, HLR, and DNS server.
Step 4	`Router (config-access-point)# access-type virtual` [**pre-authenticate** [**default-apn** *apn-name*]]	Specifies an APN type that is not associated with any specific physical target network on the GGSN. Optionally, can be configured to be dynamically mapped, per user, to a target (default) APN. The default access type is real.

Note Even though the Cisco IOS software allows you to configure additional access point options on a virtual access point, none of those access point options will apply if they are configured.

Configuring Other GPRS/UMTS Network Entities With the Virtual APN

When you configure the GGSN to support virtual APN access, be sure that you also meet any necessary requirements for properly configuring other GPRS/UMTS network entities to support the virtual APN implementation.

The following GPRS/UMTS network entities might also require provisioning for proper implementation of virtual APN support:

- DHCP server—Requires configuration of the real APNs.
- DNS server—The DNS server that the SGSN uses to resolve the address of the GGSN must identify the virtual APN with the IP address of the GTP virtual template on the GGSN. If GTP SLB is implemented, then the virtual APN should be associated with the IP address of the GTP load balancing virtual server instance on the SLB router.
- HLR—Requires the name of the virtual APN in subscription data, as allowable for subscribed users.
- RADIUS server—Requires configuration of the real APNs.
- SGSN—Requires the name of the virtual APN as the default APN (as desired) when the APN is not provided in user subscription data.

Verifying the Virtual Access Point Configuration

This section describes how to verify that you have successfully configured virtual APN support on the GGSN, and includes the following tasks:

- Verifying the GGSN Configuration, page 9-39
- Verifying Reachability of the Network Through the Virtual Access Point, page 9-43

Verifying the GGSN Configuration

To verify that you have properly configured access points on the GGSN, use the **show running-config** command and the **show gprs access-point** commands.

Note The **gprs access-point-list** command first appears in the output of the **show running-config** command under the virtual template interface, which indicates that the GPRS access point list is configured and is associated with the virtual template. To verify your configuration of specific access points within the GPRS access point list, look further down in the **show** command output where the **gprs access-point-list** command appears again, followed by the individual access point configurations.

Step 1 From privileged EXEC mode, use the **show running-config** command as shown in the following example. Verify the interface configuration and virtual and real access points:

```
Router# show running-config
Building configuration...

Current configuration : 3521 bytes
!
version 12.x
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
! Enable the router for GGSN services
!
service gprs ggsn
!
hostname ggsn
!
ip cef
!
no logging buffered
logging rate-limit console 10 except errors
aaa new-model
aaa group server radius abc
 server 172.18.43.7 auth-port 1645 acct-port 1646
aaa authentication ppp abc group abc
aaa authorization network abc group abc
aaa accounting network abc start-stop group abc

!
ip subnet-zero
!
...
!
interface loopback 1
 ip address 10.40.40.3 255.255.255.0
!
```

```
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list gprs
!
...
!
gprs access-point-list gprs
!
! Configure a domain-based virtual access point called corporate
!
 access-point 1
   access-point-name corporate
   access-type virtual
   exit
!
! Configure three real access points called corporatea.com,
! corporateb.com, and corporatec.com
!
 access-point 2
   access-point-name corporatea.com
   access-mode non-transparent
   aaa-group authentication abc
   exit
!
 access-point 3
   access-point-name corporateb.com
   exit
   !
 access-point 4
   access-point-name corporatec.com
   access-mode non-transparent
   aaa-group authentication abc
   exit
   !
! Configure a pre-authentication-based virtual access point called virtual-apn-all
!
 access-point 5
   access-point-name virtual-apn-all
   access-mode non-transparent
   access-type virtual pre-authenticate default-apn a1b1c1.com
   anonymous user anyone 1z1z1z
   radius attribute user-name msisdn
   exit
!
gprs maximum-pdp-context-allowed 90000
gprs gtp path-echo-interval 0
gprs default charging-gateway 10.15.15.1
!
gprs memory threshold 512
radius-server host 172.18.43.7 auth-port 1645 acct-port 1646 non-standard
radius-server retransmit 3
radius-server key 7 12150415
call rsvp-sync
!
no mgcp timer receive-rtcp
!
mgcp profile default
!
gatekeeper
 shutdown
!
end
```

Step 2 To view the configuration of a specific access point on the GGSN in further detail, use the **show gprs access-point** command and specify the index number of the access point, as shown in the following examples.

The following output shows information about a real access point:

```
Router# show gprs access-point 2
    apn_index 2          apn_name = corporatea.com
    apn_mode: non-transparent
    apn-type: Real
    accounting: Disable
    wait_accounting: Disable
    dynamic_address_pool: not configured
    apn_dhcp_server: 0.0.0.0
    apn_dhcp_gateway_addr: 0.0.0.0
    apn_authentication_server_group: abc
    apn_accounting_server_group:
    apn_username: , apn_password:
    subscribe_required: No
    deactivate_pdp_context_on violation: No
    network_activation_allowed: No
    Block Foreign-MS Mode: Disable
    VPN: Disable
    GPRS vaccess interface: Virtual-Access1
    number of ip_address_allocated 0

    Total number of PDP in this APN :1

    aggregate:
    In APN:    Disable

    In Global: Disable
```

The following output shows information about a virtual access point:

```
Router# show gprs access-point 1
    apn_index 1          apn_name = corporate
    apn_mode: transparent
    apn-type: Virtual
    accounting: Disable
    wait_accounting: Disable
    dynamic_address_pool: not configured
    apn_dhcp_server: 0.0.0.0
    apn_dhcp_gateway_addr: 0.0.0.0
    apn_authentication_server_group:
    apn_accounting_server_group:
    apn_username: , apn_password:
    subscribe_required: No
    deactivate_pdp_context_on violation: No
    network_activation_allowed: No
    Block Foreign-MS Mode: Disable
    VPN: Disable
    GPRS vaccess interface: Virtual-Access2
    number of ip_address_allocated 0

    Total number of PDP in this APN :0

    aggregate:
    In APN:    Disable

    In Global: Disable
```

The following output shows information about a pre-authentication-based virtual access point that is configured to be dynamically mapped to a default APN named a1b1c1.com:

```
Router# show gprs access-point 5
    apn_index 1          apn_name = corporate
    apn_mode: non-transparent
    apn-type: Virtual pre-authenticate default-apn a1b1c1.com
    accounting: Disable
    interim newinfo accounting: Disable
    interim periodic accounting: Enable (20 minutes)
    wait_accounting: Disable
    input ACL: None, output ACL: None
    dynamic_address_pool: not configured
    apn_dhcp_server: 0.0.0.0
    apn_dhcp_gateway_addr: 0.0.0.0
    apn_authentication_server_group:
    apn_accounting_server_group:
    apn_username: , apn_password:
    subscribe_required: No
    deactivate_pdp_context_on violation: No
    network_activation_allowed: No
    Block Foreign-MS Mode: Disable
    VPN: Disable
    GPRS vaccess interface: Virtual-Access2
    number of ip_address_allocated 0

    Total number of PDP in this APN :0

    aggregate:
    In APN:    Disable

    In Global: Disable
```

Step 3 To view a summary of every access point that is configured on the GGSN, use the **show gprs access-point all** command as shown in the following example:

```
Router# show gprs access-point all

There are 4 Access-Points configured

Index   Mode            Access-type    AccessPointName      VRF Name
-------------------------------------------------------------------------
1       transparent        Virtual    corporate
-------------------------------------------------------------------------
2       non-transparent    Real       corporatea.com
-------------------------------------------------------------------------
3       transparent        Real       corporateb.com
-------------------------------------------------------------------------
4       non-transparent    Real       corporatec.com
-------------------------------------------------------------------------
```

Verifying Reachability of the Network Through the Virtual Access Point

To verify reachability of the real destination network through the virtual access point, you can use the same procedure described in the "Verifying Reachability of the Network Through the Access Point" section on page 9-31.

In addition, you should meet the following guidelines for virtual access point testing:

- When you initiate PDP context activation at the MS, be sure that the username that you specify (in the form of login@domain in the Create PDP Context request) corresponds to a real APN that you have configured on the GGSN.
- When you generate traffic to the network, be sure to select a host on one of the real destination networks that is configured for APN support on the GGSN.

Configuring Access to External Support Servers

You can configure the GGSN to access external support servers to provide services for dynamic IP addressing of MSs using the Dynamic Host Configuration Protocol (DHCP) or using Remote Authentication Dial-In User Service (RADIUS). You can also configure RADIUS services on the GGSN to provide security, such as authentication of users accessing a network at an APN.

The GGSN allows you to configure access to DHCP and RADIUS servers globally for all access points, or to specific servers for a particular access point. For more information about configuring DHCP on the GGSN, see the "Configuring Dynamic Addressing on the GGSN" chapter. For more information about configuring RADIUS on the GGSN, see the "Configuring Security on the GGSN" chapter.

Blocking Access to the GGSN by Foreign Mobile Stations

This section describes how to restrict access to the GGSN from mobile stations outside their home PLMN. It includes the following topics:

- Overview of Blocking Foreign Mobile Stations, page 9-43
- Blocking Foreign Mobile Stations Configuration Task List, page 9-44

Overview of Blocking Foreign Mobile Stations

The GGSN allows you to block access by mobile stations that are outside of the PLMN. When you enable blocking of foreign mobile stations, the GGSN determines whether an MS is inside or outside of the PLMN, based on the mobile country code (MCC) and mobile network code (MNC). You must specify the MCC and MNC codes on the GGSN to properly configure the home public land mobile network (HPLMN) values.

When you enable the blocking foreign MS access feature on the access point, then whenever the GGSN receives a Create PDP Context request, the GGSN compares the MCC and MNC in the TID against the home operator codes that you configure on the GGSN. If the MS mobile operator code fails the matching criteria on the GGSN, then the GGSN rejects the Create PDP Context request.

Blocking Foreign Mobile Stations Configuration Task List

To implement blocking of foreign mobile stations on the GGSN, you must enable the function and specify the supporting criteria for determining whether an MS is outside its home PLMN.

To configure blocking of foreign mobile stations on the GGSN, perform the following tasks:

- Configuring the MCC and MNC Values, page 9-44 (Required)
- Enabling Blocking of Foreign Mobile Stations on the GGSN, page 9-45 (Required)
- Verifying the Blocking of Foreign Mobile Stations Configuration, page 9-45

Configuring the MCC and MNC Values

The MCC and MNC together identify a public land mobile network (PLMN). The values that you configure using the **gprs mcc mnc** command without the **trusted** keyword option specified, are those of the home PLMN ID, which is the PLMN to which the GGSN belongs.

Only one home PLMN can be defined for a GGSN at a time. The GGSN compares the IMSI in Create PDP Context requests with the values configured using this command to determine if a request is from a foreign MS.

You can also configure up to 5 *trusted* PLMNs by specifying the **trusted** keyword when issuing the **gprs mcc mnc** command. A Create PDP Context request from an MS in a trusted PLMN is treated the same as a Create PDP Context request from an MS in the home PLMN.

To configure the MCC and MNC values that the GGSN uses to determine whether a request is from a roaming MS, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs mcc mcc-num mnc mnc-num [trusted]`	Configures the mobile country code and mobile network node that the GGSN uses to determine whether a Create PDP Context request is from a foreign MS. Optionally, use the **trusted** keyword to define up to 5 trusted PLMNs. **Note** The Create PDP Context requests from a trusted PLMN are treated the same as those from the home PLMN.

Note The GGSN automatically specifies values of 000 for the MCC and MNC. However, you must configure non-zero values for both the MCC and MNC before you can enable the GGSN to create CDRs for roamers.

Enabling Blocking of Foreign Mobile Stations on the GGSN

To enable the GGSN to block foreign mobile stations from establishing PDP contexts, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# block-foreign-ms`	Restricts GGSN access at a particular access point based on the mobile user's HPLMN.

Note The MCC and MNC values that are used to determine whether a request is from a roaming MS must be configured before the GGSN can be enabled to block foreign mobile stations.

Verifying the Blocking of Foreign Mobile Stations Configuration

This section describes how to verify the blocking of foreign mobile stations configuration on the GGSN. It includes the following topics:

- Verifying Blocking of Foreign Mobile Stations at an Access Point, page 9-45
- Verifying the MCC and MNC Configuration on the GGSN, page 9-46

Verifying Blocking of Foreign Mobile Stations at an Access Point

To verify whether the GGSN is configured to support blocking of foreign mobile stations at a particular access point, use the **show gprs access-point** command. Observe the value of the Block Foreign-MS Mode output field as shown in bold in the following example:

```
Router# show gprs access-point 1
    apn_index 1          apn_name = gprs.corporate.com
    apn_mode: transparent
    apn-type: Real
    accounting: Disable
    interim newinfo accounting: Disable
    interim periodic accounting: Enable (20 minutes)
    wait_accounting: Disable
    input ACL: None, output ACL: None
    dynamic_address_pool: dhcp-proxy-client
    apn_dhcp_server: 10.99.100.5
    apn_dhcp_gateway_addr: 10.27.1.1
    apn_authentication_server_group: abc
    apn_accounting_server_group: abc1
    apn_username: , apn_password:
    subscribe_required: No
    deactivate_pdp_context_on violation: Yes
    network_activation_allowed: Yes
    Block Foreign-MS Mode: Enable
    VPN: Enable  (VRF Name : vpn1)
    GPRS vaccess interface: Virtual-Access2
    number of ip_address_allocated 0
```

```
Total number of PDP in this APN :0

aggregate:
In APN:    auto

In Global: 30.30.0.0/16
           21.21.0.0/16
```

Verifying the MCC and MNC Configuration on the GGSN

To verify the configuration elements that the GGSN uses as matching criteria to determine whether a request is coming from a foreign mobile station, use the **show gprs plmn** privileged EXEC command. Observe the values of the output fields shown in bold in the following example. The example shows that the GGSN is configured for the USA country code (310) and for the Bell South network code (15) and four trusted PLMNs have been configured:

```
Router# show gprs plmn
Home PLMN
  MCC = 302  MNC = 678
Trusted PLMN
  MCC = 346  MNC = 123
  MCC = 234  MNC = 67
  MCC = 123  MNC = 45
  MCC = 100  MNC = 35
```

Controlling Access to the GGSN by MSs with Duplicate IP Addresses

An MS cannot have the same IP address as another GPRS/UMTS network entity. You can configure the GGSN to reserve certain IP address ranges for use by the GPRS/UMTS network, and to disallow them from use by an MS.

During a Create PDP Context request, the GGSN verifies whether the IP address of an MS falls within the specified excluded range. If there is an overlap of the MS IP address with an excluded range, then the Create PDP Context request is rejected. This measure prevents duplicate IP addressing in the network.

You can configure up to 100 IP address ranges. A range can be one or more addresses. However, you can configure only one IP address range per command entry. To exclude a single IP address, you can repeat the IP address in the start-ip and end-ip arguments. IP addresses are 32-bit values.

Note On the Cisco 7600 series router platform, identical configurations must exist on each GGSN that is load-balanced by means of a virtual server.

To reserve IP address ranges for use by the GPRS/UMTS network and block their use by an MS, use the following command in global configuration mode:

Command	Purpose
Router(config)# **gprs ms-address exclude-range** *start-ip end-ip*	Specifies the IP address ranges used by the GPRS/UMTS network, and thereby excluded from the MS IP address range.

Configuring Routing Behind the Mobile Station under an APN

The routing behind the MS feature enables the routing of packets to IPv4 addresses that do not belong to the PDP context (the MS), but exist behind it. The network address of the destination can be different than the MS address.

Before enabling routing behind the MS, the following requirements must be met:

- The MS must use RADIUS for authentication and authorization.
- The Framed-Route (attribute 22) as defined in Internet Engineering Task Force (IETF) standard RFC 2865, must be configured in the profile of a user and contain at least one route, and up to 16 routes for each MS that is to use the routing behind the MS feature.

  When configured, the Framed-Route attribute is automatically downloaded to the GGSN during the RADIUS authentication and authorization phase of the PDP context creation. If routing behind the MS has not been enabled using the **network-behind-mobile** command in access-point configuration mode, the GGSN ignores the Framed-Route attribute.

  When the MS session is no longer active, the routes are deleted.
- For PPP Regen or PPP with L2TP sessions, the Framed-Route attribute must be configured in the RADIUS server of the LNS.
- For PPP Regen sessions, if the **security verify source** command is configure, the Framed-Route attribute must also be configured in the user profile in the GGSN RADIUS server.
- Static routes are not configured. The configuration of the routing behind the mobile station feature (Framed Route, attribute 22) and static routes at the same time is not supported.

Enabling Routing Behind the Mobile Station

To enable routing behind an MS, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# network-behind-mobile [max-subnets number]`	Enables an access point to support routing behind an MS. Optionally, specifies the maximum number of subnets permitted behind the MS. The valid values is a number between 1 and 16.

Note The routing behind an MS is supported only for IPv4 PDP contexts.

Packets routed behind the MS share the same 3GPP QoS settings of the MS.

Use the **show ip route** command in privileged EXEC mode to view the current state of the routing table. To display a list of currently active mobile sessions, use the **show pdp** command.

Verifying the Routing Behind the Mobile Station Configuration

To verify the routing behind the mobile station configuration, use the following **show** commands.

Step 1 From privileged EXEC mode, use the **show gprs gtp pdp-context tid** and **show ip route** commands to view the framed route and the static route added for the framed route that uses the IP address of the PDP context as the gateway address:

```
Router#show gprs gtp pdp-context tid 1234567809000010
TID              MS Addr               Source  SGSN Addr       APN
1234567809000010 83.83.0.1             Static  2.1.1.1         ippdp1

    current time :Feb 09 2004 12:52:49
    user_name (IMSI):214365879000000    MS address:83.83.0.1
    MS International PSTN/ISDN Number (MSISDN):123456789
    sgsn_addr_signal:2.1.1.1            sgsn_addr_data:  2.1.1.1
    control teid local: 0x637F00EC
    control teid remote:0x01204611
    data teid local:    0x637DFF04
    data teid remote:   0x01204612
    primary pdp:Y           nsapi:1
    signal_sequence: 11                 seq_tpdu_up:     0
    seq_tpdu_down:   0
    upstream_signal_flow:  0            upstream_data_flow:  0
    downstream_signal_flow:0            downstream_data_flow:0
    RAupdate_flow:         0
    pdp_create_time:  Feb 09 2004 12:50:41
    last_access_time: Feb 09 2004 12:50:41
    mnrgflag:         0                 tos mask map:00
    gtp pdp idle time:72
    gprs qos_req:000000               canonical Qos class(reg.):03
    gprs qos_neg:000000               canonical Qos class(neg.):03
    effective bandwidth:0.0
    rcv_pkt_count:    0             rcv_byte_count:  0
    send_pkt_count:   0             send_byte_count: 0
    cef_up_pkt:       0             cef_up_byte:     0
    cef_down_pkt:     0             cef_down_byte:   0
    cef_drop:         0             out-sequence pkt:0
    charging_id:        736730069
    pdp reference count:2
    primary dns:        0.0.0.0
    secondary dns:      0.0.0.0
    primary nbns:       0.0.0.0
    secondary nbns:     0.0.0.0
    ntwk_init_pdp:      0
    Framed_route 5.5.5.0 mask 255.255.255.0
Router#

Router#show ip route
Codes:C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
C    2.0.0.0/8 is directly connected, FastEthernet6/0
     5.0.0.0/24 is subnetted, 1 subnets
U       5.5.5.0 [1/0] via 83.83.0.1
     83.0.0.0/32 is subnetted, 1 subnets
```

```
U       83.83.0.1 [1/0] via 0.0.0.0, Virtual-Access2
     8.0.0.0/32 is subnetted, 1 subnets
C       8.8.0.1 is directly connected, Loopback0
Router#

Router#show ip route vrf vpn4

Routing Table:vpn4
Codes:C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     80.0.0.0/16 is subnetted, 1 subnets
C       80.1.0.0 is directly connected, FastEthernet3/0
     5.0.0.0/24 is subnetted, 1 subnets
U       5.5.5.0 [1/0] via 123.123.123.123
     123.0.0.0/32 is subnetted, 1 subnets
U       123.123.123.123 [1/0] via 0.0.0.0, Virtual-Access9
Router#
```

Step 2 From privileged EXEC mode, use the **show gprs gtp statistics** command to view network-behind-mobile-station statistics (displayed in bold in the following example):

```
Router#show gprs gtp statistics
GPRS GTP Statistics:
  version_not_support        0            msg_too_short              0
  unknown_msg                0            unexpected_sig_msg         0
  unexpected_data_msg        0            unsupported_comp_exthdr    0
  mandatory_ie_missing       0            mandatory_ie_incorrect     0
  optional_ie_invalid        0            ie_unknown                 0
  ie_out_of_order            0            ie_unexpected              0
  ie_duplicated              0            optional_ie_incorrect      0
  pdp_activation_rejected    2            tft_semantic_error         0
  tft_syntactic_error        0            pkt_ftr_semantic_error     0
  pkt_ftr_syntactic_error    0            non_existent               0
  path_failure               0            total_dropped              0
  signalling_msg_dropped     0            data_msg_dropped           0
  no_resource                0            get_pak_buffer_failure     0
  rcv_signalling_msg         7            snd_signalling_msg         7
  rcv_pdu_msg                0            snd_pdu_msg                0
  rcv_pdu_bytes              0            snd_pdu_bytes              0
  total created_pdp          3            total deleted_pdp          2
  total created_ppp_pdp      0            total deleted_ppp_pdp      0
  ppp_regen_pending          0            ppp_regen_pending_peak     0
  ppp_regen_total_drop       0            ppp_regen_no_resource      0
  ntwk_init_pdp_act_rej      0            total ntwkInit created pdp 0
GPRS Network behind mobile Statistics:
  network_behind_ms APNs      1          total_download_route       5
  save_download_route_fail    0          insert_download_route_fail 2
  total_insert_download_route 3
```

Configuring Proxy-CSCF Discovery Support under an APN

The GGSN can be configured to return a list of preconfigured Proxy Call Session Control Function (P-CSCF) server addresses for an APN when it receives a Create PDP Context Request that contains a "P-CSCF Address Request" field in the PCO.

The MS sets the P-CSCF Address Request field of the PCO in the Activate PDP Context Request. This request is forwarded to the GGSN in the Create PDP Context Request from the SGSN. Upon receiving, the GGSN returns in the "P-CSCF Address" field of the PCO, all the P-CSCF addresses configured.

If a Create PDP Context Request does not contain the P-CSCF address request field in the PCO, or if no P-CSCF addresses are preconfigured, the Create PDP Context Response will not return any P-CSCF addresses. An error message will not be generated and the Create PDP Context Request will be processed.

Optionally, P-CSCF load balancing can be enabled on the Cisco GGSN.

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

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

Note The order of the addresses returned in the "P-CSCF Address Field" of the PCO is the same as the order in which they are defined in the P-CSCF server group and the groups are associated with the APN.

To enable the P-CSCF Discovery support under an APN, perform the following tasks:

- Creating P-CSCF Server Groups on the GGSN, page 9-50
- Associating a P-CSCF Server Group with an APN, page 9-51

Creating P-CSCF Server Groups on the GGSN

Up to 10 P-CSCF servers can be defined in a P-CSCF server group.

Both IPv6 and IPv4 P-CSCF servers can be defined in a server group. The PDP type dictates to which server the IP addresses are sent.

To configure a P-CSCF server group on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs pcscf group-name`	Configures a P-CSCF server group on the GGSN and enters P-CSCF group configuration mode.
Step 2	`Router(config-pcscf-group)# server [ipv6] ip-address`	Defines an IPv4 P-CSCF server by IP address. Optionally, specify the **ipv6** keyword option to define an IPv6 P-CSCF server in a P-CSCF server group.

Associating a P-CSCF Server Group with an APN

Before associating a P-CSCF group with an APN, the group must be configured globally using the **gprs pcscf** command in global configuration mode.

Note Only one P-CSCF group can be defined per APN, however a P-CSCF group can be associated with multiple APNs.

To associate a P-CSCF server group with an APN, use the following command in access point configuration mode:

Command	Purpose
`Router(config-access-point)# pcscf group-name [load-balance]`	Specifies a P-CSCF server group to use for P-CSCF discovery by an APN. Optionally, specify the **load-balance** keyword to enable P-CSCF load balancing on the APN.

Verifying the P-CSCF Discovery Configuration

Use the following show commands to verify the P-CSCF Discovery configuration:

Command	Purpose
`Router# show gprs pcscf`	Displays a summary of the P-CSCF server groups configured on the GGSN.
`Router# show gprs access-point [group-name]`	Displays a summary of the P-CSCF server group or groups configured on the GGSN.

Monitoring and Maintaining Access Points on the GGSN

This section provides a summary list of the **clear** and **show** commands that you can use to monitor access points on the GGSN.

Use the following privileged EXEC commands to monitor and maintain access points on the GGSN:

Command	Purpose
Router# **clear gprs access-point statistics** {*access-point-index* | all}	Clears statistics counters for a specific access point or for all access points on the GGSN.
Router# **clear gprs gtp pdp-context pdp-type** [**ipv6** | **ipv4**]	clear all packet data protocol (PDP) contexts (mobile sessions) that are IP version 4 (IPv4) or IP version 6 (IPv6) PDPs
Router# **show gprs access-point** {*access-point-index* | **all**}	Displays information about access points on the GGSN.
Router# **show gprs access-point statistics** {*access-point-index* | **all**}	Displays data volume and PDP activation and deactivation statistics for access points on the GGSN.
Router# **show gprs access-point-name status**	Displays the number of active PDPs on an access point, and how many of those PDPs are IPv4 PDPs and how many are IPv6 PDPs.
Router# **show gprs gtp pdp-context** {**tid** *tunnel_id* [service [all | id *id_string*]] | ms-address *ip_address* [**access-point** *access-point-index*] | **imsi** *imsi* [**nsapi** *nsapi* [**tft**]] | **path** *ip-address* [*remote-port-num*] | **access-point** *access-point-index* | **pdp-type** {**ip** [**v6** | **v4**] | **ppp**} | **qos-umts-class** {**background** | **conversational** | **interactive** | **streaming**} | **qos-precedence** {**low** | **normal** | **high**} | **qos-delay** {**class1** | **class2** | **class3** | **classbesteffort**} | **version** *gtp-version*} | **msisdn** [*msisdn*] **detail** | **ms-ipv6-addr** *ipv6-address* | **all**}	Displays a list of the currently active PDP contexts (mobile sessions).
Router# **show gprs gtp statistics**	Displays the current GTP statistics for the gateway GGSN (such as IE, GTP signaling, and GTP PDU statistics).
Router# **show gprs gtp status**	Displays information about the current status of the GTP on the GGSN.

Configuration Examples

This section includes the following configuration examples for configuring different types of network access to the GGSN:

- Static Route to SGSN Example, page 9-53
- Access Point List Configuration Example, page 9-54
- VRF Tunnel Configuration Example, page 9-55
- Virtual APN Configuration Example, page 9-56
- Blocking Access by Foreign Mobile Stations Configuration Example, page 9-59

- Duplicate IP Address Protection Configuration Example, page 9-60
- P-CSCF Discovery Configuration Example, page 9-60

Static Route to SGSN Example

Note For the SGSN to successfully communicate with the GGSN, the SGSN must configure a static route or must be able to dynamically route to the IP address used by the GGSN virtual template.

GGSN Configuration:

```
!
...
!
interface Loopback100
 description GPRS GTP V-TEMPLATE IP ADDRESS
 ip address 9.9.9.72 255.255.255.0
!
interface GigabitEthernet0/0.2
 description Ga/Gn Interface
 encapsulation dot1Q 101
 ip address 10.1.1.72 255.255.255.0
 no cdp enable
!
interface Virtual-Template1
 description GTP v-access
 ip unnumbered Loopback100
 encapsulation gtp
 gprs access-point-list gprs
!
ip route 40.1.2.1 255.255.255.255 10.1.1.1
ip route 40.1.3.10 255.255.255.255 10.1.1.1
ip route 40.2.2.1 255.255.255.255 10.1.1.1
ip route 40.2.3.10 255.255.255.255 10.1.1.1
!
...
!
```

Supervisor Engine Configuration

```
!
...
!
interface FastEthernet8/22
 no ip address
 switchport
 switchport access vlan 302
!
interface FastEthernet9/41
 no ip address
 switchport
 switchport access vlan 303
!
interface Vlan101
 description Vlan to GGSN for GA/GN
 ip address 10.1.1.1 255.255.255.0
!
interface Vlan302
 ip address 40.0.2.1 255.255.255.0
!
```

```
interface Vlan303
 ip address 40.0.3.1 255.255.255.0
!

ip route 9.9.9.72 255.255.255.255 10.1.1.72
ip route 9.9.9.73 255.255.255.255 10.1.1.73
ip route 9.9.9.74 255.255.255.255 10.1.1.74
ip route 9.9.9.75 255.255.255.255 10.1.1.75
ip route 9.9.9.76 255.255.255.255 10.1.1.76
ip route 40.1.2.1 255.255.255.255 40.0.2.11
ip route 40.1.3.10 255.255.255.255 40.0.3.10
ip route 40.2.2.1 255.255.255.255 40.0.2.11
ip route 40.2.3.10 255.255.255.255 40.0.3.10
!
...
!
```

Access Point List Configuration Example

The following example shows a portion of the GGSN configuration for a GPRS access point list:

```
!
interface virtual-template 1
 ip unnumber loopback 1
 no ip directed-broadcast
 encapsulation gtp
 gprs access-point-list abc
!
! Defines a GPRS access point list named abc
! with 3 access points
!
gprs access-point-list abc
 access-point 1
  access-point-name gprs.pdn1.com
  ip-address-pool dhcp-proxy-client
  dhcp-server 10.102.100.3
  dhcp-gateway-address 10.30.30.30
  exit
!
 access-point 2
  access-point-name gprs.pdn2.com
  ip-address-pool dhcp-proxy-client
  dhcp-server 10.60.0.1
  dhcp-gateway-address 10.27.27.27
  exit
!
 access-point 3
  access-point-name www.pdn3.com
  access-mode non-transparent
  dhcp-gateway-address 10.25.25.25
  aaa-group authentication abc
  exit
!
. . .
```

VRF Tunnel Configuration Example

The following examples show a partial configuration for two VPNs (vpn1 and vpn2) and their associated GRE tunnel configurations (Tunnel1 and Tunnel2).

GGSN Configuration

```
service gprs ggsn
!
hostname 7600-7-2
!
ip cef
!
ip vrf vpn1
 description GRE Tunnel 1
 rd 100:1
!
ip vrf vpn2
 description GRE Tunnel 3
 rd 101:1
!
interface Loopback1
 ip address 150.1.1.72 255.255.0.0
!
interface Loopback100
 description GPRS GTP V-TEMPLATE IP ADDRESS
 ip address 9.9.9.72 255.255.255.0
!
interface Tunnel1
 description VRF-GRE to PDN 7500(13) Fa0/1
 ip vrf forwarding vpn1
 ip address 50.50.52.72 255.255.255.0
 tunnel source 150.1.1.72
 tunnel destination 165.2.1.13
!
interface Tunnel2
 description VRF-GRE to PDN PDN x(12) Fa3/0
 ip vrf forwarding vpn2
 ip address 80.80.82.72 255.255.255.0
 tunnel source 150.1.1.72
 tunnel destination 167.2.1.12
!
interface GigabitEthernet0/0.1
 description Gi
 encapsulation dot1Q 100
 ip address 10.1.2.72 255.255.255.0
!
interface Virtual-Template1
 description GTP v-access
 ip unnumbered Loopback100
 encapsulation gtp
 gprs access-point-list gprs
!
ip local pool vpn1_pool 100.2.0.1 100.2.255.255 group vpn1
ip local pool vpn2_pool 100.2.0.1 100.2.255.255 group vpn2
ip route vrf vpn1 0.0.0.0 0.0.0.0 Tunnel1
ip route vrf vpn2 0.0.0.0 0.0.0.0 Tunnel2

gprs access-point-list gprs
  access-point 1
   access-point-name apn.vrf1.com
   access-mode non-transparent
   aaa-group authentication ipdbfms
```

```
   ip-address-pool local vpn1_pool
   vrf vpn1
   !
  access-point 2
   access-point-name apn.vrf2.com
   access-mode non-transparent
   aaa-group authentication ipdbfms
   ip-address-pool local vpn2_pool
   vrf vpn2
   !
```

Supervisor Engine Configuration

```
interface FastEthernet9/5
 no ip address
 switchport
 switchport access vlan 167
 no cdp enable
!
interface FastEthernet9/10
 no ip address
 switchport
 switchport access vlan 165
 no cdp enable
!
interface Vlan165
 ip address 165.1.1.1 255.255.0.0
!
interface Vlan167
 ip address 167.1.1.1 255.255.0.0
!
! provides route to tunnel endpoints on GGSNs
!
ip route 150.1.1.72 255.255.255.255 10.1.2.72
!
! routes to tunnel endpoints on PDN
!
ip route 165.2.0.0 255.255.0.0 165.1.1.13
ip route 167.2.0.0 255.255.0.0 167.1.1.12
```

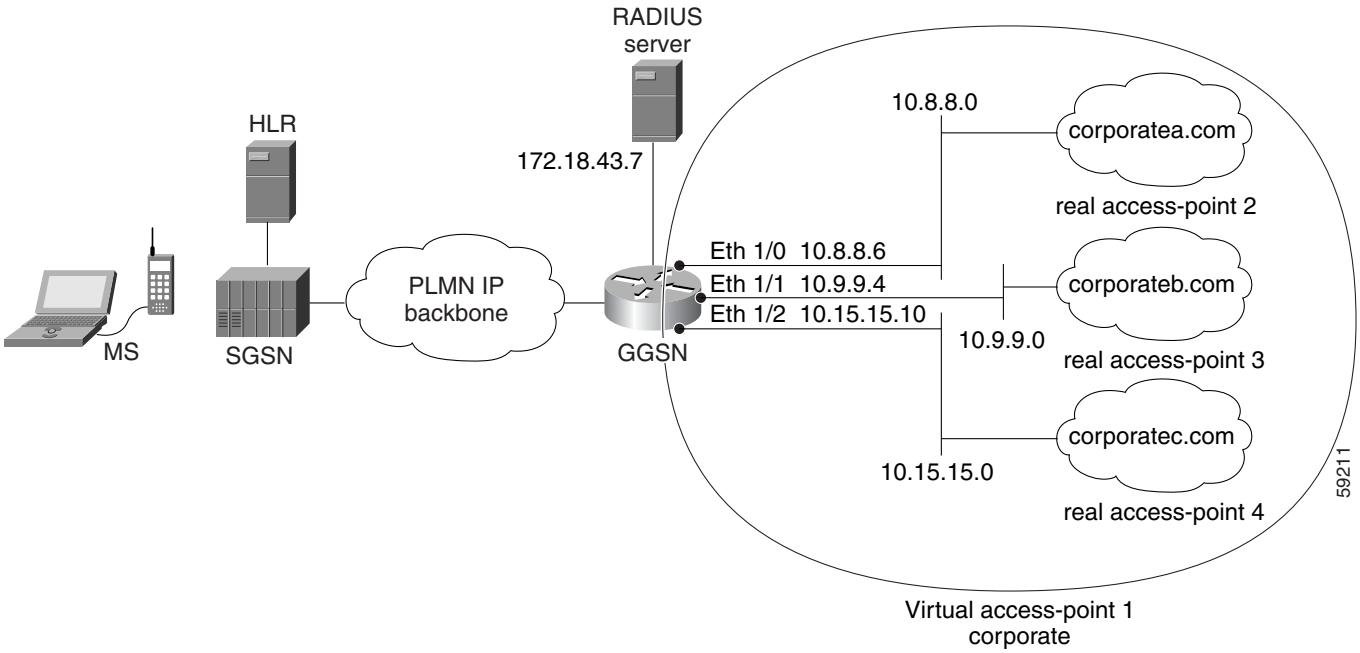
Virtual APN Configuration Example

The following example shows a GGSN that is configured for a virtual APN access point that serves as the focal connection for three different real corporate networks.

Notice the following areas in the GGSN configuration shown in this example:

- Three physical interfaces (Gi interfaces) are defined to establish access to the real corporate networks: Ethernet 1/0, Ethernet 1/1, and Ethernet 1/2.
- Four access points are configured:
  - Access point 1 is configured as the virtual access point with an APN called *corporate*. No other configuration options are applicable at the virtual access point. The “corporate” virtual APN is the APN that is provisioned at the HLR and DNS server.
  - Access points 2, 3, and 4 are configured to the real network domains: corporatea.com, corporateb.com, and corporatec.com. The real network domains are indicated in the PCO of the PDP context request.

Figure 9-2 Virtual APN Configuration Example



GGSN Configuration

```
!
version 12.x
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
! Enable the router for GGSN services
!
service gprs ggsn
!
hostname ggsn
!
ip cef
!
no logging buffered
logging rate-limit console 10 except errors
aaa new-model
aaa group server radius abc
 server 172.18.43.7 auth-port 1645 acct-port 1646
aaa authentication ppp abc group abc
aaa accounting network abc start-stop group abc

!
ip subnet-zero
!
!
no ip dhcp-client network-discovery
!
!
interface Loopback1
 ip address 10.2.3.4 255.255.255.255
!
```

```
interface FastEthernet0/0
 ip address 172.18.43.174 255.255.255.240
 duplex half
!
interface GigabitEthernet2/0
 description Gn interface
 ip address 192.168.10.56 255.255.255.0
!
! Define Gi physical interfaces to real networks
!
interface Ethernet1/0
 description Gi interface to corporatea.com
 ip address 10.8.8.6 255.255.255.0
 no ip mroute-cache
 duplex half
!
interface Ethernet1/1
 description Gi interface to corporateb.com
 ip address 10.9.9.4 255.255.255.0
 no ip mroute-cache
 duplex half
!
interface Ethernet1/2
 description Gi interface to corporatec.com
 ip address 10.15.15.10 255.255.255.0
 no ip mroute-cache
 duplex half
!
interface loopback 1
 ip address 10.40.40.3 255.255.255.0
!
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list gprs
!
ip default-gateway 172.18.43.161
ip kerberos source-interface any
ip classless
ip route 10.7.7.0 255.255.255.0 10.8.8.2
ip route 10.21.21.0 255.255.255.0 Ethernet1/1
ip route 10.102.82.0 255.255.255.0 172.18.43.161
ip route 192.168.1.1 255.255.255.255 FastEthernet2/0
ip route 172.18.0.0 255.255.0.0 172.18.43.161
no ip http server
!
gprs access-point-list gprs
!
! Configure a virtual access point called corporate
!
 access-point 1
   access-point-name corporate
   access-type virtual
   exit
!
! Configure three real access points called corporatea.com,
! corporateb.com, and corporatec.com
!
 access-point 2
   access-point-name corporatea.com
   access-mode non-transparent
   aaa-group authentication abc
   exit
 access-point 3
```

```
   access-point-name corporateb.com
   access-mode transparent
   ip-address-pool dhcp-client
   dhcp-server 10.21.21.1
   exit
   !
 access-point 4
   access-point-name corporatec.com
   access-mode non-transparent
   aaa-group authentication abc
   exit
   !
 !
gprs maximum-pdp-context-allowed 90000
gprs gtp path-echo-interval 0
gprs default charging-gateway 10.15.15.1
!
gprs memory threshold 512
!
radius-server host 172.18.43.7 auth-port 1645 acct-port 1646 non-standard
radius-server retransmit 3
radius-server key 7 12150415
call rsvp-sync
!
no mgcp timer receive-rtcp
!
mgcp profile default
!
!
gatekeeper
 shutdown
!
end
```

Blocking Access by Foreign Mobile Stations Configuration Example

The following example shows a partial configuration in which access point 100 blocks access by foreign mobile stations:

```
!
version 12.x
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
! Enables the router for GGSN services
!
service gprs ggsn
!
hostname ggsn
!
ip cef
!
gprs access-point-list gprs
!
access-point 100
 access-point-name blocking
!
! Enables blocking of MS to APN 100
! that are outside ! of the PLMN
```

```
!
 block-foreign-ms
exit
!
. . .
!
! Configures the MCC and MNC codes
!
gprs mcc 123 mnc 456
```

Duplicate IP Address Protection Configuration Example

The following example shows a partial configuration that specifies three different sets of IP address ranges used by the GPRS/UMTS network (which are thereby excluded from the MS IP address range):

```
gprs ms-address exclude-range 10.0.0.1 10.20.40.50
gprs ms-address exclude-range 172.16.150.200 172.30.200.255
gprs ms-address exclude-range 192.168.100.100 192.168.200.255
```

P-CSCF Discovery Configuration Example

The following example shows a partial configuration in which P-CSCF server groups have been configured on the GGSN and one is assigned to an access point:

```
!
version 12.x
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
! Enables the router for GGSN services
!
service gprs ggsn
!
hostname ggsn
!
ip cef
!
gprs pcscf groupA
server 172.10.1.1
server 10.11.1.2
server ipv6 2001:999::9
!
gprs pcscf groupB
server 172.20.2.1
server 10.21.2.2
gprs access-point-list gprs
!
access-point 100
access-point-name pcscf
pcscf groupA
!
```

CHAPTER 10

Configuring PPP Support on the GGSN

The gateway GPRS support node (GGSN) supports the GPRS tunneling protocol (GTP) with the Point to Point Protocol (PPP) in three different ways. The different types of PPP support on the GGSN are differentiated by where the PPP endpoints occur within the network, whether Layer 2 Tunneling Protocol (L2TP) is in use, and where IP packet service occurs. This chapter describes the different methods of PPP support on the GGSN and how to configure those methods.

For complete descriptions of the GGSN commands in this chapter, see *Cisco GGSN Command Reference* for the Cisco GGSN release you are using. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

This chapter includes the following sections:

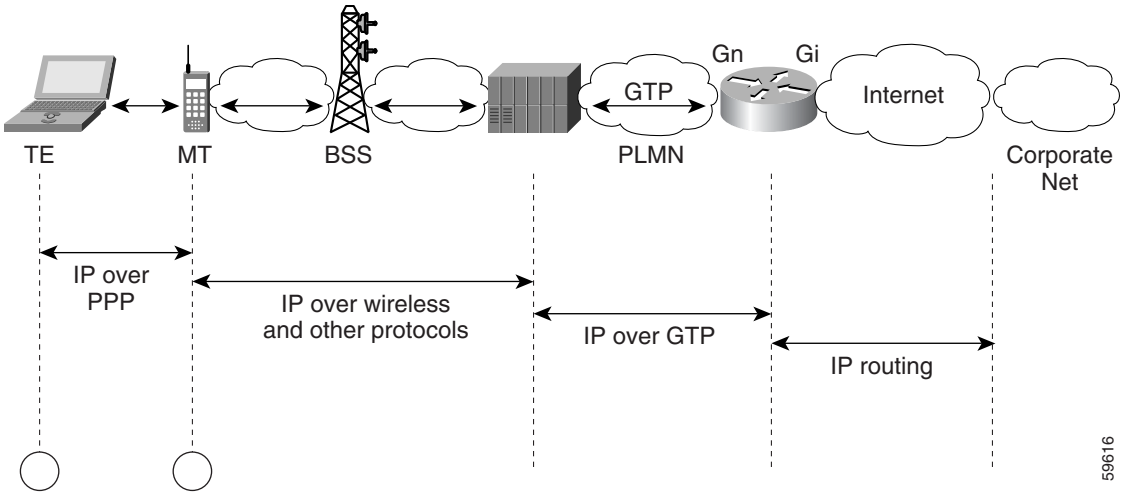
- Overview of PPP Support on the GGSN, page 10-1
- Configuring GTP-PPP Termination on the GGSN, page 10-3
- Configuring GTP-PPP with L2TP on the GGSN, page 10-7
- Configuring GTP-PPP Regeneration on the GGSN, page 10-14
- Monitoring and Maintaining PPP on the GGSN, page 10-21
- Configuration Examples, page 10-22

Overview of PPP Support on the GGSN

Before GGSN Release 3.0, the GGSN supported a topology of IP over PPP between the terminal equipment (TE) and mobile termination (MT). Only IP packet services and routing were supported from the MT through the serving GPRS support node (SGSN), over the Gn interface and the GTP tunnel to the GGSN, and over the Gi interface to the corporate network. No PPP traffic flow was supported over the GTP tunnel or between the GGSN and the corporate network.

