Cisco GGSN Release 8.0 Command Reference

Cisco IOS Release 12.4(24)T

Last updated February 27, 2009

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

Cisco GGSN Release 8.0 Command Reference, Cisco IOS Release 12.4(24)T

CONTENTS

Cisco IOS Mobile Wireless GGSN Commands

This book documents the Cisco Gateway GPRS Support Note (GGSN) commands available with Cisco IOS Release 12.4(24)T, in alphabetical order.

aaa accounting

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the **aaa accounting** command in global configuration mode. To disable AAA accounting, use the **no** form of this command.

aaa accounting {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level* | **dot1x**} {**default** | *list-name* | **guarantee-first**} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name*

no aaa accounting {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level* | **dot1x**} {**default** | *list-name* | **guarantee-first**} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name*

Syntax Description

auth-proxy	Provides information about all authenticated-proxy user events.
system	Performs accounting for all system-level events not associated with users, such as reloads. **Note** When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes.
network	Runs accounting for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Protocols (NCPs), and AppleTalk Remote Access Protocol (ARAP).
exec	Runs accounting for the EXEC shell session. This keyword might return user profile information such as what is generated by the **autocommand** command.
connection	Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler and disassembler (PAD), and rlogin.
commands *level*	Runs accounting for all commands at the specified privilege level. Valid privilege level entries are integers from 0 through 15.
dot1x	Provides information about all IEEE 802.1x-related user events.
default	Uses the listed accounting methods that follow this keyword as the default list of methods for accounting services.
list-name	Character string used to name the list of at least one of the following accounting methods: • **group radius**—Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command. • **group tacacs+**—Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command. • **group** *group-name*—Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name* argument.
guarantee-first	Guarantees system accounting as the first record.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration. VRF is used *only* with system accounting.

start-stop	Sends a “start” accounting notice at the beginning of a process and a “stop” accounting notice at the end of a process. The “start” accounting record is sent in the background. The requested user process begins regardless of whether the “start” accounting notice was received by the accounting server.
stop-only	Sends a “stop” accounting notice at the end of the requested user process.
none	Disables accounting services on this line or interface.
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
group *group-name*	Specifies the accounting method list. Enter at least one of the following keywords: • **auth-proxy**—Creates a method list to provide accounting information about all authenticated hosts that use the authentication proxy service. • **commands**—Creates a method list to provide accounting information about specific, individual EXEC commands associated with a specific privilege level. • **connection**—Creates a method list to provide accounting information about all outbound connections made from the network access server. • **exec**—Creates a method list to provide accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times. • **network**—Creates a method list to provide accounting information for SLIP, PPP, NCPs, and ARAP sessions. • **resource**—Creates a method list to provide accounting records for calls that have passed user authentication or calls that failed to be authenticated. • **tunnel**—Creates a method list to provide accounting records (Tunnel-Start, Tunnel-Stop, and Tunnel-Reject) for virtual private dialup network (VPDN) tunnel status changes. • **tunnel-link**—Creates a method list to provide accounting records (Tunnel-Link-Start, Tunnel-Link-Stop, and Tunnel-Link-Reject) for VPDN tunnel-link status changes.

Defaults

AAA accounting is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	Group server support was added.
12.1(1)T	The **broadcast** keyword was introduced on the Cisco AS5300 and Cisco AS5800 universal access servers.

Release	Modification
12.1(5)T	The **auth-proxy** keyword was added.
12.2(1)DX	The **vrf** keyword and *vrf-name* argument were introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were integrated into Cisco IOS Release 12.2(13)T.
12.2(15)B	The tunnel and tunnel-link accounting methods were introduced.
12.3(4)T	The tunnel and tunnel-link accounting methods were integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **dot1x** keyword was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.(33)SXH.

Usage Guidelines

General Information

Use the **aaa accounting** command to enable accounting and to create named method lists that define specific accounting methods on a per-line or per-interface basis.

Table 1 contains descriptions of keywords for AAA accounting methods.

Table 1 aaa accounting Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.
group tacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name* argument.

In Table 1, the **group radius** and **group tacacs+** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Cisco IOS software supports the following two methods of accounting:

- RADIUS—The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.
- TACACS+—The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

Method lists for accounting define the way accounting will be performed. Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for particular types of accounting services. Create a list by entering values for the *list-name* argument where *list-name* is any character string used to name this list (excluding the names of methods, such as RADIUS or TACACS+) and method list keywords to identify the methods to be tried in sequence as given.

If the **aaa accounting** command for a particular accounting type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this accounting type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no accounting takes place.

Note System accounting does not use named accounting lists; you can define the default list only for system accounting.

For minimal accounting, include the **stop-only** keyword to send a "stop" record accounting notice at the end of the requested user process. For more accounting, you can include the **start-stop** keyword, so that RADIUS or TACACS+ sends a "start" accounting notice at the beginning of the requested process and a "stop" accounting notice at the end of the process. Accounting is stored only on the RADIUS or TACACS+ server. The **none** keyword disables accounting services for the specified line or interface.

To specify an accounting configuration for a particular VRF, specify a default system accounting method list, and use the **vrf** keyword and *vrf-name* argument. System accounting does not have knowledge of VRF unless specified.

When AAA accounting is activated, the network access server monitors either RADIUS accounting attributes or TACACS+ AV pairs pertinent to the connection, depending on the security method you have implemented. The network access server reports these attributes as accounting records, which are then stored in an accounting log on the security server. For a list of supported RADIUS accounting attributes, see the appendix "RADIUS Attributes" in the *Cisco IOS Security Configuration Guide*. For a list of supported TACACS+ accounting AV pairs, see the appendix "TACACS+ Attribute-Value Pairs" in the *Cisco IOS Security Configuration Guide*.

Note This command cannot be used with TACACS or extended TACACS.

Cisco Service Selection Gateway Broadcast Accounting

To configure Cisco Service Selection Gateway (SSG) broadcast accounting, use ssg_broadcast_accounting for the *list-name* argument. For more information about configuring SSG, see the chapter "Configuring Accounting for SSG" in the *Cisco IOS Service Selection Gateway Configuration Guide*, Release 12.4.

Layer 2 LAN Switch Port

You must configure the RADIUS server to perform accounting tasks, such as logging start, stop, and interim-update messages and time stamps. To turn on these functions, enable logging of "Update/Watchdog packets from this AAA client" in your RADIUS server Network Configuration tab. Next, enable "CVS RADIUS Accounting" in your RADIUS server System Configuration tab.

You must enable AAA before you can enter the **aaa accounting** command. To enable AAA and 802.1X (port-based authentication), use the following global configuration mode commands:

- **aaa new-model**
- **aaa authentication dot1x default group radius**

- **dot1x system-auth-control**

Use the **show radius statistics** command to display the number of RADIUS messages that do not receive the accounting response message.

Establishing a Session with a Router if the AAA Server is Unreachable

The **aaa accounting system guarantee-first** command guarantees system accounting as the first record, which is the default condition. In some situations, users may be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than three minutes.

To establish a console or telnet session with the router if the AAA server is unreachable when the router reloads, use the **no aaa accounting system guarantee-first** command.

Note Entering the **no aaa accounting system guarantee-first** command is not the only condition by which the console or telnet session can be started. For example, if the privileged EXEC session is being authenticated by TACACS and the TACACS server is not reachable, then the session cannot start.

Examples

The following example defines a default commands accounting method list, where accounting services are provided by a TACACS+ security server, set for privilege level 15 commands with a stop-only restriction.

```
aaa accounting commands 15 default stop-only group tacacs+
```

The following example defines a default auth-proxy accounting method list, where accounting services are provided by a TACACS+ security server with a start-stop restriction. The **aaa accounting** command activates authentication proxy accounting.

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization auth-proxy default group tacacs+
aaa accounting auth-proxy default start-stop group tacacs+
```

The following example defines a default system accounting method list, where accounting services are provided by RADIUS security server “server1” with a start-stop restriction. The **aaa accounting** command specifies accounting for vrf “vrf1.”

```
aaa accounting system default vrf vrf1 start-stop group server1
```

The following example defines a default IEEE 802.1x accounting method list, where accounting services are provided by a RADIUS server. The **aaa accounting** command activates IEEE 802.1x accounting.

```
aaa new model
aaa authentication dot1x default group radius
aaa authorization dot1x default group radius
aaa accounting dot1x default start-stop group radius
```

The following example shows how to enable network accounting and send tunnel and tunnel-link accounting records to the RADIUS server. (Tunnel-Reject and Tunnel-Link-Reject accounting records are automatically sent if either start or stop records are configured.)

```
aaa accounting network tunnel start-stop group radius
aaa accounting network session start-stop group radius
```

The following example shows how to enable IEEE 802.1x accounting:

```
aaa accounting dot1x default start-stop group radius
aaa accounting system default start-stop group radius
```

Related Commands

Command	Description
aaa authentication dot1x	Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa group server tacacs+	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
dot1x system-auth-control	Enables port-based authentication.
radius-server host	Specifies a RADIUS server host.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.
tacacs-server host	Specifies a TACACS+ server host.

aaa group server diameter

To group different server hosts into distinct lists and distinct methods, use the **aaa group server diameter** command in access-point configuration mode. To remove a group, use the **no** form of this command

aaa group server diameter *group-name*

no aaa group server diameter *group-name*

Syntax Description

diameter	Defines a Diameter authentication, authorization, and accounting (AAA) group.
group name	Character string used to name the group of servers.

Defaults

No default behavior or values.

Command Modes

Access-point configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The AAA server-group feature provides a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.

A server group is a list of server hosts of a particular type. Currently supported server host types are RADIUS server hosts, TACACS+ server hosts, and Diameter server hosts. A server group is used in conjunction with a global server host list. The server group lists the IP addresses of the selected server hosts.

Note Using the **aaa group server diameter** command you can configure a primary and secondary Diameter credit control applicaiton (DCCA) server. If the transport connection to the primary DCCA server should fail, a connection to the secondary DCCA server in the group will be established.

Examples

The following example shows the configuration of two AAA consisting of DCCA server hosts named dcca-sg1 and dcca-sg2:

```
aaa group server diameter dcca-sg1
  server dcca1

aaa group server diameter dcca-sg2
  server dcca2
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authorization	Sets parameters that restrict user access to a network.
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa accounting	Enables or disables accounting for a particular access point on the GGSN.
show gprs access-point	Displays information about access points on the GGSN.

aaa-group

To specify an authentication, authorization, and accounting (AAA) server group and assign the type of AAA services to be supported by the server group for a particular access point on the gateway GPRS support node (GGSN), use the **aaa-group** command in access-point configuration mode. To remove an AAA server group, use the **no** form of this command.

aaa-group {**authentication** | **accounting**} *server-group*

no aaa-group {**authentication** | **accounting**} *server-group*

Syntax Description

authentication	Assigns the selected server group for authentication services on the access point name (APN).
accounting	Assigns the selected server group for accounting services only on the APN.
server-group	Specifies the name of an AAA server group to be used for AAA services on the APN. **Note** The name of the AAA server group that you specify must correspond to a server group that you configure using the **aaa group server** command.

Defaults

No default behavior or values.

Command Modes

Access-point configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The Cisco GGSN supports authentication and accounting at APNs using AAA server groups. By using AAA server groups, you gain the following benefits:

- You can selectively implement groups of servers for authentication and accounting at different APNs.
- You can configure different server groups for authentication services and accounting services in the same APN.

- You can control which RADIUS services you want to enable at a particular APN, such as AAA accounting.

The GGSN supports the implementation of AAA server groups at both the global and access-point configuration levels. You can minimize your configuration by specifying the configuration that you want to support across most APNs, at the global configuration level. Then, at the access-point configuration level, you can selectively modify the services and server groups that you want to support at a particular APN. Therefore, you can override the AAA server global configuration at the APN configuration level.

To configure a default AAA server group to be used for all APNs on the GGSN, use the **gprs default aaa-group** global configuration command. To specify a different AAA server group to be used at a particular APN for authentication or accounting, use the **aaa-group** access-point configuration command.

If accounting is enabled on the APN, then the GGSN looks for an accounting server group to be used for the APN in the following order:

- First, at the APN for an accounting server group—configured in the **aaa-group accounting** command.
- Second, for a global GPRS default accounting server group—configured in the **gprs default aaa-group accounting** command.
- Third, at the APN for an authentication server group—configured in the **aaa-group authentication** command.
- Last, for a global GPRS default authentication server group—configured in the **gprs default aaa-group authentication** command.

If none of the above commands is configured on the GGSN, then AAA accounting is not performed.

If authentication is enabled on the APN, then the GGSN first looks for an authentication server group at the APN, configured in the **aaa-group authentication** command. If an authentication server group is not found at the APN, then the GGSN looks for a globally configured, GGSN default authentication server group, configured in the **gprs default aaa-group authentication** command.

To complete the configuration, you also must specify the following configuration elements on the GGSN:

- Enable AAA services using the **aaa new-model** global configuration command.
- Configure the RADIUS servers using the **radius-server host** command.
- Define a server group with the IP addresses of the RADIUS servers in that group using the **aaa group server** global configuration command.
- Configure the following AAA services:
  - AAA authentication using the **aaa authentication** global configuration command
  - AAA authorization using the **aaa authorization** global configuration command
  - AAA accounting using the **aaa accounting** global configuration command
- Enable the type of AAA services (accounting and authentication) to be supported on the APN.
  - The GGSN enables accounting by default for non-transparent APNs.

    You can enable or disable accounting services at the APN using the **aaa-accounting** command.
  - Authentication is enabled by default for non-transparent APNs. There is not any specific command to enable or disable authentication. Authentication cannot be enabled for transparent APNs.

You can verify the AAA server groups that are configured for an APN using the **show gprs access-point** command.

Note For more information about AAA and RADIUS global configuration commands, see the *Cisco IOS Security Command Reference.*

Examples

The following configuration example defines four AAA server groups on the GGSN: foo, foo1, foo2, and foo3, shown by the **aaa group server** commands.

Using the **gprs default aaa-group** command, two of these server groups are globally defined as default server groups: foo2 for authentication, and foo3 for accounting.

At access-point 1, which is enabled for authentication, the default global authentication server group of foo2 is overridden and the server group named foo is designated to provide authentication services on the APN. Notice that accounting services are not explicitly configured at that access point, but are automatically enabled because authentication is enabled. Because there is a globally defined accounting server-group defined, the server named foo3 will be used for accounting services.

At access-point 2, which is enabled for authentication, the default global authentication server group of foo2 is used. Because there is a globally defined accounting server-group defined, the server named foo3 will be used for accounting services.

At access-point 4, which is enabled for accounting using the **aaa-accounting enable** command, the default accounting server group of foo3 is overridden and the server group named foo1 is designated to provide accounting services on the APN.

Access-point 5 does not support any AAA services because it is configured for transparent access mode, and accounting is not enabled.

```
aaa new-model
!
aaa group server radius foo
 server 10.2.3.4
 server 10.6.7.8
aaa group server radius foo1
 server 10.10.0.1
aaa group server radius foo2
 server 10.2.3.4
 server 10.10.0.1
aaa group server foo3
 server 10.6.7.8
 server 10.10.0.1
!
aaa authentication ppp foo group foo
aaa authentication ppp foo2 group foo2
aaa authorization network default group radius
aaa accounting exec default start-stop group foo
aaa accounting network foo1 start-stop group foo1
aaa accounting network foo2 start-stop group foo2
aaa accounting network foo3 start-stop group foo3
!
gprs access-point-list gprs
 access-point 1
  access-mode non-transparent
  access-point-name www.pdn1.com
  aaa-group authentication foo
!
 access-point 2
  access-mode non-transparent
```

```
  access-point-name www.pdn2.com
!
 access-point 4
  access-point-name www.pdn4.com
  aaa-accounting enable
  aaa-group accounting foo1
!
 access-point 5
  access-point-name www.pdn5.com
!
gprs default aaa-group authentication foo2
gprs default aaa-group accounting foo3
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.10.0.1 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authorization	Sets parameters that restrict user access to a network.
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa accounting	Enables or disables accounting for a particular access point on the GGSN.
gprs default aaa-group	Specifies a default RADIUS server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN.
radius-server host	Specifies a RADIUS server host.
show gprs access-point	Displays information about access points on the GGSN.

access-mode

To specify whether the gateway GPRS support node (GGSN) requests user authentication at the access point to a public data network (PDN), use the **access-mode** command in access-point configuration mode. To remove an access mode and return to the default value, use the **no** form of this command.

access-mode {**transparent** | **non-transparent**}

no access-mode {**transparent** | **non-transparent**}

Syntax Description

transparent	Specifies that the users who access the PDN through the access point associated with the current virtual template are allowed access without authorization or authentication.
non-transparent	Specifies that the users who access the PDN through the current virtual template must be authenticated by the GGSN acting as a proxy for the authentication.

Defaults

transparent

Command Modes

Access-point configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **access-mode** command to specify whether users accessing a PDN through a particular access point associated with the virtual template interface will have transparent or non-transparent access to the network.

Transparent access means that users who access the PDN through the current virtual template are granted access without further authentication.

Non-transparent access means that users who access the PDN through the current virtual template must be authenticated by the GGSN. You must configure non-transparent access to support RADIUS services at an access point. Authentication is performed by the GGSN while establishing the PDP context.

Examples

Example 1

The following example specifies transparent access to the PDN, gprs.pdn2.com, through access point 2:

```
interface virtual-template 1
 gprs access-point-list abc
!
gprs access-point-list abc
 access-point 2
  access-point-name gprs.pdn2.com
```

Example 2

The following example specifies non-transparent access to the PDN, gprs.pdn.com, through access point 1:

```
interface virtual-template 1
 gprs access-point-list abc
!
gprs access-point-list abc
 access-point 1
  access-point-name gprs.pdn.com
  access-mode non-transparent
```

Note Because transparent is the default access mode, it does not appear in the output of the **show running-configuration** command for the access point.

Related Commands

Command	Description
aaa-group	Specifies an AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN.
access-point	Specifies an access-point number and enters access-point configuration mode.
gprs default aaa-group	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN.

access-point

To specify an access point number and enter access-point configuration mode, use the **access-point** command in access-point list configuration mode. To remove an access point number, use the **no** form of this command.

access-point *access-point-index*

no access-point *access-point-index*

Syntax Description

access-point-index	Integer from 1 to 65535 that identifies a gateway GPRS support node (GGSN) access point.

Defaults

No default behavior or values.

Command Modes

Access-point list configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **access-point** command to create an access point to a public data network (PDN).

To configure an access point, first set up an access-point list using the **gprs access-point-list** command, and then add the access point to the access-point list.

You can specify access point numbers in any sequence.

Note Memory constraints might occur if you define a large number of access points to support VPN routing and forwarding (VRF).

Examples

The following example configures an access point with an index number of 7 in an access-point-list named “abc” on the GGSN:

```
gprs access-point-list abc
 access-point 7
```

Related Commands

Command	Description
access-point-name	Specifies the network (or domain) name for a PDN that users can access from the GGSN at a defined access point.
gprs access-point-list	Configures an access point list that you use to define PDN access points on the GGSN.

access-point-name

To specify the network (or domain) name for a public data network (PDN) that users can access from the gateway GPRS support node (GGSN) at a defined access point, use the **access-point-name** command in access-point configuration mode. To remove an access point name, use the **no** form of this command.

access-point-name *apn-name*

no access-point-name

Syntax Description

apn-name	Specifies the network or domain name of the private data network that can be accessed through the current access point.

Defaults

There is no default value for this command.

Command Modes

Access-point configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **access-point-name** command to specify the PDN name of a network that can be accessed through a particular access point. An access-point name is mandatory for each access point.

To configure an access point, first set up an access-point list using the **gprs access-point-list** command, and then add the access point to the access-point list.

The access point name typically is the domain name of the service provider that users access—for example, www.isp.com.

Examples

The following example specifies the access-point name for a network:

```
access-point 1
 access-point-name www.isp.com
 exit
```

Related Commands

Command	Description
access-point	Specifies an access point number and enters access-point configuration mode.

access-type

To specify whether an access point is real or virtual on the gateway GPRS support node (GGSN), use the **access-type** command in access-point configuration mode. To return to the default value, use the **no** form of this command.

access-type {**virtual** [**pre-authenticate [default-apn** *apn-name***]**] | **real**}

no access-type

Syntax Description

virtual [pre-authenticate [default-apn *apn-name***]]**	Specifies an access point name (APN) type that is not associated with any specific physical target network on the GGSN. Optionally, specify the **pre-authenticate** keyword to enable a virtual APN to be dynamically mapped, per-user, to a target APN during a pre-authentication phase, and if desired, specify a default real APN to be used if the target APN is not resolved.
real	Specifies an APN type that corresponds to an external physical network to a public data network (PDN) on the GGSN. This is the default value.

Defaults

real

Command Modes

Access-point configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into the Cisco IOS Release 12.3(14)YU and the **pre-authenticate** keyword option was added.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **access-type** command to specify whether an access point is real or virtual on the GGSN.

The default access-type is real. Therefore, you need to configure this command only if the APN needs to be a virtual access point.

Virtual access types are used to configure virtual APN support on the Cisco GGSN to minimize provisioning issues in other GPRS/UMTS network entities that require configuration of APN information.

By default, using the virtual APN feature on the GGSN, home location register (HLR) subscription data can simply provide the name of the virtual APN. Users can still request access to specific target networks that are accessible by the GGSN without requiring each of those destination APNs to be provisioned at the HLR.

The default keyword, **real**, identifies a physical target network that the GGSN can reach. Real APNs must always be configured on the GGSN to reach external networks.

Virtual APNs can be configured in addition to real access points to ease provisioning in the GPRS/UMTS public land mobile network (PLMN).

Note If the access type is virtual, some of the access-point configuration commands are not applicable, and if configured, will be ignored.

The default virtual APN support relies on the domain portion of the username to resolve the target APN. Once, the target is resolved, the user is then connection to that APN on the GGSN.

Cisco GGSN Release 6.0, Cisco IOS Release 12.3(14) and later, supports pre-authentication-based virtual access points. The pre-authentication-based virtual APN feature utilizes AAA servers to provide dynamic, per-user mapping of a virtual APN to a target (real) APN.

When the **pre-authenticate** keyword option is specified when configuring a virtual APN, a pre-authentication phase is applied to Create PDP Context requests received that include a virtual APN in the APN information element.

Pre-authentication-based virtual APN requires that the AAA server be configured to provision user profiles to include the target APN. The AAA maps a user to the target using user identifications such as the IMSI, user name, or MSISDN, etc. Additionally, the target APN must be locally configured on the GGSN.

The following is the typical call flow with regard to external AAA servers when a virtual APN is involve:

1. The GGSN receives a Create PDP Context Request that includes a virtual APN. It locates the virtual APN and starts a pre-authentication phase for the PDP context by sending an Access-Request message to an AAA server.
2. The AAA server does a lookup based on the user identification (username, MSISDN, IMSI, etc.) included in the Access-Request message, and determines the target-APN for the user from the user profile. The target APN is returned as a Radius attribute in the Access-Accept message to the GGSN.
3. The GGSN checks for a locally-configured APN that matches the APN name in the target APN attribute in the Access-Accept message.
   - I f a match is found, the virtual APN is resolved and the Create PDP Context Request is redirected to the target APN and is further processed using the target APN (just as if the target APN was included in the original Create PDP Context request). If the real APN is non-transparent, another Access-Request is sent out. Typically, the AAA server should be different.
   - If a match is not found, the Create PDP Context Request is rejected.
   - If there is no target APN included in the RADIUS attribute in the access-accept message to the GGSN, or if the target APN is not locally configured, the Create PDP Context Request is rejected.
4. GGSN receives an access-accept from the AAA server for the second round of authentication.

When configuring pre-authentication-based virtual APN functionality, please note the following:

When configuring pre-authentication-based virtual APN functionality, please note the following:

- If a user profile on the AAA server is configured to include a target APN, then the target APN should be a real APN, and it should be configured on the GGSN.
- An APN can only be configured for domain-based virtual APN functionality or pre-authentication-based APN functionality, not both.
- The target APN returned from AAA must be a real APN, and if more than one APN is returned, the first one is used and the rest ignored.
- Configure anonymous user access under the virtual APN (using the **anonymous user** access-point configuration command) to mobile stations (MS) to access without supplying the username and password (the GGSN uses the common password configured on the APN).
- At minimum, an AAA access-method must be configured under the virtual APN, or globally. If a method is not configured, the create PDP request will be rejected.
- The associated real APN name is used in G-CDRs and authentication requests sent to a virtual APN

Note For virtual APNs, the domain is always removed from the username attribute. The associated real APN name is used in G-CDRs and authentication requests sent to a virtual APN.

Examples

Example 1

The following example shows configuration of a virtual access point type and a real access point type:

```
access-point 1
 access-point-name corporate
 access-type virtual
 exit
access-point 2
 access-point-name corporatea.com
 ip-address-pool dhcp-client
 dhcp-server 10.21.21.1
```

Example 2

The following example enables pre-authentication-based virtual APN functionality for virtual access point and specifies “cisco.com” as the default APN if a target APN is not resolved.

```
access-point 1
 access-point-name virtual-apn-all
 access-type virtual pre-authenticate default-apn cisco.com
 anonymous user anyone abc
 radius attribute user-name msisdn
 exit
```

Related Commands

Command	Description
access-point	Specifies an access point number and enters access-point configuration mode.
access-point-name	Specifies the network (or domain) name for a PDN that users can access from the GGSN at a defined access point.

access-violation deactivate-pdp-context

To specify that a user's session be ended and the user packets discarded when a user attempts unauthorized access to a public data network (PDN) through an access point, use the **access-violation deactivate-pdp-context** command in access-point configuration mode. To return to the default value, use the **no** form of this command.

access-violation deactivate-pdp-context

no access-violation deactivate-pdp-context

Syntax Description

This command has no arguments or keywords.

Defaults

The user's session remains active and the user packets are discarded.

Command Modes

Access-point configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW and the **discard-packets** option was removed.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **access-violation deactivate-pdp-context** command to specify the action that is taken if a user attempts unauthorized access through the specified access point.

The default is that the gateway GPRS support node (GGSN) simply drops user packets when an unauthorized access is attempted. However, if you specify **access-violation deactivate-pdp-context**, the GGSN terminates the user's session in addition to discarding the packets.

Examples

The following example shows deactivation of a user's access and discarding of the user packets:

```
access-point 1
 access-point-name pdn.aaaa.com
 ip-access-group 101 in
 access-violation deactivate-pdp-context
 exit
```

Related Commands

Command	Description
access-point-name	Specifies the network (or domain) name for a PDN that users can access from the GGSN at a defined access point.

address ipv4

To configure a route to the host of the Diameter peer using IPv4, use the **address ipv4** command in Diameter peer configuration mode. To remove the address, use the **no** form of this command.

address ipv4 *ip-address*

no address ipv4 *ip-address*

Syntax Description

ip-address	IP address of the host of the Diameter peer.

Defaults

No default behavior or values.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **address ipv4** command to define the IP address of the host of the Diameter peer using IPv4.

Examples

The following configuration example defines the IP address of the host of the Diameter peer as 10.10.10.1:

```
diameter peer dcca1
 address ipv4 10.10.10.1
```

Related Commands .

Command	Description
destination host	Configures the Fully Qualified Domain Name (FQDN) of the Diameter peer
destination realm	Configures the destination realm (domain name) in which the Diameter host is located.
diameter peer	Defines the Diameter peer (server) and enters diameter peer configuration mode.
ip vrf forwarding	Defines the VRF associated with the Diameter peer.
security	Configures the security protocol to use for the Diameter peer-to-peer connection.
source interface	Configures the interface to use to connect to the Diameter peer.
timer	Configures Diameter base protocol timers for peer-to-peer communication.
transport	Configures the transport protocol to use to connect with the Diameter peer.

advertise downlink next-hop

To configure the next hop address (the user address) on the gateway GPRS support node (GGSN) downlink traffic to be advertised in Accounting Start requests, use the **advertise downlink next-hop** command in access-point configuration mode. To remove a next hop address configuration, use the **no** form of this command.

advertise downlink next-hop *ip-address*

no advertise downlink next-hop *ip-address*

Syntax Description

ip-address	IP address of the next hop for downlink traffic destined for the GGSN.

Defaults

No default behavior or values.

Command Modes

Access-point configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **advertise downlink next-hop** command to configure the next hop IP address, to which downlink traffic destined for the GGSN is to be routed (Cisco Content Services Gateway [CSG]-to-GGSN) , to be advertised in Accounting Start requests.

Examples

The following configuration example configures 10.10.150.2 as the next hop address to be advertised:

```
advertise downlink next-hop 10.10.150.2
```

Related Commands

Command	Description
show access-point	Displays information about access points on the GGSN.

aggregate

To configure the gateway GPRS support node (GGSN) to create an aggregate route in its IP routing table, when receiving packet data protocol (PDP) requests from mobile stations (MSs) on the specified network, for a particular access point on the GGSN, use the **aggregate** command in access-point configuration mode. To remove an aggregate route, use the **no** form of this command.

aggregate {**auto** | *ip-network-prefix*{*/mask-bit-length* | *ip-mask*}}

no aggregate {**auto** | *ip-network-prefix*{*/mask-bit-length* | *ip-mask*}}

Syntax Description

auto	IP address mask sent by the DHCP or RADIUS server is used by the access point for route aggregation.
ip-network-prefix	Dotted decimal notation of the IP network address to be used by the GGSN for route aggregation, in the format *a.b.c.d*.
/mask-bit-length	Number of bits (as an integer) that represent the network portion of the specified IP network address. A forward slash is required before the integer. **Note** There is no space between the *ip-network-prefix* and the slash (/).
ip-mask	Dotted decimal notation of the IP network mask (in the format *e.f.g.h*.), which represents the network and host portion of the specified IP network address.

Defaults

No default behavior or values.

Command Modes

Access-point configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The GGSN uses a static host route to forward user data packets received from the Gi interface to the Gn interface, using the virtual template interface of the GPRS tunneling protocol (GTP) tunnel.

Without the **aggregate** command or **gprs default aggregate** command, the GGSN creates a static host route for each PDP context. For example, for 45,000 PDP contexts supported, the GGSN creates 45,000 static host routes in its IP routing table.

You can use the **aggregate** command to reduce the number of static routes implemented by the GGSN for PDP contexts at a particular access point. The **aggregate** command allows you to specify an IP network prefix to combine the routes of PDP contexts from the same network as a single route on the GGSN.

To configure the GGSN to automatically aggregate routes that are returned by a DHCP or RADIUS server, use the **aggregate auto** command at the APN.

Note The **aggregate auto** command will not aggregate routes when using local IP address pools.

Automatic route aggregation can be configured only at the access-point configuration level on the GGSN. The **gprs default aggregate** global configuration command does not support the **auto** option; therefore, you cannot configure automatic route aggregation globally on the GGSN.

You can specify multiple **aggregate** commands at each access point to support multiple network aggregates. However, if you use the **aggregate auto** command at the access point name (APN), you cannot specify any other aggregate route ranges at the APN.

To globally define an aggregate IP network address range for all access points on the GGSN for statically derived addresses, you can use the **gprs default aggregate** command. You can use the **aggregate** command to override this default address range at a particular access point.

The GGSN responds in the following manner to manage routes for MSs through an access point, when route aggregation is configured in the following scenarios:

- No aggregation is configured on the GGSN, at the APN or globally—The GGSN inserts the 32-bit host route of the MS into its routing table as a static route.
- A default aggregate route is configured globally, but no aggregation is configured at the APN:
  - If a statically or dynamically derived address for an MS matches the default aggregate route range, the GGSN inserts an aggregate route into its routing table.
  - If the MS address does not match the default aggregate route, the GGSN inserts the 32-bit host route as a static route into the routing table.
- A default aggregate route is configured globally, and automatic route aggregation is configured at the APN:
  - If a statically derived address for an MS matches the default aggregate route range, the GGSN inserts an aggregate route into its routing table.
  - If a statically derived address for an MS does not match the default aggregate route, the GGSN inserts the 32-bit host route as a static route into its routing table.
  - If a dynamically derived address for an MS is received, the GGSN aggregates the route, based on the address and mask returned by the DHCP or RADIUS server.

- A default aggregate route is configured globally, and an aggregate route is also configured at the APN:
  - If a statically or dynamically derived address for an MS matches the aggregate range at the APN through which it was processed, or otherwise matches the default aggregate range, the GGSN inserts an aggregate route into its routing table.
  - If a statically or dynamically derived address for an MS does not match either the aggregate range at the APN or the global default aggregate range, the GGSN inserts the 32-bit host route as a static route into its routing table.

Use care when assigning IP addresses to an MS before you configure the aggregation ranges on the GGSN. A basic guideline is to aggregate as many addresses as possible, but to minimize your use of aggregation with respect to the total amount of IP address space being used by the access point.

Note The **aggregate** command and **gprs default aggregate** commands affect routing on the GGSN. Use care when planning and configuring IP address aggregation.

Use the **show gprs access-point** command to display information about the aggregate routes that are configured on the GGSN. The aggregate output field appears only when aggregate routes have been configured on the GGSN or when the **auto** option is configured.

Use the **show ip route** command to verify whether the static route is in the current IP routing table on the GGSN. The static route created for any PDP requests (aggregated or non-aggregated) appears with the code "U" in the routing table, indicating a per-user static route.

Note The **show ip route** command displays a static route for aggregated PDP contexts only if PDP contexts on that network have been created on the GGSN. If you configure route aggregation on the GGSN, but no PDP requests have been received for that network, the static route does not appear.

Examples

Example 1

The following example specifies two aggregate network address ranges for access point 8. The GGSN will create aggregate routes for PDP context requests received from MSs with IP addresses on the networks 172.16.0.0 and 10.0.0.0:

```
gprs access-point-list gprs
 access-point 8
   access-point-name pdn.aaaa.com
   aggregate 172.16.0.0/16
   aggregate 10.0.0.0/8
```

Note Regardless of the format in which you configure the **aggregate** command, the output from the **show running-configuration** command always displays the network in the dotted decimal/integer notation.

Example 2

The following example shows a route aggregation configuration for access point 8 using DHCP on a GGSN implement on the Cisco 7200 series router platform, along with the associated output from the **show gprs gtp pdp-context all** command and the **show ip route** commands.

Notice that the **aggregate auto** command is configured at the access point where DHCP is being used. The **dhcp-gateway-address** command specifies the subnet addresses to be returned by the DHCP server. This address should match the IP address of a loopback interface on the GGSN. In addition, to accommodate route aggregation for another subnet 10.80.0.0, the **gprs default aggregate** global configuration command is used.

In this example, the GGSN aggregates routes for dynamically derived addresses for MSs through access point 8, based on the address and mask returned by the DHCP server. For PDP context requests received for statically derived addresses on the 10.80.0.0 network, the GGSN also implements an aggregate route into its routing table, as configured by the **gprs default aggregate** command.

```
interface Loopback0
 ip address 10.80.0.1 255.255.255.255
!
interface Loopback2
 ip address 10.88.0.1 255.255.255.255
!
gprs access-point-list gprs
 access-point 8
   access-point-name pdn.aaaa.com
   ip-address-pool dhcp-proxy-client
   aggregate auto
   dhcp-server 172.16.43.35
   dhcp-gateway-address 10.88.0.1
   exit
!
gprs default aggregate 10.80.0.0 255.255.255.0
```

In the following output for the **show gprs gtp pdp-context all** command, 5 PDP context requests are active on the GGSN for pdn.aaaa.com from the 10.88.0.0/24 network:

```
GGSN# show gprs gtp pdp-context all
TID              MS Addr         Source  SGSN Addr       APN
6161616161610001 10.88.0.1       DHCP    172.16.123.1    pdn.aaaa.com
6161616161610002 10.88.0.2       DHCP    172.16.123.1    pdn.aaaa.com
6161616161610003 10.88.0.3       DHCP    172.16.123.1    pdn.aaaa.com
6161616161610004 10.88.0.4       DHCP    172.16.123.1    pdn.aaaa.com
6161616161610005 10.88.0.5       DHCP    172.16.123.1    pdn.aaaa.com
```

The following output for the **show ip route** command shows a single static route in the IP routing table for the GGSN, which routes the traffic for the 10.88.0.0/24 subnet through the virtual template (or Virtual-Access1) interface:

```
GGSN# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.80.0.0/16 is subnetted, 1 subnets
C       10.80.0.0 is directly connected, Loopback0
     10.113.0.0/16 is subnetted, 1 subnets
C       10.113.0.0 is directly connected, Virtual-Access1
     172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
C       172.16.43.192/28 is directly connected, FastEthernet0/0
S       172.16.43.0/24 is directly connected, FastEthernet0/0
S       172.16.43.35/32 is directly connected, Ethernet2/3
```

```
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
U       10.88.0.0/24 [1/0] via 0.0.0.0, Virtual-Access1
C       10.88.0.0/16 is directly connected, Loopback2
```

Related Commands

Command	Description
gprs default aggregate	Configures the GGSN to create an aggregate route in its IP routing table when receiving PDP requests from MSs on the specified network for any access point on the GGSN.
show gprs access-point	Displays information about access points on the GGSN.
show ip route	Displays all static IP routes, or those installed using the AAA route download function.

anonymous user

To configure anonymous user access at an access point, use the **anonymous user** command in access-point configuration mode. To remove the username configuration, use the **no** form of this command.

anonymous user *username* [*password*]

no anonymous user

Syntax Description

username	Alphanumeric string identifying user. The username argument can be only one word. It can contain any combination of numbers and characters.
password	Alphanumeric string. The password argument can be only one word. It can contain any combination of numbers and characters.

Defaults

No default behavior or values.

Command Modes

Access-point configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use this command to allow a mobile station (MS) to access a non-transparent mode access point name (APN) without supplying the username and password in the GPRS tunneling protocol (GTP) protocol configuration option (PCO) information element (IE) of the Create PDP Context request message. The GGSN will use the username and password configured on the APN for the user session.

This command enables anonymous access, which means that a PDP context can be created by an MS to a specific host without specifying a username and password.

Examples

The following example specifies the username george and the password abcd123 for anonymous access at access point 49:

```
gprs access-point-list abc
 access-point 49
   access-point-name www.pdn.com
   anonymous user george abcd123
```

authorization

To define a method of authorization (AAA method list), in the Diameter credit control application (DCCA) client profile, that is used to specify the Diameter server groups, use the **authorization** command in DCCA client profile configuration mode. To remove the method list configuration, use the **no** form of this command

authorization *method-list*

no authorization *method-list*

Syntax Description

method-list	Name of the method list defined using the **aaa authorization** command that describes the authorization methods to be queried for a user.

Defaults

No default behavior or values.

Command Modes

DCCA client profile configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **authorization** command to define the method list to be used by the DCCA client to authorize users. The method list specifies the Diameter server groups to use for authorization and was created using the **aaa authorization** global configuration command.

Examples

The following configuration example defines dcca-method1 as the method of authorization for a DCCA client:

```
gprs dcca profile dcca-profile1
  authorization dcca-method
```

Related Commands

Command	Description
ccfh	Configures the CCFH AVP locally to use for a credit-control session when the CCA sent by the DCCA server does not contain CCFH value.
content dcca profile	Defines the DCCA client profile in a GGSN charging profile.
destination-realm	Configures the destination realm to be sent in CCR initial requests to a DCCA server.
gprs dcca profile	Defines a DCCA client profile on the GGSN and enters DCCA client profile configuration mode.

Command	Description
session-failover	Configures CCSF AVP support when a CCA message from the DCCA server does not contain a value for the CCSF AVP.
trigger	Specifies that SGSN and QoS changes will trigger a DCCA client to request quota-reauthorization
tx-timeout	Configures a TX timeout value used by the DCCA client to monitor the communication of CCRs with a Diameter server.

auto-retrieve

To configure the gateway GPRS support node (GGSN) to automatically initiate a G-CDR retrieval from the PSDs defined in a Cisco Persitent Storage Device (PSD) server group when a charging gateway becomes active, use the **auto-retrieve** command in PSD group configuration mode. To return to the default value, use the **no** form of this command.

auto-retrieve *max-retrieve-rate*

no auto-retrieve *max-retrieve-rate*

Syntax Description

group-name	Specifies the maximum number of retrieval requests that can be sent from the GGSN to the PSDs per minute. Valid value is a number between 1 and 600.

Defaults

60.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YU	This command was introduced.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.
12.4(9)XG	This command was integrated into Cisco IOS Release 12.4(9)XG.

Usage Guidelines

Use the **auto-retrieve** command to configure the GGSN to automatically retrieve G-CDRs from a PSD. When the **auto-retrieve** command is configured, the GGSN retrieves G-CDRs from the PSDs defined in the PSD server group. It initiates a retrieval from the "retrieve-only" PSD first, and then retrieves the G-CDRs from the local PSD.

If a retrieve-only PSD has been configured without the **auto-retrieve** command configured, the GGSN will not initiate a start retrieve when a retrieving event occurs.

Note PSD auto-retrieval is supported for GTPv0 and GTPv1 IP PDP type PDP contexts on the Cisco 7600 series router platform.

Examples

The following example configures the GGSN to automatically retrieve G-CDRs from the PSDs, using the default 60 as the number of retrieval requests that can be sent from the GGSN to the PSD per minute:

```
auto-retrieve
```

Command History

Command	Description
clear data-store statistics	Clears PSD-related statistics.
data-store	Configures a PSD server group on the GGSN to use for GGSN-to-PSD communication.
show data-store	Displays the status of the PSD client and PSD server-related information.
show data-store statistics	Displays PSD client statistics.

bandwidth

To define the total bandwidth for a bandwidth pool, use the **bandwidth** command in bandwidth pool configuration mode. To return to the default value, use the **no** form of this command.

bandwidth *value*

no bandwidth *value*

Syntax Description

value	Specifies the total bandwidth, in kilobits per second, for a bandwidth pool. Valid value is a number from 1 to 4294967295.

Defaults

No default behavior or values.

Command Modes

Bandwidth pool configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **bandwidth** bandwidth pool configuration command to define the total bandwidth for a bandwidth pool.

Note Before configuring the total bandwidth for a bandwidth pool, the pool must be created using the **gprs qos bandwidth-pool** global configuration command.

The total bandwidth defined for a bandwidth pool can be subdivided among traffic classes using the **traffic-class** bandwidth pool configuration command.

Examples

The following example allocates 10000 kilobits per second for the bandwidth pool “poolA”:

```
gprs qos bandwidth-pool poolA
 bandwidth 10000
```

Related Commands

Command	Description
bandwidth	Defines the total bandwidth, in kilobits per second, for a bandwidth pool. Valid values are 1 to 4292967295.
bandwidth-pool	Enables the CAC bandwidth management function and applies a bandwidth pool to an APN.
gprs qos bandwidth-pool	Creates or modifies a bandwidth pool.
traffic-class	Allocates bandwidth pool bandwidth to a specific traffic class.

bandwidth-pool

To enable the Call Admission Control (CAC) bandwidth management function and apply a bandwidth pool to anaccess point name (APN), use the **bandwidth-pool** command in access-point configuration mode. To return to the default value, use the **no** form of this command.

bandwidth-pool {input | output} *pool-name*

no bandwidth-pool {input | output} *pool-name*

Syntax Description

input	Specifies that the bandwidth pool applies to the output (Gn) interface in the downlink direction.
output	Specifies that the bandwidth pool applies to the output (Gi) interface in the uplink direction.
pool-name	Name (up to 40 characters) of the bandwidth pool that is being associated to an APN.

Defaults

Disabled

Command Modes

Access-point configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **bandwidth-pool** access-point configuration command to enable the CAC bandwidth management function and apply a bandwidth pool to an APN.

Note A CAC bandwidth pool can be applied to one or multiple APNs. If a bandwidth pool is not applied to an APN, the bandwidth management function is disabled.

Examples

The following example enables the CAC bandwidth management function and applies bandwidth pool “pool A” to the Gn interface of an APN:

