



## **Cisco IOS Mobile Wireless Configuration Guide**

Release 12.2

### **Corporate 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: 408 526-4100

Customer Order Number: DOC-7812098=  
Text Part Number: 78-12098-02

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.

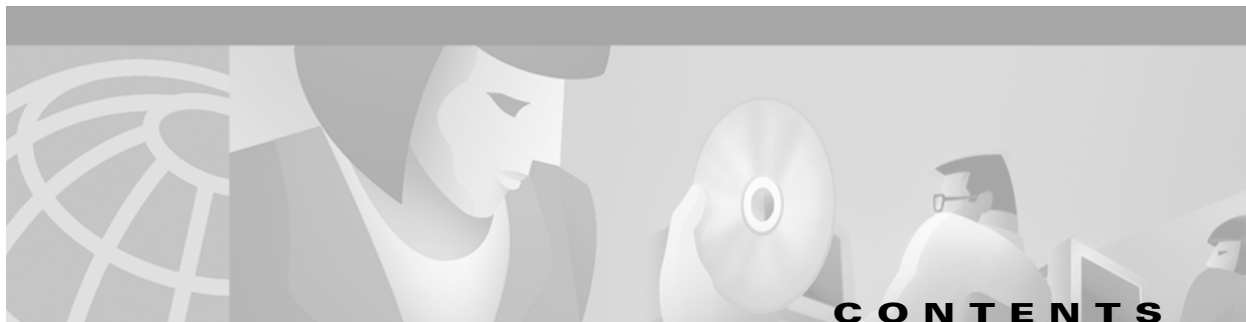
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE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

AccessPath, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco *NetWorks* logo, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, PIX, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Unity, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, and Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site 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. (0102R)

*Cisco IOS Mobile Wireless Configuration Guide*  
Copyright © 2001–2006 Cisco Systems, Inc.  
All rights reserved.



## **About Cisco IOS Software Documentation**    **vii**

Documentation Objectives	<b>vii</b>
Audience	<b>vii</b>
Documentation Organization	<b>vii</b>
Documentation Modules	<b>vii</b>
Master Indexes	<b>x</b>
Supporting Documents and Resources	<b>x</b>
Document Conventions	<b>xi</b>
Obtaining Documentation	<b>xii</b>
World Wide Web	<b>xii</b>
Documentation CD-ROM	<b>xii</b>
Ordering Documentation	<b>xiii</b>
Documentation Feedback	<b>xiii</b>
Obtaining Technical Assistance	<b>xiii</b>
Cisco.com	<b>xiii</b>
Technical Assistance Center	<b>xiv</b>
Contacting TAC by Using the Cisco TAC Website	<b>xiv</b>
Contacting TAC by Telephone	<b>xiv</b>

## **Using Cisco IOS Software**    **xv**

Understanding Command Modes	<b>xv</b>
Getting Help	<b>xvi</b>
Example: How to Find Command Options	<b>xvii</b>
Using the no and default Forms of Commands	<b>xix</b>
Saving Configuration Changes	<b>xx</b>
Filtering Output from the show and more Commands	<b>xx</b>
Identifying Platform Support for Cisco IOS Software Features	<b>xxi</b>
Using Feature Navigator	<b>xxi</b>
Using Software Release Notes	<b>xxi</b>

## **Mobile Wireless Overview**    **MWC-1**

Introduction to Mobile Wireless Technology	<b>MWC-1</b>
Overview of Basic Network Elements Associated with Cellular Networks and Mobile Wireless	<b>MWC-2</b>
Wireless Standards Development	<b>MWC-4</b>

Model for IP Integration into Mobile Wireless **MWC-5**

Mobile Wireless in Cisco IOS Software **MWC-7**

IP Data Services **MWC-7**

GPRS **MWC-7**

## **GENERAL PACKET RADIO SERVICE (GPRS)**

### **Overview of GPRS MWC-11**

Overview **MWC-11**

Benefits **MWC-14**

### **Planning to Configure the GGSN MWC-15**

Prerequisites **MWC-15**

Restrictions **MWC-15**

Supported Platforms **MWC-16**

Supported Standards, MIBs, and RFCs **MWC-16**

Related Documents **MWC-16**

### **Configuring GGSN Services MWC-17**

Configuring the GGSN **MWC-17**

Customizing the GPRS Configuration **MWC-19**

### **Configuring Charging on the GGSN MWC-21**

Configuring the Charging Gateway **MWC-21**

Changing the Default Charging Gateway **MWC-22**

Configuring the Transport Protocol for the Charging Gateway **MWC-22**

Configuring TCP as the Charging Gateway Path Protocol **MWC-22**

Configuring UDP as the Charging Gateway Path Protocol **MWC-22**

Customizing the Charging Gateway **MWC-23**

Disabling Charging Processing **MWC-24**

### **Configuring Network Access to the GGSN MWC-25**

Configuring an Interface to the SGSN **MWC-25**

Configuring a Route to the SGSN **MWC-26**

Configuring a Static Route to the SGSN **MWC-26**

Configuring Access to a PDN **MWC-26**

Configuring an Interface to a PDN **MWC-27**

Configuring an Access Point for a PDN **MWC-27**

Configuring the GPRS Access Point List on the GGSN **MWC-27**

Configuring Access to a VPN **MWC-29**

Configuring Access to a VPN Without a Tunnel	MWC-30
Configuring Access to a VPN With a Tunnel	MWC-30
Configuring the VPN Access Point	MWC-30
Configuring the IP Tunnel	MWC-31
<b>Optimizing GPRS Performance</b>	<b>MWC-33</b>
Configuring Fast Switching for GPRS	MWC-33
Enabling Fast Switching on the Virtual Template Interface	MWC-33
Enabling Fast Switching on a Physical Interface	MWC-34
<b>Configuring Security on the GGSN</b>	<b>MWC-35</b>
Configuring AAA Security Globally	MWC-36
Configuring RADIUS Server Communication Globally	MWC-36
Configuring RADIUS at the GPRS Configuration Level	MWC-38
Configuring Non-Transparent Access Mode	MWC-38
Specifying a RADIUS Server for All Access Points	MWC-39
Specifying a RADIUS Server for a Particular Access Point	MWC-39
Configuring the MSISDN IE for RADIUS Requests	MWC-40
Suppressing the MSISDN Number for RADIUS Authentication	MWC-40
Configuring IPSec Network Security	MWC-40
Configuring an IKE Policy	MWC-41
Configuring Pre-Shared Keys	MWC-42
Configuring Transform Sets	MWC-43
<b>Configuring DHCP on the GGSN</b>	<b>MWC-45</b>
Configuring DHCP Server Communication Globally	MWC-45
Configuring DHCP at the GPRS Configuration Level	MWC-46
Specifying a DHCP Server for All Access Points	MWC-46
Specifying a DHCP Server for a Particular Access Point	MWC-47
<b>Verifying the GPRS Configuration</b>	<b>MWC-49</b>
Verifying Global GPRS Configuration	MWC-49
Verifying Interface Configuration to the SGSN	MWC-50
Verifying Interface Configuration to the PDN	MWC-50
Verifying an Interface to the Private Network	MWC-50
Verifying Configuration to the Virtual Template	MWC-50
Verifying Access-Point Configuration	MWC-51
Verifying DHCP Configuration	MWC-52

**Monitoring and Maintaining GPRS** MWC-53

**GGSN Configuration Examples** MWC-55

Virtual Template Interface Configuration on GGSN Example MWC-55

Static Route to SGSN Example MWC-56

Access Point List Configuration Example MWC-56

VPN Tunnel Configuration Example MWC-57

AAA Security Configuration Example MWC-57

RADIUS Server Global Configuration Example MWC-58

RADIUS Server Access Point Configuration Example MWC-58

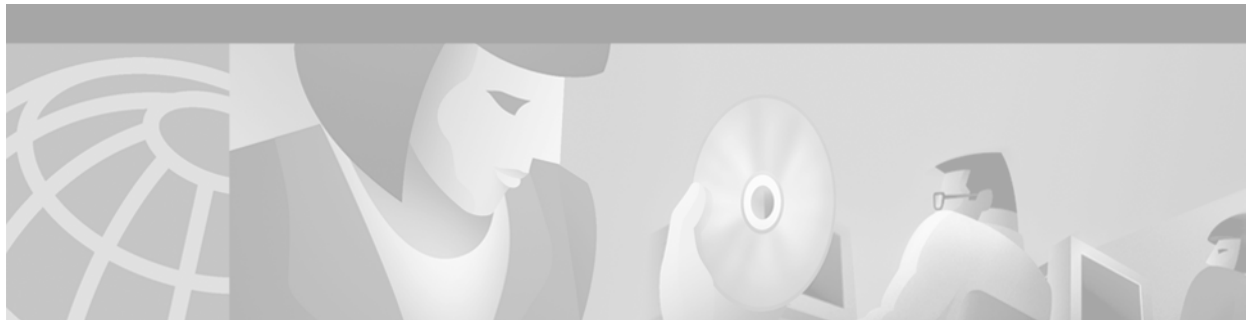
IPSec Configuration Example MWC-59

DHCP Server Configuration Example MWC-62

Charging Gateway Configuration Example MWC-63

Complete GGSN Configuration Example MWC-64

**INDEX**



## About Cisco IOS Software Documentation

---

This chapter discusses the objectives, audience, organization, and conventions of Cisco IOS software documentation. It also provides sources for obtaining documentation from Cisco Systems.

### Documentation Objectives

Cisco IOS software documentation describes the tasks and commands necessary to configure and maintain Cisco networking devices.

### Audience

The Cisco IOS software documentation set is intended primarily for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the tasks, the relationship between tasks, or the Cisco IOS software commands necessary to perform particular tasks. The Cisco IOS software documentation set is also intended for those users experienced with Cisco IOS software who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS software release.

### Documentation Organization

The Cisco IOS software documentation set consists of documentation modules and master indexes. In addition to the main documentation set, there are supporting documents and resources.

### Documentation Modules

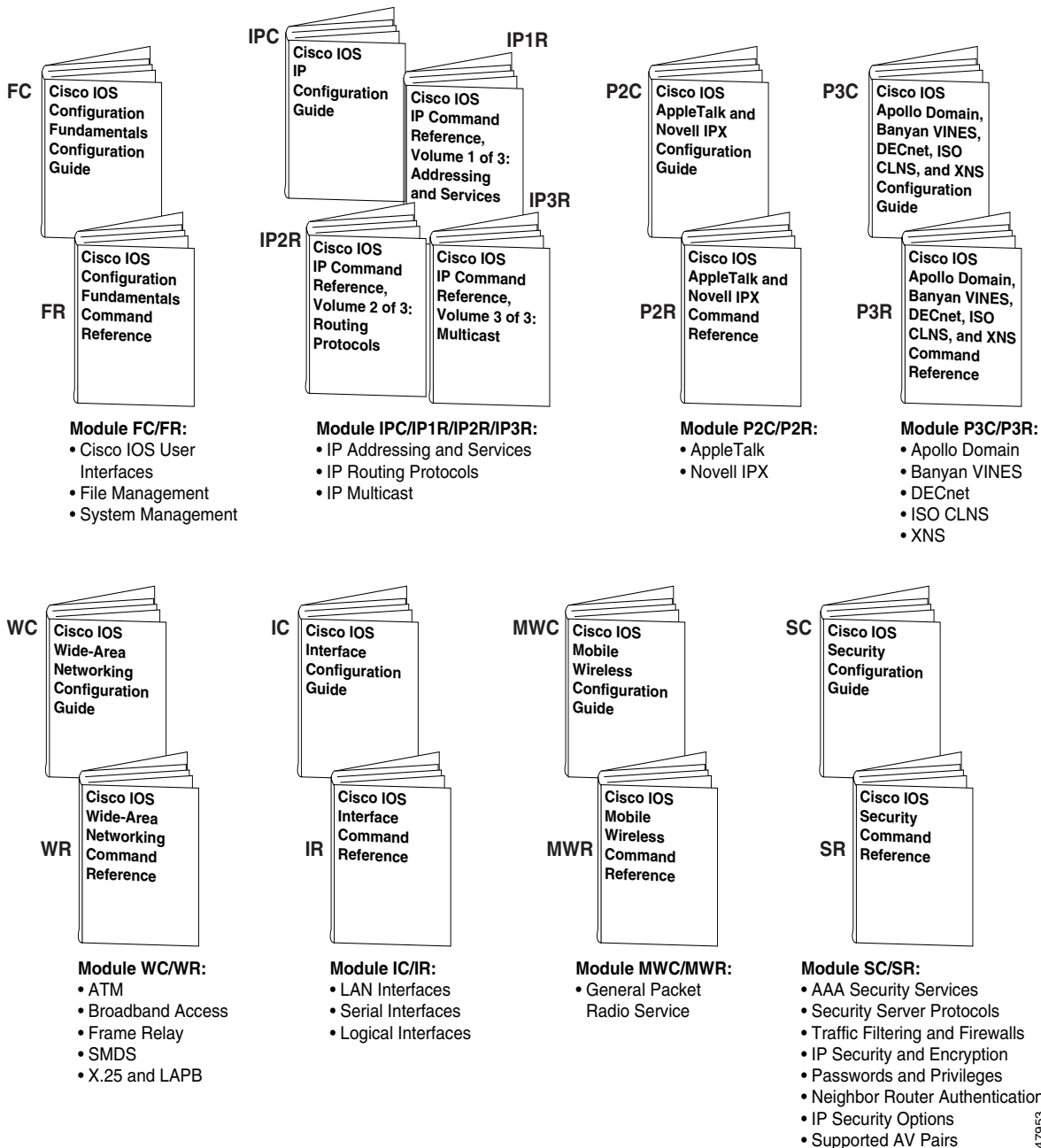
The Cisco IOS documentation modules consist of configuration guides and corresponding command reference publications. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality and contain comprehensive configuration examples. Chapters in a command reference publication provide complete Cisco IOS command syntax information. Use each configuration guide in conjunction with its corresponding command reference publication.

Figure 1 shows the Cisco IOS software documentation modules.

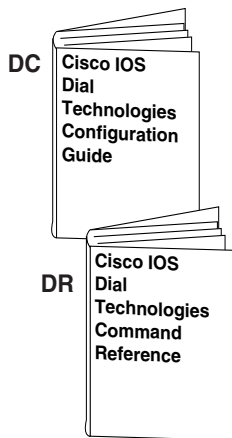
**Note**

The abbreviations (for example, FC and FR) next to the book icons are page designators, which are defined in a key in the index of each document to help you with navigation. The bullets under each module list the major technology areas discussed in the corresponding books.

**Figure 1 Cisco IOS Software Documentation Modules**

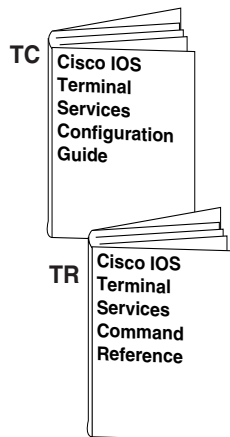


47953



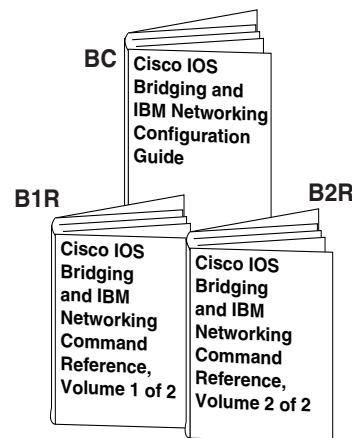
**Module DC/DR:**

- Preparing for Dial Access
- Modem and Dial Shelf Configuration and Management
- ISDN Configuration
- Signalling Configuration
- Dial-on-Demand Routing Configuration
- Dial-Backup Configuration
- Dial-Related Addressing Services
- Virtual Templates, Profiles, and Networks
- PPP Configuration
- Callback and Bandwidth Allocation Configuration
- Dial Access Specialized Features
- Dial Access Scenarios



**Module TC/TR:**

- ARA
- LAT
- NAS1
- Telnet
- TN3270
- XRemote
- X.28 PAD
- Protocol Translation

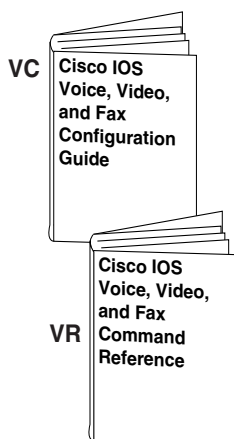


**Module BC/B1R:**

- Transparent Bridging
- SRB
- Token Ring Inter-Switch Link
- Token Ring Route Switch Module
- RSRB
- DLSw+
- Serial Tunnel and Block Serial Tunnel
- LLC2 and SDLC
- IBM Network Media Translation
- SNA Frame Relay Access
- NCIA Client/Server
- Airline Product Set

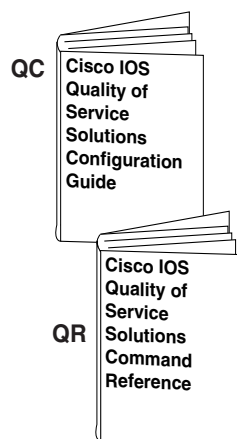
**Module BC/B2R:**

- DSPU and SNA Service Point
- SNA Switching Services
- Cisco Transaction Connection
- Cisco Mainframe Channel Connection
- CLAW and TCP/IP Offload
- CSNA, CMPC, and CMPC+
- TN3270 Server



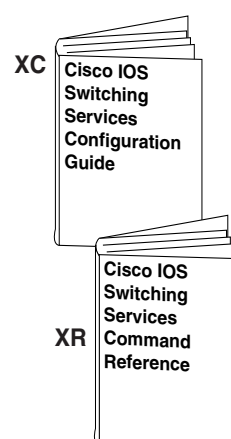
**Module VC/VR:**

- Voice over IP
- Call Control Signalling
- Voice over Frame Relay
- Voice over ATM
- Telephony Applications
- Trunk Management
- Fax, Video, and Modem Support



**Module QC/QR:**

- Packet Classification
- Congestion Management
- Congestion Avoidance
- Policing and Shaping
- Signalling
- Link Efficiency Mechanisms



**Module XC/XR:**

- Cisco IOS Switching Paths
- NetFlow Switching
- Multiprotocol Label Switching
- Multilayer Switching
- Multicast Distributed Switching
- Virtual LANs
- LAN Emulation

47954

## Master Indexes

Two master indexes provide indexing information for the Cisco IOS software documentation set: an index for the configuration guides and an index for the command references. Individual books also contain a book-specific index.

The master indexes provide a quick way for you to find a command when you know the command name but not which module contains the command. When you use the online master indexes, you can click the page number for an index entry and go to that page in the online document.