Figure 10-1 shows the implementation of IP over GTP without any PPP support within a GPRS network.

Figure 10-1 IP Over GTP Topology Without PPP Support on the GGSN



The PPP packet data protocol (PDP) type was added to the GSM standards in GSM 04.08 version 7.4.0 and GSM 09.60 version 7.0.0. PPP is a Layer 2 protocol that is widely used in a variety of WAN environments, including Frame Relay, ATM, and X.25 networks.

PPP provides security checking through the Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP), and it uses the IP Control Protocol (IPCP) sublayer to negotiate IP addresses. Perhaps the most important characteristic of PPP support within the general packet radio service/Universal Mobile Telecommunication System (GPRS/UMTS) network is PPP's tunneling capability through a virtual private data network (VPDN) using L2TP. Tunneling allows PPP sessions to be transported through public networks to a private corporate network, without any security exposure in the process. Authentication and dynamic IP address allocation can be performed at the edge of the corporate network.

The Cisco GGSN provides the following three methods of PPP support on the GGSN:

- GTP-PPP
- GTP-PPP with L2TP
- GTP-PPP Regeneration

Note GTP-PPP and GTP-PPP Regeneration IPv6 PDP contexts are not supported.

Note Under optimal conditions, the GGSN supports 8000 PDP contexts when a PPP method is configured. However, the platform, amount of memory installed, method of PPP support configured, and rate of PDP context creation configured will all affect this number.

The following sections in this chapter describe each method in more detail and describe how to configure and verify each type of PPP support on the GGSN.

Configuring GTP-PPP Termination on the GGSN

This section provides an overview of and describes how to configure PPP over GTP on the GGSN. It includes the following topics:

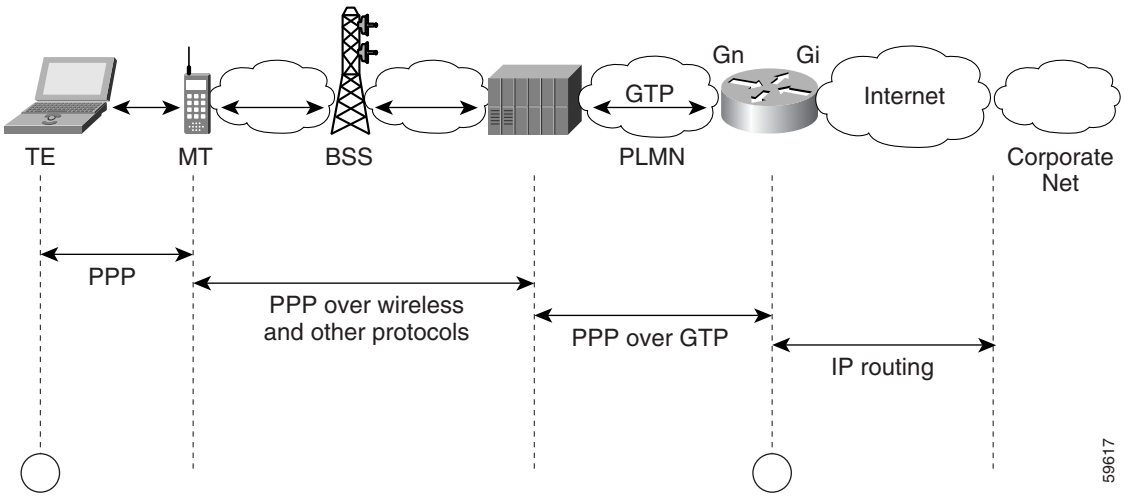
- Overview of GTP-PPP Termination on the GGSN, page 10-3
- Preparing to Configure PPP over GTP on the GGSN, page 10-4
- GTP-PPP Termination Configuration Task List, page 10-4
- GTP-PPP Termination on the GGSN Configuration Examples, page 10-22

Overview of GTP-PPP Termination on the GGSN

The GGSN supports the PPP PDP type over GTP without using L2TP. In this topology, the GGSN provides PPP support from the terminal equipment (TE) and mobile termination (MT) or mobile station (MS) through the SGSN, over the Gn interface and the GTP tunnel to the GGSN. The PPP endpoints are at the terminal equipment (TE) and the GGSN. IP routing occurs from the GGSN over the Gi interface to the corporate network.

Figure 10-2 shows the implementation of PPP over GTP without L2TP support within a GPRS network.

Figure 10-2 PPP Over GTP Topology With PPP Termination at the GGSN



Benefits

PPP over GTP support on the GGSN provides the following benefits:

- Different traffic types can be supported over GTP.
- Authentic negotiation of PPP options can occur for PPP endpoints (no need for proxy PPP negotiation).
- Provides the foundation for GTP to interwork with other PPP networking protocols, such as L2TP.

- Requirements for MT intelligence are simplified, with no need for support of a PPP stack on the MT.
- Additional session security is provided.
- Provides increased flexibility of IP address assignment to the TE.

Preparing to Configure PPP over GTP on the GGSN

Before you begin to configure PPP over GTP support on the GGSN, you need to determine the method that the GGSN will use to allocate IP addresses to users. There are certain configuration dependencies that are based on the method of IP address allocation that you want to support.

Be sure that the following configuration guidelines are met to support the type of IP address allocation in use on your network:

- RADIUS IP address allocation
  - Be sure that users are configured on the RADIUS server using the complete username@domain format.
  - Specify the **no peer default ip address** command at the PPP virtual template interface.
  - For more information about configuring RADIUS services on the GGSN, see the "Configuring Security on the GGSN" chapter in this guide.
- DHCP IP address allocation
  - Be sure that you configure the scope of the addresses to be allocated on the same subnet as the loopback interface.
  - Do not configure an IP address for users on the RADIUS server.
  - Specify the **peer default ip address dhcp** command at the PPP virtual template interface.
  - Specify the **aaa authorization network** *method_list* **none** command on the GGSN.
  - For more information about configuring DHCP services on the GGSN, see the "Configuring Dynamic Addressing on the GGSN" chapter in this guide.
- Local pool IP address allocation
  - Be sure to configure a local pool using the **ip local pool** command.
  - Specify the **aaa authorization network** *method_list* **none** command on the GGSN.
  - Specify the **peer default ip address pool** *pool-name* command.

GTP-PPP Termination Configuration Task List

To configure PPP over GTP support on the GGSN, perform the following tasks:

- Configuring a Loopback Interface, page 10-5 (Recommended)
- Configuring a PPP Virtual Template Interface, page 10-5 (Required)
- Associating the Virtual Template Interface for PPP on the GGSN, page 10-7 (Required)

Configuring a Loopback Interface

We recommend that you configure the virtual template interface as unnumbered, and associate its IP numbering with a loopback interface.

A loopback interface is a software-only interface that emulates an interface that is always up. It is a virtual interface supported on all platforms. The interface-number is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces that you can create. The GGSN uses loopback interfaces to support the configuration of several different features.

To configure a loopback interface on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface loopback interface-number`	Defines a loopback interface on the GGSN, where *interface-number* identifies the loopback interface.
Step 2	`Router(config-if)# ip address ip-address mask [secondary]`	Specifies an IP address for the interface, where: • *ip-address*—Specifies the IP address of the interface in dotted decimal format. • *mask*—Specifies a subnet mask in dotted decimal format. • **secondary**—Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

Configuring a PPP Virtual Template Interface

To support PPP over GTP, you must configure a virtual template interface on the GGSN that supports PPP encapsulation. Therefore, the GGSN will have two virtual template interfaces: one for GTP encapsulation and one for PPP encapsulation. The GGSN uses the PPP virtual template interface to create all PPP virtual access interfaces for PPP sessions on the GGSN.

We recommend that you configure the virtual template interface as unnumbered, and associate its IP numbering with a loopback interface.

Because it is the default, PPP encapsulation does not appear in the **show running-config** output for the interface.

To configure a PPP virtual template interface on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface virtual-template` *number*	Creates a virtual template interface, where *number* identifies the virtual template interface. This command enters you into interface configuration mode. **Note** This number must match the *number* configured in the corresponding **gprs gtp ppp vtemplate** command.
Step 2	`Router(config-if)# ip unnumbered` *type number*	Enables IP processing on the virtual template interface without assigning an explicit IP address to the interface, where *type* and *number* specify another interface for which the router is assigned an IP address. For the GGSN, this can be a Gi interface or a loopback interface. We recommend using a loopback interface.
Step 3	`Router(config-if)# no peer default ip address` (for RADIUS server) or `Router(config-if)# peer default ip address dhcp` (for DHCP server) or `Router(config-if)# peer default ip address pool` *pool-name* (for local pool)	Specifies the prior peer IP address pooling configuration for the interface. If you are using a RADIUS server for IP address allocation, then you need to disable peer IP address pooling.
Step 4	`Router(config-if)# encapsulation ppp`	(Optional) Specifies PPP as the encapsulation type for packets transmitted over the virtual template interface. PPP is the default encapsulation. **Note** PPP is the default encapsulation and does not appear in the output of the **show running-config** command for the virtual template interface unless you manually configure the command.
Step 5	`Router(config-if)# ppp authentication {pap [chap]} [default]`	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface, where • **pap** [**chap**]—Enables PAP, CHAP, or both on the interface. • **default**—Name of the method list created with the **aaa authentication ppp** command.

Associating the Virtual Template Interface for PPP on the GGSN

Before you associate the virtual template interface for PPP, you must configure the virtual template interface. The number that you configure for the virtual template interface must correspond to the number that you specify in the **gprs gtp ppp vtemplate** command.

To associate the virtual template interface for GGSN, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs gtp ppp vtemplate` *number*	Associates the virtual template interface that defines the PPP characteristics with support for the PPP PDP type over GTP on the GGSN. **Note** This number must match the *number* configured in the corresponding **interface virtual-template** command.

Configuring GTP-PPP with L2TP on the GGSN

This section provides an overview of and describes how to configure PPP over GTP with L2TP support on the GGSN. It includes the following topics:

- Overview of GTP-PPP with L2TP on the GGSN, page 10-7
- GTP-PPP With L2TP Configuration Task List, page 10-8

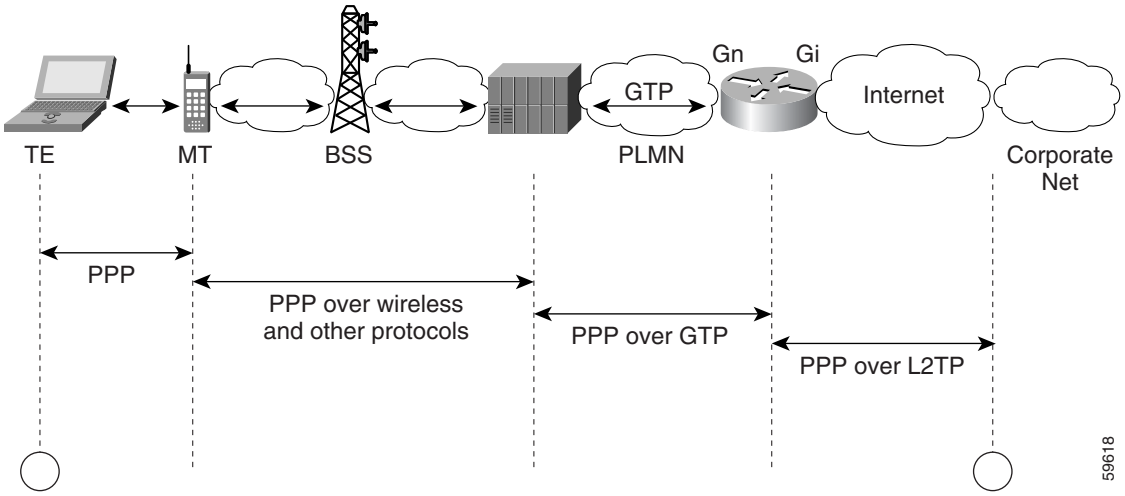
Overview of GTP-PPP with L2TP on the GGSN

The GGSN supports PPP over GTP using L2TP, without IP routing. The GGSN provides PPP support from the TE and MT through the SGSN, over the Gn interface and the GTP tunnel to the GGSN, and over the Gi interface and an L2TP tunnel to the corporate network. In this scenario, the PPP termination endpoints are at the TE and the L2TP network server (LNS) at the corporate network.

With L2TP support, packets are delivered to the LNS by routing L2TP- and PPP-encapsulated IP payload. Without L2TP, pure IP payload is routed to the LNS at the corporate network.

Figure 10-3 shows the implementation of PPP over GTP with L2TP support within a GPRS network.

Figure 10-3 PPP Over GTP With L2TP Topology on the GGSN



Benefits

PPP over GTP with L2TP support on the GGSN provides the following benefits:

- VPN security using L2TP tunnels provides secure delivery of user data over the public network to a corporate network.
- Real end-to-end PPP sessions, with authentication and address negotiation and assignment.
- Corporate networks can retain control over access to their servers and do not need to provide access by the GGSN to those servers.
- Configuration changes on corporate servers can occur without requiring an update to the GGSN.

Restrictions

The GGSN supports PPP over GTP with L2TP with the following restriction:

- At least one PPP authentication protocol must be enabled using the **ppp authentication** command in interface configuration mode.

GTP-PPP With L2TP Configuration Task List

Configuring GTP over PPP with L2TP requires many of the same configuration tasks as those required to configure GTP over PPP without L2TP, with some additional tasks to configure the GGSN as an L2TP access concentrator (LAC) and to configure authentication, authorization, and accounting (AAA) services.

To configure PPP over GTP with L2TP support on the GGSN, perform the following tasks:

- Configuring the GGSN as a LAC, page 10-9 (Required)
- Configuring AAA Services for L2TP Support, page 10-10 (Required)
- Configuring a Loopback Interface, page 10-11 (Recommended)

- Configuring a PPP Virtual Template Interface, page 10-12 (Required)
- Associating the Virtual Template Interface for PPP on the GGSN, page 10-13 (Required)

Configuring the GGSN as a LAC

When you use L2TP services on the GGSN to the LNS in the corporate network, you need to configure the GGSN as a LAC by enabling VPDN services on the GGSN.

For more information about VPDN configuration and commands in the Cisco IOS software, see *Cisco IOS Dial Technologies Configuration Guide* and *Command Reference* publications.

To configure the GGSN as a LAC where the tunnel parameters are configured locally on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# vpdn enable`	Enables VPDN on the router or instance of Cisco IOS software and directs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present. **Note** Only this step is required if you are using a RADIUS server to provide tunnel parameters.
Step 2	`Router(config)# vpdn-group group-number`	Defines a VPDN group, and enters VPDN group configuration mode.
Step 3	`Router(config-vpdn)# request-dialin`	Enables the router or instance of Cisco IOS software to request dial-in tunnels, and enters request dial-in VPDN subgroup configuration mode.
Step 4	`Router(config-vpdn-req-in)# protocol l2tp`	Specifies the L2TP protocol for dial-in tunnels.
Step 5	`Router(config-vpdn-req-in)# domain domain-name`	Specifies that users with this domain name will be tunneled. Configure this command for every domain name you want to tunnel.
Step 6	`Router(config-vpdn-req-in)# exit`	Returns you to VPDN group configuration mode.
Step 7	`Router(config-vpdn)# initiate-to ip ip-address [limit limit-number] [priority priority-number]`	Specifies the destination IP address for the tunnel.
Step 8	`Router(config-vpdn)# local name name`	Specifies the local name that is used to authenticate the tunnel.

Note You can configure the L2TP tunnel parameters locally on the GGSN, or the tunnel parameters can be provided by a RADIUS server. If a RADIUS server is providing the tunnel parameters, then in this procedure you only need to configure the **vpdn enable** command on the GGSN.

Configuring AAA Services for L2TP Support

Before the VPDN stack on the GGSN opens an L2TP tunnel to an LNS, it tries to authorize the tunnel first. The GGSN consults its local database to perform this authorization. Therefore, you need to configure the appropriate AAA services for the GGSN to support L2TP tunnel authorization. Note that this is for authorization of the tunnel itself—not for user authorization.

This section describes only those commands required to implement authorization for L2TP support on the GGSN. It does not describe all of the tasks required to configure RADIUS and AAA support on the GGSN. For more information about enabling AAA services and configuring AAA server groups on the GGSN, see the "Configuring Security on the GGSN" chapter in this book.

Note To correctly implement authentication and authorization services on the GGSN for L2TP support, you must configure the same methods and server groups for both.

To configure authorization for L2TP support on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa authorization network default local`	(Optional) Specifies that the GGSN consults its local database, as defined by the **username** command, for tunnel authorization.

	Command	Purpose
Step 2	`Router(config)# aaa authorization network {default | list-name} group group-name [group group-name...]`	Specifies one or more AAA methods for use on interfaces running PPP, where: • **network**—Runs authorization for all network-related service requests, including SLIP1, PPP2, PPP NCPs3, and ARA4. • **default**—Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in. • *list-name*—Specifies the character string used to name the list of authentication methods tried when a user logs in. • **group** *group-name*—Uses a subset of RADIUS servers for authentication as defined by the **aaa group server radius** command. **Note** Be sure to use a method list and do not use the **aaa authorization network default group radius** form of the command. For L2TP support, the *group-name* must match the group that you specify in the **aaa authentication ppp** command.
Step 3	`Router(config)# username name password secret`	Specifies the password to use in CHAP caller identification, where *name* is the name of the tunnel. **Note** Usernames in the form of *ciscouser*, *ciscouser@corporate1.com*, and *ciscouser@corporate2.com* are considered to be three different entries. Repeat this step to add a username entry for each remote system from which the local router or access server requires authentication.

Note You can configure the L2TP tunnel parameters locally on the GGSN, or the tunnel parameters can be provided by a RADIUS server. If a RADIUS server is providing the tunnel parameters, then in this procedure you only need to configure the **username** command on the GGSN.

Configuring a Loopback Interface

We recommend that you configure the virtual template interface as unnumbered and that you associate its IP numbering with a loopback interface.

A loopback interface is a software-only interface that emulates an interface that is always up. It is a virtual interface supported on all platforms. The interface number is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces you can create. The GGSN uses loopback interfaces to support the configuration of several different features.

To configure a loopback interface on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface loopback` *interface-number*	Defines a loopback interface on the GGSN, where *interface-number* identifies the loopback interface.
Step 2	`Router(config-if)# ip address` *ip-address mask* [**secondary**]	Specifies an IP address for the interface, where: • *ip-address*—Specifies the IP address of the interface in dotted decimal format. • *mask*—Specifies a subnet mask in dotted decimal format. • **secondary**—Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

Note IP addresses on the loopback interface are needed only for PPP PDPs that are not using L2TP. We recommend using IP addresses when PPP PDPs are destined to a domain that is not configured with L2TP.

Configuring a PPP Virtual Template Interface

To support PPP over GTP, you must configure a virtual template interface on the GGSN that supports PPP encapsulation. Therefore, the GGSN will have two virtual template interfaces: one for GTP encapsulation and one for PPP encapsulation. The GGSN uses the PPP virtual template interface to create all PPP virtual access interfaces for PPP sessions on the GGSN.

Note If you are planning to support both GTP-PPP and GTP-PPP-L2TP (PPP PDPs with and without L2TP support), then you must use the same virtual template interface for PPP.

We recommend that you configure the virtual template interface as unnumbered and that you associate its IP numbering with a loopback interface.

Because PPP is the default encapsulation, it does not need to be explicitly configured, and it does not appear in the **show running-config** output for the interface.

To configure a PPP virtual template interface on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface virtual-template number`	Creates a virtual template interface, where *number* identifies the virtual template interface. This command enters you into interface configuration mode. **Note** This number must match the *number* configured in the corresponding **gprs gtp ppp vtemplate** command.
Step 2	`Router(config-if)# ip unnumbered type number`	Enables IP processing on the virtual template interface without assigning an explicit IP address to the interface, where *type* and *number* specify another interface for which the router is assigned an IP address. For the GGSN, this can be a Gi interface or a loopback interface. Cisco recommends using a loopback interface.
Step 3	`Router(config-if)# encapsulation ppp`	Specifies PPP as the encapsulation type for packets transmitted over the virtual template interface. PPP is the default encapsulation. **Note** PPP is the default encapsulation and does not appear in the output of the **show running-config** command for the virtual template interface unless you manually configure the command.
Step 4	`Router(config-if)# ppp authentication {protocol1 [protocol2...]} [if-needed] [list-name | default] [callin] [one-time] [optional]`	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

Associating the Virtual Template Interface for PPP on the GGSN

Before you associate the virtual template interface for PPP, you must configure the virtual template interface. The number that you configure for the virtual template interface must correspond to the number that you specify in the **gprs gtp ppp vtemplate** command.

To associate the virtual template interface for GGSN, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs gtp ppp vtemplate number`	Associates the virtual template interface that defines the PPP characteristics with support for the PPP PDP type over GTP on the GGSN. **Note** This number must match the *number* configured in the corresponding **interface virtual-template** command.

Configuring GTP-PPP Regeneration on the GGSN

This section provides an overview of and describes how to configure PPP over GTP with L2TP support on the GGSN. It includes the following topics:

- Overview of GTP-PPP Regeneration on the GGSN, page 10-14
- GTP-PPP Regeneration Configuration Task List, page 10-15

Overview of GTP-PPP Regeneration on the GGSN

The GGSN supports PPP in two different areas of the network, with two different sets of PPP endpoints, and supports IP over GTP in between. First, IP over PPP is in use between the TE and MT. From there, IP packet support occurs between the MT through the SGSN, over the Gn interface and the GTP tunnel to the GGSN. The GGSN initiates a new PPP session on the Gi interface over an L2TP tunnel to the corporate network. So, the second set of PPP endpoints occurs between the GGSN and the LNS at the corporate network.

PPP regeneration on the GGSN supports the use of an IP PDP type in combination with PPP and L2TP. For each IP PDP context that the GGSN receives at an access point that is configured to support PPP regeneration, the GGSN regenerates a PPP session. The GGSN encapsulates any tunnel packet data units (TPDUs) in PPP and L2TP headers as data traffic and forwards them to the LNS.

PPP regeneration on the GGSN implements VPN routing and forwarding (VRF) to handle overlapping IP addresses. A VRF routing table is automatically enabled at each access point name (APN) when you configure PPP regeneration at that APN.

PPP-Regeneration Scalability

With Cisco GGSN Release 8.0 and later, the GGSN allows PDPs regenerated to a PPP session to run on software interface description blocks (IDBs), which increases the number of supported sessions.

Anonymous User Access

Additionally, with Cisco GGSN Release8.0, 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** command in access-point user configuration mode 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 9-20.

Restrictions

The GGSN supports PPP regeneration with the following restriction:

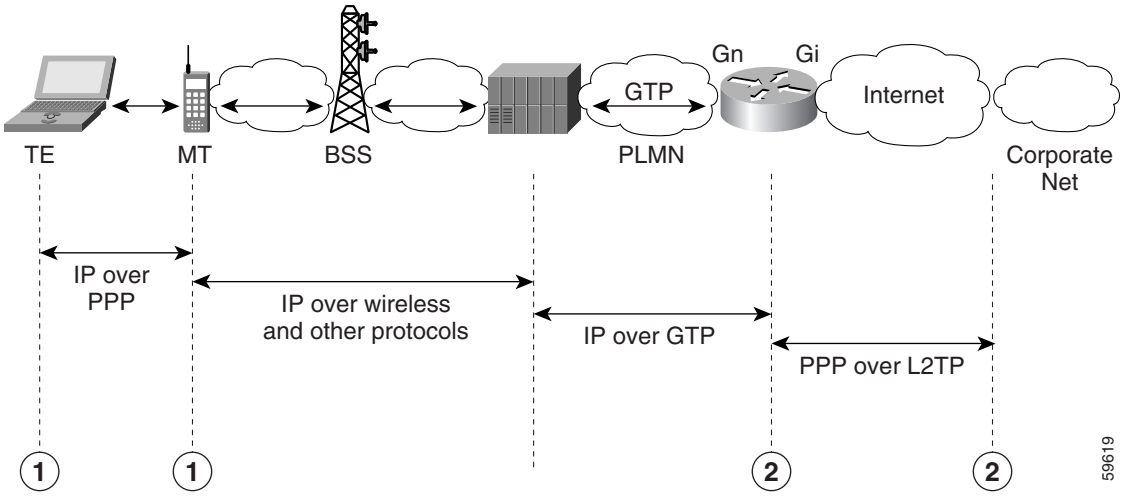
- Manual configuration of VRF is not supported.

- At least one PPP authentication protocol must be enabled using the **ppp authentication** command in interface configuration mode.
- Ensure that the **no peer default ip address** command is configured under the PPP-Regen virtual template.

Caution The creation of PPP-Regen contexts on the GGSN can lead to higher than usual CPU utilization on the GGSN when console logging is enabled (**logging console** command) and the link status log is not turned off under the PPP-Regen virtual template.

Figure 10-4 shows the implementation of PPP support within a GPRS network using PPP regeneration on the GGSN.

Figure 10-4 PPP Regeneration Topology on the GGSN



GTP-PPP Regeneration Configuration Task List

Configuring IP over GTP with PPP regeneration on the GGSN requires similar configuration tasks as those required to configure GTP over PPP with L2TP, with some exceptions in the implementation.

To configure GTP-PPP regeneration support on the GGSN, perform the following tasks:

- Configuring the GGSN as a LAC, page 10-16 (Required)
- Configuring AAA Services for L2TP Support, page 10-17 (Required)
- Configuring a PPP Virtual Template Interface, page 10-18 (Required)
- Associating the Virtual Template Interface for PPP Regeneration on the GGSN, page 10-20 (Required)
- Configuring PPP Regeneration at an Access Point, page 10-20 (Required)

Configuring the GGSN as a LAC

When you use L2TP services on the GGSN to the LNS in the corporate network, you need to configure the GGSN as a LAC by enabling VPDN services on the GGSN.

For more information about VPDN configuration and commands in the Cisco IOS software, see *Cisco IOS Dial Technologies Configuration Guide* and *Command Reference* publications.

To configure the GGSN as a LAC where the tunnel parameters are configured locally on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# vpdn enable`	Enables VPDN on the router or instance of Cisco IOS software and directs the router or instance to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present. **Note** Only this step is required if you are using a RADIUS server to provide tunnel parameters.
Step 2	`Router(config)# vpdn domain-delimiter` *characters* `[suffix | prefix]`	(Optional) Specifies the characters to use to delimit the domain prefix or domain suffix. Available characters are %, -, @, \ , #, and /. The default is @. **Note** If a backslash (\) is the last delimiter in the command line, enter it as a double backslash (\\).
Step 3	`Router(config)# vpdn-group` *group-number*	Defines a VPDN group, and enters VPDN group configuration mode.
Step 4	`Router(config-vpdn)# request-dialin`	Enables the router or instance of Cisco IOS software to request dial-in tunnels, and enters request dial-in VPDN subgroup configuration mode.
Step 5	`Router(config-vpdn-req-in)# protocol l2tp`	Specifies use of the L2TP protocol for dial-in tunnels.
Step 6	`Router(config-vpdn-req-in)# domain` *domain-name*	Specifies that users with this domain name will be tunneled. Configure this command for every domain name you want to tunnel.
Step 7	`Router(config-vpdn-req-in)# exit`	Returns you to VPDN group configuration mode.
Step 8	`Router(config-vpdn)# initiate-to ip` *ip-address* `[limit` *limit-number*`] [priority` *priority-number*`]`	Specifies the destination IP address for the tunnel.
Step 9	`Router(config-vpdn)# local name` *name*	Specifies the local name that is used to authenticate the tunnel.

Note You can configure the L2TP tunnel parameters locally on the GGSN, or the tunnel parameters can be provided by a RADIUS server. If a RADIUS server is providing the tunnel parameters, then in this procedure you only need to configure the **vpdn enable** command on the GGSN.

Configuring AAA Services for L2TP Support

Before the VPDN stack on the GGSN opens an L2TP tunnel to an LNS, it tries to authorize the tunnel first. The GGSN consults its local database to perform this authorization. Therefore, you need to configure the appropriate AAA services for the GGSN to support L2TP tunnel authorization. Note that this is for authorization of the tunnel itself—not for user authorization.

This section describes only those commands required to implement authorization for L2TP support on the GGSN. It does not describe all of the tasks required to configure RADIUS and AAA support on the GGSN. For more information about enabling AAA services and configuring AAA server groups on the GGSN, see the "Configuring Security on the GGSN" chapter in this book.

Note To correctly implement authentication and authorization services on the GGSN for L2TP support, you must configure the same methods and server groups for both.

To configure authorization for L2TP support on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa authorization network default local`	(Optional) Specifies that the GGSN consults its local database, as defined by the **username** command, for tunnel authorization.

	Command	Purpose
Step 2	`Router(config)# aaa authorization network {default | list-name} group group-name [group group-name...]`	Specifies one or more AAA methods for use on interfaces running PPP, where: • **network**—Runs authorization for all network-related service requests, including SLIP1, PPP2, PPP NCPs3, and ARA4. • **default**—Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in. • *list-name*—Specifies the character string used to name the list of authentication methods tried when a user logs in. • **group** *group-name*—Uses a subset of RADIUS servers for authentication as defined by the **aaa group server radius** command. **Note** Be sure to use a method list and do not use the **aaa authorization network default group radius** form of the command. For L2TP support, the *group-name* must match the group that you specify in the **aaa authentication ppp** command.
Step 3	`Router(config)# username name password secret`	Specifies the password to use in CHAP caller identification, where *name* is the name of the tunnel. **Note** Usernames in the form of *ciscouser*, *ciscouser@corporate1.com*, and *ciscouser@corporate2.com* are considered to be three different entries. Repeat this step to add a username entry for each remote system from which the local router or access server requires authentication.

Note You can configure the L2TP tunnel parameters locally on the GGSN, or the tunnel parameters can be provided by a RADIUS server. If a RADIUS server is providing the tunnel parameters, then in this procedure you only need to configure the **username** command on the GGSN.

Configuring a PPP Virtual Template Interface

To support IP over GTP with PPP regeneration, you must configure a virtual template interface on the GGSN that supports PPP encapsulation. Therefore, the GGSN will have two virtual template interfaces: one for GTP encapsulation and one for PPP encapsulation. The GGSN uses the PPP virtual template interface to create all PPP virtual access interfaces for PPP sessions on the GGSN.

Because PPP is the default encapsulation, it does not need to be explicitly configured, and it does not appear in the **show running-config** output for the interface.

Be aware that the configuration commands for the PPP virtual template interface to support PPP regeneration on the GGSN are different from the previous configurations shown for GTP over PPP support.

To configure a PPP virtual template interface on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface virtual-template number`	Creates a virtual template interface, where *number* identifies the virtual template interface. This command enters you into interface configuration mode. **Note** This number must match the *number* configured in the corresponding **gprs gtp ppp-regeneration vtemplate** command.
Step 2	`Router(config-if)# ip address negotiated`	Specifies that the IP address for a particular interface is obtained via PPP/IPCP (IP Control Protocol) address negotiation.
Step 3	`Router(config-if)# no peer neighbor-route`	Disables creation of neighbor routes.
Step 4	`Router(config-if)#no peer default ip address`	Disables an IP address from being returned to a remote peer connecting to this interface.
Step 5	`Router(config-if)# encapsulation ppp`	(Optional) Specifies PPP as the encapsulation type for packets transmitted over the virtual template interface. PPP is the default encapsulation. **Note** PPP is the default encapsulation and does not appear in the output of the **show running-config** command for the virtual template interface unless you manually configure the command.
Step 6	`Router(config-if)# ppp authentication {protocol1 [protocol2...]} [if-needed] [list-name | default] [callin] [one-time] [optional]`	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

Associating the Virtual Template Interface for PPP Regeneration on the GGSN

Before you associate the virtual template interface for PPP regeneration, you must configure a virtual template interface. The number that you configure for the virtual template interface must correspond to the number that you specify in the **gprs gtp ppp-regeneration vtemplate** command.

To associate the virtual template interface for PPP regeneration, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs gtp ppp-regeneration vtemplate` *number*	Associates the virtual template interface that defines the PPP characteristics with support for the PPP regeneration on the GGSN. **Note** This number must match the *number* configured in the corresponding **interface virtual-template** command.

Configuring PPP Regeneration at an Access Point

To enable PPP regeneration on the GGSN, you must configure each access point for which you want to support PPP regeneration. There is no global configuration command for enabling PPP regeneration for all access points on the GGSN.

To create an access point and specify its type, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs access-point-list` *list-name*	Specifies a name for a new access point list, or references the name of the existing access point list, and enters access-point list configuration mode.
Step 2	`Router(config-ap-list)# access-point` *access-point-index*	Specifies an index number for a new access point definition, or references an existing access point definition, and enters access point configuration mode.
Step 3	`Router(config-access-point)# access-point-name` *apn-name*	Specifies the access point network ID, which is commonly an Internet domain name. **Note** The *apn-name* must match the APN that is provisioned at the MS, home location register (HLR), and Domain Name System (DNS) server.

	Command	Purpose
Step 4	`Router(config-access-point)# access-mode transparent`	(Optional) Specifies that no security authorization or authentication is requested by the GGSN for this access point. **Note** Transparent access is the default value, but it must be *manually* configured to support PPP regeneration at the access point if the access mode was previously non-transparent.
Step 5	`Router(config-access-point)# ppp-regeneration [max-session number | setup-time seconds | verify-domain | fixed-domain]`	Enables an access point to support PPP regeneration, where: • **max-session** *number*—Specifies the maximum number of PPP regenerated sessions allowed at the access point. The default value is 65535. • **setup-time** *seconds*—Specifies the maximum amount of time (between 1 and 65535 seconds) within which a PPP regenerated session must be established. The default value is 60 seconds. • **verify-domain**—Configures the GGSN to verify the domain sent in the protocol configuration option (PCO) IE sent in a Create PDP Context request against the APN sent out by the user when PPP-regeneration is being used. If a mismatch occurs, the Create PDP Context request is rejected with the cause code "Service not supported." • **fixed-domain**—Configures the GGSN to use the access point name as the domain name with which it initiates an L2TP tunnel to the user when PPP-regeneration is being used. The **ppp-regeneration fixed-domain** and **ppp-regeneration verify-domain** command configurations are mutually exclusive. When the **ppp-regeneration fixed-domain** command is configured, domain verification cannot be performed.

Monitoring and Maintaining PPP on the GGSN

This section provides a summary list of the **show** commands that you can use to monitor the different aspects of PPP configuration on the GGSN. Not all of the **show** commands apply to every method of configuration.

Use the following privileged EXEC commands to monitor and maintain PPP status on the GGSN:

Command	Purpose
Router# **show derived-config interface virtual-access** *number*	Displays the PPP options that GTP has configured on the virtual access interface for PPP regenerated sessions.
Router# **show gprs gtp pdp-context all**	Displays all currently active PDP contexts.
Router# **show gprs gtp pdp-context path** *ip-address*	Displays all currently active PDP contexts for the specified SGSN path.
Router# **show gprs gtp pdp-context pdp-type ppp**	Displays all currently active PDP contexts that are transmitted using PPP.
Router# **show gprs gtp status**	Displays information about the current status of the GTP on the GGSN.
Router# **show interfaces virtual-access** *number* [**configuration**]	Displays status, traffic data, and configuration information about a specified virtual access interface.
Router# **show vpdn session** [**all** | **packets** | **sequence** | **state** | **timers** | **window**] [**interface** | **tunnel** | **username**]	Displays VPN session information including interface, tunnel, username, packets, status, and window statistics.
Router# **show vpdn tunnel** [**all** | **packets** | **state** | **summary** | **transport**] [**id** | **local-name** | **remote-name**]	Displays VPN tunnel information including tunnel protocol, ID, local and remote tunnel names, packets sent and received, tunnel, and transport status.

Configuration Examples

This section provides configuration examples for the different types of PPP support on the GGSN. It includes the following examples:

- GTP-PPP Termination on the GGSN Configuration Examples, page 10-22
- GTP-PPP–Over–L2TP Configuration Example, page 10-24
- GTP-PPP Regeneration Configuration Example, page 10-25
- AAA Services for L2TP Configuration Example, page 10-26

GTP-PPP Termination on the GGSN Configuration Examples

The following example shows a GGSN configuration for GTP over PPP using PAP authentication using a RADIUS server at 172.16.0.2 to allocate IP addresses:

```
Router# show running-config
Building configuration...
Current configuration : 3521 bytes
!
version 12.2
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
! Enables the router for GGSN services
!
```

```
service gprs ggsn
!
ip cef
!
no logging buffered
logging rate-limit console 10 except errors
!
! Enables AAA globally
!
aaa new-model
!
! Defines AAA server group
!
aaa group server radius gtp_ppp
 server 172.16.0.2 auth-port 2001 acct-port 2002
!
! Configures authentication and authorization
! methods for PPP support.
!
aaa authentication ppp gtp_ppp group gtp_ppp
aaa authorization network gtp_ppp group gtp_ppp
aaa accounting network default start-stop group gtp_ppp
!
ip subnet-zero
!
! Configures a loopback interface
! for the PPP virtual template interface
!
interface Loopback2
 ip address 10.88.0.4 255.255.0.0
!
...
!
! Configures a VT interface for
! GTP encapsulation
!
interface loopback 1
 ip address 10.30.30.1 255.255.255.0
!
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list gprs
!
! Configures a VT interface for
! PPP encapsulation
!
interface Virtual-Template2
 ip unnumbered Loopback2
 no peer default ip address
 ppp authentication pap
!
...
!
gprs access-point-list gprs
  access-point 1
   access-point-name gprs.cisco.com
   aaa-group authentication gtp_ppp
   aaa-group accounting gtp_ppp
   exit
   !
! Associates the PPP virtual template
! interface for use by the GGSN
!
```

```
gprs gtp ppp-vtemplate 2
gprs default charging-gateway 10.7.0.2
!
gprs memory threshold 512
!
! Configures a global RADIUS server host
! and specifies destination ports for
! authentication and accounting requests
!
radius-server host 172.16.0.2 auth-port 2001 acct-port 2002
radius-server retransmit 3
radius-server key cisco
!
!
end
```

GTP-PPP–Over–L2TP Configuration Example

The following example shows a partial configuration of the GGSN to support PPP over GTP with L2TP. Tunnel parameters are configured locally on the GGSN and are not provided by a RADIUS server.

```
. . .
!
! Enables AAA globally
!
aaa new-model
!
aaa authorization network default local
!
vpdn enable
!
! Configures a VPDN group
!
vpdn-group 1
  request-dialin
  protocol l2tp
  domain ppp-lns
  initiate-to ip 4.0.0.78 priority 1
  local name nas
!
! Configures a loopback interface
! for the PPP virtual template interface
!
interface Loopback2
 ip address 10.88.0.1 255.255.255.255
!
interface Virtual-Template2
 description VT for PPP L2TP
 ip unnumbered Loopback2
 no peer default ip address
 no peer neighbor-route
 ppp authentication pap chap
!
```

```
gprs access-point-list gprs
 access-point 15
 access-point-name ppp-lns
 exit
!
! Associates the PPP virtual template
! interface for use by the GGSN
!
gprs gtp ppp vtemplate 2
!
. . .
!
```

GTP-PPP Regeneration Configuration Example

The following example shows a partial configuration of the GGSN to support IP over GTP with PPP regeneration on the GGSN. Tunnel parameters are configured locally on the GGSN and are not provided by a RADIUS server.

```
!
. . .
!
! Enables AAA globally
!
vpdn enable
!
! Configures a VPDN group
!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain ppp_regen1
 initiate-to ip 4.0.0.78 priority 1
 l2tp tunnel password 7 0114161648
!
! Configures a virtual template
! interface for PPP regeneration
!
interface Virtual-Template2
 description VT for PPP Regen
 ip address negotiated
 no peer neighbor-route
 no peer default ip address
 ppp authentication pap chap
!
gprs access-point-list gprs
 access-point 6
  access-point-name ppp_regen1
  ppp-regeneration
  exit
!
! Associates the PPP-regeneration
! virtual template interface for use by the GGSN
!
gprs gtp ppp-regeneration vtemplate 2
```

AAA Services for L2TP Configuration Example

L2TP support is used on the GGSN to support both the PPP-over-GTP topology and the IP–over–GTP with PPP regeneration topology. The following examples shows a partial configuration of RADIUS and AAA services on the GGSN to provide L2TP support:

```
!
! Enables AAA globally
!
aaa new-model
!
! Defines AAA server group
!
aaa group server radius gtp_ppp
 server 172.16.0.2 auth-port 2001 acct-port 2002
!
! Configures authentication and authorization
! method gtp_ppp and AAA server group gtp_ppp
! for PPP support.
!
! NOTE: You must configure the same methods and groups
! to support L2TP as shown by the
! aaa authentication ppp gtp_ppp
! and aaa authorization network gtp_ppp commands.
!
aaa authentication ppp gtp_ppp group gtp_ppp
aaa authorization network default local
aaa authorization network gtp_ppp group gtp_ppp
aaa accounting network default start-stop group radius
username nas password 0 lab
username hgw password 0 lab
!
. . .
!
! Configures a global RADIUS server host
! and specifies destination ports for
! authentication and accounting requests
!
radius-server host 172.16.0.2 auth-port 2001 acct-port 2002
radius-server retransmit 3
radius-server key cisco
!
. . .
!
```

CHAPTER 11

Configuring QoS on the GGSN

This chapter describes how to configure Quality of Service (QoS) functions to differentiate traffic flow through the gateway GPRS support node (GGSN).

For complete descriptions of the GGSN commands in this chapter, see *Cisco GGSN Command Reference* for the Cisco GGSN release you are using. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

This chapter includes the following sections:

- Overview of QoS Support on the GGSN, page 11-1
- Configuring UMTS QoS on the GGSN, page 11-2
- Configuring the GGSN Default QoS as Requested QoS, page 11-13
- Configuring Call Admission Control on the GGSN, page 11-13
- Configuring Per-PDP Policing, page 11-17
- Monitoring and Maintaining QoS on the GGSN, page 11-20
- Configuration Examples, page 11-22

Overview of QoS Support on the GGSN

The Cisco GGSN software supports 3G Universal Mobile Telecommunication System (UMTS) QoS. Each GPRS/UMTS packet data protocol (PDP) context request contains a UMTS QoS profile.

The implementation of QoS support in the GPRS/UMTS public LAN mobile network (PLMN) varies by the service provider and the available resources in the network. The 3GPP standards define the UMTS QoS classes that can be defined by a UMTS MS. However, the resulting QoS is negotiated and variable within the GPRS/UMTS network backbone according to the implementations of the service provider.

UMTS QoS

To manage different level of QoS, UMTS has defined the four QoS traffic classes based on delay, jitter, bandwidth, and reliability factors:

- Conversational
- Streaming
- Interactive
- Background

The Cisco GGSN delivers end-to-end UMTS QoS by implementing it using the Cisco IOS QoS differentiated services (Diffserv).

This chapter describes the QoS support that the GGSN provides for the UMTS QoS classes.