```
bandwidth-pool input poolA
```

Related Commands

Command	Description
bandwidth	Defines the total bandwidth, in kilobits per second, for a bandwidth pool. Valid values are 1 to 4292967295.
gprs qos bandwidth-pool	Creates or modifies a bandwidth pool.
traffic-class	Allocates bandwidth pool bandwidth to a specific traffic class.

block-foreign-ms

To restrict GPRS access based on the mobile user's home public land mobile network (PLMN) (where the MCC and MNC are used to determine the point of origin), use the **block-foreign-ms** command in access-point configuration mode. To disable blocking of foreign subscribers, use the **no** form of this command.

block-foreign-ms

no block-foreign-ms

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Access-point configuration

Command History

Release	Modification
12.2(8)YD	This command was introduced.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The **block-foreign-ms** command enables the gateway GRPS support node (GGSN) to block foreign mobile stations (MSs) from accessing the GGSN via a particular access point.

When you use this command, the GGSN determines if an MS is inside or outside of the PLMN, based on the MCC and MNC. The MCC and MNC are specified using the **gprs mcc mnc** command.

Note The MCC and MNC values used to determine whether a request is from a roaming MS must be configured using the **gprs mcc mnc** global configuration command before the GGSN can be enabled to block foreign mobile stations.

Additionally, before a GGSN is enabled to block foreign MSs, a valid PLMN should be configured using the **gprs plmn ip address** command. The block foreign MS feature will not take affect until a valid PLMN is configured and the GGSN will allow Create PDP Context requests from foreign MSs until then.

Examples

The following example blocks access to foreign MSs at access point 49:

```
gprs access-point-list abc
 access-point 49
   access-point-name www.pdn.com
   block-foreign-ms
```

Related Commands

Command	Description
gprs mcc mnc	Configures the MCC and MNC that the GGSN uses to determine whether a Create PDP Context request is from a foreign MS.

cac-policy

To enable the maximum quality of service (QoS) policy function of the Call Admission Control (CAC) feature and apply a policy to an access point name (APN), use the **cac-policy** command in access-point configuration mode. To return to the default value, use the **no** form of this command.

cac-policy *policy-name*

cac-policy *policy-name*

Syntax Description

policy-name	Name of the policy (between 1 and 40 characters).

Defaults

There is no policy attached to an APN.

Command Modes

Access-point configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **cac-policy** command to enable maximum QoS policy function of the CAC feature and apply a policy to an APN.

Note The CAC feature requires that UMTS QoS has been configured. For information on configuring UMTS QoS, see the *GGSN Release 5.1 Configuration Guide*.

Examples

The following example attaches maximum QoS policy A to an access point:

```
cac-policy A
```

Related Commands

Command	Description
gbr traffic-class	Specifies the maximum guaranteed bit rate (GBR) that can be allowed in uplink and downlink directions for real-time classes (conversational and streaming) at an APN.
gprs qos cac-policy	Creates or modifies a CAC maximum QoS policy.

Command	Description
maximum delay-class	Defines the maximum delay class for R97/R98 (GPRS) QoS that can be accepted.
maximum peak-throughput	Defines the maximum peak throughput for R97/R98 (GPRS) QoS that can be accepted.
maximum pdp-context	Specifies the maximum PDP contexts that can be created for a particular APN.
maximum traffic-class	Defines the highest traffic class that can be accepted.
mbr traffic-class	Specifies the highest maximum bit rate (MBR) that can be allowed for each traffic class for both directions (downlink and uplink).

category

To identify the subscriber billing method category to which a charging profile applies, enter the **category** command in charging profile configuration mode. To return to the default value, issue the **no** form of this command.

category {hot | flat | prepaid | normal}

no category {hot | flat | prepaid | normal}

Syntax Description

hot	Specifies that the profile apply to subscribers who use a hot billing scheme.
flat	Specifies that the profile apply to subscribers who use a flat-rate billing scheme.
prepaid	Specifies that the profile apply to subscribers who use a prepaid billing scheme.
normal	Specifies that the profile apply to subscribers who use a normal billing scheme.

Defaults

Flat

Command Modes

Charging profile configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **category** charging profile configuration command to identify to which subscriber billing method category a charging profile applies.

Examples

The following example indicates hot is the subscriber billing method category to which the profile applies:

```
category hot
```

Related Commands.

Command	Description
cdr suppression	Specifies that CDRs be suppressed as a charging characteristic in a charging profile.
charging profile	Associates a default charging profile to an access point.
content dcca profile	Defines a DCCA client profile in a GGSN charging profile.
content postpaid time	Specifies as a trigger condition for postpaid users in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
content postpaid validity	Specifies as a trigger condition in a charging profile, the amount of time quota granted to a postpaid user is valid.
content postpaid volume	Specifies as a trigger condition for postpaid users in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
content rulebase	Associates a default rule-base ID with a charging profile.
description	Specifies the name or a brief description of a charging profile.
gprs charging characteristics reject	Specifies that Create PDP Context requests for which no charging profile can be selected be rejected by the GGSN.
gprs charging container time-trigger	Specifies a global time limit, that when exceeded by a PDP context causes the GGSN to close and update the G-CDR for that particular PDP context.
gprs charging profile	Creates a new charging profile (or modifies an existing one), and enters charging profile configuration mode.
limit duration	Specifies, as a trigger condition in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
limit sgsn-change	Specifies, as a trigger condition in a charging profile, the maximum number of SGSN changes that can occur before closing and updating the G-CDR for a particular PDP context.
limit volume	Specifies, as a trigger condition in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
tariff-time	Specifies that a charging profile use the tariff changes configured using the **gprs charging tariff-time** global configuration command.

ccfh

To configure a default Credit Control Failure Handling (CCFH) action to apply to credit control (CC) sessions (PDP context) when a failure occurs and the credit control answer (CCA) received from the Diameter credit control application (DCCA) server does not contain a value for the CCFH attribute-value pair (AVP), use the **ccfh** command in DCCA client profile configuration mode. To return to the default value, use the **no** form of this command

ccfh [continue | terminate | retry_terminate]

no ccfh [continue | terminate | retry_terminate]

Syntax Description

continue	Allows the PDP context and user traffic for the relevant category (or categories) to continue, regardless of the interruption. Quota management of other categories is not affected.
terminate	Terminates the PDP context and the CC session, affecting all categories.
retry_terminate	Allows the PDP context and user traffic for the relevant category or categories to continue. Hard-coded quota (1 GB) is passed to the CSG when the first DCCA server is unavailable. The DCCA client retries to send the credit control request (CRR) to an alternate server and if a failure-to-send condition occurs with the alternate server, the PDP context is terminated.

Defaults

Terminate.

Command Modes

DCCA client profile configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **ccfa** command to configure the CCFH AVP locally. The CCFH determines the behavior of the DCCA client in fault situations. The CCFH AVP can also be received from the Diameter home authentication, authorization, and accounting (AAA) server and DCCA server. A CCFH value received from the DCCA server in a CCA overrides the value configured locally.

The CCFH AVP is determines the action the DCCA client takes on a session, when the following fault conditions occur:

- Transmission time (Tx timeout) expires.
- CCA message containing protocol error (Result-Code 3xxx) is received.

- CCA fails (for example, a CCA with a permanent failure notification [Result-Code 5xxx]) is received).
- Failure-to-send condition exists (the DCCA client is not able to communicate with the desired destination).
- An invalid answer is received

Examples

The following configuration example configures the DCCA client to allow a CC session and user traffic for the relevant category (or categories) to continue:

```
gprs dcca profile dcca-profile1
  authorization dcca-method
  tx-timeout 12
  ccfh continue
```

Related Commands

Command	Description
authorization	Defines a method of authorization (AAA method list), in the DCCA client profile, that specifies the Diameter server groups.
content dcca profile	Defines the DCCA client profile in a GGSN charging profile.
destination-realm	Configures the destination realm to be sent in CCR initial requests to a DCCA server.
gprs dcca profile	Defines a DCCA client profile on the GGSN and enters DCCA client profile configuration mode.
session-failover	Configures Credit Control Session Failover (CCSF) AVP support when a credit control answer (CCA) message from the DCCA server does not contain a value for the CCSF AVP.
trigger	Specifies that SGSN and QoS changes will trigger a DCCA client to request quota-reauthorization
tx-timeout	Configures a TX timeout value used by the DCCA client to monitor the communication of Credit Control Requests (CCRs) with a Diameter server.

cdr suppression

To specify that call detail records (CDRs) be suppressed as a charging characteristic in a charging profile, use the **cdr suppression** command in charging profile configuration mode. To return to the default value, use the **no** form of the command.

cdr suppression

no cdr suppression

Syntax Description

This command has no arguments or keywords.

Defaults

CDRs are not suppressed.

Command Modes

Charging profile configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **cdr suppression** charging profile configuration command to specify that CDRs be suppressed as a charging characteristic in a charging profile.

Examples

The following example specifies that CDRs be suppressed:

```
cdr suppression
```

Related Commands.

Command	Description
category	Identifies the subscriber category to which a charging profile applies.s
charging profile	Associates a default charging profile to an access point.
content dcca profile	Defines a DCCA client profile in a GGSN charging profile.
content postpaid time	Specifies as a trigger condition for postpaid users in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
content postpaid validity	Specifies as a trigger condition in a charging profile, the amount of time quota granted to a postpaid user is valid.

Command	Description
content postpaid volume	Specifies as a trigger condition for postpaid users in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
content rulebase	Associates a default rule-base ID with a charging profile.
description	Specifies the name or a brief description of a charging profile.
gprs charging characteristics reject	Specifies that Create PDP Context requests for which no charging profile can be selected be rejected by the GGSN.
gprs charging container time-trigger	Specifies a global time limit, that when exceeded by a PDP context causes the GGSN to close and update the G-CDR for that particular PDP context.
gprs charging profile	Creates a new charging profile (or modifies an existing one), and enters charging profile configuration mode.
limit duration	Specifies, as a trigger condition in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
limit sgsn-change	Specifies, as a trigger condition in a charging profile, the maximum number of SGSN changes that can occur before closing and updating the G-CDR for a particular PDP context.
limit volume	Specifies, as a trigger condition in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
tariff-time	Specifies that a charging profile use the tariff changes configured using the **gprs charging tariff-time** global configuration command.

cdr suppression prepaid

To specify that call detail records (CDRs) be suppressed for prepaid users, use the **cdr suppression** command in charging profile configuration mode. To return to the default value, use the **no** form of the command.

cdr suppression prepaid

no cdr suppression prepaid

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled (CDRs are generated for users).

Command Modes

Charging profile configuration

CommandHistory

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **cdr suppression prepaid** charging profile configuration command to specify that CDRs be suppressed users with an active connection to a DCCA server.

Charging for prepaid users is handled by the DCCA client, therefore G-CDRs do not need to be generated for prepaid users.

Note When CDR suppression for prepaid users is enabled, if a Diameter server error occurs while a session is active, the user is reverted to postpaid status, but CDRs for the PDP context are not generated.

Examples

The following example specifies that CDRs be suppressed for online users:

```
cdr suppression prepaid
```

Related Commands.

Command	Description
category	Identifies the subscriber category to which a charging profile applies.s
charging profile	Associates a default charging profile to an access point.
content dcca profile	Defines a DCCA client profile in a GGSN charging profile.

Command	Description
content postpaid time	Specifies as a trigger condition for postpaid users in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
content postpaid validity	Specifies as a trigger condition in a charging profile, the amount of time quota granted to a postpaid user is valid.
content postpaid volume	Specifies as a trigger condition for postpaid users in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
content rulebase	Associates a default rule-base ID with a charging profile.
description	Specifies the name or a brief description of a charging profile.
gprs charging characteristics reject	Specifies that Create PDP Context requests for which no charging profile can be selected be rejected by the GGSN.
gprs charging container time-trigger	Specifies a global time limit, that when exceeded by a PDP context causes the GGSN to close and update the G-CDR for that particular PDP context.
gprs charging profile	Creates a new charging profile (or modifies an existing one), and enters charging profile configuration mode.
limit duration	Specifies, as a trigger condition in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
limit sgsn-change	Specifies, as a trigger condition in a charging profile, the maximum number of SGSN changes that can occur before closing and updating the G-CDR for a particular PDP context.
limit volume	Specifies, as a trigger condition in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
tariff-time	Specifies that a charging profile use the tariff changes configured using the **gprs charging tariff-time** global configuration command.

charging profile

To specify a default charging profile for a user type for an access point, use the **charging profile** command in access-point configuration mode. To remove the profile, use the **no** form of this command.

charging profile {home | roaming | visiting | any} [trusted] *profile-number* **[override]**

no charging profile {home | roaming | visiting | any} *profile-number* **[trusted]** *profile-number* **[override]**

Syntax Description

home	Specifies that the charging profile applies to home users.
roaming	Specifies that the charging profile applies to roaming users (users whose serving GPRS support node [SGSN] public land mobile network [PLMN] ID differs from the gateway GPRS support node's [GGSN's]).
visiting	Specifies that the charging profile applies to visiting users (users whose International Mobile Subcriber Indentity [IMSI] contains a foreign PLMN ID).
any	Specifies that the charging profile will apply to all types of users.
trusted	(Optional) Specifies that the charging profile applies if the user is a visiting or roaming user (depending on whether **roaming** or **visiting** has been specified) whose PLMN ID is a trusted one (as configured using the **gprs mcc mnc** command).
profile-number	Number of the charging profile that is being associated with the access point. Valid values are 0 to 15. If 0 is specified, charging behavior is defined by global charging characteristics (those not defined in a charging profile).
override	(Optional) Specifies that the charging characteristic value received from the SGSN in the Create PDP Context request be ignored and the APN default used instead.

Defaults

No profile is associated with an APN.

Command Modes

Access-point configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **charging profile** access-point configuration command to apply a default charging profile to an access point name (APN) for a specific type of use.

For complete information on configuring and using charging profiles, and the order in which charging profiles are selected for a PDP context, see the "Configuring Charging Profiles" section of the "Configuring Charging on the GGSN" chapter of the *Cisco GGSN Configuration Guide*.

Examples

The following example specifies charging profile number 10 to be the APN default for home users:

```
charging profile 10 home
```

Related Commands.

Command	Description
category	Identifies the subscriber category to which a charging profile applies.s
cdr suppression	Specifies that CDRs be suppressed as a charging characteristic in a charging profile.
description	Specifies the name or a brief description of a charging profile.
gprs charging characteristics reject	Specifies that Create PDP Context requests for which no charging profile can be selected be rejected by the GGSN.
gprs charging container time-trigger	Specifies a global time limit, that when exceeded by a PDP context causes the GGSN to close and update the G-CDR for that particular PDP context.
gprs charging profile	Creates a new charging profile (or modifies an existing one), and enters charging profile configuration mode.
limit duration	Specifies, as a trigger condition in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
limit sgsn-change	Specifies, as a trigger condition in a charging profile, the maximum number of SGSN changes that can occur before closing and updating the G-CDR for a particular PDP context.
limit volume	Specifies, as a trigger condition in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
tariff-time	Specifies that a charging profile use the tariff changes configured using the **gprs charging tariff-time** global configuration command.

clear aaa counters server sg

To clear the counters for all RADIUS servers that are part of a specific server group, use the **clear aaa counters servers sg** command in privileged EXEC mode.

clear aaa counters servers sg *sg-name*

Syntax Description

sg-name	Name of the server group for which you want to clear counters for all the RADIUS servers in the group.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)XG	This command was introduced.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **clear aaa counters server sg** command to clear counters for all the RADIUS servers in a specific server-group, and to reset the counters to 0.

Use the **show aaa servers sg** command to display the counters that are reset by this command.

Examples

The following example clears the counters for all the RADIUS servers in server group “group1”:

```
clear aaa counters servers sg group1
```

Related Commands

Command	Description
show aaa servers sg	Displays counters and statistics for all RADIUS servers that are a part of a server group.

clear data-store statistics

To clear Persistent Storage Device (PSD)-related statistics, use the **clear data-store statistics** command in privilege EXEC mode.

clear data-store statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)YU	This command was introduced.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

Use the **clear data-store statistics** command to clear PSD-related statistics. These statistics are displayed using the **show data-store statistics** command.

Examples

The following example clears PSD-related statistics on the GGSN:

```
clear data-store statistics
```

Related Commands

Command	Description
auto-retrieve	Configures the GGSN to automatically initiate a retrieval of G-CDRs from PSDs defined in a PSD server group.
data-store	Configures a PSD server group on the GGSN to use for GGSN-to-PSD communication.
show data-store	Displays the status of the PSD client and PSD server-related information.
show data-store statistics	Displays statistics related to the PSD client.

clear ggsn quota-server statistics

To clear statistics (message and error counts) related to quota server processing, use the **clear ggsn quota-server statistics** command in privilege EXEC mode.

clear ggsn quota-server statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privilege EXEC

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **clear ggsn quota-server statistics** command to clear statistics related to quota server process operations (displayed using the **show ggsn quota server statistics** command).

Examples

The following configuration example clears all statistics related to quota server operations:

```
clear ggsn quota-server statistics
```

Related Commands .

Command	Description
show ggsn quota-server	Displays quota server parameters or statistics about the message and error counts.

clear gprs access-point statistics

To clear statistics counters for a specific access point or for all access points on the gateway GPRS support node (GGSN), use the **clear gprs access-point statistics** command in privileged EXEC mode.

clear gprs access-point statistics {*access-point-index* | **all**}

Syntax Description

access-point-index	Index number of an access point. Information about that access point is cleared.
all	Information about all access points on the GGSN is cleared.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

This command clears the statistics that are displayed by the **show gprs access-point statistics** command and **show policy-map apn** command.

Examples

The following example clears the statistics at access point 2:

```
clear gprs access-point statistics 2
```

The following example clears the statistics for all access points:

```
clear gprs access-point statistics all
```

Related Commands

Command	Description
show gprs access-point statistics	Displays data volume and PDP context activation and deactivation statistics for access points on the GGSN.

clear gprs charging cdr

To clear GPRS call detail records (CDRs), use the **clear gprs charging cdr** command in privileged EXEC configuration mode.

clear gprs charging cdr {**access-point** *access-point-index* | **all** | **partial-record** | **tid** *tunnel-id*}

Syntax Description

access-point *access-point-index*	Closes CDRs for a specified access-point index.
all	Closes all CDRs on the GGSN.
partial-record	Closes all CDRs, and opens partial CDRs for any existing PDP contexts.
tid *tunnel-id*	Closes CDRs by tunnel ID.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX and the **partial-record** keyword was added.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **clear gprs charging cdr** command to clear the CDRs for one or more PDP contexts.

To clear CDRs by tunnel ID (TID), use the **clear gprs charging cdr** command with the **tid** keyword and specify the corresponding TID for which you want to clear the CDRs. To determine the tunnel ID (TID) of an active PDP context, you can use the **show gprs gtp pdp-context all** command to obtain a list of the currently active PDP contexts (mobile sessions).

To clear CDRs by access point, use the **clear gprs charging cdr** command with the **access-point** keyword and specify the corresponding access-point index for which you want to clear CDRs. To obtain a list of access points, you can use the **show gprs access-point** command.

When you clear CDRs for a tunnel identifier (TID), an access point, or for all access points, charging data records for the specified TID or access point(s) are sent immediately to the charging gateway. When you run these versions of this command, the following things occur:

- The GGSN no longer sends charging data that has been accumulated for the PDP context to the charging gateway.
- The GGSN closes the current CDRs for the specified PDP contexts.
- The GGSN no longer generates CDRs for existing PDP contexts.

To close all CDRs and open partial CDRs for existing PDP contexts on the GGSN, use the **clear gprs charging cdr partial-record** command.

The **clear gprs charging cdr** command is normally used before disabling the charging function.

Examples

The following example shows how to clear CDRs by tunnel ID:

```
Router# show gprs gtp pdp-context all
TID              MS Addr         Source  SGSN Addr       APN
1234567890123456 10.11.1.1       Radius  10.4.4.11       www.pdn1.com
2345678901234567 Pending         DHCP    10.4.4.11       www.pdn2.com
3456789012345678 10.21.1.1       IPCP    10.1.4.11       www.pdn3.com
4567890123456789 10.31.1.1       IPCP    10.1.4.11       www.pdn4.com
5678901234567890 10.41.1.1       Static  10.4.4.11       www.pdn5.com

Router# clear gprs gtp charging cdr tid 1234567890123456
```

The following example shows how to clear CDRs for access point 1:

```
Router# clear gprs charging cdr access-point 1
```

Related Commands

Command	Description
show gprs charging statistics	Displays current statistics about the transfer of charging packets between the GGSN and charging gateways.
show gprs access-point	Displays information about an access point.

clear gprs charging cdr all no-transfer

To clear all stored call detail records (CDRs) when a gateway GPRS support node (GGSN) is in charging and global maintenance mode, including those in the pending queue, use the **clear gprs charging cdr all no-transfer** command in privileged EXEC configuration mode.

clear gprs charging cdr all no-transfer

SyntaxDescription This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines Use the **clear gprs cdr all no-transfer** command to clear stored and pending CDRs when the GGSN is in charging and global maintenance modes.

When you clear stored CDRs, the GGSN does not send the charging data accumulated for packet data protocol (PDP) contexts to the charging gateway when the global and charging service-mode states are returned to operational. Additionally, once the service-mode states are returned to operational, the GGSN no longer generates CDRs for the existing PDP contexts. Therefore, to return to normal CDR generation, clear existing PDP contexts using the **clear gprs gtp pdp-context** global configuration command.

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

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

Examples

The following example shows how to clear CDRs:

```
Router# clear gprs cdr all no-transfer
```

Related Commands

Command	Description
gprs charging service-mode	Specifies the service-mode state of a GGSN's charging function.
gprs service-mode	Configures the service-mode state of a GGSN.
show gprs service-mode	Displays the current global service mode state of the GGSN and the last time it was changed.

clear gprs gtp pdp-context

To clear one or more packet data protocol (PDP) contexts (mobile sessions), use the **clear gprs gtp pdp-context** command in privileged EXEC configuration mode.

clear gprs gtp pdp-context {**tid** *tunnel-id* | **imsi** *imsi_value* | **path** *ip-address* [*remote_port_num*] | **access-point** *access-point-index* **[no-wait-sgsn** | **local-delete** | **pdp-type** {**ipv6** | **ipv4}** | **all**]}

Syntax Description

tid *tunnel-id*	Tunnel ID (TID) for which PDP contexts are to be cleared.
imsi *imsi_value*	International mobile subscriber identity (IMSI) value for which PDP contexts are to be cleared.
path *ip-address* [*remote_port_num*]	Remote serving GPRS support node (SGSN) IP address for which all PDP contexts associated with the SGSN are to be cleared. Optionally, the remote SGSN IP address and remote port number for which all PDP contexts are to be cleared.
access-point *access-point-index*	Access point index for which PDP contexts are to be cleared.
no-wait-sgsn	(Optional) Configures the GGSN to not wait for an SGSN response to a delete PDP context requests before clearing the PDP context. This keyword option is only available when the APN is in maintenance mode.
local-delete	(Optional) Configures the GGSN not send delete PDP context requests to the SGSN and to delete the PDP contexts locally. This keyword option is only available when the APN is in maintenance mode.
pdp-type {**ipv6** | **ipv4}**	Clears PDP contexts by IP version. • **ipv6**—Clears IPv6 PDPs • **ipv4**—Clears IPv4 PDPs.
all	Clear all active PDP contexts.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.

Release	Modification
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.
12.4(9)XG	This command was integrated into Cisco IOS Release 12.4(9)XG and the following keyword options were added: • **pdp-type** [**ipv6** | **ipv4**] • **no-wait-sgsn** • **local-delete**
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.

Usage Guidelines

Use the **clear gprs gtp pdp-context** command to clear one or more PDP contexts (mobile sessions). Use this command when operator intervention is required for administrative reasons—for example, when there are problematic user sessions or when the system must be taken down for maintenance.

After the **clear gprs gtp pdp-context** command is issued, those users who are accessing the public data network (PDN) through the specified TID, IMSI, path, or access point are disconnected.

Caution In a GTP session redundancy (GTP-SR) environment, *do not* use the **clear gprs gtp pdp-context** command on the Standby gateway GPRS support node (GGSN). If you issue this command on the Standby GGSN, you are prompted to confirm before the command is processed. Issue the **show grps redundancy** command to confirm which GGSN is the Standby GGSN in a GTP-SR configuration before you use this command.

TID

To determine the tunnel ID of an active PDP context, you can use the **show gprs gtp pdp-context** command to obtain a list of the currently active PDP contexts (mobile sessions). Then, to clear a PDP context by tunnel ID, use the **clear gprs gtp pdp-context** command with the **tid** keyword and the corresponding tunnel ID that you want to clear.

IMSI

If you know the IMSI of the PDP context, you can use the **clear gprs gtp pdp-context** with the **imsi** keyword and the corresponding IMSI of the connected user to clear the PDP context. If you want to determine the IMSI of a PDP context, you can use the **show gprs gtp pdp-context all** command, which displays a list of the currently active PDP contexts. Then, after finding the TID value that corresponds to the session that you want to clear, you can use the **show gprs gtp pdp-context tid** command to display the IMSI.

Access Point

To clear PDP contexts by access point, use the **clear gprs gtp pdp-context** command with the **access-point** keyword and the corresponding access point index. To display a list of access points that are configured on the GGSN, use the **show gprs access-point** command.

Access Point, Fast PDP Delete

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

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

When using the Fast PDP Delete feature, note the following:

- The **no-wait-sgsn** and **local-delete** keyword options are available only when the APN is in maintenance mode.
- The **no-wait-sgsn** and **local-delete** keyword options are not available in a Standby GGSN.
- When the **no-wait-sgsn** and **local-delete** keyword options are specified, and the command entered, the GGSN prompts you with the following caution:

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

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

Examples

The following example shows how to clear PDP contexts by tunnel ID:

```
GGSN# show gprs gtp pdp-context all
TID              MS Addr         Source  SGSN Addr       APN
1234567890123456 10.11.1.1       Radius  10.4.4.11       www.pdn1.com
2345678901234567 Pending         DHCP    10.4.4.11       www.pdn2.com
3456789012345678 10.21.1.1       IPCP    10.1.4.11       www.pdn3.com
4567890123456789 10.31.1.1       IPCP    10.1.4.11       www.pdn4.com
5678901234567890 10.41.1.1       Static  10.4.4.11       www.pdn5.com

GGSN# clear gprs gtp pdp-context tid 1234567890123456
```

The following example shows how to clear PDP contexts at access point 1:

```
GGSN# clear gprs gtp pdp-context access-point 1
```

clear gprs gtp statistics

To clear the current gateway GPRS support node (GGSN) GPRS tunneling protocol (GTP) statistics, use the **clear gprs gtp statistics** command in privileged EXEC configuration mode.

clear gprs gtp statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **clear gprs gtp statistics** command to clear the current GPRS GTP statistics. This command clears the counters that are displayed by the **show gprs gtp statistics** command.

Note The **clear gprs gtp statistics** command does not clear the counters that are displayed by the **show gprs gtp status** command.

Examples

The following example clears the GPRS GTP statistics:

```
GGSN# clear gprs gtp statistics
```

clear gprs iscsi statistics

To clear the current GPRS-related iSCSI statistics, use the **clear gprs iscsi statistics** command in privileged EXEC configuration mode.

clear gprs iscsi statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

The **clear gprs iscsi statistics** command clears the statistics displayed using the **show gprs iscsi statistics** privileged EXEC command.

Examples

The following example clears GGSN iSCSI-related statistics:

```
clear gprs iscsi statistics
```

Related Commands

Command	Description
show gprs iscsi statistics	Displays GPRS iSCSI-related statistics.

clear gprs redundancy statistics

To clear statistics related to GPRS tunneling protocol (GTP) session redundancy (GTP-SR), use the **clear gprs redundancy statistics** command in privileged EXEC configuration mode.

clear gprs redundancy statistics

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(11)YJ	This command was introduced.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **clear gprs redundancy statistics** command to clear the GTP-SR statistics that are displayed using the **show gprs redundancy** command.

Examples

The following example clears all redundancy-related statistics:

```
clear gprs redundancy statistics
```

Related Commands

Command	Description
gprs redundancy	Enables GTP-SR on a GGSN.
gprs redundancy charging sync-window cdr rec-seqnum	Configures the window size used to determine when the CDR record sequence number needs to be synchronized to the Standby GGSN.
gprs redundancy charging sync-window gtpp seqnum	Configures the window size used to determine when the GTP' sequence number needs to be synchronized to the Standby GGSN.
show gprs redundancy	Displays statistics related to GTP-SR.

clear gprs service-aware statistics

To clear statistics (message and error counts) related to the service-aware features of the gateway GPRS support node (GGSN), use the **clear ggsn quota-server statistics** command in privilege EXEC configuration mode.

clear gprs service-aware statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privilege EXEC

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **clear gprs service-aware statistics** command to clear statistics related to the service-aware features of the GGSN (displayed using the **show gprs service-aware statistics** command).

Examples

The following configuration example clears all statistics related to the service-aware features of the GGSN:

```
clear gprs service-aware statistics
```

Related Commands .

Command	Description
show gprs service-aware statistics	Displays statistics related to the service-aware features of the GGSN, such as packets sent to, and received from, the Diameter server or CSG.

clear gprs slb statistics

To clear Cisco IOS Server Load Balancing (SLB) statistics, use the **clear gprs slb statistics** command in privileged EXEC configuration mode.

clear gprs slb statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(8)XU1	This command was integrated into Cisco IOS Release 12.3(8)XU1.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **clear gprs slb statistics** command to clear Cisco IOS SLB statistics. This command clears the counters that are displayed by the **show gprs slb statistics** command.

Examples

The following example clears the Cisco IOS SLB statistics:

```
GGSN# clear gprs slb statistics
```

Related Commands

Command	Description
gprs slb mode	Defines the Cisco IOS SLB operation mode.
gprs slb notify	Enables the GGSN to provide feedback to the Cisco IOS SLB about a certain condition, for example, a Create PDP Create request rejection because of a Call Admission Control failure.
gprs slb vserver	Configures the Cisco IOS SLB virtual servers to be notified about a condition if the **gprs slb notify** command is configured and the Cisco IOS SLB is in directed server NAT mode.
show gprs slb detail	Displays Cisco IOS SLB related information, such as the operation mode, virtual servers addresses, and statistics.
show gprs slb mode	Displays the Cisco IOS SLB mode of operation defined on the GGSN.

Command	Description
show gprs slb statistics	Displays Cisco IOS SLB statistics.
show gprs slb vservers	Displays the list of defined Cisco IOS SLB virtual servers.

clear gprs statistics all

To clear all gateway GPRS support node (GGSN) counters and statistics (both global and per-access point name [APN]), use the **clear gprs statistics** command in privileged EXEC mode.

clear gprs statistics all

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)XG	This command was introduced.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **clear gprs statistics all** command to clear, and to reset to 0, the global and per-APN GPRS and Universal Mobile Telecommunication Systems (UMTS) statistics displayed by the following **show** commands:

- **show gprs service-aware statistics**
- **show ggsn quota-server statistics**
- **show ggsn csg statistics**
- **show gprs gtp path statistics remote-address**
- **show gprs access-point statistics**
- **show gprs gtp statistics**

After issuing the **clear gprs statistics all** command, you will be prompted for confirmation before the counters and statistics are cleared.

Examples

The following example clears all GPRS/UMTS global and access point counters and statistics:

```
clear gprs statistics all
```

Related Commands.

Command	Description
show gprs access-point statistics	Displays data volume and PDP activation and deactivation statistics for access points on the GGSN.
show gprs access-point status	Displays the current status of an APN, including the number of active PDPs, number of IPv4 addresses allocated, and the number of IPv6 addresses allocated.
show gprs gtp statistics	Displays the current GTP statistics for the GGSN, such as IE, GTP signaling, and GTP PDU statistics.
show gprs gtp status	Displays information about the current status of the GTP on the GGSN, such as activated PDP contexts, throughput, and QoS statistics.

clear ip iscsi statistics

To clear current iSCSI statistics, use the **clear ip iscsi statistics** command in privileged EXEC configuration mode.

clear ip iscsi statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

The **clear ip iscsi statistics** command clears the statistics displayed using the **show ip iscsi stats** privileged EXEC command.

Examples

The following example clears iSCSI-related statistics:

```
clear ip iscsi statistics
```

Related Commands

Command	Description
show ip iscsi stats	Displays iSCSI-related statistics.

clear record-storage-module stats

To clear current record storage module (RSM) statistics, use the **clear record-storage-module stats** command in privileged EXEC configuration mode.

clear record-storage-module stats

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

The **clear record-storage-module stats** command clears the statistics displayed using the **show record-storage-module stats** privileged EXEC command.

Examples

The following example clears RSM-related statistics:

```
clear record-storage-module stats
```

Related Commands

Command	Description
show record-storage-module stats	Displays RSM-related statistics.

content dcca profile

To specify a Diameter credit control application (DCCA) client to use to communicate with a DCCA server in a gateway GPRS support node (GGSN) charging profile, use the **dcca profile** command in charging profile configuration mode. To remove the profile configuration, use the **no** form of this command.

content dcca profile *dcca-profile-name*

no content dcca profile

Syntax Description

dcca-profile-name	Name of the DCCA client profile configured on the GGSN that defines the DCCA client to use to communicate with the DCCA server.

Defaults

No default behavior or values.

Command Modes

Charging profile configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The presence of the **content dcca profile** statement in a charging profile indicates online billing is required. Therefore, regardless of whether a subscriber is prepaid or postpaid, the GGSN will contact the DCCA server if the content dcca profile command has been configured.

If the user is to be treated as a postpaid user, the server returns ***X*** and the user is treated as a postpaid user. If a charging profile does not contain a **content dcca profile** configuration, users using the charging profile will be treated as postpaid (offline billing).

Examples

The following configuration example defines a DCCA client profile named dcca-profile1 in Charging Profile 1:

```
gprs charging profile 1
  content dcca profile dcca-profile1
```

Related Commands.

Command	Description
category	Identifies the subscriber category to which a charging profile applies.
charging profile	Associates a default charging profile to an access point.

Command	Description
content postpaid time	Specifies as a trigger condition for postpaid users in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
content postpaid validity	Specifies as a trigger condition in a charging profile, the amount of time quota is valid for postpaid users.
content postpaid volume	Specifies as a trigger condition for postpaid users in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
content rulebase	Associates a default rule-base ID with a charging profile.
description	Specifies the name or a brief description of a charging profile.
gprs charging characteristics reject	Specifies that Create PDP Context requests for which no charging profile can be selected be rejected by the GGSN.
gprs charging container time-trigger	Specifies a global time limit, that when exceeded by a PDP context causes the GGSN to close and update the G-CDR for that particular PDP context.
gprs charging profile	Creates a new charging profile (or modifies an existing one), and enters charging profile configuration mode.
limit duration	Specifies, as a trigger condition in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
limit sgsn-change	Specifies, as a trigger condition in a charging profile, the maximum number of SGSN changes that can occur before closing and updating the G-CDR for a particular PDP context.
limit volume	Specifies, as a trigger condition in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
tariff-time	Specifies that a charging profile use the tariff changes configured using the **gprs charging tariff-time** global configuration command.

content postpaid time

To specify as a trigger condition for postpaid users in a charging profile, the time duration limit that when exceeded causes the gateway GPRS support node (GGSN) to collect upstream and downstream traffic byte counts and close and update the call detail record (CDR) for a particular packet data protocol (PDP) context, use the **content postpaid time** command in charging profile configuration mode. To return to the default value, use the **no** form of this command.

content postpaid time *number*

no content postpaid time

Syntax Description

number	A value, in seconds, between 300 and 4294967295 that specifies the time duration limit.

Defaults

1048576 seconds.

Command Modes

Charging profile configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **content postpaid time** charging profile configuration command to specify the time limit, for postpaid users, that when exceeded, causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a PDP context.

Examples

The following configuration example specifies a postpaid time duration limit 400 minutes in Charging Profile 1:

```
gprs charging profile 1
  content dcca profile dcca-profile1
  content postpaid time 400
```

Related Commands.

Command	Description
category	Identifies the subscriber category to which a charging profile applies.s
charging profile	Associates a default charging profile to an access point.
content dcca profile	Defines a DCCA client profile in a GGSN charging profile.

Command	Description
content postpaid validity	Specifies as a trigger condition in a charging profile, the amount of time quota granted to a postpaid user is valid.
content postpaid volume	Specifies as a trigger condition for postpaid users in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
content rulebase	Associates a default rule-base ID with a charging profile.
description	Specifies the name or a brief description of a charging profile.
gprs charging characteristics reject	Specifies that Create PDP Context requests for which no charging profile can be selected be rejected by the GGSN.
gprs charging container time-trigger	Specifies a global time limit, that when exceeded by a PDP context causes the GGSN to close and update the G-CDR for that particular PDP context.
gprs charging profile	Creates a new charging profile (or modifies an existing one), and enters charging profile configuration mode.
limit duration	Specifies, as a trigger condition in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
limit sgsn-change	Specifies, as a trigger condition in a charging profile, the maximum number of SGSN changes that can occur before closing and updating the G-CDR for a particular PDP context.
limit volume	Specifies, as a trigger condition in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
tariff-time	Specifies that a charging profile use the tariff changes configured using the **gprs charging tariff-time** global configuration command.

content postpaid validity

To specify as a trigger condition in a charging profile, the amount of time quota granted to a postpaid user is valid, use the **content postpaid validity** command in charging profile configuration mode. To return to the default value, use the **no** form of this command.

content postpaid validity *seconds*

no content postpaid validity

Syntax Description

seconds	A value between 900 and 4294967295 seconds that specifies the amount of time granted quota is valid.

Defaults

Disabled.

Command Modes

Charging profile configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **content postpaid validity** charging profile configuration command to configure the amount of time quota granted to postpaid users is valid.

Examples

The following example specifies a value of 21600:

```
gprs charging profile 1
  content dcca profile dcca-profile1
  content postpaid time 400
  content postpaid volume 2097152
  content postpaid validity 21600
```

Related Commands.

Command	Description
category	Identifies the subscriber category to which a charging profile applies.s
charging profile	Associates a default charging profile to an access point.
content dcca profile	Defines a DCCA client profile in a GGSN charging profile.

Command	Description
content postpaid time	Specifies as a trigger condition for postpaid users in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
content postpaid volume	Specifies as a trigger condition for postpaid users in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
content rulebase	Associates a default rule-base ID with a charging profile.
description	Specifies the name or a brief description of a charging profile.
gprs charging characteristics reject	Specifies that Create PDP Context requests for which no charging profile can be selected be rejected by the GGSN.
gprs charging container time-trigger	Specifies a global time limit, that when exceeded by a PDP context causes the GGSN to close and update the G-CDR for that particular PDP context.
gprs charging profile	Creates a new charging profile (or modifies an existing one), and enters charging profile configuration mode.
limit duration	Specifies, as a trigger condition in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
limit sgsn-change	Specifies, as a trigger condition in a charging profile, the maximum number of SGSN changes that can occur before closing and updating the G-CDR for a particular PDP context.
limit volume	Specifies, as a trigger condition in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
tariff-time	Specifies that a charging profile use the tariff changes configured using the **gprs charging tariff-time** global configuration command.

content postpaid volume

To specify as a trigger condition for postpaid users in a charging profile, the maximum number of bytes that the gateway GPRS support node (GGSN) maintains across all containers for a particular packet data protocol (PDP) context before closing and updating the call detail record (CDR), use the **content postpaid volume** command in charging profile configuration mode. To return to the default value, use the **no** form of this command.

content postpaid volume *threshold_value*

no content postpaid volume

Syntax Description

threshold_value	A value between 1 and 4294967295 that specifies the container threshold value, in bytes. The default is 1,048,576 bytes (1 MB).

Defaults

1,048,576 bytes (1 MB).

Command Modes

Charging profile configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **content postpaid volume** charging profile configuration command to configure as a trigger condition for postpaid users, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.

Examples

The following example specifies a threshold value of 2097152:

```
gprs charging profile 1
  content dcca profile dcca-profile1
  content postpaid time 400
  content postpaid volume 2097152
```

Related Commands.

Command	Description
category	Identifies the subscriber category to which a charging profile applies.s
charging profile	Associates a default charging profile to an access point.
content dcca profile	Defines a DCCA client profile in a GGSN charging profile.

Command	Description
content postpaid time	Specifies as a trigger condition for postpaid users in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
content postpaid validity	Specifies as a trigger condition in a charging profile, the amount of time quota granted to a postpaid user is valid.
content rulebase	Associates a default rule-base ID with a charging profile.
description	Specifies the name or a brief description of a charging profile.
gprs charging characteristics reject	Specifies that Create PDP Context requests for which no charging profile can be selected be rejected by the GGSN.
gprs charging containter time-trigger	Specifies a global time limit, that when exceeded by a PDP context causes the GGSN to close and update the G-CDR for that particular PDP context.
gprs charging profile	Creates a new charging profile (or modifies an existing one), and enters charging profile configuration mode.
limit duration	Specifies, as a trigger condition in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
limit sgsn-change	Specifies, as a trigger condition in a charging profile, the maximum number of SGSN changes that can occur before closing and updating the G-CDR for a particular PDP context.
limit volume	Specifies, as a trigger condition in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
tariff-time	Specifies that a charging profile use the tariff changes configured using the **gprs charging tariff-time** global configuration command.

content rulebase

To associate a default rule-base ID to apply to packet data protocol (PDP) contexts using a particular charging profile, use the **rulebase** command in charging profile configuration mode. To return to the default value, use the **no** form of the command.

content rulebase *id*

no content rulebase

Syntax Description

name	16-character string that identifies the rulebase.

Defaults

Disabled.

Command Modes

Charging profile configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **content rulebase** charging profile configuration command to define a default rulebase ID to a charging profile.

Rulebases contain the rules for defining categories of traffic; categories on which decisions such as whether to allow or disallow traffic, and how to measure the traffic, are based. The GGSN maps Diameter Rulebase IDs to Cisco Content Services Gateway (CSG) billing plans.

Note The rulebase value presented in a RADIUS Access Accept message overrides the default rulebase ID configured in a charging profile. A rulebase ID received in a credit control answer (CCA) initial message from a Diameter credit control application (DCCA) server overrides the Rulebase ID received from the RADIUS server and the default rulebase ID configured in a charging profile.

Examples

The following example specifies a default rulebase with the ID of “PREPAID” in Charging Profile 1:

```
gprs charging profile 1
  content dcca profile dcca-profile1
  content postpaid time 400
  content rulebase PREPAID
```

Related Commands.

Command	Description
category	Identifies the subscriber category to which a charging profile applies.s
charging profile	Associates a default charging profile to an access point.
content dcca profile	Defines a DCCA client profile in a GGSN charging profile.
content postpaid time	Specifies as a trigger condition for postpaid users in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
content postpaid volume	Specifies as a trigger condition for postpaid users in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
description	Specifies the name or a brief description of a charging profile.
gprs charging characteristics reject	Specifies that Create PDP Context requests for which no charging profile can be selected be rejected by the GGSN.
gprs charging container time-trigger	Specifies a global time limit, that when exceeded by a PDP context causes the GGSN to close and update the G-CDR for that particular PDP context.
gprs charging profile	Creates a new charging profile (or modifies an existing one), and enters charging profile configuration mode.
limit duration	Specifies, as a trigger condition in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
limit sgsn-change	Specifies, as a trigger condition in a charging profile, the maximum number of SGSN changes that can occur before closing and updating the G-CDR for a particular PDP context.
limit volume	Specifies, as a trigger condition in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
tariff-time	Specifies that a charging profile use the tariff changes configured using the **gprs charging tariff-time** global configuration command.

csg-group

To associate the quota server to a Cisco Content Services Gateway (CSG) server group that is to be used for quota server-to-CSG communication, use the **csg-group** command in quota server configuration mode. To remove the association to a CSG group, use the **no** form of this command

csg-group *csg-group-name*

no csg-group *csg-group-name*

Syntax Description

csg-group-name	Specifies the name of a CSG server group to be used for quota server-to-CSG communication. **Note** The name of the CSG group that you specify must correspond to a CSG server group you created using the **ggsn csg-group** global configuration command.

Defaults

No default behavior or values.

Command Modes

Quota server configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **csg-group** command to associate the quota server with the CSG server group to use for quota server-to-CSG communication.

This functionality requires that a CSG server group has been defined on the gateway GPRS support node (GGSN) using the **ggsn csg-group** global configuration command and associated CSG group configuration commands.

Caution Deconfiguring this command will disassociate the quota server and CSG group and bring the path to the CSG down if it is up.

Examples

The following configuration example specifies for the quota server to use CSG group "csg1" for quota server-to-CSG communication:

```
ggsn quota-server qs1
 interface loopback1
 echo-interval 90
 n3-requests 3
 t3-response 524
 csg group csg1
```

Related Commands .

Command	Description
echo-interval	Specifies the number of seconds that the quota server waits before sending an echo-request message to the CSG.
ggsn quota-server	Configures the quota server process that interfaces with the CSG for enhanced service aware billing.
interface	Specifies the logical interface, by name, that the quota server will use to communicate with the CSG.
n3-requests	Specifies the maximum number of times that the quota server attempts to send a signaling request to the CSG.
t3-response	Specifies the initial time that the quota server waits before resending a signaling request message when a response to a request has not been received.
show ggsn quota-server	Displays quota server parameters or statistics about the message and error counts.

data-store

To configure a Cisco Persistent Storage Device (PSD) server group to be used for gateway GPRS support node (GGSN)-to-PSD communication, and enter data-store configuration mode, use the **data-store** command in global configuration mode. To disable the PSD server group, issue the **no** form of this command.

data-store *psd-group-name*

no data-store *psd-group-name*

Syntax Description

psd-group-name	Specifies the name of a PSD server group to be used for GGSN-to-PSD server communication.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YU	This command was introduced.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

Use the **data-store** command to define a PSD server group for GGSN-to-PSD communication and enter data-store configuration mode.

When in data-store configuration mode, you can define PSDs and configure auto-retrieve options.

Note Up to two PSDs can be defined in per PSD server group. One local PSD (backup) and one remote PSD (retrieve-only).

Note One PSD server group can be configured per GGSN.

Examples

The following example configures a PSD server group identified as “groupA”:

```
data-store groupA
```

Related Commands

Command	Description
auto-retrieve	Configures the GGSN to automatically initiate a retrieval of G-CDRs from PSDs defined in a PSD server group.
clear data-store statistics	Clears PSD-related statistics.
show data-store	Displays the status of the PSD client and PSD server-related information.
show data-store statistics	Displays statistics related to the PSD client.

description

To specify the name or a brief description of a charging profile, use the **description** command in charging profile configuration mode. To delete a charging profile description, use the **no** form of the command.

description *string*

no description

Syntax Description

string	Text string (up to 99 characters) that describes the charging profile.

Defaults

There is no charging profile description.

Command Modes

Charging profile configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **description** charging profile configuration mode command to provide a description of a charging profile.

Examples

The following example describes a profile as access point name (APN)-level default for home users:

```
description APN-level_default_for_home_users
```

Related Commands.

Command	Description
category	Identifies the subscriber category to which a charging profile applies.s
cdr suppression	Specifies that CDRs be suppressed as a charging characteristic in a charging profile.
charging profile	Associates a default charging profile to an access point.
content dcca profile	Defines a DCCA client profile in a GGSN charging profile.
content postpaid time	Specifies as a trigger condition for postpaid users in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.

Command	Description
content postpaid validity	Specifies as a trigger condition in a charging profile, the amount of time quota granted to a postpaid user is valid.
content postpaid volume	Specifies as a trigger condition for postpaid users in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
content rulebase	Associates a default rule-base ID with a charging profile.
gprs charging characteristics reject	Specifies that Create PDP Context requests for which no charging profile can be selected be rejected by the GGSN.
gprs charging container time-trigger	Specifies a global time limit, that when exceeded by a PDP context causes the GGSN to close and update the G-CDR for that particular PDP context.
gprs charging profile	Creates a new charging profile (or modifies an existing one), and enters charging profile configuration mode.
limit duration	Specifies, as a trigger condition in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
limit sgsn-change	Specifies, as a trigger condition in a charging profile, the maximum number of SGSN changes that can occur before closing and updating the G-CDR for a particular PDP context.
limit volume	Specifies, as a trigger condition in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
tariff-time	Specifies that a charging profile use the tariff changes configured using the **gprs charging tariff-time** global configuration command.

destination host

To configure the Fully Qualified Domain Name (FQDN) of the Diameter peer, use the **destination host** command in Diameter peer configuration mode. To remove the FQDN, use the **no** form of this command

destination host *string*

no destination host

Syntax Description

string	FQDN string of the Diameter peer.

Defaults

No default behavior or values.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **destination host** command to define the FQDN of the Diameter peer. This FQDN will be sent in various messages so that intermediate proxies can properly route packets.

Examples

The following configuration example specifies “dcca1.cisco.com as the FQDN of the Diameter peer:

```
diameter peer dcca1
 address ipv4 10.10.10.1
 transport tcp port 4000
 security ipsec
 source interface fastEthernet0
 timer connection 120
 destination host dcca1.cisco.com
```

Related Commands .

Command	Description
address ipv4	Configures the IP address of the Diameter peer host.
destination realm	Configures the destination realm (domain name) in which the Diameter host is located.
diameter peer	Defines the Diameter peer (server) and enters diameter peer configuration mode.
ip vrf forwarding	Defines the VRF associated with the Diameter peer.

Command	Description
security	Configures the security protocol to use for the Diameter peer-to-peer connection.
source interface	Configures the interface to use to connect to the Diameter peer.
timer	Configures Diameter base protocol timers for peer-to-peer communication.
transport	Configures the transport protocol to use to connect with the Diameter peer.

destination realm

To configure the destination realm (part of the domain "*@realm*") in which the Diameter peer is located, use the **destination realm** command in Diameter peer configuration mode. To remove the destination realm configuration, use the **no** form of this command

destination realm *name*

no destination realm

Syntax Description

name	Name of the domain (i.e. *cisco*.com) in which the Diameter peer is located.

Defaults

No default behavior or values.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **diameter realm** command to specify the destination realm to be included in messages exchanged with a Diameter peer.

The realm might be added by an authentication, authorization, and accounting (AAA) client when sending an AAA request. However, if the client does not add the attribute, then the value configured while in Diameter peer configuration mode is used when sending messages to the destination Diameter peer. If a value is not configured for a Diameter peer, the global value specified using the **diameter destination realm** global configuration command is used.

Examples

The following configuration example configures "cisco.com" as the destination realm:

```
Diameter peer dcca1
 address ipv4 10.10.10.1
 transport tcp port 4000
 security ipsec
 source interface fastEthernet0
 timer connection 120
 destination host dcca1.cisco.com
 destination realm cisco.com
```

Related Commands .

Command	Description
address ipv4	Configures the IP address of the Diameter peer host.
destination host	Configures the Fully Qualified Domain Name (FQDN) of the Diameter peer
diameter peer	Defines the Diameter peer (server) and enters diameter peer configuration mode.
ip vrf forwarding	Defines the VRF associated with the Diameter peer.
security	Configures the security protocol to use for the Diameter peer-to-peer connection.
source interface	Configures the interface to use to connect to the Diameter peer.
timer	Configures Diameter base protocol timers for peer-to-peer communication.
transport	Configures the transport protocol to use to connect with the Diameter peer.

destination-realm

To configure the destination realm to be sent in credit control response (CCR) initial requests to a Diameter credit control application (DCCA) server, use the **destination-realm** command in DCCA profile configuration mode. To remove the destination realm configuration, use the **no** form of this command

destination-realm *name*

no destination-realm

Syntax Description

name	Name of the domain (i.e. *cisco*.com) in which the DCCA client is located.

Defaults

No default behavior or values.

Command Modes

DCCA client configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **diameter-realm** command to specify the destination realm to be sent in CCR initial requests to a DCCA server.

Examples

The following configuration example configures “cisco.com” as the destination realm:

```
Diameter peer dcca1
 address ipv4 10.10.10.1
 transport tcp port 4000
 security ipsec
 source interface fastEthernet0
 timer connection 120
 destination host dcca1.cisco.com
 destination realm cisco.com
```

Related Commands

Command	Description
authorization	Defines a method of authorization (AAA method list), in the DCCA client profile, that specifies the Diameter server groups.
ccfh	Configures the Credit Control Failure Handling (CCFH) AVP locally to use for a credit-control session when the Credit Control Answer (CCA) sent by the DCCA server does not contain CCFH value.

Command	Description
content dcca profile	Defines the DCCA client profile in a GGSN charging profile.
gprs dcca profile	Defines a DCCA client profile on the GGSN and enters DCCA client profile configuration mode.
session-failover	Configures Credit Control Session Failover (CCSF) AVP support when a credit control answer (CCA) message from the DCCA server does not contain a value for the CCSF AVP.
trigger	Specifies that SGSN and QoS changes will trigger a DCCA client to request quota-reauthorization
tx-timeout	Configures a TX timeout value used by the DCCA client to monitor the communication of Credit Control Requests (CCRs) with a Diameter server.

dhcp-gateway-address

To specify the subnet in which the DHCP server should return addresses for DHCP requests for mobile station (MS) users entering a particular public data network (PDN) access point, use the **dhcp-gateway-address** command in access-point configuration mode. To remove a DHCP gateway address and return to the default, use the **no** form of this command.

dhcp-gateway-address *ip-address*

no dhcp-gateway-address

Syntax Description

ip-address	The IP address of the DHCP gateway to be used in DHCP requests for users who connect through the specified access point.

Defaults

When you do not configure a **dhcp-gateway-address**, the gateway GPRS support node (GGSN) uses the virtual template interface address as the DHCP gateway address.

Command Modes

Access-point configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The **dhcp-gateway-address** specifies the value of the giaddr field that is passed in DHCP messages between the GGSN and the DHCP server. If you do not specify a DHCP gateway address, the address assigned to the virtual template is used.

Though a default value for the virtual template address will occur, you should configure another value for the **dhcp-gateway-address** command whenever you are implementing DHCP services at an access point.

If the access point is configured for VPN routing and forwarding (VRF), then the dynamic (or static addresses) returned for MSs of packet data protocol (PDP) contexts at the access point will also be part of that VRF address space. If the DHCP server is located within the VRF address space, then the corresponding loopback interface for the **dhcp-gateway-address** must also be configured within the VRF address space.

Examples

The following example specifies an IP address of 10.88.0.1 for the giaddr field (the **dhcp-gateway-address**) of DHCP server requests. Note that the IP address of a loopback interface, in this case Loopback2, matches the IP address specified in the **dhcp-gateway-address** command. This is required for proper configuration of DHCP on the GGSN.

```
interface Loopback2
 ip address 10.88.0.1 255.255.255.255
!
gprs access-point-list gprs
 access-point 8
   access-point-name pdn.aaaa.com
   ip-address-pool dhcp-proxy-client
   aggregate auto
   dhcp-server 172.16.43.35
   dhcp-gateway-address 10.88.0.1
   exit
```

Related Commands

Command	Description
dhcp-server	Specifies a primary (and backup) DHCP server to allocate IP addresses to MS users entering a particular PDN access point.
gprs default ip-address-pool	Specifies a dynamic address allocation method using IP address pools for the GGSN.
ip-address-pool	Specifies a dynamic address allocation method using IP address pools for the current access point.

dhcp-server

To specify a primary (and backup) DHCP server to allocate IP addresses to mobile station (MS) users entering a particular public data network (PDN) access point, use the **dhcp-server** command in access-point configuration mode. To remove the DHCP server from the access-point configuration, use the **no** form of this command.

dhcp-server {*ip-address*} [*ip-address*] [**vrf**]

no dhcp-server

Syntax Description

ip-address	IP address of a DHCP server. The first *ip-address* argument specifies the IP address of the primary DHCP server. The second (optional) *ip-address* argument specifies the IP address of a backup DHCP server.
vrf	DHCP server uses the VPN routing and forwarding (VRF) table that is associated with the access point name (APN).

Defaults

Global routing table

Command Modes

Access-point configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX, with the following changes: • The **vrf** keyword was added. • The *name* argument, as an option for a host name in place of the IP address of a host, has been removed.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

To configure DHCP on the gateway GPRS support node (GGSN), you must configure either the **gprs default ip-address-pool** global configuration command, or the **ip-address-pool** access-point configuration command with the **dhcp-proxy-client** keyword option.

After you configure the access point for DHCP proxy client services, use the **dhcp-server** command to specify a DHCP server.

Use the *ip-address* argument to specify the IP address of the DHCP server. The second, optional *ip-address* argument can be used to specify the IP address of a backup DHCP server to be used in the event that the primary DHCP server is unavailable. If you do not specify a backup DHCP server, then no backup DHCP server is available.

The DHCP server can be specified in two ways:

- At the global configuration level, using the **gprs default dhcp-server** command.
- At the access-point configuration level, using the **dhcp-server** command.

If you specify a DHCP server at the access-point level, using the **dhcp-server** command, then the server address specified at the access point overrides the address specified at the global level. If you do not specify a DHCP server address at the access-point level, then the address specified at the global level is used.

Therefore, you can have both a global address setting one or more local access-point level settings if you need to use different DHCP servers for different access points.

Use the **vrf** keyword when the DHCP server itself is located within the address space of a VRF interface on the GGSN. If the DHCP server is located within the VRF address space, then the corresponding loopback interface for the **dhcp-gateway-address** must also be configured within the VRF address space.

Examples

Example 1

The following example specifies both primary and backup DHCP servers to allocate IP addresses to mobile station users through a non-VPN access point. Because the **vrf** keyword is not configured, the default global routing table is used. The primary DHCP server is located at IP address 10.60.0.1, and the secondary DHCP server is located at IP address 10.60.0.2:

```
access-point 2
 access-point-name xyz.com
 dhcp-server 10.60.0.1 10.60.0.2
 dhcp-gateway-address 10.60.0.1
 exit
```

Example 2

The following example from an implementation on the Cisco 7200 series router platform shows a VRF configuration for vpn3 (without tunneling) using the **ip vrf** global configuration command. Because the **ip vrf** command establishes both VRF and Cisco Express Forwarding (CEF) routing tables, notice that **ip cef** also is configured at the global configuration level to enable CEF switching at all of the interfaces.

The following other configuration elements must also associate the same VRF named vpn3:

- FastEthernet0/0 is configured as the Gi interface, using the **ip vrf forwarding** interface configuration command.
- Access point 2 implements VRF, using the **vrf** command access-point configuration command.

The DHCP server at access-point 2 is also configured to support VRF. Notice that access point 1 uses the same DHCP server, but does not support the VRF address space. The IP addresses for access point 1 will apply to the global routing table:

```
aaa new-model
!
aaa group server radius foo
 server 10.2.3.4
 server 10.6.7.8
!
aaa authentication ppp foo group foo
aaa authorization network default group radius
aaa accounting exec default start-stop group foo
!
ip cef
!
ip vrf vpn3
 rd 300:3
!
interface Loopback1
 ip address 10.30.30.30 255.255.255.255
!
interface Loopback2
 ip vrf forwarding vpn3
 ip address 10.27.27.27 255.255.255.255
!
interface FastEthernet0/0
 ip vrf forwarding vpn3
 ip address 10.50.0.1 255.255.0.0
 duplex half
!
interface FastEthernet1/0
 ip address 10.70.0.1 255.255.0.0
 duplex half
!
interface loopback 1
 ip address 10.8.0.1 255.255.255.0
!
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list gprs
!
ip route 10.10.0.1 255.255.255.255 Virtual-Template1
ip route vrf vpn3 10.100.0.5 255.255.255.0 fa0/0 10.50.0.2
ip route 10.200.0.5 255.255.255.0 fa1/0 10.70.0.2
!
no ip http server
!
gprs access-point-list gprs
 access-point 1
  access-point-name gprs.pdn.com
  ip-address-pool dhcp-proxy-client
  dhcp-server 10.200.0.5
  dhcp-gateway-address 10.30.30.30
  network-request-activation
  exit
  !
 access-point 2
  access-point-name gprs.pdn2.com
  access-mode non-transparent
  ip-address-pool dhcp-proxy-client
  dhcp-server 10.100.0.5 10.100.0.6 vrf
  dhcp-gateway-address 10.27.27.27
```

```
  aaa-group authentication foo
  vrf vpn3
  exit
!
gprs default ip-address-pool dhcp-proxy-client
gprs gtp ip udp ignore checksum
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

Related Commands

Command	Description
dhcp-gateway-address	Specifies the subnet in which the DHCP server should return addresses for DHCP requests for MS users entering a particular PDN access point.
ip-address-pool	Specifies a dynamic address allocation method using IP address pools for the current access point.
vrf	Configures VPN routing and forwarding at a GGSN access point and associates the access point with a particular VRF instance.

diameter origin host

To define the host name of the host of a Diameter node, use the **diameter origin host** command in global configuration mode. To remove the configuration, use the **no** form of this command

diameter origin host *string*

no diameter origin host

Syntax Description

string	FQDN string of the host of a Diameter peer.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **diameter origin host** command to define the host name of a Diameter node. This information will be sent in requests to Diameter peers.

The global level configuration takes affect if an origin host is not defined at the server level using the **destination host** Diameter peer configuration command.

Examples

The following configuration example defines ggsn.cisco.com as the originating host:

```
diameter origin host ggsn.cisco.com
```

Related Commands

Command	Description
diameter origin realm	Configures the origin realm (domain name) to be sent in each request to a diameter peer.
diameter redundancy	Enables the Diameter base protocol to be a Cisco IOS Redundancy Facility (RF) client and monitor and report Active/Standby transitions.
diameter timer	Configures Diameter base protocol timers.
diameter vendor support	Configures the Diameter node to advertise various vendor AVPs that it supports in capability exchange messages to a Diameter peer.

diameter origin realm

To configure the origin realm to be sent in requests to a Diameter peer for a Diameter node, use the **diameter origin realm** command in global configuration mode. To remove the origin realm configuration, use the **no** form of this command

diameter origin realm *name*

no diameter origin realm

Syntax Description

name	Name of the domain to which the Diameter node belongs.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **diameter origin realm** command to specify the domain to which a Diameter client belongs. Origin realm information is included in each request sent to a Diameter client.

This global level configuration takes affect if an origin realm is not defined at the server level using the **destination realm** Diameter peer configuration command.

Examples

The following configuration example defines cisco.com as the origin to which a Diameter client belongs:

```
diameter origin realm cisco.com
```

Related Commands

Command	Description
diameter origin host	Defines the host name of the originating Diameter peer.
diameter redundancy	Enables the Diameter base protocol to be a Cisco IOS Redundancy Facility (RF) client and monitor and report Active/Standby transitions.
diameter timer	Configures Diameter base protocol timers.
diameter vendor support	Configures the Diameter node to advertise various vendor AVPs that it supports in capability exchange messages to a Diameter peer.

diameter peer

To define a Diameter peer (server) and enter Diameter peer configuration mode, use the **diameter peer** command in global configuration mode. To remove a Diameter peer configuration, use the **no** form of this command

diameter peer *name*

no diameter peer *name*

Syntax Description

name

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **diameter peer** command to define a Diameter peer and enter Diameter peer configuration mode. From Diameter peer configuration mode, you define the parameters to use to contact a Diameter server. These parameters include:

- IP address of the Diameter peer
- Transport protocol to use to connect to the peer
- Security protocol to use for peer-to-peer communication
- Source interface to use to connect with peer
- Diameter base protocol timers
- Destination host and realm
- VRF associated with Diameter peer

Examples

The following configuration example defines Diameter peer “dcca1”:

```
diameter peer dcca1
```

Related Commands .

Command	Description
address ipv4	Configures the IP address of the Diameter peer host.
destination host	Configures the FQDN of the Diameter peer
destination realm	Configures the destination realm (domain name) in which the Diameter host is located.
ip vrf forwarding	Defines the VRF associated with the Diameter peer.
security	Configures the security protocol to use for the Diameter peer-to-peer connection.
source interface	Configures the interface to use to connect to the Diameter peer.
timer	Configures Diameter base protocol timers for peer-to-peer communication.
transport	Configures the transport protocol to use to connect with the Diameter peer.

diameter redundancy

To enable a Diameter node to be a Cisco IOS Redundancy Facility (RF) client and to track session states, use the **diameter redundancy** command in global configuration mode. To disable redundancy, use the **no** form of this command.

diameter redundancy

no diameter redundancy

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **diameter redundancy** command to enable the Diameter base protocol to be a Cisco IOS Redundancy Facility (RF) client and monitor and report Active/Standby transitions.

When a Diameter device is in Standby mode, it will not initiation a TCP connection to a peer. Upon a Standby to Active transition state, the Diameter device initiates a TCP connection to the Diameter peer.

Examples

The following example enables Diameter redundancy on a gateway GPRS support node (GGSN):

```
diameter redundancy
```

Related Commands

Command	Description
diameter origin host	Defines the host name of the originating Diameter peer.
diameter origin realm	Configures the origin realm (domain name) to be sent in each request to a diameter peer.
diameter timer	Configures Diameter base protocol timers.
diameter vendor support	Configures the Diameter node to advertise various vendor AVPs that it supports in capability exchange messages to a Diameter peer.

diameter timer

To configure Diameter protocol timers, use the **diameter timer** command in global configuration mode. To remove the timer configurations, use the **no** form of this command

diameter timer {connection | transaction | watchdog} *seconds*

no diameter timer {connection | transaction | watchdog}

Syntax Description

connection	Sets the maximum amount of time the gateway GPRS support node (GGSN) attempts to reconnect to a Diameter peer after a connection to the peer has been brought down due to a transport failure. A value of 0 configures the GGSN to not try to reconnect.
transaction	Sets the maximum amount of time the GGSN waits for a Diameter peer to respond before trying another peer.
watchdog	Sets the maximum period of time the GGSN will wait for a Diameter peer to respond to a watchdog packet. When this timer expires, a Device-Watchdog-Request (DWR) is sent to the Diameter peer and the watchdog timer is reset. If a Device-Watchdog-Answer (DWA) is not received before the next expiration of the watchdog timer, a transport failure to the Diameter peer has occur.
seconds	Maximum amount of time, in seconds, of the timer. Valid range, in seconds, is 0 to 1000. The default is 30.

Defaults

30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.

Usage Guidelines

Use the **diameter timer** command to configure global Diameter timers for a Diameter node.

The global level timers takes affect only if timers are not configured at the Diameter server level using the **timer** Diameter peer configuration command.

When configuring timers, note that the value for the transaction timers, should be larger than the value for the TX timer, and, on the serving GPRS support node (SGSN), the values configured for the number GPRS tunneling protocol (GTP) N3 requests and T3 retransmissions must be larger than the sum of all possible server timers (RADIUS, Diameter credit control application [DCCA], and Cisco Content Services Gateway [CSG]). Specifically, the SGSN N3*T3 must be greater than 2 x RADIUS timeout + *N* x DCCA timeout + CSG timeout where:

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

Examples

The following configuration example sets the global connection timer to 120 seconds:

```
global diameter timer connection 120
```

Related Commands

Command	Description
diameter origin host	Defines the host name of the originating Diameter peer.
diameter origin realm	Configures the origin realm (domain name) to be sent in each request to a diameter peer.
diameter redundancy	Enables the Diameter base protocol to be a Cisco IOS Redundancy Facility client and monitor and report Active/Standby transitions.
diameter vendor support	Configures the Diameter node to advertise various vendor AVPs that it supports in capability exchange messages to a Diameter peer.

diameter vendor support

To configure the Diameter node to advertise various vendor attribute-value pairs (AVPs) that it supports in capability exchange messages to a Diameter peer, use the **diameter vendor support** command in global configuration mode. To remove the advertising of a vendor AVP, use the **no** form of this command

diameter vendor support {Cisco | 3gpp | Vodafone}

no diameter vendor support {Cisco | 3gpp | Vodafone}

Syntax Description

Cisco	Advertises Cisco AVP support in capability exchange messages.
3gpp	Advertises 3GPP AVP support in capability exchange messages.
Vodafone	Advertises Vodafone AVP support in capability exchange messages.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Multiple instances of this command can be configured if the vendor IDs differ.

Examples

The following configuration example configures the 3GPP AVPs to be advertised as a supported vendor AVP in capability exchange messages:

```
diameter vendor support 3gpp
```

Related Commands

Command	Description
diameter origin host	Defines the host name of the originating Diameter peer.
diameter origin realm	Configures the origin realm (domain name) to be sent in each request to a diameter peer.
diameter redundancy	Enables the Diameter base protocol to be a Cisco IOS Redundancy Facility client and monitor and report Active/Standby transitions.
diameter timer	Configures Diameter base protocol timers.

dns primary

To specify a primary (and backup) Domain Name System (DNS) to be sent in Create packet data protocol (PDP) Context responses at the access point, use the **dns primary** command in access-point configuration mode. To remove the DNS from the access-point configuration, use the **no** form of this command.

dns primary *ip-address* [**secondary** *ip-address*]

no dns primary *ip-address* [**secondary** *ip-address*]

Syntax Description

ip-address	IP address of the primary DNS.
secondary *ip-address*	(Optional) Specifies the IP address of the backup DNS.

Defaults

No default behavior or values.

Command Modes

Access-point configuration

Command History

Release	Modification
12.2(8)YY	This command was introduced.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **dns primary** command to specify the primary (and backup) DNS at the access-point level.

This feature benefits address-allocation schemes which have no mechanism for obtaining these addresses. Also, for a RADIUS-based allocation scheme, this feature prevents the operator from having to configure a NetBIOS Name Server (NBNS) and DNS for each user profile.

The DNS address can come from three possible sources: DHCP server, RADIUS server, or local access point name (APN) configuration. The criterion for selecting the DNS address depends on the IP address allocation scheme configured under the APN. Depending on the configuration, the criterion for selecting the DNS address is as follows:

1. DHCP-based IP address allocation scheme (local and external)—A DNS address returned from the DHCP server is sent to the mobile station (MS). If the DHCP server does not return a DNS address, the local APN configuration is used.
2. RADIUS-based IP address allocation scheme—A DNS address returned from the RADIUS server (in Access-Accept responses) is used. If the RADIUS server does not return a DNS address, the local APN configuration is used.
3. Local IP address pool-based IP address allocation scheme—A local APN configuration is used.
4. Static IP addresses—A local APN configuration is used.

Note The gateway GPRS support node (GGSN) sends DNS addresses in the Create PDP Context response only if the MS is requesting the DNS address in the protocol configuration option (PCO) information element (IE).

Examples

The following example specifies a primary DNS and a secondary DNS at the access point level:

```
access-point 2
 access-point-name xyz.com
 dns primary 10.60.0.1 secondary 10.60.0.2
 exit
```

Related Commands

Command	Description
ip-address-pool	Specifies a dynamic address allocation method using IP address pools for the current access point.
nbns primary	Specifies a primary (and backup) NBNS at the access point level.

echo-interval

To specify the number of seconds that the quota server waits before sending an echo-request message to the Cisco Content Services Gateway (CSG), use the **echo-interval** command in quota server configuration mode. To return to the default value, use the **no** form of this command

echo-interval *interval*

no echo-interval *interval*

Syntax Description

interval	Number of seconds that the quota server waits before sending an echo request message to the CSG. Valid values are 0 (quota server-initiated echo messages are disabled) or a value between 60 to 65535. The default is 60.

Defaults

60 seconds.

Command Modes

Quota server configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **echo-interval** command to specify the interval that the quota server waits before sending an echo-request message to the CSG to check for GPRS tunneling protocol (GTP) path failure.

Note A value of 0 seconds disables echo requests on the quota server.

Examples

The following example configures the quota server to wait 90 seconds before sending an echo-request message:

```
ggsn quota-server qs1
 interface loopback1
 echo-interval 90
```

Related Commands .

Command	Description
clear ggsn quota-server statistics	Clears the quota server-related statistics displayed using the **show ggsn quota-server statistics** command.
csg-group	Associates the quota server to a CSG group that is to be used for quota server-to-CSG communication.

Command	Description
ggsn quota-server	Configures the quota server process that interfaces with the CSG for enhanced service aware billing.
interface	Specifies the logical interface, by name, that the quota server will use to communicate with the CSG.
n3-requests	Specifies the maximum number of times that the quota server attempts to send a signaling request to the CSG.
t3-response	Specifies the initial time that the quota server waits before resending a signaling request message when a response to a request has not been received.
show ggsn quota-server	Displays quota server parameters or statistics about the quota server message and error counts.

encapsulation gtp

To specify the GPRS tunneling protocol (GTP) as the encapsulation type for packets transmitted over the virtual template interface, use the **encapsulation gtp** command in interface configuration mode. To remove the GTP encapsulation type and return to the default, use the **no** form of this command.

encapsulation gtp

no encapsulation gtp

Syntax Description

This command has no arguments or keywords.

Defaults

Point-to-point protocol (PPP) encapsulation

Command Modes

Interface configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **encapsulation gtp** command to specify the GTP as the encapsulation type for a virtual template. This is a mandatory setting for the gateway GPRS support node (GGSN).

Examples

The following example specifies the GTP as the encapsulation type:

```
interface virtual-template 1
 ip unnumber loopback 1
 no ip directed-broadcast
 encapsulation gtp
```

gbr traffic-class

To define in a Call Admission Control (CAC) maximum quality of service (QoS) policy, the highest guaranteed bit rate (GBR) that can be allowed for real-time traffic, use the **gbr traffic-class** command in CAC maximum QoS policy configuration mode. To return to the default value, use the **no** form of this command.

gbr traffic-class *traffic-class-name bitrate* **{uplink | downlink} [reject]**

no gbr traffic-class *traffic-class-name bitrate* **{uplink | downlink} [reject]**

Syntax Description

traffic-class-name	Specifies the Universal Mobile Telecommunication System (UMTS) traffic class to which the GBR applies. Valid values are Conversational and Streaming.
bitrate	Guaranteed bit rate in kilobits per second. Valid value is between 1 and 16000. **Note** Although the valid command range for both the uplink and downlink direction is 1 to 16000, the maximum rate that can be acheived in the uplink direction is 8640. Additionally, a value greater than 8640 in the downlink direction is supported for GTPv1 packet data protocol (PDP) contexts only.
uplink	Specifies GBR applies to a traffic-class for uplink traffic.
downlink	Specifies GBR applies to a traffic-class for downlink traffic.
reject	(Optional) Specifies that when the GBR exceeds the configured value, the Create PDP Context request is rejected. This option is ignored for Update PDP Context requests.

Defaults

If the GBR in a Create PDP Context request or Update PDP Context request is greater than the configured value, the requested GBR is downgraded to the configured value.

Command Modes

CAC maximum QoS policy configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into the Cisco IOS Release 12.3(14)YU, and to support High Speed Downlink Packet Access, the maximum data transmission rate in the downlink direction was increased to 16000 kilobits.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gbr traffic-class** CAC maximum QoS policy configuration command to define the highest GBR that can be accepted for real-time traffic on an APN.

When the **reject** optional keyword is specified, if the requested GBR exceeds the configured value, the Create PDP Context is rejected.

If the **reject** keyword is not specified and the GBR in a create or update PDP context is greater than the configured value, the requested GBR is downgraded to the configured value.

Note This command does not apply to non real-time traffic classes (Interactive or Background).

Examples

The following example configures the maximum GBR for conversational class as 1000 kilobits in the uplink direction:

```
gbr traffic-class conversational 1000 uplink
```

Related Commands

Command	Description
cac-policy	Enables the maximum QoS policy function of the CAC feature and applies a policy to an APN.
gprs qos cac-policy	Creates or modifies a CAC maximum QoS policy.
maximum delay-class	Defines the maximum delay class for R97/R98 (GPRS) QoS that can be accepted.
maximum peak-throughput	Defines the maximum peak throughput for R97/R98 (GPRS) QoS that can be accepted.
maximum pdp-context	Specifies the maximum PDP contexts that can be created for a particular APN.
maximum traffic-class	Defines the highest traffic class that can be accepted.
mbr traffic-class	Specifies the highest maximum bit rate that can be allowed for each traffic class for both directions (downlink and uplink).

ggsn csg-group

To configure a Cisco Content Services Gateway (CSG) group on the gateway GPRS support node (GGSN), to use for quota server-to-CSG communication, use the **ggsn csg-group** command in global configuration mode. To deconfigure the CSG group, use the **no** form of this command

ggsn csg-group *csg-group-name*

no ggsn csg-group *csg-group-name*

Syntax Description

csg-group-name	Name of the CSG group.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **ggsn csg-group** command to configure a CSG server group on the GGSN that will be used for quota server-to-CSG communication when service-aware billing is enabled.

Only one CSG server group can be defined per quota server. Therefore, only on GPRS tunneling protocol (GTP) path is established between the quota server and CSG at a time. On this GTP path, echo and node alive messages are exchanged.

Note Dynamic echo, recovery IE detection are not supported.

Issuing the **ggsn csg-group** command enters CSG server group configuration mode. In CSG server group configuration mode, you can define the virtual address of the CSG server group, the port number on which the CSG listens for quota server traffic, and the real addresses of up to two CSGs (Active and Standby).

Examples

The following configuration example configures a CSG server group named “csg1” and enters CSG server group configuration mode:

```
ggsn csg-group csg1
```

Related Commands

Command	Description
port	Configures the port number on which the CSG listens for quota server traffic.
real-address	Configures the IP address of a real CSG for source checking on inbound messages from a CSG.
show ggsn csg	Displays the parameters used by the CSG group or the number of path and quota management messages sent and received by the quota server.
virtual-address	Configures a virtual IP address to which the quota server will send all requests.

ggsn quota-server

To configure the quota server process that interfaces with the Cisco Content Services Gateway (CSG) in a service-aware gateway GPRS support node (GGSN) implementation, use the **ggsn quota-server** command in global configuration mode. To disable the quota server process on the GGSN, use the **no** form of this command.

ggsn quota-server *server-name*

no ggsn quota-server *server-name*

Syntax Description

server-name	Name of the quota server process.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **ggsn quota-server** command to configure the quota server process on a GGSN and to enter quota server configuration mode. In a service-aware GGSN configuration, the quota server process on the GGSN:

- Receives incoming path management and quota management messages from the CSG
- Maps Diameter credit control application (DCCA) categories to CSG services and vice versa
- Maps DCCA rulebase IDs to CSG billing plans
- Provides a Diameter/DCCA interface to the CSG for quota requests and returns

Note One quota server process can be configured per GGSN. Configuring more than one quota server process will overwrite the existing process.

To complete the quota server configuration, while in quota server configuration mode, you must also complete the following tasks:

- Configure a logical interface via which the quota server communicates with the CSG using the **interface** command
- Configure the duration of the echo interval for quota server path management using the **echo-interval** command. The GGSN quota server and CSG use echo timing to determine the health of the path between them.

- Configure the number of times a message is retransmitted to the CSG using the **n3-requests** command.
- Configure the amount of time the quota server waits for a response from the CSG using the **t3-response** command.
- Associate the quota server with a CSG group using the **csg-group** command.

Examples

The following configuration example configures the GGSN quota server "gs1" and enters quota server configuration mode:

```
gprs quota-server qs1
```

Related Commands .

Command	Description
csg-group	Associates the quota server to a CSG group that is to be used for quota server-to-CSG communication.
echo-interval	Specifies the number of seconds that the quota server waits before sending an echo-request message to the CSG.
interface	Specifies the logical interface, by name, that the quota server will use to communicate with the CSG.
n3-requests	Specifies the maximum number of times that the quota server attempts to send a signaling request to the CSG.
t3-response	Specifies the initial time that the quota server waits before resending a signaling request message when a response to a request has not been received.
show ggsn quota-server	Displays quota server parameters or statistics about the quota server message and error counts.

gprs access-point-list

To configure an access point list that you use to define public data network (PDN) access points on the gateway GPRS support node (GGSN), use the **gprs access-point-list** command in global configuration mode. To remove an existing access-point list, use the **no** form of this command.

gprs access-point-list *list_name*

no gprs access-point-list

Syntax Description

list_name	The name of the access-point list.

Defaults

No access-point list is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs access-point-list** command to configure an access list that you use to define PDN access points on the GGSN. Currently, only one access list can be defined per virtual template.

Examples

The following example sets up an access-point list that is used to define two GGSN access points:

```
! Virtual Template configuration
interface virtual-template 1
 ip unnumber loopback 1
 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
  exit
!
 access-point 2
  access-point-name xyz.com
  exit
```

Related Commands

Command	Description
access-point	Specifies an access point number and enters access-point configuration mode.

gprs canonical-qos best-effort bandwidth-factor

To specify the bandwidth factor to be applied to the canonical best-effort quality of service (QoS) class, use the **gprs canonical-qos best-effort bandwidth-factor** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs canonical-qos best-effort bandwidth-factor *bandwidth-factor*

no gprs canonical-qos best-effort bandwidth-factor *bandwidth-factor*

Syntax Description

bandwidth-factor	Integer from 1 to 4000000 that specifies the desired bandwidth factor (in bits per second). The default is 10 bits per second.

Defaults

10 bits per second

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The **canonical qos best-effort bandwidth-factor** command specifies an average bandwidth that is expected to be used by best-effort QoS class mobile sessions. The default value of 10 bps is chosen arbitrarily. If you observe that users accessing the gateway GPRS support node (GGSN) are using a higher average bandwidth, then you should increase the bandwidth value.

Note Before configuring the average bandwidth expected to be used by the best-effort QoS class using the **gprs canonical-qos best-effort bandwidth-factor** command, canonical QoS must be enabled using the **gprs qos map canonical-qos** command.

Examples

The following example configures a bandwidth factor of 20:

```
gprs canonical-qos best-effort bandwidth-factor 20
```

Related Commands

Command	Description
gprs canonical-qos gsn-resource-factor	Specifies the total amount of resource that the GGSN uses to provide canonical QoS service levels to mobile users.
gprs qos map canonical-qos	Enables the mapping of GPRS QoS categories to a canonical QoS method.

gprs canonical-qos gsn-resource-factor

To specify the total amount of resource that the gateway GPRS support node (GGSN) uses to provide canonical quality of service (QoS) service levels to mobile users, use the **gprs canonical-qos gsn-resource-factor** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs canonical-qos gsn-resource-factor *resource-factor*

no gprs canonical-qos gsn-resource-factor *resource-factor*

Syntax Description

resource-factor	Integer between 1 and 4294967295 that represents an amount of resource that the GGSN calculates internally for canonical QoS processing. The default value is 3145728000.

Defaults

3145728,000

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX, and the default value was changed from 1,048,576 to 3,145,728,000 bits per second.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The default value for this command was chosen to support 10,000 packet data protocol (PDP) contexts with a premium QoS class. If a greater throughput is required for general packet radio service (GPRS) user data, increase the resource factor value. However, selecting a high value may result in exceeding the actual processing capacity of the GGSN.

Examples

The following example configures a resource factor of 1048576:

```
gprs canonical-qos gsn-resource-factor 1048576
```

Related Commands

Command	Description
gprs canonical-qos best-effort bandwidth-factor	Specifies the bandwidth factor to be applied to the canonical best-effort QoS class.
gprs canonical-qos premium mean-throughput-deviation	Specifies a mean throughput deviation factor that the GGSN uses to calculate the allowable data throughput for the premium QoS class.

gprs canonical-qos map tos

To specify a quality of service (QoS) mapping from the canonical QoS classes to an IP type of service (ToS) precedence value, use the **gprs canonical-qos map tos** command in global configuration mode. To remove a QoS mapping and return to the default values, use the **no** form of this command.

gprs canonical-qos map tos [**premium** *tos-value* [**normal** *tos-value* [**best-effort** *tos-value*]]]

no gprs canonical-qos map tos [**premium** *tos-value* [**normal** *tos-value* [**best-effort** *tos-value*]]]

Syntax Description

premium *tos-value*	ToS mapping for a premium QoS. The *tos-value* can be a number from 0 to 5. A higher number indicates a higher service priority. The default is 2.
normal *tos-value*	ToS mapping for a normal QoS. The *tos-value* can be a number from 0 to 5. A higher number indicates a higher service priority. The default is 1.
best-effort *tos-value*	ToS mapping for a best effort QoS. The *tos-value* can be a number from 0 to 5. A higher number indicates a higher service priority. The default is 0.

Defaults

When canonical QoS is enabled on the gateway GPRS support node (GGSN), the default IP ToS precedence values are assigned according to the canonical QoS class as follows:

- Premium—2
- Normal—1
- Best effort—0

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs canonical-qos map tos** command to specify a mapping between various QoS categories and the ToS precedence bits in the IP header for packets transmitted over the Gn (GPRS tunneling protocol [GTP] tunnels) and Gi interfaces.

All the keyword arguments for the command are optional. However, if you specify a value for the **normal** argument, you must specify a value for the **premium** argument. And if you specify a value with the **best-effort** argument, then you must specify a value for both the **premium** and the **normal** arguments.

When a request for a user session comes in (a packet data protocol [PDP] context activation request), the GGSN determines whether the requested QoS for the session packets can be handled based on the maximum packet handling capability of the GGSN. Based on this determination, one of the following occurs:

- If the requested QoS can be provided, then it is maintained.
- If the requested QoS cannot be provided, then the QoS for the requested session is either lowered or the session is rejected.

Examples

The following example specifies a QoS mapping from the canonical QoS classes to a premium ToS category of 5, a normal ToS category of 3, and a best-effort ToS category of 2:

```
gprs canonical-qos map tos premium 5 normal 3 best-effort 2
```

Related Commands

Command	Description
gprs canonical-qos best-effort bandwidth-factor	Specifies the bandwidth factor to be applied to the canonical best-effort QoS class.
gprs canonical-qos gsn-resource-factor	Specifies the total amount of resource that the GGSN uses to provide canonical QoS service levels to mobile users.
gprs canonical-qos premium mean-throughput-deviation	Specifies a mean throughput deviation factor that the GGSN uses to calculate the allowable data throughput for the premium QoS class.
gprs qos map canonical-qos	Enables mapping of GPRS QoS categories to a canonical QoS method that includes best effort, normal, and premium QoS classes.

gprs canonical-qos premium mean-throughput-deviation

To specify a mean throughput deviation factor that the gateway GPRS support node (GGSN) uses to calculate the allowable data throughput for the premium quality of service (QoS) class, use the **gprs canonical-qos premium mean-throughput-deviation** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs canonical-qos premium mean-throughput-deviation *deviation_factor*

no gprs canonical-qos premium mean-throughput-deviation *deviation_factor*

Syntax Description

deviation_factor	Value that specifies the deviation factor. This value can range from 1 to 1000. The default value is 100.

Defaults

100

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The GGSN uses the **gprs canonical-qos premium mean-throughput-deviation** command to calculate a mean throughput value that determines the amount of data throughput used for a premium QoS. The calculation is made based on the following formula, which includes the input deviation factor:

EB = Min[p, m + a(p - m)]

Where:

EB = the effective bandwidth
p = peak throughput from the GPRS QoS profile in packet data protocol (PDP) context requests
m = mean throughput from the GPRS QoS profile in PDP context requests
a = the deviation factor divided by 1000 (a/1000)

Examples

The following example configures a mean throughput deviation of 1000:

```
gprs canonical-qos premium mean-throughput-deviation 1000
```

Related Commands

Command	Description
gprs canonical-qos best-effort bandwidth-factor	Specifies the bandwidth factor to be applied to the canonical best-effort QoS class.
gprs canonical-qos gsn-resource-factor	Specifies the total amount of resource that the GGSN uses to provide canonical QoS service levels to mobile users.
gprs canonical-qos map tos	Specifies a QoS mapping from the canonical QoS classes to an IP ToS category.

gprs charging cdr-aggregation-limit

To specify the maximum number of call detail records (CDRs) that the gateway GPRS support node (GGSN) aggregates in a charging data transfer message to a charging gateway, use the **gprs charging cdr-aggregation-limit** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging cdr-aggregation-limit *cdr-limit*

no gprs charging cdr-aggregation-limit *cdr-limit*

Syntax Description

cdr-limit	An integer between 1 and 255 that specifies the number of CDRs that can be accumulated in a charging data transfer message. The default is 255 CDRs.

Defaults

255 CDRs

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs charging cdr-aggregation-limit** command to specify the maximum number of CDRs that can be accumulated in a charging data transfer message to a charging gateway connected to the GGSN.

When the aggregation limit is reached, the GGSN puts the CDRs into a message and immediately sends it to the charging gateway.

To view the configured CDR aggregation limit, use the **show gprs charging parameters** command.