## Supporting Documents and Resources

The following documents and resources support the Cisco IOS software documentation set:

- *Cisco IOS Command Summary* (two volumes)—This publication explains the function and syntax of the Cisco IOS software commands. For more information about defaults and usage guidelines, refer to the Cisco IOS command reference publications.
- *Cisco IOS System Error Messages*—This publication lists and describes Cisco IOS system error messages. Not all system error messages indicate problems with your system. Some are purely informational, and others may help diagnose problems with communications lines, internal hardware, or the system software.
- *Cisco IOS Debug Command Reference*—This publication contains an alphabetical listing of the **debug** commands and their descriptions. Documentation for each command includes a brief description of its use, command syntax, usage guidelines, and sample output.
- *Dictionary of Internetworking Terms and Acronyms*—This Cisco publication compiles and defines the terms and acronyms used in the internetworking industry.
- New feature documentation—The Cisco IOS software documentation set documents the mainline release of Cisco IOS software (for example, Cisco IOS Release 12.2). New software features are introduced in early deployment releases (for example, the Cisco IOS “T” release train for 12.2, 12.2(x)T). Documentation for these new features can be found in standalone documents called “feature modules.” Feature module documentation describes new Cisco IOS software and hardware networking functionality and is available on Cisco.com and the Documentation CD-ROM.
- Release notes—This documentation describes system requirements, provides information about new and changed features, and includes other useful information about specific software releases. See the section “Using Software Release Notes” in the chapter “Using Cisco IOS Software” for more information.
- Caveats documentation—This documentation provides information about Cisco IOS software defects in specific software releases.
- RFCs—RFCs are standards documents maintained by the Internet Engineering Task Force (IETF). Cisco IOS software documentation references supported RFCs when applicable. The full text of referenced RFCs may be obtained on the World Wide Web at <http://www.rfc-editor.org/>.
- MIBs—MIBs are used for network monitoring. For lists of supported MIBs by platform and release, and to download MIB files, see the Cisco MIB website on Cisco.com at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

# Document Conventions

Within Cisco IOS software documentation, the term *router* is generally used to refer to a variety of Cisco products (for example, routers, access servers, and switches). Routers, access servers, and other networking devices that support Cisco IOS software are shown interchangeably within examples. These products are used only for illustrative purposes; that is, an example that shows one product does not necessarily indicate that other products are not supported.

The Cisco IOS documentation set uses the following conventions:

Convention	Description
^ or Ctrl	The ^ and Ctrl symbols represent the Control key. For example, the key combination ^D or Ctrl-D means hold down the Control key while you press the D key. Keys are indicated in capital letters but are not case sensitive.
<i>string</i>	A string is a nonquoted set of characters shown in italics. For example, when setting an SNMP community string to public, do not use quotation marks around the string or the string will include the quotation marks.

Command syntax descriptions use the following conventions:

Convention	Description
<b>boldface</b>	Boldface text indicates commands and keywords that you enter literally as shown.
<i>italics</i>	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x   y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x   y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example:

Convention	Description
[x {y   z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
screen	Examples of information displayed on the screen are set in Courier font.
<b>boldface screen</b>	Examples of text that you must enter are set in Courier bold font.
< >	Angle brackets enclose text that is not printed to the screen, such as passwords.

Convention	Description
!	An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the Cisco IOS software for certain processes.)
[ ]	Square brackets enclose default responses to system prompts.

The following conventions are used to attract the attention of the reader:

**Caution**

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

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

**Timesaver**

Means the *described action saves time*. You can save time by performing the action described in the paragraph.

## Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

### World Wide Web

The most current Cisco documentation is available on the World Wide Web at the following website:

<http://www.cisco.com>

Translated documentation is available at the following website:

[http://www.cisco.com/public/countries\\_languages.html](http://www.cisco.com/public/countries_languages.html)

### Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

## Ordering Documentation

Cisco documentation can be ordered in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products Marketplace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

## Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems, Inc.  
Document Resource Connection  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

### Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

<http://www.cisco.com/register/>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

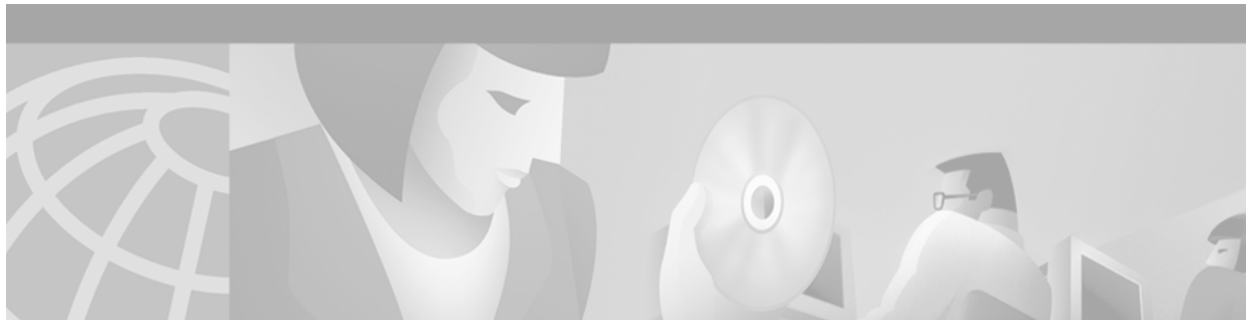
### Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.



## Using Cisco IOS Software

---

This chapter provides helpful tips for understanding and configuring Cisco IOS software using the command-line interface (CLI). It contains the following sections:

- Understanding Command Modes, page xv
- Getting Help, page xvi
- Using the no and default Forms of Commands, page xix
- Saving Configuration Changes, page xx
- Filtering Output from the show and more Commands, page xx
- Identifying Platform Support for Cisco IOS Software Features, page xxi

For an overview of Cisco IOS software configuration, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information on the conventions used in the Cisco IOS software documentation set, see the chapter “About Cisco IOS Software Documentation” located at the beginning of this book.

## Understanding Command Modes

You use the CLI to access Cisco IOS software. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode you are currently in. Entering a question mark (?) at the CLI prompt allows you to obtain a list of commands available for each command mode.

When you log in to the CLI, you are in user EXEC mode. User EXEC mode contains only a limited subset of commands. To have access to all commands, you must enter privileged EXEC mode, normally by using a password. From privileged EXEC mode you can issue any EXEC command—user or privileged mode—or you can enter global configuration mode. Most EXEC commands are one-time commands. For example, **show** commands show important status information, and **clear** commands clear counters or interfaces. The EXEC commands are not saved when the software reboots.

Configuration modes allow you to make changes to the running configuration. If you later save the running configuration to the startup configuration, these changed commands are stored when the software is rebooted. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

ROM monitor mode is a separate mode used when the Cisco IOS software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode.

Table 1 describes how to access and exit various common command modes of the Cisco IOS software. It also shows examples of the prompts displayed for each mode.

**Table 1 Accessing and Exiting Command Modes**

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	Router>	Use the <b>logout</b> command.
Privileged EXEC	From user EXEC mode, use the <b>enable</b> EXEC command.	Router#	To return to user EXEC mode, use the <b>disable</b> command.
Global configuration	From privileged EXEC mode, use the <b>configure terminal</b> privileged EXEC command.	Router(config)#	To return to privileged EXEC mode from global configuration mode, use the <b>exit</b> or <b>end</b> command, or press <b>Ctrl-Z</b> .
Interface configuration	From global configuration mode, specify an interface using an <b>interface</b> command.	Router(config-if)#	To return to global configuration mode, use the <b>exit</b> command. To return to privileged EXEC mode, use the <b>end</b> command, or press <b>Ctrl-Z</b> .
ROM monitor	From privileged EXEC mode, use the <b>reload</b> EXEC command. Press the <b>Break</b> key during the first 60 seconds while the system is booting.	>	To exit ROM monitor mode, use the <b>continue</b> command.

For more information on command modes, refer to the “Using the Command-Line Interface” chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

## Getting Help

Entering a question mark (?) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands:

Command	Purpose
<b>help</b>	Provides a brief description of the help system in any command mode.
<i>abbreviated-command-entry?</i>	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
<i>abbreviated-command-entry</i> <Tab>	Completes a partial command name.
<b>?</b>	Lists all commands available for a particular command mode.
<i>command ?</i>	Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.)

## Example: How to Find Command Options

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords and arguments. To display keywords and arguments for a command, enter a question mark (?) at the configuration prompt or after entering part of a command followed by a space. The Cisco IOS software displays a list and brief description of available keywords and arguments. For example, if you were in global configuration mode and wanted to see all the keywords or arguments for the **arap** command, you would type **arap ?**.

The <cr> symbol in command help output stands for “carriage return.” On older keyboards, the carriage return key is the Return key. On most modern keyboards, the carriage return key is the Enter key. The <cr> symbol at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by itself indicates that no more arguments or keywords are available and that you must press **Enter** to complete the command.

Table 2 shows examples of how you can use the question mark (?) to assist you in entering commands. The table steps you through configuring an IP address on a serial interface on a Cisco 7206 router that is running Cisco IOS Release 12.0(3).

**Table 2** How to Find Command Options

Command	Comment
<pre>Router&gt; enable Password: &lt;password&gt; Router#</pre>	Enter the <b>enable</b> command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to Router#.
<pre>Router# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#</pre>	Enter the <b>configure terminal</b> privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to Router(config)#.
<pre>Router(config)# interface serial ? &lt;0-6&gt;      Serial interface number Router(config)# interface serial 4 ? / Router(config)# interface serial 4/ ? &lt;0-3&gt;      Serial interface number Router(config)# interface serial 4/0 Router(config-if)#</pre>	<p>Enter interface configuration mode by specifying the serial interface that you want to configure using the <b>interface serial</b> global configuration command.</p> <p>Enter ? to display what you must enter next on the command line. In this example, you must enter the serial interface slot number and port number, separated by a forward slash.</p> <p>You are in interface configuration mode when the prompt changes to Router(config-if)#.</p>

**Table 2** How to Find Command Options (continued)

Command	Comment
<pre>Router(config-if)# ? Interface configuration commands: . . . ip                Interface Internet Protocol config commands keepalive         Enable keepalive lan-name          LAN Name command llc2              LLC2 Interface Subcommands load-interval     Specify interval for load calculation for an                   interface locaddr-priority  Assign a priority group logging           Configure logging for interface loopback          Configure internal loopback on an interface mac-address       Manually set interface MAC address mls               mls router sub/interface commands mpoa              MPOA interface configuration commands mtu               Set the interface Maximum Transmission Unit (MTU) netbios           Use a defined NETBIOS access list or enable                   name-caching no                Negate a command or set its defaults nrzi-encoding     Enable use of NRZI encoding ntp               Configure NTP . . . Router(config-if)#</pre>	<p>Enter ? to display a list of all the interface configuration commands available for the serial interface. This example shows only some of the available interface configuration commands.</p>
<pre>Router(config-if)# ip ? Interface IP configuration subcommands: access-group      Specify access control for packets accounting        Enable IP accounting on this interface address           Set the IP address of an interface authentication    authentication subcommands bandwidth-percent Set EIGRP bandwidth limit broadcast-address Set the broadcast address of an interface cgmp              Enable/disable CGMP directed-broadcast Enable forwarding of directed broadcasts dvmrp            DVMRP interface commands hello-interval    Configures IP-EIGRP hello interval helper-address    Specify a destination address for UDP broadcasts hold-time         Configures IP-EIGRP hold time . . . Router(config-if)# ip</pre>	<p>Enter the command that you want to configure for the interface. This example uses the <b>ip</b> command.</p> <p>Enter ? to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.</p>

**Table 2** How to Find Command Options (continued)

Command	Comment
<pre>Router(config-if)# ip address ? A.B.C.D          IP address negotiated       IP Address negotiated over PPP Router(config-if)# ip address</pre>	<p>Enter the command that you want to configure for the interface. This example uses the <b>ip address</b> command.</p> <p>Enter <b>?</b> to display what you must enter next on the command line. In this example, you must enter an IP address or the <b>negotiated</b> keyword.</p> <p>A carriage return (&lt;cr&gt;) is not displayed; therefore, you must enter additional keywords or arguments to complete the command.</p>
<pre>Router(config-if)# ip address 172.16.0.1 ? A.B.C.D          IP subnet mask Router(config-if)# ip address 172.16.0.1</pre>	<p>Enter the keyword or argument you want to use. This example uses the 172.16.0.1 IP address.</p> <p>Enter <b>?</b> to display what you must enter next on the command line. In this example, you must enter an IP subnet mask.</p> <p>A &lt;cr&gt; is not displayed; therefore, you must enter additional keywords or arguments to complete the command.</p>
<pre>Router(config-if)# ip address 172.16.0.1 255.255.255.0 ? secondary       Make this IP address a secondary address &lt;cr&gt; Router(config-if)# ip address 172.16.0.1 255.255.255.0</pre>	<p>Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask.</p> <p>Enter <b>?</b> to display what you must enter next on the command line. In this example, you can enter the <b>secondary</b> keyword, or you can press <b>Enter</b>.</p> <p>A &lt;cr&gt; is displayed; you can press <b>Enter</b> to complete the command, or you can enter another keyword.</p>
<pre>Router(config-if)# ip address 172.16.0.1 255.255.255.0 Router(config-if)#</pre>	<p>In this example, Enter is pressed to complete the command.</p>

## Using the no and default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to reenable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip routing** command; to reenable IP routing, use the **ip routing** command. The Cisco IOS software command reference publications provide the complete syntax for the configuration commands and describe what the **no** form of a command does.

Configuration commands also can have a **default** form, which returns the command settings to the default values. Most commands are disabled by default, so in such cases using the **default** form has the same result as using the **no** form of the command. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** form of the command enables the command and sets the variables to their default values. The Cisco IOS software command reference publications describe the effect of the **default** form of a command if the command functions differently than the **no** form.

## Saving Configuration Changes

Use the **copy system:running-config nvram:startup-config** command to save your configuration changes to the startup configuration so that the changes will not be lost if the software reloads or a power outage occurs. For example:

```
Router# copy system:running-config nvram:startup-config
Building configuration...
```

It might take a minute or two to save the configuration. After the configuration has been saved, the following output appears:

```
[OK]
Router#
```

On most platforms, this task saves the configuration to NVRAM. On the Class A Flash file system platforms, this task saves the configuration to the location specified by the CONFIG\_FILE environment variable. The CONFIG\_FILE variable defaults to NVRAM.

## Filtering Output from the show and more Commands

In Cisco IOS Release 12.0(1)T and later releases, you can search and filter the output of **show** and **more** commands. This functionality is useful if you need to sort through large amounts of output or if you want to exclude output that you need not see.

To use this functionality, enter a **show** or **more** command followed by the “pipe” character (|); one of the keywords **begin**, **include**, or **exclude**; and a regular expression on which you want to search or filter (the expression is case-sensitive):

```
command | {begin | include | exclude} regular-expression
```

The output matches certain lines of information in the configuration file. The following example illustrates how to use output modifiers with the **show interface** command when you want the output to include only lines in which the expression “protocol” appears:

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

For more information on the search and filter functionality, refer to the “Using the Command-Line Interface” chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

# Identifying Platform Support for Cisco IOS Software Features

Cisco IOS software is packaged in feature sets consisting of software images intended for specific routing and switching platforms. The feature sets available for a specific hardware platform depend on which Cisco IOS software images are included in a release. Information in the following sections will help you identify the set of software images available in a specific release or to determine if a feature is available in a given Cisco IOS software image:

- Using Feature Navigator
- Using Software Release Notes

## Using Feature Navigator

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image.

Feature Navigator is available 24 hours a day, 7 days a week. To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at [cdbadmin@cisco.com](mailto:cdbadmin@cisco.com). If you do not have an account on Cisco.com, go to <http://www.cisco.com/register> and follow the directions to establish an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

<http://www.cisco.com/go/fn>

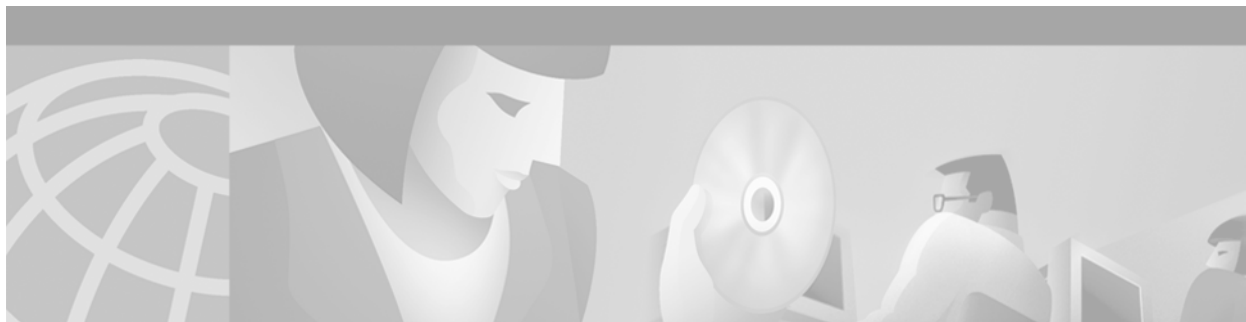
## Using Software Release Notes

Cisco IOS software releases include release notes that provide the following information:

- Platform support information
- Memory recommendations
- Microcode support information
- Feature set tables
- Feature descriptions
- Open and resolved severity 1 and 2 caveats for all platforms

Release notes are intended to be release-specific for the most current release, and the information provided in these documents may not be cumulative in providing information about features that first appeared in previous releases.





## Mobile Wireless Overview

---

A fast-paced technological transition is occurring today in the world of internetworking. This transition is marked by the convergence of the telecommunications infrastructure with that of IP data networking to provide integrated voice, video, and data services.

As this transition progresses, the standards are continuing to evolve and many new standards are being developed to enable and accelerate this convergence of telecommunications and IP networking to mobilize the internet and provide new multimedia services.

The *Cisco IOS Mobile Wireless Configuration Guide* discusses the technologies implemented in the Cisco IOS software that support mobile wireless communication and IP data services in a mobile wireless environment.

This chapter includes the following sections:

- [Introduction to Mobile Wireless Technology, page 1](#)
- [Model for IP Integration into Mobile Wireless, page 5](#)
- [Mobile Wireless in Cisco IOS Software, page 7](#)

## Introduction to Mobile Wireless Technology

The technologies related to wireless communication can be complex to differentiate. Wireless technology has been around for a while; however, there has been a relatively recent and rapid surge in the evolution of new wireless standards to support the convergence of voice, video and data communication. Much of this rapid evolution, or revolution, is a result of people seeking ubiquitous and immediate access to information and the assimilation of the internet into business practices and for personal use. People “on the go” want their internet access to move with them, so that their information is available at anytime, anywhere.

There are many factors that can be used to characterize wireless technologies:

- Spectrum, or the range of frequencies in which the network operates
- Transmission speeds supported
- Underlying transmission mechanism, such as frequency division multiple access (FDMA), time division multiple access (TDMA), or code division multiple access (CDMA)
- Architectural implementation, such as enterprise based (or in-building), fixed, or mobile

In addition, the mobile wireless technologies [such as Global System for Mobile Communications (GSM), TDMA, CDMA] are differentiated by a number of different factors, including some of the following:

- Control of the transmitted power
- Radio resource management and channel allocation
- Coding algorithms
- Network topology and frequency reuse
- Handoff mechanisms

The *Cisco IOS Mobile Wireless Configuration Guide* focuses on technologies that are directly related to the mobile wireless segment of wireless communication. As suggested by its name, mobile wireless communication addresses those wireless technologies that support mobility of a subscriber, which provide seamless and real-time services without interruption. Mobile wireless technologies support network access whether subscribers roam within or outside their home wireless coverage area.

## Overview of Basic Network Elements Associated with Cellular Networks and Mobile Wireless

This section provides a brief introduction to a few of the basic network components associated with the existing telecommunications infrastructure. It specifically discusses the existing mobile wireless network infrastructure components for TDM-based wireless networks, some of which eventually will be replaced by new IP-based components.

In the early 1980s, support for mobile wireless communications was introduced using cellular networks, which were based on analog technologies such as AMPS. Many of the telecommunications entities associated with cellular networks still play a vital role in today's wireless networks. As wireless communications technologies continue to progress and IP data networking is further integrated into the existing infrastructure, some of the functions of these entities might still exist within the network, but will be implemented in different and more effective ways.