Note 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. 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.

Configuring UMTS QoS on the GGSN

This section describes how to configure the UMTS QoS on the GGSN. It includes the following topics:

- Overview of UMTS QoS, page 11-2
- Configuring UMTS QoS Task Lists, page 11-4
- Enabling UMTS QoS Mapping on the GGSN, page 11-4
- Mapping UMTS QoS Traffic Classes to a DiffServ PHB Group, page 11-4
- Assigning a DSCP to a DiffServ PHB Group, page 11-5
- Configuring the DSCP in the Subscriber Datagram, page 11-7
- Configuring the Cisco 7600 Platform GGSN UMTS QoS Requirements, page 11-8
- Verifying the UMTS QoS Configuration, page 11-11

Overview of UMTS QoS

3GPP standards define four QoS traffic classes based on delay, jitter, bandwidth, and reliability for UMTS. Table 11-1 describes these UMTS traffic classes and their characteristics, applications, and the mapped Cisco IOS QoS Diffserv class.

Table 11-1 UMTS Traffic Classes

Traffic Class	Conversational (Real Time)	Streaming (Real Time)	Interactive (Best Effort)	Background (Best Effort)
Characteristics	Preserve time relation (variation) between information entities of the stream. Conversational pattern, therefore, very low delay and jitter.	Preserve time relation (variation) between information entities of the stream. Delay and jitter requirements are not as strict as with the conversational class.	Request/response pattern. Retransmission of payload content in-route.	Destination is not expecting the data with a stringent time. Retransmission of payload content in-route might occur.
Example Applications	Voice over IP	Streaming audio and video	Web browsing	Downloading email
Diffserv Class / Map to DSCP	Expedited Forwarding Class	Assured Forwarding 2 Class	Assured Forwarding 3 Class	Best Effort

The Cisco GGSN supports end-to-end UMTS QoS by implementing it using the Cisco IOS Differentiated Services (DiffServ) model. The DiffServ model is a multiple-service model that can satisfy differing QoS requirements. With DiffServ, the network tries to deliver a particular kind of service based on the QoS specified by each packet. This specification can occur in different ways, for example, using the 6-bit differentiated services code point (DSCP) setting in IP packets or source and destination addresses. The network uses the QoS specification to classify, mark, shape, and police traffic, and to perform intelligent queueing.

For complete information on Cisco IOS QoS and the DiffServ service model, see *Cisco IOS Quality of Service Solutions Configuration Guide*.

Configuring UMTS QoS Task Lists

To implement the UMTS QoS method on a GGSN, you must first enable the function. From there, you can modify the UMTS QoS options to support your network needs.

Configuring GGSN UMTS QoS on the Cisco 7600 Platform Task List

If configuring UMTS QoS on a GGSN on the Cisco 7600 platform, perform the following tasks:

- Enabling UMTS QoS Mapping on the GGSN, page 11-4 (Required)
- Mapping UMTS QoS Traffic Classes to a DiffServ PHB Group, page 11-4 (Optional)
- Assigning a DSCP to a DiffServ PHB Group, page 11-5 (Optional)
- Configuring the DSCP in the Subscriber Datagram, page 11-7 (Optional)
- Configuring the Cisco 7600 Platform GGSN UMTS QoS Requirements, page 11-8 (Required)
- Configuring Call Admission Control on the GGSN, page 11-13 (Optional)
- Verifying the UMTS QoS Configuration, page 11-11

Enabling UMTS QoS Mapping on the GGSN

By default, UMTS QoS is not enabled on the GGSN. To enable UMTS QoS on the GGSN, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs qos map umts`	Enables UMTS QoS mapping on the GGSN.

Mapping UMTS QoS Traffic Classes to a DiffServ PHB Group

Before you can specify a QoS mapping from the UMTS QoS traffic classes to a DiffServ per-hop behavior (PHB) group, you must enable UMTS QoS mapping using the **gprs qos map umts** command in global configuration mode.

The default mapping values for UMTS QoS traffic classes are as follows:

- Conversational traffic class to the ef-class DiffServ PHB group
- Streaming traffic class to the af2-class DiffServ PHB group

- Interactive traffic class to the af3-class DiffServ PHB group
- Background traffic class to the best-effort DiffServ PHB group

If you wish to use mapping values other than these defaults, you can use the **gprs umts-qos map traffic-class** command to map a UMTS traffic class to another DiffServ PHB group.

Note To successfully map UMTS QoS traffic classes to a DiffServ PHB, the class maps must be configured using the **class map** and **match ip dscp** Cisco IOS software commands. For more information about configuring class maps, see *Cisco IOS Quality of Service Solutions Configuration Guide*.

To map a UMTS traffic class to a DiffServ PHB group, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs umts-qos map traffic-class` *traffic-class diffserv-phb-group*	Enables mapping of UMTS QoS traffic classes to a DiffServ PHB, where the UMTS traffic classes are: • signalling • conversational • streaming • interactive • background and the DiffServ PHB groups are: • signalling-class • ef-class • af1-class • af2-class • af3-class • af4-class • best-effort

Assigning a DSCP to a DiffServ PHB Group

By default, the default differentiated services code point (DSCP) value associated with a PHB class is used. Table 11-2 lists the default DSCP values for each PHB group.

Table 11-2 Default DSCP Values for PHB Groups

PHB Group	DSCP Value
EF	101110
AF11	001010
AF12	001100
AF13	001110

Table 11-2 Default DSCP Values for PHB Groups (continued)

PHB Group	DSCP Value
AF21	010010
AF22	010100
AF23	010110
AF31	011010
AF32	011100
AF33	011110
AF41	100010
AF42	100100
AF43	100110
Best Effort	000000

However, you can assign a DSCP to PHB groups.

For the Assured Forwarding (AF) PHB group, you can specify up to three DSCPs for each drop precedence. The signalling, EF, and best-effort classes do not have drop precedence, so only the first DSCP value is used. If you enter a value for the *dscp2* or *dscp3* arguments for these classes, it is ignored.

Note Drop precedence indicates the order in which a packet will be dropped when there is congestion on the network.

Note To successfully map UMTS QoS traffic classes to a DiffServ PHB and assign a DSCP value to a DiffServ PHB group, the class maps must be configured using the **class map** and **match ip dscp** commands. For more information about configuring class maps, see *Cisco IOS Quality of Service Solutions Configuration Guide* and *Cisco IOS Quality of Service Solutions Command Reference*.

Note By default, signalling class is assigned to CS5 (101000), which is the equivalent of IP precedence 5.

To assign a DSCP value to a DiffServ PHB group, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs umts-qos map diffserv-phb diffserv-phb-group [dscp1] [dscp2] [dscp3]`	Assigns a DSCP to a DiffServ PHB group where the DiffServ PHB groups are: • signalling • ef-class • af1-class • af2-class • af3-class • af4-class • best-effort and the DSCPs are: • dscp1—Required for all classes. Specifies one of 64 DSCP values from 0 to 63. This DSCP value corresponds to drop precedence 1. • dscp2—(Optional for AF classes) Specifies one of 64 DSCP values from 0 to 63. This DSCP value corresponds to drop precedence 2. • dscp3—(Optional for AF classes) Specifies one of 64 DSCP values from 0 to 63. This DSCP value corresponds to drop precedence 3.

Configuring the DSCP in the Subscriber Datagram

By default, the DSCP in subscriber datagrams is re-marked with the DSCP assigned to the traffic class when the PDP context was created.

To specify that the subscriber datagram be forwarded through the GTP path without modifying its DSCP, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs umts-qos dscp unmodified [up | down | all]`	Specifies that the subscriber datagram be forwarded through the GTP path without modifying its DSCP.

To return to the default value, issue the **no gprs umts-qos dscp unmodified** command.

Configuring the Cisco 7600 Platform GGSN UMTS QoS Requirements

When configuring UMTS QoS for a GGSN running on a Cisco Service and Application Module for IP (SAMI) in the Cisco 7600 platform, the different components of the platform perform different QoS functions. Table 11-3 summarizes the QoS function performed by the Cisco 7600 platform component.

Table 11-3 QoS Function by Cisco 7600 Platform Component

Cisco 7600 Component	UMTS QoS Function
Catalyst Line Card	Classification and ingress and egress scheduling
Supervisor Engine	Classification and aggregate policing
Cisco IOS GGSN image on the Cisco SAMI	Classification, DSCP marking, and output queuing

After you configure UMTS QoS on the GGSN, ensure the following tasks are completed:

Supervisor Engine

Note The following list is a summary of the required tasks that need to be completed on the supervisor engine for UMTS QoS on a GGSN. For complete information each of these tasks, see *Cisco 7600 Series Cisco IOS Software Configuration Guide*.

1. Enable Mutlilayer Switching QoS using the **mls qos** command in global configuration mode.

```
Router# mls qos
```

2. On the supervisor engine, configure aggregate policing for Gi traffic.

Note Because there can be multiple Gn and Gi interfaces, but all the traffic eventually needs to go to a single GE port on the SAMI (one GE port for two GGSNs), we recommend that you use a Named Aggregate Policer to rate limit the traffic to the SAMI. We also recommend dropping all non-conforming traffic.

The following example illustrates the configuration for a named aggregate policer. The named policer is attached to the Gi interface:

```
Access-list 101 permit ip any any dscp ef
Access-list 102 permit ip any any dscp af21
Access-list 103 permit ip any any dscp af31
Access-list 103 permit ip any any dscp af32
Access-list 103 permit ip any any dscp af33
Access-list 104 permit ip any any

Class-map match-all conversational
    Match access-group 101
Class-map match-all streaming
    Match access-group 102
Class-map match-all interactive
    Match access-group 103
Class-map match-all background
    Match access-group 104
```

```
Mls qos aggregate-policer AGGREGATE-CONV bit-rate1 normal-burst max-burst
conform-action transmit exceed-action drop
Mls qos aggregate-policer AGGREGATE-STREAMING bit-rate1 normal-burst max-burst
conform-action transmit exceed-action drop
Mls qos aggregate-policer AGGREGATE-INTERACTIVE bit-rate1 normal-burst max-burst
conform-action transmit exceed-action drop
Mls qos aggregate-policer AGGREGATE-BACKGROUND bit-rate1 normal-burst max-burst
conform-action transmit exceed-action drop

Policy-map Gi-incoming
     Class conversational
         Police aggregate AGGREGATE-CONV
     Class streaming
         Police aggregate AGGREGATE-STREAMING
     Class interactive
         Police aggregate AGGREGATE-INTERACTIVE
     Class background
         Police aggregate AGGREGATE-BACKGROUND

Router(config-if)# service-policy input Gi-incoming
```

Note To monitor policing statistics, you can use the following **show** commands:
- **show mls qos aggregate-policer** *name*
- **show policy-map interface** *interface*
- **show policy interface** *interface*

3. Set the trust state of the ingress ports to trust-dscp mode using the **msl qos trust dscp** command in interface configuration mode:

```
Router(config)# interface FastEthernet2/1
Router(config-if)# mls qos trust dscp
```

4. Configure egress port scheduling by completing the following tasks:

   a. Obtain the UMTS traffic class-to-DSCP mappings using the **show gprs umts-qos traffic class** privileged EXEC command on the GGSN running on the Cisco SAMI:

```
Router# ggsn show gprs umts-qos traffic-class
```

   b. Obtain the default DSCP-to-CoS mapping by displaying the QoS mapping information using the **show mls qos maps** privileged EXEC command.

```
Router# show mls qos maps
```

   c. Obtain the default CoS-to-queue mapping by displaying the queueing statistics of an interface using the **show queuing interface** privileged EXEC command.

```
Router# show queuing interface interface
```

d. Using the information obtained in Steps A, B, and C, determine if customized egress DSCP-to-CoS mapping is necessary and if so, define the mapping using the **mls qos map dscp-cos** command in global configuration mode.

```
Router(config)# mls qos map dscp-cos dscp to cos
```

When customizing DSCP-CoS mapping, ensure that:

- Conversational and streaming traffic are put into egress queue 4
- Interactive and background traffic are equally distributed between the two normal queues.
- Interactive traffic is mapped to different CoS values so that different thresholds can be configured on the queue to take advantage of WRED.

5. If the line card supports Weighted Random Early Detection WRED, configure congestion avoidance by completing the following tasks:

a. Enable WRED and specify the minimum and maximum threshold for specified queues using the **wrr-queue random-detect max-threshold** command in interface configuration mode (the defaults are recommended).

```
Router(config-if)# wrr-queue random-detect max-threshold queue
percent-of-queue-size
```

b. Map CoS values to drop thresholds using the **wrr-queue cos map** command in interface configuration mode. When the threshold is exceeded, frames with specific CoS values will be dropped.

```
wrr-queue cos-map queue-id threshold-id cos-1 ... cos-n
```

In the following example, CoS values 3 and 4 are assigned to transmit queue 1/threshold 2 and transmit 2/threshold 1.

```
Router(config-if)# wrr-queue cos-map 1 1 3
Router(config-if)# wrr-queue cos-map 1 2 4
```

c. Allocate bandwidth between standard transmit queue 1 (low priority) and standard transmit queue 2 (high priority) using the **wrr-queue bandwidth** command in interface configuration mode.

```
Router(config-if)# wrr-queue bandwidth weight1 weight2 weight3
```

Cisco GGSN

1. Configure an output queueing strategy for the UMTS traffic classes for each GGSN.

You can configure a queueing strategy for each of the UMTS traffic classes for each GGSN.

The following configuration example assumes that the UMTS traffic classes and class maps have been defined.

```
Interface GigabitEthernet0/0
    Bandwidth <max-bandwidth>
       Service-policy output sami-output

Policy-map sami-output
    Class conversational
        Priority percent 5
    Class streaming
        Priority percent15
    Class interactive
        Bandwidth 20
    Class background
```

```
        Bandwidth 20
    Class signaling
        Bandwidth 15
```

Verifying the UMTS QoS Configuration

To verify your UMTS QoS configuration, use the **show running-config** command on the supervisor engine and the GGSN running on the Cisco SAMI and observe the UMTS QoS parameters in the following example:

Supervisor Engine Configuration:

```
Mls qos

Mls qos map dscp-cos 18 20 22 to 5
Mls qos map dscp-cos 26 to 4
Mls qos map dscp-cos 28,30 to 3


Access-list 101 permit ip any any dscp ef
Access-list 102 permit ip any any dscp af21
Access-list 103 permit ip any any dscp af31
Access-list 103 permit ip any any dscp af32
Access-list 103 permit ip any any dscp af33
Access-list 104 permit ip any any

Class-map match-all conversational
    Match access-group 101
Class-map match-all streaming
    Match access-group 102
Class-map match-all interactive
    Match access-group 103
Class-map match-all background
    Match access-group 104


Mls qos aggregate-policer AGGREGATE-CONV <bit rate1> <normal-burst> <max-burst>
Conform-action transmit exceed-action drop
Mls qos aggregate-policer AGGREGATE-STREAMING <bit rate2> <normal-burst> <max-burst>
conform-action transmit exceed-action drop
Mls qos aggregate-policer AGGREGATE-INTERACTIVE <bit rate3> <normal-burst> <max-burst>
conform-action transmit exceed-action drop
Mls qos aggregate-policer AGGREGATE-BACKGROUND <bit rate4> <normal-burst> <max-burst>
conform-action transmit exceed-action drop

Policy-map Gi-incoming
    Class conversational
        Police aggregate AGGREGATE-CONV
    Class streaming
        Police aggregate AGGREGATE-STREAMING
    Class interactive
        Police aggregate AGGREGATE-INTERACTIVE
    Class background
        Police aggregate AGGREGATE-BACKGROUND
```

```
Interface FastEthernet2/1
    Description "Gi interface"
    Mls qos trust dscp
    Wrr-queue cos-map 1 1 3
        Wrr-queue cos-map 1 2 4
        Wrr-queue bandwidth 50 40 10
    Service-policy input Gi-incoming

Interface FastEthernet2/2
    Description "Gn interface"
    Mls qos trust dscp
```

GGSN Configuration

```
Gprs qos map umts

Class-map match-all conversational
    Match ip dscp 46
Class-map match-any interactive
    Match ip dscp 26
    Match ip dscp 28
    Match ip dscp 30
Class-map match-any streaming
    Match ip dscp 18
    Match ip dscp 20
    Match ip dscp 22
Class-map match-all signaling
    Match ip dscp 40
Class-map match-any background
    Description default class
    Match ip dscp 0

Policy-map sami-output
    Class conversational
        Priority percent 5
    Class streaming
        Priority percent 15
    Class interactive
        Bandwidth 20
    Class background
        Bandwidth 20
    Class signaling
        Bandwidth 15

interface Gigabitthernet 0/0
        bandwidth 250000
        service-policy output max-output
```

Configuring the GGSN Default QoS as Requested QoS

If you are not using UMTS QoS mapping on the GGSN, you can configure the GGSN to set its default QoS values in the response message exactly as requested in the Create PDP Context request. By using this command, you can prevent the GGSN from lowering the requested QoS.

To configure the GGSN to set the requested QoS as the default QoS, use the following command, beginning in global configuration mode:

Command	Purpose
`Router(config)# gprs qos default-response requested`	(Optional) Specifies that the GGSN sets its default QoS values in the response message exactly as requested in the Create PDP Context request.

Note When the **gprs qos default-response requested** command is not configured, and GPRS canonical QoS is not enabled, the GGSN sets its default QoS class to best effort.

Configuring Call Admission Control on the GGSN

The Call Admission Control (CAC) feature on the GGSN ensures that required network resources are available for real-time data traffic such as voice and video. CAC is applied at the APN and consists of two functions: maximum QoS authorization and bandwidth management.

The following sections describe how to configure these functions on the GGSN:

- Configuring Maximum QoS Authorization, page 11-13
- Configuring Bandwidth Management, page 11-16
- Configuration Examples, page 11-22
- CAC Configuration Example, page 11-24

Note CAC on the GGSN requires that UMTS QoS is enabled using the **gprs qos map umts** command in global configuration mode, and that traffic class criterion and traffic policies have been created.

Configuring Maximum QoS Authorization

The CAC maximum QoS authorization function ensures that the QoS requested by a Create PDP Context does not exceed the maximum QoS configured within an APN. Using a *CAC maximum QoS policy*, you define certain QoS parameters within a policy and attach the policy to an APN. The CAC maximum QoS policy limits the QoS requested by the PDP during its creation and modification process.

Note A CAC maximum QoS policy can be attached to multiple APNs.

The following parameters can be defined in a CAC maximum QoS policy:

- **Maximum number of active PDP contexts**—Maximum number of active PDP contexts for an APN. If the total number of active PDPs on an APN exceeds the number configured with this parameter in a policy, the GGSN rejects the PDP context. Optionally, you can configure CAC to accept only PDP contexts with Allocation/Retention priority set to 1 after the threshold is reached.
- **Maximum bit rate**—Highest maximum bit rate (MBR) that can be allowed for each traffic class in both the uplink and downlink directions for an APN. If an MBR is configured in the policy, CAC ensures that the MBR is greater than the maximum GBR. If an MBR is not configured, CAC accepts any MBR requested by a PDP context.
- **Guaranteed bit rate**—Highest guaranteed bit rate (GBR) that can be accepted for real-time traffic (conversational and streaming) in both the uplink and downlink directions for an APN. If a GBR is not configured in the policy, the CAC accepts any GBR requested by a PDP context.
- **Highest traffic class**—Highest traffic class that can be accepted at an APN. If the requested traffic class is higher than the highest traffic class specified in the policy, the PDP context is rejected. If this parameter is not configured, any traffic class is accepted.

  The GGSN does not downgrade the traffic classes during PDP context creation, however, the GGSN does downgrade the traffic class during the PDP context modification if the highest traffic class configured in an APN is changed after the PDP context creation and the GGSN receives a request for a new traffic class (in a PDP context update request) that is greater than the new highest traffic class. If this occurs, the GGSN downgrades the request to the new highest traffic class.
- **Maximum traffic handling priority**—Specifies the maximum traffic handling priority for interactive traffic class that can be accepted at an APN. If this parameter is not specified, all traffic handling priorities are accepted.
- **Maximum delay class**—Defines the maximum delay class for R97/R98 QoS that can be accepted at an APN.
- **Maximum peak throughput class**—Defines the maximum peak throughput class for R97/R98 QoS that can be accepted at an APN.

Configuring a CAC Maximum QoS Policy

To configure a CAC maximum QoS policy, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs qos cac-policy` *policy-name*	Creates or modifies a CAC maximum QoS policy.
Step 2	`Router(config-umts-cac-policy)# maximum pdp-context` *number* `[threshold` *number2*`]`	Specifies the maximum number of PDP contexts that can be created for a particular APN. Optionally, a second threshold can be configured that after reached, only PDP contexts with allocation/retention priority 1 are accepted.
Step 3	`Router(config-umts-cac-policy)# maximum traffic-class` *traffic-class-name* `[priority` *value*`]`	Specifies the highest traffic class that can be accepted at an APN. The valid values are conversational, streaming, interactive, or background. Optionally, the highest traffic handling priority for the interactive traffic class can be specified.

	Command	Purpose
Step 4	`Router(config-umts-cac-policy)# maximum peak-throughput value [reject]`	Defines the maximum peak throughput for R97/R98 QoS that can be accepted at an APN. The valid values are between 1 and 9. By default, PDP contexts for which the peak throughput is higher than the configured value are downgraded to the configured value. Optionally, you can specify the **reject** keyword to have these PDP contexts rejected instead.
Step 5	`Router(config-umts-cac-policy)# maximum delay-class value [reject]`	Specifies the maximum delay class for R97/R98 QoS that can be accepted at an APN. By default, PDP contexts for which the maximum delay-class is higher than the configured value are downgraded to the configured value. Optionally, you can specify the **reject** keyword to have these PDP contexts rejected instead.
Step 6	`Router(config-umts-cac-policy)# mbr traffic-class traffic-class-name bitrate {uplink | downlink} [reject]`	Specifies the maximum bit rate (MBR) that can be allowed for each traffic class in both directions (downlink and uplink). The valid value is between 1 and 256000. Optionally, using the **reject** keyword option, you can specify for Create PDP Context requests to be rejected when the MBR exceeds the configured value.
Step 7	`Router(config-umts-cac-policy)# gbr traffic-class traffic-class-name bitrate {uplink | downlink} [reject]`	Specifies the highest guaranteed bit rate (GBR) that can be allowed in uplink and downlink directions for real-time classes (conversational and streaming) at an APN. The valid value is between 1 and 1 and 256000. Optionally, using the **reject** keyword option, you can specify for Create PDP Context requests to be rejected when the GBR exceeds the configured value.

Enabling the CAC Maximum QoS Policy Function and Attaching a Policy to an APN

To enable the CAC maximum QoS policy function and attach a policy to an APN, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# cac-policy`	Enables the maximum QoS policy function of the CAC feature and applies a policy to an APN.

Configuring Bandwidth Management

The CAC bandwidth management function ensures that there is sufficient bandwidth for real-time PDP contexts during the PDP context activation and modification process.

The CAC feature uses user-defined bandwidth pools to negotiate and reserve bandwidth. In these pools, you define the total bandwidth allocated to that pool and then allocate a percentage of that bandwidth to each traffic class.

In the following example, bandwidth pool (pool A) is created with 100000 kbps allocated to it. In addition, a percentage of that 100000 kbps of bandwidth is allocated to each traffic class, creating four "traffic class-based" bandwidth pools.

```
gprs bandwidth-pool A
  bandwidth 100000
  traffic-class conversational percent 40
  traffic-class streaming percent 30
  traffic-class interactive percent 20
  traffic-class background percent 10
```

Configuring a CAC Bandwidth Pool

Note The CAC bandwidth pool is used by CAC to negotiate and reserve bandwidth. However, to guarantee reserved bandwidth, a Cisco IOS QoS service policy that defines queuing and scheduling must be created and attached to the physical interface.

To configure a CAC bandwidth pool, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs qos bandwidth-pool` *pool-name*	Creates or modifies a CAC bandwidth pool.
Step 2	`Router(config-gprs-bw-pool)# bandwidth` *value*	Specifies the total bandwidth, in kilobits per second, for a bandwidth pool. The valid value is a number from 1 to 4294967295.
Step 3	`Router(config-gprs-bw-pool)# traffic-class` *traffic-class* [**percent**] *value*	Allocates bandwidth from a bandwidth pool to a specific traffic class in either a percentage (1 to 100% when used with the optional **percent** keyword), or absolute value in kilobits per second (0 to 4292967295). The same unit (percentage or absolute value) must be used for all traffic classes.

Enabling the CAC Bandwidth Management Function and Applying a Bandwidth Pool to an APN

To enable the CAC bandwidth management function and apply a bandwidth pool to an APN, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# bandwidth pool {input | output} pool-name`	Enables the CAC bandwidth management function and applies a bandwidth pool to the input (Gn) interface in the downlink direction (**input** keyword) or output (Gi) interface in the uplink direction (**output** keyword) of an APN.

Note A CAC bandwidth pool can be applied to multiple APNs.

Configuring Per-PDP Policing

Per-PDP policing (session-based policing) is a GGSN Traffic Conditioner (3G TS 23.107) function that can be used to limit the maximum rate of traffic received on the Gi interface for a particular PDP context.

The policing function enforces the CAC-negotiated data rates for a PDP context. The GGSN can be configured to either drop non-conforming traffic or mark non-conforming traffic for preferential dropping if congestion occurs.

The policing parameters used depends on the PDP context. Specifically,

- For GTPv1 PDPs with R99 QoS profiles, the MBR and GBR parameters from the CAC-negotiated QoS profile are used. For non real time traffic, only the MBR parameter is used.
- For GTPv1 PDPs with R98 QoS profiles and GTPv0 PDPs, the peak throughput parameter from the CAC-negotiated QoS policy is used.

Restrictions

The following restrictions apply to per-PDP policing:

- Per-PDP policing is supported for IPv4 PDP contexts only.
- UMTS QoS mapping must be enabled on the GGSN.
- Cisco Express Forwarding (CEF) must be enabled on Gi interface.
- Per-PDP policing is supported for downlink traffic at the Gi interface only.
- The initial packets of a PDP context are not policed.
- Hiearchical policing is not supported.
- If flow-based policing is configured in a policy map that is attached to an APN, the **show policy-map apn** command displays the total number of packets received before policing and does not display the policing counters.
- A service policy that is applied to an APN cannot be modified. To modify a service policy, remove the service policy from the APN, modify it, and then re-apply it.
- Multiple class maps, each with **match flow pdp** configured and a different differentiated services code point (DSCP), are supported in a policy map only if the DSCP is trusted (the **gprs umts-qos dscp unmodified** command in global configuration mode has not been configured on the GGSN).

Per-PDP Policing Configuration Task List

To configure per-PDP policing on the GGSN, perform the following tasks:

- Creating a Class Map with PDP Flows as the Match Criterion, page 11-18
- Creating a Policy Map and Configuring Traffic Policing, page 11-19
- Attaching the Policy to an APN, page 11-20
- Resetting APN Policing Statistics, page 11-20

Creating a Class Map with PDP Flows as the Match Criterion

To create a class match and specify PDP flows as the match criterion, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# class-map class-map-name`	Creates a class map to use for matching packets.
Step 2	`Router(config-cmap)# match flow pdp`	Specifies PDP flows as the match criterion in a class map.
Step 3	`Router(config-cmap)# exit`	Exits class map configuration mode.

Note Do no specify the **match-any** option when defining a class for PDP flow classification. The default is **match-all**.

Note Additional match criteria can also be configured in the class map. DSCP and precedence-based classifications are supported.

Creating a Policy Map and Configuring Traffic Policing

To create a policy map and assign the class map, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# policy map policy-map-name`	Creates or modifies a policy map that can be attached to one or more APN to specify a service policy.
Step 2	`Router(config-pmap)# class class-map-name`	Specifies the name of the class whose policy you want to create or change.
Step 3	`Router(config-pmap)# police rate pdp [burst bytes] [peak-rate pdp [peak-burst bytes]] conform-action action exceed-action action [violate-action action]`	Configures traffic policing and the action to take on non-conforming packets. The rate and peak-rate parameters are obtained from individual flows. **Note** When configuring the **police** command, burst sizes may be specified but are not recommended. Incorrect configuration of burst values results in incorrect behavior. Possible values for the *action* variable are: • **drop**—Drops the packet. • **set-dscp-transmit**—Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value setting. • **set-prec-transmit**—Sets the IP precedence and transmits the packet with the new IP precedence value setting. • **transmit**—Transmits the packet. The packet is not altered.
Step 4	`Router(config-pmap)# exit`	Exits policy map configuration mode.

Attaching the Policy to an APN

To attach the policy map to an APN, use the following commands, beginning in access-point configuration mode:

	Command	Purpose
Step 1	`Router(config-)# access-point index`	Specifies an access point number and enters access-point configuration mode.
Step 2	`Router(config-access-point)# service-policy input policy-map-name`	Attaches a service policy to an APN to use as the service policy in the downlink direction for PDP flows of that APN.
Step 3	`Router(config-access-point)# exit`	Exits access-point configuration mode.

Resetting APN Policing Statistics

To reset policing counters displayed by the **show policy-map apn** command, use the following command in global configuration mode

Command	Purpose
`Router(config)# clear gprs access-point statistics access-point-index`	Clears statistics counters for a specific access point.

Monitoring and Maintaining QoS on the GGSN

This section describes the commands used to display QoS configuration parameters and status on the GGSN. It contains the following information:

- show Command Summary, page 11-20
- Monitoring UMTS QoS, page 11-21

show Command Summary

This section provides a summary list of the **show** commands that you can use to monitor GPRS and UMTS QoS on the GGSN. Not all commands provide information for all types of QoS methods on the GGSN.

The following privileged EXEC commands are used to monitor and maintain QoS on the GGSN:

Command	Purpose
`Router# show gprs bandwidth-pool status pool-name`	Displays a list of configured CAC bandwidth pools, along with their status.
`Router# show gprs gtp pdp-context imsi hex-data`	Displays PDP contexts by international mobile subscriber identity (IMSI).
`Router# show gprs gtp pdp-context tid hex-data`	Displays PDP contexts by tunnel ID.

Command	Purpose
`Router# show gprs gtp pdp-context qos-umts-class {conversational | streaming | interactive | background}`	Displays PDP context by UMTS QoS traffic class. Applies to UMTS QoS only.
`Router# show gprs qos status`	Displays QoS statistics for the GGSN.
`Router# show gprs umts-qos map traffic-class`	Displays UMTS QoS mapping information.
`Router# show gprs umts-qos police pdp tid tid`	Displays policing statistics for a PDP context.
`Router# show gprs umts-qos profile pdp tid tid`	Displays requested and negotiated QoS information for a PDP context.

Monitoring UMTS QoS

This section describes the commands used to display UMTS QoS configuration parameters and status on the GGSN.

It includes the following topics:

- Displaying UMTS QoS Status on the GGSN, page 11-21
- Displaying UMTS QoS Information for a PDP Context, page 11-21

Displaying UMTS QoS Status on the GGSN

You can use the **show gprs qos status** command to display the number of current active PDP contexts by UMTS traffic class.

The following example shows 100 active PDP contexts on the GGSN that are using the UMTS QoS conversational traffic class, 140 active PDP contexts that have a streaming UMTS QoS traffic class, 1345 active PDP contexts that have an interactive UMTS traffic class, and 2000 active PDP contexts that have a background UMTS QoS traffic class.

The following example shows output from the **show gprs qos status** command for UMTS QoS:

```
Router# show gprs qos status
GPRS QoS Status:
  type:UMTS
  conversational_pdp      100   streaming_pdp      150
  interactive_pdp         1345  background_pdp     2000
```

Displaying UMTS QoS Information for a PDP Context

To display UMTS QoS information for a particular PDP context, you can use the **show gprs gtp pdp-context** command with the **tid** or **imsi** keyword. The following example shows sample output for the **show gprs gtp pdp-context tid** command for a PDP context in the Interactive UMTS QoS traffic class. The output fields displaying QoS information are shown in bold:

```
Router#show gprs gtp pdp-context tid 1234000000000014
TID              MS Addr                  Source  SGSN Addr       APN
1234000000000014 1.2.3.18                 Static  4.4.4.10        gtpv1.com

    current time :Feb 15 2010 04:11:17
    user_name (IMSI): 214300000000004    MS address: 1.2.3.18
    MS International PSTN/ISDN Number (MSISDN): 112000000000004
    sgsn_addr_signal: 4.4.4.10           sgsn_addr_data:   4.4.4.10
```

```
control teid local:  0x0210001F
control teid remote: 0x00000041
data teid local:     0x02100020
data teid remote:    0x00000042
primary pdp: Y           nsapi: 1
signal_sequence:  1                  seq_tpdu_up:      0
seq_tpdu_down:    0
upstream_signal_flow:   0            upstream_data_flow:   0
downstream_signal_flow: 0            downstream_data_flow: 0
RAupdate_flow:          0
pdp_create_time:   Feb 15 2010 04:07:59
last_access_time:  Feb 15 2010 04:07:59
mnrgflag:          0               tos mask map: B8
session timeout: 86400
idle timeout: 720000
umts qos_req:0911016901010111050101
umts qos_neg:0911016901010111050101
QoS class:interactive
QoS for charging:       qos_req:000000      qos_neg:000000
rcv_pkt_count:       10026         rcv_byte_count:    1824732
send_pkt_count:      5380          send_byte_count:   4207160
cef_up_pkt:        0             cef_up_byte:      0
cef_down_pkt:      0             cef_down_byte:    0
cef_drop:          0             out-sequence pkt: 0
charging_id:         42194519
visitor: No          roamer: Unknown
charging characteristics:          1
charging characteristics received: 0
csg: csggroup1, address: 75.75.75.1
pdp reference count: 2
primary dns:         0.0.0.0
secondary dns:       0.0.0.0
primary nbns:        0.0.0.0
secondary nbns:      0.0.0.0
ntwk_init_pdp:       0
single pdp-session: Disabled

absolute session start time:   NOT SET
Accounting Session ID: 161616010283D657
Periodic accounting interval: NOT SET
AAA Unique ID: 16 (0x10)
Interim Update statistics:
    records sent 0, records failed 0
Direct Tunnel: Disabled
Eggsn mode: 0x06 (QS: disabled, EGCDR: enabled, SVC-MESG: enabled)
PDP internal flags: 7C0001
MCB internal flags: 0
```

Configuration Examples

This section includes the following examples:

- UMTS QoS Configuration Examples, page 11-23
- CAC Configuration Example, page 11-24
- Per-PDP Policing Configuration Example, page 11-26

UMTS QoS Configuration Examples

Supervisor Engine Configuration:

```
Mls qos

Mls qos map dscp-cos 18 20 22 to 5
Mls qos map dscp-cos 26 to 4
Mls qos map dscp-cos 28,30 to 3


Access-list 101 permit ip any any dscp ef
Access-list 102 permit ip any any dscp af21
Access-list 103 permit ip any any dscp af31
Access-list 103 permit ip any any dscp af32
Access-list 103 permit ip any any dscp af33
Access-list 104 permit ip any any

Class-map match-all conversational
    Match access-group 101
Class-map match-all streaming
    Match access-group 102
Class-map match-all interactive
    Match access-group 103
Class-map match-all background
    Match access-group 104


Mls qos aggregate-policer AGGREGATE-CONV <bit rate1> <normal-burst> <max-burst>
Conform-action transmit exceed-action drop
Mls qos aggregate-policer AGGREGATE-STREAMING <bit rate2> <normal-burst> <max-burst>
conform-action transmit exceed-action drop
Mls qos aggregate-policer AGGREGATE-INTERACTIVE <bit rate3> <normal-burst> <max-burst>
conform-action transmit exceed-action drop
Mls qos aggregate-policer AGGREGATE-BACKGROUND <bit rate4> <normal-burst> <max-burst>
conform-action transmit exceed-action drop

Policy-map Gi-incoming
    Class conversational
        Police aggregate AGGREGATE-CONV
    Class streaming
        Police aggregate AGGREGATE-STREAMING
    Class interactive
        Police aggregate AGGREGATE-INTERACTIVE
    Class background
        Police aggregate AGGREGATE-BACKGROUND


Interface FastEthernet2/1
    Description "Gi interface"
    Mls qos trust dscp
    Wrr-queue cos-map 1 1 3
         Wrr-queue cos-map 1 2 4
         Wrr-queue bandwidth 50 40 10
    Service-policy input Gi-incoming

Interface FastEthernet2/2
    Description "Gn interface"
    Mls qos trust dscp
```

GGSN Configuration

```
Gprs qos map umts

Class-map match-all conversational
    Match ip dscp 46
Class-map match-any interactive
    Match ip dscp 26
    Match ip dscp 28
    Match ip dscp 30
Class-map match-any streaming
    Match ip dscp 18
    Match ip dscp 20
    Match ip dscp 22
Class-map match-all signaling
    Match ip dscp 40
Class-map match-any background
    Description default class
    Match ip dscp 0

Policy-map sami-output
    Class conversational
        Priority percent 5
    Class streaming
        Priority percent 15
    Class interactive
        Bandwidth 20
    Class background
        Bandwidth 20
    Class signaling
        Bandwidth 15

interface Gigabitthernet 0/0
        bandwidth 250000
        service-policy output max-output
```

CAC Configuration Example

The following is a configuration example of CAC and QoS implemented on a GGSN running on the Cicso SAMI in a Cisco 7600 series router.

```
!Enable UMTS QoS Mapping

gprs qos map umts

!Create CAC Maximum QoS authorization policy
gprs qos cac-policy abc_qos_policy1
  maximum pdp-context 1200 threshold 1000
  maximum traffic-class conversational
  mbr traffic-class conversational 100 uplink
  mbr traffic-class conversational 100 downlink
  mbr traffic-class streaming 100 uplink
  mbr traffic-class streaming 100 downlink
  mbr traffic-class interactive 120 uplink
  mbr traffic-class interactive 120 downlink
  mbr traffic-class background 120 uplink
  mbr traffic-class background 120 downlink
  gbr traffic-class conversational 64 uplink
  gbr traffic-class conversational 80 uplink
  gbr traffic-class streaming 80 downlink
  gbr traffic-class streaming 80 downlink
```

```
gprs qos cac-policy max_qos_policy2
  maximum pdp-context 1500
  maximum traffic-class interactive priority 1
  mbr traffic-class interactive 200
  mbr traffic-class background 150

! Create class-map to classify UMTS traffic class

class-map match-any conversational
  match ip dscp ef

class-map match-any streaming
  match ip dscp af21
  match ip dscp af22
  match ip dscp af23

class-map match-any interactive
  match ip dscp af31
  match ip dscp af32
  match ip dscp af33

class-map match-any background
  match ip dscp default

!Create traffic policy

policy-map ggsn1_traffic_policy
  class conversational
  priority percent 25

class streaming
  bandwidth percent 20

class interactive
  bandwidth percent 20
  random-detect dscp-based

 class background
  bandwidth percent 10
  random-detect dscp-based

! Create bandwidth pool

gprs qos bandwidth-pool ggsn1_bw_pool
  bandwidth 500000

  traffic-class streaming percent 20
  traffic-class interactive percent 20
  traffic-class background percent 10

! Set interface bandwidth

int gigabitEthernet 0/0
  bandwidth  500000
  service-policy output ggsn1_traffic_policy

!Attach bandwidth pool to the APN

gprs access-point-list gprs
 access-point 1
  access-point-name abc.com
  cac-policy abc_qos_policy1
  bandwidth-pool output ggsn1_bw_pool
```

```
 bandwidth-pool input ggsn1_bw_pool

access-point 2
 access-point-name xyz.com
 cac-policy xyz_qos_policy1
 bandwidth-pool output ggsn1_bw_pool
 bandwidth-pool input ggsn1_bw_pool
```

Per-PDP Policing Configuration Example

The following is a configuration example of per-pdp policing.

```
! Create a class for PDP flows
class-map class-pdp
  Match flow pdp
```

```
! Create a policy map and assign a class to the map
policy-map policy-gprs
  class class-pdp

! Configure traffic policing
  police rate pdp conform-action action exceed-action action violate-action action

! Attach a service policy to an APN
gprs access-point-list gprs
 access-point 1
  service-policy in policy-gprs
```

CHAPTER 12

Configuring Security on the GGSN

This chapter describes how to configure security features on the gateway GPRS support node (GGSN), including Authentication, Authorization, and Accounting (AAA), and RADIUS.

Note IPSec on the Cisco 7600 series router platform is performed on the IPSec VPN Acceleration Services module and requires no configuration on the GGSNs running on the Cisco SAMI.

For information about configuring IPSec on the Cisco 7600 series router platform, see *IPSEC VPN Acceleration Services Module Installation and Configuration Not*e.

The security configuration procedures and examples in this publication (aside from those related to GGSN-specific implementation) describe the basic commands that you can use to implement the security services.

For more detailed information about AAA, RADIUS, and IPSec security services in the Cisco IOS software, see *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications. For information about IPSec security services on Cisco 7600 platform, see *IPSec VPN Acceleration Services Module Installation and Configuration Note*.

For complete descriptions of the GGSN commands in this chapter, see *Cisco GGSN Command Reference* for the Cisco GGSN release you are using. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

This chapter includes the following sections:

- Overview of Security Support on the GGSN, page 12-2
- Configuring AAA Security Globally, page 12-4 (Required)
- Configuring RADIUS Server Communication Globally, page 12-5 (Required)
- Configuring RADIUS Server Communication at the GGSN Configuration Level, page 12-6 (Required)
- Configuring Additional RADIUS Services, page 12-10 (Optional)
- Securing the GGSN Gn Interface, page 12-28 (Optional)
- Segregating GRX Traffic on GGSN Gn Interface, page 12-31
- Configuring Simultaneous Broadcast and Wait Accounting, page 12-31 (Optional)
- Periodic Accounting Timer, page 12-33 (Optional)
- Implementing Lawful Intercept Support on the Cisco GGSN (Optional)
- Configuration Examples, page 12-45

Overview of Security Support on the GGSN

The GGSN supports many of the same levels of security that are available through the Cisco IOS software on the router, including the following types of security:

- Authentication, authorization, and accounting (AAA) network security services and server groups
- RADIUS security services
- IP Security Protocol (IPSec)

In addition, the GGSN software provides the ability to configure additional security features such as the following:

- Address verification
- Traffic redirection
- IP access lists

AAA and RADIUS support provides the security services to authenticate and authorize access by mobile users to the GGSN and its access point names (APNs). IPSec support allows you to secure your data between the GGSN and its associated peers.

In some cases, such as with AAA and IPSec support, the GGSN works with the standard Cisco IOS software configuration without requiring configuration of any additional GGSN commands.

With RADIUS server configuration, the GGSN requires that you enable AAA security and establish RADIUS server communication globally on the router. From there, you can configure RADIUS security for all GGSN access points, or per access point, using new GGSN configuration commands.

Note In addition to the AAA, RADIUS, and IPSec security services, the GGSN also supports IP access lists to further control access to APNs. The Cisco IOS GGSN software implements the new **ip-access-group** command in access-point configuration mode to apply IP access list rules at an APN.

AAA Server Group Support

The Cisco GGSN supports authentication and accounting at APNs using AAA server groups. By using AAA server groups, you gain the following benefits:

- You can selectively implement groups of servers for authentication and accounting at different APNs.
- You can configure different server groups for authentication services and accounting services in the same APN.
- You can control which RADIUS services you want to enable at a particular APN, such as AAA accounting.

For GPRS tunneling protocol (GTP)-PPP termination and GTP-PPP regeneration on the GGSN, transparent access mode is used to allow PPP to perform the appropriate AAA functions; however, you can still configure AAA server groups to specify the corresponding server groups for AAA support.