Examples

The following example specifies 128 CDRs:

```
gprs charging cdr-aggregation-limit 128
```

Related Commands

Command	Description
gprs charging container volume-threshold	Specifies the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
gprs charging packet-queue-size	Specifies the maximum number of unacknowledged charging data transfer requests that the GGSN maintains in its queue.
gprs charging transfer interval	Specifies the number of seconds that the GGSN waits before it transfers charging data to the charging gateway.
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging cdr-option

To configure the gateway GPRS support node (GGSN) to include or not include certain information elements (IEs) in call detail records (CDRs), use the **gprs charging cdr-option** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging cdr-option [**apn** [**virtual**] | **apn-selection-mode** | **camel-charge-info** | **chch-selection-mode** | **dynamic-address** | **imeisv** | **local-record-sequence-number** | **ms-time-zone** | **nip** | **no-partial-cdr-generation** [**all**] | **node-id** | **packet-count** | **pdp-address** | **pdp-type** | **rat-type** | **served-msisdn** | **sgsn-plmn** | **service-record [***value***]** | **user-loc-info**]

no charging cdr-option [**apn** [**virtual**] | **apn-selection-mode** | **camel-charge-info** | **chch-selection-mode** | **dynamic-address** | **imeisv** | **external-charging-id** | **local-record-sequence-number** | **ms-time-zone** | **nip** | **no-partial-cdr-generation** [**all**] | **node-id** | **packet-count** | **pdp-address** | **pdp-type** | **rat-type** | **served-msisdn** | **sgsn-plmn** | **service-record [***value***]** | **user-loc-info**]

Syntax Description

apn [virtual]	Specifies that the access point name (APN) IE be included or not included in G-CDRs. Optionally, specify the **virtual** keyword to include the virtual APN in G-CDRs, accounting records, and credit control requests (CCRs).
apn-selection-mode	Specifies that the reason code for APN selection be included or not included in G-CDRs.
camel-charge-info	Specifies that a copy of the tag and length of the Customized Application for Mobile Enhanced Logic (CAMEL) from the serving GPRS support node's (SGSN's) CDR be included in G-CDRs.
chch-selection-mode	Specifies that the charging characteristics selection mode IE be included or not included in G-CDRs.
dynamic-address	Specifies that the dynamic address flag IE be included or not included in G-CDRs.
imeisv	Specifies that the International Mobile Equipment Identity IMEI software version (IMEISV) be included in G-CDRs. The IMEISV identifies the mobile equipment used by the subscriber.
local-record-sequence-number	Enables the GGSN to use the local record sequence number field in G-CDRs.
ms-time-zone	Specifies that the Mobile Station Time Zone (MSTZ) IE be included in G-CDRs. The MSTZ IE indicates the offset between universal time and local time.
nip	Specifies that the Network-Initiated PDP IE be included in G-CDRs.
no-partial-cdr-generation [**all**]	Enables the GGSN to create fully-qualified partial G-CDRs. Optionally, specify the **all** keyword option to configure the GGSN to copy the SGSN list for charging releases prior to Release 4 when an SGSN change limit trigger is configure as well.
node-id	Specifies that the GGSN includes the node that generated the CDR in the node ID field in G-CDRs.
packet-count	Enables the GGSN to provide uplink and downlink packet counts in the optional record extension field of a G-CDR.
pdp-address	Specifies that the packet data protocol (PDP) address IE be included or not included in G-CDRs.

pdp-type	Specifies that the PDP type IE be included or not included in G-CDRs.
rat-type	Specifies that the radio access technology (RAT) IE be included in G-CDRs. The RAT indicates whether the SGSN serves the user equipment (UE) by Universal Terrestrial Radio Access Network (UTRAN) or GSM/EDGE RAN (GERAN).
served-msisdn	Enables the GGSN to provide the mobile station integrated digital network (MSISDN) number from the Create PDP Context request in a G-CDR.
sgsn-plmn	Specifies that the SGSN PLMN identifier be included or not included in G-CDRs.
service-record [*number*]	Enables the GGSN to generate per-service records. Optionally, the maximum number of services records in a CDR can be specified. When the limit is reached, the current G-CDR is closed and a new partial CDR is opened. If a maximum number is not specified, the default of 5 is used.
user-loc-info	Specifies that the user location information (ULI) IE be included in G-CDRs. The ULI provides the cell global identity (CGI) and service area identity (SAI) of the subscriber location.

Defaults

By default, the parameters configured by the following keyword options are included in G-CDRs:

- **apn**
- **dynamic-address**
- **nip**
- **pdp-address**
- **pdp-type**

By default, the parameters configured by the following keyword options are not included in G-CDRs:

- **apn-selection**
- **camel-charge-info**
- **imeisv**
- **local-record-sequence-number**
- **ms-time-zone**
- **node-id**
- **packet-count**
- **rat-type**
- **served-msisdn**
- **user-loc-info**

By default, fully-qualified partial CDR generation is enabled.

By default, the generation of per-service records is disabled. When enabled, by default 5 service records are allowed per G-CDR.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T and the **no-partial-cdr-generation** and **packet-count** keyword options were added.
12.2(2)	This command was integrated into Cisco IOS Release 12.2(2) and the **served-msisdn** keyword option was added.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX and the **apn-selection-mode** keyword option was added.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(2)XB2	This command was integrated into Cisco IOS Release 12.3(2)XB2 and the **sgsn-plmn** keyword option was added.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(8)XU2	This command was integrated into Cisco IOS Release 12.3(8)XU2 and the **all** keyword option was added to the **no-partial-cdr-generation** keyword options.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into the Cisco IOS Release 12.3(14)YQ and the **service-record** [*number*] keyword option was added.
12.3(14)YU	This command was integrated into the Cisco IOS Release 12.3(14)YU and the following keyword options were added: • **apn [virtual]** • **camel-charge-info** • **imeisv** • **ms-time-zone** • **rat-type** • **user-loc-info**
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs charging cdr-option** command to configure the GGSN to include or not include (using the **no** form of the command) the APN, dynamic address flag, NIP, PDP address, or PDP type parameters in G-CDRs.

apn-selection-mode

Use the **gprs charging cdr-option apn-selection-mode** command to enable the GGSN to provide the reason code for APN selection in G-CDRs.

The following are the possible APN selection reason codes:

- 0—Mobile station (MS) or network provided, subscription verified
- 1—MS provided, subscription not verified
- 2—Network provided, subscription not verified

local-record-sequence-number

Certain charging data systems use the local record sequence number field in CDRs to associate the partial records generated in the SGSN and GGSN with a particular PDP context. If the charging gateway implements this feature, use the **gprs charging cdr-option local-record-sequence-number** command to enable the feature on the GGSN.

node-id

Certain charging data systems use the node ID field in CDRs to identify the node that generated the CDR. If the charging gateway that your GGSN communicates with uses this feature, use the **gprs charging cdr-option node-id** command to enable the feature.

no-partial-cdr-generation

Use the **gprs charging cdr-option no-partial-cdr-generation all** command when you want all of the fields in the primary G-CDR to be included in any subsequent G-CDRs (partial G-CDRs) for the same PDP context request. By default, partial G-CDRs do not contain the following fields: network initiated PDP context, access point name (network identifier), PDP type, served PDP address, and dynamic address flag.

When you enable the **gprs charging cdr-option no-partial-cdr-generation** command, the GGSN creates any subsequent G-CDRs for the same PDP context request with the same fields in all G-CDRs and maintains sequence numbering.

If an SGSN change limit trigger is not configured when **gprs charging cdr-option no-partial-cdr-generation command** is configured, and a G-CDR is closed as a result of any other trigger (such as tariff times or QoS changes), the GGSN copies the last SGSN (the current SGSN) in the list in the new G-CDR. However, for charging releases prior to Release 4, by default, when the **gprs charging cdr-option no-partial-cdr-generation** command is configured and there is an SGSN change limit trigger configured either using the **gprs charging container sgsn-change-limit** global configuration or the **limit sgsn-change** charging profile configuration command, the CDR will not contain any SGSN address if it closed because of a non-SGSN-change trigger and there is no SGSN change. Therefore, to ensure that all CDR parameters are copied, including the SGSN list, specify the **all** keyword option when issuing the **gprs charging cdr-option no-partial-cdr-generation**.

Note Enable this command only when there are no active PDP contexts. Enabling this feature will affect all subsequent PDP contexts.

packet-count

When you issue the **gprs charging cdr-option packet-count** command, then the GGSN provides a packet count in the optional record extension field for all uplink and downlink packets transferred since the CDR was opened and subsequently closed.

The following object IDs (OIDs) are used in the optional record extension field of the CDR for the uplink and downlink packet counts:

- OID of the uplink packet count—1.3.6.1.4.1.9.10.48.1.2.2.98
- OID of the downlink packet count—1.3.6.1.4.1.9.10.48.1.2.2.99

served-msisdn

Use the **gprs charging cdr-option served-msisdn** command to enable the GGSN to provide the mobile station ISDN (MSISDN) number from the Create PDP Context request in a G-CDR.

To verify the options configured, use the **show gprs charging parameters** command.

Examples

The following example configures the GGSN to exclude the APN parameter in G-CDRs:

```
no gprs charging cdr-option apn
```

Related Commands

Command	Description
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging cg-path-requests

To specify the number of minutes that the gateway GPRS support node (GGSN) waits before trying to establish the TCP path to the charging gateway when TCP is the specified path protocol, use the **gprs charging cg-path-requests** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging cg-path-requests *minutes*

no gprs charging cg-path-requests

Syntax Description

minutes	Number of minutes the GGSN waits before retrying a charging request. The default value is 0 minutes, which disables the timer.

Defaults

0 minutes

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs charging cg-path-requests** command to specify 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.

Examples

The following example specifies that the GGSN waits 5 minutes before trying to establish the TCP path to the charging gateway:

```
gprs charging cg-path-requests 5
```

Related Commands

Command	Description
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging characteristics reject

To configure the gateway GPRS support node (GGSN) to reject GPRS tunneling protocol (GTP) Version 1 (GTP v1) Create PDP Context requests for which no charging profile can be selected, use the **gprs charging characteristics reject** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging characteristics reject

no gprs charging characteristics reject

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled; the GGSN accepts packet data protocol (PDP) context requests for which no charging profile can be selected and applies the global charging defaults.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs charging characteristics reject** command to configure the GGSN to reject Create PDP Context requests for which a charging profile cannot be selected.

The following restrictions apply to charging profiles selected for service-aware PDPs:

- All PDP s belonging to the same user must use the same charging profile as that of the primary PDP.
- The default charging profile, i.e. charging profile 0, is not supported for service-aware PDPs. These PDP create requests will be rejected with error code 199.

To verify whether the charging characteristics reject option is enabled or disabled on the GGSN, use the **show gprs charging parameters** command.

Note This command does not affect GTP Version 0 (GTPv0) Create PDP Context requests.

Examples

The following example configures the GGSN to reject GTP v1 Create PDP Context requests for which no charging profile can be selected:

```
gprs charging characteristics reject
```

Related Commands.

Command	Description
category	Identifies the subscriber category to which a charging profile applies.s
cdr suppression	Specifies that CDRs be suppressed as a charging characteristic in a charging profile.
charging profile	Associates a default charging profile to an access point.
content dcca profile	Defines a DCCA client profile in a GGSN charging profile.
content postpaid time	Specifies as a trigger condition for postpaid users in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
content postpaid validity	Specifies as a trigger condition in a charging profile, the amount of time quota granted to a postpaid user is valid.
content postpaid volume	Specifies as a trigger condition for postpaid users in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
content rulebase	Associates a default rule-base ID with a charging profile.
description	Specifies the name or a brief description of a charging profile.
gprs charging container time-trigger	Specifies a global time limit, that when exceeded by a PDP context causes the GGSN to close and update the G-CDR for that particular PDP context.
gprs charging profile	Creates a new charging profile (or modifies an existing one), and enters charging profile configuration mode.
limit duration	Specifies, as a trigger condition in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
limit sgsn-change	Specifies, as a trigger condition in a charging profile, the maximum number of SGSN changes that can occur before closing and updating the G-CDR for a particular PDP context.
limit volume	Specifies, as a trigger condition in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
tariff-time	Specifies that a charging profile use the global tariff changes configured using the **gprs charging tariff-time** global configuration command.

gprs charging container change-limit

To specify the maximum number of charging containers within each call detail record (CDR) from the gateway GPRS support node (GGSN), use the **gprs charging container change-limit** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging container change-limit *number*

no gprs charging container change-limit *number*

Syntax Description

number	Integer from 1 to 100. The default value is 5.

Defaults

5 containers

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

For each activated packet data protocol (PDP) context on the GGSN, the GGSN creates a G-CDR to collect charging information to be sent to the charging gateway. When certain conditions occur for a PDP context, the GGSN adds information to the CDR or closes the CDR, depending on the trigger condition.

When a CDR is open for a PDP context and the GGSN detects a trigger condition, the GGSN collects the current charging data for that PDP context and appends it to the existing G-CDR in a CDR container.

The following conditions cause the GGSN to create a CDR container and send updates to the charging gateway:

- Quality of service (QoS) change
- Tariff time change
- CDR closure

The following conditions cause the GGSN to create a CDR container and close the G-CDR:

- End of PDP context
- Partial record reason

To control the maximum number of these trigger conditions, and therefore the number of CDR containers in each G-CDR, use the **gprs charging container change-limit** command.

When the number of containers added to a G-CDR reaches the limit specified in the **gprs charging container change-limit** command, the G-CDR is closed and sent as a partial CDR to the charging gateway. If the PDP context remains active, the GGSN opens another G-CDR with a subsequent sequence number associated with that PDP context and its charging data.

Examples

The following example specifies that each CDR includes 25 charging containers:

```
gprs charging change-condition-limit 25
```

Related Commands

Command	Description
gprs charging container volume-threshold	Specifies the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging container sgsn-change-limit

To specify the maximum number of serving GPRS support node (SGSN) changes that can occur before closing and updating a call detail record (CDR) for a particular packet data protocol (PDP) context, use the **gprs charging container sgsn-change-limit** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging container sgsn-change-limit *number*

no gprs charging container sgsn-change-limit *number*

Syntax Description

number	Integer from 0 to 15. The default value is disabled.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD, with the following changes: • The **no** form of the command was added. • The default value changed from 15 to disabled.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

A value of 0 means that a CDR is closed each time that a new SGSN begins handling the PDP context.

The command specifies the number of changes, not the number of SGSNs to be supported. The number of SGSNs supported is equal to 1 more than the change limit. For example, if the SGSN change limit is 2, the maximum number of SGSNs in the list before the gateway GPRS support node (GGSN) closes the G-CDR is 3.

When you enable the **gprs charging cdr-option no-partial-cdr-generation** command, the GGSN creates any subsequent G-CDRs for the same PDP context request with the same fields in all G-CDRs and maintains sequence numbering.

If an SGSN change limit trigger is not configured when **gprs charging cdr-option no-partial-cdr-generation command** is configured, and a G-CDR is closed as a result of any other trigger (such as tariff times or quality of service [QoS] changes), the GGSN copies the last SGSN (the current SGSN) in the list in the new G-CDR. However, for charging releases prior to Release 4, by default, when the **gprs charging cdr-option no-partial-cdr-generation** command is configured and there is an SGSN change limit trigger configured either using the **gprs charging container sgsn-change-limit** global configuration or the **limit sgsn-change** charging profile configuration command, the CDR will not contain any SGSN address if it closed because of a non-SGSN-change trigger and there is no SGSN change. Therefore, to ensure that all CDR parameters are copied, including the SGSN list, specify the **all** keyword option when issuing the **gprs charging cdr-option no-partial-cdr-generation**.

Examples

The following example specifies that a G-CDR closes after five SGSN changes in a list for a particular PDP context. If the PDP context is still active, then a partial CDR is opened:

```
gprs charging container sgsn-change-limit 5
```

gprs charging container time-trigger

To specify a global time limit, that when exceeded by a packet data protocol (PDP) context causes the gateway GPRS support node (GGSN) to close and update the call detail record (CDR) for that particular PDP context, use the **gprs charging container time-trigger** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging container time-trigger *number*

no gprs charging container time-trigger *number*

Syntax Description

number	Number, in minutes from 5 to 4294967295. The default value is 0, which disables the timer.

Defaults

0—Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

If a time-trigger has been specified in a charging profile applied to an access point name (APN), that value will override the value specified globally.

Examples

The following example specifies that a G-CDR closes after a particular PDP context time duration exceeds 5 minutes. If the PDP context is still active, then a partial CDR is opened:

```
gprs charging container time-trigger 5
```

Related Commands

Command	Description
gprs charging container change-limit	Specifies the maximum number of charging containers within each CDR from the GGSN.
gprs charging container sgsn-change-limit	Specifies the maximum number of SGSN changes that can occur before closing a G-CDR for a particular PDP context.

Command	Description
gprs charging container volume-threshold	Specifies the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging container volume-threshold

To specify the maximum number of bytes that the gateway GPRS support node (GGSN) maintains across all containers for a particular packet data protocol (PDP) context before closing and updating the call detail record (CDR), use the **gprs charging container volume-threshold** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging container volume-threshold *threshold-value*

no gprs charging container volume-threshold *threshold-value*

Syntax Description

threshold-value	A value between 1 and 4294967295 that specifies the container threshold value, in bytes. The default is 1,048,576 bytes (1 MB).

Defaults

1,048,576 bytes (1 MB)

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

While a PDP context (mobile session) is active, charging events are generated based on various actions. One way that users can be charged is based on the amount of data transmitted between the PDN and the mobile station. Data volume is recorded in each container of a G-CDR record. Service providers can use this recorded data volume to bill users by volume usage.

Use the **gprs charging container volume-threshold** command to control the maximum amount of data volume that can be reported in each G-CDR from an active PDP context before the G-CDR is eligible for an update to the charging gateway for subsequent billing. The GGSN opens another partial G-CDR for that PDP context while the PDP context remains in session on the GGSN.

For example, a volume threshold setting of 1 MB is configured on the GGSN. The GGSN opens a container in a G-CDR for a new PDP context. A trigger occurs for the PDP context, and at that time the GGSN has registered transmission of 500 KB of data for the PDP context. The trigger causes the GGSN to close the container for the PDP context, which has occurred before the volume limit is reached (500 KB of data transmitted, and 1 MB allowed).

As transmission for the PDP context continues, the GGSN opens a new container in the G-CDR. The GGSN now has up to 500 KB more data that can be processed for that PDP context before reaching the volume threshold limit for the G-CDR. When the volume threshold is reached across all containers for the PDP context (that is, when the sum of all of the byte counts across all containers for the PDP context reaches 1 MB), the GGSN closes the G-CDR with a volume limit cause so that the G-CDR can be sent to the charging gateway. The GGSN opens another partial G-CDR for the PDP context while it remains in session.

Examples

The following example specifies a threshold value of 2097152:

```
gprs charging container volume-threshold 2097152
```

Related Commands

Command	Description
gprs charging container change-limit	Specifies the maximum number of charging containers within each CDR from the GGSN
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging disable

To disable charging transactions on the gateway GPRS support node (GGSN), use the **gprs charging disable** command in global configuration mode. To reenable charging transactions, use the **no** form of this command.

gprs charging disable

no gprs charging disable

Syntax Description

This command has no arguments or keywords.

Defaults

Charging is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs charging disable** command to disable charging. By default, charging processing is enabled on the GGSN.

Before the GGSN can disable charging, any currently open call detail records (CDRs) must be cleared. To clear any open CDRs, use the **clear gprs charging cdr** command. If you disable charging on the GGSN using the **gprs charging disable** command, then you can re-enable charging using the **no gprs charging disable** command.

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 neither being collected by the GGSN nor being sent to the charging gateway. We recommend that you avoid using this command in production network environments. If you must configure this command, use it with extreme care and reserve its usage only for non-production network conditions.

Examples

The following example disables GGSN charging processing:

```
gprs charging disable
```

gprs charging flow-control private-echo

To implement an echo request with private extensions for maintaining flow control on packets transmitted to the charging gateway, use the **gprs charging flow-control private-echo** command in global configuration mode. To disable private extensions for flow control, use the **no** form of this command.

gprs charging flow-control private-echo

no gprs charging flow-control private-echo

Syntax Description

This command has no arguments or keywords.

Defaults

Private flow control is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

If the charging gateway that the gateway GPRS support node (GGSN) communicates with implements a proprietary private extension to the echo signal that maintains flow control, use the **gprs charging flow-control private-echo** command to enable private echo signaling. If your charging gateway does not implement this feature, disable the feature.

Examples

The following example enables an echo request:

```
gprs charging flow-control private-echo
```

Related Commands

Command	Description
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging header short

To enable the gateway GPRS support node (GGSN) to use the GPRS tunneling protocol (GTP) short header (6-byte header), use the **gprs charging header short** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging header short

no gprs charging header short

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled. The GGSN uses the GTP long header.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)YW	This command was introduced.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs charging header short** command to specify for the GGSN to use the GTP short header (6-byte header).

Examples

The following example shows the enabling of the GTP short header:

```
gprs charging header short
```

Related Commands

Command	Description
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging interface source loopback

To configure the GGSN to use a loopback interface for charging messages, use the **gprs charging interface source loopback** command in global configuration mode. To return to the default configuration, use the **no** form of this command.

gprs charging interface source loopback *number*

no gprs charging interface source loopback *number*

Syntax Description

number	Number of the loopback interface to use for charging messages.

Defaults

The global GTP virtual template interface is used for charging messages.

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **gprs charging interface source loopback** command to configure the GGSN to use a loopback interface for charging traffic.

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

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

This feature enables you to separate charging traffic. Optionally, VRF can be configured on the loopback interface, which enables charging traffice to be separated onto a private VLAN.

When configuring a charging source interface, note the following:

- Once configured, the loopback interface cannot not be modified without removing the charging source interface configuration. All charging messages will use the new end points from the path structure.
- A charging source interface cannot be unconfigured while there are active PDPs or CDRs.

Examples

The following example configures the GGSN to use loopback interface 9 for charging traffic:

```
Router(config)# gprs charging interface source loopback 9
```

Related Commands

Command	Description
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging map data tos

To specify an IP type of service (ToS) mapping for gateway GPRS support node (GGSN) charging packets, use the **gprs charging map data tos** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging map data tos *tos-value*

no gprs charging map data tos *tos-value*

Syntax Description

tos-value	Specifies a ToS mapping value between 0 and 5. A higher number indicates a higher service priority. The default value is 3.

Defaults

3

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs charging map data tos** command to specify a value for the ToS precedence bits in the IP header for charging packets transmitted by the GGSN.

Examples

The following example shows ToS mapping value of 5:

```
gprs charging map data tos 5
```

Related Commands

Command	Description
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging message transfer-request command-ie

To specify for the gateway GPRS support node (GGSN) to include the Packet Transfer Command information element (IE) in Data Record Transfer Request messages, use the **gprs charging message transfer-request command-ie** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging message transfer-request command-ie

no gprs charging message transfer-request command-ie

Syntax Description

This command has no arguments or keywords.

Defaults

The GGSN does not include the Packet Transfer Command IE.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)YW	This command was introduced.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs charging message transfer-request command-ie** command to configure the GGSN to include the Packet Transfer Command IE in Data Record Transfer Request messages.

When the **gprs charging message transfer-request command-ie** command is enabled, the Packet Transfer Command IE is included in Data Record Transfer Request messages with the value set to Send Data Record Packet (1), unless the **gprs charging message transfer-request possibly-duplicate** command has been configured.

When the **gprs charging message transfer-request possibly-duplicate** command is configured along with the **gprs charging message transfer-request command-ie** command, if a charging gateway (CG) should fail, when the GGSN switches over to the standby CG, the GGSN will retransmit Data Record Transfer Request message (sent to the previously active CG) and set the value of the Data Record Transfer Request IE to Send Possibly Duplicate Data Record Packet (2).

The GGSN does not support the following values of the Packet Transfer Command IE:

- Cancel Data Record Packet (3)
- Release Data Record Packet (4).

Examples

The following example specifies for the GGSN to include the Packet Transfer Command IE in Data Record Transfer Response messages:

```
gprs charging message transfer-request command-ie
```

Related Commands

Command	Description
gprs charging message transfer-request possibly-duplicate	Specifies for the GGSN to retransmit Data Record Transfer Request messages (sent to a previously active charging gateway) with the value of the Packet Transfer Request IE set to Send Possibly Duplicate Data Record Packet (2).
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging message transfer-request possibly-duplicate

To specify for the gateway GPRS support node (GGSN) to retransmit Data Record Transfer Request messages (sent to a previously active charging gateway) with the value of the Packet Transfer Request information element (IE) set to Send Possibly Duplicate Data Record Packet (2), use the **gprs charging message transfer-request possibly-duplicate** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging message transfer-request possibly-duplicate

no gprs charging message transfer-request possibly duplicate

Syntax Description

This command has no arguments or keywords.

Defaults

The GGSN sets the value of the Packet Transfer Request IE to Send Data Record Packet (1).

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs charging message transfer-request possibly-duplicate** command to configure the GGSN to retransmit Data Record Transfer Request messages to a newly active charging gateway (sent to a previously active charging gateway) with the value of the Packet Transfer Request IE set to Send Possibly Duplicate Data Record Packet (2), use the **gprs charging message transfer-request possibly-duplicate** command.

This command must be used with the **gprs charging message transfer-request command-ie** command. When the **gprs charging message transfer-request command-ie** command is enabled, the Packet Transfer Command IE is included in Data Record Transfer Request messages with the value set to Send Data Record Packet (1), unless the **gprs charging message transfer-request possibly-duplicate** command has been configured.

When the **gprs charging message transfer-request possibly-duplicate** command is configured along with the **gprs charging message transfer-request command-ie** command, if a charging gateway (CG) should fail, when the GGSN switches over to the standby CG, the GGSN will retransmit Data Record Transfer Request messages (sent to the previously active CG) with the value of the Data Record Transfer Request IE set to Send Possibly Duplicate Data Record Packet (2).

The GGSN does not support the following values of the Packet Transfer Command IE:

- Cancel Data Record Packet (3)
- Release Data Record Packet (4).

Examples

The following example specifies for the GGSN to retransmit Data Record Transfer Request messages with the value of the Packet Transfer Request IE set to Send Possibly Duplicate Data Record Packet (2) in the case a charging gateway goes down and a secondary gateway becomes active:

```
gprs charging message transfer-request possibly-duplicate
```

Related Commands

Command	Description
gprs charging message transfer-request command-ie	Specifies for the GGSN to include the Packet Transfer Command IE in the Data Record Transfer Request messages.
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging message transfer-response number-responded

To specify for the gateway GPRS support node (GGSN) to use the Number of Requests Responded field instead of the Length field in the Requests Responded information element (IE) of Data Record Transfer Response messages, use the **gprs charging message transfer-response number-responded** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging message transfer-response number-responded

no gprs charging message transfer-response number-responded

Syntax Description

This command has no arguments or keywords.

Defaults

The GGSN uses the Length field.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)YW	This command was introduced.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs charging message transfer-response number-responded** command to specify for the GGSN to use the Number of Requests Responded field instead of the Length field in the Requests Responded IE of Data Record Transfer Response messages when connecting to a charging gateway that does not support the Length field.

Examples

The following example specifies for the GGSN to use the Number of Requests Responded field:

```
gprs charging message transfer-response number-responded
```

Related Commands

Command	Description
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging packet-queue-size

To specify the maximum number of unacknowledged charging data transfer requests that the gateway GPRS support node (GGSN) maintains in its queue, use the **gprs charging packet-queue-size** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging packet-queue-size *queue-size*

no gprs charging packet-queue-size *queue-size*

Syntax Description

queue-size	Value between 1 and 512 that specifies the maximum queue size for the GGSN charging packet data queue. The default is 128 packets.

Defaults

128 packets

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs charging packet-queue-size** command to specify the maximum size of the GGSN queue of outstanding charging data transfer requests. This queue stores all unacknowledged charging data requests.

When the charging packet queue reaches the specified size, the GGSN stops queuing charging packets until a packet is cleared from the queue and stores new charging packets in memory.

If monitoring of the performance of the charging gateway indicates that it is processing charging packets too slowly, you can increase the size of the charging packet queue. Conversely, if the performance of the charging gateway is fast, you can decrease the size of the charging packet queue.

Examples

The following example specifies a GGSN queue of 512 charging data transfer requests:

```
gprs charging packet-queue-size 512
```

Related Commands

Command	Description
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging path-protocol

To specify the protocol that the gateway GPRS support node (GGSN) uses to transmit and receive charging data, use the **gprs charging path-protocol** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging path-protocol {**udp** | **tcp**}

no gprs charging path-protocol {**udp** | **tcp**}

Syntax Description

udp	User Datagram Protocol (UDP), which is a connectionless transport protocol.
tcp	Transport Control Protocol (TCP), which is a connection-based transport protocol.

Defaults

UDP

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs charging path-protocol** command to specify the protocol used by the GGSN to transfer charging data.

Examples

The following example shows use of UDP:

```
gprs charging path-protocol udp
```

Related Commands

Command	Description
gprs charging cg-path-requests	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.
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging port

To configure the destination port of the charging gateway, use the **gprs charging port** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging port *port-num*

no gprs charging port *port-num*

Syntax Description

port-num	Integer from 1024 to 10000. The default port is 3386.

Defaults

Port 3386

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Examples

The following example changes the default port of 3386 to 1055:

```
gprs charging port 1055
```

Related Commands

Command	Description
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging profile

To create a new charging profile (or modify an existing one), and enter charging profile configuration mode, use the **gprs charging profile** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging profile *profile-number*

no gprs charging profile *profile-number*

Syntax Description

profile-number	Number of the charging profile. Valid values are 1 to 255.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ and the valid range of configurable profiles changed to 1 to 255.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs charging profile** global configuration command to create charging profiles. Charging profiles define the charging method to apply to a specific type of user (home, roamer, visitor), enabling you to apply a charging method on a per-packet data protocol (PDP) context basis.

The GGSN supports up to 256 charging profiles (numbered 0 to 255). Charging profiles define the charging method for a PDP context.

Profile 0 is a set profile that always exists and is not created by the user. However, it can be modified using the charging-related global configuration commands. Profiles 1 to 255 can be defined by the user and customized using the charging profile configuration commands. You can apply these charging profiles at the access point name (APN) and global level as the default charging method for a specific user type.

When using charging profiles, please note the following:

- The GGSN must be configured to include the charging characteristics selection mode parameter in CDRs using the **gprs charging cdr-option chch-selection-mode** global configuration command.
- The GGSN must be configured to receive the charging characteristics selection mode IE in CDRs using the **gprs charging release** global configuration command.

The following types of charging characteristics and trigger conditions can be configured in a charging profile:

- Subscriber category (using the **category** command)
- CDR suppression (using the **cdr-suppression** command)
- Volume limit (using the **limit volume** command)
- Duration limit (using the **limit duration** command)
- Tariff time (using the **tariff-time** command)
- SGSN change limit (using the **limit sgsn-change** command)

When a Create PDP Context request is received, the charging profile is selected based on the following sources of input:

- Serving GPRS support node (SGSN)/home location register (HLR) via the charging characteristics information element (IE).
- Local defaults.
- Charging profile index authentication, authorization, and accounting (AAA) attribute.

Note The charging profile index received from AAA will take effect only if service-awareness has been configured globally on the GGSN (using the **gprs service-aware** global configuration command), and at the APN level (using the **service-aware** access-point configuration command).

For information on configuring a service-aware GGSN, see the "Configuring Enhanced Service-Aware Billing" chapter of the Cisco GGSN Configuration Guide.

The order in which a charging profile is selected for a PDP context, is as follows:

1. Charging profile index in the override rule on the APN—If a default charging profile has been configured at both the APN and global level to override the SGSN specification, the APN default charging profile is used first.
2. Charging profile index in the override rule on the box (global default charging profile)—If there is no default charging profile default configured at the APN, the default charging profile configured globally is use.
3. Charging profile index from AAA.
4. Charging profile index from SGSN/HLR
5. Charging profile index from the non-override rule on the APN.
6. Charging profile index from non-override rule on the box (global default charging profile).

If none of the above applies, the PDP context is rejected if the **gprs charging characteristics reject** global configuration command is configured and the Create PDP Context request is GTP v1. If the **gprs charging characteristics reject** command is not configured, the GTPv1 PDP context is created using charging profile 0.

Note The default charging profile, i.e. charging profile 0, is not supported for service-aware PDPs. These Create PDP Context requests will be rejected with error code 199.

Examples

The following example creates charging profile number 10 and enters charging profile configuration mode:

```
gprs charging profile 10
```

Related Commands.

Command	Description
category	Identifies the subscriber category to which a charging profile applies.s
cdr suppression	Specifies that CDRs be suppressed as a charging characteristic in a charging profile.
charging profile	Associates a default charging profile to an access point.
content dcca profile	Defines a DCCA client profile in a GGSN charging profile.
content postpaid time	Specifies as a trigger condition for postpaid users in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
content postpaid validity	Specifies as a trigger condition in a charging profile, the amount of time quota granted to a postpaid user is valid.
content postpaid volume	Specifies as a trigger condition for postpaid users in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
content rulebase	Associates a default rule-base ID with a charging profile.
description	Specifies the name or a brief description of a charging profile.
gprs charging characteristics reject	Configures the GGSN to reject Create PDP Context requests for which no charging profile can be selected.
gprs charging container time-trigger	Specifies a global time limit, that when exceeded by a PDP context causes the GGSN to close and update the G-CDR for that particular PDP context.
limit duration	Specifies, as a trigger condition in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
limit sgsn-change	Specifies, as a trigger condition in a charging profile, the maximum number of SGSN changes that can occur before closing and updating the G-CDR for a particular PDP context.
limit volume	Specifies, as a trigger condition in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
tariff-time	Specifies that a charging profile use the tariff changes configured using the **gprs charging tariff-time** global configuration command.

gprs charging profile default

To specify a global default charging profile to be used if no charging profile is specified at the access point name (APN), use the **gprs charging profile default** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging profile default {home | roaming | visiting | any} [trusted] *profile-number* **[override]**

no gprs charging profile default {home | roaming | visiting | any} *profile-number* **[trusted]** *profile-number* **[override]**

Syntax Description

home	Specifies that the charging profile applies to home mobile subscribers.
roaming	Specifies that the charging profile applies to roaming mobile subscribers (subscribers whose serving GPRS support node (SGSN) public land mobile network (PLMN) ID differs from the gateway GPRS support node's (GGSN's).
visiting	Specifies that the charging profile applies to visiting mobile subscribers (subscribers whose internation mobile subscriber identity [IMSI] contains a foreign PLMN ID).
any	Specifies that the charging profile will apply to all types of users.
trusted	(Optional) Specifies that the charging profile applies if the user is a visiting or roaming user (depending on whether **roaming** or **visiting** has been specified) whose PLMN ID is a trusted one (as configured using the **gprs mcc mnc** command).
profile-number	Number of the charging profile that is being defined as the default for a selection method. Valid values are 0 to 15. If 0 is specified, charging behavior is defined by global charging characteristics (those not defined in a charging profile).
override	(Optional) Specifies that the charging characteristic value received from the SGSN in the Create packet data protocol (PDP) Context request be ignored and the APN default used instead.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs charging profile default** global configuration command to define a global default charging profile for a specific type of users to be used when no default is configured at the APN.

For complete information on configuring and using charging profiles, and the order in which charging profiles are selected for a PDP context, see the "Configuring Charging Profiles" section of the "Configuring Charging on the GGSN" chapter of the *Cisco GGSN Configuration Guide*.

Examples

The following example specifies charging profile number 10 to be the global default for home users:

```
gprs charging profile default 10 home
```

Related Commands.

Command	Description
category	Identifies the subscriber category to which a charging profile applies.
cdr suppression	Specifies that CDRs be suppressed as a charging characteristic in a charging profile.
charging profile	Associates a default charging profile to an access point.
description	Specifies the name or a brief description of a charging profile.
gprs charging characteristics reject	Configures the GGSN to reject Create PDP Context requests for which no charging profile can be selected.
gprs charging container time-trigger	Specifies a global time limit, that when exceeded by a PDP context causes the GGSN to close and update the G-CDR for that particular PDP context.
gprs charging profile	Creates a new charging profile (or modifies an existing one), and enters charging profile configuration mode.
limit duration	Specifies, as a trigger condition in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
limit sgsn-change	Specifies, as a trigger condition in a charging profile, the maximum number of SGSN changes that can occur before closing and updating the G-CDR for a particular PDP context.
limit volume	Specifies, as a trigger condition in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
tariff-time	Specifies that a charging profile use the tariff changes configured using the **gprs charging tariff-time** global configuration command.

gprs charging reconnect

To configure the gateway GPRS support node (GGSN) to periodically attempt to reconnect to an unreachable charging gateway (CG) in order to determine when the link is back up, use the **gprs charging reconnect** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging reconnect *minutes*

no gprs charging reconnect

Syntax Description

minutes	Number of minutes the GGSN waits between attempts to reconnect to a charging gateway. The valid range is 1 to 600 minutes.

Defaults

1 minute.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Configuring the GGSN to automatically attempt to reconnect to an unreachable CG is necessary only when User Datagram Protocol(UDP) is used as the charging transport protocol and the charging gateway does not support echo requests.

Examples

The following example configures the GGSN to try to reconnect to a charging gateway every 5 minutes:

```
gprs charging reconnect 5
```

Related Commands

Command	Description
gprs charging path-protocol	Specifies the transport path protocol to be used by the GGSN to transmit and receive charging data.
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging release

To configure the charging release with which the gateway GPRS support node (GGSN) is to comply when presenting call detail records (CDRs), use the **gprs charging release** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging release {**99** | **98** | **4** | **5**}

no gprs charging release {**99** | **98** | **4** | **5**}

Syntax Description

99	Specifies for the GGSN to present R97/R98 and R99 quality of service (QoS) profile formats in G-CDRs.
98	Specifies for the GGSN to present only R97/R98 QoS profile formats in G-CDRs.
4	Specifies for the GGSN to comply with 3GPP TS 32.215 Release 4.
5	Specifies for the GGSN to comply with 3GPP TS 32.215 Release 5.

Defaults

99

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)YW	This command was introduced.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU and the **4** and **5** keyword options were added.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

When **99** is configured, the Charging Characteristics parameter is included in G-CDRs. When **4** and **5** are configured, the Charging Characteristics Selection Mode information element (IE) is included.

To verify charging release configuration, use the **show gprs charging parameters** command.

Examples

The following example enables the GGSN to present both R97/R98 QoS profile formats and R99 QoS profile formats in G-CDRs:

```
gprs charging release 99
```

Related Commands

Command	Description
gprs charging cdr-option	Configures the GGSN to include or not include certain parameters in G-CDRs
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging roamers

To enable charging for roamers on the gateway GPRS support node (GGSN), use the **gprs charging roamers** command in global configuration mode. To disable charging for roamers on the GGSN, use the **no** form of this command.

gprs charging roamers

no gprs charging roamers

Syntax Description

This command has no arguments or keywords.

Defaults

Charging for roamers is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs charging roamers** command to enable support on the GGSN for the creation of call detail records (CDRs) for roaming mobile subscribers.

Note Before enabling the creation of CDRs for roaming mobile subscribers, an public land mobile network (PLMN) IP address range (or list of address ranges) must first be configured using the **gprs plmn ip address** command with the **sgsn** keyword option specified.

When the charging for roamers feature is enabled on the GGSN, when the GGSN receives a packet data protocol (PDP) context request, it first checks to see if both the GGSN and serving GPRS support node (SGSN) PLMN IDs are present and match (via the Routing Area Information field [RAI] information element [IE]).

If both IDs are not present or do not match, the GGSN matches the IE containing the serving GPRS support node (SGSN) Signaling Address field against a list of PLMN IP address ranges that have been defined using the **gprs plmn ip address** command with the **sgsn** keyword option specified.

Note To use the RAI IE in Create PDP Context requests to detect roamers, a valid home PLMN must be configured on the GGSN using the **gprs mcc mn** global configuration command. When a valid home PLMN is configured, or valid trusted PLMNs, a CDR will not be generated if the RAI matches the configured home (or trusted) PLMN. A CDR will be created for all PDPs with RAIs that do not match a home or trusted PLMN.

Note If the RAI field is not present in a Create PDP Context, and an address range has not been configured using the **gprs plmn ip address** command with the **sgsn** keyword option specified, the PDP will be classified as "unknown" and treated as a roamer.

If the GGSN determines that the SGSN that sent the Create PDP Context request is not located within the same PLMN in which the GGSN is located, the GGSN generates a CDR. If the GGSN determines that the SGSN is located in the same PLMN, it will not generate a CDR until it receives notification that the SGSN has changed to that of one located in another PLMN.

How the charging for roamers feature functions when the GGSN determines that a Create PDP Context request is that of a roamer by matching the PDP context request IE containing the SGSN Signaling address fields against a list of PLMN IP addresses depends on how the PLMN IP address ranges have been defined using the **gprs plmn ip address** command with the **sgsn** keyword option specified.

- If no PLMN IP address ranges are configured using the **gprs plmn ip address** *start_ip end_ip* [**sgsn**] command, the GGSN generates CDRs for all initiated PDP contexts regardless of whether the GGSN and SGSN are located within the same PLMN.
- If a list of PLMN IP address ranges has been configured using the **gprs plmn ip address** *start_ip end_ip* [**sgsn**] command, and one or more of those ranges has been defined using the **sgsn** keyword, the GGSN uses those ranges defined with the **sgsn** keyword to determine whether an SGSN is located within the same PLMN.

  With this configuration, the following scenarios outline how the charging for roamers feature will function:

  – Mobile station 1 (MS1) is subscribed to PLMN1 and attaches to an SGSN in PLMN2. From PLMN2, MS1 initiates a PDP context with the GGSN in PLMN1. In this case, MS1 is a roamer, and the GGSN generates a CDR because it determines that the SGSN is located in a different PLMN.

  – MS1 is subscribed to PLMN1 and attaches to an SGSN in PLMN2. From PLMN2, MS1 initiates a PDP context with the GGSN in PLMN2. In this case, MS1 is not a roamer because the SGSN and GGSN are in the same PLMN. The GGSN does not create a G-CDR.

Configuration Guidelines

To enable charging for roamers on the GGSN, you should first define a set of IP address ranges for a PLMN using the **gprs plmn ip address** command.

It is important that you configure the **gprs plmn ip address** and **gprs charging roamers** commands in their proper order. After you configure the IP address range for a PLMN, use the **gprs charging roamers** command to enable charging for roamers on the GGSN. You can change the IP address range by reissuing the **gprs plmn ip address** command.

To verify your configuration, use the **show gprs charging parameters** command to see if the charging for roamers feature is enabled. To verify your PLMN IP address ranges, use the **show gprs plmn ip address** command.

Examples

The following example enables the charging for roamers feature on the GGSN:

```
gprs charging roamers
```

Related Commands

Command	Description
gprs plmn ip address	Defines the IP address range for a PLMN that the GGSN uses to determine whether a Create PDP Context request is from a roamer.
show gprs charging parameters	Displays information about the current GGSN charging configuration.
show gprs plmn ip address	Displays a list of defined PLMN IP address ranges.

gprs charging send-buffer

To configure the size of the buffer that contains the GPRS tunneling protocol (GTP) packet data unit (PDU) and signaling messages on the gateway GPRS support node (GGSN), use the **gprs charging send-buffer** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging send-buffer *bytes*

no gprs charging send-buffer *bytes*

Syntax Description

bytes	Integer from 300 to 1460. The default value is 1460 bytes.

Defaults

1460 bytes

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Examples

The following example specifies a buffer size of 512 bytes:

```
gprs charging send-buffer 512
```

Related Commands

Command	Description
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging server-switch-timer

To specify a timeout value that determines when the gateway GPRS support node (GGSN) attempts to find an alternate charging gateway after a destination charging gateway cannot be located or becomes unusable, use the **gprs charging server-switch-timer** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging server-switch-timer *seconds*

no gprs charging server-switch-timer *seconds*

Syntax Description

seconds	Timeout value (between 0 and 300 seconds), that the GGSN waits before attempting to contact an alternate charging gateway. The default value is 60 seconds.

Defaults

60 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs charging server-switch-timer** command to specify a timeout value that determines when the GGSN contacts an alternate charging gateway after the current charging gateway becomes unusable or cannot be located.

To specify immediate switchover to an alternate charging gateway, specify a value of 0.

Examples

The following example configures a timeout value of 30 seconds:

```
gprs charging server-switch-timer 30
```

Related Commands

Command	Description
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging service-mode

To configure the service-mode state of the charging function of a gateway GPRS support node (GGSN), use the **gprs charging service-mode** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging service-mode {operational | maintenance}

no gprs charging service-mode {operational | maintenance}

Syntax Description

operational	Specifies that the charging service-mode state of the GGSN is operational.
maintenance	Specifies that the charging service-mode state of the GGSN is maintenance.

Defaults

Operational

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs charging service-mode** command to place the charging function of a GGSN in maintenance mode. When the charging function is in maintenance mode, you can add, delete, or modify charging gateways (CGs). For example, you can change the IP addresses of charging gateways (CGs), their priority, and the number of CGs.

When the charging function is in maintenance mode, call detail records (CDRs) are not transmitted to CGs. However, the collection of CDRs is not affected. Once the service-mode state of the charging function has been returned to operational, any pending messages are sent to the newly configured CG and the charging function operates normally. If all CGs were deleted while the GGSN was in charging maintenance mode, CDRs and messages in the pending queue are stored in the GGSN.