The following network elements are part of a typical cellular telecommunications network:

- [Public Switched Telephone Network \(PSTN\)](#)
- [Mobile Switching Center \(MSC\)](#)
- [Base Station \(BS\)](#)
- [Radio Access Network \(RAN\)](#)
- [Home Location Register \(HLR\)](#)
- [Visitor Location Register \(VLR\)](#)
- [Authentication Center \(AC\)](#)

### Public Switched Telephone Network (PSTN)

The PSTN is the foundation and remains the predominant infrastructure that currently supports the connection of millions of subscribers worldwide. The PSTN has several thousands of miles of transmission infrastructure, including fixed land lines, microwave, and satellite links. After the introduction of cellular telephone systems in the early and mid-1980s, and with the rapid development of mobile wireless communication services, the PSTN still provides the fixed network support using the Signaling System Number 7 (SS7) protocol to carry control and signaling messages in a packet-switched environment.

### Mobile Switching Center (MSC)

The MSC, usually located at the Mobile Telephone Switching Office (MTSO), is part of the mobile wireless network infrastructure that provides the following services:

- Switches voice traffic from the wireless network to the PSTN if the call is a mobile-to-landline call, or it switches to another MSC within the wireless network if the call is a mobile-to-mobile call.
- Provides telephony switching services and controls calls between telephone and data systems.
- Provides the mobility functions for the network and serves as the hub for up to as many as 100 BSs.

More specifically, the MSC provides the following functions:

- Mobility management for the subscribers (to register subscribers, to authenticate and authorize the subscribers for services and access to the network, to maintain the information on the temporary location of the subscribers so they can receive and originate voice calls).

In GSM, some of the functionality of the MSC is distributed to the Base Station Controller (BSC). In TDMA, the BSC and the MSC are integrated.

- Call setup services (call routing based on the called number). These calls can be to another mobile subscriber through another MSC, or to a landline user through the PSTN.
- Connection control services, which determine how calls are routed and establishes trunks to carry the bearer traffic to another MSC or to the PSTN.
- Service logic functions, which route the call to the requested service for the subscriber, such as an 800 service, call forwarding, or voicemail.
- Transcoding functions, which decompress the voice traffic from the mobile device going to the PSTN and compresses the traffic going from the PSTN to the mobile device.

### Base Station (BS)

The BS is the component of the mobile wireless network access infrastructure that terminates the air interface over which the subscriber traffic is transmitted to and from a mobile station (MS).

In GSM-based networks, the BS is called a Base Transceiver Station (BTS).

### Radio Access Network (RAN)

The RAN identifies the portion of the wireless network that handles the radio frequencies (RF), Radio Resource Management (RRM), which involves signaling, and the data synchronization aspects of transmission over the air interface.

In GSM-based networks, the RAN typically consists of BTSs and Base Station Controllers (BSCs). User sessions are connected from a mobile station to a BTS, which connects to a BSC. The combined functions of the BTS and BSC are referred to as the Base Station Subsystem (BSS).

### Home Location Register (HLR)

The HLR is a database that contains information about subscribers to a mobile network that is maintained by a particular service provider. In addition, for subscribers of a roaming partner, the HLR might contain the service profiles of visiting subscribers.

The MSC uses the subscriber information supplied by the HLR to authenticate and register the subscriber. The HLR stores “permanent” subscriber information (rather than temporary subscriber data, which a VLR manages), including the service profile, location information, and activity status of the mobile user.

**Visitor Location Register (VLR)**

The VLR is a database that is maintained by an MSC, to store temporary information about subscribers who roam into the coverage area of that MSC.

The VLR, which is usually part of an MSC, communicates with the HLR of the roaming subscriber to request data, and to maintain information about the subscriber's current location in the network.

**Authentication Center (AC)**

The AC provides handset authentication and encryption services for a service provider. In most wireless networks today, the AC is collocated with the HLR, and is often implemented as part of the HLR complex.

## Wireless Standards Development

This section discusses the evolution of some of the wireless networking standards and the types of services they support.

The phased evolution of wireless networking standards are referred to as generations:

- **1G**—First generation. 1G refers to the initial category of mobile wireless networks that used only analog technology and were developed primarily for voice services. Advanced Mobile Phone Service (AMPS) is an example of a 1G mobile network standard.
- **2G**—Second generation. 2G refers generically to a category of mobile wireless networks and services that use digital technology. 2G wireless networks introduce support for data services. GSM, TDMA and CDMA are examples of 2G mobile network standards.
- **2G+**—Second generation plus. 2G+ refers generically to a category of mobile wireless networks that have a packet data overlay built on top of the circuit-switched voice network to support higher data rates than 2G mobile networks (2G networks support data in a circuit-switched model). General Packet Radio Service (GPRS) is an example of a 2G+ mobile network standard.

There is a similar packet data overlay concept for CDMA called Packet Data Services Node (PDSN), but this is considered 3G as part of the CDMA 1x solution.

- **3G**—Third generation. 3G refers generically to a category of next-generation mobile networks which operate at a higher frequency bandwidth (typically 2.1 GHz and higher) and have a larger channel bandwidth. This enables 3G networks to support very high data rates, up to 2 Mbps. With the higher bandwidth, more data and multimedia services are possible. 3G refers to the radio network and RF technology, and does not affect the switching core. The switching infrastructure for 3G is still based on MSCs and the TDM model.

The Universal Mobile Telephone Service (UMTS), based on the Wideband CDMA (W-CDMA) R-99 and CDMA 2000, are examples of 3G radio networks that are being developed to fulfill the requirements in the International Mobile Telecommunications-2000 (IMT-2000) standard by the International Telecommunication Union (ITU).

- 3G+—Third generation plus. 3G+ refers to an advanced level of 3G that introduces the concept of an all-IP switching core. An all-IP switching core means that IP replaces the TDM-based MSC infrastructure with IP-based transport and IP-based signaling. IP-based signaling is implemented with new protocols like Session Initiation Protocol (SIP) and Media Gateway Control Protocol (MGCP). In 3G+ networks, the traditional MSC implementation goes away and the various MSC functions are redistributed to several other elements. A good example of this evolution in the switching core from TDM to packets is 3GPP's R4 and R5 architecture. 3GPP2 also has adopted a similar trend to transition to an all-IP network.

There are also initiatives under way to develop and migrate to a true end-to-end, all-IP mobile wireless network where both the switching core and the RAN are IP based. This evolution is being loosely referred to as R6 in 3G terminology.

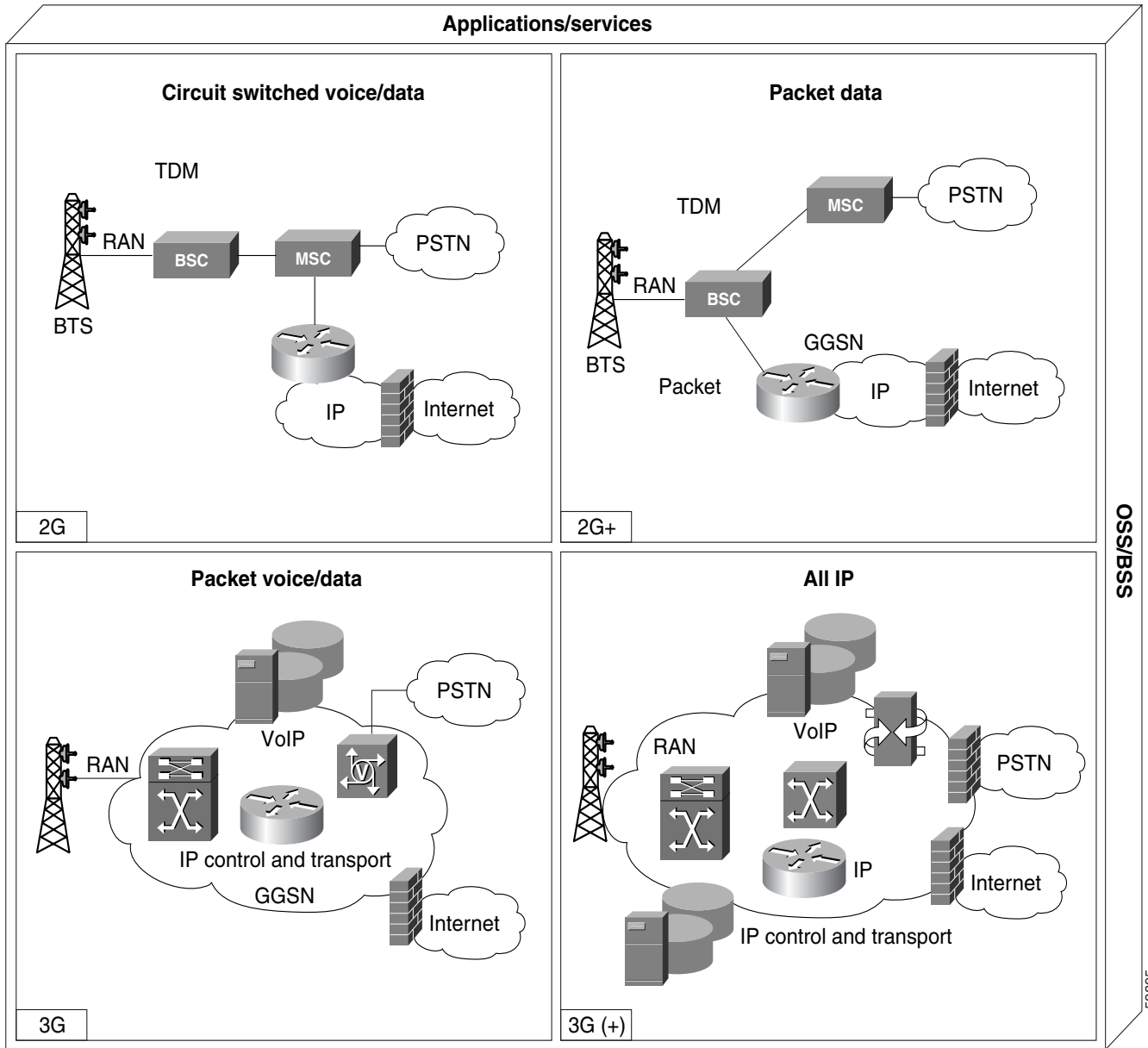
## Model for IP Integration into Mobile Wireless

The standards for the integration of IP data networking with the existing telecommunications infrastructure are rapidly developing and beginning to be realized in today's production networks.

[Figure 1](#) shows a model for IP integration based upon the current industry direction and reflects some of the latest ideas within the Mobile Wireless Internet Forum (MWIF). The MWIF is a pre-standards consortium for service providers and suppliers to collaborate on the implementation of IP-based mobile wireless networks. The MWIF influences the standards bodies such as 3GPP and 3GPP2 to successfully adopt new implementations.

In particular, [Figure 1](#) shows where Cisco Systems' GGSN product for GSM networks fits into the model.

**Figure 1 IP Integration Phases in Mobile Wireless**



The top two quadrants in [Figure 1](#) show where we are today in the telecommunications and IP data services infrastructures. The first quadrant represents the first phase of these infrastructures based on circuit-switched voice and data services. The beginnings of a core IP transport for voice and data integration can be built using Cisco Systems V.110 solutions.

The second quadrant depicts the implementation phase of 2G+ technologies, such as GPRS, supporting higher transmission speeds. In this quadrant, the Cisco Systems GGSN provides IP packet data services. It acts as an IP gateway for access to the internet and other public and private data networks for traffic that is initiated in a GSM-based mobile environment. The services anticipated in this phase include

implementing always-on data services and enabling operators to charge by packet rather than connect time. Similar services are supported by Packet Data Services Node (PDSN), for CDMA-based wireless networks.

The third quadrant represents phase three of the integration of IP networking where voice and data are consolidated onto a packet-based infrastructure from the RAN or radio network control (RNC) outward. This is considered a 3G solution. Phase three enables integrated voice and data applications and reduces costs. In addition, some of the components or functions of the MSC are distributed.

The fourth quadrant represents the final phase, which includes 3G services plus the implementation of IP-based radio and mobility components to develop a true end-to-end, all-IP wireless network solution.

## Mobile Wireless in Cisco IOS Software

Cisco Systems has a variety of products that provide wireless communications services and that can be used together as solutions for different network environments and needs. Some of these products provide fixed wireless IP data services and others address mobile wireless IP data services. Some reside in Cisco IOS software and others do not.

The *Cisco IOS Mobile Wireless Configuration Guide* focuses on a portion of the wireless communications services provided by the Cisco IOS software. It describes the segment of wireless products that provide *mobile* wireless communications services. This first version of the book describes a product that supports IP data services in a mobile environment.



### Note

---

The Cisco IOS software also supports the mobile IP protocol, which is not documented in this book. For more information about mobile IP, refer to the *Cisco IOS IP Configuration Guide*.

---

## IP Data Services

This section describes the first GSM-based technology implemented in the Cisco IOS software for IP data services in mobile wireless networks—GPRS.

### GPRS

GPRS is a new service designed for GSM networks. GSM is a digital cellular technology that is used worldwide, predominantly in Europe and Asia, with current estimates of 400 million subscribers and growing. GSM is the world's leading standard in digital wireless communications.

GPRS is standardized by the European Telecommunications Standards Institute (ETSI). The most common application of GPRS is expected to be Internet/intranet access. Cisco Systems' GPRS solution enables mobile wireless service providers to supply their mobile subscribers with packet data services.

A GPRS network has two essential elements:

- Serving GPRS Support Node (SGSN)—Sends data to and receives data from mobile stations, and maintains information about the location of a mobile station (MS). The SGSN communicates between the MS and the GGSN. SGSN support is available from Cisco partners or other vendors.
- Gateway GPRS Support Node (GGSN)—A wireless gateway that allows mobile cell phone users to access the public data network (PDN) or specified private IP networks. The GGSN function is implemented on the Cisco Systems' router.

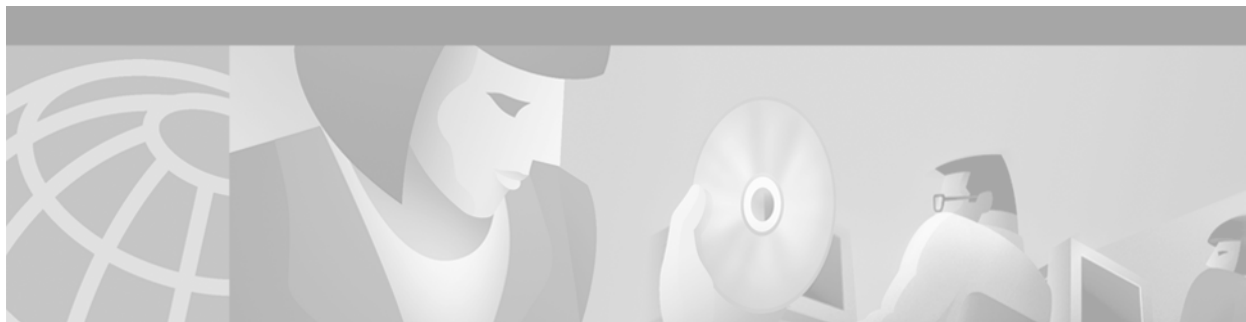
Cisco Systems is recognized as the first to market a viable GGSN product. GGSN support is available in the GPRS feature in Cisco IOS software.

The GPRS part of this *Cisco IOS Mobile Wireless Configuration Guide* describes how to configure a Cisco Systems router to function as a GGSN. While the documentation provides a brief overview of the GPRS technology and its benefits, the primary purpose of this documentation is to provide you with the necessary information to configure, verify, and monitor the GGSN portion of your GPRS network. It does not describe all of the planning considerations that might be involved in setting up your GPRS network.



**General Packet Radio Service  
(GPRS)**





## Overview of GPRS

---

This chapter provides a brief introduction to the General Packet Radio Service (GPRS) technology and its implementation in the Cisco IOS software.

This chapter includes the following sections:

- [Overview, page 11](#)
- [Benefits, page 14](#)

### Overview

GPRS is a new service designed for Global System for Mobile Communications (GSM) networks. GSM is a digital cellular technology that is used worldwide, predominantly in Europe and Asia, with current estimates of 400 million subscribers and growing. GSM is the world's leading standard in digital wireless communications.

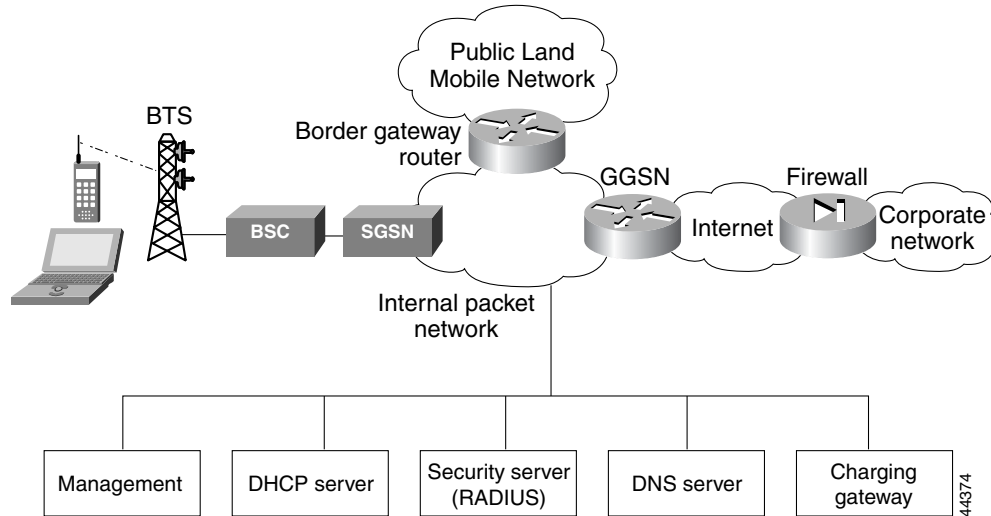
GPRS is standardized by the European Telecommunications Standards Institute (ETSI). The most common application of GPRS is expected to be Internet/intranet access. Cisco Systems' GPRS solution enables mobile wireless service providers to supply their mobile subscribers with packet-based data services in GSM networks.

GPRS introduces the following two new major network elements:

- **SGSN**—Sends data to and receives data from mobile stations, and maintains information about the location of a mobile station (MS). The SGSN communicates between the MS and the GGSN. SGSN support is available from Cisco partners or other vendors.
- **GGSN**—A wireless gateway that allows mobile cell phone users to access the public data network (PDN) or specified private IP networks. The GGSN function is implemented on the Cisco Systems' router.

Figure 2 provides a view of the basic GPRS network components. The functions shown in boxes beneath the network show the different types of network services that are commonly used in a GPRS network.

**Figure 2 GPRS Network Components**



User sessions are connected from a mobile station to a Base Transceiver Station (BTS), which connects to a Base Station Controller (BSC). The combined functions of the BTS and BSC are referred to as the Base Station Subsystem (BSS). From there, the SGSN provides access to the GGSN, which serves as the gateway to the data network.

Multiple SGSNs and GGSNs within a GPRS network are referred to collectively as GPRS Support Nodes (GSNs). The connection between the SGSN and the GGSN is enabled through a protocol called the GPRS Tunneling Protocol (GTP). The connection between the GGSN and the PDN is enabled through the Internet Protocol (IP).

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

In Cisco IOS Release 12.1(5)T and later, the GGSN (with an Industry-Standard Architecture (ISA) card), supports the IP security protocol (IPSec) to provide data confidentiality, data integrity, and data authentication between participating peers.