The GGSN supports the implementation of AAA server groups at both the global and access-point configuration levels. You can minimize your configuration by specifying the configuration that you want to support across most APNs, at the global configuration level. Then, at the access-point configuration level, you can selectively modify the services and server groups that you want to support at a particular APN. Therefore, you can override the AAA server global configuration at the APN configuration level.

To configure a default AAA server group to use for all APNs on the GGSN, use the **gprs default aaa-group** command in global configuration mode. To specify a different AAA server group to use at a particular APN for authentication or accounting, use the **aaa-group** command in access-point configuration mode.

If authentication is enabled on the APN, then the GGSN first looks for an authentication server group at the APN. If an authentication server group is not found at the APN, then the GGSN looks for a globally configured, General Packet Radio Service/Universal Mobile Telecommunication System (GPRS/UMTS) default authentication server group.

If accounting is enabled on the APN, then the GGSN looks for an accounting server group at the APN or globally in the following order:

- First, at the APN for an accounting server group—configured in the **aaa-group accounting** command.
- Second, for a global GPRS/UMTS default accounting server group—configured in the **gprs default aaa-group accounting** command.
- Third, at the APN for an authentication server group—configured in the **aaa-group authentication** command.
- Last, for a global GPRS/UMTS default authentication server group—configured in the **gprs default aaa-group authentication** command.

To complete the configuration, you also must specify the following configuration elements on the GGSN:

- Configure the RADIUS servers by using the **radius-server host** command.
- Define a server group with the IP addresses of the AAA servers in that group, using the **aaa group server** command in global configuration mode.
- Enable the type of AAA services (accounting and authentication) to be supported on the APN.
  - The GGSN enables accounting by default for non-transparent APNs.

    You can disable accounting services at the APN by using the **aaa-accounting disable** command.
  - You can enable authentication at the APN level by configuring the **access-mode non-transparent** command. When you enable authentication, the GGSN automatically enables accounting on the APN. There is not a global configuration command for enabling or disabling authentication.
- Configure AAA accounting and authentication using the **aaa accounting** and **aaa authentication** commands in global configuration mode.

Note For more information about AAA and RADIUS global configuration commands, see *Cisco IOS Security Command Reference.*

Configuring AAA Security Globally

Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which you set up access control on your GGSN. This section provides information about the basic commands used to implement AAA security on a Cisco router.

To enable AAA and configure authentication and authorization, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa new-model`	Enables AAA globally.
Step 2	`Router(config)# aaa authentication ppp {default | list-name} method1 [method2...]`	Creates a local authentication method list, with the following options: • **default**—Specifies that the authentication methods that follow this argument are the default list of authentication methods when a user logs in to the router. • *method*—Specifies a valid AAA authentication method for PPP. For example, **group** (RADIUS) enables global RADIUS authentication.
Step 3	`Router(config)# aaa authorization {auth-proxy | network | exec | commands level | reverse-access} {default | list-name} [method1 [method2...]]`	Creates an authorization method list for a particular authorization type and enables authorization.
Step 4	`Router(config)# aaa accounting {system default [vrf vrf-name] | network {default | none | start-stop | stop-only | wait-start} group group-name`	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS.

For more information about configuring AAA, see *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications.

Configuring RADIUS Server Communication Globally

This section describes how to configure a global RADIUS server host that the GGSN can use to authenticate and authorize users. You can configure additional RADIUS server communication at the GGSN global configuration level.

To globally configure RADIUS server communication on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]`	Specifies the IP address or hostname of the remote RADIUS server host. The following options are available: • **auth-port**—Specifies the User Datagram Protocol (UDP) destination port for authentication requests. • **acct-port**—Specifies the UDP destination port for accounting requests. • **timeout**—Specifies the time interval (in the range 1 to 1000 seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the **radius-server timeout** command. If no timeout value is specified, the global value is used. • **retransmit**—Specifies the number of times (in the range 1 to 100) a RADIUS request is re-sent to a server, if that server is not responding or is responding slowly. This setting overrides the global value of the **radius-server retransmit** command. • **key**—Specifies the authentication and encryption key used between the router and the RADIUS daemon running on this RADIUS server. This setting overrides the global value of the **radius-server key** command.
Step 2	`Router(config)# radius-server key string`	Specifies the shared secret text string used between the router and the vendor-proprietary RADIUS server. The router and the RADIUS server use this text string to encrypt passwords and exchange responses.

For more information about configuring RADIUS security, see *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications. For an example, see the "RADIUS Server Global Configuration Example" section on page 12-46.

Note Although you can configure the **radius-server host** command multiple times, the Cisco IOS software supports only one RADIUS server at the same IP address.

Configuring RADIUS Server Communication at the GGSN Configuration Level

To complete the security configuration for the GGSN, you must configure non-transparent access for each access point. When you configure security at the GGSN global configuration level, you can also configure RADIUS server communication for all access points or for a specific access point.

Configuring RADIUS at the GGSN global configuration level includes the following tasks:

- Configuring Non-Transparent Access Mode, page 12-6 (Required)
- Specifying an AAA Server Group for All Access Points, page 12-7 (Optional)
- Specifying an AAA Server Group for a Particular Access Point, page 12-8 (Optional)
- Configuring AAA Accounting Services at an Access Point, page 12-8 (Optional)

Configuring Non-Transparent Access Mode

To support RADIUS authentication on the GGSN, you must configure the GGSN access points for non-transparent access. You must configure non-transparent access for every access point at which you want to support RADIUS services. There is no way to globally specify the access mode.

Note For GTP-PPP termination and GTP-PPP regeneration on the GGSN, transparent access mode is used to allow PPP to perform the appropriate AAA functions; however, you can still configure AAA server groups to specify the corresponding server groups for AAA support.

To configure non-transparent access for a GGSN access point, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs access-point-list` *list-name*	Specifies the access-point list name, and enters access-point list configuration mode.
Step 2	`Router(config-ap-list)# access-point` *access-point-index*	Specifies the number associated with an existing access point definition (or creates a new access point), and enters access point configuration mode.
Step 3	`Router(config-access-point)# access-mode non-transparent`	Specifies that the GGSN requests user authentication at the access point to a PDN.

For more information about configuring GGSN access points, see the "Configuring Access Points on the GGSN" section on page 9-7.

Specifying an AAA Server Group for All Access Points

After you have configured RADIUS server communication at the global level, you can configure a default AAA server group for all GGSN access points to use.

To specify a default AAA server group for all GGSN access points, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs default aaa-group {authentication | accounting} server-group`	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN, where: • **authentication**—Assigns the selected server group for authentication services on all APNs. • **accounting**—Assigns the selected server group for accounting services on all APNs. • *server-group*—Specifies the name of an AAA server group to use for AAA services on all APNs. **Note** The name of the AAA server group that you specify must correspond to a server group that you configure using the **aaa group server** command.

Specifying an AAA Server Group for a Particular Access Point

To override the default AAA server group configured for all access points, you can specify a different AAA server group for a particular access point. Or, if you choose not to configure a default AAA server group, you can specify an AAA server group at each access point.

To specify an AAA server group for a particular access point, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# aaa-group {authentication | accounting} server-group`	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN, where: • **authentication**—Assigns the selected server group for authentication services on the APN. • **accounting**—Assigns the selected server group for accounting services on the APN. • *server-group*—Specifies the name of an AAA server group to use for AAA services on the APN. **Note** The name of the AAA server group that you specify must correspond to a server group that you configure using the **aaa group server** command.

Configuring AAA Accounting Services at an Access Point

The Cisco GGSN has different defaults for enabling and disabling accounting services for transparent and non-transparent access points:

- If you configure an APN for non-transparent access using the **access-mode** command, the GGSN automatically enables accounting with authentication at the APN.
- If you configure an APN for transparent access, which is the default access mode, the GGSN automatically disables accounting at the APN.

Therefore, if you have configured a transparent access APN and you want to provide accounting at that APN, you need to configure the **aaa-accounting enable** command at the APN.

However, for accounting to occur, you also must complete the configuration by specifying the following other configuration elements on the GGSN:

- Enable AAA services by using the **aaa new-model** command in global configuration mode.
- Define a server group with the IP addresses of the RADIUS servers in that group by using the **aaa group server** command in global configuration mode.

- Configure the following AAA services:
  - AAA authentication using the **aaa authentication** command in global configuration mode
  - AAA authorization using the **aaa authorization** command in global configuration mode
  - AAA accounting using the **aaa accounting** command in global configuration mode
- Assign the type of services that the AAA server group should provide. If you want the server group to only support accounting services, then you need to configure the server for accounting only. You can assign the AAA services to the AAA server groups either at the GGSN global configuration level by using the **gprs default aaa-group** command, or at the APN by using the **aaa-group** command.
- Configure the RADIUS servers by using the **radius-server host** command.

Note For more information about AAA and RADIUS global configuration commands, see *Cisco IOS Security Command Reference.*

To selectively disable accounting at specific APNs where you do not want that service, use the **aaa-accounting disable** command in access-point configuration mode.

There is not a **no** form of this command.

Enabling and Disabling Accounting Services on an Access Point

The Cisco Systems GGSN has different defaults for enabling and disabling accounting services for transparent and non-transparent access points:

- If you configure an APN for non-transparent access using the **access-mode** command, the GGSN automatically enables accounting with authentication at the APN.
- If you configure an APN for transparent access, which is the default access mode, the GGSN automatically disables accounting at the APN.

To selectively disable accounting at specific APNs where you do not want that service, use the **aaa-accounting disable** command in access-point configuration mode.

Configuring Interim Accounting on an Access Point

Using the **aaa-accounting** command in access-point configuration mode with an **interim** keyword option specified, you can configure the GGSN to send Interim-Update Accounting requests to the AAA server.

Note Interim accounting support requires that accounting services be enabled for the APN and that the **aaa accounting update newinfo** command in global configuration mode be configured.

To configure accounting services at an access point, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# aaa-accounting [enable | disable | interim {update | periodic` *minutes* `| periodic radius}]`	Configures accounting services on an access point on the GGSN, with the following options: • **enable**—(Optional) Enables accounting services on an access point on the GGSN. • **disable**—(Optional) Disables accounting services on an access point on the GGSN. • **interim update**—(Optional) Enables interim accounting records to be sent to an accounting server when a routing area update (resulting in a serving GPRS support node [SGSN] change) or QoS change has occurred. • **interim periodic** *minutes*—(Optional) Enables interim periodic accounting records to be sent to an accounting server on regular configured intervals. • **interim periodic radius—**(Optional) Enables GGSN to accept the periodic accounting value (Attribute 85) sent by RADIUS.

Configuring Additional RADIUS Services

This section describes how to configure RADIUS security services that the GGSN can use to authenticate and authorize users.

This section includes the following tasks:

- Configuring RADIUS Attributes in Access Requests to the RADIUS Server, page 12-11
- Configuring the Vendor-Specific Attribute in Access Requests to the RADIUS Server, page 12-13
- Suppressing Attributes for RADIUS Authentication, page 12-14
- Obtaining DNS and NetBIOS Address Information from a RADIUS Server, page 12-16
- Configuring the RADIUS Packet of Disconnect, page 12-16
- Configuring the GGSN to Wait for a RADIUS Response, page 12-18
- Configuring Access to a RADIUS Server Using VRF, page 12-19
- Configuring RADIUS Change of Authorization Support, page 12-28

Configuring RADIUS Attributes in Access Requests to the RADIUS Server

You configure the how the GGSN sends RADIUS attributes in access requests to the RADIUS server. This section includes the following tasks:

- Configuring the CHAP Challenge, page 12-11
- Configuring the MSISDN IE, page 12-11
- Configuring the NAS-Identifier, page 12-11
- Configuring the Charging ID in the Acct-Session-ID Attribute, page 12-12
- Configuring the MSISDN in the User-Name Attribute, page 12-12

Configuring the CHAP Challenge

To specify to always include the Challenge Handshake Authentication Protocol (CHAP) challenge in the Challenge Attribute field (and not in the Authenticator field) in access requests to the RADIUS server, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs radius attribute chap-challenge`	Specifies that the CHAP challenge is always included in the challenge attribute in a RADIUS request.

Note When the **gprs radius attribute chap-challenge** command is configured, the CHAP challenge is always sent in the Challenge Attribute field of an access request to the RADIUS server and not in the Authenticator field. When the command is not configured, the CHAP challenge is sent in the Authenticator field unless the challenge exceeds 16 bytes, in which case, it is sent in the Challenge Attribute field of the Access Request.

Configuring the MSISDN IE

To specify that the first byte of the mobile station ISDN (MSISDN) information element (IE) is included in access requests to the RADIUS server, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs radius msisdn first-byte`	Specifies that the first byte of the MSISDN IE is included in access requests.

Configuring the NAS-Identifier

You can configure the GGSN to send the network access server (NAS)-Identifier (RADIUS attribute 32) in access requests to a RADIUS server at a global or APN level. The APN-level configuration overrides the global-level configuration.

To specify to include the NAS-Identifier in all access requests, use the following command in global configuration mode:

Command	Purpose
`Router(config)# radius-server attribute 32 include-in-access-req format` *format*	Specifies that the GGSN sends the RADIUS attribute 32 (NAS-Identifier) in access requests where *format* is a string sent in attribute 32 containing an IP address (%i), a hostname (%h), and a domain name (%d).

To disable this global configuration, use the **no** form of this command in global configuration mode.

To specify to include the NAS-Identifier in all access requests at an APN, use the following command in access point configuration mode:

Command	Purpose
`Router(config-access-point)# radius attribute nas-id` *format*	Specifies that the GGSN sends the NAS-Identifier in access requests at an APN where *format* is a string sent in attribute 32 containing an IP address (%i), a hostname (%h), and a domain name (%d).

To disable this APN configuration, use the **no** form of this command in access point configuration mode.

Configuring the Charging ID in the Acct-Session-ID Attribute

To specify that the GGSN include the charging ID in the Acct-Session-ID (attribute 44) in accounting requests at an APN, use the following command in access-point configuration mode:

Command	Purpose
`Router(config)# radius attribute acct-session-id charging-id`	Specifies that the charging ID in the Acct-Session-ID (attribute 44) is included in accounting requests.

To disable this APN configuration, use the **no** form of this command in access point configuration mode.

Configuring the MSISDN in the User-Name Attribute

To specify that the GGSN include the MSISDN in the User-Name attribute (attribute 1) in access requests at an APN, use the following command in access-point configuration mode:

Command	Purpose
`Router(config)# radius attribute user-name msisdn`	Specifies that the MSISDN is included in the User-Name (attribute 1) field in access requests.

To disable this APN configuration, use the **no** form of this command in access point configuration mode.

Configuring the Vendor-Specific Attribute in Access Requests to the RADIUS Server

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information to the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) make a larger set of information available for communication by allowing vendors to support their own extended attributes not suitable for general use.

Table 12-1 lists and describes the Third Generation Partnership Project (3GPP) VSA sub-attributes that the GGSN can send in authentication and accounting requests to a RADIUS server when the attribute 26 is configured.

Table 12-1 3GPP VSA Sub-Attributes

Number	Vendor-Proprietary Attribute	Description
1	3GPP-IMSI	International Mobile Subscriber Identity (IMSI) number for a user. This sub-attribute can be suppressed using the **radius attribute suppress imsi** command.
2	3GPP-Charging-Id	Charging ID for this PDP context.
3	3GPP-PDP-Type	Type of PDP context (for example, IP or PPP).
4	3GPP-CG-Address	IP address of the current active charging gateway. If there is no current active charging gateway, GGSN sends 0.0.0.0.
5	3GPP-GPRS-QoS-Profile	QoS negotiated values. This sub-attribute can be suppressed using the **radius attribute suppress qos** command.
6	3GPP-SGSN-Address	IP address of the SGSN that is used by the GTP control plane for handling control messages. This address might be used to identify the public land mobile network (PLMN) to which the user is attached. This sub-attribute can be suppressed using the **radius attribute suppress sgsn-address** command.
7	3GPP-GGSN-Address	IP address of the GGSN that is used by the GTP control plane for the context establishment. This address is the same as the GGSN IP address used in gateway GPRS support node-call detail records (G-CDRs) .
8	3GPP-IMSI-MCC-MNC	Mobile country code (MCC) and mobile network code (MNC) extracted from the user's IMSI number (the first 5 or 6 digits depending on the IMSI). This sub-attribute requires that the MCC and MNC values that the GGSN uses be configured using the **gprs mcc mnc** command in global configuration mode.

Table 12-1 3GPP VSA Sub-Attributes (continued)

Number	Vendor-Proprietary Attribute	Description
9	3GPP-GGSN-MCC-MNC	MCC and MNC of the network to which the GGSN belongs. This sub-attribute requires that the MCC and MNC values that the GGSN uses be configured using the **gprs mcc mnc** command in global configuration mode.
12	3GPP-Selection-Mode	Selection mode for this PDP context received in the Create PDP Context request.
18	3GPP-SGSN-MCC-MNC	Encoding of the Routing Area Identity (RAI) MCC-MNC values.

To configure the GGSN to send and recognize VSAs as defined by RADIUS attribute 26, use the following command in global configuration mode:

Command	Purpose
`Router(config)#radius-server vsa send [accounting | authentication]`	(Optional) Enables the GGSN to send and recognized VSAs as defined by RADIUS IETF attribute 26.

For more information on configuring the use of vendor-specific attributes, see *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications.

Suppressing Attributes for RADIUS Authentication

You can configure the GGSN to suppress certain attributes in its access requests to a RADIUS server. The following sections describe the attributes you can suppress and how to do so.

The following topics are included in this section:

- Suppressing the MSISDN Number for RADIUS Authentication, page 12-14
- Suppressing the 3GPP-IMSI VSA Sub-Attribute for RADIUS Authentication, page 12-15
- Suppressing the 3GPP-GPRS-QoS Profile VSA Sub-Attribute for RADIUS Authentication, page 12-15
- Suppressing the 3GPP-GPRS-SGSN-Address VSA Sub-Attribute for RADIUS Authentication, page 12-15

Suppressing the MSISDN Number for RADIUS Authentication

Some countries have privacy laws that prohibit service providers from identifying the MSISDN number of mobile stations in authentication requests. Use the **msisdn suppression** command to specify a value that the GGSN sends instead of the MSISDN number in its authentication requests to a RADIUS server. If no value is configured, then no number is sent to the RADIUS server.

To use the **msisdn suppression** command, you must configure a RADIUS server either globally or at the access point and specify non-transparent access mode.

To specify that the GGSN override or suppress the MSISDN number in its access-requests sent to the RADIUS server, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# msisdn suppression [value]`	(Optional) Specifies that the GGSN overrides the MSISDN number with a preconfigured value in its access requests.

To disable this APN configuration, use the **no** form of this command in access point configuration mode.

Suppressing the 3GPP-IMSI VSA Sub-Attribute for RADIUS Authentication

To configure the GGSN to suppress the Third Generation Partnership Project (3GPP) vendor-specific attribute (VSA) 3GPP-International Mobile Subscriber Identity (3GPP-IMSI) number in its authentication and accounting requests to a RADIUS server, use the **radius attribute suppress imsi** command in access point configuration mode.

To configure the GGSN to suppress the 3GPP VSA 3GPP-IMSI number in its authentication and accounting requests to a RADIUS server, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# radius attribute suppress imsi`	(Optional) Configures the GGSN to suppress the 3GPP-IMSI number in its authentication and accounting requests to a RADIUS server.

To disable this APN configuration, use the **no** form of this command in access point configuration mode.

Suppressing the 3GPP-GPRS-QoS Profile VSA Sub-Attribute for RADIUS Authentication

To configure the GGSN to suppress the 3GPP-GPRS-Qos Profile in its authentication and accounting requests to a RADIUS server, use the **radius attribute suppress qos** command in access point configuration mode.

To configure the GGSN to suppress the 3GPP-GPRS-Qos Profile in its authentication and accounting requests to a RADIUS server, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# radius attribute suppress qos`	(Optional) Specifies that the GGSN suppresses the 3GPP-GPRS-Qos Profile in its authentication and accounting requests to a RADIUS server.

Suppressing the 3GPP-GPRS-SGSN-Address VSA Sub-Attribute for RADIUS Authentication

To configure the GGSN to suppress the 3GPP-GPRS-SGSN-Address in its authentication and accounting requests to a RADIUS server, use the **radius attribute suppress sgsn-address** command in access point configuration mode.

To specify that the GGSN suppress the 3GPP-GPRS-SGSN-Address in its authentication and accounting requests to a RADIUS server, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# radius attribute suppress sgsn-address`	(Optional) Specifies that the GGSN suppresses the 3GPP-GPRS-SGSN-Address in its requests.

Obtaining DNS and NetBIOS Address Information from a RADIUS Server

To obtain Domain Name System (DNS) address and Network Basic Input/Output System (NetBIOS) address information from a RADIUS server, configure the GGSN to send and recognize VSAs as defined by RADIUS attribute 26 using the following command in global configuration mode:

Command	Purpose
`Router(config)# radius-server vsa send [accounting | authentication]`	(Optional) Enables the GGSN to send and recognize VSAs as defined by RADIUS IETF attribute 26.

Note For the DNS and NetBIOS address information to be sent to an MS, the dynamic address allocation method using an IP address pool supplied by a RADIUS server must be configured for the access point by using the **ip-address-pool radius-client** command. For more information about configuring an access point, see the "Configuring Access Points on the GGSN" section on page 9-7.

Configuring the RADIUS Packet of Disconnect

The RADIUS Packet of Disconnect (PoD) feature is a method for terminating a user session after the session is established. The PoD is a RADIUS Disconnect-Req packet and is intended to be used in situations when an authenticating agent server wants to disconnect a user after a session is accepted by the RADIUS access-accept packet. For example, with pre-paid billing, a typical use of this feature would be for the pre-paid billing server to send a PoD when the quota expires for a pre-paid user.

Upon receiving a PoD, the GGSN performs the following actions:

- Identifies the PDP context for which the PoD was generated by the attribute information present in the PoD. The VSA sub-attributes 3GPP-IMSI and 3GPP-NSAPI uniquely identify a PDP context, and the presence of these sub-attributes in a POD also identifies that the POD is for a GPRS user session.
- Sends a Delete PDP Context request to the SGSN.
- Sends a Disconnect ACK or Disconnect NAK to the device that generated the POD. The GGSN sends a Disconnect ACK when it is able to terminate a user session and sends a Disconnect NAK when it is unable to terminate a user session. The Disconnect ACK/NAK requests are RADIUS packets that contain no attributes.

Note For the PoD feature to function properly on the GGSN, ensure that the IMSI attribute has not been suppressed using the **radius attribute suppress imsi** command.

To enable PoD support on the GGSN, use the following command in global configuration mode:

Command	Purpose
`Router(config)# aaa pod server [port port-number] [auth-type {any| all| session-key}] server-key [encryption-type] string`	Enables inbound user sessions to be disconnected when specific session attributes are presented. • **port** *port-number*—(Optional) Network access server User Datagram Protocol (UDP) port for PoD requests. Default value is 1700. This is the port on which GGSN listens for the PoD requests. • **auth-type**—(Optional) Type of authorization required for disconnecting sessions. – **any**—Session that matches all of the attributes sent in the PoD packet is disconnected. The PoD packet may contain one or more of four key attributes (user-name, framed-IP-address, session-ID, and session-key). – **all**—Only a session that matches all four key attributes is disconnected. **All** is the default. – **session-key**—Session with a matching session-key attribute is disconnected. All other attributes are ignored. **Note** When configuring a PoD on the GGSN, we recommend that you do not configure the **auth-type** keyword option. • **server-key**—Configures the shared-secret text string. • *encryption-type*—(Optional) Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using an encryption algorithm defined by Cisco. • *string*—Shared-secret text string that is shared between the network access server and the client workstation. This shared-secret string must be the same on both systems.

Configuring the GGSN to Wait for a RADIUS Response

Use the **gtp response-message wait-accounting** command to configure the GGSN to wait for a RADIUS accounting response from the RADIUS accounting server before sending a Create PDP Context response to the SGSN.

If the GGSN does not receive a response from the RADIUS accounting server when you have configured the **gtp response-message wait-accounting** command, it rejects the PDP context request.

When broadcast accounting is used (accounting requests are sent to multiple RADIUS servers), if a RADIUS server responds with an accounting response, the GGSN sends a Create PDP Context response and does not wait for the other RADIUS servers to respond.

The GGSN supports configuration of RADIUS response message waiting at both the global and access-point configuration levels. You can minimize your configuration by specifying the configuration that you want to support across most APNs, at the global configuration level. Then, at the access-point configuration level, you can selectively modify the behavior that you want to support at a particular APN. Therefore, at the APN configuration level, you can override the global configuration of RADIUS response message waiting.

To configure the GGSN to wait for a RADIUS accounting response as the default behavior for all APNs, use the **gprs gtp response-message wait-accounting** command in global configuration mode. To disable this behavior for a particular APN, use the **no gtp response-message wait-accounting** command in access-point configuration mode.

To verify whether RADIUS response message waiting is enabled or disabled at an APN, you can use the **show gprs access-point** command and observe the value reported in the wait_accounting output field.

To configure the GGSN to wait for a RADIUS accounting response globally, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs gtp response-message wait-accounting`	Configures the GGSN to wait for a RADIUS accounting response before sending a Create PDP Context response to the SGSN, for Create PDP Context requests received across all access points.

To configure the GGSN to wait for a RADIUS accounting response for a particular access point, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# gtp response-message wait-accounting`	Configures the GGSN to wait for a RADIUS accounting response before sending a Create PDP Context response to the SGSN, for Create PDP Context requests received at a particular access point.

Configuring Access to a RADIUS Server Using VRF

The Cisco IOS GGSN software supports access to a RADIUS server using VRF. This Cisco IOS software feature is called *Per VRF AAA* and using this feature, Internet service providers (ISPs) can partition AAA services based on VRF. This permits the GGSN to communicate directly with the customer RADIUS server associated with the customer Virtual Private Network (VPN) without having to go through a RADIUS proxy. Thus, ISPs can scale their VPN offerings more efficiently because they no longer need to proxy AAA to provide their customers the flexibility demanded.

To support this configuration, AAA must be VRF aware. ISPs must define multiple instances of the same operational parameters—such as AAA server groups, method lists, system accounting, and protocol-specific parameters—and secure the parameters to the VRF partitions.

Note VRF is not supported on the Cisco 7600 Supervisor II / MSFC2; therefore, if using the Supervisor II, you must tunnel encapsulated VRF traffic through the Supervisor via a GRE tunnel between the GGSN to RADIUS server. For more information on configuration a GRE tunnel, see "Configuring Access to a RADIUS Server With a Tunnel" section on page 12-24.

The Cisco 7600 Sup720 supports VRF.

If an AAA configuration, such as a method list, is uniquely defined many times, the specification of an AAA server that is based on IP addresses and port numbers might create an overlapping of private addresses between VRFs. Securing AAA method lists to a VRF can be accomplished from one or more of the following sources:

- Virtual Template—Used as a generic interface configuration.
- Service Provider AAA server—Used to associate a remote user with a specific VPN based on the domain name or Dialed Number Identification Service (DNIS). The server then provides the VPN-specific configuration for the virtual access interface, which includes the IP address and port number of the customer AAA server.
- Customer VPN AAA server—Used to authenticate the remote user and to provide user-specific configurations for the virtual access interface.

Note Global AAA accounting configurations and some AAA protocol-specific parameters cannot be logically grouped under the Virtual Template configuration.

When configuring the Per VRF feature, keep in mind the following:

- To prevent possible overlapping of private addresses between VRFs, define AAA servers in a single global pool that is used in the server groups.
- Servers can no longer be uniquely identified by IP addresses and port numbers.

- "Private" servers (servers with private addresses within the default server group that contains all the servers) can be defined within the server group and remain hidden from other groups. The list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

Note If private server parameters are not specified, global configurations are used. If global configurations are not specified, default values are used.

- All server operational parameters can be configured per host, per server group, or globally. Per-host configurations have precedence over per-server group configurations. Per-server group configurations have precedence over global configurations.

Note For complete information on configuring access to a RADIUS server using VRF, see *Per VRF AAA* feature module.

This section describes configuring and establishing access to a private RADIUS server using VRF. For global RADIUS services, ensure that you have configured a globally located server.

To configure access to a RADIUS server using VRF, complete the following tasks:

- Enabling AAA Globally, page 12-20 (Required)
- Configuring a VRF-Aware Private RADIUS Server Group, page 12-21 (Required)
- Configuring Authentication, Authorization, and Accounting Using Named Method Lists, page 12-22 (Required)
- Configuring a VRF Routing Table, page 12-22 (Required)
- Configuring VRF on an Interface, page 12-22 (Required)
- Configuring VRF Under an Access Point for Access to the Private RADIUS Server, page 12-23 (Required)
- Configuring a Route to the RADIUS Server Using VRF, page 12-27 (Optional)

Enabling AAA Globally

If AAA has not been enabled globally on the GGSN, you will need to enable it before configuring access to a private RADIUS server via VRF.

To enable AAA globally, use the following command in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa new-model`	Enables AAA globally.

Configuring a VRF-Aware Private RADIUS Server Group

To configure private server operational parameters, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa group server radius group-name`	Groups different RADIUS server hosts into distinct lists and distinct methods. • *group-name*—Character string used to name the group of servers.
Step 2	`Router(config-sg-radius)# server-private ip-address auth-port port_num acct-port port_num key string`	Configures the IP address of the private RADIUS server for the group server. • *ip-address*—Specifies the IP address of the private RADIUS server host. • **auth-port** *port_num*—Specifies a port solely for authentication. • **acct-port** *port_num*—Specifies a port solely for accounting. • *string*—(Optional) Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server. **Note** If private server parameters are not specified, global configurations are used. If global configurations are not specified, default values are used.
Step 3	`Router(config-sg-radius)# ip vrf forwarding vrf-name`	Configures the VRF reference of the AAA RADIUS server group. • *vrf-name*—Name assigned to a VRF.

Configuring Authentication, Authorization, and Accounting Using Named Method Lists

To configure AAA using named method lists, perform the following tasks, beginning in global configuration mode:

Step 1	`Router(config)# aaa authentication ppp {default	list-name} method1 [method2...]`	Creates a local authentication method list, with the following options: • **default**—Specifies that the authentication methods that follow this argument are the default list of authentication methods when a user logs in to the router. • *method*—Specifies a valid AAA authentication method for PPP. For example, **group RADIUS** enables global RADIUS authentication.
Step 2	`Router(config)# aaa authorization {auth-proxy	network	exec	commands level	reverse-access} {default	list-name} [method1 [method2...]]`	Creates an authorization method list for a particular authorization type and enables authorization.
Step 3	`Router(config)# aaa accounting {system default [vrf vrf-name]	network {default	none	start-stop	stop-only	wait-start} group group-name`	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS.

Configuring a VRF Routing Table

To configure a VRF routing table on the GGSN for access to the private RADIUS server, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ip vrf vrf-name`	Configures a VRF routing table, and enters VRF configuration mode.
Step 2	`Router(config-vrf)# rd route-distinguisher`	Creates routing and forwarding tables for a VRF and specifies the default route distinguisher for a VPN.

Configuring VRF on an Interface

To access the private RADIUS server, VRF must be configured on the interface to the server.

On the Cisco 7600 series router platform, this interface is a logical one (on which IEEE 802.1Q-encapsulation is configured) to a Layer 3 routed VLAN configured on the supervisor engine.

For more information about required VLANs on the supervisor engine, see the "Platform Prerequisites" section on page 3-2.

For more information about configuring interfaces, see *Cisco IOS Interface Configuration Guide* and the *Cisco IOS Interface Command Reference*.

Configuring 802.1Q-Encapsulated Subinterfaces

To configure a subinterface that supports IEEE 802.1Q encapsulation to the associated VLAN on the supervisor engine, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface gigabitethernet slot/port.subinterface-number`	Specifies the subinterface on which IEEE 802.1Q will be used.
Step 2	`Router(config-if)# encapsulation dot1q vlanid`	Defines the encapsulation format as IEEE 802.1Q (dot1q), and specifies the VLAN identifier.
Step 3	`Router(config-if)# ip address ip-address mask`	Sets a primary IP address for an interface.

Configuring VRF Under an Access Point for Access to the Private RADIUS Server

After you have completed the prerequisite configuration tasks, you can configure access to a RADIUS server with a tunnel or without a tunnel.

The following sections describe the different methods you can use to configure access a RADIUS server:

- Configuring Access to a RADIUS Server Without a Tunnel
- Configuring Access to a RADIUS Server With a Tunnel

Configuring Access to a RADIUS Server Without a Tunnel

To configure access to the RADIUS server without a tunnel, you need to configure the **vrf** command in access point configuration mode.

Note To configure access to a RADIUS server in the GPRS access point list, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs access-point-list list-name`	Specifies a name for a new access point list, or references the name of the existing access point list, and enters access-point list configuration mode.
Step 2	`Router(config-ap-list)# access-point access-point-index`	Specifies an index number for a new access point definition, or references an existing access point definition, and enters access point configuration mode.
Step 3	`Router(config-access-point)# access-point-name apn-name`	Specifies the network (or domain) name for a PDN that users can access from the GGSN at a defined access point. **Note** The *apn-name* must match the APN that is provisioned at the MS, HLR, and DNS server.

	Command	Purpose
Step 4	`Router(config-access-point)# aaa-group authentication server-group`	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN, where: • **authentication**—Assigns the selected server group for authentication services on the APN. • *server-group*—Specifies the name of a AAA server group to use for AAA services on the APN. **Note** The name of the AAA server group that you specify must correspond to a server group that you configure using the **aaa group server** command.
Step 5	`Router(config-access-point)# access-mode non-transparent`	Specifies for the GGSN to act as a proxy for authentication.
Step 6	`Router(config-access-point)# ip-address-pool radius-client`	Specifies for the RADIUS server to provide the IP address pool for the current access point. **Note** If you are using a dynamic address allocation method, then you must configure this command according to the appropriate IP address pool source.
Step 7	`Router(config-access-point)# vrf vrf-name`	Configures VPN routing and forwarding at a GGSN access point, and associates the access point with a particular VRF instance. **Note** The *vrf-name* argument should match the name of the VRF that you configured using the **ip vrf** command in the "Configuring Authentication, Authorization, and Accounting Using Named Method Lists" section on page 12-22.
Step 8	`Router(config-access-point)# exit`	Exits access point configuration mode.

Configuring Access to a RADIUS Server With a Tunnel

If you have only a single interface to a RADIUS server from which you need to access one or more private RADIUS servers, you can configure an IP tunnel to access those private servers.

To configure access to the RADIUS server using a tunnel, perform the following tasks:

- Configuring the Private RADIUS Server Access Point (Required)
- Configuring the IP Tunnel (Required)

Configuring the Private RADIUS Server Access Point

To configure access to a private RADIUS server in the GPRS access point list, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs access-point-list` *list-name*	Specifies a name for a new access point list, or references the name of the existing access point list, and enters access-point list configuration mode.
Step 2	`Router(config-ap-list)# access-point` *access-point-index*	Specifies an index number for a new access point definition, or references an existing access point definition, and enters access point configuration mode.
Step 3	`Router(config-access-point)# access-point name` *apn-name*	Specifies the access point network ID, which is commonly an Internet domain name. **Note** The *apn-name* must match the APN that is provisioned at the mobile station (MS), home location register (HLR), and DNS server.
Step 4	`Router(config-access-point)# access-mode` {**transparent** | **non-transparent**}	(Optional) Specifies whether the GGSN requests user authentication at the access point. The available options are: • **transparent**—No security authorization or authentication is requested by the GGSN for this access point. This is the default value. • **non-transparent**—GGSN acts as a proxy for authenticating.
Step 5	`Router(config-access-point)# access-type real`	Specifies an APN type that corresponds to an interface to an external network on the GGSN. Real is the default value.

	Command	Purpose
Step 6	`Router(config-access-point)# ip-address-pool {dhcp-proxy-client | radius-client | local pool-name | disable}`	(Optional) Specifies a dynamic address allocation method using IP address pools for the current access point. The available options are: • **dhcp-proxy-client**—DHCP server provides the IP address pool. • **radius-client**—RADIUS server provides the IP address pool. • **local**—Specifies that a local pool provides the IP address. This option requires that the address range be configured using the **aggregate** command in access point configuration mode and that a local pool is configured using the **ip local pool** command in global configuration mode. • **disable**—Turns off dynamic address allocation. **Note** If you are using a dynamic address allocation method, then you must configure this command according to the appropriate IP address pool source.
Step 7	`Router(config-access-point)# vrf vrf-name`	Configures VPN routing and forwarding at a GGSN access point and associates the access point with a particular VRF instance.
Step 8	`Router(config-access-point)# exit`	Exits access point configuration mode.

Configuring the IP Tunnel

When you configure a tunnel, you might consider using loopback interfaces as the tunnel endpoints instead of real interfaces because loopback interfaces are always up.

To configure an IP tunnel to a private network, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface tunnel number`	Configures a logical tunnel interface number.
Step 2	`Router(config-if)# ip vrf forwarding vrf-name`	Associates a VRF instance with the interface.
Step 3	`Router(config-if)# ip address ip-address mask [secondary]`	Specifies an IP address for the tunnel interface. **Note** This IP address is not used in any other part of the GGSN configuration.
Step 4	`Router(config-if)# tunnel source {ip-address | type number}`	Specifies the IP address (or interface type and port or card number) of the interface to the RADIUS server or a loopback interface.
Step 5	`Router(config-if)# tunnel destination {hostname | ip-address}`	Specifies IP address (or hostname) of the private network that you can access from this tunnel.

Configuring a Route to the RADIUS Server Using VRF

Be sure a route exists between the VRF instance and the RADIUS server. You can verify connectivity by using the **ping** command from the VRF to the RADIUS server. To configure a route, you can use a static route or a routing protocol.

Configuring a Static Route Using VRF

To configure a static route using, use the following command, beginning in global configuration mode:

Command	Purpose
`Router(config)# ip route vrf vrf-name prefix mask [next-hop-address] [interface {interface-number}] [global] [distance] [permanent] [tag tag]`	Configures a static IP route, where: • *vrf-name*—Specifies the name of the VPN routing/forwarding (VRF) instance for the static route. • *prefix*—Specifies the IP route prefix for the destination. • *mask*—Specifies the prefix mask for the destination. • *next-hop-address*—Specifies the IP address of the next hop that can be used to reach the destination network. • *interface interface-number*—Specifies the network interface type and interface number that can be used to reach the destination network. • **global**—Specifies that the given next hop address is in the non-VRF routing table. • *distance*—Specifies an administrative distance for the route. • **permanent**—Specifies that the route will not be removed, even if the interface shuts down. • **tag** *tag*—Specifies a tag value that can be used as a "match" value for controlling redistribution via route maps.

Verifying a Static Route Using VRF

To verify the static VRF route that you configured, use the **show ip route vrf** privileged EXEC command as shown in the following example:

```
GGSN# show ip route vrf vpn1 static

      172.16.0.0/16 is subnetted, 1 subnets
C       172.16.0.1 is directly connected, Ethernet5/1
C       10.100.0.3/8 is directly connected, Virtual-Access5
```

Configuring an OSPF Route Using VRF

To configure an OSPF route using VRF, use the following command, beginning in global configuration mode:

Command	Purpose
`Router(config)# router ospf process-id [vrf vrf-name]`	Enables OSPF routing, and enters router configuration mode, where, • *process-id*—Specifies an internally used identification parameter for an OSPF routing process. The *process-id* is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process. • **vrf** *vrf-name*—Specifies the name of the VPN routing/forwarding instance.

Configuring RADIUS Change of Authorization Support

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

Securing the GGSN Gn Interface

The following features provide additional security for the GGSN mobile interface against attacks that can lead to illegal access to a network or even network downtime: address verification and mobile-to-mobile traffic redirection. The following tasks are necessary for configuring these features:

- Configuring Address Verification, page 12-29
- Configuring Mobile-to-Mobile Traffic Redirection, page 12-30
- Redirecting All Traffic, page 12-30

Configuring Address Verification

Use the **security verify source** (IPv4 address verification) and **ipv6 security verify source** (IPv6 address verification) commands in access point configuration mode to configure the GGSN to verify the source IP address of an upstream TPDU against the address previously assigned to an MS.

When the **security verify source** or **ipv6 security verify source** commands are configured under an APN, the GGSN verifies the source address of a TPDU before GTP will accept and forward it. If the GGSN determines that the address differs from that previously assigned to the MS, it drops the TPDU and regards it as an illegal packet in its PDP context and APN. Configuring the **security verify source** and **ipv6 security verify source** commands in access point configuration mode protects the GGSN from faked user identities.

Use the **security verify destination** command in access point configuration mode (IPv4 address verification only) to have the GGSN verify the destination addresses of upstream TPDUs against global lists of PLMN addresses specified using the **gprs plmn ip address** command. If the GGSN determines that a destination address of a TPDU is within the range of a list of addresses, it drops the TPDU. If it determines that the TPDU contains a destination address that does not fall within the range of a list, it forwards the TPDU to its final destination.

Note The **security verify destination** command is not applied to APNs using VRF or IPv6 address verification. In addition, the verification of destination addresses does not apply to GTP-PPP regeneration or GTP-PPP with L2TP.

To configure IPv4 address verification on an access point, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# security verify {source | destination}`	(Optional) Specifies that the GGSN verify the source or destination address in TPDUs received from a Gn interface.

Note Both the verification of IPv4 destination addresses and source addresses can be configured under an APN.

To configure IPv6 source address verification on an access point, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# ipv6 security verify source`	(Optional) Configures the GGSN to verify the IPv6 source address of an upstream TPDU against the address previously assigned to an MS, use the **ipv6 security verify source** command in access-point configuration mode.

Configuring Mobile-to-Mobile Traffic Redirection

Mobile-to-mobile traffic enters and exits through a Gn interface. Therefore, it is switched by the GGSN without ever going through a Gi interface on the network side. Because of this, firewalls deployed on the network side of a GGSN do not have an opportunity to verify this level of traffic.

Use the **redirect intermobile ip** access-point command to redirect mobile-to-mobile traffic to an external device (such as an external firewall) for verification.

Command	Purpose
`Router(config-access-point)# redirect intermobile ip` *ip address*	(Optional) Configures the GGSN to redirect all IPv4 mobile-to-mobile traffic to an external device.
`Router(config-access-point)# ipv6 redirect intermobile` *ipv6-address*	(Optional) Configures the GGSN to redirect all IPv6 mobile-to-mobile traffic to an external IPv6 device.

Note On the Cisco 7600 series internet router platform, the mobile-to-mobile redirection feature requires that policy based routing (PBR) is configured on the supervisor engine and incoming VLAN interface from the Cisco SAMI, and that the next hop to route the packets that match the criteria is set using the **set ip next-hop** command.

Note Redirection of intermobile traffic does not occur on an ingress APN unless the TPDUs are exiting the same APN. In addition, redirection of TPDUs tunneled by L2TP from the ingress APN to the LNS of the PDN does not occur.

Redirecting All Traffic

The redirect all traffic feature enables you to do the following:

- Redirect all packets to a specified destination regardless of whether the destination address belongs to a mobile station (MS) on the same GGSN or not. If redirecting traffic using the Mobile-to-Mobile Redirect feature, only packets for which the destination address belongs to an MS that is active on the same GGSN can be redirected. If the receiving MS has no PDP context in the GGSN where the sending MS PDP context is created, the packets are dropped.
- Redirect all traffic to a specific destination when aggregate routes are configured.