Note When the charging function is in maintenance mode, CDRs stored on the GGSN, including those in the pending queue, can be manually cleared using the **clear gprs charging cdr all no-transfer** command.

Examples

The following example places the charging function of a GGSN in maintenance mode:

```
gprs charging service-mode maintenance
```

Related Commands

Command	Description
clear gprs charging cdr all no-transfer	Clears stored CDRs, including those in the pending queue, when a GGSN is in charging maintenance mode.
gprs service-mode	Configures the service-mode state of a GGSN.
service-mode	Configures the service-mode state of an APN.
gprs service-mode test imsi	Configures a test user for which you can Create PDP Contexts to test an APN configuration.
show gprs service-mode	Displays the current global service mode state of the GGSN and the last time it was changed.

gprs charging service-record include

To configure the GGSN to include the public land mobile network (PLMN) ID and radio access technology (RAT) fields in the Service Record information element (IE), use the **gprs charging service-record include** command in global configuration mode. To return to the default value, use the **no** form of the command

gprs charging service-record include [**rat** | **plmn-id**]

no gprs charging service-record include [**rat** | **plmn-id**]

Syntax Description

rat	Configures the GGSN to include the PLMN field in the Service Record IE. The RAT indicates whether the SGSN serves the user equipment (UE) UMTS or GSM/EDGE RAN (GERAN).
plmn-id	Configures the GGSN to include the RAT field in the Service Record IE.

Defaults

The PLMN ID and RAT fields are not included.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)XG	This command was introduced.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

The **gprs charging service-record include** command controls whether or not the GGSN includes the RAT or PLMN-ID in the Service Record IE.

If RAT and/or PLMN ID triggers are configured in the charging profile (using the **content postpaid** charging profile configuration command), the GGSN must be configured to include the related field in the Service Record IE by using the **gprs charging service-record include** command. If the **gprs charging service-record include** command has not been configured,then even if the triggers are configured, they are not activated and are ignored for service-aware PDPs (no quota reauthorization will occur when the trigger values change).

Examples

The following example configures the GGSN to include the RAT field in the Service Record IE:

```
Router(config)# gprs charging service-record include rat
```

Related Commands

Command	Description
content postpaid	Configures a type of condition in the charging profile used for postpaid users, that when the condition occurs, triggers the GGSN to request quota reauthorization for a PDP context.
trigger	Specifies a type of change that, when it occurs, triggers the GGSN (functioning as a DCCA client) to request quota-reauthorization and generate an eG-CDR for a service-aware prepaid PDP context.

gprs charging switchover priority

To configure the gateway GPRS support node (GGSN) to switch over to the gateway of higher priority when that gateway becomes active, use the **gprs charging switchover priority** command in global configuration mode.

gprs charging switchover priority

no gprs charging switchover priority

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

When configured for priority switchover using the **gprs charging switchover priority** charging gateway configuration command, regardless of the state of the current active charging gateway, when a higher priority gateway comes up, the GGSN will switch over and send call detail records (CDRs) to that gateway.

Examples

The following enables switch over to a higher priority charging gateway when that gateway becomes active:

```
gprs charging switchover priority
```

Related Commands

Command	Description
gprs default charging-gateway	Specifies the default charging gateways, in the order of their priority (primary, secondary, and tertiary).
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs charging tariff-time

To specify a time of day when gateway GPRS support node (GGSN) charging tariffs change, use the **gprs charging tariff-time** command in global configuration mode. To remove an existing tariff time, use the **no** form of this command.

gprs charging tariff-time *time*

no gprs charging tariff-time *time*

Syntax Description

time	A time of day when the charging tariff changes. Specify the time format as hh:mm:ss.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs charging tariff-time** command to specify when the charging tariff for using GPRS/UMTS will change. When the tariff time changes, a container is attached to the call detail record (CDR) for the user.

You can set up a maximum of 32 tariff change times.

Note If the system software clock is manually set using the the **clock set** privileged EXEC command at the supervisor console prompt, the time a tariff change will occur must be be reconfigured.

Examples

The following example specifies 14:30:00 as the time when the charging tariff changes:

```
gprs charging tariff-time 14:30:00
```

Related Commands

Command	Description
show gprs charging parameters	Displays information about the current GGSN charging configuration.
tariff-time	Specifies that a charging profile use the tariff changes configured using the **gprs charging tariff-time** global configuration command.

gprs charging transfer interval

To specify the number of seconds that the gateway GPRS support node (GGSN) waits before it transfers charging data to the charging gateway, use the **gprs charging transfer interval** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs charging transfer interval *seconds*

no gprs charging transfer interval *seconds*

Syntax Description

seconds	Interval between charging transfers, in seconds. Can be a value between 1 and 4294967295 seconds. The default is 105 seconds.

Defaults

105 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)B	This command was integrated into Cisco IOS Release 12.2(8)B.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs charging transfer interval** command to specify how often the GGSN transfers charging data for a given packet data protocol (PDP) context (mobile session) to a charging gateway.

Examples

The following example specifies an interval of 512 seconds:

```
gprs charging transfer interval 512
```

Related Commands

Command	Description
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs compliance 3gpp ggsn r4.0

To change the gateway GPRS support node (GGSN) compliance baseline in GGSN 5.0 (TSG#18) to that of GGSN 4.0 (TSG#16), use the **gprs compliance 3gpp ggsn r4.0** command in global configuration mode. To return the compliance baseline to TSG#18, use the **no** form of this command.

gprs compliance 3gpp ggsn r4.0

no gprs compliance 3gpp ggsn r4.0

Syntax Description

This command has no arguments or keywords.

Defaults

GGSN 5.0 compliance baseline (TSG#18)

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs compliance 3gpp ggsn r4.0** global configuration command to change the compliance baseline from TSG#18 to that of GGSN 4.0 (TSG#16).

The 3rd Generation Partnership Project (3GPP) compliance baseline for GGSN 5.0 is as follows:

- R98—Same as in GGSN Release 4.0.
- R99—Upgraded to TSG #18.
- R4—New support with compliance baseline up to TSG #18

By default, the 3GPP compliance baseline is TSG #18. However, it can be shifted to that of GGSN 4.0 (TSG #16) using the **gprs compliance 3gpp ggsn r4.0** global configuration command.

Examples

The following example changes the compliance baseline to that in GGSN Release 4.0 (TSG#16):

```
GGSN(conf)# gprs compliance 3gpp ggsn r4.0
```

gprs dcca profile

To enable the Diameter credit control application (DCCA) client process on the gateway GPRS support node (GGSN) and enter DCCA profile configuration mode, use the **gprs dcca profile** command in global configuration mode. To remove a DCCA client configuration, use the **no** form of this command

gprs dcca profile *profile-name*

no gprs dcca profile *profile-name*

Syntax Description

profile-name	Name of the DCCA client profile.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs dcca profile** command to enable the DCCA client process on the GGSN and enter DCCA profile configuration mode.

The GGSN functions as a DCCA client when interacting with a DCCA server to request and obtain quota. As a DCCA client, the GGSN sends Credit Control requests (CCR) to and receives Credit Control responses (CCR) from a DCCA server.

To complete the DCCA client configuration, while in DCCA client profile configuration mode, you must also complete the following tasks:

- Define a method list used to specify the Diameter authentication, authorization, and accounting (AAA) groups using the **authorization** DCCA profile configuration command.
- Configure a transmission timer to monitor the communication of CCRs with a Diameter server using the **tx-timeout** DCCA profile configuration command.
- Configure a default for the Credit Control Failure Handling (CCFH) attribute-value pair (AVP) using the **ccfh** DCCA profile configuration command.
- Specify whether session failover is supported using the **session-failover** DCCA profile configuration command.
- Configure the destination realm to be sent in CCR initial requests to the DCCA server using the **destination-realm** DCCA profile configuration command.
- Specify whether serving GPRS support node (SGSN) or quality of service (QoS) changes trigger quota-reauthorization using the **trigger** DCCA profile configuration command.

Examples

The following configuration example configures a DCCA client profile with the name dcca-profile1:

```
gprs dcca profile dcca-profile1
```

Related Commands

Command	Description
authorization	Defines a method of authorization (AAA method list), in the DCCA client profile, that specifies the Diameter server groups.
ccfh	Configures the Credit Control Failure Handling (CCFH) AVP locally to use for a credit-control session when the Credit Control Answer (CCA) sent by the DCCA server does not contain CCFH value.
content dcca profile	Defines the DCCA client profile in a GGSN charging profile.
destination-realm	Configures the destination realm to be sent in CCR initial requests to a DCCA server.
session-failover	Configures Credit Control Session Failover (CCSF) AVP support when a credit control answer (CCA) message from the DCCA server does not contain a value for the CCSF AVP.
trigger	Specifies that SGSN and QoS changes will trigger a DCCA client to request quota-reauthorization
tx-timeout	Configures a TX timeout value used by the DCCA client to monitor the communication of Credit Control Requests (CCRs) with a Diameter server.

gprs default aaa-accounting

To configure a global default periodic accounting interval, use the **gprs default aaa-accounting interim periodic** command in global configuration mode. To return to the default, use the **no** form of this command

gprs default aaa-accounting interim periodic *minutes*

no gprs default aaa-accounting interim periodic *minutes*

Syntax Description

minutes	Amount of time, in minutes, at which to send periodic accounting records. Valid values are 15 to 71582.

Defaults

There is no periodic timer configured globally. The APN-level periodic interval is used, if configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **gprs default aaa-accounting interim periodic** command to configure a global default periodic accounting interval that can be used for all APNs, eliminating the need to configure a periodic accounting interval for each APN.

Examples

The following configuration example configures a global default periodic timer:

```
gprs default aaa-accounting interim periodic 60
```

Related Commands

Command	Description
aaa-accounting interim periodic	Enables interim periodic accounting records to be sent to an accounting server on regular configured intervals.

gprs default aaa-group

To specify a default authentication, authorization, and accounting (AAA) server group and assign the type of AAA services to be supported by the server group for all access points on the gateway GPRS support node (GGSN), use the **gprs default aaa-group** command in global configuration mode. To remove the default AAA server group, use the **no** form of this command.

gprs default aaa-group {**authentication** | **accounting**} *server-group*

no gprs default aaa-group {**authentication** | **accounting**} *server-group*

Syntax Description

authentication	Assigns the selected server group for authentication services on all access point names (APNs).
accounting	Assigns the selected server group for accounting services on all APNs.
server-group	Specifies the name of an AAA server group to be used for AAA services on all APNs. **Note** The name of the AAA server group that you specify must correspond to a server group that you configure using the **aaa group server** command.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The Cisco Systems GGSN supports authentication and accounting at APNs using AAA server groups. By using AAA server groups, you gain the following benefits:

- You can selectively implement groups of servers for authentication and accounting at different APNs.
- You can configure different server groups for authentication services and accounting services in the same APN.
- You can control which RADIUS services you want to enable at a particular APN, such as AAA accounting.

The GGSN supports the implementation of AAA server groups at both the global and access-point configuration levels. You can minimize your configuration by specifying the configuration that you want to support across most APNs, at the global configuration level. Then, at the access-point configuration level, you can selectively modify the services and server groups that you want to support at a particular APN. Therefore, you can override the AAA server global configuration at the APN configuration level.

To configure a default AAA server group to be used for all APNs on the GGSN, use the **gprs default aaa-group** global configuration command. To specify a different AAA server group to be used at a particular APN for authentication or accounting, use the **aaa-group** access-point configuration command.

If accounting is enabled on the APN, then the GGSN looks for an accounting server group at the APN or globally in the following order:

- First, at the APN for an accounting server group—configured in the **aaa-group accounting** command.
- Second, for a global GPRS default accounting server group—configured in the **gprs default aaa-group accounting** command.
- Third, at the APN for an authentication server group—configured in the **aaa-group authentication** command.
- Last, for a global GPRS default authentication server group—configured in the **gprs default aaa-group authentication** command.

If authentication is enabled on the APN, then the GGSN first looks for an authentication server group at the APN. If an authentication server group is not found at the APN, then the GGSN looks for a globally configured, GPRS default authentication server group.

To complete the configuration, you must specify the following configuration elements on the GGSN:

- Configure the RADIUS servers, using the **radius-server host** command.
- Define a server group with the IP addresses of the AAA servers in that group, using the **aaa group server** global configuration command.
- Enable the type of AAA services (accounting and authentication) to be supported on the APN.
  - The GGSN enables accounting by default for non-transparent APNs.

    You can disable accounting services at the APN by using the **aaa-accounting disable** command.
  - You can enable authentication at the APN level by configuring the **access-mode non-transparent** command. When you enable authentication, the GGSN automatically enables accounting on the APN. There is not a global configuration command to enable or disable authentication.
- Configure AAA accounting and authentication using the **aaa accounting** and **aaa authentication** global configuration commands.

Note For more information about AAA and RADIUS global configuration commands, refer to the *Cisco IOS Security Command Reference*.

Examples

The following configuration example defines four AAA server groups on the GGSN: foo, foo1, foo2, and foo3, shown by the **aaa group server** commands.

Using the **gprs default aaa-group** command, two of these server groups are globally defined as default server groups: foo2 for authentication, and foo3 for accounting.

At access point 1, which is enabled for authentication, the default global authentication server group of foo2 is overridden, and the server group named foo is designated to provide authentication services on the APN. Notice that accounting services are not explicitly configured at that access point, but are automatically enabled because authentication is enabled. Because there is a globally defined accounting server group defined, the server named foo3 will be used for accounting services.

At access point 4, which is enabled for accounting using the **aaa-accounting enable** command, the default accounting server group of foo3 is overridden, and the server group named foo1 is designated to provide accounting services on the APN.

Access point 5 does not support any AAA services because it is configured for transparent access mode.

```
aaa new-model
!
aaa group server radius foo
 server 10.2.3.4
 server 10.6.7.8
aaa group server radius foo1
 server 10.10.0.1
aaa group server radius foo2
 server 10.2.3.4
 server 10.10.0.1
aaa group server foo3
 server 10.6.7.8
 server 10.10.0.1
!
aaa authentication ppp foo group foo
aaa authentication ppp foo2 group foo2
aaa authorization network default group radius
aaa accounting exec default start-stop group foo
aaa accounting network foo1 start-stop group foo1
aaa accounting network foo2 start-stop group foo2
aaa accounting network foo3 start-stop group foo3
!
gprs access-point-list gprs
 access-point 1
  access-mode non-transparent
  access-point-name www.pdn1.com
  aaa-group authentication foo
!
 access-point 4
  access-mode transparent
  access-point-name www.pdn2.com
  aaa-accounting enable
  aaa-group accounting foo1
!
 access-point 5
  access-mode transparent
  access-point-name www.pdn3.com
!
```

```
gprs default aaa-group authentication foo2
gprs default aaa-group accounting foo3
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.10.0.1 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authorization	Sets parameters that restrict user access to a network.
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa-accounting	Enables or disables accounting for a particular access point on the GGSN.
aaa-group	Specifies a RADIUS server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN.
radius-server host	Specifies a RADIUS server host.

gprs default aggregate

To configure the gateway GPRS support node (GGSN) to create an aggregate route in its IP routing table when receiving packet data protocol (PDP) requests from mobile stations (MSs) on the specified network for any access point on the GGSN, use the **gprs default aggregate** command in global configuration mode. To remove a global aggregate route, use the **no** form of this command.

gprs default aggregate *ip-network-prefix* {*/mask-bit-length* | *ip-mask*}

no gprs default aggregate *ip-network-prefix* {*/mask-bit-length* | *ip-mask*}

Syntax Description

ip-network-prefix	Dotted decimal notation of the IP network address to be used by the GGSN for route aggregation, in the format *a.b.c.d*.
/mask-bit-length	Number of bits (as an integer) that represent the network portion of the specified IP network address. A forward slash is required before the integer. **Note** There is no space between the *ip-network-prefix* and the slash (/).
ip-mask	Dotted decimal notation of the IP network mask (in the format *e.f.g.h.*), which represents the network and host portion of the specified IP network address.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The GGSN uses a static host route to forward user data packets received from the Gi interface to the Gn interface, using the virtual template interface of the GPRS tunneling protocol (GTP) tunnel.

Without the **gprs default aggregate** command or **aggregate** command, the GGSN creates a static host route for each PDP request. For example, for 45,000 PDP contexts supported, the GGSN creates 45,000 static host routes in its IP routing table.

You can use the **gprs default aggregate** command to reduce the number of static routes implemented by the GGSN for PDP requests at all access points on the GGSN. The **gprs default aggregate** command allows you to specify an IP network prefix to combine the routes of PDP requests from the same network as a single route on the GGSN.

If you use the **gprs default aggregate** command to globally define an aggregate IP network address range for all access points on the GGSN, you can use the **aggregate** command to override this default address range at a particular access point. Automatic route aggregation can be configured at the access-point configuration level only on the GGSN. The **gprs default aggregate** command does not support the **auto** option; therefore, you cannot configure automatic route aggregation globally on the GGSN.

When route aggregation is configured as in the following scenarios, the GGSN manages routes for MSs through an access point as follows:

- No aggregation is configured on the GGSN, at the APN or globally—The GGSN inserts the 32-bit host route of the MS into its routing table as a static route.
- A default aggregate route is configured globally, but no aggregation is configured at the APN:
  - If a statically or dynamically derived address for an MS matches the default aggregate route range, the GGSN inserts an aggregate route into its routing table.
  - If the MS address does not match the default aggregate route, the GGSN inserts the 32-bit host route as a static route into the routing table.
- A default aggregate route is configured globally, and automatic route aggregation is configured at the APN:
  - If a statically derived address for an MS matches the default aggregate route range, the GGSN inserts an aggregate route into its routing table.
  - If a statically derived address for an MS does not match the default aggregate route, the GGSN inserts the 32-bit host route as a static route into its routing table.
  - If a dynamically derived address for an MS is received, the GGSN aggregates the route-based on the address and mask returned by the DHCP or RADIUS server.
- A default aggregate route is configured globally, and an aggregate route is also configured at the APN:
  - If a statically or dynamically derived address for an MS matches the aggregate range at the APN through which it was processed, or otherwise matches the default aggregate range, the GGSN inserts an aggregate route into its routing table.
  - If a statically or dynamically derived address for an MS does not match either the aggregate range at the APN or the global default aggregate range, the GGSN inserts the 32-bit host route as a static route into its routing table.

Use care when assigning IP addresses to an MS before you configure the aggregation ranges on the GGSN. A basic guideline is to aggregate as many addresses as possible, but to minimize your use of aggregation with respect to the total amount of IP address space being used by the access point.

Note The **aggregate** command and **gprs default aggregate** commands affect routing on the GGSN. Use care when planning and configuring IP address aggregation.

Examples

The following example shows a route aggregation configuration for access point 8 using DHCP on the GGSN, along with the associated output from the **show gprs gtp pdp-context all** command and the **show ip route** commands.

Notice that the **aggregate auto** command is configured at the access point where DHCP is being used. The **dhcp-gateway-address** command specifies the subnet addresses to be returned by the DHCP server. This address should match the IP address of a loopback interface on the GGSN. In addition, to accommodate route aggregation for another subnet, 10.80.0.0, the **gprs default aggregate** command is used.

In this example, the GGSN aggregates routes for dynamically derived addresses for MSs through access point 8-based on the address and mask returned by the DHCP server. For PDP context requests received for statically derived addresses on the 10.80.0.0 network, the GGSN also implements an aggregate route into its routing table, as configured by the **gprs default aggregate** command.

```
interface Loopback0
 ip address 10.80.0.1 255.255.255.255
!
interface Loopback2
 ip address 10.88.0.1 255.255.255.255
!
gprs access-point-list gprs
 access-point 8
   access-point-name pdn.aaaa.com
   ip-address-pool dhcp-proxy-client
   aggregate auto
   dhcp-server 172.16.43.35
   dhcp-gateway-address 10.88.0.1
   exit
!
gprs default aggregate 10.80.0.0 255.255.255.0
```

In the following output for the **show gprs gtp pdp-context all** command, five PDP context requests are active on the GGSN for pdn.aaaa.com from the 10.88.0.0/24 network:

```
Router# show gprs gtp pdp-context all
TID              MS Addr         Source  SGSN Addr       APN
6161616161610001 10.88.0.1       DHCP    172.16.123.1    pdn.aaaa.com
6161616161610002 10.88.0.2       DHCP    172.16.123.1    pdn.aaaa.com
6161616161610003 10.88.0.3       DHCP    172.16.123.1    pdn.aaaa.com
6161616161610004 10.88.0.4       DHCP    172.16.123.1    pdn.aaaa.com
6161616161610005 10.88.0.5       DHCP    172.16.123.1    pdn.aaaa.com
```

The following output for the **show ip route** command shows a single static route in the IP routing table for the GGSN, which routes the traffic for the 10.88.0.0/24 subnet through the virtual template (or Virtual-Access1) interface:

```
Router# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.80.0.0/16 is subnetted, 1 subnets
C       10.80.0.0 is directly connected, Loopback0
     10.113.0.0/16 is subnetted, 1 subnets
```

```
C       10.113.0.0 is directly connected, Virtual-Access1
     172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
C       172.16.43.192/28 is directly connected, FastEthernet0/0
S       172.16.43.0/24 is directly connected, FastEthernet0/0
S       172.16.43.35/32 is directly connected, Ethernet2/3
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
U       10.88.0.0/24 [1/0] via 0.0.0.0, Virtual-Access1
C       10.88.0.0/16 is directly connected, Loopback2
```

Related Commands

Command	Description
aggregate	Configures the GGSN to create an aggregate route in its IP routing table when receiving PDP requests from MSs on the specified network for a particular access point on the GGSN.
show gprs access-point	Displays information about access points on the GGSN.

gprs default charging-gateway

To specify the default charging gateways, in the order of their priority (primary, secondary, and tertiary), use the **gprs default charging gateway** command in global configuration mode. To remove a charging gateway, use the **no** form of this command.

gprs default charging-gateway {*ip-address* | *name*} [{*ip-address* | *name*}] [{*ip-address* | *name*}]

no gprs default charging-gateway

Syntax Description

ip-address	IP address of a default gateway.
name	Host name for a default gateway.

Defaults

No default charging gateway is assigned.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU and the ability to configure a third charging gateway was added.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs default charging-gateway** command to specify the IP address or host name of a default charging gateway that the gateway GPRS support node (GGSN) uses to communicate charging information. If you specify three gateways, then the first gateway is the primary gateway, and the second and third charging gateways are backups.

All charging gateways share the same global parameters.

When the GGSN is configured for priority switchover using the **gprs charging switchover priority** global configuration command, regardless of the state of the current active charging gateway, when the higher priority gateway comes up, the GGSN will switch over and send G-CDRs to that charging gateway.

Examples

The following example specifies three default charging gateway IP addresses:

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

Related Commands

Command	Description
gprs charging container volume-threshold	Specifies the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the CDR.
gprs charging flow-control private-echo	Implements an echo request with private extensions for maintaining flow control on packets transmitted to the charging gateway.
gprs charging packet-queue-size	Specifies the maximum number of unacknowledged charging data transfer requests that the GGSN maintains in its queue.
gprs charging server-switch-timer	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.
gprs charging tariff-time	Specifies a time of day when GGSN charging tariffs change.
gprs charging message transfer-response number-responded	Specifies the number of seconds that the GGSN waits before it transfers charging data to the charging gateway.
gprs charging switchover priority	Configures the GGSN to switch over to the gateway of higher priority whenever a higher priority charging gateway becomes active.
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs default dhcp-server

To specify a default DHCP server from which the gateway GPRS support node (GGSN) obtains IP address leases for mobile users, use the **gprs default dhcp-server** command in global configuration mode. To remove the default DHCP server, use the **no** form of this command.

gprs default dhcp-server {*ip-address* | *name*} [{*ip-address* | *name*}]

no gprs default dhcp-server

Syntax Description

ip-address	IP address of a DHCP server. The first IP address is the name of the primary DHCP server. The second (optional) *ip-address* argument specifies the IP address of a backup DHCP server.
name	Host name of a DHCP server. The second (optional) *name* argument specifies the host name of a backup DHCP server.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs default dhcp-server** command to specify a DHCP server from which the GGSN obtains IP address leases for mobile users across all access points. Use the optional second set of arguments to specify the name, or IP address, of a backup DHCP server to use if the primary DHCP server is unavailable. If you do not specify a backup DHCP server, then no backup DHCP server is available.

In addition to specifying a DHCP server for the GGSN, you must also specify the GGSN as a DHCP proxy client. You can configure the GGSN as a DHCP proxy client using either the **gprs default ip-address-pool dhcp-proxy-client** global configuration command or the **ip-address-pool dhcp-proxy-client** access-point configuration command.

You can override the DHCP server that is configured globally, and specify a different DHCP server for a particular access point using the **dhcp-server** access-point configuration command. If you do not specify a DHCP server for a specified access point, then the DHCP server specified with the **gprs default dhcp-server** command is used for that access point.

Note You cannot specify a DHCP server that is located within a private network using VPN routing and forwarding (VRF) with the **gprs default dhcp-server global configuration** command. To specify a DHCP server that is within a VRF address space, you must use the **dhcp-server** access-point configuration command.

Examples

The following example specifies 10.101.100.3 as the GPRS/UMTS default DHCP server for GGSN, using the **gprs default dhcp-server** command. Although this DHCP server is also configured globally on the router or instance of Cisco IOS software using the **ip dhcp-server** global configuration command, this is not required.

Because DHCP is the default dynamic addressing method specified by the **gprs default ip-address-pool dhcp-proxy-client** command, access point 3 will use the DHCP server located at 10.101.100.3 for IP addressing support. Access point 1 and access point 2 override the default DHCP server using the **dhcp-server** access-point configuration command to specify alternative DHCP servers:

```
interface Loopback1
 ip address 10.30.30.30 255.255.255.255
!
interface Loopback2
 ip address 10.27.27.27 255.255.255.255
!
interface Loopback3
 ip address 10.25.25.25 255.255.255.255
!
interface loopback 1
 ip address 10.15.10.1 255.255.255.0
!
interface Virtual-Template1
 ip unnumber loopback 1
 no ip directed-broadcast
 encapsulation gtp
 gprs access-point-list abc
!
gprs access-point-list abc
 access-point 1
  access-point-name gprs.pdn1.com
  dhcp-server 10.102.100.3
  dhcp-gateway-address 10.30.30.30
  exit
!
```

```
 access-point 2
  access-point-name gprs.pdn2.com
  dhcp-server 10.60.0.1
  dhcp-gateway-address 10.27.27.27
  exit
!
 access-point 3
  access-point-name www.pdn3.com
  access-mode non-transparent
  dhcp-gateway-address 10.25.25.25
  exit
!
gprs default ip-address-pool dhcp-proxy-client
gprs default dhcp-server 10.101.100.3
```

Related Commands

Command	Description
dhcp-server	Specifies a primary (and backup) DHCP server to allocate IP addresses to MS users entering a particular PDN access point.
gprs default ip-address-pool	Specifies a dynamic address allocation method using IP address pools for the GGSN.
ip-address-pool	Specifies a dynamic address allocation method using IP address pools for the current access point.

gprs default ip-address-pool

To specify a dynamic address allocation method using IP address pools for the gateway GPRS support node (GGSN), use the **gprs default ip-address-pool** command in global configuration mode. To disable dynamic address allocation, use the **no** form of this command.

gprs default ip-address-pool {**dhcp-proxy-client** | **disable** | **radius-client**}

no gprs default ip-address-pool {**dhcp-proxy-client** | **disable** | **radius-client**}

Syntax Description

dhcp-proxy-client	GGSN dynamically acquires IP addresses for an MS from a DHCP server.
disable	Disables dynamic address allocation by the GGSN.
radius-client	GGSN dynamically acquires IP addresses for an MS from a RADIUS server.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs default ip-address-pool** command to specify the method by which the GGSN obtains address leases for mobile stations (MSs) across all access points.

If you specify **dhcp-proxy-client** for the GPRS/UMTS default IP address pool, then you must specify a DHCP server for address allocation. To specify a DHCP server, use either the **gprs default dhcp-server** global configuration command or the **dhcp-server** access-point configuration command.

If you specify **radius-client** as the method for IP address allocation, then you must configure RADIUS services at the GGSN. This involves configuring authentication, authorization, and accounting (AAA) server groups using the **gprs default aaa-group** or **aaa-group** commands and configuring the **radius-server hos**t commands to specify the RADIUS servers that provide the address pool. You also need to configure AAA on the GGSN. For more information about configuring RADIUS on the GGSN, refer to the "Usage Guidelines" section for the **aaa-group** and **gprs default aaa-group** commands.

To disable the selected IP address allocation method, use the **no** form of this command or issue the command with the **disable** keyword (the default form of this command).

Examples

The following example specifies **gprs default ip-address-pool dhcp-proxy-client** as the dynamic address allocation method for the GGSN across all access points.

Access point 3 overrides the default by specifying **ip-address-pool radius-client** as the dynamic address allocation method for that access point. The corresponding RADIUS and AAA configurations are also shown as examples.

```
aaa new-model
!
aaa group server radius foo
 server 10.2.3.4
 server 10.6.7.8
!
aaa authentication ppp foo group foo
aaa authorization network default group radius
aaa accounting exec default start-stop group foo
!
interface Loopback1
 ip address 10.30.30.30 255.255.255.255
!
interface Loopback2
 ip address 10.27.27.27 255.255.255.255
!
interface loopback 1
 ip address 10.15.10.1 255.255.255.0
!
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list abc
!
gprs access-point-list abc
 access-point 1
  access-point-name gprs.pdn1.com
  dhcp-server 10.102.100.3
  dhcp-gateway-address 10.30.30.30
  exit
!
 access-point 2
  access-point-name gprs.pdn2.com
  dhcp-server 10.60.0.1
  dhcp-gateway-address 10.27.27.27
  exit
!
 access-point 3
  access-point-name www.pdn3.com
  access-mode non-transparent
  ip-address-pool radius-client
  aaa-group authentication foo
  exit
!
```

```
gprs default ip-address-pool dhcp-proxy-client
gprs default dhcp-server 10.101.100.3
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

Related Commands

Command	Description
dhcp-server	Specifies a primary (and backup) DHCP server to allocate IP addresses to MS users entering a particular PDN access point.
gprs default dhcp-server	Specifies a default DHCP server from which the GGSN obtains IP address leases for mobile users.
ip-address-pool	Specifies a dynamic address allocation method using IP address pools for the current access point.
aaa-group	Specifies an AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN.
gprs default aaa-group	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN

gprs default map-converting-gsn

To specify the IP address or host name of the primary (and backup) GPRS support node (GSN) to communicate with the home location register (HLR) in sending and receiving Mobile Application Protocol (MAP) messages, use the **gprs default map-converting-gsn** command in global configuration mode. To remove the GSN configuration, use the **no** form of this command.

gprs default map-converting-gsn {*ip-address* | *hostname*} [*ip-address* | *hostname*]

no gprs default map-converting-gsn {*ip-address* | *hostname*} [*ip-address* | *hostname*]

Syntax Description

ip-address	IP address of the GSN handling MAP messages with the HLR. The first *ip-address* argument specifies the IP address of the primary GSN. The second (optional) *ip-address* argument specifies the IP address of a backup GSN.
hostname	Host name of the GSN handling MAP messages with the HLR. The second (optional) *name* argument specifies the host name of a backup GSN.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs default map-converting-gsn** command to identify an GSN that can convert GPRS tunneling protocol (GTP) messages to and from MAP messages. This GTP-to-MAP and MAP-to-GTP conversion allows the GSN to communicate with an HLR.

The gateway GPRS support node (GGSN) supports a maximum of two protocol-converting GSNs. Therefore, you can specify both a primary GSN and a backup GSN by using a single **gprs default map-converting-gsn** command. However, you cannot configure more than one instance of the **gprs default map-converting-gsn** command.

The GGSN uses the backup GSN when the GGSN reaches the maximum signaling threshold (N3 GTP signaling requests x T3).

Examples

The following example configures the GSN, located at IP address 172.16.10.10, to convert MAP messages between the HLR and the GGSN:

```
gprs default map-converting-gsn 172.16.10.10
```

gprs delay-qos map tos

To specify a quality of service (QoS) mapping from the delay QoS classes to an IP type of service (ToS) precedence value, use the **gprs delay-qos map tos class** command in global configuration mode. To return to the default values, use the **no** form of this command.

gprs delay-qos map tos class1 *tos-value* [**class2** *tos-value* [**class3** *tos-value* [**class-best-effort** *tos-value*]]]

no gprs delay-qos map tos class1 *tos-value* [**class2** *tos-value* [**class3** *tos-value* [**class-best-effort** *tos-value*]]]

Syntax Description

class1 *tos-value*	ToS mapping for a delay1 class QoS. The *tos-value* can be a number from 0 to 4. The default is 3.
class2 *tos-value*	ToS mapping for a delay2 class QoS. The *tos-value* can be a number from 0 to 4. The default is 2.
class3 *tos-value*	ToS mapping for a delay3 class QoS. The *tos-value* can be a number from 0 to 4. The default is 1.
class-best-effort *tos-value*	ToS mapping for a delay best-effort class QoS. The *tos-value* can be a number from 0 to 4. The default is 0.

Defaults

The default value for the class1 ToS category is 3.

The default value for the class2 ToS category is 2.

The default value for the class3 ToS category is 1.

The default value for the class-best-effort ToS category is 0.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs delay-qos map tos** command to specify a mapping between various QoS categories and the ToS precedence bits in the IP header for packets transmitted over the Gn interface (GPRS tunneling protocol [GTP] tunnels).

Note You must enable delay QoS mapping by configuring the **gprs qos map delay** command *before* you configure the **gprs delay-qos map tos** command.

The **class2**, **class3,** and **class-best-effort** keyword arguments are optional. However, if you specify a value for the **class3** argument, you must specify a value for the **class2** argument. And, if you specify a value for the **class-best-effort** argument, then you must specify a value for both the **class2** and **class3** arguments.

Only ToS classes 0 through 5 will be used for gateway GPRS support node (GGSN) signaling and user data. The GTP signaling message should have the highest precedence. ToS class 5 is the default ToS for GTP signaling. Use the **gprs gtp map signalling tos** command to specify an IP ToS mapping for GTP signaling packets.

The ToS precedence classes are defined as follows:

0 Routine

1 Priority

2 Immediate

3 Flash

4 Flash Override

5 Critical ECP

6 Internetwork Control

7 Network Control

Examples

The following example specifies a QoS mapping from the delay QoS classes to a class1 ToS category of 4, a class2 ToS category of 3, a class3 ToS category of 2, and a best-effort ToS category of 1.

```
gprs delay-qos map tos class1 4 class2 3 class3 2 class-best-effort 1
```

Related Commands

Command	Description
gprs gtp map signalling tos	Specifies an IP ToS mapping for GPRS signaling packets.
gprs qos default-response requested	Configures the GGSN to set its default QoS values in the response message exactly as requested in the Create PDP Context request message.
gprs qos map delay	Enables mapping of GPRS QoS categories to a delay QoS method that includes the delay best-effort, delay1, delay2, and delay3 classes.

gprs dfp max-weight

To specify the maximum weight sent to a dynamic feedback protocol (DFP) manager by a gateway GPRS support node (GGSN) acting as a DFP agent, use the **gprs dfp max-weight** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs dfp max-weight [*max-weight-value*]

no gprs dfp max-weight [*max-weight-value*]

Syntax Description

max-weight-value	Specifies the maximum weight sent by the GGSN, acting as a DFP agent, to a DFP manager. The valid range is 1 to 100. The default value is 8.

Defaults

8

Command Modes

Global configuration

Command History

Release	Modification
12.1(9)E	This command was introduced.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

If you use DFP with GPRS tunneling protocol (GTP) load balancing, you must also specify a maximum number of packet data protocol (PDP) contexts for each GGSN, using the **gprs maximum-pdp-context-allowed** command. *Do not* accept the default value of 10000 PDP contexts.

We recommend using a value of 45000. Significantly lower values can impact performance in a GTP load-balancing environment.

Note DFP weighs PPP PDPs against IP PDPs (one PPP PDP equals 8 IP PDPs).

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

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

Examples

The following example sets the maximum weight sent by GGSN to 43:

```
gprs dfp max-weight 43
```

Related Commands

Command	Description
agent	Identifies a DFP agent to which Cisco IOS SLB can connect.
gprs maximum-pdp-context-allowed	Specifies the maximum number of PDP contexts (mobile sessions) that can be activated on the GGSN.
ip dfp agent	Identifies a DFP agent subsystem and enters DFP agent configuration mode.
ip slb dfp	Configures DFP, supplies an optional password, and enters DFP configuration mode.

gprs gtp echo-timer dynamic enable

To enable the dynamic echo timer on the gateway GPRS support node (GGSN), use the **gprs gtp echo-timer dynamic enable** command in global configuration mode. To disable the dynamic echo timer, use the **no** form of this command.

gprs gtp echo-timer dynamic enable

no gprs gtp echo-timer dynamic enable

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

For a GPRS tunneling protocol (GTP) path to be active, the serving GPRS support node (SGSN) needs to be active. To determine that an SGSN is active, the GGSN and SGSN exchange echo messages. Although the GGSN supports different methods of echo message timing, the basic echo flow begins when the GGSN sends an echo request message to the SGSN. The SGSN sends a corresponding echo response message back to the GGSN.

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

The GGSN supports two different methods of echo timing—the default echo timer and the dynamic echo timer.

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

Default echo timer

The dynamic echo timer is based on the default echo timer in the GGSN. A description of the default echo timer follows as a means of comparison.

The default echo timer configuration uses the following commands:

- **gprs gtp n3-requests**—Specifies maximum number of times that the GGSN attempts to send a echo-request message. The default is 5 times.
- **gprs gtp path-echo-interval**—Specifies the number of seconds that the GGSN waits before sending an echo-request message. The default is 60 seconds.
- **gprs gtp t3-response**—Specifies the number of seconds that the GGSN waits before resending an echo-request message after the path echo interval has expired and the echo response has not been received. The default is 1 second.

If the GGSN receives the echo response within the path echo interval (as specified in the **gprs gtp path-echo-interval** command; default is 60 seconds), it sends another echo request message after 60 seconds (or whatever time was configured in the **gprs gtp path-echo-interval** command). This message flow continues as long as the GGSN receives an echo response message within the specified path echo interval.

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

For example, if N3 is set to the default of 5, and T3 is set to the default of 1 second, the GGSN will resend 4 echo request messages (the initial request + 4 retries = 5). The T3 time increments for each additional echo request by a factor of 2 seconds. So, the GGSN resends a message in 2 seconds, 4 seconds, 8 seconds, and 16 seconds. If the GGSN fails to receive an echo response message within the time period of the N3-requests counter, it clears the GTP path and deletes all the PDP contexts.

For the above example, the total elapsed time from when the first request message is sent, to when the GTP path is cleared, is: 60 + 2 + 4 + 8 + 16 = 90 seconds,

where 60 is the initial value of the path echo interval, and the remaining four time periods are the increments of the T3 timer for the subsequent retries.

Dynamic echo timer

The dynamic echo timer method is different from the default echo timer method on the GGSN because it uses a calculated round-trip time (RTT), as well as a configurable factor or multiplier to be applied to the RTT statistic.

The dynamic echo timer configuration uses the following commands:

- **gprs gtp echo-timer dynamic enable**—Enables the dynamic echo timer on the GGSN.
- **gprs gtp echo-timer dynamic minimum**—Specifies the minimum time period (in seconds) for the dynamic echo timer. If the RTT is less than this value, the GGSN uses the value set in this command.
- **gprs gtp echo-timer dynamic smooth-factor**—Configures the multiplier that the dynamic echo timer uses when calculating the time to wait to send retries, when it has not received a response from the SGSN within the path echo interval.

- **gprs gtp n3-requests**—Specifies the maximum number of times that the GGSN attempts to send an echo-request message. The default is 5 times.
- **gprs gtp path-echo-interval**—Specifies the number of seconds within which the GGSN expects to receive an echo response. This is the period of time that the GGSN waits before sending another echo-request message. The default is 60 seconds.

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

If the GGSN fails to receive an echo response message within the path echo interval, the GGSN goes into retransmission, or path failure mode. During path failure mode, the GGSN uses a value referred to as the T-dynamic. The T-dynamic is the greater of either the dynamic minimum, or the RTT statistic multiplied by the smooth factor.

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

For example, if the RTT is 6 seconds, N3 is set to 5, and the smooth factor is set to 3, the GGSN will resend 4 echo request messages in path failure mode. The T-dynamic value is 18 (RTT x smooth factor), so the GGSN sends a retry echo request message in 36 seconds, 72 seconds, 144 seconds, and 288 seconds. If the GGSN fails to receive an echo response message in this time period, it clears the GTP path and deletes all PDP contexts. The total elapsed time from when the first request message is sent to when the GTP path is cleared is: 60 + 36 + 72 + 144 + 288 = 600 seconds,

where 60 is the initial value of the path echo interval, and the remaining 4 time periods are the increments of the T-dynamic for the subsequent retries.

Examples

The following example turns on the dynamic echo timer, sets the minimum value to 5 seconds, and configures a smooth factor of 3:

```
gprs gtp echo-timer dynamic enable
gprs gtp echo-timer dynamic minimum 5
gprs gtp echo-timer dynamic smooth-factor 3
```

Related Commands

Command	Description
gprs gtp echo-timer dynamic minimum	Specifies the minimum time period used by the dynamic echo timer.
gprs gtp echo-timer dynamic smooth-factor	Configures the multiplier that the GGSN uses to calculate the time to wait to send retries of the dynamic echo timer.
gprs gtp n3-requests	Specifies the maximum number of times that the GGSN attempts to send a signaling request.
gprs gtp path-echo-interval	Specifies the number of seconds that the GGSN waits before sending an echo-request message.

gprs gtp echo-timer dynamic minimum

To specify the minimum time period used by the dynamic echo timer, use the **gprs gtp echo-timer dynamic minimum** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs gtp echo-timer dynamic minimum *number*

no gprs gtp echo-timer dynamic minimum *number*

Syntax Description

number	Minimum time period (between 1 and 60 seconds) of the dynamic echo timer. Value must be an integer. The default value is 5 seconds.

Defaults

5 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use this command to specify the minimum time period (in seconds) used by the dynamic echo timer, also referred to as the T-dynamic. If the gateway GPRS support node's (GGSN's) current calculation of the round-trip time (RTT) statistic, multiplied by the smooth factor, is less than the configured dynamic minimum value, then the GGSN uses the configured minimum as the T-dynamic.

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

If the GGSN fails to receive an echo response message from the serving GPRS support node (SGSN) within the path echo interval, the GGSN goes into retransmission, or path failure mode. During path failure mode, the GGSN uses a value referred to as the T-dynamic. The T-dynamic is the greater of either the dynamic minimum, or the RTT statistic multiplied by the smooth factor.

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

Note For more information about the dynamic echo timer on the GGSN, see the "Usage Guidelines" section for the **gprs gtp echo-timer dynamic enable** command.

Examples

The following example turns on the dynamic echo timer, sets the minimum value to 6 seconds, and configures a smooth factor of 2:

```
gprs gtp echo-timer dynamic enable
gprs gtp echo-timer dynamic minimum 6
gprs gtp echo-timer dynamic smooth-factor 2
```

Related Commands

Command	Description
gprs gtp echo-timer dynamic enable	Enables the dynamic echo timer on the GGSN.
gprs gtp echo-timer dynamic smooth-factor	Configures the multiplier that the GGSN uses to calculate the time to wait to send retries of the dynamic echo timer.
gprs gtp n3-requests	Specifies the maximum number of times that the GGSN attempts to send a signaling request.
gprs gtp path-echo-interval	Specifies the number of seconds that the GGSN waits before sending an echo-request message to the SGSN.

gprs gtp echo-timer dynamic smooth-factor

To configure the multiplier that the gateway GPRS support node (GGSN) uses to calculate the time to wait to send retries of the dynamic echo timer, use the **gprs gtp echo-timer dynamic smooth-factor** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs gtp echo-timer dynamic smooth-factor *number*

no gprs gtp echo-timer dynamic smooth-factor *number*

Syntax Description

number	Integer (between 1 and 100) used by the GGSN as a multiplier for the round-trip time (RTT) statistic, to calculate the T-dynamic. The default is 2.

Defaults

2

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The dynamic echo timer uses the smooth factor to calculate what is known as the T-dynamic. The T-dynamic is calculated by multiplying the RTT (or the value configured in the **gprs gtp echo-timer dynamic minimum**, whichever is greater) times the smooth-factor.