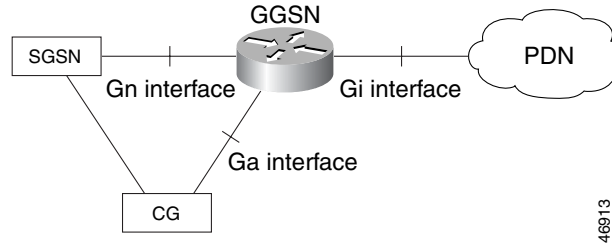
### GPRS Interface Reference Model

The GPRS standards use the term *interface* to label (or identify) the communication path between different GPRS network elements. The GPRS standards define the requirements and characteristics of communication between different GPRS network elements over these interfaces. These interfaces are commonly referred to when describing aspects of a GPRS network.

Figure 3 shows the GPRS interfaces that are implemented in the Cisco IOS GPRS feature:

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

**Figure 3 GPRS Interfaces Implemented in the Cisco IOS GPRS Feature**



46913

### Virtual Template Interface

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

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

### Access Points

The GPRS standards define a network identity called an access point name (APN). An APN identifies a PDN that is configured on and accessible from a GGSN in a GPRS network. To configure APNs, the Cisco Systems GPRS software uses the following configuration elements:

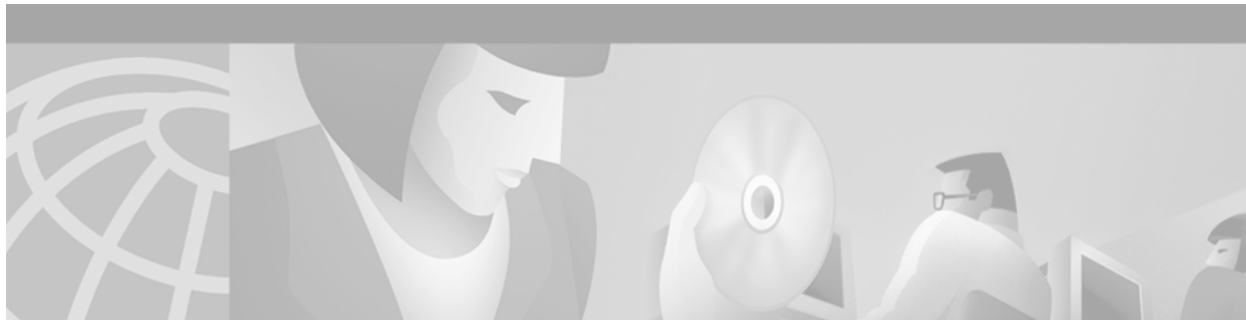
- Access point—Defines an APN and its associated access characteristics, including security and method of dynamic addressing.
- Access point list—Logical interface that is associated with the virtual template of the GGSN. Each access-point list contains one or more access points.
- Access group—An additional level of 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.

For more detailed information on access-point configuration, refer to the [“Configuring the GPRS Access Point List on the GGSN”](#) section on page 27 in the [“Configuring Network Access to the GGSN”](#) chapter.

# Benefits

The GPRS technology provides the following benefits:

- Enables the use of a packet-based air interface over the existing circuit-switched GSM network, which allows greater efficiency in the radio spectrum because the radio bandwidth is used only when packets are sent or received.
- Supports minimal upgrades to the existing GSM network infrastructure for those network service providers who want to add GPRS services on top of GSM, which is currently widely deployed.
- Supports data rates of about 115 Kbps, which is greater than the traditional 9.6 Kbps rate available in a circuit-switched connection.
- Supports larger message lengths than Short Message Services (SMS).
- Supports virtual private network (VPN)/Internet service provider (ISP) corporate site access.



## Planning to Configure the GGSN

---

This chapter describes information that you should know before configuring the Gateway General Packet Radio Service (GPRS) Support Node (GGSN).

This chapter includes the following sections:

- [Prerequisites, page 15](#)
- [Restrictions, page 15](#)
- [Supported Platforms, page 16](#)
- [Supported Standards, MIBs, and RFCs, page 16](#)
- [Related Documents, page 16](#)

### Prerequisites

#### Planning Your Access Point Configuration

Before you begin to configure the GGSN on your router, you should know which networks your mobile users will be allowed to access using the GGSN. Once you identify the networks, you can plan the physical interfaces to configure on the router for those networks. Then you can 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 World Wide Web through a 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 private intranet.

### Restrictions

Before configuring GGSN, please note the following:

- By default, Cisco Express Forwarding (CEF) switching is enabled in GPRS Release 1.4 in Cisco IOS Release 12.2 and earlier. However, CEF is not supported in GPRS Release 1.4 in Cisco IOS Release 12.2 and earlier. Therefore, ensure that CEF is not configured on your GGSN router by issuing the **no ip cef** command while in global configuration mode.
- The following list shows the maximum number of PDP contexts that are supported on the GGSN according to the router series and amount of memory:
  - Cisco 7206 router with 128Mb RAM—45,000 PDP contexts.
  - Cisco 7206 VXR NPE-300 router with 256 Mb RAM—90,000 PDP contexts.

## Supported Platforms

To identify the hardware platform or software image information associated with the GPRS feature, use the Feature Navigator on Cisco.com to search for information about the feature, or refer to the software release notes for a specific release. For more details on how to use the Feature Navigator, see the “Identifying Platform Support for Cisco IOS Software Features” section on page xxi in the “Using Cisco IOS Software” chapter.

## Supported Standards, MIBs, and RFCs

### Standards

GPRS Release 1.4 supports the following ETSI standards:

- GSM 02.60 v6.3.0
- GSM 03.6.0 v6.7.0
- GSM 04.08 v6.9.0
- GSM 09.60 v6.6.0
- GSM 09.61 v6.4.0
- GSM 12.15 v7.1.0

The GPRS Gn interface complies with SMG#31 R97, and the Ga interface complies with SMG#29 R98 (12.15 v7.1.0).

### MIBs

- CISCO-GPRS-ISGSN-MIB
- CISCO-GPRS-L2RLY-MIB
- CISCO-GPRS-GTP-MIB

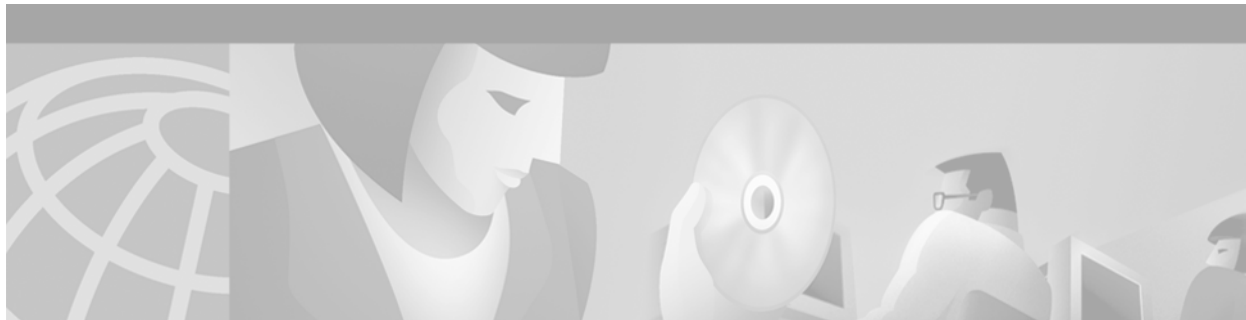
For descriptions of other supported MIBs and how to use MIBs, see the Cisco MIB web site on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

### RFCs

None.

## Related Documents

- *Cisco IOS Interface Configuration Guide*
- *Cisco IOS Interface Command Reference*
- *Cisco IOS IP Configuration Guide*
- *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*
- *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*
- *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*
- *Cisco IOS Security Configuration Guide*
- *Cisco IOS Security Command Reference*



## Configuring GGSN Services

---

This chapter describes how to configure a Cisco router as a Gateway GPRS Support Node (GGSN). For a complete description of the GPRS commands in this chapter, refer to the *Cisco IOS Mobile Wireless Command Reference*. 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 the GGSN, page 17](#) (Required)
- [Customizing the GPRS Configuration, page 19](#) (Optional)

### Configuring the GGSN

GPRS uses a logical interface called a virtual template to configure the router as a GGSN. This section describes the primary commands used to configure the router for GGSN services. Once the router has been configured as a GGSN, the subsequent configuration tasks describe how to establish connectivity from the GGSN to the SGSN and PDNs.

The following requirements must be met when configuring the GGSN on a Cisco Systems router:

- Configure only a single GGSN entity on each router using the **service gprs ggsn** global configuration command.
- Configure only a single virtual template interface (as virtual template 1) with GTP encapsulation on the GGSN.
- Configure the IP address of the virtual template for the GGSN on a different network than the physical interfaces that are configured on the router.
- Disable CEF switching using the **no ip cef** command while in global configuration mode. By default, CEF is enabled in GPRS 1.4 in Cisco IOS Release 12.2 and earlier. However, CEF is not supported in GPRS 1.4 in Cisco IOS Release 12.2 and earlier. Therefore, ensure CEF is not configured on your GGSN router.

To configure the GGSN, issue the following commands beginning in global configuration mode:

	Command	Purpose
<b>Step 1</b>	<code>router(config)# <b>service gprs ggsn</b></code>	Specifies that the router functions as a GGSN.
<b>Step 2</b>	<code>router(config)# <b>interface virtual-template</b> <i>number</i></code>	Creates a virtual template interface, where <i>number</i> identifies the virtual template interface. This command enters you into interface configuration mode.  <b>Note</b> The GGSN supports only a single virtual template for the GTP virtual interface.
<b>Step 3</b>	<code>router(config-if)# <b>ip address</b> <i>ip-address mask</i> [<b>secondary</b>]</code>	Specifies an IP address for the interface.  <b>Note</b> The IP address of the virtual template interface must be on a different network than the physical interfaces on the GGSN.
<b>Step 4</b>	<code>router(config-if)# <b>encapsulation gtp</b></code>	Specifies GTP as the encapsulation type for packets transmitted over the virtual template interface.
<b>Step 5</b>	<code>router(config-if)# <b>gprs fastswitch</b></code>	(Optional) Enables fast switching on the GTP virtual template interface.

## Customizing the GPRS Configuration

In addition to the commands used to configure the router for GGSN support, the GPRS feature supports several optional commands that you can use to customize your GPRS and GTP configuration.

For certain GPRS GTP processing options, the default values represent recommended values. Other optional commands also are set to default values, but Cisco Systems recommends modifying these commands to optimize your network as necessary, or according to your router hardware.

Some of the parameters that you should consider optimizing are configured using the following global configuration commands:

Command	Purpose
<code>router(config)# <b>gprs gtp n3-requests</b> requests</code>	Specifies the maximum number of times that the GGSN attempts to send a signaling request.
<code>router(config)# <b>gprs gtp path-echo-interval</b> interval</code>	Specifies the number of seconds that the GGSN waits before sending an echo-request message to check for GTP path failure.
<code>router(config)# <b>gprs gtp t3-response</b> response_interval</code>	Specifies the maximum time that the GGSN waits for a response from a signaling request message.
<code>router(config)# <b>gprs maximum-pdp-context-allowed</b> pdp_contexts</code>	Specifies the maximum number of PDP contexts (mobile sessions) that can be activated on the GGSN.

For information about configuring GPRS charging options, see the [“Customizing the Charging Gateway”](#) section on page 23 in the [“Configuring Charging on the GGSN”](#) chapter.





## Configuring Charging on the GGSN

This chapter describes how to configure the charging function on the GGSN. Charging processing is enabled by default on the GGSN. There are several ways to customize communication with a charging gateway. Many of the default values for the charging options will provide a satisfactory configuration until you become more familiar with your network and decide to customize the charging interface.

For a complete description of the GPRS commands in this chapter, refer to the *Cisco IOS Mobile Wireless Command Reference*. 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 the Charging Gateway, page 21](#) (Required)
- [Configuring the Transport Protocol for the Charging Gateway, page 22](#) (Optional)
- [Customizing the Charging Gateway, page 23](#) (Optional)
- [Disabling Charging Processing, page 24](#) (Optional)

## Configuring the Charging Gateway

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

Command	Purpose
<pre>router(config)# gprs default charging-gateway {ip-address   name} [{ip-address   name}]</pre>	<p>Specifies a primary charging gateway (and backup), where:</p> <ul style="list-style-type: none"><li>• <i>ip-address</i>—Specifies the IP address of a charging gateway. The second (optional) <i>ip-address</i> argument specifies the IP address of a secondary charging gateway.</li><li>• <i>name</i>—Specifies the host name of a charging gateway. The second (optional) <i>name</i> argument specifies the host name of a secondary charging gateway.</li></ul>

## Changing the Default Charging Gateway

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

	Command	Purpose
Step 1	<code>router(config)# gprs default charging-gateway 10.1.1.1</code>	Specifies a primary charging gateway at IP address 10.1.1.1.
Step 2	<code>router(config)# no gprs default charging-gateway 10.1.1.1</code>	Removes the primary charging gateway at IP address 10.1.1.1.
Step 3	<code>router(config)# gprs default charging-gateway 10.2.2.2</code>	Specifies the new default primary charging gateway at IP address 10.2.2.2.

## Configuring the Transport Protocol for the Charging Gateway

You can configure the 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 GPRS default configuration specifies UDP, which is 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	<code>router(config)# gprs charging path-protocol tcp</code>	Specifies that the TCP networking protocol is used by the GGSN to transmit and receive charging data.
Step 2	<code>router(config)# gprs charging cg-path-requests 1</code>	Specifies that the GGSN waits 1 minute before retrying a request over the data path to the charging gateway.

### Configuring UDP as the Charging Gateway Path Protocol

The GPRS default configuration specifies UDP as the transport path protocol to the charging gateway. If you need to reconfigure the charging gateway for UDP transport, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>router(config)# gprs charging path-protocol udp</code>	Specifies that the UDP networking protocol is used by the GGSN to transmit and receive charging data. The default value is UDP.
Step 2	<code>router(config)# gprs gtp path-echo-interval interval</code>	Specifies the number of seconds that the GGSN waits before sending an echo-request message to check for GTP path failure. The default value is 60 seconds.

## Customizing the Charging Gateway

For the GPRS charging options, the default values represent recommended values. Other optional commands also are set to default values, but Cisco Systems recommends modifying these commands to optimize your network as necessary, or according to your router hardware.

Use the following global configuration commands to fine-tune charging processing on the GGSN:

Command	Purpose
<code>router(config)# gprs charging cdr-aggregation-limit <i>CDR_limit</i></code>	Specifies the maximum number of CDRs that the GGSN aggregates in a charging data transfer message to a charging gateway.
<code>router(config)# gprs charging cdr-option local-record-sequence-number</code>	Enables the GGSN to use the local record sequence number field in G-CDRs.
<code>router(config)# gprs charging cdr-option node-id</code>	Enables the GGSN to specify the node that generated the CDR in the node ID field in G-CDRs.
<code>router(config)# gprs charging cdr-option no-partial-cdr-generation</code>	Disables the GGSN from creating non-primary partial G-CDRs.
<code>router(config)# gprs charging cdr-option packet-count</code>	Enables the GGSN to provide uplink and downlink packet counts in the optional record extension field in G-CDRs.
<code>router(config)# gprs charging cdr-option served-msisdn</code>	Enables the GGSN to provide the MSISDN number from the create PDP context request in G-CDRs.
<code>router(config)# gprs charging cg-path-requests <i>minutes</i></code>	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.
<code>router(config)# gprs charging container volume-threshold <i>threshold_value</i></code>	Specifies the maximum number of bytes that the GGSN maintains in a user's charging container before closing it and updating the CDR.
<code>router(config)# gprs charging disable</code>	Disables charging transactions on the GGSN.
<code>router(config)# gprs charging flow-control private-echo</code>	Implements an echo request with private extensions for maintaining flow control on packets transmitted to the charging gateway.
<code>router(config)# gprs charging map data tos <i>tos_value</i></code>	Specifies an IP ToS mapping for GPRS charging packets.
<code>router(config)# gprs charging packet-queue-size <i>queue_size</i></code>	Specifies the maximum number of unacknowledged charging data transfer requests that the GGSN maintains in its queue.
<code>router(config)# gprs charging path-protocol {udp   tcp}</code>	Specifies the protocol that the GGSN uses to transmit and receive charging data.
<code>router(config)# gprs charging server-switch-timer <i>seconds</i></code>	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.
<code>router(config)# gprs charging tariff-time <i>time</i></code>	Specifies a time of day when GPRS charging tariffs change.
<code>router(config)# gprs charging transfer interval <i>seconds</i></code>	Specifies the number of seconds that the GGSN waits before it transfers charging data to the charging gateway.

For information about configuring GPRS GTP options, see the [“Customizing the GPRS Configuration” section on page 19](#) in the [“Configuring GGSN Services”](#) chapter.

# Disabling Charging Processing



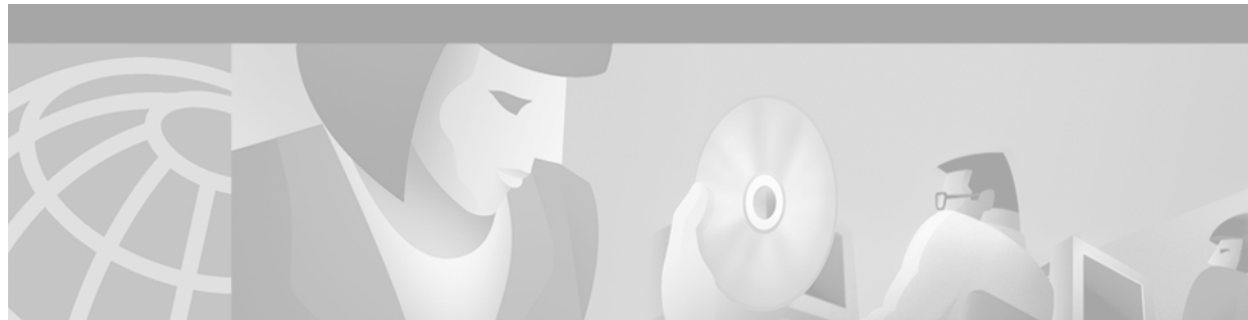
## Caution

The **gprs charging disable** command removes charging data processing on the GGSN, which means that the data required to bill customers for network usage is not being collected by the GGSN nor sent to the charging gateway. Cisco Systems, Inc. recommends that you avoid using this command in production GPRS network environments. When necessary to use this command, use it with extreme care and reserve its usage only under non-production network conditions.

You can disable charging on the GGSN only when all open CDRs have been processed and sent to the charging gateway. To clear the current GPRS CDRs, use the **clear gprs charging cdr** privileged EXEC command.

To disable charging processing on the GGSN, use the following command beginning in global configuration mode:

Command	Purpose
<code>router(config)# gprs charging disable</code>	Disables charging transactions on the GGSN.



## Configuring Network Access to the GGSN

This chapter describes how to configure access to an SGSN, PDN, and optionally to a VPN. It includes information about configuring access points on the GGSN.

For a complete description of the GPRS commands in this chapter, refer to the *Cisco IOS Mobile Wireless Command Reference*. 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 25](#) (Required)
- [Configuring a Route to the SGSN, page 26](#) (Required)
- [Configuring Access to a PDN, page 26](#) (Required)
- [Configuring the GPRS Access Point List on the GGSN, page 27](#) (Required)
- [Configuring Access to a VPN, page 29](#) (Optional)

## Configuring an Interface to the SGSN

The type of physical interface that you configure on the GGSN depends on whether you are supporting an SGSN that is collocated with a GGSN, or an enterprise GGSN that is connected to the SGSN through a WAN interface.

When a GGSN is collocated with the SGSN, the physical interface is frequently configured for Fast Ethernet. The supported WAN interfaces for a remote SGSN include T1/E1, T3/E3, and Frame Relay.

For more information about configuring physical interfaces on Cisco Systems' routers, see the *Cisco IOS Interface Configuration Guide* and the *Cisco IOS Interface Command Reference*.