To redirect all traffic to a specific IP address, issue the following commands in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# redirect all ip` *ip address*	(Optional) Configures the GGSN to redirect all IPv4 traffic to an external device.
`Router(config-access-point)# ipv6 redirect all intermobile` *ipv6-address*	(Optional) Configures the GGSN to redirect all IPv6 traffic to an external IPv6 device.

Segregating GRX Traffic on Gn/Gp Interface

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

To ensure privacy and security, the Cisco GGSN supports Virtual Private Network (VPN) routing and forwarding (VRF) instances on the Gn/Gp interface so that you can segregate GRX traffic to be a part of separate routing tables.

When configuring a Gn VRF virtual template interface to segregate GRX traffic, note the following:

- You must configure the default GTP virtual template (Virtual-Template 1), and never unconfigured it as long as **service gprs ggsn** is configured. You must assign a valid IP address to the default GTP virtual template (Virtual-Template 1) by using either the **ip address** or **ip unnumbered** command. Do not use the default GTP Virtual-Template in a VRF.
- You must configure a separate GTP virtual template interface for each VRF.
- Never place two virtual templates with GTP encapsulation under the same VRF.
- Unless a charging source interface is configured, use the same IP address for all loopback interfaces create for and associated with the GTP virtual template interfaces to ensure that CDRs for a PDP context contain the same GGSN address.
- Configure all GTP virtual template interfaces with the same access point list name.

To create a Gn VRF virtual template interface, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface virtual-template number`	Creates a virtual template interface, where *number* identifies the virtual template interface. This command takes you to interface configuration mode.
Step 2	`Router(config-if)# description description`	Description of the interface.
Step 3	`Router(config-if)# ip vrf forwarding vrf-name`	Associates a VRF instance with an interface.
Step 4	`Router(config-if)# ip unnumber loopback number`	Assigns a previously defined loopback IP address to the GTP virtual template interface.
Step 5	`Router(config-if)# encapsulation gtp`	Specifies GTP as the encapsulation type for packets transmitted over the virtual template interface.
Step 6	`Router(config-if)# gprs access-point-list list-name`	Specifies a name for a new access point list, or references the name of the existing access point list, and enters access-point list configuration mode.

The following is an example Gn VRF virtual template interface configuration:

```
ip vrf example
   rd 60:110
!
interface Loopback0
   ip address 172.0.0.100 255.255.0.0
!
interface Loopback52
   ip vrf forwarding example
   ip address 172.0.0.100 255.255.0.0
!
interface Virtual-Template1
   ip unnumbered Loopback0
   encapsulation gtp
   gprs access-point-list MWAM
!
interface Virtual-Template30
   ip vrf forwarding example
   ip unnumbered Loopback52
   encapsulation gtp
   gprs access-point-list MWAM
!
```

To remove the Gn VRF virtual template interface configuration using the **no** form of the **interface virtual-template** command in global configuration mode and specify the number of the Gn VRF virtual template interface.

Configuring Simultaneous Broadcast and Wait Accounting

With Cisco GGSN Release 8.0 and later, broadcast and wait accounting can be configured to work together. The wait accounting feature is configured at the APN level, while broadcast accounting is specified at the AAA method level.

Broadcast accounting sends start, stop and interim accounting records to all the server groups configured in a method list. Within a server group, the accounting records are sent to the first active server. If the active server cannot be reached, then the accounting records are sent to the next server within a group.

In addition, one or more server groups within a method list can be configured as “mandatory,” meaning that a server from that server group has to respond to the Accounting Start message. The APN-level wait accounting ensures that an accounting response is received from all mandatory server groups before the PDP context is established.

The advantages of broadcast and wait accounting together include:

- Accounting records are sent to multiple servers and once the entry is made, the user can start using different services.
- Records are sent to multiple AAA servers serve for redundancy purposes.
- A PDP context is established only when a valid Accounting Start record is received by all essential servers, avoiding information loss.
- Broadcast records can be sent to as many as 10 server groups within a method-list.

When configuring broadcast and wait accounting together:

- Under the method list configuration, the **mandatory** keyword is available only if broadcast accounting is configured.
- If wait accounting is not required, broadcast accounting to all server groups is available without any mandatory groups defined.

- If you do not specify any mandatory server groups when configuring broadcast accounting, wait accounting will function as it does in Cisco GGSN Release 7.0 and prior releases.
- Wait accounting does not apply to PPP PDP contexts.
- A PDP is successfully created only when a Accounting response is received from all the mandatory servers.
- The periodic timer starts when an Accounting Response (PDP creation) is received.

Note More than one server-group can be defined as a mandatory server-group in a method list.

To configure broadcast and wait accounting on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa accounting network methodlist-name`	Enables authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS.
Step 2	`Router(cfg-acct-mlist)# action-type {start-stop | stop-only | none}`	Type of action to be performed on accounting records. Possible values are: • **start-stop**—Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. • **stop-only**—Sends a "stop" accounting notice at the end of the requested user process. • **none**—Disables accounting services on this line or interface.
Step 3	`Router(cfg-acct-mlist)# broadcast`	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, switchover occurs using the backup servers defined within that group.
Step 4	`Router(cfg-acct-mlist)# group {server-group} [mandatory]`	Specifies the server group. Optionally, specify mandatory to define this server group as mandatory. If a server group is mandatory, a server from the server group has to respond to the Accounting Start message. **Note** Up to 10 server groups can be defined within a method list.
Step 5	`Router(cfg-acct-mlist)# exit`	Exits from accounting method list mode.
Step 1	`Router(config)# gprs access-point-list list_name`	Configures an access point list that you use to define public data network (PDN) access points on the GGSN.
Step 2	`Router(config-ap-list)#access-point access-point-index`	Specifies an access point number and enters access point configuration mode.

	Command	Purpose
Step 3	`Router(config-access-point)#`**`aaa-group accounting`** *`method-list name`*	Specifies an accounting server group.
Step 4	`Router(config-access-point)#` **`gtp-response-message wait-accounting`**	Configure APN to wait for a RADIUS accounting response before sending a Create PDP Context response to the SGSN.

Periodic Accounting Timer

The Cisco IOS software supports a global AAA configuration command that enables the sending of periodic accounting records for AAA sessions. However, the GGSN does not use this configuration to send periodic accounting records for PDP contexts.

With Cisco GGSN Release 8.0 and later, the periodic accounting timer interval value is obtained using one of the following:

- Configured periodic timer at an APN level
- Configured periodic timer at the GGSN global configuration level
- An accounting-interim interval attribute in access-accept messages

When these configurations exist, “interim” type accounting records are sent at the configured interval for the applicable PDP contexts. The following precedence applies:

- The APN-level configuration
- GGSN global configuration
- Attribute 85 (in access-accept messages)

Note If the value is obtained through Attribute 85 in an access-accept message, the GGSN verifies that the minimum and maximum values are within range configured on the GGSN, and if not, the attribute is ignored. In addition, if accounting is not enabled on the APN, Attribute 85 is ignored.

When the GGSN sends an interim update accounting (IAU) record, the periodic timer is reset so that next periodic accounting record will be sent after the periodic interval expires, starting from the instance when the IAU record is sent.

This limits the RADIUS accounting traffic as both types of records contain the same information. However, after a switchover, the records sent out will be aligned with the original START record.

Caution If the **aaa accounting update periodic** command is configured on the GGSN, and GGSN-level periodic accounting is not configured, the GGSN will send interim accounting records after the Accounting Start message is sent to AAA server. This might have adverse effects on the GGSN, therefore ensure that the **aaa accounting update periodic** command has not been configured.

When configuring periodic accounting timers on the GGSN:

- Timers are supported for PPP-Regen, IPv4, and IPv6 PDP’s. Timers do not apply to do PPP PDPs.
- The send/receive byte counts for a PDP is reset to 0 upon switchover.

- Redundant systems should have their clocks synchronized with a mechanism such as NTP to ensure that their timer intervals to be accurate
- Periodic accounting on a redundant configuration maintains intervals across switchovers.
- A timer is initiated only on successful PDP creation, for example, with wait accounting, after a successful accounting response is received.

Configuring a Default GGSN Periodic Accounting Timer

To enable a default periodic accounting value for all APNs, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs default aaa-accounting interim periodic` *minutes*	Configures a default periodic accounting timer on the GGSN. The valid values are 15 to 71582. The default is no periodic accounting timer is configured globally.

Configuring an APN-Level Periodic Accounting Timer

To configure the periodic accounting timer under an APN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs access-point-list` *list_name*	Configures an access point list.
Step 2	`Router(config-ap-list)#access-point` *access-point-index*	Specifies an access point number and enters access point configuration mode.
Step 3	`Router(config-access-point)#aaa-accounting interim periodic` *minutes*	Configures a periodic accounting timer under an APN. The valid values are 15 to 71582. The default is no periodic accounting timer is configured at the APN level.
Step 4	`Router(config-access-point)#aaa-accounting interim periodic radius`	Enables the APN to accept the periodic accounting value (Attribute 85) sent by RADIUS.

Note AAA global configuration value (**aaa accounting update periodic** *minutes*) will be ignored always. Also, unless APN accounting is enabled, the periodic accounting will not take effect regardless of how it is configured.

Implementing Lawful Intercept Support on the Cisco GGSN

This section provides information about Lawful Intercept and contains the following subsections:

- Lawful Intercept Overview, page 12-36
- Network Components Used for Lawful Intercept, page 12-37
- Lawful Intercept Processing, page 12-38
- Lawful Intercept MIBs, page 12-39
- Lawful Intercept Topology, page 12-40
- Configuring Lawful Intercept Support, page 12-40

Caution This section does not address legal obligations for the implementation of lawful intercept. As a service provider, you are responsible to ensure that your network complies with applicable lawful intercept statutes and regulations. We recommend that you seek legal advice to determine your obligations.

Lawful Intercept Overview

Lawful intercept is a process that enables a Law Enforcement Agency (LEA) to perform electronic surveillance on an individual (a target) 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.

The surveillance is performed through the use of wiretaps on traditional telecommunications and Internet services in voice, data, and multiservice networks. The LEA delivers a request for a wiretap to the target's service provider, who is responsible for intercepting data communication to and from the individual. The service provider uses the target's IP address or session to determine which of its edge routers handles the target's traffic (data communication). The service provider then intercepts the target's traffic as it passes through the router, and sends a copy of the intercepted traffic to the LEA without the target's knowledge.

The Lawful Intercept feature supports the Communications Assistance for Law Enforcement Act (CALEA), which describes how service providers in the United States must support lawful intercept. Currently, lawful intercept is defined by the following standards:

- Telephone Industry Association (TIA) specification J-STD-025
- Packet Cable Electronic Surveillance Specification (PKT-SP-ESP-101-991229)

For information about the Cisco lawful intercept solution, contact your Cisco account representative.

Lawful intercept support on the Cisco GGSN provides the following benefits:

- Allows multiple LEAs to run a lawful intercept on the same target without each other's knowledge.
- Does not affect subscriber services on the GGSN.
- Supports wiretaps in both the input and output direction.
- Supports wiretaps of Layer 3 and Layer 2 traffic.
- Cannot be detected by the target. Neither the network administrator nor the calling parties is aware that packets are being copied or that the call is being tapped.
- ***Uses Simple Network Management Protocol Version 3 (SNMPv3) and security features such as the View-based Access Control Model (SNMP-VACM-MIB) and User-based Security Model (SNMP-USM-MIB) to restrict access to lawful intercept information and components.***
- Hides information about lawful intercepts from all but the most privileged users. An administrator must set up access rights to enable privileged users to access lawful intercept information.
- Provides two secure interfaces for performing an intercept: one for setting up the wiretap and one for sending the intercepted traffic to the LEA.

Network Components Used for Lawful Intercept

The following network components are used for lawful intercepts:

- **Mediation Device—**A mediation device (supplied by a third-party vendor) handles most of the processing for the lawful intercept. The mediation device:
  - Provides the interface used to set up and provision the lawful intercept.
  - Generates requests to other network devices to set up and run the lawful intercept.
  - Converts the intercepted traffic into the format required by the LEA (which can vary from country to country) and sends a copy of the intercepted traffic to the LEA without the target's knowledge.

Note If multiple LEAs are performing intercepts on the same target, the mediation device must make a copy of the intercepted traffic for each LEA. The mediation device is also responsible for restarting any lawful intercepts that are disrupted due to a failure.

- **Intercept Access Point**—An intercept access point (IAP) is a device that provides information for the lawful intercept. There are two types of IAPs:
  - Identification (ID) IAP—A device, such as an authentication, authorization, and accounting (AAA) server, that provides intercept-related information (IRI) for the intercept (for example, the target's username and system IP address). The IRI helps the service provider determine which content IAP (router) the target's traffic passes through.
  - Content IAP—A device, such as a Cisco 7600 series router, that the target's traffic passes through. The content IAP:

    - Intercepts traffic to and from the target for the length of time specified in the court order. The router continues to forward traffic to its destination to ensure that the wiretap is undetected.

    - Creates a copy of the intercepted traffic, encapsulates it in User Datagram Protocol (UDP) packets, and forwards the packets to the mediation device without the target's knowledge.

    Note The content IAP sends a single copy of intercepted traffic to the mediation device. If multiple LEAs are performing intercepts on the same target, the mediation device must make a copy of the intercepted traffic for each LEA.

- **Collection Function**—The collection function is a program that stores and processes traffic intercepted by the service provider. The program runs on equipment at the LEA.

Lawful Intercept Processing

After acquiring a court order or warrant to perform surveillance, the LEA delivers a surveillance request to the target's service provider. Service provider personnel use an admin function that runs on the mediation device to configure a lawful intercept to monitor the target's electronic traffic for a specific period of time (as defined in the court order).

After the intercept is configured, user intervention is no longer required. The admin function communicates with other network devices to set up and execute the lawful intercept. The following sequence of events occurs during a lawful intercept:

1. The admin function contacts the ID IAP for intercept-related information (IRI), such as the target's username and the IP address of the system, to determine which content IAP (router) the target's traffic passes through.
2. After identifying the router that handles the target's traffic, the admin function sends SNMPv3 get and set requests to the router's MIBs to set up and activate the lawful intercept. The GGSN lawful intercept MIBs include the CISCO-TAP2-MIB and the CISCO-MOBILITY-TAP-MIB.
3. During the lawful intercept, the router:
   a. Examines incoming and outgoing traffic and intercepts any traffic that matches the specifications of the lawful intercept request.
   b. Creates a copy of the intercepted traffic and forwards the original traffic to its destination so the target does not suspect anything.
   c. Encapsulates the intercepted traffic in UDP packets and forwards the packets to the mediation device without the target's knowledge.

   Note The process of intercepting and duplicating the target's traffic adds no detectable latency in the traffic stream.

4. The mediation device converts the intercepted traffic into the required format and sends it to a collection function running at the LEA. Here, the intercepted traffic is stored and processed.

   Note If the router intercepts traffic that is not allowed by the judicial order, the mediation device filters out the excess traffic and sends the LEA only the traffic allowed by the judicial order.

5. When the lawful intercept expires, the router stops intercepting the target's traffic.

Lawful Intercept MIBs

To perform lawful intercept, the GGSN uses the following MIBs:

- **CISCO-TAP2-MIB**—The CISCO-TAP2-MIB contains SNMP management objects that control lawful intercepts on the router. The mediation device uses the MIB to configure and run lawful intercepts on targets whose traffic passes through the router. The MIB is bundled with Cisco software images that support lawful intercept.

  The CISCO-TAP2-MIB contains several tables that provide information for lawful intercepts that are running on the router:

  - cTap2MediationTable—Contains information about each mediation device that is currently running a lawful intercept on the router. Each table entry provides information that the router uses to communicate with the mediation device (for example, the device's address, the interfaces to send intercepted traffic over, and the protocol to transmit the intercepted traffic).
  - cTap2StreamTable—Contains information used to identify the traffic to intercept. Each table entry contains a pointer to a filter that is used to identify the traffic stream associated with the target of a lawful intercept. Traffic that matches the filter is intercepted, copied, and sent to the corresponding mediation device application (cTap2MediationContentId).
  - The table also contains counts of the number of packets that were intercepted, and counts of dropped packets that should have been intercepted, but were not.
  - cTap2DebugTable—Contains debug information for troubleshooting lawful intercept errors.

  The CISCO-TAP2-MIB also contains several SNMP notifications for lawful intercept events. For detailed descriptions of MIB objects, see the MIB itself.

  The admin function (running on the mediation device) issues SNMPv3 **set** and **get** requests to the router's CISCO-TAP2-MIB to set up and initiate a lawful intercept. To do this, the admin function performs the following actions:

  a. Creates a cTap2MediationTable entry to define how the router is to communicate with the mediation device executing the intercept.

     Note The cTap2MediationNewIndex object provides a unique index for the mediation table entry.

  b. Creates an entry in the cTap2StreamTable to identify the traffic stream to intercept.
  c. Creates an entry in the cmTapStreamTable and sets the cmTapStreamStatus to active (1).
  d. Sets cTap2StreamInterceptEnable to true(1) to start the intercept. The router intercepts traffic in the stream until the intercept expires (cTap2MediationTimeout).

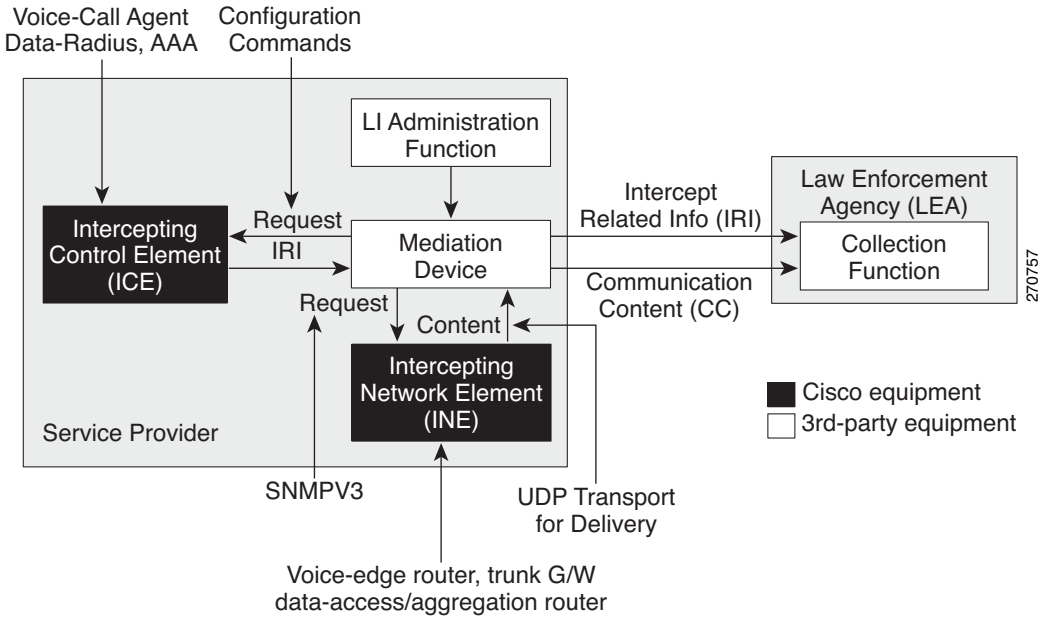
- **CISCO-MOBILITY-TAP-MIB—**The CISCO-MOBILITY-TAP-MIB contains the SNMP management objects to configure and execute wiretaps on mobility gateway traffic.

The CISCO-MOBILITY-TAP-MIB contains the cmtapStreamTable (the Mobility Stream table) that lists the data streams to be intercepted. The same data stream might be required by multiple taps. This table essentially provides options for packet selection, only some of which might be used. For example, if all of the traffic to or from a subscriber is to be intercepted, an entry listing would be configured listing the SubscriberID along with the SubscriberIDType corresponding to the stream to be intercepted. (More details can be found in CISCO-MOBILITY-TAP-MIB.)

Lawful Intercept Topology

The following illustration shows intercept access points and interfaces in a lawful intercept topology for both voice and data interception (Figure 1).

Figure 12-1 Lawful Intercept Topologies



Configuring Lawful Intercept Support

This section contains the following information:

- Prerequisites, page 12-41
- Security Considerations, page 12-41
- Configuration Guidelines and Limitations, page 12-41
- Accessing the Lawful Intercept MIBs, page 12-42
- Configuring SNMPv3, page 12-43

- Creating a Restricted SNMP View of Lawful Intercept MIBs, page 12-43
- Configuring the Cisco GGSN to Send SNMP Notifications for Lawful Intercept, page 12-45

Prerequisites

To configure support for lawful intercept, the following prerequisites must be met:

- You must be logged in to the GGSN with the highest access level (level 15). To log in with level-15 access, enter the **enable** command and specify the highest-level password defined for the router.
- You must issue commands in global configuration mode. Enter **config** to enter global configuration mode.
- (Optional) It might be helpful to use a loopback interface for the interface through which the GGSN communicates with the mediation device.
- The mediation device must be provisioned. For detailed information, see the vendor documentation associated with your mediation device. For a list of Cisco-preferred mediation device equipment suppliers, see http://www.cisco.com/wwl/regaffairs/lawful_intercept/index.html.

Security Considerations

Consider the following security issues as you configure the GGSN for lawful intercept support:

- SNMP notifications for lawful intercept must be sent to User Datagram Protocol (UDP) port 161 on the mediation device, not port 162 (which is the Simple Network Management Protocol (SNMP) default). See the "Configuring the Cisco GGSN to Send SNMP Notifications for Lawful Intercept" section on page 12-45 for instructions.
- The only users who should be allowed to access the lawful intercept MIBs are the mediation device and system administrators who need to know about lawful intercepts on the router. In addition, these users must have authPriv or authNoPriv access rights to access the lawful intercept MIBs. Users with NoAuthNoPriv access cannot access the lawful intercept MIBs.
- The default SNMP view excludes the following MIBs:

  CISCO-TAP2-MIB
  CISCO-MOBILITY-TAP-MIB

Configuration Guidelines and Limitations

This section and the sections that follow describe the general limitations and configuration guidelines for lawful intercept, Cisco GGSN-specific guidelines, and per-subscriber guidelines.

- To maintain GGSN performance, lawful intercept is limited to no more than 0.2% of active sessions. For example, if the GGSN is handling 4000 sessions, 8 of those sessions can be intercepted.
- **General Configuration Guidelines**—For the GGSN to communicate with the mediation device to execute a lawful intercept, the following configuration requirements must be met:
  - The domain name for both the GGSN and the mediation device must be registered in the Domain Name System (DNS).
  - In DNS, the router IP address is typically the address of the FastEthernet0/0/0 interface on the router.
  - The mediation device must have an access function (AF) and an access function provisioning interface (AFPI).

  - You must add the mediation device to the SNMP user group that has access to the CISCO-TAP2-MIB view. Specify the username of the mediation device as the user to add to the group.
  - When you add the mediation device as a CISCO-TAP2-MIB user, you can include the mediation device's authorization password if you want. The password must be at least eight characters in length.
- **MIB Guidelines**—The following Cisco MIBs are used for lawful intercept processing. Include these MIBs in the SNMP view of lawful intercept MIBs to enable the mediation device to configure and execute wiretaps on traffic that flows through the router.
  - CISCO-TAP2-MIB—Required for both types of lawful intercepts: regular and broadband.
  - CISCO-MOBILITY-TAP-MIB—Required for wiretaps on mobility gateway traffic.
- **Cisco GGSN Configuration Guidelines and Limitations**—The following is a list of configuration guidelines for regular lawful intercept on the Cisco GGSN:
  - Lawful intercept can intercept traffic at a rate of 6000 packets per second (pps) without affecting the packet forwarding rate. This intercept rate includes all active intercepts and assumes that packets are 150 to 200 bytes long. If the intercept rate exceeds 6000 pps, the packet forwarding rate will decrease slightly because lawful intercept is processor intensive.
  - Lawful intercept is not supported on Layer 2 interfaces. However, lawful intercept can intercept traffic on VLANs that run over the Layer 2 interface if the VLAN interface is a Layer 3 interface and traffic is routed by the VLAN interface.
  - Packets that are subject to hardware rate limiting are processed by lawful intercept as follows:
  - Packets that are dropped by the rate limiter are not intercepted or processed.
  - Packets that are passed by the rate limiter are intercepted and processed.
  - If multiple law enforcement agencies (LEAs) are using a single mediation device and each is executing a wiretap on the same target, the router sends a single packet to the mediation device. It is up to the mediation device to duplicate the packet for each LEA.
  - Lawful intercept on the GGSN is based on the subscriber IMSI value as described in CISCO-MOBILITY-MIB.

Accessing the Lawful Intercept MIBs

Due to its sensitive nature, the Cisco lawful intercept MIBs are only available in software images that support the lawful intercept feature. These MIBs are not accessible through the Network Management Software MIBs Support page (http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml).

Restricting Access to the Lawful Intercept MIBs

Only the mediation device and users who need to know about lawful intercepts should be allowed to access the lawful intercept MIBs. To restrict access to these MIBs, you must:

1. Create a view that includes the Cisco lawful intercept MIBs.
2. Create an SNMP user group that has read-and-write access to the view. Only users assigned to this user group can access information in the MIBs.

3. Add users to the Cisco lawful intercept user groups to define who can access the MIBs and any information related to lawful intercepts. Be sure to add the mediation device as a user in this group; otherwise, the router cannot perform lawful intercepts.

Note Access to the Cisco lawful intercept MIB view should be restricted to the mediation device and to system administrators who need to be aware of lawful intercepts on the router. To access the MIB, users must have level-15 access rights on the router.

Configuring SNMPv3

To perform the following procedures, SNMPv3 must be configured on the GGSN. For information about how to configure SNMPv3, and for detailed information about the commands described in the sections that follow, see the following Cisco documents:

- *Cisco IOS Configuration Fundamentals Configuration Guide*, Part 3: System Management, "Configuring SNMP Support" section, available at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf014.htm

- *Cisco IOS Configuration Fundamentals and Network Management Command Reference*, available at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/fun_r/cfr_1g11.htm

Creating a Restricted SNMP View of Lawful Intercept MIBs

To create and assign users to an SNMP view that includes the Cisco lawful intercept MIBs, perform the following procedure at the CLI, in global configuration mode with level-15 access rights. For command examples, see the "Configuration Example" section on page 12-44.

Note The command syntax in the following steps includes only those keywords required to perform each task. For details on command syntax, see the documents listed in the previous section ("Configuring SNMPv3").

Step 1 Make sure that SNMPv3 is configured on the GGSN. For instructions, see the documents listed in the "Configuring SNMPv3" section on page 12-43.

Step 2 Create an SNMP view that includes the CISCO-TAP2-MIB (where *view_name* is the name of the view to create for the MIB). This MIB is required for both regular and broadband lawful intercept.

```
Router(config)# snmp-server view view_name ciscoTap2MIB included
```

Step 3 Add the following MIB to the SNMP view to configure support for wiretaps on mobility gateway streams (where *view_name* is the name of the view you created in Step 2).

```
Router(config)# snmp-server view view_name ciscoMobilityTapMIB included
```

Step 4 Create an SNMP user group (*groupname*) that has access to the lawful intercept MIB view and define the group's access rights to the view.

```
Router(config)# snmp-server group groupname v3 auth read view_name write view_name
notify notify-view
```

Step 5 Add users to the user group you just created (where *username* is the user, *groupname* is the user group, and *auth_password* is the authentication password):

```
Router(config)# snmp-server user username groupname v3 auth md5 auth_password
```

Note Both the **priv** and **auth** keyword options are valid options when adding users.

Note Be sure to add the mediation device to the SNMP user group; otherwise, the router cannot perform lawful intercepts. Access to the lawful intercept MIB view should be restricted to the mediation device and to system administrators who need to know about lawful intercepts on the router.

Step 6 Specify the host from which the user will be allowed to connect:

```
Router(config)# snmp-server host ip-address version 3 auth user-name
```

Step 7 Specify the engine identifier:

```
Router(config)# snmp-server engineID local engine-ID
```

The mediation device is now able to access the lawful intercept MIBs, and issue SNMP **set** and **get** requests to configure and run lawful intercepts on the router.

For instructions on how to configure the router to send SNMP notifications to the mediation device, see the "Configuring the Cisco GGSN to Send SNMP Notifications for Lawful Intercept" section on page 12-45.

Configuration Example

The following commands show an example of how to enable the mediation device to access the lawful intercept MIBs.

```
Router(config)# snmp-server view tapV ciscoTap2MIB included
Router(config)# snmp-server view tapV ciscoMobilityTapMIB included
Router(config)# snmp-server group tapGrp v3 auth read tapV write tapV notify tapV
Router(config)# snmp-server user ss8user tapGrp v3 auth md5 ss8passwd
Router(config)# snmp-server host 172.10.10.1 version 3 auth ss8usr
Router(config)# snmp-server engineID local 0123467891
```

1. Create a view (tapV) that includes the appropriate lawful intercept MIBs (CISCO-TAP2-MIB and CISCO-MOBILITY-TAP-MIB).
2. Create a user group (tapGrp) that has read, write, and notify access to MIBs in the tapV view.
3. Add the mediation device (ss8user) to the user group, and specify MD5 authentication with a password (ss8passwd).
4. (Optional) Assign a 24-character SNMP engine ID (for example, 123400000000000000000000) to the router for administration purposes. If you do not specify an engine ID, one is automatically generated. You can omit the trailing zeros from the engine ID, as shown in the last line of the example above.

Note Changing an engine ID has consequences for SNMP user passwords and community strings.

Configuring the Cisco GGSN to Send SNMP Notifications for Lawful Intercept

SNMP automatically generates notifications for lawful intercept events (see Table 12-2). This is because the default value of the cTap2MediationNotificationEnable object is true(1).

To configure the GGSN to send lawful intercept notifications to the mediation device, issue the following commands in global-configuration mode with level-15 access rights (where *MD-ip-address* is the IP address of the mediation device and *community-string* is the password-like community string to send with the notification request):

```
Router(config)# snmp-server host MD-ip-address community-string udp-port 161 snmp
```

- For lawful intercept, **udp-port** must be 161 and not 162 (the SNMP default).

Table 12-2 lists the SNMP notifications generated for lawful intercept events.

Table 12-2 SNMP Notifications for Lawful Intercept Events

Notification	Description
cTap2MIBActive	The router is ready to intercept packets for a traffic stream configured in the CISCO-TAP2-MIB.
cTap2MediationTimedOut	A lawful intercept was terminated (for example, because cTap2MediationTimeout expired).
cTap2MediationDebug	Debugging information for events related to cTap2MediationTable entries.
cTap2StreamDebug	Debugging information for events related to cTap2StreamTable entries.
cTap2Switchover	A redundant, active route processor (RP) is going into standby mode and the standby is the active RP.

Disabling SNMP Notifications

You can disable SNMP notifications on the GGSN as follows:

- To disable all SNMP notifications, issue the **no snmp-server enable traps** command.
- To disable lawful intercept notifications, use SNMPv3 to set the CISCO-TAP2-MIB object cTap2MediationNotificationEnable to false(2). To re-enable lawful intercept notifications through SNMPv3, reset the object to true(1).

Configuration Examples

This section includes the following configuration examples for security on the GGSN:

- AAA Security Configuration Example, page 12-46
- RADIUS Server Global Configuration Example, page 12-46
- RADIUS Server Group Configuration Example, page 12-46
- RADIUS Response Message Configuration Example, page 12-48
- Address Verification and Mobile-to-Mobile Traffic Redirection Example, page 12-49
- “Periodic Accounting Timer Example” section on page 12-52

AAA Security Configuration Example

The following example shows how to enable AAA security globally on the router and how to specify global RADIUS authentication and authorization:

```
! Enables AAA globally
aaa new-model
!
! Creates a local authentication list for use on
! serial interfaces running PPP using RADIUS
!
aaa authentication ppp abc group abc
!
! Enables authorization and creates an authorization
! method list for all network-related service requests
! and enables authorization using a RADIUS server
!
aaa authorization network network abc group abc
```

For more information about configuring AAA, see *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications.

RADIUS Server Global Configuration Example

The following example shows how to globally configure RADIUS server communication on the router:

```
! Specifies a global RADIUS server host at IP address 10.100.0.2
! Port 1645 is destination port for authentication requests
! Port 1646 is the destination port for accounting requests
! Specifies the key "abc" for this radius host only
!
radius-server host 10.100.0.2 auth-port 1645 acct-port 1646 key abc
!
! Sets the authentication and encryption key to mykey for all
! RADIUS communications between the router and the RADIUS daemon
!
radius-server key mykey
```

Note Although you can configure the **radius-server host** command multiple times, the Cisco IOS software supports only one RADIUS server at the same IP address.

For more information about configuring RADIUS security, see *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications.

RADIUS Server Group Configuration Example

The following configuration example defines four AAA server groups on the GGSN: abc, abc1, abc2, and abc3, shown by the **aaa group server** commands.

Using the **gprs default aaa-group** command, two of these server groups are globally defined as default server groups: abc2 for authentication, and abc3 for accounting.

At access-point 1, which is enabled for authentication, the default global authentication server group of abc2 is overridden and the server group named abc is designated to provide authentication services on the APN. Notice that accounting services are not explicitly configured at that access point, but are automatically enabled because authentication is enabled. Because there is a globally defined accounting server-group defined, the server named abc3 will be used for accounting services.

At access-point 4, which is enabled for accounting using the **aaa-accounting enable** command, the default accounting server group of abc3 is overridden and the server group named abc1 is designated to provide accounting services on the APN.

Access-point 5 does not support any AAA services because it is configured for transparent access mode.

```
! Enables AAA globally
!
aaa new-model
!
! Defines AAA server groups
!
aaa group server radius abc
 server 10.2.3.4 auth-port 1645 acct-port 1646
 server 10.6.7.8 auth-port 1645 acct-port 1646
aaa group server radius abc1
 server 10.10.0.1 auth-port 1645 acct-port 1646
aaa group server radius abc2
 server 10.2.3.4 auth-port 1645 acct-port 1646
 server 10.10.0.1 auth-port 1645 acct-port 1646
aaa group server abc3
 server 10.6.7.8 auth-port 1645 acct-port 1646
 server 10.10.0.1 auth-port 1645 acct-port 1646
!
! Configures AAA authentication
! and authorization
!
aaa authentication ppp abc group abc
aaa authentication ppp abc2 group abc2
aaa authorization network abc group abc
aaa accounting network abc start-stop group abc
aaa accounting network abc1 start-stop group abc1
aaa accounting network abc2 start-stop group abc2
aaa accounting network abc3 start-stop group abc3
!
gprs access-point-list gprs
 access-point 1
  access-mode non-transparent
  access-point-name www.pdn1.com
!
! Specifies a RADIUS server group
! for use by the GGSN to authenticate
! mobile users at this access point
!
  aaa-group authentication abc
!
 access-point 4
  access-point-name www.pdn2.com
!
! Enables AAA accounting services
!
  aaa-accounting enable
!
! Specifies a RADIUS server group
! for use by the GGSN for accounting
! services at this access point
```

```
  aaa-group accounting abc1
!
 access-point 5
  access-point-name www.pdn3.com
!
! Configures default AAA server
! groups for the GGSN for authentication
! and accounting services
!
gprs default aaa-group authentication abc2
gprs default aaa-group accounting abc3
!
! Configures global RADIUS server hosts
! and specifies destination ports for
! authentication and accounting requests
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.10.0.1 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

Note Although you can configure the **radius-server host** command multiple times, the Cisco IOS software supports only one RADIUS server at the same IP address.

RADIUS Response Message Configuration Example

The following example globally configures the GGSN to wait for a RADIUS accounting response from the RADIUS server before sending a Create PDP Context response to the SGSN. The GGSN waits for a response for PDP context requests received across all access points, except access-point 1. RADIUS response message waiting is overridden at access-point 1 by using the **no gtp response-message wait-accounting** command:

```
! Enables AAA globally
!
aaa new-model
!
! Defines AAA server group
!
aaa group server radius abc
 server 10.2.3.4 auth-port 1645 acct-port 1646
 server 10.6.7.8 auth-port 1645 acct-port 1646
!
! Configures AAA authentication
! and authorization
!
aaa authentication ppp abc group abc
aaa authorization network abc group abc
aaa accounting network abc start-stop group abc
!
gprs access-point-list gprs
 access-point 1
  access-mode non-transparent
  access-point-name www.pdn1.com
  aaa-group authentication abc
!
! Disables waiting for RADIUS response
! message at APN 1
!
  no gtp response-message wait-accounting
```

```
  exit
access-point 2
 access-mode non-transparent
 access-point-name www.pdn2.com
 aaa-group authentication abc
!
! Enables waiting for RADIUS response
! messages across all APNs (except APN 1)
!
gprs gtp response-message wait-accounting
!
! Configures global RADIUS server hosts
! and specifies destination ports for
! authentication and accounting requests
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

Address Verification and Mobile-to-Mobile Traffic Redirection Example

The following examples show how to enable IPv4 address verification and specify that IPv4 mobile-to-mobile traffic be redirected to an external device.

GGSN Configuration

```
service gprs ggsn
!
hostname t7600-7-2
!
ip cef
!
ip vrf vpn4
 description abc_vrf
 rd 104:4
!
!
interface Loopback2
 description USED FOR DHCP2 - range IN dup prot range
 ip address 111.72.0.2 255.255.255.255
!
interface Loopback100
 description GPRS GTP V-TEMPLATE IP ADDRESS
 ip address 9.9.9.72 255.255.255.0
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.2
 description Ga/Gn Interface
 encapsulation dot1Q 101
 ip address 10.1.1.72 255.255.255.0
 no cdp enable
!
interface GigabitEthernet0/0.3
 encapsulation dot1Q 103
 ip vrf forwarding vpn4
 ip address 10.1.3.72 255.255.255.0
 no cdp enable
!
interface GigabitEthernet0/0.95
```

```
 description CNR and CAR
 encapsulation dot1Q 95
 ip address 10.2.25.72 255.255.255.0
!
interface Virtual-Template1
 description GTP v-access
 ip unnumbered Loopback100
 encapsulation gtp
 gprs access-point-list gprs
!
! In case the ms is on another SAMI GGSN
ip route vrf vpn4 0.0.0.0 0.0.0.0 10.1.3.1
!
gprs access-point-list gprs
  access-point 7
   access-point-name ms_redirect.com
   ip-address-pool dhcp-proxy-client
   aggregate auto
   dhcp-server 10.2.25.90
   dhcp-gateway-address 111.72.0.2
   vrf vpn4
   ! In case the ms is on this GGSN.
   redirect intermobile ip 10.1.3.1
   !
```

Supervisor Engine Configuration

```
hostname 7600-a

interface FastEthernet9/15
 description OUT to Firewall
 no ip address
 duplex half
 switchport
 switchport access vlan 162
!
interface FastEthernet9/16
 description In from Firewall
 no ip address
 switchport
 switchport access vlan 163
!
interface Vlan103
 description Vlan to GGSN redirect to FW
 ip address 10.1.3.1 255.255.255.0
 ip policy route-map REDIRECT-TO-FIREWALL
!
interface Vlan162
 ip address 162.1.1.1 255.255.255.0
!
interface Vlan163
 ip address 163.1.1.1 255.255.255.0
!
ip route 111.72.0.0 255.255.0.0 10.1.3.72
ip route 111.73.0.0 255.255.0.0 10.1.3.73
ip route 111.74.0.0 255.255.0.0 10.1.3.74
ip route 111.75.0.0 255.255.0.0 10.1.3.75
ip route 111.76.0.0 255.255.0.0 10.1.3.76
!
access-list 102 permit ip any any
!
route-map REDIRECT-TO-FIREWALL permit 10
 match ip address 102
 set ip next-hop 162.1.1.11
```

Access to a Private RADIUS Server Using VRF Configuration Example

The following examples shows an example of configuring access to a private RADIUS server using VRF.

GGSN Configuration

```
aaa new-model
!

aaa group server radius vrf_aware_radius
 server-private 99.100.0.2 auth-port 1645 acct-port 1646 key cisco
 ip vrf
!
aaa authentication ppp vrf_aware_radius group vrf_aware_radius
aaa authorization network default local group radius
aaa authorization network vrf_aware_radius group vrf_aware_radius
aaa accounting network vrf_aware_radius start-stop group vrf_aware_radius
aaa session-id common

!
ip vrf vpn2
 rd 101:1
!
interface Loopback1
 ip address 150.1.1.72 255.255.0.0
!
interface Tunnel2
 ip vrf forwarding vpn2
 ip address 80.80.72.72 255.255.255.0
 tunnel source 150.1.1.72
 tunnel destination 167.2.1.12
!
ip local pool vpn2_pool 100.72.0.1 100.72.255.255 group vpn2
ip route vrf vpn2 0.0.0.0 0.0.0.0 Tunnel2
!
gprs access-point-list gprs
  access-point 1
   access-point-name apn.vrf2.com
   access-mode non-transparent
   aaa-group authentication vrf_aware_radius
   aaa-group accounting vrf_aware_radius
   ip-address-pool local vpn2_pool
   aggregate 100.72.0.0 255.255.0.0
   vrf vpn2
   !
```

Supervisor Engine Configuration

```
...
!
interface FastEthernet9/5
 switchport
 switchport access vlan 167
!

interface Vlan167
 ip address 167.1.1.1 255.255.0.0
!
ip route 150.1.1.72 255.255.255.255 10.1.1.72
ip route 167.2.0.0 255.255.0.0 167.1.1.12
!
...
```

Periodic Accounting Timer Example

The following example shows a period accounting timer configured at the APN level and globally.

```
gprs default aaa-accounting interim periodic 60
!
gprs access-point-list APLIST
  access-point 100
   access-point-name peracct.com
   access-mode non-transparent
   aaa-accounting interim update
   aaa-accounting interim periodic 15
   aaa-group authentication radaccess
   aaa-group accounting default
   ip-address-pool radius-client
   gtp response-message wait-accounting
!
```

CHAPTER 13

Configuring Dynamic Addressing on the GGSN

This chapter describes how to configure dynamic IP addressing on the gateway GRPS support node (GGSN).

Note Dynamic IP addressing is not supported for IPv6 and PPP PDP types. Therefore, the tasks in this chapter apply to IPv4 PDP contexts only. For information on IPv6 addressing, see Chapter 5, "Configuring IPv6 PDP Support on the GGSN."

For complete descriptions of the GGSN commands in this chapter, see *Cisco GGSN Command Reference* for the Cisco GGSN release you are using. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

This chapter includes the following sections:

- Overview of Dynamic IP Addressing on the GGSN, page 13-1
- Configuring DHCP on the GGSN, page 13-2
- Configuring MS Addressing via Local Pools on the GGSN, page 13-10
- Configuring MS Addressing via RADIUS, page 13-12
- Configuring Overlapping Local IP Address Pools, page 13-12
- Configuring the NBNS and DNS Address for an APN, page 13-16
- Using Dynamic IP Address Management on the Cisco GGSN, page 13-17

Overview of Dynamic IP Addressing on the GGSN

There are three methods for configuring the GGSN to assign IP addresses to mobile station users who need to access the public data network (PDN): Dynamic Host Configuration Protocol (DHCP) allocation, Remote Authentication Dial-In User Service (RADIUS) allocation, and local IP address pool allocation configured at the access point name (APN) or downloaded.

A method of dynamic IP addressing can be configured either globally or at the access-point configuration level.