Note See the "Usage Guidelines" section for the **gprs gtp echo-timer dynamic enable** command for a detailed explanation of how the dynamic echo timer works.

Examples

The following example turns on the dynamic echo timer, sets the minimum value to 1 second, and configures a smooth factor of 2:

```
gprs gtp echo-timer dynamic enable
gprs gtp echo-timer dynamic minimum 1
gprs gtp echo-timer dynamic smooth-factor 2
```

Related Commands

Command	Description
gprs gtp echo-timer dynamic enable	Enables the dynamic echo timer on the GGSN.
gprs gtp echo-timer dynamic minimum	Specifies the minimum time period used by the dynamic echo timer.
gprs gtp n3-requests	Specifies the maximum number of times that the GGSN attempts to send a signaling request.
gprs gtp path-echo-interval	Specifies the number of seconds that the GGSN waits before sending an echo-request message to the SGSN.
gprs gtp t3-response	Specifies the initial time that the GGSN waits before resending a signaling request message when a response to a request has not been received

gprs gtp error-indication-throttle

To specify the maximum number of error indication messages that the gateway GPRS support node (GGSN) sends out in one second, use the **gprs gtp error-indication-throttle** command in global configuration mode. To return to the default value, issue the **no** form of this command.

gprs gtp error-indication-throttle window-size *size*

no gprs gtp error-indication-throttle

Syntax Description

size	Integer (between 0 and 256) that specifies the maximum number of error indication messages that the GGSN sends in one second.

Defaults

Error indication throttling is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

GPRS tunneling protocol (GTP) error indication messages are sent by the GGSN to the serving GPRS support node (SGSN) when the SGSN sends data for packet data protocol (PDP) context the GGSN cannot locate. The error indication message informs the SGSN that the PDP context cannot be located so that the SGSN can clean up the PDP context on its end.

Use the **gprs gtp error-indication-throttle** command to specify the maximum number of error indication messages that are sent by the GGSN in one second. This provides a way to implement flow control for transmission of GTP error messages. This command sets the initial value of a counter which is decremented each time an error indication message is sent. When the counter reaches zero, the GGSN stops transmitting error indication messages. The GGSN resets this counter to the configured throttle value after one second.

If you do not issue the command, error indication throttling is not enabled. To restore the default value (error indication throttling is disabled) use the **no** form of this command.

Examples

The following example shows a throttle value of 150:

```
gprs gtp error-indication-throttle window-size 150
```

gprs gtp ip udp ignore checksum

To configure the GGSN to ignore user datagram protocol (UDP) checksums (in order to support CEF switching on the GGSN), use the **gprs gtp ip udp ignore checksum** global configuration command. To disable the ignoring of UDP checksums on the GGSN, use the **no** form of this command.

gprs gtp ip udp ignore checksum

no gprs gtp ip udp ignore checksum

Syntax Description

This command has no arguments or keywords.

Defaults

In releases prior to Cisco IOS Release 12.3(14)XU, UDP checksums are verified by default.

With Cisco IOS Release 12.3(14)XU and later, UDP checksums are ignored by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was incorporated in Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was incorporated in Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was incorporated in Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was incorporated in Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was incorporated in Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was incorporated in Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU and the default was changed to have the GGSN ignore UDP checksums.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

UDP checksum verification can prohibit operation of CEF switching processing on the GGSN if the checksum should have a non-zero result. Therefore, if you want to enable CEF switching on the GGSN, ensure that the GGSN is configured to ignore UPD checksums (the default).

If UDP checksum verification remains enabled on the GGSN and a non-zero result occurs, the GTP T-PDUs will be process switched, even if you have configured the GGSN for CEF switching.

The **gprs gtp ip udp ignore checksum** command does not apply if you are only using process switching on the GGSN.

Note When downgrading to an image prior to Cisco IOS Release 12.3(14)YU when using the default for the **gprs gtp ip udp ignore checksum** command (UDP checksums are ignored), you will need to manually configure the GGSN to ignore UPD checksums. In releases prior to Cisco IOS Release 12.3(14)YU, UDP checksums are verified by the GGSN by default.

For more information about switching processes, refer to the *Cisco IOS Switching Services Configuration Guide*.

Examples

The following example disables UDP checksum verification on the GGSN:

```
gprs gtp ip udp ignore checksum
```

Related Commands

Command	Description
ip cef	Enables CEF on the route processor card.

gprs gtp map signalling tos

To specify an IP type of service (ToS) mapping for GPRS tunneling protocol (GTP) signaling packets, use the **gprs gtp map signalling tos** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs gtp map signalling tos *tos-value*

no gprs gtp map signalling tos *tos-value*

Syntax Description

tos-value	Value between 0 and 7 that specifies the IP ToS mapping. The default value is 5.

Defaults

ToS value 5

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs gtp map signalling tos** command to specify the IP ToS mapping for GTP signaling packets transmitted by the gateway GPRS support node (GGSN). The higher the value, the higher the class of service provided to the packets.

Examples

The following example specifies a IP ToS mapping value of 3:

```
gprs gtp map signalling tos 3
```

Related Commands

Command	Description
gprs canonical-qos map tos	Specifies a QoS mapping from the canonical QoS classes to an IP ToS category.
gprs charging container volume-threshold	Specifies the maximum number of bytes that the GGSN maintains in a user's charging container before closing the charging container and updating the CDR.
gprs charging map data tos	Specifies an IP ToS mapping for GGSN charging data packets.
gprs charging packet-queue-size	Specifies the maximum number of unacknowledged charging data transfer requests that the GGSN maintains in its queue.
gprs charging message transfer-response number-responded	Specifies the number of seconds that the GGSN waits before it transfers charging data to the charging gateway.

gprs gtp n3-buffer-size

To specify the size of the receive buffer that the gateway GPRS support node (GGSN) uses to receive GPRS tunneling protocol (GTP) signaling messages and packets sent through the tunneling protocol, use the **gprs gtp n3-buffer-size** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs gtp n3-buffer-size *bytes*

no gprs gtp n3-buffer-size

Syntax Description

bytes	Number of bytes (between 2048 and 65535) that specifies the size of the N3 buffer. The default is 8192 bytes.

Defaults

8192 bytes

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs gtp n3-buffer-size** command to specify the size of the GTP N3 buffer on the GGSN. The N3 buffer is a receive buffer that the GGSN uses to receive GTP signaling messages and packets sent through the tunneling protocol. The recommended value for the N3 buffer size is 8192 bytes (the default size).

Examples

The following example specifies a buffer size of 2084 bytes:

```
gprs gtp n3-buffer-size 2048
```

gprs gtp n3-requests

To specify the maximum number of times that the gateway GPRS support node (GGSN) attempts to send a signaling request to a serving GPRS support node (SGSN), use the **gprs gtp n3-requests** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs gtp n3-requests *requests*

no gprs gtp n3-requests *requests*

Syntax Description

requests	A number between 1 and 65535 that specifies the number of times that a request is attempted. The default is 5 requests.

Defaults

5 requests

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The value of the **gprs gtp n3-requests** command is used for all signaling requests on the GGSN.

The GGSN supports two different methods of echo timing—the default echo timer and the dynamic echo timer. The **gprs gtp n3-requests** command is used by the GGSN to perform either type of echo processing.

Examples

The following example shows the GGSN attempting to send a signaling request 3 times:

```
gprs gtp n3-requests 3
```

Related Commands

Command	Description
gprs gtp echo-timer dynamic enable	Enables the dynamic echo timer on the GGSN.
gprs gtp n3-buffer-size	Specifies the size of the receive buffer that the GGSN uses to receive GTP signaling messages and packets sent through the tunneling protocol.
gprs gtp path-echo-interval	Specifies the number of seconds that the GGSN waits before sending an echo-request message to the SGSN.
gprs gtp t3-response	Specifies the initial time that the GGSN waits before resending a signaling request message when a response to a request has not been received.

gprs gtp path-echo-interval

To specify the number of seconds that the gateway GPRS support node (GGSN) waits before sending an echo-request message to the serving GPRS support node (SGSN) or charging gateway, use the **gprs gtp path-echo-interval** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs gtp path-echo-interval *interval*

no gprs gtp path-echo-interval *interval*

Syntax Description

interval	Number of seconds that the GGSN waits before sending an echo-request message. Specify a value between 60 and 65535 seconds. The value 0 disables the echo-request feature. The default is 60 seconds.

Defaults

60 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The GGSN supports two different methods of echo timing—the default echo timer and the dynamic echo timer. The **gprs gtp path-echo-interval** command is used on the GGSN to perform either type of echo processing.

Use the **gprs gtp path-echo-interval** command to specify the interval that the GGSN waits before sending an echo-request message to the SGSN or charging gateway to check for GPRS tunneling protocol (GTP) path failure.

Note A value of 0 seconds disables echo requests on the GGSN.

Examples

The following example shows the GGSN waiting 90 seconds before sending an echo-request message:

```
gprs gtp path echo-interval 90
```

Related Commands

Command	Description
gprs gtp echo-timer dynamic enable	Enables the dynamic echo timer on the GGSN.
gprs gtp n3-requests	Specifies the maximum number of times that the GGSN attempts to send a signaling request to an SGSN.
gprs gtp t3-response	Specifies the initial time that the GGSN waits before resending a signaling request message when a response to a request has not been received.

gprs gtp path history

To configure the maximum number of path entries for which the gateway GRPS serving node (GGSN) stores statistics after the path is deleted, use the **gprs gtp path history** command in global configuration mode.

gprs gtp path history *number*

no gprs gtp path history

Syntax Description

number	Number of path entries for which to store statistics in history when the path is deleted. A valid value is between 1 and 1000.

Defaults

100 entries.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)XG	This command was introduced.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **gprs gtp path history** command to configure the number of path entries for which the GGSN stores statistics after the path is deleted.

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

Examples

The following example configures the GGSN to store statistics for up to 250 entries:

```
gprs gtp path history 250
```

Related Commands

Command	Description
show gprs gtp path history	Displays summary details of past GTP path entries stored in history.
show gprs gtp path statistics remote-address	Displays the details of counters for a current path, or the details of counters maintained in history for a deleted path.

gprs gtp path sgsn

To suppress echo requests per SGSN and/or UDP port, use the **gprs gtp path sgsn** command in global configuration mode. To remove this configuration, use the **no** form of this command.

gprs gtp path sgsn *start-ip-address* [*end-ip-address*] [*UDP port*] **echo 0**

no gprs gtp path sgsn *start-ip-address* [*end-ip-address*] [*UDP port*] **echo 0**

Syntax Description

start-ip-address	Specifies the first IP address of the range.
end-ip-address	Specifies the last IP address of the range.
udp port	Specifies the corresponding UDP port.
echo 0	Disables echo requests.

Command Default

There are no default behaviors or values.

Command Modes

Global configuration

Command History

Release	Modification
12.(4)15XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

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

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

Examples

The following example disables echo requests for one SGSN:

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

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

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

gprs gtp pdp-context timeout idle

To specify the time, in seconds, that a gateway GPRS support node (GGSN) allows a session to remain idle at any access point before purging the packet data protocol (PDP) context, use the **gprs gtp pdp-context timeout idle** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs gtp pdp-context timeout idle *seconds* [**uplink**]

no gprs gtp pdp-context timeout idle

Syntax Description

seconds	Time, in seconds, that the GGSN allows a PDP context to remain idle on any access point before terminating the context. Specify a value between 30 and 4294967 seconds.
uplink	(Optional) Enables the session idle timer in the uplink direction only. When the **uplink** keyword option is not specified, the session idle timer is enabled in both directions (uplink and downlink).

Defaults

259200 seconds (72 hours)

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(8)XU1	This command was integrated into Cisco IOS Release 12.3(8)XU1 and the **uplink** keyword option was added.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

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

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

On the GGSN, the session idle timer can be configured globally and at the access point name (APN). The value configured at the APN level using the **gtp pdp-context timeout idle** access-point configuration command overrides the value configured globally using the **gprs gtp pdp-context timeout idle** global configuration command. The value configured in the user profile on the RADIUS server overrides the value configured at the APN.

Note The session idle timer started for a PDP context is reset by Transport Protocol Data Unit (TPDU) traffic and GPRS tunneling protocol (GTP) signaling messages for that PDP context. For example, if an Update PDP Context request is received, the session idle timer is reset for that PDP context.

You can disable the session idle timer for a particular user by configuring 0 as the session idle time duration in the user profile on the RADIUS server. If a user is authenticated by RADIUS, the session idle time cannot be disabled.

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

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

Examples

The following example shows configuring the GGSN to wait 18000 seconds before ending an idle PDP context:

```
gprs gtp pdp-context timeout idle 18000
```

Related Commands

Command	Description
gprs gtp pdp-context timeout session	Specifies the time, in seconds, that the GGSN allows a session to be active on any access point before terminating the session.
gprs idle-pdp-context purge-time	Specifies the time, in hours, that the GGSN waits before purging idle mobile sessions.
gtp pdp-context timeout idle	Specifies the time, in seconds, that a GGSN allows a session to be idle at a particular APN before terminating the session.
gtp pdp-context timeout session	Specifies the time, in seconds, that a GGSN allows a session to be active at a particular APN before terminating the session.
session idle-time	Specifies the time, in hours, that the GGSN waits before purging idle mobile sessions for an access point.
show gprs gtp pdp-context	Displays a list of the currently active PDP contexts (mobile sessions).

gprs gtp pdp-context timeout session

To specify the time, in seconds, that the gateway GPRS support node (GGSN) allows a session to exist at any access point before terminating the session, use the **gprs gtp pdp-context timeout session** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs gtp pdp-context timeout session *seconds*

no gprs gtp pdp-context timeout session

Syntax Description

seconds	Time, in seconds, that the GGSN allows a session to exist at any access point. Specify a value between 30 and 4294967 seconds.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

When enabled using the **gprs radius attribute session-timeout** command, the GGSN supports the RADIUS Session-Timeout (Attribute 27). The GGSN stores the attribute timeout value received in access-accept packets sent by the authentication, authorization, and accounting (AAA) server and when the duration of a session exceeds the duration configured as absolute session timer, the GGSN terminates the session and all packet data protocol (PDP) contexts belonging to the session (those with the same International Mobile Subscriber Identity [IMSI] or mobile station [MS] address).

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

Note The active session timeout feature requires that the **gprs radius attribute session-timeout** command has been enabled.

On the GGSN, the absolute session timer can be configured globally and at the access point name (APN). The value configured at the APN level using the **gtp pdp-context timeout session** access-point configuration command overrides the value configured globally using the **gprs gtp pdp-context timeout session** global configuration command. The value configured in the user profile on the RADIUS server overrides the value configured at the APN.

Examples

The following example shows configuring the GGSN to end any session that exceeds 86400 seconds in duration:

```
gprs gtp pdp-context timeout session 86400
```

Related Commands

Command	Description
gprs gtp pdp-context timeout idle	Specifies the time, in seconds, that a GGSN allows a session to be idle at any access point before terminating the session.
gprs idle-pdp-context purge-timer	Specifies the time, in hours, that the GGSN waits before purging idle mobile sessions.
gtp pdp-context timeout idle	Specifies the time, in seconds, that a GGSN allows a session to be idle at a particular APN before terminating the session.
gtp pdp-context timeout session	Specifies the time, in seconds, that a GGSN allows a session to be active at a particular APN before terminating the session.
session idle-time	Specifies the time, in hours, that the GGSN waits before purging idle mobile sessions for an access point.
show gprs gtp pdp-context	Displays a list of the currently active PDP contexts (mobile sessions).

gprs gtp ppp vtemplate

To associate the virtual template interface that defines the PPP characteristics with support for the PPP packet data protocol (PDP) type over GPRS tunneling protocol (GTP) on the gateway GPRS support node (GGSN), use the **gprs gtp ppp vtemplate** command in global configuration mode. To remove specification of the PPP virtual template interface for GTP on the GGSN, use the **no** form of this command.

gprs gtp ppp vtemplate *number*

no gprs gtp ppp vtemplate

Syntax Description

number	Integer identifier of the virtual template interface over which the PPP characteristics are defined on the GGSN. This number must match the number configured in the corresponding **interface virtual-template** command.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Before you configure the **gprs gtp ppp vtemplate** command, you must configure the virtual template interface with the necessary PPP characteristics. The number that you configure for the virtual template interface that defines the PPP characteristics, must correspond to the number that you specify in the **gprs gtp ppp vtemplate** command.

Examples

The following example configures two virtual template interfaces on the GGSN, one for GTP encapsulation and one for PPP, and specifies the PPP virtual template interface for GTP on the GGSN.

Note The virtual template interface for PPP is a different virtual template interface than the GPRS/UMTS virtual template interface for GTP encapsulation.

The first section of commands configures the GPRS virtual template interface for GTP:

```
interface Virtual-Template 1
 ip unnumber loopback 1
 no ip directed-broadcast
 encapsulation gtp
 no ip route-cache
 gprs access-point-list gprs
```

The following example configures a virtual template interface for PPP and associates the virtual template for support of the PPP PDP type over GTP on the GGSN:

```
interface Virtual-Template 2
 ip unnumbered FastEthernet 1/0
 no ip directed-broadcast
 no peer default ip address
 ppp authentication chap
 ppp timeout retry 30

gprs gtp ppp vtemplate 2
```

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.

gprs gtp ppp-regeneration vtemplate

To associate the virtual template interface that is configured for PPP encapsulation with support for regenerated PPP sessions on the GGSN, use the **gprs gtp ppp-regeneration vtemplate** global configuration command. To remove specification of the PPP virtual template interface for regenerated PPP sessions on the GGSN, use the **no** form of this command.

gprs gtp ppp-regeneration vtemplate *number*

no gprs gtp ppp-regeneration vtemplate

Syntax Description

number	Integer identifier of the virtual template interface which defines PPP encapsulation on the GGSN. This number must match the number configured in the corresponding **interface virtual-template** command.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Before you configure the **gprs gtp ppp-regeneration vtemplate** command, you must configure the virtual template interface for PPP encapsulation using the **encapsulation ppp** command. In addition, you must also configure the **ip address negotiated** command and the **no peer neighbor-route** command at the virtual template interface for PPP encapsulation.

The number that you configure for the virtual template interface to support PPP encapsulation, must correspond to the number that you specify in the **gprs gtp ppp-regeneration vtemplate** command.

Examples

The following example configures two virtual template interfaces on the GGSN, one for GTP encapsulation for communication between the GGSN and the SGSN, and one for PPP regeneration. The virtual template interface for PPP regeneration supports the creation of PPP sessions from the GGSN over Layer 2 Tunneling Protocol (L2TP) tunnels to an L2TP network server (LNS).

Note The virtual template interface for PPP regeneration is a different virtual template interface than the GPRS virtual template interface for PPP PDP type support and for GTP encapsulation.

The first section of commands configures the GPRS virtual template interface for GTP:

```
interface Virtual-Template 1
 ip unnumber loopback 1
 no ip directed-broadcast
 encapsulation gtp
 no ip route-cache
 gprs access-point-list gprs
```

The following example configures a virtual template interface for PPP regeneration:

```
interface Virtual-Template 11
 ip address negotiated
 no peer neighbor-route
 encapsulation ppp
```

Note The **encapsulation ppp** configuration will not display in a show running configuration because it is the default encapsulation.

The following example specifies virtual template interface 11 for PPP regeneration on the GGSN:

```
gprs gtp ppp-regeneration vtemplate 11
```

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.

gprs gtp response-message pco ipcp nack

To configure IP control protocol (IPCP) options returned in the protocol control option (PCO) information element (IE) by the gateway GPRS support node (GGSN) in the Create packet data protocol (PDP) Context responses, use the **gprs gtp response-message pco ipcp** global configuration field. To return to the default values, use the **no** form of the command.

gprs gtp response-message pco ipcp {**nack** | **message-length**}

no gprs gtp response-message pco ipcp {**nack** | **message-length**}

Syntax Description

nack	Specifies for the GGSN to return an IPCP Conf-Nack (Code 03) in the GTP PCO IE of the Create PDP Context response when returning IPCP options for which the granted values (non-zero) differ from those requested. (IPCP Conf-Reject [Code 04) is returned for those options for which the returned address values are zero).
message-length	Configures an extra field that indicates the message length to be added to the header in the PCO IE of the Create PDP Context response when returning IPCP options.

Defaults

The GGSN sends an IPCP Conf-Ack (Code 02) in the PCO IE of the Create PDP Context response for the the requested IPCP address options supported by the GGSN. The values being returned might be the same as or differ from those requested, or be zero. For unsupported options, an IPCP Conf-Reject is returned.

The GGSN does not add an extra fieldthat indicates the message length to the PCO IE, when returning IPCP options.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)XB	This command was introduced.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB and the **message-length** keyword option was added.

Usage Guidelines

Use the **gprs gtp response-message pco ipcp** command to configure IPCP options returned by the GGSN in the PCO IE of a Create PDP Context response.

Use the **gprs gtp response-message pco ipcp** command, with the **nack** keyword option specified, to configure the GGSN to return an IPCP Conf-Nack in the PCO IE of a Create PDP Context response when returning IPCP options for which the granted values differ from those requested (non-zero values).

When the **gprs gtp response-message pco ipcp nack** command is configured, and the PCO IE of the Create PDP Context request contains IPCP options, the PCO IE in the create PDP response includes the following, depending on the whether options are supported by (and values are acceptable to) the GGSN:

- IPCP Conf-Ack—One or (zero) IPCP Conf-Ack for the IPCP options for which the requested values are acceptable by the GGSN.
- IPCP Conf-Nack—One or (zero) IPCP Conf-Nack containing the IPCP options for which the granted values differ from those requested.
- IPCP Conf-Reject—One (or zero) IPCP Conf-Reject containing the requested options which are not supported by the GGSN, or, if supported, for which no values can be granted.

Use the **gprs gtp response-message pco ipcp** command, with the **message-length** keyword option specified, to configured the GGSN to add a message length field to the PCO IE in the Create PDP Context response, when returning IPCP options.

Examples

The following configures the GGSN to include an extra field in the header of the PCO IE when returning IPCP options that indicates the message length in Create PDP Context responses.

```
gprs gtp response-message pco ipcp message-length
```

Related Commands

Command	Description
show gprs access-point	Displays information about access points on the GGSN.

gprs gtp response-message wait-accounting

To configure the gateway GPRS support node (GGSN) to wait for a RADIUS accounting response before sending a Create packet data protocol (PDP) Context response to the serving GPRS support node (SGSN) for Create PDP Context requests received across all access points, use the **gprs gtp response-message wait-accounting** command in global configuration mode. To configure the GGSN to send a Create PDP Context response to the SGSN after sending a RADIUS start accounting message to the RADIUS server (without waiting for a response from the RADIUS accounting server), use the **no** form of this command.

gprs gtp response-message wait-accounting

no gprs gtp response-message wait-accounting

Syntax Description

This command has no arguments or keywords.

Defaults

The GGSN sends a Create PDP Context response to the SGSN after sending a RADIUS start accounting message to the RADIUS accounting server. The GGSN does not wait for a RADIUS accounting response from the RADIUS accounting server.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs gtp response-message wait-accounting** command to configure the GGSN to wait for a RADIUS accounting response from the RADIUS accounting server before sending a Create PDP Context response to the SGSN for Create PDP Context requests received across all access points.

If the GGSN does not receive a response from the RADIUS accounting server when you have configured the **gprs gtp response-message wait-accounting** command, it rejects the PDP context request.

When broadcast accounting is used (accounting requests are sent to multiple RADIUS servers), if a RADIUS server responds with an accounting response, the GGSN sends a Create PDP Context response and does not wait for the other RADIUS servers to respond.

The GGSN supports configuration of RADIUS response message waiting at both the global and access-point configuration levels. You can minimize your configuration by specifying the configuration that you want to support across most access point names (APNs), at the global configuration level. Then, at the access-point configuration level, you can selectively modify the behavior that you want to support at a particular APN. Therefore, at the APN configuration level, you can override the global configuration of RADIUS response message waiting.

To configure the GGSN to wait for a RADIUS accounting response as the default behavior for all APNs, use the **gprs gtp response-message wait-accounting** global configuration command. To disable this behavior for a particular APN, use the **no response-message wait-accounting** access-point configuration command.

To verify whether RADIUS response message waiting is enabled or disabled at an APN, you can use the **show gprs access-point** command and observe the value reported in the wait_accounting output field.

Examples

The following example globally configures the GGSN to wait for a RADIUS accounting response from the RADIUS accounting server before sending an Activate PDP Context response to the SGSN, for PDP context requests received across all access points except access-point 1. RADIUS response message waiting has been overridden at access-point 1 using the **no gtp response-message wait-accounting** command.

Note This example shows only a partial configuration of the GGSN, to highlight the commands for implementing RADIUS response message waiting. Additional configuration statements are required to complete a full configuration of the GGSN.

```
aaa new-model
!
aaa group server radius foo
 server 10.2.3.4
 server 10.6.7.8
!
aaa authentication ppp foo group foo
aaa authorization network default group radius
aaa accounting exec default start-stop group foo
!
gprs access-point-list gprs
 access-point 1
  access-mode non-transparent
  access-point-name www.pdn1.com
  aaa-group authentication foo
  no gtp response-message wait-accounting
  exit
 access-point 2
  access-mode non-transparent
  access-point-name www.pdn2.com
  aaa-group authentication foo
!
gprs gtp response-message wait-accounting
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

Related Commands

Command	Description
gtp response-message wait-accounting	Configures the GGSN to wait for a RADIUS accounting response before sending a Create PDP Context response to the SGSN, for Create PDP Context requests received at a particular APN.
show gprs access-point	Displays information about access points on the GGSN.

gprs gtp t3-response

To specify the initial time that the gateway GPRS support node (GGSN) waits before resending a signaling request message when a response to a request has not been received, use the **gprs gtp t3-response** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs gtp t3-response *response-interval*

no gprs gtp t3-response

Syntax Description

response-interval	A value between 1 and 65535 that specifies the length of the T3 response interval, in seconds. The default is 1 second.

Defaults

1 second

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The **gprs gtp t3-response** command is used by the GGSN to process Delete packet data protocol (PDP) Context requests and to perform the default method of echo timing.

For delete PDP context requests, the **gprs gtp t3-response** command is used by the GGSN to specify how long the GGSN waits before sending a retry of the delete PDP context request when a response is not received from the serving GPRS support node (SGSN), until the **gprs gtp n3-requests** limit is reached.

The GGSN supports two echo timer implementations—the default echo timer and the dynamic echo timer. The **gprs gtp t3-response** command is also used on the GGSN to perform the default type of echo processing, when the dynamic echo timer is not enabled.

If the GGSN receives the echo response within the path echo interval (as specified in the **gprs gtp path-echo-interval** command; default is 60 seconds), it sends another echo request message after 60 seconds (or whatever time was configured in the **gprs gtp path-echo-interval** command). This message flow continues as long as the GGSN receives an echo response message within the specified path echo interval.

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

For example, if N3 is set to the default of 5, and T3 is set to the default of 1 second, the GGSN will resend 4 echo request messages (the initial request + 4 retries = 5). The T3 time increments for each additional echo request, by a factor of 2 seconds. So, the GGSN resends a message in 2 seconds, 4 seconds, 8 seconds, and 16 seconds. If the GGSN fails to receive an echo response message from the SGSN within the time period of the N3-requests counter, it clears the GPRS tunneling protocol (GTP) path and deletes all the PDP contexts.

For the above example, the total elapsed time from when the first request message is sent, to when the GTP path is cleared, is: 60 + 2 + 4 + 8 + 16 = 90 seconds,

where 60 is the initial value of the path echo interval, and the remaining 4 time periods are the increments of the T3 timer for the subsequent retries.

Examples

The following example shows a T3 interval response interval of 524 seconds:

```
gprs gtp t3-response 524
```

Related Commands

Command	Description
gprs gtp n3-requests	Specifies the maximum number of times that the GGSN attempts to send a signaling request to an SGSN.
gprs gtp path-echo-interval	Specifies the number of seconds that the GGSN waits before sending an echo request message to the SGSN.

gprs gtp update qos-fail delete

To configure the GGSN to delete a PDP context if a GGSN-initiated QoS update fails, and no GGSN-initiated Update PDP Context Request failure action has been configured at the APN, use the **gprs gtp update qos-fail delete** command in global configuration mode. To return to the default value, use the **no** form of the command.

gprs gtp update qos-fail delete

no gprs gtp update qos-fail delete

Syntax Description

This command has no arguments or keywords.

Defaults

PDP contexts are not deleted.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use this command to configure the GGSN to generate a Delete PDP Context request when a GGSN-initiated Update PDP Context Request for a QoS update fails.

The Acct Stop record generated by the GGSN indicates the update failure.

This configuration applies when the Update PDP Context Response from the SGSN, initiated for a QoS change, times out after n3 tries or the Cause value is a value other than “Request Accepted.”

Note The GGSN-initiated Update PDP Context Request failure action defined at the APN overrides this global configuration.

Examples

The following is an example:

```
Router(config)#gprs gtp update qos-fail delete
```

Related Commands

Command	Description
gtp update qos-fail delete	Configures the GGSN to delete PDP contexts for an APN when GGSN-initiated QoS updates fail.

gprs idle-pdp-context purge-timer

To specify the time, in hours, that the gateway GPRS support node (GGSN) waits before purging idle mobile sessions, use the **gprs idle-pdp-context purge-timer** command in global configuration mode. To return to the default value, use the **no** form of this command**.**

gprs idle-pdp-context purge-timer *hours*

no gprs idle-pdp-context purge-timer

Syntax Description

hours	Value between 0 and 255 that specifies the number of hours that the GGSN waits before purging idle sessions. The value 0 disables the purge timer. The default is 72 hours.

Defaults

72 hours

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

To specify the time that the GGSN waits before purging idle mobile sessions, use the **gprs idle-pdp-context purge-timer** command. To disable this feature, specify a purge-timer value of 0.

You can override the value of the global purge timer using the **session idle-time** access-point configuration command.

Note With GGSN Release 5.0 and later, you can also configure the session idle timer globally using the **gprs gtp pdp-context timeout idle** access-point configuration command, however, the two methods cannot be configured at the same time.

Examples

The following example specifies for the GGSN to wait 60 hours before purging idle sessions:

```
gprs idle-pdp-context purge-timer 60
```

Related Commands

Command	Description
gprs gtp pdp-context timeout idle	Specifies the number of seconds that a GGSN allows a session to be idle before terminating the session.
gprs gtp pdp-context timeout session	Specifies the number of seconds that the GGSN allows a session to be active before terminating the session.
gtp pdp-context timeout idle	Specifies the number of seconds that a GGSN allows a session to be idle at a particular APN before terminating the session.
gtp pdp-context timeout session	Specifies the number of seconds that a GGSN allows a session to be active at a particular APN before terminating the session.
session idle-time	Specifies the time that the GGSN waits before purging idle mobile sessions for the current access point.

gprs iscsi

To configure the GGSN to use an iSCSI target interface profile for record storage, use the **gprs iscsi** command in global configuration mode. To remove this configuration, use the **no** form of this command.

gprs iscsi *target_profile_name*

no gprs iscsi *target_profile_name*

Syntax Description

target_profile_name	Name of the iSCSI target interface profile. The profile name specified must be the same as the one configured using the **ip iscsi target-profile** command.

Command Default

iSCSI storage is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Multiple iSCSI profiles can be configured on the GGSN, however, only one target can be defined per profile, and the GGSN can be configured to use only one profile at a time using the **gprs iscsi** global configuration command.

Examples

The following example configures the GGSN to use an iSCSI target interface profile named “targetA” to store and retrieve G-CDRs:

```
gprs iscsi targetA
```

Related Commands

Command	Description
ip iscsi target-profile	Creates an iSCSI target interface profile for an SCSI target (or modifies an existing one), and enters iSCSI interface configuration mode.

gprs maximum-pdp-context-allowed

To specify the maximum number of packet data protocol (PDP) contexts (mobile sessions) that can be activated on the gateway GPRS support node (GGSN), use the **gprs maximum-pdp-context-allowed** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs maximum-pdp-context-allowed *pdp-contexts*

no gprs maximum-pdp-context-allowed

Syntax Description

pdp-contexts	Integer between 1 and 4294967295 that specifies the number of active PDP contexts allowed. The default is 10000 PDP contexts.

Defaults

10000 PDP contexts

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX, and the default value was changed from 1000 to 10000.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs maximum-pdp-context-allowed** command to specify the maximum number of PDP contexts allowed on the GGSN. When the maximum allowable number of PDP contexts is reached, the GGSN refuses new PDP contexts (mobile sessions) until sessions are available.

The practical upper limit for the maximum number of PDP contexts supported on a GGSN is dependent on the memory and platform in use and the GGSN configuration (for example, whether or not a method of PPP has been configured to forward packets beyond the terminal equipment and mobile termination, whether Dynamic Feedback Protocol [DFP] is being used or the memory protection feature is enabled, and the rate of PDP context creation to be supported).

Note DFP weighs PPP PDPs against IP PDPs with one PPP PDP equal to 8 IP PDPs.

Cisco 7200 Series Router

The following list shows the maximum number of PDP contexts supported on the GGSN according to the memory and Cisco 7206 router in use when a method of PPP has not been configured:

- Cisco 7206 VXR NPE-300 with 256 Mb of RAM—80,000 IP PDP contexts.
- Cisco 7206 VXR NPE-400 router with 512 Mb of RAM—135,000 IP PDP contexts.

Catalyst 6500 Series Switch / Cisco 7600 Series Router

The Cisco Multi-processor WAN Application Module (MWAM) can support up to 60,000 IP PDP contexts per GGSN instance with a maximum number of 300,000 IP PDP contexts per MWAM on which five GGSNs are configured.

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

Note If you use dynamic feedback protocol (DFP) with GPRS tunneling protocol (GTP) load balancing, you must also specify a maximum number of PDP contexts for each GGSN, using the **gprs maximum-pdp-context-allowed** command. Do not accept the default value of 10000 PDP contexts. Significantly lower values can impact performance in a GTP load-balancing environment.

DFP weighs PPP PDPs against IP PDPs, with one PPP PDP equal to 8 IP PDPs. Therefore, when using DFP, be aware that the configured maximum number of PDP contexts affects the GGSN weight. The lower the maximum number of PDP contexts, the lower the weight when all other parameters remain the same.

Note For more information about configuring GTP load balancing, see the *IOS Server Load Balancing*, documentation located at Cisco.com.

Examples

In the following example 15000 PDP contexts are allowed on the GGSN:

```
gprs maximum-pdp-context-allowed 15000
```

Related Commands

Command	Description
gprs idle-pdp-context purge-timer	Specifies the time that the GGSN waits before purging idle mobile sessions.

gprs mcc mnc

To configure the mobile country code (MCC) and mobile network code (MNC) that the gateway GPRS support node (GGSN) uses to determine if a Create packet data protocol (PDP) Context request is from a roamer, use the **gprs mcc mnc** command in global configuration mode. To return to the default values, use the **no** form of this command.

gprs mcc *mcc-num* **mnc** *mnc-num* **[trusted]**

no gprs mcc *mcc-num* **mnc** *mnc-num* **[trusted]**

Syntax Description

mcc *mcc-num*	3-digit decimal number for the MCC. The valid range for the MCC is 000 to 999. The default value is 000, which is not a valid code.
mnc *mnc-num*	2- or 3-digit decimal number for the MNC. The valid range for the MNC is 00 to 999. The default value is 000, which is not a valid code.
trusted	Specifies that the MCC and MNC defined are those of a trusted PLMN. Up to 5 trusted PLMNs can configured as trusted.

Defaults

000—For both the MCC and MNC. A valid code must be a non-zero value.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU and the **trusted** keyword option added.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs mcc mnc** command as part of the configuration required on the GGSN to support creation of call detail records (CDRs) for roaming mobile subscribers, or to block roamers from being able to Create PDP Context requests.

The MCC and MNC together identify a GPRS/UMTS public land mobile network (PLMN). The values you configure using the **gprs mcc mnc** command without the **trusted** keyword option specified are those of the home PLMN ID - the PLMN to which the GGSN belongs. Only one home PLMN can be defined for a GGSN at a time. The GGSN uses the values that you configure in this command to compare with the international mobile subscriber identity (IMSI) in a Create PDP Context request.

The GGSN automatically specifies values of 000 for the MCC and MNC. However, you must configure non-zero values for both the MCC and MNC before you can enable the GGSN to create charging CDRs for roamers.

To properly issue the **gprs mcc mnc** command, you must specify both the **mcc** keyword with its argument and the **mnc** keyword with its argument. You cannot issue the command without specifying both keywords.

It is important that you configure the **gprs mcc mnc** and **gprs charging roamers** commands in their proper order. After you configure the MCC and MNC values, use the **gprs charging roamers** command to enable charging for roamers on the GGSN. You can change the MCC and MNC values by reissuing the **gprs mcc mnc** command.

Using the **gprs mcc mnc** command, you can also configure up to 5 “trusted” PLMNs by specifying the **trusted** keyword. A Create PDP Context request from a mobile subscriber in a trusted PLMN is treated the same as a Create PDP Context request from a mobile subscriber in the home PLMN.

To verify your configuration of these codes on the GGSN, use the **show gprs charging parameters** command.

Note To see a list of some established MCC and MNC codes, see the “Table of MCC and MNC Codes” appendix in the *Cisco GGSN Configuration Guide*. To find more information about MCC and MNC codes, see the ITU E.212 recommendation, *Identification Plan for Land Mobile Stations*.

Examples

The following example replaces the default values of 000 on the GGSN, and specifies an MCC code of 310 for the USA and an MNC code of 15 for the Bell South service provider:

```
gprs mcc 310 mnc 15
```

Related Commands

Command	Description
block-foreign-ms	Restricts GPRS access based on the mobile user’s home PLMN.
gprs charging roamers	Enables charging for roamers on the GGSN.
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs memory threshold

To prevent the gateway GPRS support node (GGSN) from draining processor memory during abnormal conditions (such as charging gateways [CGs] being down), use the **gprs memory threshold** command in global configuration mode to configure a memory threshold, that when reached, activates the memory protection feature on the GGSN.

gprs memory threshold *threshold*

no gprs memory threshold

Syntax Description

threshold	Memory threshold, that when fallen below enables the memory protection feature on the GGSN. Valid range is 0 to 1024.

Defaults

The default is 10% of the total memory available at the time GGSN services are enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)XB	This command was introduced.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU and changed to enabled by default.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

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

By default, the memory threshold is 10% of the total memory available at the time GGSN services are enabled using the **gprs ggsn service** global configuration command. You can use the **gprs memory threshold** global configuration command to configure the threshold according to the router and memory size.

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

- Rejects new Create packet data protocol (PDP) Context requests with the cause value “No Resource.”
- Drops any existing PDPs for which an update is received with the cause value “Management Intervention.”
- Drops any PDPs for which a volume trigger has occurred.

Examples

The following example sets the memory threshold to 50 KB:

```
gprs memory threshold 512
```

gprs ms-address exclude-range

To specify the IP address range(s) used by the GPRS/UMTS network, and thereby excluded from the mobile station (MS) IP address range, use the **gprs ms-address exclude-range** command in global configuration mode. To remove the specified range(s), use the **no** form of this command.

gprs ms-address exclude-range *start-ip end-ip*

no gprs ms-address exclude-range *start-ip end-ip*

Syntax Description

start-ip	IP address at the beginning of the range.
end-ip	IP address at the end of the range.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

An MS cannot have the same IP address as another GPRS network entity. Use the **gprs ms-address exclude-range** command to reserve certain IP address ranges for use by the GPRS/UMTS network, and to disallow these address ranges from use by an MS.

The **gprs ms-address exclude range** command verification is performed only for IP PDPs and does not apply to MS addresses assigned to virtual private networks (VPNs) or for PPP Regen or PPP PDP types.

During processing of a Create packet data protocol (PDP) Context request, the gateway GPRS support node (GGSN) verifies whether the IP address of an MS falls within the specified excluded range. If there is an overlap of the MS IP address with an excluded range, then the Create PDP Context request is rejected. This measure prevents duplicate IP addressing in the network.

You can configure up to 100 IP address ranges. A range can be one or more addresses. However, you can configure only one IP address range per command entry. To exclude a single IP address, you can repeat the IP address in the *start-ip* and *end-ip* arguments. IP addresses are 32-bit values.

Examples

Example 1

The following example specifies the IP address ranges used by the GPRS/UMTS network (which are thereby excluded from the MS IP address range):

```
gprs ms-address exclude-range 10.0.0.1 10.20.40.50
gprs ms-address exclude-range 172.16.150.200 172.30.200.255
gprs ms-address exclude-range 192.168.100.100 192.168.200.255
```

Example 2

The following example excludes an MS from using the IP address 10.10.10.1:

```
gprs ms-address exclude-range 10.10.10.1 10.10.10.1
```

Related Commands

Command	Description
show gprs ms-address exclude-range	Displays the IP address range(s) configured on the GGSN for the GPRS/UMTS network.

gprs plmn ip address

To specify the IP address range of a public land mobile network (PLMN), use the **gprs plmn ip address** command in global configuration mode.

gprs plmn ip address *start_ip end_ip* [**sgsn**]

no gprs plmn ip address *start_ip end_ip* [**sgsn**]

Syntax Description

start_ip	IP address at the beginning of the range.
end_ip	IP address at the end of the range.
sgsn	(Optional) Specifies that only the PLMN IP address ranges defined with the **sgsn** keyword specified be used to determine if an serving GPRS support node (SGSN) is located in a PLMN other than the gateway GPRS support node (GGSN).

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)YW	This command was introduced.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs plmn ip address** global configuration command to specify the IP address range of the PLMN.

The **gprs plmn ip address** command defines addresses that belong to a PLMN. To indicate that the addresses are SGSN addresses within the PLMN, issue the **gprs plmn ip address** command with the **sgsn** keyword option specified. This option is used by the charging for roamers feature (**gprs charging roamers** command).

When using the **gprs plmn ip address** command with the GGSN charging for roamers feature, depending on how the PLMN IP address ranges have been defined using the **gprs plmn ip address** *start_ip end_ip* [**sgsn**] command, the charging for roamers feature operates as follows:

- If no PLMN IP address ranges are configured using the **gprs plmn ip address** *start_ip end_ip* [**sgsn**] command, the GGSN generates CDRs for all initiated PDP contexts regardless of whether the GGSN and SGSN are located within the same PLMN.
- If a list of PLMN IP address ranges has been configured using the **gprs plmn ip address** *start_ip end_ip* [**sgsn**] command, and one or more of those ranges has been defined using the **sgsn** keyword, the GGSN uses those ranges defined with the **sgsn** keyword to determine whether an SGSN is located within the same PLMN.

  With this configuration, the following scenarios outline how the charging for roamers feature will function:

  – Mobile station 1 (MS1) is subscribed to PLMN1 and attaches to an SGSN in PLMN2. From PLMN2, MS1 initiates a packet data protocol (PDP) context with the GGSN in PLMN1. In this case, MS1 is a roamer, and the GGSN generates a call detail record (CDR) because it determines that the SGSN is located in a different PLMN.

  – MS1 is subscribed to PLMN1 and attaches to an SGSN in PLMN2. From PLMN2, MS1 initiates a PDP context with the GGSN in PLMN2. In this case, MS1 is not a roamer because the SGSN and GGSN are in the same PLMN. The GGSN does not create a CDR.

Configuration Guidelines

To enable charging for roamers on the GGSN, you should first define a set of IP address ranges for a PLMN using the **gprs plmn ip address** command.

It is important that you configure the **gprs plmn ip address** and **gprs charging roamers** commands in their proper order. After you configure the IP address range for a PLMN, use the **gprs charging roamers** command to enable charging for roamers on the GGSN. You can change the IP address range by reissuing the **gprs plmn ip address** command.

To verify your configuration, use the **show gprs charging parameters** command to see if the charging for roamers feature is enabled. To verify your PLMN IP address ranges, use the **show gprs plmn ip address** command.

Examples

The following example specifies the IP address range of a PLMN:

```
gprs plmn ip address 10.0.0.1 10.20.40.50
```

Related Commands

Command	Description
gprs charging roamers	Enables charging for roamers on the GGSN.
show gprs plmn ip address	Displays a list of IP address ranges defined for the PLMN.

gprs pcscf

To configure a group of P-CSCF addresses and enter P-CSCF group configuration mode, use the **gprs pcscf** command in global configuration mode. To disable the P-CSCF server group, issue the **no** form of this command.

gprs pcscf *group-name*

no gprs pcscf *group-name*

Syntax Description

group-name	Specifies the name of a P-CSCF server group and enters P-CSCF group configuration mode.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)XB	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

Use the **gprs pcscf** command to define a P-CSCF server group for P-CSCF Discovery and enter P-CSCF group configuration mode.

The GGSN can be configured to return a list of preconfigured Proxy Call Session Control Function (P-CSCF) server addresses for an APN when it receives a Create PDP Context request that contains a "P-CSCF Address Request" field in the PCO.

The MS sets the P-CSCF Address Request field of the PCO in the Activate PDP Context request. This request is forwarded to the GGSN in the Create PDP Context request from the SGSN. Upon receiving, the GGSN returns all the P-CSCF addresses configured for the APN in the "P-CSCF Address" field of the PCO.

If a Create PDP Context Request does not contain the P-CSCF address request field in the PCO, or if no P-CSCF addresses are preconfigured, the Create PDP Context Response will not return any P-CSCF addresses. An error message will not be generated and the Create PDP Context Request will be processed.

To configure the P-CSCF Discovery support, you must preconfigure P-CSCF server groups on the GGSN using the **gprs pcscf** command and configure P-CSCF server groups for an APN using the **pcscf** access-point configuration command.

Note The order of the addresses returned in the "P-CSCF Address Field" of the PCO is the same as the order in which they are defined in the P-CSCF server group and the groups are associated with the APN.

Examples

The following example configures a P-CSCF group identified as “groupA”:

```
gprs pcscf groupA
```

Related Commands

Command	Description
pcscf	Assigns a P-CSCF server group to an APN.
server	Specifies the IP address of a P-CSCF server you want to include in the P-CSCF server group.
show gprs access-point	Displays information about access points on the GGSN.
show gprs pcscf	Displays a summary of the P-CSCF groups configured on the GGSN.

gprs qos bandwidth-pool

Command	Description
pcscf	Assigns a P-CSCF server group to an APN.
server	Specifies the IP address of a P-CSCF server you want to include in the P-CSCF server group.
show gprs access-point	Displays information about access points on the GGSN.
show gprs pcscf	Displays a summary of the P-CSCF groups configured on the GGSN.

To create or modify a Call Admission Control (CAC) bandwidth pool that can be attached to one or more APNs, use the **gprs qos bandwidth-pool** command in global configuration mode. To delete the bandwidth pool, use the **no** form of this command.

gprs qos bandwidth-pool *pool-name*

no gprs qos bandwidth-pool *pool-name*

Syntax Description

pool-name	Name of the bandwidth pool (between 1 and 40 characters).

Defaults

No bandwidth pools are configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The CAC feature ensures that required network resources are available for real-time data traffic (such as voice, video, etc.). The CAC feature consists of two functions: maximum quality of service (QoS) authorization using CAC maximum QoS policies and bandwidth management.

The CAC bandwidth management function ensures that there is sufficient bandwidth for real-time packet data protocol (PDP) contexts during the PDP context activation and modification process.

The CAC feature uses user-defined bandwidth pools to negotiate and reserve bandwidth. In these pools, you define the total bandwidth allocated to that pool and then allocate a percentage of that bandwidth to each traffic class.

In the following example, bandwidth pool (pool A) has been created with 100000 kbps allocated to it. Additionally, a percentage of that 100000 kbps of bandwidth has been allocated to each traffic class, creating four “traffic class-based” bandwidth pools.