To configure a physical interface to the SGSN that supports Fast Ethernet on a Cisco 7200 series router, issue the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>router(config)# <b>interface</b> type slot/port</code>	Defines a physical interface on the GGSN, where <i>type</i> is <b>fastethernet</b> , and <i>slot/port</i> is the hardware slot and port on the interface.
Step 2	<code>router(config-if)# <b>ip address</b> ip-address mask [secondary]</code>	Specifies an IP address for the interface.
Step 3	<code>router(config-if)# <b>ip route-cache</b></code>	(Optional) Configures fast switching on the interface to the SGSN.

## 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 physical interface.

For more information about configuring IP routes, see the *Cisco IOS IP Configuration Guide* and *Cisco IOS IP Command References*.

## Configuring a Static Route to the SGSN

A static route establishes a fixed route between the GGSN and the SGSN that is stored in the routing table.

To configure a static route from a physical interface on the GGSN to the SGSN, issue the following commands beginning in global configuration mode:

Command	Purpose
<pre>router(config)# ip route network-number network-mask {IP address   interface} [distance] [name name]</pre>	<p>Configures a static IP route. Typically, the following arguments are used for the Gn interface:</p> <ul style="list-style-type: none"> <li><i>network-number</i>—IP address of the SGSN.</li> <li><i>network-mask</i>—IP mask of the SGSN network.</li> <li><i>interface</i>—Physical interface on the GGSN for the Gn interface.</li> </ul>

## Configuring Access to a PDN

Configuring a connection to a public packet data network includes the following tasks:

- [Configuring an Interface to a PDN](#) (Gi interface)
- [Configuring an Access Point for a PDN](#)

## Configuring an Interface to a PDN

To configure a physical interface to the PDN using Fast Ethernet over the Gi interface, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>router(config)# <b>interface</b> type slot/port</code>	Defines a physical interface on the GGSN, where <i>type</i> is <b>fastethernet</b> , and <i>slot/port</i> is the hardware slot and port on the interface.
Step 2	<code>router(config-if)# <b>ip address</b> ip-address mask [secondary]</code>	Specifies an IP address for the interface.
Step 3	<code>router(config-if)# <b>ip route-cache</b></code>	(Optional) Configures fast switching on the interface to the PDN.

## Configuring an Access Point for a PDN

To configure an access point for a PDN, you must define an access point in the GPRS access point list.

For information about how to configure an access point in the GPRS access point list, see the [“Configuring the GPRS Access Point List on the GGSN”](#) section on page 27.

For an example of a GPRS access point configuration, see the [“Access Point List Configuration Example”](#) section on page 56 in the [“GGSN Configuration Examples”](#) chapter.

## 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 access points that the GGSN uses to communicate to PDNs (public or private) that are available over a Gi interface on the GGSN.

When you configure the GPRS access point list in global configuration mode, the GPRS 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.

### Viewing the Access Point List Configuration

After you configure the access point list, you can view the access point list configuration using the **show run** command. The output shows the **gprs access-point-list** command under both the virtual template interface and in the global configuration in the output from the **show run** command. However, note that the individual access points that you have configured within the access point list are shown only in the global configuration output area of the **show run** command.



#### Note

Be careful to observe that the GPRS access point list and an IP access list are different entities in the Cisco IOS software. A GPRS 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 access point list and configure access points within it, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>router(config)# <b>gprs access-point-list</b> list_name</code>	Specifies the access-point list name and enters access-point list configuration mode.
Step 2	<code>router(config-ap-list)# <b>access-point</b> ap_number</code>	Specifies a number associated with this access point definition and enters access point configuration mode.
Step 3	<code>router(config-access-point)# <b>access-point-name</b> apn_name</code>	Specifies a name associated with the access point.
Step 4	<code>router(config-access-point)# <b>access-mode</b> {transparent   non-transparent}</code>	(Optional) Specifies whether the GGSN requests user authentication at the access point to a PDN. The available options are: <ul style="list-style-type: none"> <li>• <b>transparent</b>—No security authorization or authentication is requested by the GGSN for this access point.</li> <li>• <b>non-transparent</b>—GGSN acts as a proxy for authenticating.</li> </ul>
Step 5	<code>router(config-access-point)# <b>access-violation</b> {discard-packets   deactivate-pdp-context}</code>	(Optional) Specifies the action to take when a user attempts unauthorized access to a PDN through an access point. The available options are: <ul style="list-style-type: none"> <li>• <b>discard-packets</b>—Discards user packets when an unauthorized access attempt is detected.</li> <li>• <b>deactivate-pdp-context</b>—Ends mobile session when an unauthorized access attempt is detected.</li> </ul>
Step 6	<code>router(config-access-point)# <b>dhcp-server</b> {ip-address   name} [{ip-address   name}]</code>	(Optional) Specifies a primary (and backup) DHCP server to allocate IP addresses to MS users entering a particular PDN access point.
Step 7	<code>router(config-access-point)# <b>dhcp-gateway-address</b> ip-address</code>	(Optional) Specifies a DHCP gateway to handle DHCP requests for MS users entering a particular PDN access point.
Step 8	<code>router(config-access-point)# <b>ip-access-group</b> access_list_number {in   out}</code>	(Optional) Specifies access permissions between an MS and a PDN through the GGSN at a particular access point, where <i>access_list_number</i> specifies the IP access list definition to be used at the access point. The available options are: <ul style="list-style-type: none"> <li>• <b>in</b>—Applies the IP access list definition from the PDN to the MS.</li> <li>• <b>out</b>—Applies the IP access list definition from the MS to the PDN.</li> </ul>

	Command	Purpose
Step 9	<code>router(config-access-point)# ip-address-pool {dhcp-proxy-client   radius-client   disable}</code>	(Optional) Specifies a dynamic address allocation method using IP address pools for the current access point. The available options are: <ul style="list-style-type: none"> <li>• <b>dhcp-proxy-client</b>—DHCP server provides the IP address pool.</li> <li>• <b>radius-client</b>—RADIUS server provides the IP address pool.</li> <li>• <b>disable</b>—Turns off dynamic address allocation.</li> </ul>
Step 10	<code>router(config-access-point)# msisdn suppression [value]</code>	(Optional) Specifies that the GGSN overrides the MSISDN number with a pre-configured value in its authentication requests to a RADIUS server.
Step 11	<code>router(config-access-point)# radius-server {ip-address   name} [{ip-address   name}]</code>	(Optional) Specifies a primary (and backup) RADIUS server that the GGSN uses at a particular access point to authenticate mobile users for access to a PDN.
Step 12	<code>router(config-access-point)# subscription-required</code>	(Optional) Specifies that a subscription is required to access a PDN through a particular access point.
Step 13	<code>router(config-access-point)# use-interface interface_name next-hop-address ip-address</code>	(Optional) Specifies either a logical or a physical interface that will be used by this access point, where <b>next-hop-address</b> specifies the IP address of the network to be accessed.

## Configuring Access to a VPN

The GPRS software provides a couple of ways that you can configure access to a VPN, depending on your network configuration over the Gi interface between the GGSN and your PDNs, and the VPN that you want to access.

### Prerequisites

Before you begin to configure access to a VPN, be sure to satisfy the following prerequisites:

- Gi interface configuration—Before you configure access to the VPN, be sure that you have configured the Gi interface to the PDN from which you will access the VPN. For more information about configuring the Gi interface, see the [“Configuring an Interface to a PDN”](#) section on page 27.
- Route to the private network—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.

After you have completed the prerequisite configuration tasks, you can use one of the following methods to configure access to a VPN:

- [Configuring Access to a VPN Without a Tunnel](#)
- [Configuring Access to a VPN With a Tunnel](#)

## 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 **use-interface** access point configuration command.

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	<code>router(config)# <b>gprs access-point-list</b> list_name</code>	Specifies the access-point list name and enters access-point list configuration mode.
Step 2	<code>router(config-ap-list)# <b>access-point</b> ap_number</code>	Specifies a number associated with this access point definition and enters access point configuration mode.
Step 3	<code>router(config-access-point)# <b>access-point-name</b> apn_name</code>	Specifies a name associated with this the access point.
Step 4	<code>router(config-access-point)# <b>use-interface</b> interface_name <b>next-hop-address</b> ip-address</code>	Specifies the name of the Gi interface that provides access to the PDN, and the <b>next-hop-address</b> specifies the IP address of the private network to be accessed through that PDN. The next-hop-address could be the address of a router on the other side of the PDN.

For information about the other access point configuration options, see the [“Configuring the GPRS Access Point List on the GGSN”](#) section on page 27.

## 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 in this case, perform the following tasks:

- [Configuring the VPN Access Point](#)
- [Configuring the IP Tunnel](#)

### 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	<code>router(config)# <b>gprs access-point-list</b> list_name</code>	Specifies the access-point list name and enters access-point list configuration mode.
Step 2	<code>router(config-ap-list)# <b>access-point</b> ap_number</code>	Specifies a number associated with this access point definition and enters access point configuration mode.

	Command	Purpose
Step 3	router(config-access-point)# <b>access-point name</b> <i>apn_name</i>	Specifies a name associated with the access point.
Step 4	router(config-access-point)# <b>use-interface</b> <i>interface_name next-hop-address ip-address</i>	Specifies the name of the Gi interface that provides access to the PDN, and the <b>next-hop-address</b> specifies the IP address of the private network to be accessed through that PDN. The next-hop-address could be the address of a router on the other side of the PDN.  <b>Note</b> The <b>next-hop-address</b> value should match the IP address that you specify in the <b>tunnel destination</b> command. For more information, see the “ <a href="#">Configuring the IP Tunnel</a> ” section on page 31.

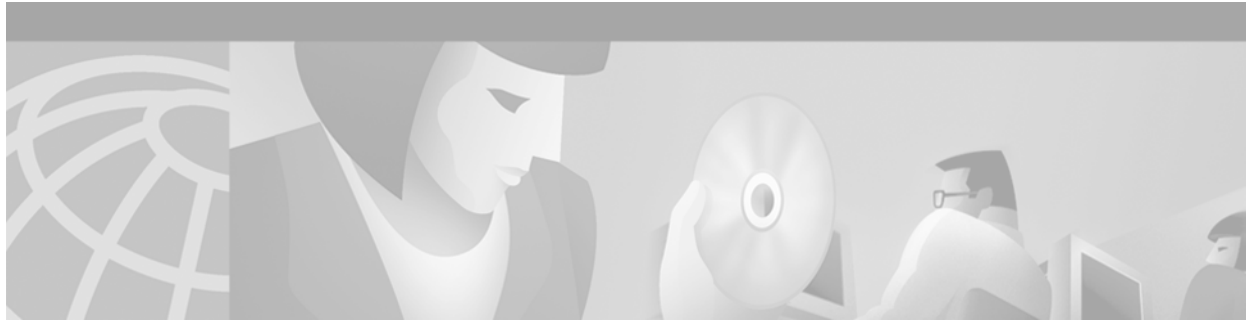
For information about the other access point configuration options, see the “[Configuring the GPRS Access Point List on the GGSN](#)” section on page 27.

## Configuring the IP Tunnel

To configure an IP tunnel to a private network, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	router(config)# <b>interface tunnel</b> <i>number</i>	Configures a logical tunnel interface number.
Step 2	router(config-if)# <b>ip address</b> <i>ip-address mask</i> [ <b>secondary</b> ]	Specifies an IP address for the tunnel interface.  <b>Note</b> This IP address is not used in any other part of the GGSN configuration.
Step 3	router(config-if)# <b>tunnel source</b> { <i>ip-address</i>   <i>type number</i> }	Specifies the IP address (or interface type and port or card number) of the Gi interface to the PDN.
Step 4	router(config-if)# <b>tunnel destination</b> { <i>hostname</i>   <i>ip-address</i> }	Specifies IP address (or host name) of the private network that you can access from this tunnel.  <b>Note</b> The <b>tunnel destination</b> address should match the IP address that you specify in the <b>next-hop-address</b> of the <b>use-interface</b> command. For more information, see the “ <a href="#">Configuring the VPN Access Point</a> ” section on page 30.





## Optimizing GPRS Performance

---

This chapter describes how to optimize performance on the GGSN by configuring fast switching.

For a complete description of the GPRS commands in this chapter, refer to the *Cisco IOS Mobile Wireless Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

### Configuring Fast Switching for GPRS

GPRS supports fast switching to improve the performance on the Gn and Gi interfaces of the GGSN. With traditional fast switching support, GPRS uses high-speed switching caches for IP routing.



#### Note

CEF switching is not supported in GPRS Release 1.4 in Cisco IOS Release 12.2 and earlier. However, CEF is enabled by default. Therefore, ensure that CEF is disabled by issuing the **no ip cef** command while in global configuration mode.

To achieve the maximum performance benefits of fast switching on the GGSN, you should configure all of the following entities for fast switching:

- Virtual template interface of the GGSN
- Physical interfaces that support GTP on the SGSN (the Gn interface)
- Physical interfaces over which MSs will access the PDNs (the Gi interface)



#### Caution

G-PDUs (GTP PDUs) with a non-zero User Datagram Protocol (UDP) checksum will be process switched, not fast switched.

### Enabling Fast Switching on the Virtual Template Interface

Before you enable fast switching on the GGSN, be sure to configure the virtual template interface with GTP encapsulation first. For further information about the steps to configure the virtual template interface on the GGSN, see the [“Configuring the GGSN”](#) section on page 17 in the [“Configuring GGSN Services”](#) chapter.

To enable fast switching on the GGSN, issue the following commands beginning in global configuration mode:

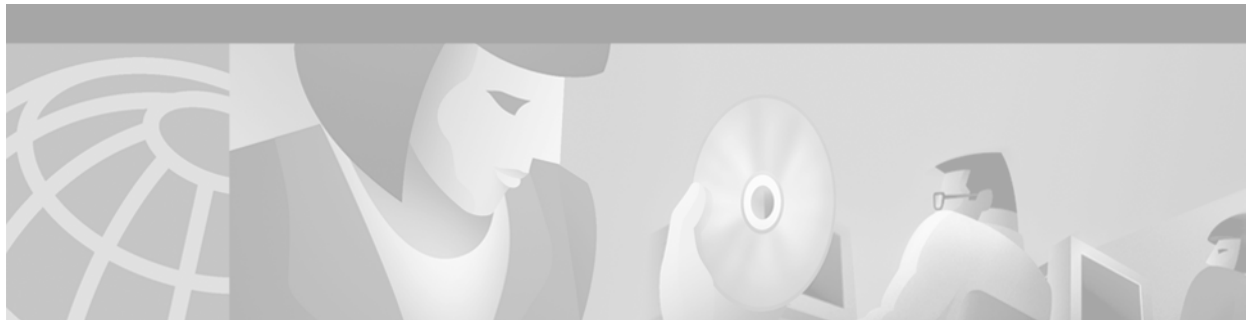
	Command	Purpose
Step 1	<code>router(config)# <b>interface virtual-template</b> <i>number</i></code>	Creates, or accesses, a virtual template interface, where <i>number</i> identifies the virtual template interface. This command enters you into interface configuration mode.  <b>Note</b> The GGSN supports only a single virtual template for the GTP virtual interface.
Step 2	<code>router(config-if)# <b>gprs fastswitch</b></code>	Enables fast switching on the virtual template interface.

## Enabling Fast Switching on a Physical Interface

After you enable fast switching on the virtual template interface of the GGSN, you should also enable fast switching on the Gn and Gi interfaces of the GGSN to achieve maximum performance benefits.

To enable fast switching on the physical interface between the GGSN and SGSN (over the Gn interface), and between the GGSN and PDNs (over the Gi interface), issue the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>router(config)# <b>interface</b> <i>type slot/port</i></code>	Accesses the physical interface configuration.  <b>Note</b> The actual syntax of the <b>interface</b> command depends on the type of physical interface that you have configured for the Gn or Gi interfaces.
Step 2	<code>router(config-if)# <b>ip route-cache</b></code>	Enables fast switching on the physical interface.



## Configuring Security on the GGSN

---

This chapter describes how to configure security 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
- RADIUS security services
- IP Security Protocol (IPSec)

AAA and RADIUS support provides the security services to authenticate and authorize access by mobile users to the GGSN and its 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 GPRS commands.

In the case of 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 on a per-access-point basis, using new GPRS 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 GPRS software implements the new **ip-access-group** access-point configuration command to apply IP access list rules at an APN.

---

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 some examples of configuring security on the GGSN, see the [“GGSN Configuration Examples”](#) chapter.

For more detailed information about AAA, RADIUS, and IPSec security services in the Cisco IOS software, refer to the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications.

For a complete description of the GPRS commands in this chapter, refer to the *Cisco IOS Mobile Wireless Command Reference*. 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 AAA Security Globally, page 36](#) (Required)
- [Configuring RADIUS Server Communication Globally, page 36](#) (Required)
- [Configuring RADIUS at the GPRS Configuration Level, page 38](#) (Required)
- [Configuring IPSec Network Security, page 40](#) (Optional)

## 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 Systems' router.

To enable AAA and configure authentication and authorization, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>router(config)# aaa new-model</code>	Enables AAA globally.
Step 2	<code>router(config)# aaa authentication ppp {default   list-name} method1 [method2...]</code>	Creates a local authentication list, with the following options: <ul style="list-style-type: none"> <li>• <b>default</b>—Specifies that the authentication methods that follow this argument are the default list of authentication methods when a user logs in to the router.</li> <li>• <b>method</b>—Specifies a valid AAA authentication method for PPP. For example, <b>group RADIUS</b> enables global RADIUS authentication.</li> </ul>
Step 3	<code>router(config)# aaa authorization {auth-proxy   network   exec   commands level   reverse-access} {default   list-name} [method1 [method2...]]</code>	Creates an authorization method list for a particular authorization type and enables authorization.

For more information about configuring AAA, refer to the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications.

For an example, see the “AAA Security Configuration Example” section on page 57 in the “GGSN Configuration Examples” chapter.

## 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 GPRS configuration level.

To globally configure RADIUS server communication on the router, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<pre>router(config)# radius-server host {hostname   ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]</pre>	<p>Specifies the IP address or host name of the remote RADIUS server host. The following options are available:</p> <ul style="list-style-type: none"> <li>• <b>auth-port</b>—Specifies the UDP destination port for authentication requests.</li> <li>• <b>acct-port</b>—Specifies the UDP destination port for accounting requests.</li> <li>• <b>timeout</b>—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 <b>radius-server timeout</b> command. If no timeout value is specified, the global value is used.</li> <li>• <b>retransmit</b>—Specifies the number of times (in the range 1 to 100) a RADIUS request is resent to a server, if that server is not responding or is responding slowly. This setting overrides the global value of the <b>radius-server retransmit</b> command.</li> <li>• <b>key</b>—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 <b>radius-server key</b> command.</li> </ul>
Step 2	<pre>router(config)# radius-server key string</pre>	<p>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.</p>

For more information about configuring RADIUS security, refer to the *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 58 in the “[GGSN Configuration Examples](#)” chapter.



**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 at the GPRS 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 GPRS configuration level, you also can configure RADIUS server communication for all access points or for a specific access point.

Configuring RADIUS at the GPRS configuration level includes the following tasks:

- [Configuring Non-Transparent Access Mode, page 38](#) (Required)
- [Specifying a RADIUS Server for All Access Points, page 39](#) (Optional)
- [Specifying a RADIUS Server for a Particular Access Point, page 39](#) (Optional)
- [Configuring the MSISDN IE for RADIUS Requests, page 40](#) (Optional)
- [Suppressing the MSISDN Number for RADIUS Authentication, page 40](#) (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 not a way to globally specify the access mode.