Be sure that the following configuration guidelines are met to support the type of IP address allocation in use on your network:

- DHCP IP address allocation
  - Be sure that you configure the scope of the addresses to be allocated on the same subnet as the loopback interface.
  - Do not configure an IP address for users on the RADIUS server.
  - Specify the **peer default ip address dhcp** command at the PPP virtual template interface.
  - Specify the **aaa authorization network** *method_list* **none** command on the GGSN.
- RADIUS IP address allocation
  - Be sure that users are configured on the RADIUS server using the complete username@domain format.
  - Specify the **no peer default ip address** command at the PPP Virtual Template interface.
  - For more information about configuring RADIUS services on the GGSN, see the "Configuring Security on the GGSN" chapter in this book.
- Local pool IP address allocation
  - Be sure to configure a local pool using the **ip local pool** command.
  - Specify the **aaa authorization network** *method_list* **none** command on the GGSN.
  - Specify the **peer default ip address pool** *pool-name* command.

Note On the Cisco 7600 platform, dynamic address allocation using the DHCP or RADIUS server methods requires that the DHCP or RADIUS server be Layer 3 routeable from the supervisor engine.

Configuring DHCP on the GGSN

You can use local DHCP services within the Cisco IOS software, or you can configure the GGSN to use an external DHCP server such as the Cisco Network Registrar (CNR). For information about configuring internal DHCP services in the Cisco IOS software, see *Cisco IOS Configuration Fundamentals Configuration Guide*.

The DHCP server can be specified in two ways:

- At the global configuration level, using the **gprs default dhcp-server** command
- At the access-point configuration level, using the **dhcp-server** command

To configure DHCP support on the GGSN, you must configure either the **gprs default ip-address-pool** command in global configuration mode or the **ip-address-pool** command in access-point configuration mode with the **dhcp-proxy-client** keyword option.

After you configure the access point for DHCP proxy client services, use the **dhcp-server** command in access-point configuration mode to specify a DHCP server.

Use the *ip-address* argument to specify the IP address of the DHCP server. The second, optional *ip-address* argument can be used to specify the IP address of a backup DHCP server to use in the event that the primary DHCP server is unavailable. If you do not specify a backup DHCP server, then no backup DHCP server is available.

If you specify a DHCP server at the access-point level by using the **dhcp-server** command, then the server address specified at the access point overrides the address specified at the global level. If you do not specify a DHCP server address at the access-point level, then the address specified at the global level is used.

Therefore, you can have a global address setting and also one or more local access-point level settings if you need to use different DHCP servers for different access points.

Use the **vrf** keyword when the DHCP server itself is located within the address space of a VRF interface on the GGSN. If the DHCP server is located within the VRF address space, then the corresponding loopback interface for the **dhcp-gateway-address** must also be configured within the VRF address space.

This section contains the following information:

- Configuring DHCP Server Communication Globally, page 13-3
- Configuring DHCP at the GGSN Global Configuration Level, page 13-4
- Configuring a Local DHCP Server, page 13-8
- Configuration Example, page 13-8

Configuring DHCP Server Communication Globally

This section describes how to configure a global DHCP server host that the GGSN can use to assign IP addresses to mobile users. You can configure additional DHCP server communication at the GGSN global configuration level.

To globally configure DHCP server communication on the router or instance of Cisco IOS software, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ip address-pool {dhcp-proxy-client | local}`	Specifies an IP address pool mechanism, where: • **dhcp-proxy-client**—Specifies the router or instance of Cisco IOS software as the proxy-client between a third-party DHCP server and peers connecting to the router or IOS instance. • **local**—Specifies the local address pool named "default". **Note** There is no default option for the **ip address-pool** command. If you configure a local address pool using the **local** keyword, you can also configure the optional commands in Step 4 and Step 5.
Step 2	`Router(config)# ip dhcp-server {ip-address | name}`	Specifies the IP address or name of a DHCP server.

	Command	Purpose
Step 3	`Router(config)# ip dhcp excluded address low-address [high-address]`	(Optional) Specifies IP addresses that a DHCP server should not assign to DHCP clients, where: • *low-address*—Specifies the first IP address in an excluded address range. This address is typically the address of the DHCP server itself. • *high-address*—(Optional) Specifies the last IP address in the excluded address range.
Step 4	`Router(config)# ip dhcp pool name`	(Optional—Supports **ip address-pool local** command only.) Configures a DHCP address pool, and enters DHCP pool configuration mode, where *name* can be either a symbolic string (such as "engineering") or an integer (such as 0).
Step 5	`Router(config-dhcp)# network network-number [mask | /prefix-length]`	(Optional—Supports **ip address-pool local** command only.) Specifies the subnet network number and mask of the DHCP address pool. The prefix length specifies the number of bits in the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).

For more information about configuring global DHCP services, see *Cisco IOS IP Configuration Guide*, *Cisco IOS IP Command References*, and the *Cisco IOS Dial Technologies Command Reference* publications.

Configuring DHCP at the GGSN Global Configuration Level

To complete the DHCP configuration for the GGSN, you can configure DHCP at the GGSN global configuration level. When you configure DHCP at the GGSN configuration level, you can configure DHCP server communication for all access points or for a specific access point.

Configuring DHCP at the GGSN configuration level includes the following tasks:

- Configuring a Loopback Interface, page 13-4 (Required)
- Specifying a DHCP Server for All Access Points, page 13-5 (Optional)
- Specifying a DHCP Server for a Particular Access Point, page 13-6 (Optional)

Configuring a Loopback Interface

When you configure a DHCP gateway address for DHCP services at an access point, and when you are supporting unique supernets across all access points on the GGSN for DHCP, then you must configure a loopback interface for each unique network.

A loopback interface is a software-only interface that emulates an interface that is always up. It is a virtual interface supported on all platforms. The interface number is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces you can create.

To configure a loopback interface on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface loopback` *interface-number*	Defines a loopback interface on the GGSN, where *interface-number* identifies the loopback interface.
Step 2	`Router(config-if)# ip address` *ip-address mask* [**secondary**]	Specifies an IP address for the interface, where: • *ip-address*—Specifies the IP address of the interface in dotted decimal format. • *mask*—Specifies a subnet mask in dotted decimal format. • **secondary**—Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. **Note** The *ip-address* corresponds to the IP address of the DHCP gateway address at the access point. The mask should be 255.255.255.255 to match the **dhcp-gateway-address** value exactly.

Specifying a DHCP Server for All Access Points

When processing DHCP address allocation, the GGSN software first checks to see whether a DHCP server is specified at the access-point configuration level. If a server is specified, the GGSN uses the DHCP server specified at the access point. If no DHCP server is specified at the access-point configuration level, then the GGSN uses the default GGSN DHCP server.

To specify a DHCP server for all GGSN access points, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs default ip-address-pool {dhcp-proxy-client | radius-client | disable}`	Specifies a dynamic address allocation method using IP address pools for the GGSN, where: • **dhcp-proxy-client**—Specifies that the GGSN dynamically acquires IP addresses for a mobile station (MS) from a DHCP server. Use this keyword to enable DHCP services. • **radius-client**—Specifies that the GGSN dynamically acquires IP addresses for an MS from a RADIUS server. • **disable**—Disables dynamic address allocation by the GGSN. There is no default option for this command.
Step 2	`Router(config)# gprs default dhcp-server {`*ip-address* `|` *name*`} [{`*ip-address* `|` *name*`}]`	Specifies a primary (and backup) DHCP server from which the GGSN obtains IP address leases for mobile users, where: • *ip-address*—Specifies the IP address of a DHCP server. The second (optional) *ip-address* argument specifies the IP address of a backup DHCP server. • *name*—Specifies the hostname of a DHCP server. The second (optional) *name* argument specifies the hostname of a backup DHCP server.

Specifying a DHCP Server for a Particular Access Point

To override the default DHCP server configured for all access points, you can specify a different DHCP server for a particular access point. Or, if you choose not to configure a default GGSN DHCP server, you can specify a DHCP server at each access point.

To specify a DHCP server for a particular access point, use the following commands, beginning in access-point configuration mode:

	Command	Purpose
Step 1	`Router(config-access-point)# ip-address-pool {dhcp-proxy-client | radius-client | local pool-name | disable}`	(Optional) Specifies a dynamic address allocation method using IP address pools for the current access point. The available options are: • **dhcp-proxy-client**—DHCP server provides the IP address pool. • **radius-client**—RADIUS server provides the IP address pool. • **local**—Specifies that a local pool provides the IP address. This option requires that a local pool is configured using the **ip local pool** command in global configuration mode. • **disable**—Turns off dynamic address allocation. **Note** If you are using a dynamic address allocation method, then you must configure this command according to the appropriate IP address pool source.
Step 2	`Router(config-access-point)# dhcp-server {ip-address} [ip-address] [vrf]`	Specifies a primary (and backup) DHCP server that the GGSN uses at a particular access point to obtain IP address leases for mobile users for access to a PDN, where: • *ip-address*—Specifies the IP address of a DHCP server. The second (optional) *ip-address* argument specifies the IP address of a backup DHCP server. • **vrf**—DHCP server uses the VPN routing and forwarding (VRF) table that is associated with the APN.
Step 3	`Router(config-access-point)# dhcp-gateway-address ip-address`	Specifies the subnet in which the DHCP server should return addresses for DHCP requests for MS users entering a particular PDN access point. **Note** You must configure a corresponding loopback interface with the same IP address as the DHCP gateway address.

Configuring a Local DHCP Server

Note We do not recommend using a local DHCP server on the Cisco 7600 platform.

Although most networks use external DHCP servers, such as that available through the Cisco Network Registrar (CNR), you can also configure internal DHCP services on the GGSN. If you use local DHCP services on the GGSN, then there are a couple of commands that you should configure to improve the internal DHCP response times.

To optimize local DHCP services on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ip dhcp ping packets 0`	Specifies that the Cisco IOS DHCP Server sends 0 packets to a pool address as part of a ping operation.
Step 2	`Router(config)# ip dhcp ping timeout 100`	Specifies that the Cisco IOS DHCP Server waits for a ping reply from an address pool for 100 milliseconds.

Configuration Example

The following example shows a VRF configuration for vpn3 (without tunneling) using the **ip vrf** command in global configuration mode. Because the **ip vrf** command establishes both VRF and CEF routing tables, notice that **ip cef** also is configured at the global configuration level to enable CEF switching at all of the interfaces.

The following other configuration elements must also associate the same VRF named vpn3:

- FastEthernet0/0 is configured as the Gi interface using the **ip vrf forwarding** command in interface configuration mode.
- Access-point 2 implements VRF using the **vrf** command access-point configuration mode.

The DHCP server at access-point 2 also is configured to support VRF. Notice that access-point 1 uses the same DHCP server, but is not supporting the VRF address space. The IP addresses for access-point 1 will apply to the global routing table:

```
aaa new-model
!
aaa group server radius abc
 server 10.2.3.4
 server 10.6.7.8
!
aaa authentication ppp abc group abc
aaa authorization network abc group abc
aaa accounting network abc start-stop group abc
!
ip cef
!
ip vrf vpn3
 rd 300:3
!
interface Loopback1
 ip address 10.30.30.30 255.255.255.255
!
interface Loopback2
```

```
 ip vrf forwarding vpn3
 ip address 10.27.27.27 255.255.255.255
!
interface FastEthernet0/0
 ip vrf forwarding vpn3
 ip address 10.50.0.1 255.255.0.0
 duplex half
!
interface FastEthernet1/0
 ip address 10.70.0.1 255.255.0.0
 duplex half
!
interface loopback 1
 ip address 10.8.0.1 255.255.255.0
!
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list gprs
!
ip route 10.10.0.1 255.255.255.255 Virtual-Template1
ip route vrf vpn3 10.100.0.5 255.255.255.0 fa0/0 10.50.0.2
ip route 10.200.0.5 255.255.255.0 fa1/0 10.70.0.2
!
no ip http server
!
gprs access-point-list gprs
 access-point 1
  access-point-name gprs.pdn.com
  ip-address-pool dhcp-proxy-client
  dhcp-server 10.200.0.5
  dhcp-gateway-address 10.30.30.30
  network-request-activation
  exit
  !
 access-point 2
  access-point-name gprs.pdn2.com
  access-mode non-transparent
  ip-address-pool dhcp-proxy-client
  dhcp-server 10.100.0.5 10.100.0.6 vrf
  dhcp-gateway-address 10.27.27.27
  aaa-group authentication abc
  vrf vpn3
  exit
!
gprs default ip-address-pool dhcp-proxy-client
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

Configuring MS Addressing via Local Pools on the GGSN

As the number of PDP contexts increases, allocating IP addresses via locally-configured address pools improves the PDP context activation rate. Whether or not addresses are allocated to MSs using local pools is specified at the access-point configuration level and requires that a local pool or pools of IP address have been configured on the GGSN using the **ip local pool** configuration command.

Holdback Timer

The IP local pool holdback timer feature (**recycle delay** keyword option) enables you to configure a specific amount of time a newly released IP address is held before being made available for reassignment. This ensures that an IP address recently released after a PDP session is deleted is not reassigned to another PDP context before the IP-to-user relationship is 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 could incorrectly associate the new user with the record of the previous user, therefore erroneously associating the charging and service access of the new user to the previous user.

The holdback functionality is provided by the support of a new timestamp field added to the pool element data structure. When a request to allocate a specific address is made, if the address is available for reassignment, the current time is checked against the timestamp field of the element. If that number is equal to, or exceeds the number of seconds configured for the recycle delay, the address is reassigned.

When a request is made to allocate the first free address from the free queue, the difference between the current timestamp and the timestamp stored for the element is calculated. If the number is equal to, or exceeds, the configured recycle delay, the address is allocated. If the number is not equal to, or does not exceed the configured recycle delay, the address is not allocated for that request. (The free queue is a first-in first-out [FIFO] queue. Therefore, all other elements will have a great recycle delay than the first element.)

When an address assignment is blocked because an IP address is held for some time, a count of blocked address assignments that is maintained for the local pool is incremented.

Note The holdback timer feature does not support IPv6 local pools.

To configure a local IP address pool, use the following command in global configuration mode:

	Command	Purpose
Step 1	`Router(config)#ip local pool {default | pool-name low-ip-address [high-ip-address]} [recycle delay seconds]`	Configures a local pool of IP addresses to use when a remote peer connects to a point-to-point interface, where: • **default**—Default local address pool is used if no other pool is named. • *pool-name*—Name of a specific local address pool. • *low-ip-address*—Lowest IP address in the pool. • *high-ip-address*—(Optional) Highest IP address in the pool. If this value is omitted, only the low-ip-address IP address argument is included in the local pool. • **recycle delay** *seconds*—(Optional) The time, in seconds, addresses should be held before making them available for reassignment.

To assign a local pool to an access-point, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# ip-address-pool local pool-name`	(Optional) Specifies that a local pool provides the IP address.

Note Using VRF at the access point, you can configure APNs that use the same IP address pool (overlapping addresses).

Fore more information on configuring VPN access via VRF from an access point, see the "VPN Access Using VRF Configuration Task Lists" section on page 9-13.

To verify the local pool configure, use the **show ip local** [*pool name*] command in privileged EXEC mode:

```
Router#show ip local pool
Pool    Begin       End         Free    In use  Blocked
poola   10.8.8.1    10.8.8.5    5       0       0

Router #show ip local pool poolA
Pool    Begin       End         Free    In use  Blocked
poola   10.8.8.1    10.8.8.5    5       0       0

Available addresses:
10.8.8.1
10.8.8.2
10.8.8.3
10.8.8.4
10.8.8.5

Inuse addresses:
None

Held addresses: Time Remaining
None
```

Configuration Example

The following is a configuration example of a local address pool configured at the APN.

```
!
ip local pool local_pool1 128.1.0.1 128.1.255.254
!
access-point 1
access-point-name gprs.pdn.com
ip-address-pool local local_pool1
aggregate 128.1.0.0/16
exit
```

Configuring MS Addressing via RADIUS

Dynamic IP addressing via a RADIUS server is configured at the access-point configuration level using the **ip-address-pool** command in access-point configuration mode.

For more information about the ip-address-pool access-point configuration command, see "Configuring Additional Real Access Point Options" section on page 9-20. For more information about configuring RADIUS, see *Cisco IOS Security Configuration Guide*.

Configuring Overlapping Local IP Address Pools

The Overlapping Local IP Address Pools feature improves flexibility in assigning IP addresses dynamically. This feature allows you to configure overlapping IP address pool groups to create different address spaces and concurrently use the same IP addresses in different address spaces.

Overlapping Local IP Address Pools gives greater flexibility in assigning IP addresses dynamically. It allows you to configure overlapping IP address pool groups to create different address spaces and concurrently use the same IP addresses in different address spaces.

With Cisco IOS Release 12.3(2)XB and later, the GGSN supports the concept of an IP address group to support multiple IP address spaces and still allow the verification of non overlapping IP address pools within a pool group. Pool names must be unique within the GGSN. The pool name carries an implicit group identifier because that pool name can be associated only with one group. Pools without an explicit group name are considered members of the base system group and are processed in the same manner as the original IP pool implementation.

Existing configurations are not affected by the new pool feature. The "group" concept is an extension of the existing **ip local pool** command. Processing of pools that are not specified as a member of a group is unchanged from the existing implementation.

To configure a local IP address pool group and verify that it exists, use the following commands in global configuration mode:

	Command	Purpose

Step 1	`Router(config)#ip local pool {default | pool-name} [low-ip-address [high-ip-address]] [group group-name]`
	
	Example:
	`GGSN(config)# ip local pool testpool 10.2.2.1 10.2.2.10 group testgroup cache-size 10000`
		Configures a local pool of IP addresses to use when a remote peer connects to a point-to-point interface, where:
		• **default**—Defaults local address pool that is used if no other pool is named.
		• *pool-name*—Name of a specific local address pool.
		• *low-ip-address*—Lowest IP address in the pool.
		• *high-ip-address*—(Optional) Highest IP address in the pool. If this value is omitted, only the low-ip-address IP address argument is included in the local pool.
		• **group** *group-name*—(Optional) Creates a pool group.

Step 2	`Router(config)# show ip local pool [poolname | [group group-name]]`
	
	Example:
	`GGSN(config)# show ip local pool group testgroup testpool`
		Displays statistics for any defined IP address pools.

Overlapping Local IP Address Pools Configuration Examples

The following are configuration examples for configuring IP overlapping address pools.

- Defining Local Address Pooling as the Global Default, page 13-14
- Configuring Multiple Ranges of IP Addresses into One Pool Example, page 13-14
- Configuring IP Overlapping Address Pools on a GGSN on the Cisco 7600 Platform with Supervisor II / MSFC2 Example, page 13-14

Defining Local Address Pooling as the Global Default

The following example shows how to configure local pooling as the global default mechanism:

```
ip address-pool local ip local pool default 192.169.15.15 192.68.15.16
```

Configuring Multiple Ranges of IP Addresses into One Pool Example

The following example shows how to configure two ranges of IP addresses for one IP address pool:

```
ip local pool default 192.169.10.10 192.169.10.20
ip local pool default 192.169.50.25 192.169.50.50
```

Configuring IP Overlapping Address Pools on a GGSN on the Cisco 7600 Platform with Supervisor II / MSFC2 Example

The following example shows how to configure IP overlapping address pools on the Cisco 7600 platform

The following examples also show a partial configuration for two VPNs (vpn1 and vpn2) and their associated GRE tunnel configurations (Tunnel1 and Tunnel2).

On the GGSN:

```
service gprs ggsn
!
hostname 7600-7-2
!
ip cef
!
ip vrf vpn1
 description GRE Tunnel 1
 rd 100:1
!
ip vrf vpn2
 description GRE Tunnel 3
 rd 101:1
!
interface Loopback1
 ip address 150.1.1.72 255.255.0.0
!
interface Loopback100
 description GPRS GTP V-TEMPLATE IP ADDRESS
 ip address 9.9.9.72 255.255.255.0
!
interface Tunnel1
 description VRF-GRE to PDN 7500(13) Fa0/1
 ip vrf forwarding vpn1
 ip address 50.50.52.72 255.255.255.0
 tunnel source 150.1.1.72
 tunnel destination 165.2.1.13
!
interface Tunnel2
 description VRF-GRE to PDN PDN x(12) Fa3/0
 ip vrf forwarding vpn2
 ip address 80.80.82.72 255.255.255.0
 tunnel source 150.1.1.72
 tunnel destination 167.2.1.12
!
interface GigabitEthernet0/0.1
 description Gi
 encapsulation dot1Q 100
```

```
 ip address 10.1.2.72 255.255.255.0
!
interface Virtual-Template1
 description GTP v-access
 ip unnumbered Loopback100
 encapsulation gtp
 gprs access-point-list gprs
!
router ospf 10
 network 10.1.2.0 0.0.0.255 area 10
 network 150.1.0.0 0.0.255.255 area 10
!
ip local pool vpn1_pool 100.2.0.1 100.2.255.255 group vpn1
ip local pool vpn2_pool 100.2.0.1 100.2.255.255 group vpn2
ip route vrf vpn1 0.0.0.0 255.255.255.0 Tunnel1
ip route vrf vpn2 0.0.0.0 255.255.255.0 Tunnel2

gprs access-point-list gprs
  access-point 1
   access-point-name apn.vrf1.com
   access-mode non-transparent
   aaa-group authentication ipdbfms
   ip-address-pool local vpn1_pool
   vrf vpn1
   !
  access-point 2
   access-point-name apn.vrf2.com
   access-mode non-transparent
   aaa-group authentication ipdbfms
   ip-address-pool local vpn2_pool
   vrf vpn2
   !
```

Related configuration on the Supervisor / MSFC2:

```
interface FastEthernet9/5
 no ip address
 switchport
 switchport access vlan 167
 no cdp enable
!
interface FastEthernet9/10
 no ip address
 switchport
 switchport access vlan 165
 no cdp enable
!
interface Vlan165
 ip address 165.1.1.1 255.255.0.0
!
interface Vlan167
 ip address 167.1.1.1 255.255.0.0
!
! provides route to tunnel endpoints on GGSNs
router ospf 10
 network 10.1.2.0 0.0.0.255 area 10
!
! routes to tunnel endpoints on PDN
!
ip route 165.2.0.0 255.255.0.0 165.1.1.13
ip route 167.2.0.0 255.255.0.0 167.1.1.12
```

Configuring the NBNS and DNS Address for an APN

You can configure a primary and secondary NetBIOS Name Service (NBNS) and domain name system (DNS) under an APN. This feature is benefits address allocation schemes where there is no mechanism to obtain these address. Also, for a RADIUS-based allocation scheme, it prevents the operator from having to configure a NBNS and DNS under each user profile.

The NBNS and DNS addresses can come from three possible sources: DHCP server, RADIUS server, or local APN configuration. The criterion for selecting the addresses depends on the IP address allocation scheme configured under the APN. Depending on the configuration, the criterion for selecting the DNS and NBNS addresses is as follows:

1. DHCP-based IP address allocation scheme (local and external)—NBNS address returned from the DHCP server is sent to the MS. If the DHCP server does not return an NBNS address, the local APN configuration is used.
2. RADIUS-based IP address allocation scheme—NBNS address returned from the RADIUS server (in Access-Accept responses) is used. If the RADIUS server does not return an NBNS address, the local APN configuration is used.
3. Local IP Address Pool-based IP address allocation scheme—Local APN configuration is used.
4. Static IP Addresses—Local APN configuration is used.

Note The GGSN sends NBNS and DNS addresses in the create PDP response only if the MS is requesting the DNS address in the PCO IE.

To specify a primary (and backup) NBNS to be sent in create PDP responses at the access point, use the **nbns primary** command in access-point configuration mode. To remove the NBNS from the access-point configuration, use the **no** form of this command

nbns primary *ip-address* [**secondary** *ip-address*]

To specify a primary (and backup) DNS to be sent in create PDP responses at the access point, use the **dns primary** command in access-point configuration mode. To remove the DNS from the access-point configuration, use the **no** form of this command

dns primary *ip-address* [**secondary** *ip-address*]

Using Dynamic IP Address Management on the Cisco GGSN

With Cisco GGSN Release 10.0 and later, the Dynamic IP Address Management feature enables dynamic IP address allocation to support operators who might not initially know the IP address range of a subscriber, and therefore, the routing table cannot be preconfigured on the supervisor module to provide the proper routing of downlink traffic.

Cisco GGSN Release 10.0 and later introduces a *subnet manager* function that enables the dynamic creation of subnet routes . This enables multiple host routesto be aggregated into a single subnet route. Dynamic subnet routes are created only in an eGGSN implementation when Cisco CSG2 is present. Dynamic subnets cannot be created in a non-eGGSN implementation.

When configuring dynamic IP address management:

- Routing entries are dynamically created.
- OSPF routing protocol is used to propagate dynamic routes from the PCOP to the supervisor in a non-eGGSN implementation. In an eGGSN implementation, OSPF on the Cisco CSG2 propagates the routes to the supervisor.
- Dynamic subnet creation is only supported in an eGGSN implementation when a Cisco CSG2 is present and reduces the total number of dynamic routing entries.
- In both eGGSN and non eGGSN implementations, pre-existing aggregate route schemes are supported.
- Dynamic routes are synchronized to the standby GGSN.

Subnet Management in an Enhanced GGSN Implementation

In an eGGSN implementation with the Cisco CSG2, when a default subnet mask is specified under an APN, dynamic subnet creation is automatically enabled.

During the create PDP context process, once the IP address of a subscriber is determined (via a local pool, DHCP, or RADIUS), the Cisco GGSN subnet manager attempts to match the IP address with one of the configured aggregate routes. The aggregate routes can be under the APN, or globally defined if **aggregate auto** is enabled.

The selection rules give the highest priority to Framed-IP-Address/Mask attributes in Radius Access Requests, followed by APN aggregate routes, and then global aggregate routes. If none of those are matched, the Cisco GGSN applies the APN default subnet mask, if configured, to generate a dynamic subnet route. If you have not configured a default subnet mask under an APN, the Cisco GGSN uses the host route.

Once the route is determined, the Cisco GGSN invokes a Cisco CSG2 *load balancing* (see "Configuring Cisco CSG2 Load Balancing" section on page 8-43). The Cisco CSG2 load balancing determines the serving Cisco CSG2 for the given subscriber IP address and subnet mask. The same Cisco CSG2 is selected across Cisco SAMIs if the Cisco CSG2 and subscriber IP address and subnet mask configuration is identical in the same APN.

When the Cisco CSG2 is selected, the Cisco GGSN sends the Accounting-Start messages to the selected Cisco CSG2, along with a new route-info VSA that includes the subscriber IP address and subnet mask. The Cisco CSG2 propagates the subnet route to the supervisor via OSPF.

Subnet Management in an Non Enhanced GGSN Implementation

Dynamic subnet creation is disable in a non-eGGSN implementation. If a default subnet mask is configured under an APN, it is ignored.

During the create PDP context processing, when the IP address of a subscriber is determined (via local pool, DHCP, or RADIUS), the subnet manager attempts to match the IP address with one of the configured aggregate routes. The aggregate rouates can be under the APN, or globally defined if aggregate-auto is enabled.

The selection rules give the highest priority to Framed-IP-Address/Mask attributes in Radius Access Requests, followed by APN aggregate routes, and then global aggregate routes. If none of those match, a host route is created.

The Cisco GGSN propagates the downlink route to the supervisor.

Enabling Mobile Routes on the GGSN

To support dynamic IP address management, before the creation of any PDP contexts, you must configure the **router mobile** command in global configuration mode on the Cisco GGSN to enable mobile routes.

Note The **router mobile** command is an existing Cisco IOS command that is used in a Cisco GGSN and Cisco CSG2 implementation to *only* enable the dynamic IP address manager feature. The Cisco GGSN utilization of the **router mobile** command is not related to any other Cisco IOS **router mobile** command usage. No other routing mobile subcommand is supported on the Cisco GGSN.

In the service-aware GGSN implementation, the **router mobile** command in global configuration mode enables the GGSN to manage routing entries for subscribers more efficiently. These entries are idefintified by the leter “M” in the routing table displayed using the **show ip route** command. When OSPF is enabled, these routing entries can be propagated to a routing peer.

To enable mobile routes on the Cisco GGSN, use the following command:

Command	Purpose
`Router(config)# router mobile`	Enables mobile routes on the Cisco GGSN.

To display the routes, use **show ip route** command in privileged EXEC mode:

```
GGSN-8#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C       20.1.1.23 is directly connected, Loopback1
     23.0.0.0/16 is subnetted, 1 subnets
M       23.23.0.0 [1/0] via 0.0.0.0, 00:17:11, Virtual-Access3
```

Configuring a Default Subnet Mask for Dynamic Subnet Management

To configure a default subnet mask under an APN, and enable dynamic IP address management in an eGGSN implementation with a Cisco CSG2, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# aggregate 0.0.0.0 sub-mask`	Configures a default subnet mask for subnet management and enables dynamic subnet creation.

Disabling Route Propagation from the Cisco GGSN to the Supervisor

By default, route distribution is enabled. However, for an eGGSN implementation, OSPF route redistribution is not required and should be disabled because the Cisco CSG2 propagates downlink routes to the supervisor.

To configure the Cisco GGSN to not propagate downlink routes to the supervisor, use the following command in access-point configuration mode:

	Command	Purpose
Step 3	`Router(config-access-point)# ip-address-pool {dhcp-proxy-client | radius-client [no-redistribute] | local pool-name | disable}`	Specifies a dynamic address allocation method using IP address pools for the current access point, where: • **dhcp-proxy-client—**The access point IP address pool is allocated using a DHCP server • **radius-client**—The access point IP address pool is allocated using a RADIUS server. Optionally, specify the **no-redistribute** keyword option to disable • route propagation from the Cisco GGSN to the supervisor. • **local**—The access point IP address pool is allocated using a locally configured address pool. • **disable**—Disables dynamic address allocation for this access point.

Configuration Examples

The following are dynamic ip address management configuration examples:

```
gprs access-point-list gprs
  access-point 1
   access-point-name static-ip
   access-mode non-transparent
   aaa-accounting interim update
   aaa-group authentication ra_aaa
   aaa-group accounting ra_aaa
   csg-group csg1
```

```
 csg-group csg2
 gtp response-message wait-accounting
 charging profile any 1 override
 service-aware
 !
access-point 2
 access-point-name dhcp-ip
 access-mode non-transparent
 aaa-accounting interim update
 aaa-group authentication ra_aaa
 aaa-group accounting ra_aaa
 ip-address-pool dhcp-proxy-client
 csg-group csg1
 aggregate 0.0.0.0 255.255.0.0
 dhcp-server 172.64.110.38
 dhcp-gateway-address 172.69.69.1
 gtp response-message wait-accounting
 charging profile any 1 override
 service-aware
 !
access-point 3
 access-point-name radius-ip
 access-mode non-transparent
 aaa-accounting interim update
 aaa-group authentication ra_aaa
 aaa-group accounting ra_aaa
 ip-address-pool radius-client no-redistribute
 csg-group csg1
 aggregate 0.0.0.0 255.255.0.0
 gtp response-message wait-accounting
 charging profile any 1 override
 service-aware
 !
access-point 4
 access-point-name localpool-ip
 access-mode non-transparent
 aaa-accounting interim update
 aaa-group authentication ra_aaa
 aaa-group accounting ra_aaa
 ip-address-pool local ra_localpool
 csg-group csg1
 aggregate 0.0.0.0 255.255.255.255
 gtp response-message wait-accounting
 charging profile any 1 override
 service-aware
 advertise downlink next-hop 7.19.18.103
 !
access-point 5
 access-point-name dhcpvrf-ip
 ip-address-pool dhcp-proxy-client
 csg-group csg1
 dhcp-server 172.64.110.38
 dhcp-gateway-address 169.69.69.1
 !
access-point 6
 access-point-name dhcp-ip2
 ip-address-pool dhcp-proxy-client
 aggregate 172.0.0.0 255.0.0.0
 dhcp-server 172.64.110.38
 dhcp-gateway-address 172.69.69.1
 !
!
```

CHAPTER 14

Configuring Load Balancing on the GGSN

This chapter describes how to configure a gateway GPRS support node (GGSN) to support load balancing functions using the Cisco IOS software Server Load Balancing (SLB) feature. GTP load balancing provides increased reliability and availability when you are using multiple Cisco GGSNs or non-Cisco GGSNs in your GPRS/UMTS network.

For complete descriptions of the GGSN commands in this chapter, see *Cisco GGSN Command Reference* for the Cisco GGSN release you are using. For complete descriptions of the other Cisco IOS SLB commands in this chapter, see the *IOS Server Load Balancing* feature module.

To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

This chapter includes the following sections:

- Overview of GTP Load Balancing, page 14-1
- Configuring GTP Load Balancing, page 14-7
- Monitoring and Maintaining the Cisco IOS SLB Feature, page 14-25
- Configuration Examples, page 14-26

Overview of GTP Load Balancing

This section provides an overview of the Cisco IOS SLB feature and GTP load balancing support on the GGSN. It includes the following sections:

- Overview of Cisco IOS SLB, page 14-1
- Overview of GTP Load Balancing, page 14-2
- GTP SLB Restrictions, page 14-7

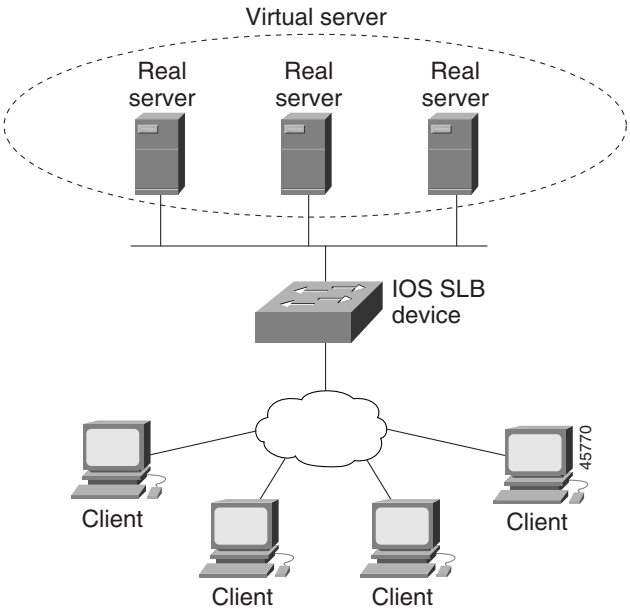
Overview of Cisco IOS SLB

The Cisco SLB feature is an IOS-based solution that provides IP server load balancing. Using the Cisco IOS SLB feature, you can define a *virtual server* that represents a group of *real servers* in a cluster of network servers called a *server farm*. In this environment, the clients connect to the IP address of the virtual server. When a client initiates a connection to the virtual server, the Cisco IOS SLB feature chooses a real server for the connection, based on a configured *load-balancing algorithm*.

The Cisco IOS SLB feature also provides firewall load balancing, which balances flows across a group of *firewalls* called a *firewall farm*.

Figure 14-1 presents a logical view of a simple Cisco IOS SLB network.

Figure 14-1 Logical View of IOS SLB



Overview of GTP Load Balancing

Cisco IOS SLB provides GGSN GTP load balancing and increased reliability and availability for the GGSN. GGSN GTP load balancing supports a subset of the overall server load-balancing functions that are available in the Cisco IOS SLB feature. Therefore, the full scope of Cisco IOS SLB functions is not applicable to the general packet radio service/Universal Mobile Telecommunication System (GPRS/UMTS) environment. For more information about unsupported functions, see the "GTP SLB Restrictions" section on page 14-7.

When configuring GTP load balancing, a pool of GGSNs is configured as a server farm in Cisco IOS SLB. These are the GGSNs across which you want to load-balance GTP sessions. A virtual server instance is configured in Cisco IOS SLB to load balance GTP sessions across the GGSN farm. This virtual server is associated with the server farm that you configured in Cisco IOS SLB.

When configuring GTP load balancing:

- GTP load balancing is supported by using the Cisco IOS SLB feature on the supervisor engine.
- The IOS SLB on the supervisor engine processes only the Create PDP Context requests sent to the GGSN virtual IP address. When a Create PDP Context request is received, a real GGSN is selected based on the load at that time. Once the PDP context is established, all subsequent transactions corresponding to the PDP contexts occurs directly between that GGSN and corresponding SGSN, bypassing the Cisco IOS SLB on the supervisor engine.

- In addition:
  - Multiple virtual servers are supported
  - Load-balanced real servers can be internal or external to the Cisco 7600 chassis
  - Each virtual server must have one unique public IP address that is reachable from the SGSNs
  - Each virtual server can correspond to one or more APNs.
  - The DNS server used by the SGSNs to resolve the APNs to a GGSN IP address should use the GGSN virtual IP address.

Supported GTP Load Balancing Types

The Cisco IOS SLB supports two types of GTP load balancing:

- GTP Load Balancing Without GTP Cause Code Inspection, page 14-3
- GTP Load Balancing With GTP Cause Code Inspection, page 14-3

GTP Load Balancing Without GTP Cause Code Inspection

GTP load balancing *without* GTP cause code inspection enabled is recommended for Cisco GGSNs. It has the following characteristics:

- Can operate in dispatched mode or in directed server Network Address Translation (NAT) mode, but not in directed client NAT mode. In dispatched mode, the GGSNs must be Layer 2–adjacent to the Cisco IOS SLB device.
- Does not support stateful backup.
- Delivers tunnel creation messages destined to the virtual GGSN IP address to one of the real GGSNs, using the weighted round-robin load-balancing algorithm. See the "Weighted Round-Robin" section on page 14-4 for more information about this algorithm.
- Requires Dynamic Feedback Protocol (DFP) to account for GTPv1 secondary PDP contexts.

GTP Load Balancing With GTP Cause Code Inspection

GTP load balancing *with* GTP cause code inspection enabled allows Cisco IOS SLB to monitor all PDP context signaling flows to and from server farms. This enables Cisco IOS SLB to monitor GTP failure cause codes, detecting system-level problems in both Cisco and non-Cisco GGSNs.

Table 14-1 lists the Create PDP Context response cause codes and the corresponding actions taken by Cisco IOS SLB.

Table 14-1 PDP Create Response Cause Codes and Corresponding Cisco IOS SLB Actions

Cause Code	Cisco IOS SLB Action
Request Accepted	Establish session
No Resource Available	Fail current real, reassign session, drop the response
All dynamic addresses are occupied	Fail current real, reassign session, drop the response
No memory is available	Fail current real, reassign session, drop the response
System Failure	Fail current real, reassign session, drop the response
Missing or Unknown APN	Forward the response
Unknown PDP Address or PDP type	Forward the response

Table 14-1 PDP Create Response Cause Codes and Corresponding Cisco IOS SLB Actions

Cause Code	Cisco IOS SLB Action
User Authentication Failed	Forward the response
Semantic error in TFT operation	Forward the response
Syntactic error in TFT operation	Forward the response
Semantic error in packet filter	Forward the response
Syntactic error in packet filter	Forward the response
Mandatory IE incorrect	Forward the response
Mandatory IE missing	Forward the response
Optional IE incorrect	Forward the response
Invalid message format	Forward the response
Version not supported	Forward the response
PDP context without TFT already activated	Fail current real, reassign session, drop the response

GTP load balancing *with* GTP cause code inspection enabled has the following characteristics:

- Must operate in directed server NAT mode.
- Assigns PDP context creates from a specific International Mobile Subscriber ID (IMSI) to the same GGSN, or, if GTP APN-aware load balancing is configured, to the same server farm.
- Supports stateful backup.
- Tracks the number of open PDP contexts for each GGSN or APN, which enables server farms to use the weighted least connections (**leastconns**) algorithm for GTP load balancing. See the "Weighted Least Connections" section on page 14-5 for more information about this algorithm.
- Enables Cisco IOS SLB to deny access to a virtual GGSN if the carrier code of the requesting IMSI does not match a specified value.
- Enables Cisco IOS SLB to support secondary IPDP contexts, even without DFP.

Cisco IOS SLB Algorithms Supported for GTP Load Balancing

The following two Cisco IOS SLB algorithms are supported for GTP load balancing:

- Weighted Round-Robin, page 14-4
- Weighted Least Connections, page 14-5

Weighted Round-Robin

The weighted round- robin algorithm specifies that the real server used for a new connection to the virtual server is chosen from the server farm in a circular fashion. Each real server is assigned a weight, *n*, that represents its capacity to handle connections, as compared to the other real servers associated with the virtual server. That is, new connections are assigned to a given real server *n* times before the next real server in the server farm is chosen.

For example, assume a server farm made up of three real servers: ServerA with $n = 3$, ServerB with $n = 1$, and ServerC with $n = 2$. The first three connections to the virtual server are assigned to ServerA, the fourth connection to ServerB, and the fifth and sixth connections to ServerC.

Note Assigning a weight of $n = 1$ to all of the servers in the server farm configures the Cisco IOS SLB device to use a simple round-robin algorithm.

GTP load balancing *without* GTP cause code inspection enabled requires the weighted round-robin algorithm. A server farm that uses weighted least connections can be bound to a virtual server that provides GTP load balancing without GTP cause code inspection enabled, but you cannot place that virtual server **INSERVICE**. If you try to do so, Cisco IOS SLB issues an error message.

Weighted Least Connections

When GTP cause code inspection is enabled, GTP load balancing supports the Cisco IOS SLB weighted least connections algorithm.

The weighted least connections algorithm specifies that the next real server chosen from a server farm for a new connection to the virtual server is the server with the fewest active connections. Each real server is assigned a weight for this algorithm, also. When weights are assigned, the server with the fewest connections is determined on the basis of the number of active connections on each server and the relative capacity of each server. The capacity of a given real server is calculated as the assigned weight of that server divided by the sum of the assigned weights of all the real servers associated with that virtual server, or $n_1/(n_1+n_2+n_3...)$.

For example, assume a server farm made up of three real servers: ServerA with $n = 3$, ServerB with $n = 1$, and ServerC with $n = 2$. ServerA would have a calculated capacity of 3/(3+1+2), or half of all active connections on the virtual server, ServerB would have a calculated capacity of one-sixth of all active connections, and ServerC one-third of all active connections. At any point in time, the next connection to the virtual server would be assigned to the real server whose number of active connections is farthest below its calculated capacity.

Note Assigning a weight of $n = 1$ to all of the servers in the server farm configures the Cisco IOS SLB device to use a simple least-connection algorithm.

GTP load balancing *without* GTP cause code inspection enabled *does not* support the weighted least connections algorithm.

GTP load balancing *with* GTP cause code inspection *does* support the weighted least connections algorithm.

Dynamic Feedback Protocol for Cisco IOS SLB

In GTP load balancing, Cisco IOS SLB detects when a PDP context is established, but it does not detect when PDP contexts are cleared, and therefore it cannot determine the number of open PDP contexts for each GGSN. Use the Cisco IOS SLB DFP to calculate GPRS/UMTS load-balancing weights dynamically.

With Cisco IOS SLB DFP support, a *DFP manager* in a load-balancing environment can initiate a TCP connection with a *DFP agent*. Thereafter, the DFP agent collects status information from one or more real host servers, converts the information to relative weights, and reports the weights to the DFP manager. The DFP manager factors in the weights when load balancing the real servers. In addition to reporting at user-defined intervals, the DFP agent sends an early report if there is a sudden change in a real server's status.

The weights calculated by DFP override the static weights you define using the **weight (server farm)** command. If DFP is removed from the network, Cisco IOS SLB reverts to the static weights.

You can define Cisco IOS SLB as a DFP manager, as a DFP agent for another DFP manager (such as DistributedDirector), or as both at the same time. In such a configuration, Cisco IOS SLB sends periodic reports to DistributedDirector, which uses the information to choose the best server farm for each new connection request. Cisco IOS SLB then uses the same information to choose the best real server within the chosen server farm.

DFP also supports the use of multiple DFP agents from different client subsystems (such as Cisco IOS SLB and GPRS/UMTS) at the same time.

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

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

By default, the CPU and memory utilization become part of the DFP weight calculation only after the utilization exceeds 85 percent. You can use the **min-cpu-load** and **mem-load** keyword options added to the **gprs dfp** global configuration command to customize the percentage of utilization at which the CPU and memory loads are included in the weight calculation.

Note Because the maximum number of allowed PDP contexts is considered to be the GGSNs maximum load, you should carefully consider the value that you configure in the **gprs maximum-pdp-context-allowed** command, which defaults to 10,000 PDP contexts.

GTP IMSI Sticky Database Support

Cisco IOS SLB can select a GGSN, or APN if GTP APN-aware load balancing is configured, for a given International Mobile Subscriber ID (IMSI), and forward all subsequent Packet Data Protocol (PDP) create requests from the same IMSI to the selected GGSN or APN.

To enable this feature, Cisco IOS SLB uses a GTP IMSI sticky database, which maps each IMSI to its corresponding real server, in addition to its session database.

The Cisco IOS SLB creates a sticky database object when it processes the first Create PDP Context request for a given IMSI. The Cisco IOS SLB removes the sticky object when it receives a notification to do so from the real server, or as a result of inactivity. When the last PDP belonging to an IMSI is deleted, the GGSN notifies Cisco IOS SLB to remove the sticky object.

Sticky Database Support and GTP APN-Aware Load Balancing

The sticky IMSI feature prevents sessions from the same user for the same APN being assigned to different GGSNs. With server farm selection based on APN (PAN-aware load balancing), the sticky IMSI feature ensures that a sticky entry is for the same server farm based on the APN before the IMSI can be issued. If a new Create PDP Context request is for a different APN, which causes GTP SLB to select a different server farm than the one for which the sticky entry was created, the server farm is respected over the real because if the real belongs to a different server farm, the serverfarm might not support the APN.

GTP APN-Aware Load Balancing

With Cisco IOS software release 12.2(18) SRB and later on the supervisor engine, *GTP APN-aware* load balancing can be configured.

Using the GTP APN-aware feature, a set of APNs can be mapped to a server farm in the Cisco IOS SLB. Multiple server farms can be created, each supporting a different set of APNs. Create PDP context requests are balanced across APNs.

For information on configuring GTP APN-aware load balancing, see the "Configuring GTP APN-Aware Load Balancing" section on page 14-15.

GTP SLB Restrictions

The following restrictions apply when configuring GTP load balancing:

- For GTP load balancing without GTP cause code inspection enabled:
  - Operates in either dispatched mode or directed server NAT mode only
  - Cannot load balance network-initiated PDP context requests
  - Does not support the following Cisco IOS SLB functions:
    - Bind IDs
    - Client-assigned load balancing
    - Slow Start
    - Stateful backup (not supported on the Cisco 7600 platform)
    - Weighted least connections load-balancing algorithm
- For GTP load balancing *with* GTP cause code inspection enabled:
  - Operates in directed server NAT mode only
  - Cannot load-balance network-initiated PDP context requests
  - Requires either the SGSN or the GGSN to echo its peer
  - Inbound and outbound traffic should be routed via Cisco IOS SLB
  - Does not support the following Cisco IOS SLB functions:
    - Bind IDs
    - Client-assigned load balancing
    - Slow Start
    - Sticky connections

Configuring GTP Load Balancing

This section includes the following topics:

- GTP Load Balancing Configuration Task List, page 14-8
- Configuration Guidelines, page 14-8

GTP Load Balancing Configuration Task List

This section lists the tasks used to configure GTP load balancing. Detailed configuration information is contained in the referenced sections of this document or other documents. Required and optional tasks are indicated.

1. On the Cisco IOS SLB, complete the following tasks:
   a. Configuring a Server Farm and Real Server, page 14-9 (Required)
   b. Configuring a Virtual Server, page 14-11 (Required)
   c. Configuring a GSN Idle Timer, page 14-14 (Optional if GTP cause code inspection is enabled)
   d. Configuring DFP Support, page 14-14 (Optional, but recommended)
   e. Configuring GTP APN-Aware Load Balancing, page 14-15 (Optional)
2. On the GGSN, complete the following tasks:
   a. Configuring a Loopback Interface for GTP SLB, page 14-19 (Required)
   b. Configuring DFP Support on the GGSN, page 14-20 (Optional, but recommended)
   c. Configuring Messaging from the GGSN to the Cisco IOS SLB, page 14-21 (Optional)
3. Routing each GGSN to each associated serving GPRS support node (SGSN) (Required)

   The route can be static or dynamic but the GGSN needs to be able to reach the SGSN. For more information, see the "Configuring a Route to the SGSN" section on page 9-4.
4. On the SGSN, route each SGSN to the virtual templates on each associated GGSN, and to the GGSN load-balancing virtual server (Required)

Configuration Guidelines

When configuring the network shared by Cisco IOS SLB and the GGSNs, keep the following considerations in mind:

- Specify static routes (using **ip route** commands) and real server IP addresses (using **real** commands) so that the Layer 2 information is correct and unambiguous.
- Configure the static route from the SGSN to the virtual server.
- Choose subnets carefully, using one of the following methods:
  - Do not overlap virtual template address subnets.
  - Specify next-hop addresses to real servers, not to interfaces on those servers.
- Cisco IOS SLB supports two types of GTP load balancing:
  - GTP Load Balancing Without GTP Cause Code Inspection, page 14-3
  - GTP Load Balancing With GTP Cause Code Inspection, page 14-3
- Cisco IOS SLB supports both GTP v0 and GTP v1. Support for GTP enables Cisco IOS SLB to become "GTP aware," extending Cisco IOS SLB's knowledge into Layer 5.

- On the Cisco 7600 platform, the following apply:
  - Multiple GTP virtual servers are supported.
  - Load balanced real servers can be internal or external to the Cisco 7600 chassis.
  - Each GTP virtual server must have one unique public IP address that is reachable from the SGSNs.
  - Each virtual server can correspond to one or more APNs.
  - The DNS server used by the SGSNs to resolve the APNs to a GGSN IP address should use the GTP virtual IP address.
- When configuring GTP APN-aware load balancing:
  - Cisco IOS software release 12.2(18) SRB and later is required on the supervisor engine and Cisco GGSN Release 7.0, Cisco IOS Release 12.4(9)XG and later is required on the GGSN.
  - GTP load balancing with GTP cause code inspection enabled is not supported.
  - For a given IOS SLB GTP map, you can configure up to 100 **pan** commands, however, because APN maps can impact performance, we recommend that you do not configure more than 10 APN maps per vserver.
  - The primary and backup virtual servers should have the same mapping rules.
  - The same real cannot be configured in multiple server farms.

Configuring the Cisco IOS SLB for GTP Load Balancing

To configure GTP load balancing, you must complete the following tasks on the Cisco IOS SLB:

- Configuring a Server Farm and Real Server, page 14-9 (Required)
- Configuring a Virtual Server, page 14-11 (Required)
- Configuring a GSN Idle Timer, page 14-14 (Optional)
- Configuring DFP Support, page 14-14 (Optional, but recommended)
- Configuring GTP APN-Aware Load Balancing, page 14-15 (Optional)
- Verifying the Cisco IOS SLB Configuration, page 14-18 (Optional)

Configuring a Server Farm and Real Server

When you configure the server farm and real server on the Cisco IOS SLB for GTP load balancing, use the following guidelines to ensure proper configuration:

- If GTP cause code inspection is not enabled, accept the default setting (the weighted round-robin algorithm) for the **predictor** command.

  If GTP cause code inspection is enabled, you can specify either the weighted round-robin algorithm (**roundrobin**) or the weighted least connections (**leastconns**) algorithm.
- Specify the IP addresses (virtual template addresses, for Cisco GGSNs) of the real servers performing the GGSN function, using the **real** command.
- Specify a reassign threshold less than the SGSN's N3-REQUESTS counter value by using the **reassign** command.

To configure a Cisco IOS SLB server farm, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router-SLB(config)# ip slb serverfarm serverfarm-name` `Router(config-slb-sfarm)#`	Adds a server farm definition to the Cisco IOS SLB configuration, and enters server farm configuration mode.
Step 2	`Router-SLB(config-slb-sfarm)# predictor [roundrobin | leastconns]`	Specifies the algorithm to use to determine how a real server is selected. **Note** In GTP load balancing *without* GTP cause code inspection enabled, you must accept the default setting (the weighted round-robin algorithm). See the following sections for more details about each algorithm: • Weighted Round-Robin, page 14-4 • Weighted Least Connections, page 14-5
Step 3	`Router-SLB(config-slb-sfarm)# nat server`	(Required if GTP cause code inspection is enabled; optional for GTP load balancing *without* cause code inspection enabled) Configures NAT server address translation mode on the server farm.
Step 4	`Router-SLB(config-slb-sfarm)# real ip-address [port]`	Identifies a real GGSN as a member of a server farm, using the IP address of the GGSN's virtual template interface, and enters real server configuration mode.
Step 5	`Router-SLB(config-slb-real)# faildetect numconns number-conns [numclients number-clients]`	(Optional) Specifies the number of consecutive connection failures and, optionally, the number of unique client connection failures, that constitute failure of the real server.
Step 6	`Router-SLB(config-slb-real)# maxconns number-conns`	(Optional) Specifies the maximum number of active connections allowed on the real server at one time. **Note** In GTP load balancing *without* cause code inspection enabled, the impact of this command is minimal because a session will last no longer than the duration specified with the **ip gtp request** command.
Step 7	`Router-SLB(config-slb-real)# reassign threshold`	(Optional) Specifies the threshold of consecutive unacknowledged synchronizations or Create PDP Context requests that, if exceeded, results in an attempted connection to a different real server.
Step 8	`Router-SLB(config-slb-real)# retry retry-value`	(Optional) Specifies the interval, in seconds, to wait between the detection of a server failure and the next attempt to connect to the failed server.

	Command	Purpose
Step 9	`Router-SLB(config-slb-real)# weight weighting-value`	(Optional) Specifies the real server's workload capacity relative to other servers in the server farm. **Note** If you use DFP, the static weights you define using the **weight (server farm)** command are overridden by the weights calculated by DFP. If DFP is removed from the network, Cisco IOS SLB reverts to the static weights.
Step 10	`Router-SLB(config-slb-real)# inservice`	Enables the real server for use by Cisco IOS SLB.

Configuring a Virtual Server

When you configure the virtual server on the Cisco IOS SLB for GTP load balancing, use the following guidelines to ensure proper configuration:

- Configure a static route from the SGSN to the virtual server.
- Specify a virtual GGSN IP address as the virtual server, and use the **udp** keyword option.
- To load-balance GTP v1 sessions, specify port number **2123**, if the GGSNs and SGSNs are in compliance with the ETSI standard, or specify port number **0** or **any** to configure an all-port virtual server (that is, a virtual server that accepts flows destined for all ports).
- To load-balance GTP v0 sessions, specify port number **3386**, if the GGSNs and SGSNs are in compliance with the European Telecommunications Standards Institute (ETSI) standard, or specify port number **0** or **any** to configure an all-port virtual server.
- To enable GTP load balancing *without* GTP cause code inspection, specify the **service gtp** keyword option.
- To enable GTP load balancing *with* GTP cause code inspection, specify the **service gtp-inspect** keyword option.

  In GTP load balancing *without* GTP cause code inspection enabled, when you configure the GTP idle timer using the **idle** command, specify a GTP idle timer greater than the longest possible interval between PDP context requests on the SGSN.

To configure an Cisco IOS SLB virtual server, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router-SLB(config)# ip slb vserver virtual_server-name`	Identifies a virtual server, and enters virtual server configuration mode.

Step 2	`Router-SLB(config-slb-vserver)# virtual ip-addr [netmask [group]] {esp | gre | protocol}`
	
	or
	
	`Router(config-slb-vserver)# virtual ip-addr [netmask [group]] {tcp | udp} [port | any] [service service]`
		Specifies the virtual server IP address, type of connection, and optional TCP or UDP port number, Internet Key Exchange (IKE) Internet Security Association and Key Management Protocol (ISAKMP) or Wireless Session Protocol (WSP) setting, and service coupling.
		
		Note For GTP load balancing:
		
		– Specify a virtual GGSN IP address as the virtual server, and specify the **udp** keyword option.
		
		– To load-balance GTP v1 sessions, specify port number **2123**, if the GGSNs and SGSNs are in compliance with the ETSI standard, or specify port number **0** or **any** to configure an all-port virtual server (that is, a virtual server that accepts flows destined for all ports).
		
		– To load-balance GTP v0 sessions, specify port number **3386**, if the GGSNs and SGSNs are in compliance with the ETSI standard, or specify port number **0** or **any** to configure an all-port virtual server.
		
		– To enable GTP load balancing *without* GTP cause code inspection, specify the **service gtp** keyword option.
		
		– To enable GTP load balancing *with* GTP cause code inspection, specify the **service gtp-inspect** keyword option.

	Command	Purpose
Step 3	`Router-SLB(config-slb-vserver)# serverfarm` *primary-farm* [**backup** *backup-farm* [**sticky**]] [**map** *map-id* **priority** *priority*]	Associates a real server farm with a virtual server. • **backup**—(Optional) Configures a backup server farm • **backup** *backup-farm* [**sticky**]—(Optional) Configures a backup server farm and optionally specifies to use sticky connections in the backup server farm. • **map** *map-id* **priority** *priority*—(Optional) Associates an IOS SLB protocol map to a server farm for GTP APN-aware load balancing and defines the priority for that map. Maps are searched based on priority. The lower the number, the higher the priority. **Note** Multiple instances of the **serverfarm** command are allowed if configured with the **map** keyword option. The default server farm (without the **map** keyword option) is limited to a single instance. **Note** To change map configurations the virtual server must be taken out of service. **Note** The NAT modes on the primary and backup server farms for each map must match.
Step 4	`Router-SLB(config-slb-vserver)# idle` [**gtp request**] *duration*	(Optional) Specifies the minimum amount of time that Cisco IOS SLB maintains connection context in the absence of packet activity. The **idle** command specified without the **gtp request** keyword option controls the GTP idle timer for GTP load balancing *without* cause code inspection enable. The **idle gtp request** command controls the GTP idle timer for both GTP load balancing *without* cause code inspection enabled and for GTP load balancing *with* cause code inspection enabled. The **idle gtp request** is the recommended configuration. **Note** In GTP load balancing *without* GTP cause code inspection enabled, specify a GTP idle timer greater than the longest possible interval between PDP context requests on the SGSN.
Step 5	`Router-SLB(config-slb-vserver)# inservice`	Enables the virtual server for use by Cisco IOS SLB.

	Command	Purpose
Step 6	`Router-SLB(config-slb-vserver)# client {ip-address network-mask [exclude] | gtp carrier-code [code]}`	(Optional) Specifies which clients are allowed to use the virtual server. **Note** GTP load balancing supports only the **gtp carrier-code** option, and only if GTP cause code inspection is enabled.
Step 7	`Router-SLB(config-slb-vserver)# replicate casa listen-ip remote-ip port [interval] [password [0 | 7] password timeout]`	(Optional) Configures a stateful backup of Cisco IOS SLB decision tables to a backup switch. **Note** GTP load balancing *without* GTP cause code inspection enabled does not support this command.

Configuring a GSN Idle Timer

When GTP cause code inspection is enabled, you can configure the amount of time that the Cisco IOS SLB will maintain sessions to and from and idle GGSN or SGSN.

To configure a GSN idle timer, enter the following command in global configuration mode on the Cisco IOS SLB:

Command	Purpose
`Router-SLB(config)# ip slb timers gtp gsn duration`	Changes the amount of time that Cisco IOS SLB maintains sessions to and from an idle GGSN or SGSN.

Configuring DFP Support

You can define Cisco IOS SLB as a DFP manager, as a DFP agent for another DFP manager (such as DistributedDirector), or as both at the same time. Depending on your network configuration, you might enter the commands for configuring Cisco IOS SLB as a DFP manager and the commands for configuring Cisco IOS SLB as a DFP agent on the same device or on different devices.

To configure Cisco IOS SLB as a DFP manager, and to identify a DFP agent with which Cisco IOS SLB can initiate connections, use the following commands, beginning in global configuration mode:

	Command	Description
Step 1	`Router-SLB(config)# ip slb dfp [password [0|7] password [timeout]]`	Configures DFP, supplies an optional password, and enters DFP configuration mode.
Step 2	`Router-SLB(config-slb-dfp)# agent ip_address port-number [timeout [retry_count [retry_interval]]]`	Identifies a DFP agent to which Cisco IOS SLB can connect.

Configuring GTP APN-Aware Load Balancing

GTP APN-aware load balancing enables you to load balance across APNs.

When implementing GTP APN-aware load balancing, a set of APNs must be defined in a Cisco IOS SLB GTP map created on the IOS SLB. Then, the IOS SLB GTP map must be associated with a server farm under the virtual template on the IOS SLB.

To configure GTP APN-aware load balancing, complete the tasks in the following sections:

- Configuring a Cisco IOS SLB GTP Map for GTP APN-Aware Load Balancing, page 14-15
- Associating an IOS SLB GTP Map to a Server Farm on the Virtual Server, page 14-16

Prerequisites and Restrictions

When configuring GTP APN-aware load balancing:

- Cisco IOS software release 12.2(18) SRB and later is required on the supervisor engine and Cisco GGSN Release 7.0, Cisco IOS Release 12.4(9)XG and later is required on the GGSN.
- GTP load balancing with GTP cause code inspection enabled is not supported.
- For a given IOS SLB GTP map, you can configure up to 100 **apn** commands, however, because APN maps can impact performance, we recommend that you do not configure more than 10 APN maps per vserver.
- The primary and backup virtual servers should have the same mapping rules.
- The same real cannot be configured in multiple server farms.

Configuring a Cisco IOS SLB GTP Map for GTP APN-Aware Load Balancing

To enable APN-aware load balancing, an IOS SLB GTP map that groups certain APNs must be configured.

To configure an IOS SLB GTP map for load balancing across APNs, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router-SLB(config)# ip slb map` *map-id protocol*	Configures an IOS SLB protocol map and enter SLB map configuration mode. • *map-id*—IOS SLB protocol map identifier. The valid range is from 1 to 255. The map ID must be globally unique across all service types. • *protocol*—Protocol associated with the map. This should match the vserver service type. – **gtp**—For general packet radio service (GPRS) load balancing, configures an IOS SLB GPRS Tunneling Protocol (GTP) map and enters SLB GTP map configuration mode. – **radius**—For RADIUS load balancing, configures an IOS SLB RADIUS map and enters SLB RADIUS map configuration mode. **Note** With this release, GTP maps are supported.
Step 2	`Router-SLB(config-slb-map)# apn` *string*	Configures an ASCII regular expression string to be matched against the access point name (APN) for general packet radio service (GPRS) load balancing. **Note** For a given IOS SLB GTP map, you can configure up to 100 **apn** commands, however, because APN maps can impact performance, we recommend that you do not configure more than 10 APN maps per vserver.

Associating an IOS SLB GTP Map to a Server Farm on the Virtual Server

After an IOS SLB GTP map is created, it must be associated to the server farm when configuring the virtual server.

Note To change map configurations the virtual server must be taken out of service. The NAT modes on the primary and backup server farms for each map must match.

To specify a IOS SLB GTP map when associating a server farm with the virtual server, use the following command in virtual server configuration mode on the IOS SLB:

Command	Purpose
`Router-SLB(config-slb-vserver)# serverfarm` *primary-farm* [**backup** *backup-farm* [**sticky**]] [**map** *map-id* **priority** *priority*]	Associates a real server farm with a virtual server. • **backup**—(Optional) Configures a backup server farm • **backup** *backup-farm* [**sticky**]—(Optional) Configures a backup server farm and optionally specifies to use sticky connections in the backup server farm. • **map** *map-id* **priority** *priority*—(Optional) Associates an IOS SLB protocol map to a server farm for GTP APN-aware load balancing and defines the priority for that map. Maps are searched based on priority. The lower the number, the higher the priority. **Note** Multiple instances of the **serverfarm** command are allowed if configured with the **map** keyword option. The default server farm (without the **map** keyword option) is limited to a single instance. **Note** To change map configurations the virtual server must be taken out of service. **Note** The NAT modes on the primary and backup server farms for each map must match.

GTP APN-Aware Load Balancing Configuration Example

The following configuration example, from the IOS SLB, shows the IOS SLB GTP map configuration, and the map-to-server farm association under the virtual template.

```
!
/* server-farm configurations */
ip slb serverfarm farm1
 real 10.0.0.1
  inservice
 real 10.0.0.2
  inservice
ip slb serverfarm farm4
 real 10.0.0.7
  inservice
 real 10.0.0.8
  inservice
ip slb serverfarm farm5
 real 10.0.0.9
  inservice
 real 10.0.0.10
  inservice
!
/* GTP maps for GTP APN-aware SLB */
ip slb map 1 gtp
  apn www.*.edu
ip slb map 4 gtp
  apn abc.company1.com
  apn xyz.company2.com
ip slb map 5 gtp
```

```
  apn company3.com
!
/* associate the GTP map with server farm under virtual server */
ip slb vserver GGSN_SERVER
  virtual 10.10.10.10 udp 0 service gtp
  serverfarm farm1 map 1 priority 3
  serverfarm farm2 backup farm4 map 1 priority 2
  serverfarm farm4 map 4 priority 5
  serverfarm farm5 map 5 priority 4
  serverfarm farm6
```

Verifying the Cisco IOS SLB Configuration

This section describes how to verify the Cisco IOS SLB configuration. It includes the following topics:

- Verifying the Virtual Server, page 14-18
- Verifying the Server Farm, page 14-18
- Verifying Cisco IOS SLB Connectivity, page 14-19

Verifying the Virtual Server

The following **show ip slb vserver** command verifies the configuration of the virtual servers PUBLIC_HTTP and RESTRICTED_HTTP:

```
Router-SLB# show ip slb vserver

slb vserver      prot  virtual               state         conns
-------------------------------------------------------------------
PUBLIC_HTTP      TCP   10.0.0.1:80           OPERATIONAL     0
RESTRICTED_HTTP  TCP   10.0.0.2:80           OPERATIONAL     0
IOSSLB#
```

Verifying the Server Farm

The following **show ip slb reals** command displays the status of server farms PUBLIC and RESTRICTED, the associated real servers, and their status:

```
Router-SLB# show ip slb real

real                    farm name        weight   state          conns
-------------------------------------------------------------------------
10.1.1.1                 PUBLIC           8       OPERATIONAL      0
10.1.1.2                 PUBLIC           8       OPERATIONAL      0
10.1.1.3                 PUBLIC           8       OPERATIONAL      0
10.1.1.20                RESTRICTED       8       OPERATIONAL      0
10.1.1.21                RESTRICTED       8       OPERATIONAL      0
IOSSLB#
```

The following **show ip slb serverfarm** command displays the configuration and status of server farms PUBLIC and RESTRICTED:

```
Router-SLB# show ip slb serverfarm

server farm      predictor    nat   reals   bind id
-------------------------------------------------
PUBLIC           ROUNDROBIN   none  3       0
RESTRICTED       ROUNDROBIN   none  2       0
IOSSLB#
```

Verifying Cisco IOS SLB Connectivity

To verify that the Cisco IOS SLB feature is installed and is operating correctly, ping the real servers from the Cisco IOS SLB switch, and then ping the virtual servers from the clients.

The following **show ip slb stats** command displays detailed information about the Cisco IOS SLB network status:

```
Router-SLB# show ip slb stats
Pkts via normal switching:     0
Pkts via special switching:    0
Pkts via slb routing:          0
Pkts Dropped:                  0
Connections Created:           0
Connections Established:       0
Connections Destroyed:         0
Connections Reassigned:        0
Zombie Count:                  0
Connections Reused:            0
Connection Flowcache Purges:   0
Failed Connection Allocs:      0
Failed Real Assignments:       0
RADIUS framed-ip Sticky Count:0
RADIUS username Sticky Count:  0
```

See the "Monitoring and Maintaining the Cisco IOS SLB Feature" section on page 14-25 for additional commands used to verify Cisco IOS SLB networks and connections.

Configuring the GGSN for GTP Load Balancing

To configure GTP load balancing on the GGSN, complete the tasks in the following sections:

- Configuring a Loopback Interface for GTP SLB, page 14-19 (Required if using dispatched mode without GTP cause code inspection enabled)
- Configuring DFP Support on the GGSN, page 14-20 (Optional, but recommended)

Configuring a Loopback Interface for GTP SLB

To enable GTP load balancing, a loopback interface must be configured with the same IP address as the virtual server on the Cisco IOS SLB on each GGSN in a farm.

To create a loopback interface, use the following commands, beginning in global configuration mode:

	Command	Description
Step 1	`Router-GGSN(config)# interface loopback` *number*	Creates a loopback interface. A loopback interface is a virtual interface that is always up.
Step 2	`Router-GGSN(config-if)# ip address` *ip-address mask*	Assigns an IP address to the loopback interface.

Configuring DFP Support on the GGSN

To configure DFP support for GTP SLB, you must complete the following tasks:

- Configuring the GGSN as a DFP Agent, page 14-20
- Configuring the DFP Weight for a GGSN, page 14-20
- Configuring the Maximum Number of PDP Contexts for a GGSN, page 14-21

Configuring the GGSN as a DFP Agent

For complete information on configuring a DFP agent, see *DFP Agent Subsystem* feature module.

To define the port number for the DFP manager (the Cisco IOS SLB in this instance) to use to connect to the DFP agent, enter the following commands in order, beginning in global configuration mode:

	Command	Description
Step 1	`Router-GGSN(config)# ip dfp agent gprs`	Identifies a DFP agent subsystem and initiates DFP agent configuration mode.
Step 2	`Router-GGSN(config-dfp)# interval seconds`	(Optional) Configures a DFP agent weight recalculation interval.
Step 3	`Router-GGSN(config-dfp)# password [0|7] password [timeout]`	Optional) Configures a DFP agent password for MD5 authentication.
Step 4	`Router-GGSN(config-dfp)# port port-number`	Defines the port number for the DFP manager to use to connect to the DFP agent.
Step 5	`Router-GGSN(config-dfp)# inservice`	Enables the DFP agent for communication with a DFP manager. A DFP agent is inactive until both of the following conditions are met: • The DFP agent is enabled using the inservice (DFP agent) command. • The client subsystem has changed the DFP agent's state to ACTIVE.

Configuring the DFP Weight for a GGSN

If you use DFP with GTP load balancing, each GGSN that acts as a DFP agent has a maximum weight that it can send to a DFP manager. For each GGSN, you can accept the default maximum weight (85%), or you can specify a different maximum weight. You can also configure the percentage of utilization at which the CPU and memory loads are included in the weight calculation using the **cpu-load** and **mem-load** keyword options.

To specify the maximum weight for a GGSN, use the following command in global configuration mode on the GGSN:

Command	Purpose
`Router-GGSN(config)# gprs dfp {max-weight max-weight | min-cpu-load min-cpu-load | mem-load min-mem-load}`	Specifies DFP weight parameters of a GGSN that is acting as a DFP agent, where: • **max-weight**—Specifies the maximum weight sent by the GGSN, acting as a DFP agent, to a DFP manager. The valid range is 1 to 100. The default is 8. • **min-cpu-load**—Specifies the minimum percentage at which to start including the CPU load in the DFP weight calculation. The valid range is 10 to 75 percent. • **mem-load**—Specifies the minimum percentage at which to start including the memory load in the DFP weight calculation. The valid range is 10 to 75 percent

Configuring the Maximum Number of PDP Contexts for a GGSN

If you use DFP with GTP load balancing, you must specify a maximum number of PDP contexts for each GGSN, using the **gprs maximum-pdp-context-allowed** command. *Do not* accept the default value of 10000 PDP contexts. Significantly lower values, including the default value of 10,000, can impact capacity in a GPRS/UMTS load-balancing environment.

Note DFP weighs PPP PDPs against IP PDPs, with one PPP PDP equal to 8 IPv4 PDPs. One IPv6 PDP counts as four IPv4 PDPs. Therefore, when using DFP, be aware that the configured maximum number of PDP contexts affects the GGSN weight. The lower the maximum number of PDP contexts, the lower the weight, when all other parameters remain the same.

To configure a maximum number of PDP contexts for a GGSN, use the following command in global configuration mode on the GGSN:

Command	Purpose
`Router-GGSN(config)# gprs maximum-pdp-context-allowed [pdp-contexts]`	Specifies the maximum number of PDP contexts (mobile sessions) that can be activated on the GGSN.

Configuring Messaging from the GGSN to the Cisco IOS SLB

The GGSN-IOS SLB messaging feature enables you to configure the GGSN to notify the Cisco IOS SLB when a certain condition exists that affects a session forwarded by the Cisco IOS SLB. The notification also instructs the Cisco IOS SLB on how to react to the condition.

There are two types of GGSN-IOS SLB notifications that can be configured using the **gprs slb notify** command—CAC failure notifications and delete notifications (for GTP IMSI sticky database support). The following sections describe how to configure each of them:

- Configuring Support for GGSN-IOS SLB Messaging CAC Failure Notifications, page 14-22
- Configuring Support for GGSN-IOS SLB Messaging Delete Notifications (GTP IMSI Sticky Database Support), page 14-23

Configuring Support for GGSN-IOS SLB Messaging CAC Failure Notifications

The GGSN can be configured to notify the Cisco IOS SLB when a UMTS QoS CAC failure has caused a Create PDP Context request to be rejected.

CAC failure notifications sent by the GGSN include the following information elements (IEs):

- Type—Notification type (reassign).
- Session identifier—Session key on the Cisco IOS SLB that identifies the session to which a notification belongs.
- Create response—Create response that the GGSN would send to the SGSN when a failure occurred. If there is not an alternate GGSN available to which to reassign the session, or if the maximum number of reassign attempts is exceeded, the Cisco IOS SLB relays this information to the SGSN.

The way you configure support for CAC failure notifications depends on whether the Cisco IOS SLB is operating in dispatched mode or directed server NAT mode. For information on each procedure, see the following sections:

- Configuring CAC Failure Notification Support when the Cisco IOS SLB is in Dispatched Mode, page 14-22
- Configuring CAC Failure Notification Support when the Cisco IOS SLB is in Directed Server NAT Mode, page 14-23

Configuring CAC Failure Notification Support when the Cisco IOS SLB is in Dispatched Mode

If the Cisco IOS SLB is functioning in dispatched mode, the virtual server that forwarded the Create PDP Context request to the GGSN is known to the GGSN, and the GGSN can send CAC failure notifications directly to the server.

To configure the GGSN to send CAC failure notifications to the Cisco IOS SLB when the Cisco IOS SLB is in dispatched mode, use the following command in global configuration mode:

	Command	Description
Step 1	`Router-GGSN(config)# gprs slb mode dispatched`	Defines dispatched as the Cisco IOS SLB operation mode for GGSN-IOS SLB messaging. **Note** The default is dispatched mode.
Step 2	`Router-GGSN(config)# gprs slb notify cac-failure`	Enables the GGSN to notify the Cisco IOS SLB when a UMTS QoS CAC failure has caused a Create PDP Context request to be rejected.

To enable CAC failure notification support on the Cisco IOS SLB, use the following command in virtual server mode:

Command	Purpose
`Router-SLB(config-slb-vserver)# gtp notification cac` *count*	Enables support of GGSN-IOS SLB messaging CAC failure notifications and configures the maximum number of times a rejected Create PDP Context can be reassigned to a new real GGSN. The default is 2 (which is 3 real selections per session, including the initial send).

Configuring CAC Failure Notification Support when the Cisco IOS SLB is in Directed Server NAT Mode

If the Cisco IOS SLB is functioning in directed server NAT mode, the virtual server is not known to the GGSN. Therefore, in addition to configuring the GGSN to send CAC failure notifications to the Cisco IOS SLB, a list of virtual servers must be defined on the GGSN using the **gprs slb vserver** command in global configuration mode, and the Cisco IOS SLB mode of operation must be defined using the **gprs slb mode** command in global configuration mode.

Note If the Cisco IOS SLB operation mode and virtual servers are not defined on the GGSN when the Cisco IOS SLB is functioning in directed server NAT mode, support for CAC failure notification is not enabled, even if the **gprs slb notify cac-failure** and **gtp notification cac** commands are configured.

To enable the GGSN to send CAC failure notifications to the Cisco IOS SLB when the Cisco IOS SLB is in directed server NAT mode, use the following commands in global configuration mode:

	Command	Description
Step 1	`Router-GGSN(config)# gprs slb mode directed`	Defines directed server NAT as the Cisco IOS SLB operation mode for GGSN-IOS SLB messaging. **Note** The default is dispatched mode.
Step 2	`Router-GGSN(config)# gprs slb notify cac-failure`	Enables the GGSN to notify the Cisco IOS SLB when a UMTS QoS CAC failure has caused a Create PDP Context request to be rejected.
Step 3	`Router-GGSN(config)# gprs slb vserver` *ip_address* `[next-hop ip` *ip-address* `[vrf` *name*`]]`	Configures the Cisco IOS SLB virtual server(s) to be notified by a GGSN when the condition defined using the **gprs slb notify** command occurs. Optionally, also configures the IP address of the next-hop that can be used to reach the virtual server and specifies the VPN routing and forwarding instance.

To enable CAC failure notification support on the Cisco IOS SLB, use the following command in virtual server mode:

Command	Purpose
`Router-SLB(config-slb-vserver)# gtp notification cac` *count*	Enables support of GGSN-IOS SLB messaging CAC failure notifications and configures the maximum number of times a rejected Create PDP Context can be reassigned to a new real GGSN. The default is 2 (including the initial send, 3 real selections per session).

Configuring Support for GGSN-IOS SLB Messaging Delete Notifications (GTP IMSI Sticky Database Support)

When support for delete notifications is configured on the GGSN and the Cisco IOS SLB, a sticky database entry is created on the Cisco IOS SLB when the first Create PDP Context request from a subscriber is received. When the last PDP context of that IMSI is deleted on the GGSN, the GGSN sends a delete notification to the Cisco IOS SLB that instructs the Cisco IOS SLB to remove the sticky entry from the database.

Note This configuration requires that the **virtual** virtual server configuration command be configured with the **service gtp** keywords specified.

Note If the **sticky gtp imsi** command is configured under multiple vservers, the group number configuration facilitate sharing of the sticky object in the event the same MS connects through different vservers. All vservers that have the same sticky group number share the sticky IMSI entry for a user.

To configure the GGSN to send a delete notification to the Cisco IOS SLB when the last PDP context of an IMSI is deleted on the GGSN, use the following commands in global configuration mode:

	Command	Description
Step 1	`Router-GGSN(config)# gprs slb mode {dispatched | directed}`	Defines the Cisco IOS SLB operation mode for GGSN-IOS SLB messaging. The default is dispatched mode.
Step 2	`Router-GGSN(config)# gprs slb notify session-deletion`	Configures the GGSN to send a delete notification message to the Cisco IOS SLB when the last PDP context associated with an IMSI is deleted.
Step 3	`Router-GGSN(config)# gprs slb vservers ip_address [next-hop ip ip-address [vrf name]]`	Configures the Cisco IOS SLB virtual server(s) to be notified by a GGSN when the condition defined using the **gprs slb notify** command occurs. Optionally, also configures the IP address of the next-hop that can be used to reach the virtual server and specifies the VPN routing and forwarding instance.

To configure GTP IMSI sticky database support on the Cisco IOS SLB, use the following command in virtual server configuration mode:

Command	Purpose
`Router-SLB(config-slb-vserver)# sticky gtp imsi [group number]`	Enables Cisco IOS SLB to load-balance GTP Create PDP Context requests to the same real server that processed all previous create requests for a given IMSI.

Monitoring and Maintaining the Cisco IOS SLB Feature

To clear, obtain, and display GTP SLB information on the GGSN, use the following commands in privileged EXEC mode:

Command	Purpose
`Router-GGSN# clear gprs slb statistics`	Clears Cisco IOS SLB statistics.
`Router-GGSN# show gprs slb detail`	Displays all Cisco IOS SLB-related information, such as operation mode, virtual server addresses for GGSN-IOS SLB messaging, SLB notifications, and statistics.
`Router-GGSN# show gprs slb mode`	Displays the Cisco IOS SLB mode of operation.
`Router-GGSN# show gprs slb statistics`	Displays Cisco IOS SLB statistics.
`Router-GGSN# show gprs slb vservers`	Displays a list of defined Cisco IOS SLB virtual servers for GGSN-IOS SLB messaging.

To obtain and display information about the GTP SLB on the Cisco IOS SLB, use the following commands in privileged EXEC mode on the Cisco IOS SLB:

Command	Purpose
`Router-SLB# show ip slb conns [vserver virtual_server-name | client ip-address | firewall firewallfarm-name] [detail]`	Displays all connections handled by Cisco IOS SLB, or, optionally, only the connections associated with a particular virtual server or client.
`Router-SLB# show ip slb dfp [agent agent_ip_address port-number | manager manager_ip_address | detail | weights]`	Displays information about DFP and DFP agents, and about the weights assigned to real servers.
`Router-SLB# show ip slb gtp {gsn [gsn-ip-address] | nsapi [nsapi-key] [detail]`	Displays Cisco IOS SLB GTP information when GTP load balancing with cause code inspection is enabled.
`Router-SLB# show ip slb map [id]`	Displays information about Cisco IOS SLB protocol maps.
`Router-SLB# show ip slb reals [sfarm server-farm] [detail]`	Displays information about the real servers defined to Cisco IOS SLB.
`Router-SLB# show ip slb replicate`	Displays information about the Cisco IOS SLB replication configuration.
`Router-SLB# show ip slb serverfarms [name serverfarm-name] [detail]`	Displays information about the server farms defined to Cisco IOS SLB.
`Router-SLB show ip slb sessions [gtp | gtp-inspect | radius] [vserver virtual-server] [client ip-addr netmask] [detail]`	Displays information about sessions handled by Cisco IOS SLB. **Note** With GTP load balancing *without* cause code inspection, a session lasts no longer than the duration of the virtual server GTP idler time specified using the **idle gtp request command**.

Command	Purpose
`Router=SLB# show ip slb stats`	Displays Cisco IOS SLB statistics.
`Router-SLB# show ip slb sticky gtp imsi [id imsi]`	Displays only entries of the Cisco IOS SLB sticky database associated with the Cisco IOS SLB GTP IMSI sticky database, and shows all of the Network Service Access Point Identifiers (NSAPIs) that the user has used as primary PDPs. Optionally, displays only those sticky database entries associated with the specified IMSI.
`Router-SLB# show ip slb vserver [name virtual_server] [redirect] [detail]`	Displays information about the virtual servers defined to Cisco IOS SLB.

Configuration Examples

This section provides an example of the GGSN Cisco IOS SLB examples. For complete descriptions of the GGSN commands in this section, see *Cisco GGSN Release Command Reference*. For complete descriptions of the Cisco IOS SLB commands in this section, see the *IOS Server Load Balancing* feature module documentation.

This section includes examples of Cisco IOS SLB with GTP load balancing and NAT configured on the Cisco 7600 platform:

- Cisco IOS SLB Configuration Example, page 14-26
- GGSN1 Configuration Example, page 14-28

Cisco IOS SLB Configuration Example

```
hostname 7600-a
!
ip slb probe PINGPROBE ping
 interval 3
 faildetect 3
!
ip slb serverfarm SAMI1
 nat server
 probe PINGPROBE
!
 real 9.9.9.72
  reassign 4
  faildetect numconns 255 numclients 8
  inservice
!
 real 9.9.9.73
  reassign 4
  faildetect numconns 255 numclients 8
  inservice
!
 real 9.9.9.74
  reassign 4
  faildetect numconns 255 numclients 8
  inservice
!
 real 9.9.9.75
  reassign 4
```

```
  faildetect numconns 255 numclients 8
  inservice
!
 real 9.9.9.76
  reassign 4
  faildetect numconns 255 numclients 8
  inservice
!
ip slb vserver V0-GGSN
 virtual 10.10.10.10 udp 3386 service gtp
 serverfarm SAMI1
 idle gtp request 100
 inservice
!
ip slb vserver V1-GGSN
 virtual 10.10.10.10 udp 2123 service gtp
 serverfarm SAMI1
 idle gtp request 100
 inservice
!
ip slb dfp password ciscodfp 0
 agent 9.9.9.72 1111 30 0 10
 agent 9.9.9.73 1111 30 0 10
 agent 9.9.9.74 1111 30 0 10
 agent 9.9.9.75 1111 30 0 10
 agent 9.9.9.76 1111 30 0 10
!
interface FastEthernet9/36
 description TO SGSN
 no ip address
 switchport
 switchport access vlan 302
!
interface Vlan101
 description Vlan to GGSN for GN
 ip address 10.1.1.1 255.255.255.0
!
interface Vlan302
 ip address 40.0.2.1 255.255.255.0
!
router ospf 300
 log-adjacency-changes
 summary-address 9.9.9.0 255.255.255.0
 redistribute static subnets route-map GGSN-routes
 network 40.0.2.0 0.0.0.255 area 300
 network 40.0.3.0 0.0.0.255 area 300
!
ip route 9.9.9.72 255.255.255.255 10.1.1.72
ip route 9.9.9.73 255.255.255.255 10.1.1.73
ip route 9.9.9.74 255.255.255.255 10.1.1.74
ip route 9.9.9.75 255.255.255.255 10.1.1.75
ip route 9.9.9.76 255.255.255.255 10.1.1.76
!
access-list 1 permit 9.9.9.0 0.0.0.255
!
route-map GGSN-routes permit 10
 match ip address 1
!
!
```

GGSN1 Configuration Example