To configure non-transparent access for a GGSN access point, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>router(config)# <b>gprs access-point-list</b> list_name</code>	Specifies the access-point list name and enters access-point list configuration mode.
Step 2	<code>router(config-ap-list)# <b>access-point</b> ap_number</code>	Specifies the number associated with an existing access point definition (or creates a new access point), and enters access point configuration mode.
Step 3	<code>router(config-access-point)# <b>access-mode non-transparent</b></code>	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 the GPRS Access Point List on the GGSN”](#) section on page 27.

## Specifying a RADIUS Server for All Access Points

After you have configured RADIUS server communication at the global level, you can configure a default RADIUS server to be used by all GGSN access points.

To specify a default RADIUS server for all GGSN access points, use the following command in global configuration mode:

Command	Purpose
<pre>router(config)# <b>gprs default radius-server</b> {ip-address   name} [{{ip-address   name}}</pre>	<p>Specifies a primary (and backup) RADIUS server that the GGSN uses to authenticate mobile users for access to PDNs, where:</p> <ul style="list-style-type: none"> <li>• <i>ip-address</i>—Specifies the IP address of a RADIUS server. The second (optional) <i>ip-address</i> argument specifies the IP address of a backup RADIUS server.</li> <li>• <i>name</i>—Specifies the host name of a RADIUS server. The second (optional) <i>name</i> argument specifies the host name of a backup RADIUS server.</li> </ul>

## Specifying a RADIUS Server for a Particular Access Point

To override the default RADIUS server configured for all access points, you can specify a different RADIUS server for a particular access point. Or, if you choose not to configure a default GPRS RADIUS server, you can specify a RADIUS server at each access point.

To specify a RADIUS server for a particular access point, use the following command in access-point configuration mode:

Command	Purpose
<pre>router(config-access-point)# <b>radius-server</b> {ip-address   name} [{{ip-address   name}}</pre>	<p>Specifies a primary (and backup) RADIUS server that the GGSN uses at a particular access point to authenticate mobile users for access to a PDN, where:</p> <ul style="list-style-type: none"> <li>• <i>ip-address</i>—Specifies the IP address of a RADIUS server. The second (optional) <i>ip-address</i> argument specifies the IP address of a backup RADIUS server.</li> <li>• <i>name</i>—Specifies the host name of a RADIUS server. The second (optional) <i>name</i> argument specifies the host name of a backup RADIUS server.</li> </ul>

## Configuring the MSISDN IE for RADIUS Requests

To specify that the first byte of the Mobile Station International PSTN/ISDN (MSISDN) information element is included in a RADIUS request, use the following command beginning in global configuration mode:

Command	Purpose
<code>router(config)# gprs radius msisdn first-byte</code>	Specifies that the first byte of the MSISDN IE is included in a RADIUS request.

## Suppressing the MSISDN Number for RADIUS Authentication

Certain countries have privacy laws which 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 in place 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 overrides or suppresses the MSISDN number in its RADIUS authentication, use the following command beginning in access-point configuration mode:

Command	Purpose
<code>router(config-access-point)# msisdn suppression [value]</code>	(Optional) Specifies that the GGSN overrides the MSISDN number with a pre-configured value in its authentication requests to a RADIUS server.

## Configuring IPsec Network Security

In Cisco IOS Release 12.1(5)T and later, the GGSN software supports the IP security protocol for data authentication, confidentiality, encryption and integrity. IPsec data security can be implemented between the GGSN and another router on the PDN.



### Note

To support IPsec on the GGSN, you must install an ISA card on your router.

Configuring IPsec network security includes the following tasks:

- [Configuring an IKE Policy, page 41](#) (Required)
- [Configuring Pre-Shared Keys, page 42](#) (Required, when pre-shared authentication is configured)
- [Configuring Transform Sets, page 43](#) (Optional)
- [Configuring Crypto Map Entries that Use IKE to Establish Security Associations, page 43](#) (Optional)

For more information about configuring IPsec, refer to the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications.

For an example, see the “IPsec Configuration Example” section on page 59 in the “GGSN Configuration Examples” chapter.

## Configuring an IKE Policy

You can create multiple Internet Key Exchange (IKE) policies, each with a different combination of parameter values. For each policy that you create, you assign a unique priority (1 through 10,000, with 1 being the highest priority).

You can configure multiple policies on each peer—but at least one of these policies must contain exactly the same encryption, hash, authentication, and Diffie-Hellman parameter values as one of the policies on the remote peer. For example, you can configure multiple policies on the GGSN to correlate with the policies for different PDNs.


**Note**

The 3DES security encryption algorithm is not supported in this GPRS release.

To configure an IKE policy on the GGSN and corresponding PDN, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>router(config)# <b>crypto isakmp policy</b> <i>priority</i></code>	Identifies the IKE policy, where <i>priority</i> is an integer (from 1 to 10,000) that uniquely identifies the policy. This command enters you into ISAKMP policy configuration mode.
Step 2	<code>router(config-isakmp)# <b>encryption des</b></code>	Specifies the encryption algorithm, where: <ul style="list-style-type: none"> <li><b>des</b>—Specifies 56-bit Data Encryption Standard (DES)-Cipher Block Chaining (CBC). This is the default value.</li> </ul> <b>Note</b> Triple DES, or 168-bit DES encryption is supported in the Cisco IOS software. It can be configured by using this command and specifying the <b>3des</b> optional keyword. However, GPRS Release 1.4 in Cisco IOS Release 12.2 does not support the <b>3des</b> optional keyword.
Step 3	<code>router(config-isakmp)# <b>hash</b> {<b>sha</b>   <b>md5</b>}</code>	Specifies the hash algorithm, where: <ul style="list-style-type: none"> <li><b>sha</b>—Specifies the Secure Hash Algorithm (SHA)-1. This is the default value.</li> <li><b>md5</b>—Specifies the Message Digest 5 hash algorithm.</li> </ul>

	Command	Purpose
Step 4	router(config-isakmp)# <b>authentication</b> { <b>rsa-sig</b>   <b>rsa-encr</b>   <b>pre-share</b> }	<p>Specifies the authentication method, where:</p> <ul style="list-style-type: none"> <li>• <b>rsa-sig</b>—Specifies the public key encryption system developed by Ron Rivest, Adi Shamir, and Leonard Adleman, which provides non-repudiation. This is the default value.</li> <li>• <b>rsa-encr</b>—Specifies RSA encrypted nonces, which provide repudiation.</li> <li>• <b>pre-share</b>—Specifies a pre-shared key that does not require use of a certification authority. Pre-shared keys might be easier to configure in a small network with less than 10 nodes. RSA signatures can be considered more secure than pre-shared keys. If you configure <b>pre-share</b> authentication, then you must configure the pre-shared keys on both the local and remote peer (GGSN and PDN).</li> </ul>
Step 5	router(config-isakmp)# <b>group</b> { <b>1</b>   <b>2</b> }	<p>Specifies the Diffie-Hellman group identifier, where:</p> <ul style="list-style-type: none"> <li>• <b>1</b>—Specifies 768-bit Diffie-Hellman. This is the default value.</li> <li>• <b>2</b>—Specifies 1024-bit Diffie-Hellman.</li> </ul> <p><b>Note</b> The 1024-bit Diffie-Hellman option is harder to crack, but requires more CPU time to execute.</p>
Step 6	router(config-isakmp)# <b>lifetime</b> <i>seconds</i>	Specifies the security association's lifetime (in seconds). The default value is 86,400 seconds (1 day).

For more information about the meaning of the IKE policy parameters, refer to the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications.

## Configuring Pre-Shared Keys

When you configure the **pre-share** authentication method for your IKE policy, you also must configure the pre-shared keys on the GGSN and remote peer, or PDN.

To configure pre-shared keys on the GGSN and corresponding PDN, use one of the following commands beginning in global configuration mode:

Command	Purpose
<pre>router(config)# <b>crypto isakmp key</b> <i>keystring</i> <b>address</b> <i>peer-address</i> or router(config)# <b>crypto isakmp key</b> <i>keystring</i> <b>hostname</b> <i>peer-hostname</i></pre>	<p>Specifies the shared key to be used between a local peer (GGSN) and particular remote peer (PDN).</p> <p>If the remote peer, or PDN, specifies the ISAKMP identity with an address, use the <b>address</b> keyword; otherwise use the <b>hostname</b> keyword.</p> <p>When configuring the pre-shared keys on the GGSN, use the address or hostname of the PDN. When configuring the pre-shared keys on the PDN, use the address or hostname of the GGSN.</p>

## Configuring Transform Sets

A transform set represents a certain combination of security protocols and algorithms. During the IPSec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

To configure a transform set on the GGSN and corresponding PDN, use the following commands beginning in global configuration mode:

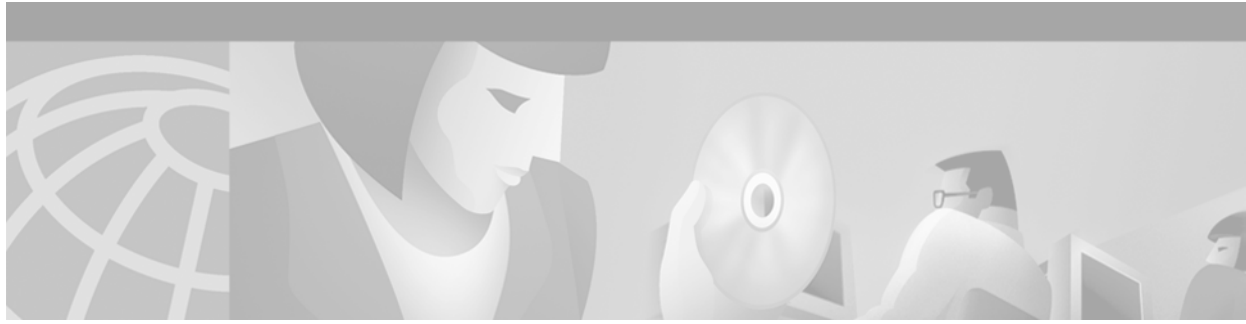
	Command	Purpose
<b>Step 1</b>	<pre>router(config)# <b>crypto ipsec transform-set</b> <i>transform-set-name</i> <i>transform1</i> [<i>transform2</i> <i>transform3</i>]</pre>	<p>Defines a transform set and enters crypto transform configuration mode.</p> <p>There are complex rules defining which entries you can use for the transform arguments. For more information, refer to the <i>Cisco IOS Security Configuration Guide</i> and <i>Cisco IOS Security Command Reference</i> publications.</p>
<b>Step 2</b>	<pre>router(config-crypto-transform)# <b>mode</b> [<b>tunnel</b>   <b>transport</b>]</pre>	<p>(Optional) Changes the mode associated with the transform set. The following options are available:</p> <ul style="list-style-type: none"> <li><b>tunnel</b>—Protects (encrypts, authenticates) and encapsulates the entire original IP packet</li> <li><b>transport</b>—Protects (encrypts, authenticates) and encapsulates the payload or data portion of the IP packet.</li> </ul> <p><b>Note</b> The mode setting is applicable only to traffic whose source and destination addresses are the IPSec peer addresses; it is ignored for all other traffic.</p>

## Configuring Crypto Map Entries that Use IKE to Establish Security Associations

When you use IKE to establish security associations, you can specify a list of acceptable settings to be used during IPSec peer negotiation using a crypto map entry.

To configure crypto map entries on the GGSN and corresponding PDN, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	router(config)# <b>crypto map</b> <i>map-name seq-num ipsec-isakmp</i>	Creates or modifies a crypto map entry and enters crypto map configuration mode.
Step 2	router(config-crypto-map)# <b>match address</b> <i>access-list-id</i>	Names an extended access list. This access list determines which traffic should be protected by IPSec and which traffic should not be protected by IPSec in the context of the current crypto map entry.
Step 3	router(config-crypto-map)# <b>set peer</b> { <i>hostname</i>   <i>ip-address</i> }	Specifies a remote IPSec peer. This is the peer to which IPSec-protected traffic can be forwarded.
Step 4	router(config-crypto-map)# <b>set transform-set</b> <i>transform-set-name1</i> [ <i>transform-set-name2</i> ... <i>transform-set-name6</i> ]	Specifies which transform sets are allowed for this crypto map entry. List multiple transform sets in order of priority (highest priority first).
Step 5	router(config-crypto-map)# <b>set security-association lifetime seconds</b> <i>seconds</i> and/or <b>set security-association lifetime kilobytes</b> <i>kilobytes</i>	(Optional) Specifies a security association lifetime for the crypto map entry, if you want the security associations for the current crypto map entry to be negotiated using different IPSec security association lifetimes than the global lifetimes.
Step 6	router(config-crypto-map)# <b>set security-association level per-host</b>	(Optional) Specifies that separate security associations should be established for each source/destination pair.  <b>Note</b> Use this command with care, as multiple streams between given subnets can rapidly consume resources.
Step 7	router(config-crypto-map)# <b>set pfs</b> [ <i>group1</i>   <i>group2</i> ]	(Optional) Specifies that IPSec should ask for perfect forward secrecy (PFS) when requesting new security associations for the current crypto map entry, or should demand PFS in requests received from the IPSec peer.



## Configuring DHCP on the GGSN

This chapter describes how to configure the Dynamic Host Configuration Protocol (DHCP) on the Gateway General Packet Radio Service (GPRS) Support Node (GGSN). The GGSN uses DHCP to assign IP addresses to mobile station users who need to access the PDN.

For a complete description of the GPRS commands in this chapter, refer to the *Cisco IOS Mobile Wireless Command Reference*. 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 DHCP Server Communication Globally, page 45](#) (Required)
- [Configuring DHCP at the GPRS Configuration Level, page 46](#) (Optional)

### 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 GPRS configuration level.

To globally configure DHCP server communication on the router, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>router(config)# ip address-pool {dhcp-proxy-client   local}</code>	<p>Specifies an IP address pool mechanism, where:</p> <ul style="list-style-type: none"> <li>• <b>dhcp-proxy-client</b>—Specifies the router as the proxy-client between a third-party DHCP server and peers connecting to the router.</li> <li>• <b>local</b>—Specifies the local address pool named “default”.</li> </ul> <p><b>Note</b> There is no default option for the <b>ip address-pool</b> command. If you configure a local address pool using the <b>local</b> keyword, you can also configure the optional commands in Step 4 and Step 5.</p>
Step 2	<code>router(config)# ip dhcp-server {ip-address   name}</code>	Specifies the IP address or name of a DHCP server.

	Command	Purpose
Step 3	<code>router(config)# ip dhcp excluded address low-address [high-address]</code>	(Optional) Specifies IP addresses that a DHCP server should not assign to DHCP clients, where: <ul style="list-style-type: none"> <li><i>low-address</i>—Specifies the first IP address in an excluded address range. This address is typically the address of the DHCP server itself.</li> <li><i>high-address</i>—(Optional) Specifies the last IP address in the excluded address range.</li> </ul>
Step 4	<code>router(config)# ip dhcp pool name</code>	(Optional—Supports <b>ip address-pool local</b> command only.) Configures a DHCP address pool and enters DHCP pool configuration mode, where <i>name</i> can be either a symbolic string (such as “engineering”) or an integer (such as 0).
Step 5	<code>router(config-dhcp)# network network-number [mask   /prefix-length]</code>	(Optional—Supports <b>ip address-pool local</b> command only.) Specifies the subnet network number and mask of the DHCP address pool.  The prefix length specifies the number of bits that comprise 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, refer to the *Cisco IOS IP Configuration Guide*, *Cisco IOS IP Command References*, and the *Cisco IOS Dial Technologies Command Reference* publications.

## Configuring DHCP at the GPRS Configuration Level

To complete the DHCP configuration for the GGSN, you can configure DHCP at the GPRS configuration level. When you configure DHCP at the GPRS configuration level, you can configure DHCP server communication for all access points, or for a specific access point.

Configuring DHCP at the GPRS configuration level includes the following tasks:

- [Specifying a DHCP Server for All Access Points, page 46](#) (Optional)
- [Specifying a DHCP Server for a Particular Access Point, page 47](#) (Optional)

## Specifying a DHCP Server for All Access Points

When processing DHCP address allocation, the GGSN software first checks to see whether a DHCP server has been specified at the access-point configuration level. If so, it 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 GPRS DHCP server.

To specify a DHCP server for all GGSN access points, use the following commands beginning in global configuration mode:

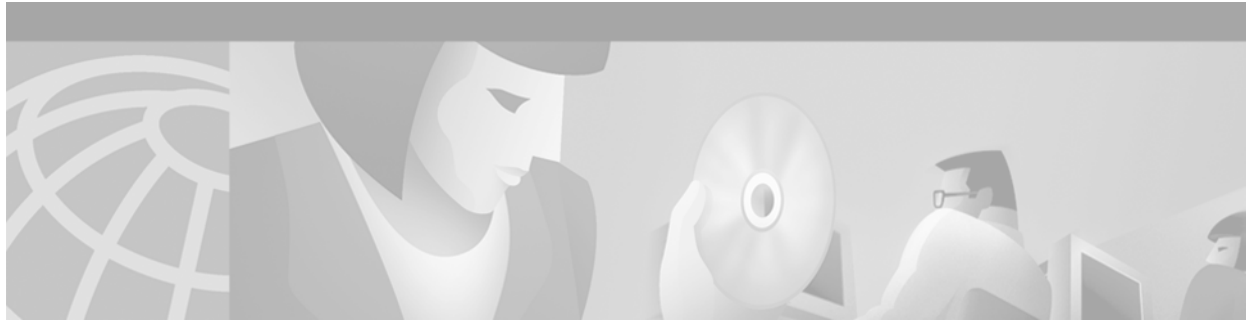
	Command	Purpose
Step 1	<pre>router(config)# gprs default ip-address-pool {dhcp-proxy-client   radius-client   disable}</pre>	<p>Specifies a dynamic address allocation method using IP address pools for the GGSN, where:</p> <ul style="list-style-type: none"> <li>• <b>dhcp-proxy-client</b>—Specifies that the GGSN dynamically acquires IP addresses for an MS from a DHCP server. Use this keyword to enable DHCP services.</li> <li>• <b>radius-client</b>—Specifies that the GGSN dynamically acquires IP addresses for an MS from a RADIUS server.</li> <li>• <b>disable</b>—Disables dynamic address allocation by the GGSN.</li> </ul> <p>There is no default option for this command.</p>
Step 2	<pre>router(config)# gprs default dhcp-server {ip-address   name} [{ip-address   name}]</pre>	<p>Specifies a primary (and backup) DHCP server from which the GGSN obtains IP address leases for mobile users, where:</p> <ul style="list-style-type: none"> <li>• <i>ip-address</i>—Specifies the IP address of a DHCP server. The second (optional) <i>ip-address</i> argument specifies the IP address of a backup DHCP server.</li> <li>• <i>name</i>—Specifies the host name of a DHCP server. The second (optional) <i>name</i> argument specifies the host name of a backup DHCP server.</li> </ul>

## 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 GPRS 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	<pre>router(config-access-point)# <b>ip-address-pool</b> {<b>dhcp-proxy-client</b>   <b>radius-client</b>   <b>disable</b>}</pre>	<p>Specifies a dynamic address allocation method using IP address pools for the current access point, where:</p> <ul style="list-style-type: none"> <li>• <b>dhcp-proxy-client</b>—Specifies that the access point IP address pool is maintained on a DHCP server. Use this keyword to enable DHCP services.</li> <li>• <b>radius-client</b>—Specifies that the access point IP address pool is allocated through a RADIUS server.</li> <li>• <b>disable</b>—Disables dynamic address allocation for the current access point.</li> </ul> <p>There is no default option for this command.</p>
Step 2	<pre>router(config-access-point)# <b>dhcp-server</b> {<i>ip-address</i>   <i>name</i>} [{<i>ip-address</i>   <i>name</i>}]</pre>	<p>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:</p> <ul style="list-style-type: none"> <li>• <i>ip-address</i>—Specifies the IP address of a DHCP server. The second (optional) <i>ip-address</i> argument specifies the IP address of a backup DHCP server.</li> <li>• <i>name</i>—Specifies the host name of a DHCP server. The second (optional) <i>name</i> argument specifies the host name of a backup DHCP server.</li> </ul>



## Verifying the GPRS Configuration

---

This chapter describes how to verify the GGSN configuration. For a complete description of the GPRS commands in this chapter, refer to the *Cisco IOS Mobile Wireless Command Reference*. 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:

- [Verifying Global GPRS Configuration, page 49](#)
- [Verifying Interface Configuration to the SGSN, page 50](#)
- [Verifying Interface Configuration to the PDN, page 50](#)
- [Verifying an Interface to the Private Network, page 50](#)
- [Verifying Configuration to the Virtual Template, page 50](#)
- [Verifying Access-Point Configuration, page 51](#)
- [Verifying DHCP Configuration, page 52](#)

### Verifying Global GPRS Configuration

Enter the **show running-configuration** command to see if GPRS GGSN services are enabled with the **service gprs ggsn** command:

```
router# show running-configuration

Building configuration...

Current configuration:
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
service tcp-small-servers
→ service gprs ggsn
!
hostname GGSN_1
```

## Verifying Interface Configuration to the SGSN

Enter the **show running-configuration** command to view the interface configuration to the SGSN:

```
router# show running-configuration

interface FastEthernet0/0
description Gn interface to SGSN
ip address 44.44.44.44 255.0.0.0
half-duplex
```

## Verifying Interface Configuration to the PDN

Enter the **show running-configuration** command to view the interface configuration to the PDN:

```
router# show running-configuration

interface FastEthernet3/0
description Gi interface to PDN
ip address 4.0.0.44 255.0.0.0
half-duplex
```

## Verifying an Interface to the Private Network

Enter the **show running-configuration** command to view the interface configuration to the private network:

```
router# show running-configuration

gprs access-point-list gprs
access-point 1
access-point-name gprs.company.com
ip-address-pool dhcp-proxy-client
dhcp-server 99.100.0.3
use-interface Tunnel0 next-hop-address 97.0.0.2
exit
```

## Verifying Configuration to the Virtual Template

- Step 1** Use the **show running-configuration** command to view the virtual template configuration. Note that the **encapsulation gtp** command must be configured on the virtual template interface of the GGSN:

```
router# show running-configuration

interface virtual-template 1
ip address 10.10.10.1 255.0.0.0
→ encapsulation gtp
ip mroute-cache
gprs fastswitch
gprs access-point-list gprs
```

- Step 2** Enter the **show interface** command to view the virtual template configuration:

```

router# show interface virtual-template 1

→ virtual-template 1 is up, line protocol is up
Hardware is Virtual Template interface
→ Internet address is 10.10.10.1/8
MTU 1500 bytes, BW 100000 Kbit, DLY 100000 usec,
reliability 255/255, txload 1/255, rxload 1/255
→ Encapsulation GPRS-GTP, loopback not set
Keepalive set (10 sec)
DTR is pulsed for 5 seconds on reset
Last input never, output never, output hang never
Last clearing of "show interface" counters 02:17:14
Queueing strategy:fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions

```

## Verifying Access-Point Configuration

**Step 1** Use the **show running-configuration** command to view the access-point configuration:

```

router# show running-configuration

gprs access-point-list gprs
access-point 1
access-point-name gprs.company.com
ip-address-pool dhcp-proxy-client
dhcp-server 99.100.0.3
dhcp-gateway-address 80.0.0.1

```

**Step 2** Use the **show gprs access-point all** command to view all access points:

```

router# show gprs access-point all

There are 3 Access-Points configured

Index   Type   Mode           AccessPointName      Interface
-----
1       ip     transparent    gprs.company.com
-----
2       ip     transparent    abc.com
-----
3       ip     non-transparent xyz.com
-----

```

## Verifying DHCP Configuration

Use the **show running-configuration** command to view the DHCP-related configuration. The following example shows the configuration of both global DHCP services, and DHCP services configured at the access point level:

```
router# show running-configuration
!
→ ip address-pool dhcp-proxy-client
interface Ethernet2/1
description interface to DHCP server
ip address 99.102.0.54 255.255.0.0
no ip mroute-cache
!
gprs access-point-list gprs
access-point 1
access-point-name gprs.company.com
→ ip-address-pool dhcp-proxy-client
→ dhcp-server 99.100.0.3
→ dhcp-gateway-address 99.102.0.54
exit
!
→ gprs default dhcp-server 99.100.0.3
```



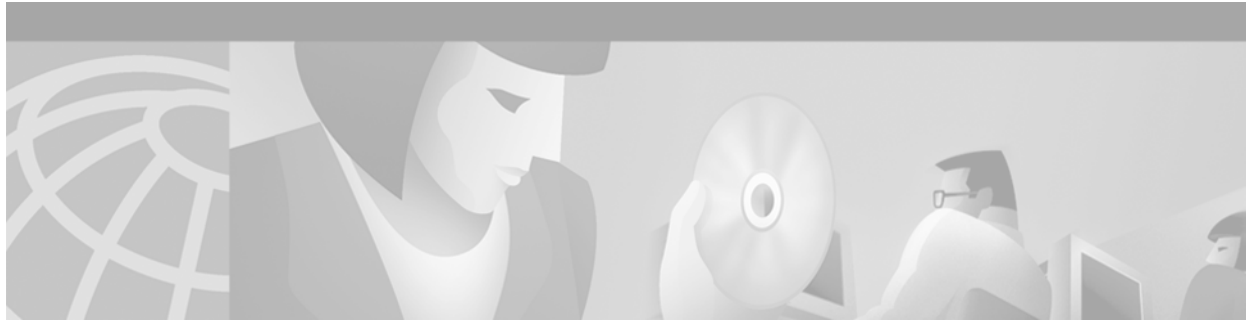
## Monitoring and Maintaining GPRS

This chapter describes the commands used to display configuration parameters and statistics, and to monitor network status on the GGSN. For a complete description of the GPRS commands in this chapter, refer to the *Cisco IOS Mobile Wireless Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

The following global configuration commands are used to monitor and maintain the GPRS feature:

Command	Purpose
<code>router(config)# clear gprs charging cdr {tid tunnel-id   access-point access-point-index   all}</code>	Clears GPRS charging data records.
<code>router(config)# clear gtp pdp-context {tid tunnel-id   imsi imsi_value   path ip-address   access-point access-point-index   all}</code>	Clears one or more PDP contexts (mobile sessions).
<code>router(config)# clear gprs gtp statistics</code>	Clears GPRS GTP statistics.
<code>router(config)# clear gprs isgsn statistics</code>	Clears the current GPRS intra-Serving GPRS Support Node (iSGSN).
<code>router(config)# clear l2relay statistics</code>	Clears the l2relay statistics for the SGSN (SGSN D-node only).
<code>router(config)# clear l2relay topology-map</code>	Clears the l2relay topology map for the SGSN (SGSN D-node only).
<code>router(config)# show gprs access-point [access-point-index] [address-allocation] [all]</code>	Displays information about an access point.
<code>router(config)# show gprs charging parameters</code>	Displays the current GPRS charging parameters.
<code>router(config)# show gprs charging statistics {tid tunnel_id   access-point access-point-index   all}</code>	Displays current statistics for the transfer of charging packets between the GGSN and charging gateways.
<code>router(config)# show gprs isgsn statistics</code>	Displays statistics that show the status of the intra-Serving GPRS Support Node running on the router (SGSN D-node only).
<code>router(config)# show l2relay statistics</code>	Displays statistics that show the status of the l2relay protocol running on the SGSN (SGSN D-node only).
<code>router# show gprs gtp parameters</code>	Displays the current GTP parameters configured on the GGSN.
<code>router# show gprs gtp path {ip-address   all}</code>	Displays information about one or more GTP paths between the GGSN and other GPRS devices.

Command	Purpose
router(config)# <b>show gprs gtp pdp-context</b> { <b>tid</b> <i>tunnel_id</i>   <b>imsi</b> <i>imsi</i>   <b>path</b> <i>ip-address</i>   <b>access-point</b> <i>access-point-index</i>   <b>pdp-type</b> <b>ip</b>   <b>qos-precedence</b> { <b>low</b>   <b>normal</b>   <b>high</b> }   <b>all</b> }	Displays a list of the currently active PDP contexts (mobile sessions).
router(config)# <b>show gprs gtp status</b>	Displays information about the current status of GTP on the GGSN.



## GGSN Configuration Examples

---

This chapter contains GGSN configuration examples. For a complete description of the GPRS commands in this chapter, refer to the *Cisco IOS Mobile Wireless Command Reference*. 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:

- [Virtual Template Interface Configuration on GGSN Example, page 55](#)
- [Static Route to SGSN Example, page 56](#)
- [Access Point List Configuration Example, page 56](#)
- [VPN Tunnel Configuration Example, page 57](#)
- [AAA Security Configuration Example, page 57](#)
- [RADIUS Server Global Configuration Example, page 58](#)
- [RADIUS Server Access Point Configuration Example, page 58](#)
- [IPSec Configuration Example, page 59](#)
- [DHCP Server Configuration Example, page 62](#)
- [Charging Gateway Configuration Example, page 63](#)
- [Complete GGSN Configuration Example, page 64](#)

### Virtual Template Interface Configuration on GGSN Example

The following example shows a sample configuration for virtual template 1 on the GGSN:

```
! Virtual Template configuration
interface virtual-template 1
 ip address 10.10.10.1 255.255.255.0
 no ip directed-broadcast
 encapsulation gtp
 gprs fastswitch
 gprs access-point-list abc
 ip classless
```



**Note**

The **gprs access-point-list** command is configured in global configuration, but the **show running-configuration** command on the router automatically includes it in the virtual template interface section of the output.

## Static Route to SGSN Example

The following example shows how to configure a static route from a physical interface on the GGSN to the SGSN. This configures what is known as the GPRS Gn interface.

```
! Gn Interface on GGSN to communicate with SGSN
interface FastEthernet0/0
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 no keepalive
!
ip route 192.168.1.1 255.255.255.255 FastEthernet0/0
```

In the first part of the sample configuration, physical interface FastEthernet0/0 on the GGSN is shown as the interface to the SGSN. In this example, the SGSN is located at IP address 192.168.1.1. Using the **ip route** command, a static route is configured to the SGSN located at 192.168.1.1 from the FastEthernet0/0 interface on the GGSN.



### Note

---

For the SGSN to successfully communicate with the GGSN, the SGSN must configure a static route, or be able to dynamically route to the IP address used by the GGSN virtual template.

---

## Access Point List Configuration Example

The following example shows the configuration of a GPRS access point list on the GGSN:

```
! Defines a GPRS access point list
! named abc
gprs access-point-list abc
!
! Defines an APN number 1 called gprs.company.com,
! which defines access to a PDN through the domain gprs.company.com
!
access-point 1
 access-point-name gprs.company.com
!
!DHCP server at 10.100.0.3 assigns IP addresses to
!mobile users who access APN gprs.company.com.
!
 dhcp-server 10.100.0.3
 exit
!Defines an APN number 2 called xyz.com,
!which defines access to a private network through xyz.com
!
access-point 2
 access-point-name xyz.com
 dhcp-server 10.0.0.1
 dhcp-gateway-address 10.0.0.1
!Configures the router to use the Tunnel0 interface to
!set up an IP tunnel to the private network
!
 use-interface Tunnel0 next-hop-address 10.10.0.21
 exit
! Defines an APN number 3 called www.gprs_mycompany,
! which defines access to a PDN through the domain www.gprs_mycompany
!
```

```
access-point 3
  access-point-name www.gprs_mycompany
! Requires security authorization for access to this network.
! GGSN acts as a client to the RADIUS server at 10.100.0.2.
!
  access-mode non-transparent
  radius-server 10.100.0.2
exit
```

## VPN Tunnel Configuration Example

The following example shows the configuration for the physical interface that is used to connect to the PDN (Gi interface) from which you can access a private network:

```
! interface to communicate with the PDN
interface FastEthernet1/0
  ip address 10.0.0.1 255.0.0.0
  no ip directed-broadcast
  no ip route-cache
  no ip mroute-cache
!
```

In addition, a logical interface called Tunnel0 defines an IP tunnel to the private networks:

```
interface Tunnel0
  ip address 97.0.0.1 255.0.0.0
  no ip directed-broadcast
  ip mtu 1476
  tunnel source 4.0.0.1
  tunnel destination 131.108.164.19
!
```

## AAA Security Configuration Example

The following example shows how to enable AAA security globally on the router, and 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 default group radius
!
! Enables authorization and creates an authorization
! method list for all network-related service requests
! and enables authorization using a RADIUS server
!
aaa authorization network default group radius
```

For more information about configuring AAA, refer to the *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 "foo" for this radius host only
!
radius-server host 10.100.0.2 auth-port 1645 acct-port 1646 key foo
!
! 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, refer to the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications.

## RADIUS Server Access Point Configuration Example

The following example shows a complete RADIUS configuration, including global AAA and RADIUS configuration, and RADIUS configuration at one of the GGSN access points:

```
! Enables AAA globally
aaa new-model
!
! Configures AAA authentication
! and authorization
!
aaa authentication ppp default group radius
aaa authorization network default group radius

! Configures global RADIUS server hosts
! and specifies destination ports for
! authentication and accounting requests
!
radius-server host 10.10.10.1 auth-port 1645 acct-port 1646
radius-server host 10.11.11.1 auth-port 1645 acct-port 1646

radius-server key mykey

gprs default ip-address-pool radius-client
!
! Configures a primary RADIUS server for the GGSN
!
gprs default radius-server 10.10.10.1
!
! Virtual Template configuration
interface virtual-template 1
 ip address 10.10.10.1 255.255.255.0
 no ip directed-broadcast
 encapsulation gtp
 gprs access-point-list abc
!
```

```

!
! Access point list configuration
gprs access-point-list abc
  access-point 1
    access-point-name gprs.somewhere.com
    access-mode transparent
  exit
!
  access-point 2
    access-point-name xyz.com
    access-mode transparent
  exit
!
  access-point 3
    access-point-name www.gprs_somewhere.fr
    access-mode non-transparent
!
! Specifies a RADIUS server
! for use by the GGSN to authenticate
! mobile users at this access point
!
  radius-server 10.11.11.1
  exit

```

Notice the following areas of interest in the RADIUS configuration shown in this example:

- Two global RADIUS server hosts are configured for the router at 10.10.10.1 and 10.11.11.1 using the **radius-server host** global configuration command.
- The default RADIUS server for all GGSN access points is configured as 10.10.10.1 using the **gprs default radius-server** global configuration command.
- The first two access points are configured for transparent access. For mobile users attempting access at these APNs, the GGSN does not perform authentication.
- The third access point specifies a RADIUS server located at 10.11.11.1, using the **radius-server** access-point configuration command.



**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.

## IPSec Configuration Example

IP Security Protocol is configured between two peers to establish data security services. For GPRS, IPSec configuration is applicable between the GGSN and a router on a PDN. The following example shows configuration of IPSec on the GGSN and an associated PDN, including the complete global and GPRS configuration commands:

### GGSN configuration

```

hostname ggsn1

enable password ggsn1password

ip host pdn1a 10.58.0.8

interface Ethernet5/0
  description TFTP DOWNLOAD
  ip address 10.103.0.7 255.255.0.0

```

```

ip helper-address 10.100.0.3
no shut

interface FastEthernet0/0
description CONNECT TO ggsn-a
ip address 10.56.0.7 255.255.0.0
no shut

interface FastEthernet4/0
description CONNECT TO Gi
ip address 10.58.0.7 255.255.0.0
no shut

ip classless
ip route 10.100.0.0 255.255.0.0 Ethernet5/0

! IPsec configuration for GGSN

crypto isakmp policy 1
authentication pre-share
group 2
!
! 10.58.0.8 is address of peer, or PDN
!
crypto isakmp key sharedkey address 10.58.0.8

crypto ipsec transform-set auth2 esp-des esp-sha-hmac

crypto map test 10 ipsec-isakmp
set peer 10.58.0.8
set transform-set auth2
match address 133

! ISA card is required for IPsec support
!
controller ISA 1/1

interface FastEthernet4/0
crypto map test

router eigrp 10
network 10.56.0.0
network 10.58.0.0

access-list 133 permit ip 10.56.0.0 0.0.255.255 10.59.0.0 0.0.255.255

! GPRS configuration on the GGSN

service gprs ggsn

ip dhcp-server 10.40.0.3
ip dhcp-server 10.100.0.3
ip address-pool dhcp-proxy-client

interface Virtual-Template1
ip address 10.7.7.7 255.255.255.0
encapsulation gtp
ip mroute-cache
no gprs fastswitch
gprs access-point-list abc

router eigrp 10
network 10.2.0.0

```

```
ip route 10.5.5.5 255.255.255.255 FastEthernet0/0
access-list 133 permit ip 10.2.0.0 0.0.255.255 10.59.0.0 0.0.255.255

gprs access-point-list abc
access-point 1
access-point-name apn1.cisco.com
dhcp-server 10.100.0.3
exit
!
access-point 2
access-point-name apn2.cisco.com
dhcp-server 10.100.0.3
exit
!
access-point 3
access-point-name www.apn3.com
dhcp-server 10.100.0.3
exit
!
!
gprs default charging-gateway 10.58.0.4 10.58.0.2
gprs charging server-switch-timer 0

line con 0
exec-timeout 0 0
transport input none
line aux 0
exec-timeout 0 0
line vty 0 4
exec-timeout 0 0
password vtypassword
login
end
```

### PDN configuration

```
hostname pdn1a

enable password pdn1apassword

ip host ggsn1 10.58.0.7

interface Ethernet5/0
description TFTP DOWNLOAD
ip address 10.103.0.8 255.255.0.0
ip helper-address 10.100.0.3
no shut

interface FastEthernet2/0
description CONNECT TO Gn
ip address 10.56.0.8 255.255.0.0
shutdown

interface FastEthernet4/0
description CONNECT TO Gi
ip address 10.58.0.8 255.255.0.0
no shut

interface FastEthernet0/0
description CONNECT TO Intranet
ip address 10.59.0.8 255.255.0.0
no shut

ip route 10.100.0.0 255.255.0.0 Ethernet5/0
```

```

! IPsec configuration on the PDN

crypto isakmp policy 1
  authentication pre-share
  group 2
!
! 10.58.0.7 is address of peer, or GGSN
!
crypto isakmp key sharedkey address 10.58.0.7

crypto ipsec transform-set auth2 ah-sha-hmac esp-des esp-sha-hmac

crypto map test 10 ipsec-isakmp
  set peer 10.58.0.7
  set transform-set auth2
  match address 144
!
! ISA card is required for IPsec support
!
controller ISA 1/1

interface FastEthernet4/0
  crypto map test

router eigrp 10
  network 10.58.0.0
  network 10.59.0.0

access-list 144 permit ip 10.59.0.0 0.0.255.255 10.56.0.0 0.0.255.255
!
! GPRS configuration on the PDN
!
router eigrp 10
  network 10.2.0.0

ip route 10.2.0.0 255.255.0.0 FastEthernet4/0
access-list 144 permit ip 10.59.0.0 0.0.255.255 10.2.0.0 0.0.255.255

line con 0
  exec-timeout 0 0
  transport input none
line aux 0
  exec-timeout 0 0
line vty 0 4
  exec-timeout 0 0
  password vtypassword
  login
end

```

## DHCP Server Configuration Example

The following example shows a complete DHCP configuration, including global DHCP configuration, default GPRS DHCP configuration, and DHCP configuration at the GGSN access points:

```

ip address-pool dhcp-proxy-client
ip dhcp-server 10.60.0.1
ip dhcp-server 10.101.100.3
ip dhcp-server 10.102.100.3
ip dhcp excluded address 10.60.0.1
gprs default ip-address-pool dhcp-proxy-client

```

```
gprs default dhcp-server 10.101.100.3
!
interface virtual-template 1
 ip address 10.10.10.1 255.255.255.0
 no ip directed-broadcast
 encapsulation gtp
 gprs access-point-list abc
!
gprs access-point-list abc
 access-point 1
  access-point-name gprs.everywhere.com
  ip-address-pool dhcp-proxy-client
  dhcp-server 10.101.100.3
  ip-access-group 101 in
 exit
!
 access-point 2
  access-point-name xyz.com
  ip-address-pool dhcp-proxy-client
  dhcp-server 10.60.0.1
  dhcp-gateway-address 10.60.0.1
 exit
!
 access-point 3
  access-point-name www.my_isp.com
 exit
!
```

Notice the following areas of interest in the DHCP configuration shown in this example:

- Three global DHCP servers are configured for the router at 10.60.0.1, 10.101.100.3, and 10.102.100.3 using the **ip dhcp-server** global configuration command.
- The default DHCP server for all GGSN access points is configured as 10.101.100.3 using the **gprs default dhcp-server** global configuration command.
- The first access point specifies a DHCP server located at 10.101.100.3, using the **dhcp-server** access-point configuration command. This DHCP server is the same as the DHCP server specified by the **gprs default dhcp-server** command, and therefore is not a necessary command.
- The second access point specifies a DHCP server located at 10.60.0.1, using the **dhcp-server** access-point configuration command. This DHCP server is different than the DHCP server specified by the **gprs default dhcp-server** global configuration command.
- The third access point does not include any additional DHCP server configuration. For mobile users attempting access at these APNs, the GGSN uses the DHCP server 10.101.100.3 to assign IP addresses, according to the value of the **gprs default dhcp-server** command.

## Charging Gateway Configuration Example

The following example configures a primary charging gateway at IP address 10.100.0.3, and a backup charging gateway at IP address 10.100.0.2:

```
gprs default charging-gateway 10.100.0.3 10.100.0.2
```

# Complete GGSN Configuration Example

This example shows a complete GGSN router configuration. For detailed information on commands used with the GPRS interface, refer to the “Command Reference” section on page 45. For detailed information on the basic Cisco IOS commands shown in the example, refer to the *Cisco IOS Interface Command Reference*, the *Cisco IOS IP Command References*, or the *Cisco IOS Security Command Reference*.