```
!
ip dfp agent gprs
 port 1111
 password ciscodfp 0
 inservice
!
interface Loopback100
 description GPRS GTP V-TEMPLATE IP ADDRESS
 ip address 9.9.9.72 255.255.255.0
!
interface GigabitEthernet0/0.2
 description Gn Interface
 encapsulation dot1Q 101
 ip address 10.1.1.72 255.255.255.0
 no cdp enable
!
interface Virtual-Template1
 description GTP v-access
 ip unnumbered Loopback100
 encapsulation gtp
 gprs access-point-list gprs
!
! route to SGSNs
ip route 40.1.2.1 255.255.255.255 10.1.1.1
ip route 40.2.2.1 255.255.255.255 10.1.1.1
```

CHAPTER A

Monitoring Notifications

This appendix describes enabling and monitoring Gateway GPRS Support Node (GGSN) SNMP notifications in order to manage GPRS/UMTS-related issues. SNMP uses notifications to report events on a managed device. The notifications are traps or informs for different events.

Note This appendix covers enabling and monitoring GGSN SNMP notifications only. Additional types of SNMP notifications can be enabled on your Cisco router. For more information about the types of SNMP notifications you can enable, see *Cisco IOS Configuration Fundamentals*, Release 12.4 documentation.

In addition, to display a list of notifications available on your Cisco router, enter the **snmp-server enable traps ?** command.

This appendix contains the following sections:

- SNMP Overview, page A-1
- Configuring MIB Support, page A-6
- Enabling SNMP Support, page A-9
- Enabling and Disabling SNMP Notifications, page A-9
- GGSN Notifications, page A-11

SNMP Overview

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a standardized framework and a common language used for monitoring and managing devices in a network.

The SNMP framework has three parts:

- SNMP manager—A system used to control and monitor the activities of network hosts using SNMP. The most common managing system is called a Network Management System (NMS). The term NMS can be applied to either a dedicated device used for network management, or the applications used on a network-management device. A variety of network management applications are available for use with SNMP. These features range from simple command-line applications to feature-rich graphical user interfaces (such as the CiscoWorks2000 line of products).

- SNMP agent—A software component in a managed device that maintains the data for the device and reports the data, as needed, to managing systems. The agent and MIB reside on the routing device (router, access server, or switch). To enable the SNMP agent on a managed device, you must define the relationship between the manager and the agent (see the "Enabling SNMP Support" section on page A-9).
- Management Information Base (MIB)—Collection of network-management information, organized hierarchically.

Instead of defining a large set of commands, SNMP places all operations in a get-request, get-next-request, and set-request format. For example, an SNMP manager can get a value from an SNMP agent or set a value in that SNMP agent.

MIB Description

A Management Information Base (MIB) is a collection of network-management information, organized hierarchically. The MIB consists of collections of managed objects identified by object identifiers. MIBs are accessed using a network-management protocol such as SNMP. A managed object (sometimes called a MIB object or an object) is one of a number of characteristics of a managed device, such as a router. Managed objects comprise one or more object instances, which are essentially variables. The Cisco implementation of SNMP uses the definitions of MIB II variables described in RFC 1213.

MIBs can contain two types of managed objects:

- Scalar objects—Define a single object instance (for example, ifNumber in the IF-MIB and bgpVersion in the BGP4-MIB).
- Columnar objects—Defines a MIB table that contains no rows or more than one row, and each row can contain one or more scalar objects, (for example, ifTable in the IF-MIB defines the interface).

System MIB variables are accessible through SNMP as follows:

- Accessing a MIB variable—Function is initiated by the SNMP agent in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- Setting a MIB variable—Function is initiated by the SNMP agent in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

SNMP Notifications

An SNMP agent can notify the manager when important system events occur, such as the following:

- An interface or card starts or stops running
- Temperature thresholds are crossed
- Authentication failures occur

When an agent detects an alarm condition, the agent:

- Logs information about the time, type, and severity of the condition
- Generates a notification message, which it then sends to a designated IP host

SNMP notifications are sent as either:

- Traps—Unreliable messages, which do not require receipt acknowledgment from the SNMP manager.
- Informs—Reliable messages, which are stored in memory until the SNMP manager issues a response. Informs use more system resources than traps.

Note Many commands use the word traps in the command syntax. Unless there is an option in the command to select either traps or informs, the keyword traps refers to either traps, informs, or both. Use the **snmp-server host** command to specify whether to send SNMP notifications as traps or informs.

When an agent detects an alarm condition, it logs information about the time, type, and severity of the condition and generates a notification message, which it then sends to a designated IP host.

SNMP notifications can be sent as either *traps* or *informs*. See the "Enabling SNMP Support" section on page A-9 for instructions on how to enable traps on the GGSN. See the "GGSN Notifications" section on page A-11 for information about GGSN traps.

The Cisco implementation of SNMP uses the definitions of SNMP traps described in RFC 1215.

SNMP Versions

Cisco IOS software supports the following versions of SNMP:

- SNMPv1—The Simple Network Management Protocol: An Internet standard, defined in RFC 1157. Security is based on community strings.
- SNMPv2c—The community-string based administrative framework for SNMPv2. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 classic), and uses the community-based security model of SNMPv1.
- SNMPv3—Version 3 of SNMP. SNMPv3 uses the following security features to provide secure access to devices:
  - Message integrity—Ensuring that a packet has not been tampered with in transit.
  - Authentication—Determining that the message is from a valid source.
  - Encryption—Scrambling the contents of a packet to prevent it from being learned by an unauthorized source.

SNMPv1 and SNMPv2c

Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers who are able to access the agent MIB is defined by an IP address Access Control List and password.

SNMPv2c support includes a bulk-retrieval mechanism and more detailed error message reporting to management stations. The bulk-retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trip transmissions required. SNMPv2c improved error handling support includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes now report the error type. Three kinds of exceptions are also reported:

- no such object exceptions
- no such instance exceptions
- end of MIB view exceptions

SNMPv3

SNMPv3 provides the following security models and security levels:

- Security model—Authentication strategy that is set up for a user and the group in which the user resides.
- Security level—Permitted level of security within a security model.

A combination of a security model and a security level determines the security mechanism to be employed when handling an SNMP packet.

SNMP Security Models and Levels

Table 1-1 describes the security models and levels provided by the different SNMP versions.

Table 1-1 SNMP Security Models and Levels

Model	Level	Authentication	Encryption	Description
v1	noAuthNoPriv	Community string	No	Uses match on community string for authentication.
v2c	noAuthNoPriv	Community string	No	Uses match on community string for authentication.
v3	noAuthNoPriv	User name	No	Uses match on user name for authentication.
v3	authNoPriv	MD5 or SHA	No	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithm.
v3	authPriv	MD5 or SHA	DES	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithm. Also provides DES 56-bit encryption based on CBC-DES (DES-56) standard.

You must configure the SNMP agent to use the version of SNMP supported by the management station. An agent can communicate with multiple managers; for this reason, you can configure the Cisco IOS software to support communications with one management station using the SNMPv1 protocol, one using the SNMPv2c protocol, and another using SMNPv3.

Requests for Comments

MIB modules are written in the SNMP MIB module language, and are typically defined in Request For Comments (RFC) documents submitted to the Internet Engineering Task Force (IETF). RFCs are written by individuals or groups for consideration by the Internet Society and the Internet community as a whole. Before being given RFC status, recommendations are published as Internet Draft (I-D) documents. RFCs that have become recommended standards are also labeled as standards (STD) documents. For more information, see the Internet Society and IETF websites (http://www.isoc.org and http://www.ietf.org).

We provide private MIB extensions with each Cisco system. Cisco enterprise MIBs comply with the guidelines described in the relevant RFCs unless otherwise noted in the documentation.

Object Identifiers

An object identifier (OID) uniquely identifies a MIB object on a managed network device. The OID identifies the MIB object's location in the MIB hierarchy, and provides a means of accessing the MIB object in a network of managed devices:

- Standard RFC MIB OIDs are assigned by the Internet Assigned Numbers Authority (IANA)
- Enterprise MIB OIDs are assigned by Cisco Assigned Numbers Authority (CANA).

Each number in the OID corresponds to a level of MIB hierarchy. For example, the OID 1.3.6.1.4.1.9.9.xyz represents the *xyz*-MIB whose location in the MIB hierarchy is as follows. The numbers in parentheses are included only to help show correspondence to the MIB hierarchy. In actual use, OIDs are represented as numerical values only.

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).cisco(9).ciscoMgt(9).*nn*-MIB

You can uniquely identify a managed object, such as ifNumber in the IF-MIB, by its object name (iso.org.dod.internet.mgmt.enterprises.interfaces.ifNumber) or by its OID (1.3.6.1.2.1.2.1).

For a list of OIDs assigned to MIB objects, go to the following URL:

ftp://ftp.cisco.com/pub/mibs/oid/

Related Information and Useful Links

The following URL provides access to general information about Cisco MIBs. Use the links on this page to access MIBs for download, and to access related information (such as application notes and OID listings).

- http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

TAC Information and FAQs

The following URLs provide access to SNMP information developed by the Cisco Technical Assistance Center (TAC):

- http://www.cisco.com/warp/public/477/SNMP/index.html is the Cisco TAC page for SNMP. It provides links to general SNMP information and tips for using SNMP to gather data.
- http://www.cisco.com/warp/public/477/SNMP/mibs_9226.shtml is a list of frequently asked questions (FAQs) about Cisco MIBs.

SNMP Configuration Information

The following URLs provide information about configuring SNMP:

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_c/fcprt3/fcmonitr.htm provides general information about configuring SNMP support. It is part of the *Cisco IOS Configuration Fundamentals Configuration Guide*.
- http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_r/frprt3/frmonitr.htm provides information about SNMP commands. It is part of the *Cisco IOS Configuration Fundamentals Command Reference*.

Configuring MIB Support

This chapter describes how to configure SNMP and MIB support on a Cisco router. It includes the following sections:

- Determining MIBs Included for Cisco IOS Releases, page A-6
- Downloading and Compiling MIBs, page A-7
- Enabling SNMP Support, page A-9

Determining MIBs Included for Cisco IOS Releases

Follow these steps to determine which MIBs are included in the Cisco IOS release you are using:

Step 1 Go to the Feature Navigator home page http://tools.cisco.com/ITDIT/MIBS/servlet/index.

Step 2 Click **MIB Locator** to launch the application. The MIB Locator application allows you to find a MIB in the following three ways:

a. By release, platform family, and feature set—From the MIB Locator page:

- Click the drop-down menu and select the desired Cisco IOS software release.
- From the Platform Family menu, select **7600-SAMI**. If you select the platform first, the system displays only those releases and feature sets that apply to the platform you have selected.
- From the Feature Set menu, select the appropriate GGSN release.

b. By image name—From the MIB Locator page, enter the GGSN image name you are using into the Search by Image Name field and click **Submit**: (the following image name is an example):

```
c6svcsami-g8is-mz.124-15.XQ.bin
```

c. By MIB name—From the MIB Locator page, search for the MIB from the list of MIBs in the Search for a MIB menu. You can select one, or for a multiple selection, hold down the **CTRL** key, then click **Submit**.

Note After you make a selection, follow the links and instructions.

Downloading and Compiling MIBs

The following sections provide information about how to download and compile MIBs for the GGSN:

- Considerations for Working with MIBs
- Downloading MIBs
- Compiling MIBs

Considerations for Working with MIBs

While working with MIBs, consider the following:

Mismatches on Datatype Definitions

- Mismatches on datatype definitions might cause compiler errors or warning messages. Although Cisco MIB datatype definitions are not mismatched, standard RFC MIBs do mismatch. For example:

```
MIB A defines: SomeDatatype ::= INTEGER(0..100)
MIB B defines: SomeDatatype ::= INTEGER(1..50)
```

  This example is considered to be a trivial error and the MIB loads successfully with a warning message.

  The next example is considered a nontrivial error (even though the two definitions are essentially equivalent), and the MIB is not successfully parsed.

```
MIB A defines: SomeDatatype ::= DisplayString
MIB B defines: SomeDatatype ::= OCTET STRING (SIZE(0..255))
```

  If your MIB compiler treats these as errors, or you want to delete the warning messages, edit one of the MIBs that define this same datatype so that the definitions match.

- Many MIBs import definitions from other MIBs. If your management application requires MIBs to be loaded, and you experience problems with undefined objects, you might want to load the following MIBs in this order:

  SNMPv2-SMI.my
  SNMPv2-TC.my
  SNMPv2-MIB.my
  RFC1213-MIB.my
  IF-MIB.my

CISCO-SMI.my
CISCO-PRODUCTS-MIB.my
CISCO-TC.my

- For additional information and SNMP technical tips, from the Locator page, click **SNMP MIB Technical Tips** and follow the links or go to the following URL:

  http://www.cisco.com/pcgi-bin/Support/browse/psp_view.pl?p=Internetworking:SNMP&s=Implementation_and_Configuration#Samples_and_Tips

- For a list of SNMP object identifiers (OIDs) assigned to MIB objects, go to the following URL and click on **SNMP Object Navigator** and follow the links:

  http://tools.cisco.com/ITDIT/MIBS/servlet/index

Note You must have a Cisco CCO name and password to access the MIB Locator.

- For information about how to download and compile Cisco MIBs, go to the following URL:

  http://www.cisco.com/warp/public/477/SNMP/mibcompilers.html

Downloading MIBs

Follow these steps to download the MIBs onto your system if they are not already there:

Step 1 Review the considerations in the previous section ("Considerations for Working with MIBs").

Step 2 Go to one of the following Cisco URLs. If the MIB you want to download is not there, try the other URL; otherwise, go to one of the URLs in Step 5.

ftp://ftp.cisco.com/pub/mibs/v2
ftp://ftp.cisco.com/pub/mibs/v1

Step 3 Click the link for a MIB to download that MIB to your system.

Step 4 Select **File > Save** or **File > Save As** to save the MIB on your system.

Step 5 You can download industry-standard MIBs from the following URLs:

- http://www.ietf.org
- http://www.atmforum.com

Compiling MIBs

If you plan to integrate the Cisco router with an SNMP-based management application, then you must also compile the MIBs for that platform. For example, if you are running HP OpenView on a UNIX operating system, you must compile platform MIBs with the HP OpenView Network Management System (NMS). For instructions, see the NMS documentation.

Enabling SNMP Support

The following procedure summarizes how to configure the Cisco router for SNMP support.

For detailed information about SNMP commands, see the following Cisco documents:

- *Cisco IOS Release 12.3 Configuration Fundamentals Configuration Guide*, "Monitoring the Router and Network" section, available at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/index.htm

- *Cisco IOS Release 12.3 Configuration Fundamentals Command Reference*, Part 3: System Management Commands, "Router and Network Configuration Commands" section, available at the the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_r/index.htm

To configure the Cisco router for SNMP support, follow these steps:

Step 1 Set up your basic SNMP configuration through the command line interface (CLI) on the router. These basic configuration commands are issued for SNMPv2c. For SNMPv3, you must also set up SNMP users and groups. (See the preceding list of documents for command and setup information.)

a. Define SNMP read-only and read-write communities:

```
Router (config)# snmp-server community Read_Only_Community_Name ro
Router (config)# snmp-server community Read_Write_Community_Name rw
```

b. Configure SNMP views (to limit the range of objects accessible to different SNMP user groups):

```
Router (config)# snmp-server view view_name oid-tree {included | excluded}
```

Enabling and Disabling SNMP Notifications

To enable and disable SNMP Notifications, perform the tasks in the following sections:

- Enabling and Disabling GGSN Notifications via the CLI, page A-9
- Enabling and Disabling GGSN SNMP Notifications via SNMP, page A-10
- Enabling and Disabling GGSN SNMP Notifications via SNMP, page A-10

Enabling and Disabling GGSN Notifications via the CLI

To use the command line interface (CLI) to enable the Cisco router to send GGSN SNMP notifications (traps or informs), perform the following steps.

Step 1 Make sure SNMP is configured on the router (see the "Enabling SNMP Support" section on page A-9).

Step 2 Identify (by IP address) the host to receive traps from the Cisco router:

```
Router(config)#snmp-server host host-address version SNMP version community/user(V3)
udp-port <UDP port No>
```

Step 3 Enable GGSN SNMP notifications on the Cisco router using the following command (enter a separate command for each type of notification you want to enable):

```
Router(config)#snmp-server enable traps gprs [apn | charging | ggsn | ggsn-apn |
ggsn-general | ggsn-memory | ggsn-pdp | ggsn-service | gtp | csg | dcca]
```

Where:

- **apn—**Enables APN notifications.
- **charging—**Enables charging notifications.
- **ggsn**—Enables GGSN global notifications.

Note To prevent flooding, configuring the **snmp-server enable traps gprs ggsn** command enables all GGSN-related traps except for the cGgsnGlobalErrorNotif, cGgsnAccessPointNameNotif, and the cGgsnPacketDataProtocolNotif traps.

- **ggsn-apn—**—Enables GGSN notifications specific to APN (cGgsnAccessPointNameNotif).
- **ggsn-general**—Enables GGSN general notifications (cGgsnGlobalErrorNotif).
- **ggsn-pdp**—Enables GGSN notifications specific to PDP (cGgsnPacketDataProtocolNotif).
- **ggsn-service**—Enables GGSN service-mode notifications.
- **gtp**—Enables GTP traps.
- **csg**—Enables GGSN CSG-specific notifications.
- **dcca**—Enables GGSN DCCA-specific notifications.

Note Issuing the **snmp-server enable traps gprs** command without a keyword option enables all GGSN SNMP notifications.

Step 4 To disable GGSN SNMP notifications on the Cisco router, enter the following command.

```
Router(config)# no snmp-server enable traps gprs
```

If you omit the notification type keyword (**gprs** in this example), all notifications are disabled.

Note We recommend that the **snmp-server enable traps gtp** command not be configured because all associated MIBs are deprecated.

Enabling and Disabling GGSN SNMP Notifications via SNMP

In addition, GGSN SNMP Notifications can be enabled or disabled by setting the following objects to true(1) or false(2).

- cGgsnServiceNotifEnabled—Enables/disables GGSN service-mode notifications.
- cGgsnMemoryNotifEnabled—Enables/disable memory related notifications
- cGgsnGlobalErrorNotifEnabled—Enables GGSN general notifications

- cGgsnAccessPointNotifEnabled—Enables/disables cGgsnAccessPointNameNotif notification
- cGgsnPdpNotifEnabled—Enables/disables cGgsnPacketDataProtocolNotif notification
- cGgsnSACsgNotifEnabled— Enables/disables CSG state traps.
- cGgsnSADccaNotifEnabled—Enables/disables DCCA-related notifications

GGSN Notifications

This section lists and briefly describes the notifications supported by GGSN MIBs and generated by the GGSN.

This section lists the following types of notifications:

- Global Notifications, page A-12
- Charging Notifications, page A-15
- Access-Point Notifications, page A-16
- Alarm Notifications, page A-17

Global Notifications

Table A-2 lists the global notifications supported by the CISCO-GGSN-MIB. To enable these notifications to be sent, use the **snmp-server enable traps gprs** command in global configuration mode, with the **ggsn**, **ggsn-apn**, **ggsn-memory**, **ggsn-pdp**, **ggsn-service**, **csg** and/or **dcca** keyword option specified.

Note Issue a separate command for each keyword option.

Note cGgsnNotification (1.2.6.1.4.1.9.9.240.2.0.1) is deprecated.

Table A-2 Global Notifications

Notification and Notification Objects	Notes
cGgsnInServiceNotif (1.3.6.1.4.1.9.9.240.2.0.2)	Sent when the GGSN is placed in operational (inService) mode. The GGSN is placed in operational mode using the **gprs service-mode operational** command in global configuration mode or by setting the cGgsnServiceMode object to inService(1). The service mode is identified by cGgsnServiceModeStatus. Enable the generation of this notification by setting cGgsnServiceNotifEnabled to true(1).
cGgsnMaintenanceNotif (1.3.6.1.4.1.9.9.240.2.0.3)	Sent when the GGSN is placed is maintenance mode. The GGSN is placed in maintenance mode using the **gprs service-mode maintenance** command in global configuration mode or by setting the cGgsnServiceMode object to maintenance(2). The service mode is identified by cGgsnServiceModeStatus. Enable the generation of this notification by setting cGgsnServiceNotifEnabled to true(1).
cGgsnMemThresholdReachedNotif (1.3.6.1.4.1.9.9.240.2.0.4)	Sent when the GGSN memory threshold is reached. The memory threshold is set using the **gprs memory threshold** command in global configuration mode or by setting cGgsnMemoryThreshold. Enable the generation of this notification by setting cGgsnMemoryNotifEnabled to true(1).
cGgsnMemThresholdClearedNotif (1.3.6.1.4.1.9.9.240.2.0.5)	Sent when the GGSN retains the memory and falls below the configured threshold. The memory threshold is set using the **gprs memory threshold** command in global configuration mode or by setting cGgsnMemoryThreshold. Enable the generation of this notification by setting cGgsnMemoryNotifEnabled to true(1).

Table A-2 Global Notifications (continued)

Notification and Notification Objects	Notes
cGgsnGlobalErrorNotif (1.3.6.1.4.1.9.9.240.2.0.8) cGgsnGlobalErrorTypes cGgsnHistNotifSeverity cGgsnHistNotifTimestamp cGgsnHistNotifGgsnIpAddrType cGgsnHistNotifGgsnIpAddr cGgsnHistNotifInfo	Sent when a GGSN-related alarm has occurred. If additional information is available for specific types of alarms, that information might be appended to the end of the notification in additional varbinds. Enable the generation of this notification by setting the cGgsnGlobalErrorNotifEnabled to true(1). **Note** To prevent flooding, cGgsnGlobalErrorNotif, cGgsnAccessPointNameNotif, and cGgsnPacketDataProtocolNotif replace cGgsnNotification in GGSN Release 5.1 and later. For information about cGgsnGlobalErrorNotif alarms, see the "cGgsnGlobalErrorNotif" section on page A-19.
cGgsnAccessPointNameNotif (1.3.6.1.4.1.9.9.240.2.0.9) cGgsnAccessPointErrorTypes cGgsnHistNotifSeverity cGgsnHistNotifTimestamp cGgsnHistNotifGgsnIpAddrType cGgsnHistNotifGgsnIpAddr cGgsnHistNotifInfo cGgsnNotifAccessPointName	Sent when an APN-related alarm has occurred. If additional information is available for specific types of alarms, that information might be appended to the end of the notification in additional varbinds. Enable the generation of this notification by setting the cGgsnAccessPointNotifEnabled to true(1). **Note** To prevent flooding, cGgsnGlobalErrorNotif, cGgsnAccessPointNameNotif, and cGgsnPacketDataProtocolNotif replace cGgsnNotification in GGSN Release 5.1 and later. For information about cGgsnAccessPointNameNotif alarms, see the "cGgsnAccessPointNameNotif" section on page A-20.
cGgsnPacketDataProtocolNotif (1.3.6.1.4.1.9.9.240.2.0.10) cGgsnPacketDataProtoErrorTypes cGgsnHistNotifSeverity cGgsnHistNotifTimestamp cGgsnHistNotifGgsnIpAddrType cGgsnHistNotifGgsnIpAddr cGgsnHistNotifInfo cGgsnNotifAccessPointName cGgsnNotifPdpMsisdn cGgsnNotifPdpImsi	Sent when a user-related alarm has occurred. If additional information is available for specific types of alarms, that information might be appended to the end of the notification in additional varbinds. Enable the generation of this notification by setting the cGgsnPdpNotifEnabled to true(1). **Note** To prevent flooding, cGgsnGlobalErrorNotif, cGgsnAccessPointNameNotif, and cGgsnPacketDataProtocolNotif replace cGgsnNotification in GGSN Release 5.1 and later. For information about cGgsnPacketDataProtocolNotif alarms, see the "cGgsnPacketDataProtocolNotif" section on page A-22.

Service-Aware Billing Notifications

Table A-2 lists service-aware billing notifications supported by the CISCO-GGSN-SERVICE-AWARE-MIB. To enable these notifications to be sent, use the **snmp-server enable traps gprs** command in global configuration mode, with the **csg** and/or **dcca** keyword options specified.

Note Issue a separate command for each keyword option.

Table A-3 Service-Aware Billing Notifications

Notification and Notification Objects	Notes
cGgsnSACsgStateUpNotif (1.3.6.1.4.1.9.9.497.2.0.1) cGgsnSANotifCsgRealAddressType, cGgsnSANotifCsgRealAddress, cGgsnSANotifCsgVirtualAddrType, cGgsnSANotifCsgVirtualAddress, cGgsnSANotifCsgPort	Sent when the link to a CSG becomes active. If a port number is not configured in the CSG group, the cGgsnSANotifCsgPort information uses the default value. Enable the generation of this notification by setting the cGgsnSACsgNotifEnabled to true(1).
cGgsnSACsgStateDownNotif (1.3.6.1.4.1.9.9.497.2.0.2) cGgsnSANotifCsgRealAddressType, cGgsnSANotifCsgRealAddress, cGgsnSANotifCsgVirtualAddrType, cGgsnSANotifCsgVirtualAddress, cGgsnSANotifCsgPort	Sent when the link to a CSG goes down. If a port number is not configured in the CSG group, the cGgsnSANotifCsgPort information uses the default value. Enable the generation of this notification by setting the cGgsnSACsgNotifEnabled to true(1).
cGgsnSADccaEndUsrServDeniedNotif (1.3.6.1.4.1.9.9.497.2.0.3) cGgsnNotifPdpImsi cGgsnNotifPdpMsisdn	Sent when the credit control server denies the service request because of service restrictions. When this notification is received on the category level, the DCCA client discards all future user traffic for that category on that PDP Enable the generation of this notification by setting the cGgsnSADccaNotifEnabled to true(1).
cGgsnSADccaCreditLimReachedNotif (1.3.6.1.4.1.9.9.497.2.0.4) cGgsnNotifPdpImsi cGgsnNotifPdpMsisdn	Sent when the credit limit is reached. The credit control server denies the service request since the end users account could not cover the requested service. The client behaves as it does with CGgsnDccaEndUsrServDeniedNotif. Enable the generation of this notification by setting the cGgsnSADccaNotifEnabled to true(1).
cGgsnSADccaUserUnknownNotif (1.3.6.1.4.1.9.9.497.2.0.5) cGgsnNotifPdpImsi cGgsnNotifPdpMsisdn	Sent when the specified end user is unknown to the credit-control server. Such permanent failures cause the client to enter an Idle state. The client shall reject or terminate the PDP context depending on whether the result code was received in a CCA(Initial) or a CCA(Update). Enable the generation of this notification by setting the cGgsnSADccaNotifEnabled to true(1).

Table A-3 Service-Aware Billing Notifications (continued)

Notification and Notification Objects	Notes
cGgsnSADccaRatingFailedNotif (1.3.6.1.4.1.9.9.497.2.0.6) cGgsnNotifPdpImsi cGgsnNotifPdpMsisdn	Sent when the credit control server cannot rate the service request due to insufficient rating input, incorrect AVP combination or because of an AVP or AVP value that is not recognized or supported in the rating. Enable the generation of this notification by setting the cGgsnSADccaNotifEnabled to true(1).
cGgsnSADccaAuthRejectedNotif (1.3.6.1.4.1.9.9.497.2.0.7) cGgsnNotifPdpImsi cGgsnNotifPdpMsisdn	Sent when the credit control server failed to authorize an end user. The PDP context is deleted and the category blacklisted. Enable the generation of this notification by setting the cGgsnSADccaNotifEnabled to true(1).

Charging Notifications

Table A-4 lists the charging-related traps supported in the CISCO-GPRS-CHARGING-MIB. To enable these notifications to be sent, use the **snmp-server enable traps gprs charging** command in global configuration mode.

Table A-4 Charging Notifications

Notification and Notification Objects	Notes
cgprsCgAlarmNotif (1.3.6.1.4.1.9.9.192.2.0.1) cgprsCgAlarmHistType cgprsCgAlarmHistAddrType cgprsCgAlarmHistAddress cgprsCgAlarmHistSeverity cgprsCgAlarmHistInfo	Sent when a charging-related alarm is detected in the managed system. This alarm is sent after an entry is added to the cgprsCgAlarmHistTable. Enable the generation of this notification by setting the cgprsCgAlarmEnable to true(1). For information about cgprsCgAlarmNotif alarms, see the "CgprsCgAlarmNotif" section on page A-24.
cgprsCgGatewaySwitchoverNotif (1.3.6.1.4.1.9.9.192.2.0.2) cgprsCgActiveChgGatewayAddrType cgprsCgActiveChgGatewayAddress cgprsCgOldChgGatewayAddress	Sent when the active charging gateway has switched. The switchover to a new charging gateway occurs according to the value specified for the charging gateway switch timer. The charging gateway switch timer can be set using the The charging gateway switch timer can be set using the **gprs charging server-switch-timer** command in global configuration mode or by setting cgprsCgGroupSwitchOverTime. The priority in which a new charging gateway is selected can be configured using the **gprs charging switchover priority** command in global configuration mode or by setting cgprsCgSwitchOverPriority. Enable the generation of this notification by setting cgprsCGAlarmEnable to true(1).

Table A-4 Charging Notifications (continued)

Notification and Notification Objects	Notes
cgprsCgInServiceModeNotif (1.3.6.1.4.1.9.9.192.2.0.3)	Sent when the GGSN charging function is placed in operational mode. The charging function of the GGSN is placed in operational mode using the **gprs charging service-mode** command in global configuration mode or by setting the cgprsCgServiceMode object to operational(1). Enable the generation of this notification by setting cgprsCGAlarmEnable to true(1).
cgprsCgMaintenanceModeNotif (1.3.6.1.4.1.9.9.192.2.0.4)	Sent when the GGSN charging function is placed in maintenance mode. The charging function of the GGSN is placed in maintenance mode using the **gprs charging service-mode** command in global configuration mode or by setting the cgprsCgServiceMode object to maintenance(2). Enable the generation of this notification by setting cgprsCGAlarmEnable to true(1).

Access-Point Notifications

Table A-5 lists access-point-related notifications supported by the CISCO-GPRS-ACC-PT-MIB. To enable these notifications to be sent, use the **snmp-server enable traps gprs apn** command in global configuration mode.

Table A-5 Access-point Notifications

Notification and Notification Objects	Notes
cgprsAccPtCfgNotif (1.3.6.1.4.1.9.9.183.2.0.1) cgprsAccPtCfgNotifAccPtIndex cgprsAccPtCfgNotifReason	Sent when an access-point configuration has occurred. This notification is sent after an entry is added to the cgprsAccPtCfgNotifHistTable. Enable the generation of this notification by setting the cgprsAccPtCfgNotifEnable to true(1). For information about cgprsAccPtCfgNotif alarms, see the "cgprsAccPtCfgNotif" section on page A-26.
cgprsAccPtSecSrcViolNotif (1.3.6.1.4.1.9.9.183.2.0.2) cgprsAccPtCfgNotifAccPtIndex cgprsAccPtMsAddrType cgprsAccPtMsAllocAddr cgprsAccPtMsNewAddr	Sent when a security violation has occurred, specifically, the GGSN determines that the source address of an upstream TPDU differs from that previously assigned to the MS. Enable the generation of this notification using the **security verify** (for IPv4 PDPs) or **ipv6 security verify source** (for IPv6 PDPs) access-point configuration commands or by setting the cgprsAccPtVerifyUpStrTpduSrcAddr object to true(1).

Table A-5 Access-point Notifications (continued)

Notification and Notification Objects	Notes
cgprsAccPtSecDestViolNotif (1.3.6.1.4.1.9.9.183.2.0.3) cgprsAccPtCfgNotifAccPtIndex cgprsAccPtMsAddrType cgprsAccPtMsAllocAddr cgprsAccPtMsTpduDstAddr	Sent when a security violation has occurred, specifically, the GGSN determines that the destination address of an upstream TPDU falls within the range of a user-defined global list of PLMN addresses. Enable the generation of this notification using the **security verify destination** access-point configuration command or by setting the cgprsAccPtVerifyUpStrTpduDstAddr object to true(1).
cgprsAccPtMaintenanceNotif (1.3.6.1.4.1.9.9.183.2.0.4) cgprsAccPtCfgNotifAccPtIndex	Sent when the APN is placed in maintenance mode. An APN is placed in maintenance mode using the **service-mode maintenance** access-point configuration command or by setting the cgprsAccPtOperationMode object to maintenance(1). The service mode is identified by cGgsnServiceModeStatus. Enable the generation of this notification by setting cgprsAccPtMaintenanceNotif to true(1).
cgprsAccPtInServiceNotif (1.3.6.1.4.1.9.9.183.2.0.5) cgprsAccPtCfgNotifAccPtIndex	Sent when the APN is placed in operational mode. An APN is placed in operational mode using the **service-mode operational** access-point configuration command or by setting cgprsAccPtOperationMode to inService(0). The service mode is identified by cGgsnServiceModeStatus. Enable the generation of this notification by setting cgprsAccPtMaintenanceNotif to true(1).

GTP Notification

Table A-5 lists the GTP-related notification supported by the CISCO-GTP-MIB. To enable this notification to be sent, use the **snmp-server enable traps gprs gtp** command in global configuration mode.

Table A-6 GTP Notification

Notification and Notification Objects	Notes
cGtpPathFailedNotification (1.3.6.1.4.1.9.9.188.2.0.1) cGtpLastNoRespToEchoGSNIpAddrTyp cGtpLastNoRespToEchoGSNIpAddr	Sent when a GGSN peer (SGSN or charging gateway) fails to respond to the GTP echo request message for the time period of the N3-requests counter configured using the **gprs gtp n3-requests** command in global configuration mode. Enable the generation of this notification by setting the cGtpNotifEnable to true(1).

Alarm Notifications

Depending on the severity level, notifications are considered alarms or informational events. Notifications with a severity level of critical, major, or minor are classified as alarms. An alarm must be reported when an alarm state changes (assuming the alarm does not have a nonreported severity).

Informational events do not require state changes. An informational event is a warning that an abnormal condition that does not require corrective action has occurred. The informational event is reported but is transient. No corrective action is required to fix the problem.

Table A-7 lists the severity levels and the required responses.

Table A-7 Notification Severity Levels

Severity Level	Description
Critical	A serious condition exists. If an action is recommended, clear critical alarms immediately.
Major	A disruption of service has occurred. Clear this alarm immediately.
Minor	No disruption of service has occurred, but clear this alarm as soon as possible.
Informational	A warning that an abnormal condition that does not require corrective action has occurred. An informational event is reported but is transient. No corrective action is required by the management center to fix this problem.

Alarms have a trap type associated with them. Table A-8 identifies the trap types that can be associated with an Alarm.

Table A-8 Alarm Trap Types

Trap Type	Description
1 (cleared)	Indicates a previous alarm condition is cleared. It is not required, unless specifically stated elsewhere on a case-by-case basis, that an alarm condition that is cleared will produce a notification or other even t containing an alarm severity with this value.
2 (indeterminate)	Indicates that the severity level cannot be determined.
3 (critical)	A service-affecting condition has occurred and an immediate action is possibly required.
4 (major)	A service-affecting condition has occurred and an urgent corrective action is possibly required.
5 (minor)	A nonservice-affecting condition exists and corrective action should be taken in order to prevent a more serious condition (for example, a safety-affecting condition).
6 (warning)	A potential or impending service or safety affection condition is detected before any significant affects have been felt.
7 (info)	The alarm condition does not meet any other severity definition. This can include important, but non--urgent notices or informational events.

The following sections describe alarms supported by the following notifications:

- cGgsnGlobalErrorNotif, page A-19
- cGgsnAccessPointNameNotif, page A-20
- CgprsCgAlarmNotif, page A-24
- cgprsAccPtCfgNotif, page A-26

cGgsnGlobalErrorNotif

Table A-9 lists alarms supported by the cGgsnGlobalErrorNotif notification (CISCO-GGSN-MIB). Alarms supported by the cGgsnGlobalErrorNotif notification are global-related alarms.

Table A-9 cGgsnGlobalErrorNotif Alarms

Alarm	Description
ggsnServiceUp	**Cause:** GGSN service has started. The **service gprs** command in global configuration mode has been issued. **Severity Level and Trap Type:** The severity level is critical. The trap type is 3. **Recommended Action:** This is an informational event. No action is required.
ggsnServiceDown	**Cause:** GGSN service is down. The **no gprs service** command in global configuration mode has been issued or the system service is down because of another reason. **Severity Level and Trap Type:** The severity level is critical. The trap type is 3. **Recommended Action:** Attempt to restart the GGSN service on the router by issuing the **service gprs** command in global configuration mode and if the problem persists, contact your Cisco technical support representative with the error message.
noDHCPServer	**Cause:** A DHCP server is not configured. This error notification is generated when part of the DHCP server configuration is missing or is incorrect. **Severity Level and Trap Type:** The severity level is major. The trap type is 4. **Recommended Action:** Ensure that all elements of the DHCP configuration are properly configured.

cGgsnAccessPointNameNotif

Table A-10 lists alarms supported by the cGgsnAccessPointNameNotif notification (CISCO-GGSN-MIB). Alarms supported by the cGgsnAccessPointNameNotif notification are APN-related alarms.

Table A-10 cGgsnAccessPointNameNotif Alarms

Alarm	Description
noRadius	**Cause:** A RADIUS server is not configured. This error notification is generated when part of the RADIUS server configuration is missing. **Severity Level and Trap Type:** The severity level is major. The trap type is 4. **Recommended Actions:** 1. Verify that the RADIUS server is properly configured and that you can ping it. 2. Ensure that the RADIUS server is configured properly. **Note** The error message, issue a show running configuration and contact your Cisco technical support representative.

Table A-10 cGgsnAccessPointNameNotif Alarms (continued)

Alarm	Description
ipAllocationFail	**Cause:** Dynamic IP allocation failed because of one of the following reasons: 1. One of the following DHCP or RADIUS server problem might have occurred: a. The DHCP/RADIUS server IP address is configured incorrectly in the GGSN. b. The DHCP/RADIUS server is reachable, but the configuration to allocate IP addresses might be incorrect. c. The DHCP or RADIUS server is properly configured, but cannot be reached. 2. Dynamic IP allocation is disabled in the APN configuration. 3. The PAP or CHAP username and password information is missing from the RADIUS client in transparent mode. Therefore, this information is missing in the PDP activation request. **Severity Level and Trap Type:** The severity level is major. The trap type is 4. **Recommended Actions:** 1. Check the DHCP/RADIUS server configuration, ensuring that: a. The DHCP/RADIUS server IP address configured on the GGSN is valid. b. The DHCP/RADIUS server is properly configured to allocate IP addresses. c. The DHCP/RADIUS server is reachable (via the **ping** command). 2. Configure IP allocation pool in the APN as either DHCP proxy client or RADIUS client. 3. If none of the above does not resolve the alarm condition, contact you Cisco technical support representative with the error message.
apnUnreachable	**Cause:** A PDP activation has failed because the APN requested in the Create PDP Context request is not configured on the GGSN. **Severity Level and Trap Type:** The severity level is major. The trap type is 4. **Recommended Action:** Check the configuration of the corresponding APN. If the configuration appears to be correct, contact your Cisco technical support representative with the error message and saved output of the **show running-config** and **show gprs access-point all** commands.

cGgsnPacketDataProtocolNotif

Table A-11 lists alarms supported by the cGgsnPacketDataProtocolNotif notification (CISCO-GGSN-MIB). Alarms supported by the cGgsnPacketDataProtocolNotif notification are PDP-related alarms.

Table A-11 cGgsnPacketDataProtocolNotif Alarms

Alarm	Description
noResource	**Cause:** Resources available to continue GGSN service are exhausted because of one of the following reasons: • Maximum number of PDP contexts is reached. • Maximum number of PPP regenerated PDP contexts is reached. **Severity Level and Trap Type:** The severity level is critical. The trap type is 3. **Recommended Action:** If possible, increase the number of PDP contexts that can be processed by the GGSN. If the problem persists, contact your Cisco technical support representative with the error message.
authenticationFail	**Cause:** A PDP activation has failed because of one of the following reasons: 1. There is no RADIUS server present for authentication because a RADIUS server is not configured or is unreachable. 2. An invalid username or password is used in the Create PDP Context request. 3. The PAP/CHAP information element is missing in the Create PDP Context request in non-transparent mode. 4. The username is not present in the Create PDP Context request. 5. There is a duplicate IP address to access the APN. **Severity Level and Trap Type:** The severity level is warning. The trap type is 6. **Recommended Action:** Verify that the RADIUS server is configured properly and is reachable using the **ping** command. If it is, contact your Cisco technical support representative with the error message and the saved output of the **show running-config**.

Table A-11 cGgsnPacketDataProtocolNotif Alarms (continued)

Alarm	Description
ccrInitFail	**Cause:** The CCR(Initial) is sent to a Diameter server and the Tx time expired before receiving a CCA(Initial) response. **Severity Level and Trap Type:** The severity level is major. The trap type is 4. **Recommended Action:** The action on the PDP context creation is determined by the credit control failure handling (CCFH) configuration. Check the Diameter server and DCCA Tx timer and CCFH configurations on the GGSN to ensure they have been configured correctly.
quotaPushFail	**Cause:** The quota push failed because: 1) the path between the CSG and quota server process on the GGSN is down, or 2) the CSG sent a negative Quota Push response for a Quota Push request. **Severity Level and Trap Type:** The severity level is major. The trap type is 4. **Recommended Action:** Check the CSG configuration, and the quota server configuration on the GGSN and the path state between the two. If the condition persists, contact your Cisco technical support representative with the error message.

CgprsCgAlarmNotif

Table A-12 lists alarms supported by the CgprsCgAlarmNotif notification (CISCO-GPRS-CHARGING-MIB). Alarms supported by the CgprsCgAlarmNotif notification are alarms related to the charging functions of the GGSN.

Table A-12 CgprsCgAlarmNotif Alarms

Alarm	Description
cgprsCgAlarmCgDown	**Cause:** The charging gateway (primary, secondary, and tertiary) is down because it is not configured or there is a missing response to a nodealive request on the charging gateway path. **Severity Level and Trap Type:** The severity level is critical. The trap type is 3. **Recommended Action:** Verify that a charging gateway configuration exists and that the correct IP address is assigned. If it is, then the charging gateway is down.
cgprsCgAlarmCgUp	**Cause:** The charging gateway is up. **Severity Level and Trap Type:** The severity level is critical. The trap type is 3. **Recommended Action:** This is an informational event. No action is required.
cgprsCgAlarmTransFailure	**Cause:** The GGSN has repeatedly failed to receive a response from the charging gateway for data record transfer requests. **Severity Level and Trap Type:** The severity level is critical. The trap type is 3. **Recommended Action:** Verify that the charging gateways are properly configured on the GGSN and charging functionality is active.
cgprsCgAlarmTransSuccess	**Cause:** The GGSN has successfully sent data record transfer requests to the charging gateway after the failure. **Severity Level and Trap Type:** The severity level is critical. The trap type is 3. **Recommended Action:** This is an informational event. No action is required.
cgprsCgAlarmCapacityFull	**Cause:** The GGSN buffer is full and subsequent packets might be dropped. **Severity Level and Trap Type:** The severity level is critical. The trap type is 3. **Recommended Action:** Confirm the value configured for the **gprs charging send-buffer** global configuration command, and if possible, increase the number of bytes configured for the buffer.

Table A-12 CgprsCgAlarmNotif Alarms (continued)

Alarm	Description
cgprsCgAlarmCapacityFree	**Cause:** The GGSN is able to buffer gateway GPRS support node-call detail record (G-CDR) after a failure to buffer G-CDRs has occurred. **Severity Level and Trap Type:** The severity level is critical. The trap type is 3. **Recommended Action:** This is an informational event. No action is required.
cgprsCgAlarmEchoFailure	**Cause:** The GGSN has failed to receive an echo response from the charging gateway to an echo request. **Severity Level and Trap Type:** The severity level is critical. The trap type is 3. **Recommended Action:** Verify that the charging gateways are properly configured on the GGSN. If the condition persists, contact your Cisco technical support representative with the error message.
cgprsCgAlarmEchoRestored	**Cause:** The GGSN has received an echo response from the charging gateway after an cgprsCgAlarmEchoFailure was sent. **Severity Level and Trap Type:** The severity level is critical. The trap type is 3. **Recommended Action:** This is an informational event. No action required.
cgprsCgAlarmChargingDisabled	**Cause:** Indicates that charging transactions on the GGSN are disabled. **Severity Level and Trap Type:** The severity level is critical. The trap type is 3. **Recommended Action:** This is an informational event. No action is required.
cgprsCgAlarmChargingEnabled	**Cause:** Indicates that charging transactions on the GGSN are enabled. **Severity Level and Trap Type:** The severity level is critical. The trap type is 3. **Recommended Action:** This is an informational event. No action is required.
cgprsCgGatewaySwitchoverNotif	**Cause:** Indicates that the active charging gateway has switched. **Recommended Action:** This is an informational event. Determine why the charging gateway switchover occurred.

Table A-12 CgprsCgAlarmNotif Alarms (continued)

Alarm	Description
cgprsCgInServiceModeNotif	**Cause:** Indicates that the GGSN charging function is placed in in-service/operational mode from maintenance mode. **Recommended Action:** This is an informational event. No action is required.
cgprsCgMaintenanceModeNotif	**Cause:** Indicates that the GGSN charging function is placed in maintenance mode from in-service/operational mode. **Recommended Action:** This is an informational event. No action is required.

cgprsAccPtCfgNotif

Table A-13 lists alarms supported by the cgprsAccPtCfgNotif notification (CISCO-GPRS-ACC-PT-MIB).

Table A-13 cgprsAccPtCfgNotif

Alarm	Description
cgprsAccPtCfgNotif	**Cause:** The access point configuration is created, modified, or deleted. **Severity Level and Trap Type:** Not applicable **Recommended Action:** This is an informational event. No action is required.