```

!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service gprs ggsn
!
hostname c7206-4
!
aaa new-model
aaa authentication ppp default radius
aaa authorization network default radius
enable password mypass
!
ip subnet-zero
ip domain-name gprs.com
ip name-server 99.100.0.2
ip dhcp excluded-address 60.0.0.1
!
! local IP address pool
ip dhcp pool 1
 network 60.0.0.0 255.255.255.0
!
ip address-pool dhcp-proxy-client
ip dhcp-server 60.0.0.1
ip dhcp-server 99.100.0.3
!
interface Loopback0
 ip address 60.0.0.1 255.0.0.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Tunnel0
 ip address 97.0.0.1 255.0.0.0
 no ip directed-broadcast
 ip mtu 1476
 tunnel source 4.0.0.1
 tunnel destination 131.108.164.19
!
! Interface to communicate with Virtual Template on SGSN
interface FastEthernet0/0
 ip address 35.0.0.2 255.0.0.0
 ip helper-address 99.100.0.3
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 no keepalive
!
! interface to communicate with the PDN
interface FastEthernet1/0
 ip address 4.0.0.1 255.0.0.0
 no ip directed-broadcast

```

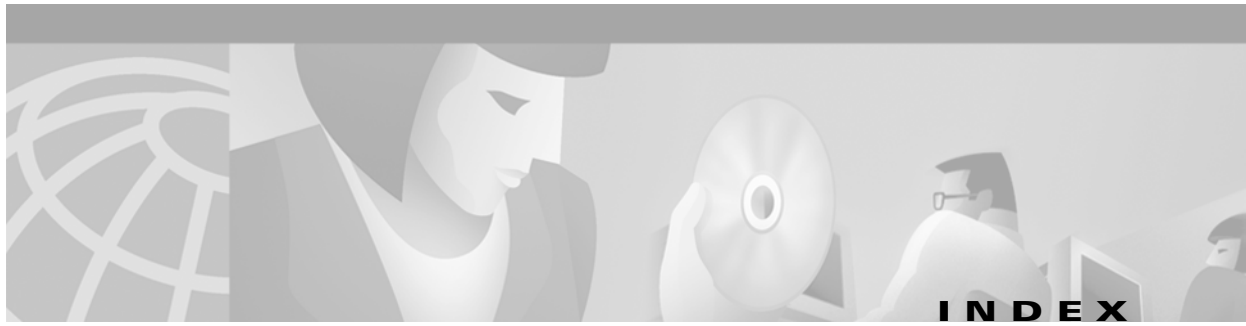
```
no ip route-cache
no ip mroute-cache
!
! Interface to TFTP server
interface Ethernet2/0
 ip address 99.102.0.54 255.255.0.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
!
! Virtual Template configuration
interface virtual-template 1
 ip address 10.10.10.1 255.255.255.0
no ip directed-broadcast
encapsulation gtp
gprs access-point-list abc
 ip classless
!
! Route for the virtual template on the SGSN
ip route 1.1.1.1 255.255.255.255 FastEthernet0/0
access-list 101 deny ip host 4.0.0.2 host 2.0.0.1
dialer-list 1 protocol ip permit
snmp-server community public RW
!
!
! Global DHCP server, charging server, and RADIUS server information
gprs default dhcp-server 99.100.0.3
gprs default charging-gateway 99.100.0.3 99.100.0.2
gprs charging server-switch-timer 0
!
radius-server host 99.100.0.2 auth-port 1645 acct-port 1646
radius-server key mykey
!
!
! access-point list configuration
! access point for access to PDN
gprs access-point-list abc
access-point 1
 access-point-name gprs.company.com
 dhcp-server 99.100.0.3
 exit
!
!access point for access to a private network
access-point 2
 access-point-name xyz.com
 dhcp-server 60.0.0.1
 dhcp-gateway-address 60.0.0.1
 use-interface Tunnel0 next-hop-address 97.0.0.21
 exit
!
```

```
! access point for access to PDN
access-point 3
  access-point-name www.gprs_mycompany
  access-mode non-transparent
  radius-server 99.100.0.2
  exit
!
line con 0
  exec-timeout 0 0
  transport input none
line aux 0
  exec-timeout 0 0
  transport input all
line vty 0 4
  exec-timeout 0 0
  password mypass
!
end
```



**Index**





---

## Symbols

<cr> [xvii](#)

? command [xvi](#)

---

## A

AAA (authentication, authorization, and accounting)

  GGSN

    configuration (example) [MWC-57](#)

    configuring globally [MWC-36](#)

aaa authentication ppp command [MWC-36](#)

aaa authorization command [MWC-36](#)

aaa new-model command [MWC-36](#)

access groups

*See also* GGSN access groups

access-mode command [MWC-28](#), [MWC-38](#)

access-point command [MWC-28](#), [MWC-38](#)

access point lists

*See* GGSN access point lists

access-point name command [MWC-28](#)

access points

*See* GGSN access points

access-violation command [MWC-28](#)

APN (access point name)

  configuring [MWC-28](#)

  description [MWC-13](#)

authentication command [MWC-42](#)

---

## B

BSC (Base Station Controller)

  (figure) [MWC-12](#)

  description [MWC-12](#)

BSS (Base Station Subsystem), description [MWC-12](#)

BTS (Base Transceiver Station)

  (figure) [MWC-12](#)

  description [MWC-12](#)

---

## C

carriage return (<cr>) [xvii](#)

cautions

  GGSN charging transactions, disabling [MWC-24](#)

  GTP (GPRS Tunneling Protocol), UDP  
    checksum [MWC-33](#)

  usage in text [xii](#)

charging gateways

*See* GGSN charging gateways

Cisco IOS configuration changes, saving [xx](#)

clear gprs charging cdr command [MWC-53](#)

clear gprs gtp statistics command [MWC-53](#)

clear gprs isgsn statistics command [MWC-53](#)

clear gtp pdp-context command [MWC-53](#)

clear l2relay statistics command [MWC-53](#)

clear l2relay topology-map command [MWC-53](#)

command modes, understanding [xv to xvi](#)

commands

  context-sensitive help for abbreviating [xvi](#)

  default form, using [xix](#)

  no form, using [xix](#)

command syntax

  conventions [xi](#)

  displaying (example) [xvii](#)

configurations, saving [xx](#)

crypto ipsec transform-set command [MWC-43](#)

crypto isakmp key command [MWC-43](#)  
 crypto isakmp policy command [MWC-41](#)  
 crypto map command [MWC-44](#)

## D

DHCP (Dynamic Host Configuration Protocol)

and GGSN mobile sessions [MWC-12](#)

GGSN

access points, configuring [MWC-46](#)

configuration (example) [MWC-62](#)

configuration, verifying [MWC-52](#)

configuring on [MWC-45](#)

dhcp-gateway-address command [MWC-28](#)

dhcp-server command [MWC-28, MWC-48](#)

documentation

conventions [xi](#)

feedback, providing [xiii](#)

modules [vii to ix](#)

online, accessing [xii](#)

ordering [xiii](#)

Documentation CD-ROM [xii](#)

documents and resources, supporting [x](#)

## E

encapsulation gtp command [MWC-18](#)

encryption command [MWC-41](#)

## F

fast switching

for GPRS, configuring [MWC-34](#)

Feature Navigator

*See* platforms, supported

filtering output, show and more commands [xx](#)

## G

Ga interfaces

*See* GPRS, interfaces

GGSN (Gateway GPRS Support Node)

configuration (example) [MWC-64](#)

configuration requirements [MWC-17](#)

configuring [MWC-18](#)

description [MWC-7, MWC-11](#)

GGSN access groups, description [MWC-13](#)

GGSN access point lists

configuration (example) [MWC-56](#)

configuring [MWC-28](#)

description [MWC-13](#)

VPN, configuring [MWC-30 to MWC-31](#)

GGSN access points

configuration

verifying [MWC-51](#)

configuring [MWC-28](#)

description [MWC-13](#)

non-transparent access, configuring [MWC-38](#)

planning [MWC-15](#)

RADIUS server, configuration (example) [MWC-58](#)

security, configuring on [MWC-39](#)

*See also* GGSN access point lists

GGSN charging gateways

(example) [MWC-63](#)

configuring [MWC-21](#)

customizing [MWC-23](#)

default, changing [MWC-22](#)

disabling [MWC-24](#)

TCP, configuring [MWC-22](#)

UDP (User Datagram Protocol), configuring [MWC-22](#)

GGSN charging transactions

disabling, (caution) [MWC-24](#)

GGSN physical interfaces

configuration (example) [MWC-57](#)

defining [MWC-25](#)

fast switching, enabling on [MWC-34](#)

- PDN, configuring to [MWC-27](#)
  - Gi interfaces
    - See* GPRS, interfaces
  - global configuration mode, summary of [xvi](#)
  - Gn interfaces
    - See* GPRS, interfaces
  - GPRS (General Packet Radio Service)
    - (figures) [MWC-12, MWC-13](#)
    - description [MWC-7 to MWC-8, MWC-11 to MWC-13](#)
    - interfaces
      - (figure) [MWC-13](#)
      - configuration (example) [MWC-57](#)
      - configuration, verifying [MWC-49](#)
      - configuring to PDN [MWC-27](#)
      - implemented on GGSN [MWC-12](#)
    - `gprs access-point-list` command [MWC-28, MWC-38](#)
    - `gprs charging cdr-aggregation-limit` command [MWC-23](#)
    - `gprs charging cdr-option local-record-sequence-number` command [MWC-23](#)
    - `gprs charging cdr-option node-id` command [MWC-23](#)
    - `gprs charging cdr-option no-partial-cdr-generation` command [MWC-23](#)
    - `gprs charging cdr-option packet-count` command [MWC-23](#)
    - `gprs charging cdr-option served-msisdn` command [MWC-23](#)
    - `gprs charging cg-path-requests` command [MWC-22, MWC-23](#)
    - `gprs charging container volume-threshold` command [MWC-23](#)
    - `gprs charging disable` command [MWC-23, MWC-24](#)
    - `gprs charging flow-control private-echo` command [MWC-23](#)
    - `gprs charging map data tos` command [MWC-23](#)
    - `gprs charging packet-queue-size` command [MWC-23](#)
    - `gprs charging path-protocol` command [MWC-22, MWC-23](#)
    - `gprs charging server-switch-timer` command [MWC-23](#)
    - `gprs charging tariff-time` command [MWC-23](#)
    - `gprs charging transfer interval` command [MWC-23](#)
    - `gprs default charging-gateway` command [MWC-21, MWC-22](#)
    - `gprs default dhcp-server` command [MWC-47](#)
    - `gprs default ip-address-pool` command [MWC-47](#)
    - `gprs default radius-server` command [MWC-39](#)
    - `gprs fastswitch` command [MWC-18, MWC-34](#)
    - `gprs gtp n3-requests` command [MWC-19](#)
    - `gprs gtp path-echo-interval` command [MWC-19, MWC-22](#)
    - `gprs gtp t3-response` command [MWC-19](#)
    - `gprs maximum-pdp-context-allowed` command [MWC-19](#)
    - `gprs radius msisdn first-byte` command [MWC-40](#)
    - `group` command [MWC-42](#)
    - GSM (Global System for Mobile Communications), description [MWC-11](#)
    - GSN (GPRS Support Nodes), description [MWC-12](#)
    - GTP (GPRS Tunneling Protocol)
      - customizing [MWC-19](#)
      - description [MWC-12](#)
      - UDP checksum, (caution) [MWC-33](#)
- 
- ## H
- hardware platforms
    - See* platforms, supported
  - `hash` command [MWC-41](#)
  - `help` command [xvi](#)
- 
- ## I
- IKE (Internet Key Exchange) security protocol
    - GSN, configuring for [MWC-41](#)
  - indexes, master [x](#)
  - `interface` command [MWC-25, MWC-34](#)
  - interface configuration mode, summary of [xvi](#)
  - `interface tunnel` command [MWC-31](#)
  - `interface virtual-template` command [MWC-18, MWC-34](#)
  - `ip-access-group` command [MWC-28](#)
  - `ip address` command [MWC-18, MWC-25, MWC-31](#)
  - `ip address-pool` command [MWC-45](#)
  - `ip-address-pool` command [MWC-29, MWC-48](#)
  - `ip dhcp excluded address` command [MWC-46](#)

ip dhcp pool command [MWC-46](#)  
 ip dhcp-server command [MWC-45](#)  
 ip route-cache command [MWC-25, MWC-34](#)  
 ip route command [MWC-26](#)  
 IPSec (IPSec network security protocol)  
   GGSN  
     configuration (example) [MWC-59](#)  
     configuring on [MWC-40 to MWC-44](#)

---

## L

lifetime command [MWC-42](#)

---

## M

match address command [MWC-44](#)  
 memory  
   GGSN PDP contexts, planning [MWC-15](#)  
 MIB  
   descriptions online [x](#)  
   GPRS [MWC-16](#)  
 mode command [MWC-43](#)  
 modes  
   *See* command modes  
 MS (mobile station), (figure) [MWC-12](#)  
 MSISDN (Mobile Station international PSTN/ISDN)  
   RADIUS requests  
     including in [MWC-40](#)  
     overriding in [MWC-40](#)  
 msisdn suppression command [MWC-29, MWC-40](#)

---

## N

network command [MWC-46](#)  
 notes, usage in text [xii](#)

---

## P

PDN (public packet data network)  
   connections, configuring [MWC-27](#)  
   GGSN access points, configuring for [MWC-28](#)  
 PDP (packet data protocol) contexts, number supported [MWC-15](#)  
 physical interfaces  
   GGSN, configuring on [MWC-25](#)  
   *See* GGSN physical interfaces  
 platforms, supported  
   Feature Navigator, identify using [xxi](#)  
   release notes, identify using [xxi](#)  
 preshared keys [MWC-42](#)  
 privileged EXEC mode, summary of [xvi](#)  
 prompts, system [xvi](#)

---

## Q

question mark (?) command [xvi](#)

---

## R

RADIUS (Remote Access Dial-In User Service)  
   GGSN  
     configuration (example) [MWC-58](#)  
     configuring globally [MWC-37](#)  
     MSISDN, overriding in request [MWC-40](#)  
     MSISDN IE, including in request [MWC-40](#)  
     non-transparent access mode, configuring [MWC-38](#)  
 radius-server command [MWC-29, MWC-39](#)  
 radius-server host command [MWC-37](#)  
 radius-server key command [MWC-37](#)  
 release notes  
   *See* platforms, supported  
 RFC  
   full text, obtaining [x](#)  
 ROM monitor mode, summary of [xvi](#)  
 routes

static  
 GGSN, configuring [MWC-26](#)

## S

security

GGSN

configuring on [MWC-35 to MWC-44](#)  
*See also* AAA (authentication, authorization, and accounting)  
*See also* Cisco IOS Security Configuration Guide  
*See also* IKE (Internet Key Exchange) security protocol  
*See also* IPSec (IPSec network security protocol)  
*See also* RADIUS (Remote Access Dial-In User Service)

service gprs command [MWC-18](#)  
 service gprs ggsn command [MWC-49](#)  
 set peer (IPSec) command [MWC-44](#)  
 set pfs command [MWC-44](#)  
 set security-association level per-host command [MWC-44](#)  
 set security-association lifetime command [MWC-44](#)  
 set transform-set command [MWC-44](#)  
 SGSN (serving GPRS support node), description [MWC-7, MWC-11](#)  
 show gprs access-point all command [MWC-51](#)  
 show gprs access-point command [MWC-53](#)  
 show gprs charging parameters command [MWC-53](#)  
 show gprs charging statistics command [MWC-53](#)  
 show gprs gtp parameters command [MWC-53](#)  
 show gprs gtp path command [MWC-53](#)  
 show gprs gtp pdp-context command [MWC-54](#)  
 show gprs gtp status command [MWC-54](#)  
 show gprs isgsn statistics command [MWC-53](#)  
 show l2relay statistics command [MWC-53](#)  
 show running-configuration command [MWC-49](#)  
 static routes  
 GGSN  
 (example) [MWC-56](#)  
 configuring [MWC-26](#)

subscription-required command [MWC-29](#)

## T

Tab key, command completion [xvi](#)

TCP

GGSN

charging gateway path [MWC-22](#)

transform sets [MWC-43](#)

tunnel destination command [MWC-31](#)

tunnel source command [MWC-31](#)

## U

UDP (User Datagram Protocol), charging gateway path [MWC-22](#)

use-interface command [MWC-29](#)

user EXEC mode, summary of [xvi](#)

## V

virtual template interfaces

GGSN

(example) [MWC-55](#)

configuring [MWC-17, MWC-34](#)

description [MWC-13](#)

fast switching, enabling on [MWC-34](#)

GTP encapsulation, configuring [MWC-18](#)

verifying [MWC-50](#)

VPN (Virtual Private Network)

GGSN, configuration (example) [MWC-57](#)