```
gprs bandwidth-pool A
  bandwidth 100000
  traffic-class conversational percent 40
  traffic-class streaming percent 30
  traffic-class interactive percent 20
  traffic-class background percent 10
```

Note The CAC feature requires that Universal Mobile Telecommunications System (UMTS) QoS is enabled on the GGSN. For more information on configuring UMTS QoS on the GGSN, see the *GGSN Release 6.0 Configuration Guide*.

Once a bandwidth pool is allocated for a traffic class, it cannot be borrowed by the other sub pools allocated for the different traffic classes. The request is only admitted within the bandwidth pool to which the traffic class belongs.

Use the **gprs qos bandwidth-pool** command to create or modify a CAC bandwidth pool and apply the bandwidth pool to one or more APNs using the **bandwidth-pool** access point configuration command.

Examples

The following example creates a bandwidth pool named “pool a”:

```
gprs qos bandwidth pool a
```

Related Commands

Command	Description
bandwidth	Defines the total bandwidth, in kilobits per second, for a bandwidth pool. Valid values are 1 to 4292967295.
bandwidth-pool	Enables the CAC bandwidth management function and applies a bandwidth pool to an APN.
gprs qos bandwidth-pool	Creates or modifies a bandwidth pool.
traffic-class	Allocates bandwidth pool bandwidth to a specific traffic class.

gprs qos cac-policy

To create or modify a Call Admission Control (CAC) maximum quality of service (QoS) policy that can be attached to one or more access point names (APNs), and enter CAC maximum QoS policy configuration mode, use the **gprs qos cac-policy** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs qos cac-policy *policy-name*

no gprs qos cac-policy *policy-name*

Syntax Description

policy-name	Name of the maximum QoS policy (between 1 and 40 characters).

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The CAC feature on the gateway GPRS support node (GGSN) ensures that required network resources are available for real-time data traffic such as voice and video. CAC is applied at the APN and consists of two functions: maximum QoS authorization and bandwidth management.

The CAC maximum QoS authorization function ensures that the QoS requested by a Create packet data protocol (PDP) Context does not exceed the maximum QoS configured within an APN. Using a *CAC maximum QoS policy*, you define certain QoS parameters within a policy and attach the policy to an APN. The CAC maximum QoS policy limits the QoS requested by the PDP during its creation and modification process.

Use the **gprs qos cac-policy** command to create or modify a CAC maximum QoS policy and apply the policy to an APN using the **cac-policy** access point configuration command.

Note The CAC feature requires that Universal Mobile Telecommunications System (UMTS) QoS has been configured. For information on configuring UMTS QoS, see the *GGSN Release 6.0 Configuration Guide*.

Once you have entered policy configuration mode using the **gprs qos cac-policy** command, you can configure the following QoS parameters in a policy and apply the policy to an APN:

- Maximum number of active PDP contexts (**maximum pdp-context** command)
- Maximum bit rate (**mbr traffic-class** command)
- Guaranteed bit rate (**gbr traffic-class** command)
- Maximum traffic class (**maximum traffic-class** command)
- Traffic handling priority (**maximum traffic-class** command with **priority** option)
- Delay class (**maximum delay-class** command)
- Peak throughput class (**maximum peak-throughput** command)

Examples

The following example creates a CAC maximum QoS policy named “policy a”:

```
gprs qos cac-policy a
```

Related Commands

Command	Description
cac-policy	Enables the maximum QoS policy function of the CAC feature and applies a policy to an APN.
gbr traffic-class	Specifies the maximum guaranteed bit rate (GBR) that can be allowed in uplink and downlink directions for real-time classes (conversational and streaming) at an APN.
maximum delay-class	Defines the maximum delay class for R97/R98 (GPRS) QoS that can be accepted.
maximum peak-throughput	Defines the maximum peak throughput for R97/R98 (GPRS) QoS that can be accepted.
maximum pdp-context	Specifies the maximum number PDP contexts that can be created for a particular APN.
maximum traffic-class	Defines the highest traffic class that can be accepted.
mbr traffic-class	Specifies the maximum bit rate (MBR) that can be allowed for each traffic class in both directions (downlink and uplink).

gprs qos default-response requested

To specify that the gateway GPRS support node (GGSN) sets its default quality of service (QoS) values in the response message exactly as requested in the Create packet data protocol (PDP) Context request message, use the **gprs qos default-response requested** command in global configuration mode. To return to the default QoS, use the **no** form of this command.

gprs qos default-response requested

no gprs qos default-response requested

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled. The GGSN sets its QoS default to the best-effort class.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)	This command was introduced.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The **gprs qos default-response requested** command is useful only when canonical QoS is not configured on the GGSN. Canonical QoS is enabled using the **gprs qos map canonical-qos** command.

When canonical QoS is not enabled, and the **gprs qos default-response requested** command has not been configured on the GGSN, the GGSN always sets its QoS values to best-effort in the response message.

Examples

The following example enables the GGSN to set its QoS values in the response message according to the QoS values requested in the Create PDP Context request message:

```
gprs qos default-response requested
```

Related Commands

Command	Description
gprs qos map canonical-qos	Enables mapping of GPRS QoS categories to a canonical QoS method that includes best-effort, normal, and premium QoS classes.

gprs qos map canonical-qos

To enable mapping of general packet radio service (GPRS) quality of service (QoS) categories to a canonical QoS method that includes best-effort, normal, and premium QoS classes, use the **gprs qos map canonical-qos** command in global configuration mode. To disable canonical mapping, use the **no** form of this command.

gprs qos map canonical-qos

no gprs qos map canonical-qos

Syntax Description

This command has no arguments or keywords.

Defaults

Canonical QoS mapping is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **qprs qos map canonical-qos** command to map GPRS QoS into the following canonical categories: best effort, normal, and premium.

Examples

The following example shows canonical QoS mapping enabled:

```
qos map canonical-qos
```

Related Commands

Command	Description
gprs canonical-qos best-effort bandwidth-factor	Specifies the bandwidth factor to be applied to the canonical best-effort QoS class.
gprs canonical-qos gsn-resource-factor	Specifies a value that is used by the GGSN to calculate the QoS level provided to mobile users.
gprs canonical-qos map tos	Specifies a QoS mapping from the canonical QoS classes to an IP ToS category.
gprs canonical-qos premium mean-throughput-deviation	Specifies a mean throughput deviation factor that the GGSN uses to calculate the allowable data throughput for QoS.

gprs qos map delay

To enable mapping of general packet radio service (GPRS) quality of service (QoS) categories to delay QoS classes, use the **gprs qos map delay** command in global configuration mode. To disable delay mapping, use the **no** form of this command.

gprs qos map delay

no gprs qos map delay

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs qos map delay** command to enable QoS delay mapping on the gateway GPRS support node (GGSN). To map the QoS delay classes (class 1, class 2, class 3, and best effort) to IP type of service (ToS) categories, use the **gprs delay-qos map tos** command.

Examples

The following example enables delay QoS mapping:

```
gprs qos map delay
```

Related Commands

Command	Description
gprs delay-qos map tos	Specifies a QoS mapping from the delay QoS classes to an IP ToS category.
gprs qos default-response requested	Configures the GGSN to set its default QoS mapping values in a Create PDP Context response which has no QoS mapping selected.

gprs qos map umts

To enable universal mobile telecommunication system (UMTS) quality of service (QoS) on the gateway GPRS support node (GGSN), use the **gprs qos map umts** command in global configuration mode. To disable this mapping and return to the default QoS mapping, use the **no** form of this command.

gprs qos map umts

no gprs qos map umts

Syntax Description

This command has no arguments or keywords.

Defaults

UMTS QoS mapping is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)YW	This command was introduced.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs qos map umts** command to enable UMTS QoS mapping.

Examples

The following example enables UMTS traffic QoS mapping:

```
gprs qos map umts
```

Related Commands

Command	Description
gprs umts-qos map traffic-class	Specifies a QoS mapping from the UMTS traffic classes to a DiffServ PHB group.
gprs umts-qos map diffserv-phb	Assigns a DSCP to a DiffServ PHB group.
gprs umts-qos dscp unmodified	Specifies that the subscriber datagram be forwarded through the GTP path without modifying its DSCP.

Command	Description
show gprs qos status	Displays QoS statistics for the GGSN.
show gprs umts-qos map traffic-class	Displays UMTS QoS mapping information.

gprs radius attribute chap-challenge

To specify that the CHAP challenge always be included in the Challenge Attribute field (and not in the Authenticator field) in an Access-Request to the Remote Access Dial-In User Service (RADIUS) server, use **gprs radius attribute chap-challenge global configuration** command in global configuration mode. To disable, use the **no** form of this command.

gprs radius attribute chap-challenge

no gprs radius attribute chap-challenge

Syntax Description

This command has no arguments or keywords.

Defaults

If the CHAP challenge length is 16 bytes, it is sent in the Authenticator field of an Access-Request. If it is greater than 16 bytes, it is sent in the Challenge Attribute field.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)	This command was introduced.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs radius attribute chap-challenge** command when configuring RADIUS security on the GGSN.

When the **gprs radius attribute chap-challenge** command is configured, the CHAP challenge is always sent in the Challenge Attribute field of an Access-Request to the RADIUS server and not in the Authenticator field. When the command is not configured, the CHAP challenge is sent in the Authenticator field unless the challenge exceeds 16 bytes, in which case, it is sent in the Challenge Attribute field of the Access-Request.

Examples

The following example configures the CHAP challenge to always be sent in an Access Request to the RADIUS server:

```
gprs radius attribute chap-challenge
```

Related Commands

show gprs gtp pdp-context	Displays a list of the currently active PDP contexts (mobile sessions).

gprs radius attribute quota-server ocs-address

To configure the GGSN to send the Online Charging Server (OCS) IP address (received in an Access-Accept response from a RADIUS server) in the csg:quota server attribute in Accounting-Start messages, use **gprs radius attribute quota-server ocs-address** global configuration command in global configuration mode. To disable this configuration, use the **no** form of this command.

gprs radius attribute quota-server ocs-address

no gprs radius attribute quota-server ocs-address

Syntax Description

This command has no arguments or keywords.

Defaults

The GGSN sends its own IP address in the csg:quota server field.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)XB2	This command was introduced.
12.4(9)XG	This command was integrated into Cisco IOS Release 12.4(9)XG.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **gprs radius attribute quota-server ocs-address** command to configure the GGSN to send the IP address and port of an external OCS (that has been received in the conditional “csg:quota_server” attribute in an Access-Accept response for a prepaid subscriber from the RADIUS server), in Accounting-Start messages to the CSG.

When the **gprs radius attribute quota-server ocs-address** command has been configured, the CSG can interface directly with an external OCS to which it has a GTP’ interface. This external OCS will function as the quota server for the prepaid users, providing an alternate online billing solution than the one provided by the GGSN, interacting with Diameter/DCCA, functioning as the quota server for prepaid users.

When the **gprs radius attribute quota-server ocs-address** command is configure, the GGSN functions as the quota server for just postpaid users. The GGSN does not generate enhance G-CDRs for prepaid users, however, it does continue to generate G-CDRs for them.

For more information about the GGSN support for OCS address selection, see the Configuring Enhance Service-Aware Billing” chapter of the *GGSN Configuration Guide*.

Examples

The following configures the GGSN to send the IP address of an external OCS in the csg:quota server attribute in Accounting-Start messages for prepaid users:

```
gprs radius attribute quota-server ocs-address
```

Related Commands

show gprs gtp pdp-context	Displays a list of the currently active PDP contexts (mobile sessions).

gprs radius attribute session-timeout

To specify that the Session-Timeout (Attribute 27) field be included in a Remote Access Dial-In User Service (RADIUS) request, use the **gprs radius attribute session-timeout** command in global configuration mode. To disable, use the **no** form of this command.

gprs radius attribute session-timeout

no gprs radius attribute session-timeout

Syntax Description

This command has no arguments or keywords.

Defaults

Attribute 27 is not included.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs radius attribute session-timeout** command to configure the Session-Timeout (Attribute 27) field be included in a Remote Access Dial-In User Service (RADIUS) request.

The GGSN stores the attribute value received in Access-Accept packets sent by the AAA server and terminates the PDP context upon expiration of the time. You can configure the number of seconds the GGSN allows a session to be active before terminating the session at the global level (**gprs gtp pdp-context timeout session** command) and at the access-point level (**gtp pdp-context timeout session** command.

Examples

The following example configures Attribute 27 to always be sent in an Access Request to the RADIUS server:

```
gprs radius attribute session-timeout
```

Related Commands

Command	Description
gprs gtp pdp-context timeout session	Specifies the time, in seconds, that the GGSN allows a session to be active at any access point before terminating the session.
gtp pdp-context timeout session	Specifies the time, in seconds, that a GGSN allows a session to be active at a particular APN before terminating the session.

gprs radius msisdn first-byte

To specify that the first byte of the mobile station ISDN (MSISDN) information element (IE) is included in a RADIUS request, use the **gprs radius msisdn first-byte** command in global configuration mode. To remove the first byte from the MSISDN IE in a RADIUS request, use the **no** form of this command.

gprs radius msisdn first-byte

no gprs radius msisdn first-byte

Syntax Description

This command has no arguments or keywords.

Defaults

The first byte is not included.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)	This command was introduced.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs radius msisdn first-byte** command when configuring RADIUS security on the gateway GPRS support node (GGSN).

The first octet of an MSISDN IE using E.164 addressing is 91 in hexadecimal, that is, 10010001. In this 91 code, the 1 is the extension bit, 001 is the international number, and 0001 indicates E.164 numbering.

Examples

The following example specifies that the first byte of the MSISDN IE is included in a RADIUS request:

```
gprs radius msisdn first-byte
```

gprs redundancy

To enable GPRS tunneling protocol session redundancy (GTP-SR) on a gateway GPRS support node (GGSN), use the **gprs redundancy** command in global configuration mode. To disable GTP-SR, use the **no** form of this command.

gprs redundancy

no gprs redundancy

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)YJ	This command was introduced.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs redundancy** command to enable GTP-SR on a GGSN.

Cisco GGSN Release 5.1 and later supports Active/Standby, 1-to-1 inter-device GTP-SR. GTP-SR enables two GGSNs to appear as one network entity and ensures that continuous service is provided to mobile subscribers in the event one of the GGSNs fails.

In a GTP-SR implementation, the Active GGSN establishes and terminates packet data protocol (PDP) sessions and sends required stateful data to the Standby GGSN. To stay current on the states of active PDP sessions, the Standby GGSN receives the stateful data sent by the Active GGSN. As soon as the Standby GGSN detects that the Active GGSN has failed, it becomes active and assumes the responsibilities of the Active GGSN.

Before GTP-SR can be enabled on two redundant GGSNs, a GTP-SR inter-device infrastructure must be configured. For information on configuring a inter-device infrastructure, see the "Configuring GTP Session Redundancy" chapter of the *Cisco GGSN Release 6.0 Configuration Guide*.

Examples

The following example enables GTP-SR on a GGSN:

```
gprs redundancy
```

Related Commands

Command	Description
clear gprs redundancy statistics	Clears statistics related to GTP-SR.
gprs redundancy charging sync-window cdr rec-seqnum	Configures the window size used to determine when the CDR record sequence number needs to be synchronized to the Standby GGSN.
gprs redundancy charging sync-window gtpp seqnum	Configures the window size used to determine when the GTP' sequence number needs to be synchronized to the Standby GGSN.
show gprs redundancy	Displays statistics related to GTP-SR.

gprs redundancy charging sync-window cdr rec-seqnum

To configure the window size used to determine when the call detail record (CDR) record sequence number needs to be synchronized to the Standby gateway GPRS support node (GGSN), use the **gprs redundancy charging sync-window cdr rec-seqnum** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs redundancy charging sync-window cdr rec-seqnum size

no gprs redundancy charging sync-window cdr rec-seqnum size

Syntax Description

size	Configures the window size used to determine when the CDR record sequence number needs to be synchronized.Valid range is 1 to 20.

Defaults

10

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)YJ	This command was introduced.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs redundancy charging sync-window cdr rec-seqnum** command to configure the window size used to determine when the record sequence number needs to be synchronized.

The record sequence number is used by the charging gateway to detect duplicate CDRs associated with a PDP context. To minimize the amount of data being synchronized to the Standby GGSN, the record sequence number is not synchronized each time a CDR is closed. Instead, a window threshold for the record sequence number is synchronized each time a CDR closes. The current value of the record sequence number and the record number last synchronized for a PDP context is checked, and if the difference is the value configured for the window size using the **gprs redundancy charging sync-window cdr rec-seqnum** global configuration command, the current record sequence number is synchronized to the Standby GGSN.

When a Standby GGSN becomes the Active GGSN, it starts from the last value synchronized, plus the window size.

Examples

The following example configures a window size of 15:

```
gprs redundancy charging sync-window cdr rec-seqnum 15
```

Related Commands

Command	Description
clear gprs redundancy statistics	Clears statistics related to GTP-SR.
gprs redundancy	Enables GTP-SR on a GGSN.
gprs redundancy charging sync-window gtpp seqnum	Configures the window size used to determine when the GTP' sequence number needs to be synchronized to the Standby GGSN.
show gprs redundancy	Displays statistics related to GTP-SR.

gprs redundancy charging sync-window gtpp seqnum

To configure the window size used to determine when the GTP' sequence number needs to be synchronized to the Standby gateway GPRS support node (GGSN), use the **gprs redundancy charging sync-window gtpp seqnum** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs redundancy charging sync-window gtpp seqnum *size*

no gprs redundancy charging sync-window gtpp seqnum *size*

Syntax Description

size	Configures the window size used to determine when the GTP' sequence number needs to be synchronized. Valid range is 5 to 65535. **Note** Since a GGSN can transmit 128 GTP packets without any acknowledgement, we recommend that you configure the window size to be greater than 128.

Defaults

10000

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)YJ	This command was introduced.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs redundancy charging sync-window gtpp seqnum** command to configure the window size used to determine when the GTP' sequence number needs to be synchronized.

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

To minimize the amount of data being synchronized to the Standby GGSN, the GTP' sequence number is not synchronized each time a CDR is closed. Instead, a window threshold for the GTP' sequence number is synchronized each time a CDR message is sent. The current value of the GTP' sequence number and the gtpp sequence number last synchronized for a PDP context is checked and if the difference is the value configured for the window size (using the **gprs redundancy charging sync-window gtpp seqnum** global configuration command), the current GTP prime sequence number is synchronized to the Standby GGSN.

When a Standby GGSN becomes the Active GGSN, it starts from the last value synchronized plus the window size.

Examples

The following example configures the window size for the GTP' sequence number synchronization to be 120:

```
gprs redundancy charging sync-window gtpp seqnum 120
```

Related Commands

Command	Description
clear gprs redundancy statistics	Clears statistics related to GTP-SR.
gprs redundancy	Enables GTP-SR on a GGSN.
gprs redundancy charging sync-window cdr rec-seqnum	Configures the window size used to determine when the CDR record sequence number needs to be synchronized to the Standby GGSN.
show grs redundancy	Displays all GTP-SR related information.

gprs service-aware

To enable service-aware billing on the gateway GPRS support node (GGSN), use the **gprs service-aware** command in global configuration mode. To disable the support, use the **no** form of this command

gprs service-aware

no gprs service-aware

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs service-aware** global configuration command to enable service-aware billing on the on the GGSN.

Note Service-aware billing must be enabled before configuring other enhanced service-aware billing features on the GGSN. These features include the GGSN-to-CSG interface, the GGSN-to-Diameter/DCCA interface, and support of enhanced service-level G-CDRs.

Examples

The following configuration example enables service-aware billing on a GGSN:

```
gprs service-aware
```

Related Commands

Command	Description
service-aware	Enables service-aware billing for a particular access point.

gprs service-mode

To configure the global service-mode state of a gateway GPRS support node (GGSN), use the **gprs service-mode** command in global configuration mode.

gprs service-mode {operational | maintenance}

no gprs service-mode {operational | maintenance}

Syntax Description

operational	Specifies that the service-mode state of the GGSN is operational.
maintenance	Specifies that the service-mode state of the GGSN is maintenance.

Defaults

Operational.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs service-mode** command to place the global service-mode state of a GGSN in maintenance mode.

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

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

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

Examples

The following example places a GGSN in maintenance mode:

```
gprs service-mode maintenance
```

Related Commands

Command	Description
service-mode	Configures the service-mode state of an APN.
gprs service-mode test imsi	Configures a test user for which you can Create PDP Contexts to test an APN configuration.
show gprs service-mode	Displays the current global service mode state of the GGSN and the last time it was changed.

gprs service-mode test imsi

To configure a test user for which you can Create PDP Contexts to test an APN configuration, use the **gprs service-mode test imsi** command in global configuration mode. To remove the test user configuration, use the **no** form of this command.

gprs service-mode test imsi *imsi-value*

no gprs service-mode test imsi *imsi-value*

Syntax Description

imsi-value	International Mobile Subscriber Identity (IMSI) value for which PDP contexts are to be created.

Defaults

No test user is configured on the GGSN.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs service-mode test imsi** command to configure a test user for which Create PDP Contexts will be created to test configurations.

Only one test user can be configured per GGSN.

Note PDP context creation from a test user is only supported while a GGSN is in operational mode.

Examples

The following example creates a test user with the IMSI 211F111130000000:

```
gprs service-mode test imsi 211F111130000000
```

Related Commands

Command	Description
gprs service-mode	Configures the service-mode state of a GGSN.
service-mode	Configures the service-mode state of an APN.
show gprs service-mode	Displays the current global service mode state of the GGSN and the last time it was changed.

gprs slb mode

To define the Cisco IOS SLB operation mode for gateway GPRS support node (GGSN)-IOS SLB messaging, use the **gprs slb mode** command in global configuration mode.

gprs slb mode {dispatched | directed}

Syntax Description

dispatched	Specifies that the Cisco IOS SLB is operating in dispatched mode.
directed	Specifies that the Cisco IOS SLB is operating in directed server NAT mode.

Defaults

Dispatched

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs slb mode** command to defined the Cisco IOS SLB mode of operation when configuring GGSN-IOS SLB messaging.

GGSN-IOS SLB Messaging CAC Failure Notification Support

When configuring support for GGSN-IOS SLB messaging CAC failure notifications, if Cisco IOS SLB is operating in dispatched mode, the virtual server that forwarded the Create PDP Context request to the GGSN is known to the GGSN, and the GGSN can send the CAC failure notification directly to that server. Therefore, only the **gprs slb notify** command is required to enable GGSN-SLB messaging on the GGSN.

However, if the Cisco IOS SLB is functioning in directed server NAT mode, the virtual server is not known to the GGSN. Therefore, a list of virtual servers that the GGSN should notify when a CAC failure occurs must be defined on the GGSN using the **gprs slb vserver** global configuration command and the Cisco IOS SLB mode of operation must be defined using the **gprs slb mode** global configuration command.

Note When configuring support for GGSN-IOS SLB messaging CAC failure notifications when the Cisco IOS SLB is functioning in directed server NAT mode, the **gprs slb mode** and **gprs slb vserver** global configuration commands are required.

GGSN-IOS SLB Messaging Delete Notification Support

When configuring support for GGSN-IOS SLB messaging delete notifications (GTP IMSI sticky database support), the Cisco IOS SLB operation mode must be defined using the **gprs slb mode** command and a list of virtual servers that the GGSN should send delete notifications must be defined on the GGSN using the **gprs slb vserver** global configuration command.

For complete information on configuring GGSN-IOS SLB messaging, refer to the "Configuring Messaging from the GGSN to the Cisco IOS SLB" section of the "Configuring Load Balancing on the GGSN" chapter for the *GGSN Configuration Guide*.

Examples

The following example defines Cisco IOS SLB to be in directed server NAT mode:

```
gprs slb mode directed
```

Related Commands

Command	Description
clear gprs slb statistics	Clears Cisco IOS SLB statistics.
gprs slb notify	Configures the GGSN to send notifications to the Cisco IOS SLB when a specific condition exists that affects a session forwarded by the Cisco IOS SLB.
gprs slb vserver	Configures the Cisco IOS SLB virtual servers to be notified by the GGSN when the specific condition defined using the **gprs slb notify** command occurs.
show gprs slb detail	Displays Cisco IOS SLB related information, such as the operation mode, virtual servers addresses, and statistics.
show gprs slb mode	Displays the Cisco IOS SLB mode of operation defined on the GGSN.
show gprs slb statistics	Displays Cisco IOS SLB statistics.
show gprs slb vservers	Displays the list of defined Cisco IOS SLB virtual servers.

gprs slb notify

To enable the gateway GPRS support node (GGSN) to notify the Cisco IOS Server Load Balancing (SLB) when a specific condition occurs, use the **gprs slb notify** global configuration command. To disable GGSN-IOS SLB messaging, issue the **no** form of this command.

gprs slb notify {cac-failure | session-deletion}

no gprs slb notify {cac-failure | session-deletion}

Syntax Description

cac-failure	Specifies that the GGSN notify the Cisco IOS SLB when a universal mobile telecommunications system (UMTS) quality of server (QoS) call admission control (CAC) or canonical QoS failure has caused a Create packet data protocol (PDP) Context request to be rejected.
session-deletion	Configures the GGSN to send a delete notification message to the Cisco IOS SLB when the last PDP context associated with an international mobile subscriber identity (IMSI) is deleted.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into the Cisco IOS Release 12.3(14)YU and the **session-deletion** keyword option was added.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs slb notify** command to enable GGSN-IOS SLB messaging.

The GGSN-IOS SLB messaging function enables you to configure the GGSN to notify the Cisco IOS SLB when a certain condition exists that affects a session forwarded by the Cisco IOS SLB. The notification also instructs the Cisco IOS SLB on how to react to the condition.

There are two types of GGSN-IOS SLB notifications that can be configured using the **gprs slb notify** command—CAC failure notifications and delete notifications (for GTP IMSI sticky database support).

CAC Failure Notifications

When support for CAC failure notifications is configured on the GGSN and the Cisco IOS SLB, when a Create PDP Context request is rejected by the GGSN because of a CAC failure, the GGSN notifies the Cisco IOS SLB that the failure has occurred, and instructs the Cisco IOS SLB to reassign the session to another GGSN in the server farm.

Note If the Cisco IOS SLB is functioning in directed server NAT mode, a list of virtual servers must be defined on the GGSN using the **gprs slb vserver** global configuration command, and the Cisco IOS SLB mode of operation must be defined using the **gprs slb mode** global configuration command.

Delete Notifications (GTP IMSI Sticky Database Support)

When support for delete notifications is configured on the GGSN and the Cisco IOS SLB, a sticky database entry is created on the Cisco IOS SLB when the first Create PDP Context request from a subscriber is received. When the last PDP context of that IMSI is deleted on the GGSN, the GGSN sends a delete notification to the Cisco IOS SLB that instructs the Cisco IOS SLB to remove the sticky entry from the database.

Note This configuration requires that the **virtual** virtual server configuration command be configured with the **service gtp** keywords specified.

For complete information on configuring GGSN-IOS SLB messaging, refer to the "Configuring Messaging from the GGSN to the Cisco IOS SLB" section of the "Configuring Load Balancing on the GGSN" chapter for the *GGSN Configuration Guide.*

Examples

Example 1

The following example configures the GGSN to notify the Cisco IOS SLB when a Create PDP Context request has been rejected because of a UMTS QoS CAC failure and the Cisco IOS SLB is functioning in dispatched mode.

On the GGSN:

```
gprs slb notify cac-failure
```

On the Cisco IOS SLB:

```
gtp notification cac 4
```

Example 2

The following example configures the GGSN to notify the Cisco IOS SLB when a Create PDP Context request has been rejected because of a UMTS QoS CAC failure and the Cisco IOS SLB is functioning in directed server NAT mode.

On the GGSN:

```
gprs slb mode directed
gprs slb notify cac-failure
gprs slb vserver 10.10.10.10
```

On the Cisco IOS SLB:

```
gtp notification cac 4
```

Example 3

The following example configures the GGSN to notify the Cisco IOS SLB (functioning in directed server NAT mode) when the last PDP context associated with a IMSI is deleted:

On the GGSN:

```
gprs slb mode directed
gprs slb notify session-deletion
gprs slb vserver 10.10.10.10
```

On the Cisco IOS SLB:

```
sticky gtp imsi group 1
```

Example 4

The following example configures the GGSN to notify the Cisco IOS SLB (functioning in dispatched mode) when the last PDP context associated with a IMSI is deleted:

On the GGSN:

```
gprs slb mode dispatched
gprs slb notify session-deletion
gprs slb vserver 10.10.10.10
```

On the Cisco IOS SLB:

```
sticky gtp imsi group 1
```

Related Commands

Command	Description
clear gprs slb statistics	Clears Cisco IOS SLB statistics.
gprs slb mode	Defines the Cisco IOS SLB operation mode.
gprs slb vserver	Configures the Cisco IOS SLB virtual servers to be notified by the GGSN when the specific condition defined using the **gprs slb notify** command occurs.
show gprs slb detail	Displays Cisco IOS SLB related information, such as the operation mode, virtual servers addresses, and statistics.
show gprs slb mode	Displays the Cisco IOS SLB mode of operation defined on the GGSN.
show gprs slb statistics	Displays Cisco IOS SLB statistics.
show gprs slb vservers	Displays the list of defined Cisco IOS SLB virtual servers.

gprs slb vserver

To configure the Cisco IOS SLB virtual server(s) to be notified by the gateway GPRS support node (GGSN) when the specfic type of condition defined using the **gprs slb notify** command occurs, use the **gprs slb vserver** command in global configuration mode. To remove a virtual server from the list, use the **no** form of this command.

gprs slb vserver *ip_address* [**next-hop ip** *ip-address* [**vrf** *name*]]

no slb vserver *ip_address* [**next-hop ip** *ip-address* [**vrf** *name*]]

Syntax Description

ip_address	IP address of the virtual server.
next-hop ip *ip-address*	(Optional) IP address of the next-hop that can be used to reach the virtual server.
vrf *name*	(Optional) Specifies VPN routing and forwarding instance.

Defaults

No virtual servers are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU and the **next hop** and **vrf** keyword options were added.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs slb vserver** global configuration command to defined a list of Cisco IOS SLB virtual servers to be notified by a GGSN when GGSN-IOS SLB messaging is enabled.

For example, if Cisco IOS SLB is functioning in directed server NAT mode, the GGSN will send the notification to all the vservers in the list. However, only the vserver that is processing the PDP context will react to the notification. The other vservers will ignore the notification.

This command is used in conjunction with the **gprs slb notify** and the **gprs slb mode** global configuration commands.

Note This command is not required when configuring support for GGSN-IOS SLB messaging CAC failure notifications when the Cisco IOS SLB is functioning in dispatched mode.

For complete information on configuring GGSN-IOS SLB messaging, refer to the “Configuring Messaging from the GGSN to the Cisco IOS SLB” section of the “Configuring Load Balancing on the GGSN” chapter for the *GGSN Configuration Guide.*

Examples

Example 1

The following example adds a GTP server with the IP address 172.10.10.10 to the list of virtual servers to be notified by the GGSN:

```
gprs slb vserver 172.10.10.10
```

Related Commands

Command	Description
clear gprs slb statistics	Clears Cisco IOS SLB statistics.
gprs slb mode	Defines the Cisco IOS SLB operation mode.
gprs slb notify	Configures the GGSN to send notifications to the Cisco IOS SLB when a certain condition exists that affects a session forwarded by the Cisco IOS SLB.
show gprs slb detail	Displays Cisco IOS SLB related information, such as the operation mode, virtual servers addresses, and statistics.
show gprs slb mode	Displays the Cisco IOS SLB mode of operation defined on the GGSN.
show gprs slb statistics	Displays Cisco IOS SLB statistics.
show gprs slb vservers	Displays the list of defined Cisco IOS SLB virtual servers.

gprs throughput interval

To configure the intervals at which the throughput data is collected for APNs, use the **gprs throughput interval** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs throughput interval *interval1 interval2*

no gprs throughput interval *interval1 interval2*

Syntax Description

interval	Number of seconds that the GGSN waits before collecting throughput data.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs throughput interval** command to configure the intervals at which the GGSN will collect throughput data for APNs.

Examples

The following example configures the GGSN to collect throughput data every 5 minutes (300 seconds):

```
gprs throughput interval 300
```

Related Commands

Command	Description
show gprs access-point throughput statistics	Displays throughput statistics for access points on a GGSN.

gprs umts-qos dscp unmodified

To specify that the subscriber datagram be forwarded through the GTP path without modifying its DSCP, use the **gprs umts-qos dscp unmodified** command in global configuration mode. To remove this specification and enable the DSCP to be re-marked with the DSCP assigned to the traffic class during the PDP context creation, use the **no** form of this command.

gprs umts-qos dscp unmodified [**up** | **down** | **all**]

no gprs umts-qos dscp unmodified [**up** | **down** | **all**]

Syntax Description

up	(Optional) Specifies subscriber datagram DSCPs in the uplink GTP path.
down	(Optional) Specifies subscriber datagram DSCPs in the downlink GTP path.
all	(Optional) Specifies subscriber datagram DSCPs in all GTP paths.

Defaults

The DSCP in the subscriber datagram is re-marked with the DSCP assigned to the traffic class during the PDP context creation.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)YW	This command was introduced.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs umts-qos dscp unmodified** command to configure the GGSN to forward subscriber datagram DSCPs through the GTP path without modifying the DSCP.

Examples

The following example sets subscriber datagrams in the uplink GTP path to retain their DSCPs:

```
gprs umts-qos dscp unmodified up
```

Related Commands

Command	Description
gprs qos map umts	Enables UMTS QoS on the GGSN.
gprs umts-qos map traffic-class	Specifies a QoS mapping from the UMTS traffic classes to a differentiated services (DiffServ) per-hop behavior (PHB) group.
gprs umts-qos map diffserv-phb	Assigns a differentiated services code point (DSCP) to a DiffServ PHB group.
show gprs qos status	Displays QoS statistics for the GGSN.
show gprs umts-qos map traffic-class	Displays UMTS QoS mapping information.

gprs umts-qos map diffserv-phb

To assign a differentiated services code point (DSCP) to a DiffServ PHB group, use the **gprs umts-qos map diffserv-phb** command in global configuration mode. To set the specified DSCP to the default DiffServ PHB group, use the **no** form of this command.

gprs umts-qos map diffserv-phb *diffserv-phb-group* [*dscp1*] [*dscp2*] [*dscp3*]

no gprs umts-qos map diffserv-phb

Syntax Description

diffserv-phb-group	Specifies the DiffServ PHB group. The PHB groups are: • signalling-class • ef-class • af1-class • af2-class • af3-class • af4-class • best-effort
dscp1	Required for all classes. Specifies one of 64 DSCP values from 0 to 63. The DSCP value corresponds to drop precedence 1.
dscp2	(Optional for AF classes only) Specifies one of 64 DSCP values from 0 to 63. The DSCP value corresponds to drop precedence 2.
dscp3	(Optional for AF classes only) Specifies one of 64 DSCP values from 0 to 63. The DSCP value corresponds to drop precedence 3.

Defaults

The default DSCP value associated with the PHB class is used.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)YW	This command was introduced.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

For the Assured Forwarding (AF) PHB group, you can specify up to three DSCP values for each drop precedence. The signalling, EF, and best-effort classes do not have drop precedence, so only the first DSCP value is used. If you enter a value for the *dscp2* or *dscp3* arguments for these classes, it is ignored.

Drop precedence indicates the order in which a packet will be dropped when there is congestion on the network.

Table 1 shows the default DSCP values for each PHB group.

Table 2 Default DSCP Values per PHB Group

PHB	DSCP
Signalling	5?
EF	101110 (46)
AF11	001010 (10)
AF12	001100 (12)
AF13	001110 (14)
AF21	010010 (18)
AF22	010100 (20)
AF23	010110 (22)
AF31	011010 (26)
AF32	011100 (28)
AF33	011110 (30)
AF41	100010 (34)
AF42	100100 (36)
AF43	100110 (38)
Best effort	000000 (0)

Examples

The following example assigns a DSCP value of 31 to the EF class and three DSCP values to AF class2 of 51, 52, and 53:

```
gprs umts-qos map diffserv-phb ef-class 31
gprs umts-qos map diffserv-phb af-class2 51 52 53
```

Related Commands

Command	Description
gprs qos map umts	Enables UMTS QoS on the GGSN.
gprs umts-qos map traffic-class	Specifies a QoS mapping from the UMTS traffic classes to a differentiated services (DiffServ) per-hop behavior (PHB) group.
gprs umts-qos dscp unmodified	Specifies that the subscriber datagram be forwarded through the GTP path without modifying its DSCP.
show gprs qos status	Displays QoS statistics for the GGSN.
show gprs umts-qos map traffic-class	Displays UMTS QoS mapping information.

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.

gprs umts-qos map traffic-class

To specify a QoS mapping from the UMTS traffic classes to a differentiated services (DiffServ) per-hop behavior (PHB) group, use the **gprs umts-qos map traffic-class** command in global configuration mode. To remove a QoS mapping and set the specified traffic class to the default mapping, use the **no** form of this command.

gprs umts-qos map traffic-class *traffic-class diffserv-phb-group*

no gprs umts-qos map traffic-class

Syntax Description

traffic-class	Specifies the traffic class. The UMTS traffic classes are: • signalling • conversational • streaming • interactive • background
diffserv-phb-group	Specifies the DiffServ PHB group. The PHB groups are: • signalling-class • ef-class • af1-class • af2-class • af3-class • af4-class • best-effort

Defaults

You must enable UMTS QoS using the **gprs qos map umts** command before entering this command.

Note Use the **gprs umts-qos map traffic-class** command only if you want to use mapping values other than the defaults.

The default mapping values for the UMTS traffic classes are as follows:

- signalling traffic class to the signalling-class DiffServ PHB group
- conversational traffic class to the ef-class DiffServ PHB group
- streaming traffic class to the af2-class DiffServ PHB group
- interactive traffic class to the af3-class DiffServ PHB group
- background traffic class to the best-effort DiffServ PHB group

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)YW	This command was introduced.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs umts-qos map traffic-class** command to specify a mapping between various QoS UMTS traffic categories and the DiffServ PHB groups.

Examples

The following example specifies a QoS mapping from the UMTS traffic class conversational to the DiffServ PHB group af-class1:

```
gprs umts-qos map traffic-class conversational af1-class
```

Related Commands

Command	Description
gprs qos map umts	Enables UMTS QoS on the GGSN.
gprs umts-qos map diffserv-phb	Assigns a differentiated services code point (DSCP) to a DiffServ PHB group.
gprs umts-qos dscp unmodified	Specifies that the subscriber datagram be forwarded through the GTP path without modifying its DSCP.
show gprs qos status	Displays QoS statistics for the GGSN.
show gprs umts-qos map traffic-class	Displays UMTS QoS mapping information.

gtp pdp-context single pdp-session

To configure the gateway GPRS support node (GGSN) to delete the primary PDP context, and any associated secondary PDP contexts, of a *hanging* PDP session upon receiving a new create request from the same MS that shares the same IP address of the hanging PDP context, use the **gtp pdp-context single pdp-session** command in global configuration mode. To return to the default value, use the **no** form of this command.

gtp pdp-context single pdp-session [**mandatory**]

[**no**] **gtp pdp-context single pdp-session** [**mandatory**]

Syntax Description

mandatory	Specifies that the primary PDP context and any associated secondary PDP contexts be deleted regardless of the RADIUS user profile configuration.

Defaults

Create PDP Context requests that share the IP address of an existing PDP context for the same MS are rejected.

Command Modes

Access-point configuration

Command History

Release	Modification
12.3(8)XU2	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gtp pdp-context single pdp-session** command to configure the GGSN to delete the primary PDP context, and any associated secondary PDP contexts, of a *hanging* PDP session upon receiving a new create request from the same MS that shares the same IP address of the hanging PDP context.

A hanging PDP context is a PDP context on the GGSN whose corresponding PDP context on the SGSN has already been deleted for some reason.

When this condition occurs and the **gtp pdp-context single pdp-session** command is not configured, if on the same APN, the same MS sends a new Create PDP Context request that has a different NSAPI but has been assigned the same IP address used by the hanging PDP context, the GGSN rejects the new Create PDP Context request.

When the **gtp pdp-context single pdp-session** is configured on an APN, the single PDP session per MS feature is enabled and applies to all users for whom the "gtp-pdp-session=single-session" Cisco VSA has been defined in their RADIUS user profile. If the command is not configured, the feature is not enabled and does not apply to any user regardless of their RADIUS user profile configuration. If the command is configured with the **mandatory** keyword option specified, the feature is enabled and applies to all users on that APN regardless of their RADIUS user profile configuration.

Note This feature is supported on the Cisco 7200 series platform.

Examples

The following example configures the GGSN to delete the primary PDP context, and associated secondary PDP contexts, of a *hanging* PDP context when it receives a new Create PDP Context request that shares the same IP address:

```
gtp pdp-context single pdp-session
```

Related Commands

Command	Description
show gprs access-point	Displays information about access points on the GGSN.
show gprs pdp-context tid	Displays PDP contexts by tunnel ID. This value corresponds to the IMSI plus NSAPI and can be up to 16 numeric digits.

gtp pdp-context timeout idle

To specify the time, in seconds, that a gateway GPRS support node (GGSN) allows a session to be idle at a particular access point before terminating the session, use the **gtp pdp-context timeout idle** access-point configuration command in global configuration mode. To return to the default value, use the **no** form of this command.

gtp pdp-context timeout idle *interval* [**uplink**]

no gtp pdp-context timeout idle

Syntax Description

interval	Time, in seconds, that the GGSN allows a session to be idle at a particular access point before terminating the session. Specify a value between 30 and 4294967 seconds. The value 0 disables the session timeout feature.
uplink	(Optional) Enables the session idle timer in the uplink direction only. When the **uplink** keyword option is not specified, the session idle timer is enabled in both directions (uplink and downlink).

Defaults

259200 seconds (72 hours)

Command Modes

Access-point configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(8)XU1	This command was integrated into Cisco IOS Release 12.3(8)XU1 and the **uplink** keyword option was added.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

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

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

On the GGSN, the session idle timer can be configured globally and at the APN. The value configured at the APN level using the **gtp pdp-context timeout idle** access-point configuration command overrides the value configured globally using the **gprs gtp pdp-context timeout idle** global configuration command. The value configured in the user profile on the RADIUS server overrides the value configured at the APN.

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

You can disable the session idle timer for a particular user by configuring 0 as the session idle time duration in the user profile on the RADIUS server. If a user is authenticated by RADIUS, the session idle time cannot be disabled.

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

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

Examples

The following example shows configuring the GGSN to wait 18000 seconds before ending an idle session:

```
gtp pdp-context timeout idle 18000
```

Related Commands

Command	Description
gprs gtp pdp-context timeout idle	Specifies the time, in seconds, that a GGSN allows a session to be idle before terminating the session.
gprs gtp pdp-context timeout session	Specifies the time, in seconds, that the GGSN allows a session to be active before terminating the session.
gprs idle-pdp-context purge-timer	Specifies the time, in hours, that the GGSN waits before purging idle mobile sessions.
gtp pdp-context timeout session	Specifies the time, in seconds, that a GGSN allows a session to be active at a particular APN before terminating the session.
session idle-time	Specifies the time, in hours, that the GGSN waits before purging idle mobile sessions for an access point.
show gprs gtp pdp-context	Displays a list of the currently active PDP contexts (mobile sessions).

gtp pdp-context timeout session

To specify the time, in seconds, that a gateway GPRS support node (GGSN) allows a session to exist at a particular access point before terminating the session, use the **gprs gtp pdp-context timeout session** command in access-point configuration mode. To return to the default value, use the **no** form of this command.

gtp pdp-context timeout session *seconds*

no gtp pdp-context timeout session *seconds*

Syntax Description

seconds	Time, in seconds, that the GGSN allows a session to exist at a particular access point. Specify a value between 30 and 4294967 seconds.

Defaults

Disabled

Command Modes

Access-point configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

When enabled using the **gprs radius attribute session-timeout** command, the GGSN supports the RADIUS Session-Timeout (Attribute 27). The GGSN stores the attribute timeout value received in access-accept packets sent by the AAA server and when the duration of a session exceeds the duration configured as absolute session timer, the GGSN terminates the session and all PDP contexts belonging to the session (those with the same IMSI or MS address).

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

Note The active session timeout feature requires that the **gprs radius attribute session-timeout** command has been enabled.

On the GGSN, the absolute session timer can be configured globally and at the APN. The value configured at the APN level using the **gtp pdp-context timeout session** access-point configuration command overrides the value configured globally using the **gprs gtp pdp-context timeout session** global configuration command. The value configured in the user profile on the RADIUS server overrides the value configured at the APN.

Examples

The following example shows configuring the GGSN to wait 86400 seconds before ending a session:

```
gtp pdp-context timeout session 86400
```

Related Commands

Command	Description
gprs gtp pdp-context timeout idle	Specifies the time, in seconds, that a GGSN allows a session to be idle at any access point before terminating the session.
gprs gtp pdp-context timeout session	Specifies the time, in seconds, that the GGSN allows a session to be active at any access point before terminating the session.
gprs idle-pdp-context purge-timer	Specifies the time, in hours, that the GGSN waits before purging idle mobile sessions.
gtp pdp-context timeout idle	Specifies the time, in seconds, that a GGSN allows a session to be idle at a particular APN before terminating the session.
session idle-time	Specifies the time, in hours, that the GGSN waits before purging idle mobile sessions for an access point.
show gprs gtp pdp-context	Displays a list of the currently active PDP contexts (mobile sessions).

gtp response-message wait-accounting

To configure the gateway GPRS support node (GGSN) to wait for a RADIUS accounting response before sending a Create PDP Context response to the SGSN, for Create PDP Context requests received at a particular APN, use the **gtp response-message wait-accounting** command in access-point configuration mode. To configure the GGSN to send a Create PDP Context response to the SGSN after sending a RADIUS start accounting message to the RADIUS server (without waiting for a response from the RADIUS accounting server), use the **no** form of this command.

gtp response-message wait-accounting

no gtp response-message wait-accounting

Syntax Description

This command has no arguments or keywords.

Defaults

The GGSN sends a Create PDP Context response to the SGSN after sending a RADIUS start accounting message to the RADIUS accounting server. The GGSN does not wait for a RADIUS accounting response from the RADIUS accounting server.

Command Modes

Access-point configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gtp response-message wait-accounting** command to configure the GGSN to wait for a RADIUS accounting response from the RADIUS accounting server, before sending a Create PDP Context response to the SGSN.

If the GGSN does not receive a response from the RADIUS accounting server when you have configured the **gtp response-message wait-accounting** command, then the GGSN rejects the PDP context request.

The GGSN supports configuration of RADIUS response message waiting at both the global and access-point configuration levels. You can minimize your configuration by specifying the configuration that you want to support across most APNs, at the global configuration level. Then, at the access-point

configuration level, you can selectively modify the behavior that you want to support at a particular APN. Therefore, at the APN configuration level, you can override the global configuration of RADIUS response message waiting.

To configure the GGSN to wait for a RADIUS accounting response as the default behavior for all APNs, use the **gprs gtp response-message wait-accounting** global configuration command. To disable this behavior for a particular APN, use the **no gtp response-message wait-accounting** access-point configuration command.

To verify whether RADIUS response message waiting is enabled or disabled at an APN, you can use the **show gprs access-point** command and observe the value reported in the wait_accounting output field.

Examples

The following examples show only a partial configuration of the GGSN, to highlight those commands related to implementing RADIUS response message waiting. Additional configuration statements are required to complete a full configuration of the GGSN.

Example 1

The following example configures the GGSN to wait for an accounting response from the RADIUS server before sending a Create PDP Context response to the SGSN, for PDP context requests at access-point 1:

```
aaa new-model
!
aaa group server radius foo
 server 10.2.3.4
 server 10.6.7.8
!
aaa authentication ppp foo group foo
aaa authorization network default group radius
aaa accounting exec default start-stop group foo
!
gprs access-point-list gprs
 access-point 1
  access-mode non-transparent
  access-point-name www.pdn1.com
  aaa-group authentication foo
  gtp response-message wait-accounting
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

Example 2

The following example globally configures the GGSN to wait for a RADIUS accounting response from the RADIUS server before sending a Create PDP Context response to the SGSN. The GGSN waits for a response for PDP context requests received across all access points, except access-point 1. RADIUS response message waiting has been overridden at access-point 1 using the **no gtp response-message wait-accounting** command:

```
aaa new-model
!
aaa group server radius foo
 server 10.2.3.4
 server 10.6.7.8
!
aaa authentication ppp foo group foo
aaa authorization network default group radius
aaa accounting exec default start-stop group foo
```

```
!
gprs access-point-list gprs
 access-point 1
  access-mode non-transparent
  access-point-name www.pdn1.com
  aaa-group authentication foo
  no gtp response-message wait-accounting
  exit
 access-point 2
  access-mode non-transparent
  access-point-name www.pdn2.com
  aaa-group authentication foo
!
gprs gtp response-message wait-accounting
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

Related Commands

Command	Description
gprs gtp response-message wait-accounting	Configures the GGSN to wait for a RADIUS accounting response before sending an activate PDP context request to the SGSN, for Create PDP Context requests received across all access points.
show gprs access-point	Displays information about access points on the GGSN.

gtp update qos-fail delete

To configure the GGSN to delete a PDP context for this APN if a GGSN-initiated QoS update fails, use the **gtp update qos-fail delete** command in global configuration mode. To return to the default value, use the **no** form of the command.

gtp update qos-fail delete

no gtp update qos-fail delete

Syntax Description

This command has no arguments or keywords.

Defaults

PDP contexts are not deleted.

Command Modes

Access point configuration

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use this command to configure the GGSN to generate a Delete PDP Context request when a GGSN-initiated Update PDP Context Request for a QoS update fails.

The Acct Stop record generated by the GGSN indicates the update failure.

This configuration applies when the Update PDP Context Response from the SGSN, initiated for a QoS change, times out after n3 tries or the Cause value is a value other than “Request Accepted.”

Note If this command is not configured, the action configured globally using the **gprs gtp update qos-fail delete** command is used.

Examples

The following is an example:

```
Router(access-point-config)# gtp update qos-fail dele
```

Related Commands

Command	Description
gprs gtp update qos-fail delete	Configures the GGSN to delete PDP contexts when GGSN-initiated QoS updates fail.

interface

To specify the logical interface, by name, that the quota server will use to communicate with the Content Services Gateway (CSG), use the **interface** command in quota server configuration mode. To remove the interface, use the **no** form of this command

interface *interface-name*

no interface *interface-name*

Syntax Description

interface-name	Name of the interface that the quota server will use to communicate with the CSG.

Defaults

No default behavior or values.

Command Modes

Quota server configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **interface** quota server configuration mode command to specify the logical interface the quota server will use to communicate with the CSG.

We recommend that a loopback interface be used as the quota server interface.

If the path to the CSG is up, using the **no** form of this command will bring the path down. Therefore, ensure that you use the command carefully. It must be configured for proper quota server-to-CSG interworking.

Examples

The following configuration specifies the logical interface “loopback1” as the interface that the quota server will use to communicate with the CSG:

```
ggsn quota-server qs1
 interface loopback1
```

Related Commands .

Command	Description
clear ggsn quota-server statistics	Clears the quota server-related statistics displayed using the **show ggsn quota-server statistics** command.
csg-group	Associates the quota server to a CSG group that is to be used for quota server-to-CSG communication.

Command	Description
echo-interval	Specifies the number of seconds that the quota server waits before sending an echo-request message to the CSG.
ggsn quota-server	Configures the quota server process that interfaces with the CSG for enhanced service-aware billing.
n3-requests	Specifies the maximum number of times that the quota server attempts to send a signaling request to the CSG.
t3-response	Specifies the initial time that the quota server waits before resending a signaling request message when a response to a request has not been received.
show ggsn quota-server	Displays quota server parameters or statistics about the message and error counts.

ip (iSCSI interface)

To specify the IP address of an iSCSI target in the target profile on the GGSN, use the **ip** command in iSCSI interface configuration mode. To remove the IP address configuration, use the **no** form of the command.

ip *ip_address*

no ip *ip_address*

Syntax Description

ip_address	IP address of the SCSI target.

Command Default

No default behavior or values.

Command Modes

iSCSI interface configuration

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **ip** command to specify the IP address of the iSCSI target in an iSCSI target interface profile on the GGSN.

Only one target can be defined per profile.

Examples

The following example configures an iSCSI target interface profile with the name “targetA” to a SCSI target with the IP address “10.0.0.1.”

```
gprs iscsi targetA
  name iqn.2002-10.edu.abc.iol.iscsi.draft20-target:1
  ip 10.0.0.1
  port 3260
```

Related Commands

Command	Description
gprs iscsi	Configures the GGSN to use the specified iSCSI profile for record storage.
gprs iscsi target	Creates an iSCSI interface profile for an iSCSI target (or modifies an existing one), and enters iSCSI interface configuration mode.

Command	Description
name	Defines the name of the target.
port	Specifies the number of the TCP port on which to listen for iSCSI traffic.

ip iscsi target-profile

To create an iSCSI interface profile for an iSCSI target (or modify an existing profile) on the GGSN, and enter iSCSI interface configuration mode, use the **ip iscsi target-profile** command in global configuration mode. To remove the iSCSI interface profile, use the **no** form of the command.

ip iscsi target-profile *target_profile_name*

no ip iscsi target-profile *target_profile_name*

Syntax Description

target_profile_name	Name of the profile.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **ip iscsi target-profile** command to configure an iSCSI target profile on the GGSN. The iSCSI profile enables the GGSN to read/write to a remote iSCSI device (target) on a SAN via an iSCSI interface.

Multiple iSCSI profiles can be configured on the GGSN, however, only one target can be defined per profile, and only one profile at a time can be associated with the GGSN to use the iSCSI interface using the **gprs iscsi** global configuration command.

Note PSD and iSCSI cannot be configured on a GGSN at the same time, therefore, with GGSN Release 8.0 and later, PSD is not supported.

When in iSCSI target interface configuration mode, the following subconfigurations are supported:

- **default**—Sets a command to its defaults
- **exit**—Exits iSCSI target submode
- **ip**—IP address of target (Required)
- **name**—iSCSI target name (Required)
- **no**—Negate a command or set its defaults
- **port**—TCP port of target (Required)
- **record-store**—Record store

- **source-interface**—iSCSI source interface for packets to target
- **target-portal**—Target portal group
- **vrf**—VRF name associated with this target interface profile

Examples

The following example configures an iSCSI interface profile with the name “targetA” to use to store and retrieve charging DTRs (which can contain multiple G-CDRs) when a charging gateway is not available:

```
ip iscsi target-profile targetA
  name iqn.2002-10.edu.abc.iol.iscsi.draft20-target:1
  ip 10.0.0.1
  port 3260
```

Related Commands

Command	Description
gprs iscsi	Configures the GGSN to use the specified iSCSI profile for record storage.
ip	Specifies the IP address of the target on the SAN.
name	Specifies the name of a SCSI target in the iSCSI profile on the GGSN.
port	Specifies the number of the TCP port on which to listen for iSCSI traffic.

ip local pool

To configure a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface, use the **ip local pool** command in global configuration mode. To remove a range of addresses from a pool (the longer of the **no** forms of this command), or to delete an address pool (the shorter of the **no** forms of this command), use one of the **no** forms of this command.

ip local pool {**default** | *poolname*} [*low-ip-address* [*high-ip-address*]] [**group** *group-name*] [**cache-size** *size*] [**recycle delay** *seconds*]

no ip local pool *poolname low-ip-address* [*high-ip-address*]

no ip local pool {**default** | *poolname*}

Syntax Description

default	Creates a default local IP address pool that is used if no other pool is named.
poolname	Name of the local IP address pool.
low-IP-address [*high-IP-address*]	(Optional) First and, optionally, last address in an IP address range.
group *group-name*	(Optional) Creates a pool group.
cache-size *size*	(Optional) Sets the number of IP address entries on the free list that the system checks before assigning a new IP address. Returned IP addresses are placed at the end of the free list. Before assigning a new IP address to a user, the system checks the number of entries from the end of the list (as defined by the **cache-size** *size* option) to verify that there are no returned IP addresses for that user. The range for the cache size is 0 to 100. The default cache size is 20.
recycle delay *seconds*	(Optional) Indicates the time (in seconds) to hold an IP address in the local pool before making it available for reuse.

Defaults

No address pools are configured. Any pool created without the optional **group** keyword is a member of the base system group.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
11.3AA	This command was enhanced to allow address ranges to be added and removed.
12.1(5)DC	This command was enhanced to allow pool groups to be created.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and support was added for the Cisco 6400 node route processor 25v (NRP-25v) and Cisco 7400 platforms.
12.4(15)T	The **recycle delay** keyword and *seconds* argument were added.

Usage Guidelines

Use the **ip local pool** command to create one or more local address pools from which IP addresses are assigned when a peer connects. You may also add another range of IP addresses to an existing pool. To use a named IP address pool on an interface, use the **peer default ip address pool** interface configuration command. A pool name can also be assigned to a specific user using authentication, authorization, and accounting (AAA) RADIUS and TACACS functions.

If no named local IP address pool is created, a default address pool is used on all point-to-point interfaces after the **ip address-pool local** global configuration command is issued. If no explicit IP address pool is assigned, but pool use is requested by use of the **ip address-pool local** command, the special pool named "default" is used.

The optional **group** keyword and associated group name allows the association of an IP address pool with a named group. Any IP address pool created *without* the **group** keyword automatically becomes a member of a *base* system group.

The optional **recycle delay** keyword and its associated time indicates the time in seconds to hold the IP address from the pool before making it available for reuse.

An IP address pool name can be associated with only one group. Subsequent use of the same pool name, within a pool group, is treated as an extension of that pool, and any attempt to associate an existing local IP address pool name with a different pool group is rejected. Therefore, each use of a pool name is an implicit selection of the associated pool group.

Note To reduce the chances of inadvertent generation of duplicate addresses, the system allows creation of the special pool named "default" only in the base system group, that is, no group name can be specified with the pool name "default."

All IP address pools within a pool group are checked to prevent overlapping addresses; however, no checks are made between any group pool member and a pool not in a group. The specification of a named pool within a pool group allows the existence of overlapping IP addresses with pools in other groups, and with pools in the base system group, but not among pools within a group. Otherwise, processing of the IP address pools is not altered by their membership in a group. In particular, these pool names can be specified in **peer** commands and returned in RADIUS and AAA functions with no special processing.

IP address pools can be associated with Virtual Private Networks (VPNs). This association permits flexible IP address pool specifications that are compatible with a VPN and a VPN routing and forwarding (VRF) instance.

The IP address pools can also be used with the **translate** commands for one-step vty-async connections and in certain AAA or TACACS+ authorization functions. Refer to the chapter "Configuring Protocol Translation and Virtual Asynchronous Devices" in the *Cisco IOS Terminal Services Configuration Guide* and the "System Management" part of the *Cisco IOS Configuration Fundamentals Configuration Guide* for more information.

IP address pools are displayed with the **show ip local pool** EXEC command.

Examples

The following example creates a local IP address pool named "pool2," which contains all IP addresses in the range 172.16.23.0 to 172.16.23.255:

```
ip local pool pool2 172.16.23.0 172.16.23.255
```

The following example configures a pool of 1024 IP addresses:

```
no ip local pool default
ip local pool default 10.1.1.0 10.1.4.255
```

Note Although not required, it is good practice to precede local pool definitions with a **no** form of the command to remove any existing pool, because the specification of an existing pool name is taken as a request to extend that pool with the new IP addresses. If the intention is to extend the pool, the **no** form of the command is not applicable.

The following example configures multiple ranges of IP addresses into one pool:

```
ip local pool default 10.1.1.0 10.1.9.255
ip local pool default 10.2.1.0 10.2.9.255
```

The following examples show how to configure two pool groups and IP address pools in the base system group:

```
ip local pool p1-g1 10.1.1.1 10.1.1.50 group grp1
ip local pool p2-g1 10.1.1.100 10.1.1.110 group grp1
ip local pool p1-g2 10.1.1.1 10.1.1.40 group grp2
ip local pool lp1 10.1.1.1 10.1.1.10
ip local pool p3-g1 10.1.2.1 10.1.2.30 group grp1
ip local pool p2-g2 10.1.1.50 10.1.1.70 group grp2
ip local pool lp2 10.1.2.1 10.1.2.10
```

In the example:

- Group grp1 consists of pools p1-g1, p2-g1, and p3-g1.
- Group grp2 consists of pools p1-g2 and p2-g2.
- Pools lp1 and lp2 are not associated with a group and are therefore members of the base system group.

Note that IP address 10.1.1.1 overlaps groups grp1, grp2, and the base system group. Also note that there is no overlap within any group including the base system group, which is unnamed.

The following examples show configurations of IP address pools and groups for use by a VPN and VRF:

```
ip local pool p1-vpn1 10.1.1.1 10.1.1.50 group vpn1
ip local pool p2-vpn1 10.1.1.100 10.1.1.110 group vpn1
ip local pool p1-vpn2 10.1.1.1 10.1.1.40 group vpn2
ip local pool lp1 10.1.1.1 10.1.1.10
ip local pool p3-vpn1 10.1.2.1 10.1.2.30 group vpn1
ip local pool p2-vpn2 10.1.1.50 10.1.1.70 group vpn2
ip local pool lp2 10.1.2.1 10.1.2.10
```

The examples show configuration of two pool groups, including pools in the base system group, as follows:

- Group vpn1 consists of pools p1-vpn1, p2-vpn1, and p3-vpn1.
- Group vpn2 consists of pools p1-vpn2 and p2-vpn2.
- Pools lp1 and lp2 are not associated with a group and are therefore members of the base system group.

Note that IP address 10.1.1.1 overlaps groups vpn1, vpn2, and the base system group. Also note that there is no overlap within any group including the base system group, which is unnamed.

The VPN needs a configuration that selects the proper group by selecting the proper pool based on remote user data. Thus, each user in a given VPN can select an address space using the pool and associated group appropriate for that VPN. Duplicate addresses in other VPNs (other group names) are not a concern, because the address space of a VPN is specific to that VPN.

In the example, a user in group vpn1 is associated with some combination of the pools p1-vpn1, p2-vpn1, and p3-vpn1, and is allocated addresses from that address space. Addresses are returned to the same pool from which they were allocated.

The following example configures a recycle delay of 30 seconds to hold IP addresses in the pool before making them available for reuse:

```
ip local pool default 10.1.1.0 10.1.9.255 recycle delay 30
```

Related Commands

Command	Description
debug ip peer	Displays additional output when IP address pool groups are defined.
ip address-pool	Enables an address pooling mechanism used to supply IP addresses to dial in asynchronous, synchronous, or ISDN point-to-point interfaces.
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.
show ip local pool	Displays statistics for any defined IP address pools.
translate lat	Translates a LAT connection request automatically to another outgoing protocol connection type.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection type.

ip vrf forwarding

To associate a Virtual Private Network (VPN) routing/forwarding instance (VRF) with a Diameter peer, use the **ip vrf forwarding** command in Diameter peer configuration mode. To remove the VRF configuration, use the **no** form of this command

ip vrf forwarding *name*

no ip vrf forward

Syntax Description

name	Name assigned to a VRF.

Defaults

The default is the global routing table.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **ip vrf** forwarding command to associate a VRF with a Diameter peer**.**

Examples

The following example shows how to link a VRF to Diameter peer “dcca1”:

```
Router(config)# diameter peer dcca1
Router(config-dia-peer)# ip vrf forwarding vpn1
```

Related Commands .

Command	Description
address ipv4	Configures the IP address of the Diameter peer host.
destination host	Configures the Fully Qualified Domain Name (FQDN) of the Diameter peer
destination realm	Configures the destination realm (domain name) in which the Diameter host is located.
diameter peer	Defines the Diameter peer (server) and enters diameter peer configuration mode.
security	Configures the security protocol to use for the Diameter peer-to-peer connection.
source interface	Configures the interface to use to connect to the Diameter peer.
timer	Configures Diameter base protocol timers for peer-to-peer communication.
transport	Configures the transport protocol to use to connect with the Diameter peer.

ip-access-group

To specify access permissions between an MS and a PDN through the gateway GPRS support node (GGSN) at a particular access point, use the **ip-access-group** command in access-point configuration mode. To disable the input access list, use the **no** form of this command.

ip-access-group *access-list-number* {**in** | **out**}

no ip-access-group *access-list-number* {**in** | **out**}

Syntax Description

access-list-number	Number of an access list that has been set up using the **access-list** command.
in	The specified access list controls access from the PDN to the mobile station.
out	The specified access list controls access from the mobile station to the PDN.

Defaults

No access list is enforced.

Command Modes

Access-point configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **ip-access-group** command to specify an access list that indicates whether users are given or denied permission to access the mobile station from the PDN through the GGSN using a specified access point.

Examples

The following example grants access-list 101 inbound access to the mobile station from the PDN through the GGSN:

```
access-list 101 permit ip 10.0.0.2 0.255.255.255 any
interface virtual-template 1
 ip unnumber loopback 1
 no ip directed-broadcast
 encapsulation gtp
 gprs access-point-list abc
!
gprs access-point-list abc
 access-point 1
  access-point-name gprs.somewhere.com
  dhcp-server 10.100.0.3
  ip-access-group 101 in
  exit
!
```

ip-address-pool

To specify a dynamic address allocation method using IP address pools for the current access point, use the **ip-address-pool** command in access-point configuration mode. To return to the default value, use the **no** form of this command.

ip-address-pool {**dhcp-proxy-client** | **radius-client** | **local** *pool-name* | **disable**}

no ip-address-pool {**dhcp-proxy-client** | **radius-client** | **local** *pool-name* | **disable**}

Syntax Description

dhcp-proxy-client	The access-point IP address pool is allocated using a DHCP server.
radius-client	The access-point IP address pool is allocated using a RADIUS server.
local	The access-point IP address pool is allocated using a locally configured address pool.
disable	Disables dynamic address allocation for this access point.

Defaults

The global setting specified with the **gprs default ip-address-pool** command is used. The default value for the global configuration command is that IP address pools are disabled.

Command Modes

Access-point configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB and the **local** option was added.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

You can specify an IP allocation method for an access point in two ways:

- Enter access-point configuration mode and use the **ip-address-pool** command to specify an IP address allocation method for the current access point.
- Specify a global value for the IP address pool by issuing the **gprs default ip-address-pool** command. In that case, you do not need to specify an address-pool method for the specific access point.

If you specify **dhcp-proxy-client** as the method for allocating IP addresses, then you must configure a DHCP server for IP address allocation. You can do this at the global configuration level using the **gprs default-dhcp server** command, or at the access point level using the **dhcp-server** command.

If you specify **radius-client** as the method for allocating IP addresses, then you must configure a RADIUS server for IP address allocation, configure AAA on the GGSN, and configure AAA server groups globally on the GGSN or at the access point. For more information about configuring RADIUS on the GGSN, refer to the Usage Guidelines section for the **aaa-group** and **gprs default aaa-group** commands.

Note Configuring a local IP address pool under an APN (using the **ip-address-pool local** access-point configuration command) improves the PDP context activation rate as the number of PDP contexts increases.

Examples

The following example configures DHCP as the IP address pool allocation method for access-point 1 and specifies that the other access points use the global default, which is specified as RADIUS:

```
aaa new-model
!
aaa group server radius foo
 server 10.2.3.4
 server 10.6.7.8
aaa group server radius foo1
 server 10.10.0.1
!
aaa authentication ppp foo group foo
aaa authentication ppp foo group foo1
aaa authorization network default group radius
aaa accounting exec default start-stop group foo
aaa accounting network foo1 start-stop group foo1
!
interface Loopback0
 ip address 10.88.0.1 255.255.255.255
!
interface virtual-template 1
 ip unnumber Loopback0
 no ip directed-broadcast
 encapsulation gtp
 gprs access-point-list abc
!
gprs access-point-list abc
 access-point 1
  access-point-name gprs.pdn1.com
  ip address-pool dhcp-proxy-client
  aggregate auto
  dhcp-server 10.100.0.3
  dhcp-gateway-address 10.88.0.1
  exit
!
```

```
 access-point 2
  access-point-name gprs.pdn2.com
  access-mode non-transparent
  aaa-group authentication foo
  exit
!
gprs default ip-address-pool radius-client
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.10.0.1 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

Related Commands

Command	Description
dhcp-server	Specifies a primary (and backup) DHCP server to allocate IP addresses to MS users entering a particular PDN access point.
gprs default dhcp-server	Specifies a default DHCP server from which the GGSN obtains IP address leases for mobile users.
gprs default ip-address-pool	Specifies a dynamic address allocation method using IP address pools for the GGSN.
aaa-group	Specifies an AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN.
gprs default aaa-group	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN

ip probe path

To enable route probe support on an APN, use the **ip probe path** command in access-point configuration mode. To return to the default, use the **no** form of this command.

ip probe path *ip_address* **protocol udp [port** *port* **ttl** *ttl***]**

no ip probe path *ip_address* **protocol udp [port** *port* **ttl** *ttl***]**

Syntax Description

ip_address	IP address to which the GGSN is to send a probe packet for each PDP context successfully created.
protocol udp	Specifies UDP.
port *port*	(Optional) UDP destination port.
ttl *ttl_value*	(Optional) IP time-to-live (TTL) value for outgoing packet.

Defaults

Disabled

Command Modes

Access-point configuration

Command History

Release	Modification
12.3(2)XB1	This command was introduced.
12.3(8)XU	This command was incorporated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **ip probe path** access-point configuration command to enable the GGSN to send a probe packet to a specific destination for each PDP context that is successfully established.

An example of how to use this feature is when a firewall load balancer (FWLB) is being used in the network. If the **ip probe path** command is configured, when a PDP context is established, the GGSN sends a probe packet the FWLB. This enables the FWLB to create an entry for the PDP context even if there is no upstream packet from the MS. Once an entry is created, the FWLB can forward any downstream packet from the network for the MS to the appropriate GGSN without depending on the MS to send the packet first.

Note If an APN is mapped to a VRF, the route probe packet will go through the VRF routing table.

ipv6 (access point)

To configure an access point to support IPv6 packet data protocol (PDP) contexts, exclusively or in addition to IPv4 PDP contexts, use the **ipv6** command in access point configuration mode. To disable the support of IPv6 PDPs on the access point, use the **no** form of this command.

ipv6 [**enable** | **exclusive**]

no ipv6 [**enable** | **exclusive**]

Syntax Description

enable	Configures an access point to support both IPv6 PDP and IPv4 PDP contexts.
exclusive	Configures an access point to allow only IPv6 PDP contexts.

Defaults

IPv6 is disabled (by default, only IPv4 PDPs are supported on an access point).

Command Modes

Access point configuration

Command History

Release	Modification
12.4(9)XG	This command was introduced.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **ipv6 enable** command to configure an access point to support both IPv6 and IPv4 PDP contexts, or, optionally, specify the **exclusive** keyword option to configure the access point to support only IPv6 PDP contexts. (If an access point is configured to support IPv6 PDPs exclusively, IPv4 PDPs are rejected by the access point).

Note IPv6 support on a gateway GPRS support node (GGSN) access point requires that a tunnel for IPv6 traffic has been configured on the supervisor engine. Tunneling encapsulates IPv6 packets in IPv4 packets for delivery across an IPv4 infrastructure. By using tunnels, you can communicate with isolated IPv6 networks without upgrading the IPv4 infrastructure between them. For information on tunneling IPv6 traffic, refer to the *Cisco IOS IPv6 Configuration Guide*.

Note On the GGSN, VPN routing and forwarding (VRF) is not supported for IPv6 PDPs. Therefore, if an access point on which VRF is enabled is configured to support IPv6 PDPs (via the **ipv6** command), the IPv4 PDPs are routed in the VRF, but the IPv6 PDPs are routed in the global routing table.

Examples

The following example enables the support of both IPv4 and IPv6 PDP on access point 1.

```
Router(config)# access-point 1
Router(access-point-config)# ipv6 enable
```

Related Commands

Command	Description
ipv6 base-template	Specifies the base virtual template interface (containing IPv6 routing advertisements (RA) parameters), that the access point copies when creating a virtual subinterface for an IPv6 PDP context.
ipv6 dns primary	Specifies the address of an IPv6 DNS (primary and secondary) to be sent in IPv6 to create PDP context responses on an access point.
ipv6 ipv6-access-group	Specifies IPv6 access permissions on an access point.
ipv6 ipv6-address-pool	Configures a dynamic IPv6 prefix allocation method on an access point.
ipv6 redirect	Redirects IPv6 traffic to an IPv6 external device.
ipv6 security verify	Enables the GGSN to verify the IPv6 source address of an upstream TPDU against the address previously assigned to an MS,

ipv6 base-vtemplate

To specify the base virtual template interface (containing IPv6 routing advertisements [RA] parameters), that an accesss point copies when creating a virtual subinterface for an IPv6 packet data protocol (PDP) context, use the **ipv6 base-vtemplate** command in access point configuration mode. To remove the configuration, use the **no** form of this command.

ipv6 base-vtemplate *number*

no ipv6 base-vtemplate *number*

Syntax Description

number	Virtual template index number.

Defaults

No default behavior or values.

Command Modes

Access point configuration

Command History

Release	Modification
12.4(9)XG	This command was introduced.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

A virtual-access subinterface is created for each IPv6 PDP session established on the gateway GPRS support node (GGSN). The configurations for the virtual-access, such as routing advertisement timers, are cloned from the base vtemplate interface associated with an access point.

Use the **ipv6 base-vtemplate** command to associate a base virtual-template interface to an access point.

When a Create PDP Context request is receive, a virtual access subinterface is cloned from the base virtual template associated with the access point; and after the IPv6 virtual access subinterface is created, an IPv6 address is allocated as defined by the configuration under the access point. The Create PDP Context response is sent back only after the virtual-access subinterface is created, and authentication and address allocation are successfully completed.

Examples

The following example specifies access point 1 to use virtual template interface 10 as the base virtual template:

```
Router(config)# access-point 1
Router(access-point-config)# ipv6 base-vtemplate 10
```

Related Commands

Command	Description
ipv6	Configures an access point to support IPv6 PDP contexts, exclusively or in addition to IPv4 PDP contexts.
ipv6 dns primary	Specifies the address of an IPv6 DNS (primary and secondary) to be sent in IPv6 Create PDP Context responses on an access point.
ipv6 ipv6-access-group	Specifies IPv6 access permissions on an access point.
ipv6 ipv6-address-pool	Configures a dynamic IPv6 prefix allocation method on an access point.
ipv6 redirect	Redirects IPv6 traffic to an IPv6 external device.
ipv6 security verify	Enables the GGSN to verify the IPv6 source address of an upstream TPDU against the address previously assigned to an MS,

ipv6 dns primary

To specify the address of a primary (and backup) Domain Name System (DNS) to be sent in IPv6 Create packet data protocol (PDP) Context response on an access point, use the **ipv6 dns primary** command in access point configuration mode. To remove the IPv6 DNS address configuration from the access point configuration, use the **no** form of this command.

ipv6 dns primary *ipv6-address* [**secondary** *ipv6-address*]

no ipv6 dns primary *ipv6-address* [**secondary** *ipv6-address*]

Syntax Description

ipv6-address	IPv6 address of the primary IPv6 DNS.
secondary *ipv6-address*	(Optional) Specifies the IPv6 address of the backup IPv6 DNS.

Defaults

No default behavior or values.

Command Modes

Access point configuration

Command History

Release	Modification
12.4(9)XG	This command was introduced.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **ipv6 dns primary** command to specify the address of the primary (and backup) IPv6 DNS at the access point level.

This feature benefits address-allocation schemes which have no mechanism for obtaining addresses. Also, for a RADIUS-based allocation scheme, this feature prevents the operator from having to configure a DNS for each user profile.

The DNS address can come from the RADIUS server or local access point name (APN) configuration. The criterion for selecting the DNS address depends on the IP address allocation scheme configured under the APN.

Depending on the configuration, the criterion for selecting the IPv6 DNS address is as follows:

7. RADIUS-based IP address allocation scheme—A DNS address returned from the RADIUS server (in Access-Accept responses) is used. If the RADIUS server does not return a DNS address, the local APN configuration is used.
8. Static IP addresses—A local APN configuration is used.

Note The gateway GPRS support node (GGSN) sends DNS addresses in the Create PDP Context response only if the mobile station (MS) is requesting the DNS address in the protocol configuration option (PCO) information element (IE).

Examples

The following example specifies a primary IPv6 DNS and a secondary IPv6 DNS for access point 2:

```
access-point 2
 access-point-name xyz.com
 ipv6 enable
 ipv6 base-vtemplate
 ipv6 dns primary 3001::99 secondary 4001::99
 exit
```

Related Commands

Command	Description
ipv6	Configures an access point to support IPv6 PDP contexts, exclusively or in addition to IPv4 PDP contexts.
ipv6 base-template	Specifies the base virtual template interface (containing IPv6 routing advertisements [RA] parameters), that the access point copies when creating a virtual subinterfaces for an IPv6 PDP context.
ipv6 ipv6-access-group	Specifies IPv6 access permissions on an access point.
ipv6 ipv6-address-pool	Configures a dynamic IPv6 prefix allocation method on an access point.
ipv6 redirect	Redirects IPv6 traffic to an IPv6 external device.
ipv6 security verify	Enables the GGSN to verify the IPv6 source address of an upstream TPDU against the address previously assigned to an MS,

ipv6 ipv6-access-group

To specify IPv6 access permissions (uplink and downlink) at an access point, use the **ipv6 ipv6-access-group** command in access point configuration mode. To disable the access list, use the **no** form of this command.

ipv6 ipv6-access-group *access-list-name* [**up** | **down**]

no ipv6 ipv6-access-group *access-list-name* [**up** | **down**]

Syntax Description

access-list-name	Name of the access list configuration to apply to IPv6 payload packets.
up	Applies the filter to uplink packets.
down	Applies the filter to downlink packets.

Defaults

No access list is enforced.

Command Modes

Access point configuration

Command History

Release	Modification
12.4(9)XG	This command was introduced.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **ipv6 ipv6-access-group** command to specify an access list that indicates whether IPv6 users are given or denied permission using a specified access point.

Examples

The following example grants access-list IPv6acl inbound access to the mobile station from the PDN through the GGSN:

```
!
gprs access-point-list abc
 access-point 1
  access-point-name gprs.somewhere.com
  ipv6 ipv6-access-group IPv6acl up
  exit
!
```

Related Commands

Command	Description
ipv6	Configures an access point to support IPv6 PDP contexts, exclusively or in addition to IPv4 PDP contexts.
ipv6 access-list	Defines an IPv6 access list and places the router in IPv6 access list configuration mode.
ipv6 base-template	Specifies the base virtual template interface (containing IPv6 routing advertisements [RA] parameters), that the access point copies when creating a virtual subinterfaces for an IPv6 PDP context.
ipv6 dns primary	Specifies the address of an IPv6 DNS (primary and secondary) to be sent in an IPv6 Create PDP Context response on an access point.
ipv6 ipv6-address-pool	Configures a dynamic IPv6 prefix allocation method on an access point.
ipv6 redirect	Redirects IPv6 traffic to an IPv6 external device.
ipv6 security verify	Enables the GGSN to verify the IPv6 source address of an upstream TPDU against the address previously assigned to an MS,

ipv6 ipv6-address-pool

To configure a dynamic IPv6 prefix allocation method on an access point, use the **ipv6 ipv6-address-pool** command in access point configuration mode. To disable a dynamic prefix address allocation, use the **no** form of this command.

ipv6 ipv6-address-pool {**local** *pool-name* | **radius-client}**

no ipv6 ipv6-address-pool {**local** *pool-name* | **radius-client}**

Syntax Description

local *pool-name*	IPv6 prefixes are allocated from a locally configured IPv6 prefix pool.
radius-client	IPv6 prefixes are allocated from a RADIUS server.

Defaults

Disabled—a dynamic IPv6 prefix allocation method is not configured.

Command Modes

Access point configuration

Command History

Release	Modification
12.4(9)XG	This command was introduced.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

The IPv6 prefix can be obtained from a locally configured prefix pool, or a RADIUS server.

Use the **ipv6 ipv6-address-pool** command to configure the dynamic IPv6 prefix allocation method that you want an access point to use.

Note DHCPv6 is not support for IPv6 PDPs as an address allocation scheme.

Examples

The following example configures an access point to use a locally configured IPv6 prefix address pool named “localv6”:

```
Router(access-point-config)# ipv6 ipv6-address-pool local localv6
```

Related Commands

Command	Description
ipv6	Configures an access point to support IPv6 PDP contexts, exclusively or in addition to IPv4 PDP contexts.
ipv6 base-template	Specifies the base virtual template interface (containing IPv6 routing advertisements [RA] parameters), that the access point copies when creating a virtual subinterface for an IPv6 PDP context.
ipv6 dns primary	Specifies the address of an IPv6 DNS (primary and secondary) to be sent in an IPv6 Create PDP Context response on an access point.
ipv6 ipv6-access-group	Specifies IPv6 access permissions on an access point.
ipv6 local pool	Configures a local IPv6 prefix pool.
ipv6 redirect	Redirects IPv6 traffic to an IPv6 external device.
ipv6 security verify	Enables the GGSN to verify the IPv6 source address of an upstream TPDU against the address previously assigned to an MS,

ipv6 redirect

To redirect IPv6 traffic to an external IPv6 device, use the **ipv6 redirect** command in access point configuration mode. To disable the redirection of IPv6 traffic, use the **no** form of this command

ipv6 redirect [all | intermobile] *destination-ipv6-address*

no ipv6 redirect [all | intermobile] *destination-ipv6-address*

Syntax Description

all	Configures the gateway GPRS support node (GGSN) to redirect all IPv6 traffic to an external IPv6 device on an access point.
intermobile	Configures the GGSN to redirect mobile-to-mobile IPv6 traffic to an external IPv6 device.
destination-ipv6-address	IP address of the IPv6 external device to which you want to redirect IPv6 traffic.

Defaults

IPv6 traffic is not redirected.

Command Modes

Access point configuration

Command History

Release	Modification
12.4(9)XG	This command was introduced.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **ipv6 redirect** command to redirect IPv6 traffic on an access point to an external device (such as an external firewall) for verification.

Use the **ipv6 redirect** command with the **all** keyword specified, to redirect all IPv6 packets to a specified destination regardless of whether the destination address belongs to a mobile station (MS) on the same GGSN or not.

Use the **ipv6 redirect** command with the **intermobile** keyword specified, to redirect IPv6 mobile-to-mobile traffic to an external device (such as an external firewall) for verification. Only IPv6 packets for which the destination address belongs to an MS that is active on the same GGSN can be redirected. If the receiving MS does not have a packate data protocol (PDP) context in the same GGSN on which the sending MS PDP context is created, the packets are dropped.

Note On the Cisco 7600 series router platform, the traffic redirection feature requires that policy based routing (PBR) is configured on the Multilayer Switch Feature Card (MSFC) and incoming VLAN interface from the Cisco Service and Application Module for IP (SAMI), and that the next hop to route the packets is set using the set **ip next-hop** command.

Examples

The following example redirects all IPv6 traffic to an external device with the IPv6 address 3001::99.

```
ipv6 redirect all 3001::99
```

The following example redirects mobile-to-mobile IPv6 traffic to an external device with the IPv6 address 3001::99.

```
ipv6 redirect intermobile 3001::99
```

Related Commands

Command	Description
ipv6	Configures an access point to support IPv6 PDP contexts, exclusively or in addition to IPv4 PDP contexts.
ipv6 base-template	Specifies the base virtual template interface (containing IPv6 routing advertisements (RA) parameters), that the access point copies when creating a virtual sub-interfaces for an IPv6 PDP context.
ipv6 dns primary	Specifies the address of an IPv6 DNS (primary and secondary) to be sent in IPv6 create PDP context responses on an access point.
ipv6 ipv6-access-group	Specifies IPv6 access permissions on an access point.
ipv6 ipv6-address-pool	Configures a dynamic IPv6 prefix allocation method on an access point.
ipv6 security verify	Enables the GGSN to verify the IPv6 source address of an upstream TPDU against the address previously assigned to an MS,

ipv6 security verify source

To enable the gateway GPRS support node (GGSN) to verify the source address of an upstream transport protocol data unit (TPDU) against the address previously assigned to an IPv6 mobile station (MS), use the **ipv6 security verify source** command in access point configuration mode. To disable IPv6 source verification, use the **no** form of this command.

ipv6 security verify source

ipv6 no security verify source

Syntax Description

This command has no arguments or keywords.

Defaults

The GGSN does not verify source addresses.

Command Modes

Access point configuration

Command History

Release	Modification
12.4(9)XG	This command was introduced.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **ipv6 security verify source** command to configure the GGSN to verify the source address of an upstream TPDU against the address previously assigned to the IPv6 MS.

When the **ipv6 security verify source** command is configured on an access point, the GGSN verifies the source address of a TPDU before GPRS tunneling protocol (GTP) will accept and forward it. If the GGSN determines that the address differs from the address previously assigned to the MS, it drops the TPDU and counts it as an illegal packet in its PDP context and access point.

Configuring the **ipv6 security verify source** command in access point configuration mode protects the GGSN from faked user identities.

Note While the GGSN supports security source address verification only, the destination field is viewable with security.

Examples

The following example enables the verification of source IPv6 addresses received in upstream TPDUs:

```
ipv6 security verify source
```

Related Commands

Command	Description
ipv6	Configures an access point to support IPv6 PDP contexts, exclusively or in addition to IPv4 PDP contexts.
ipv6 base-template	Specifies the base virtual template interface (containing IPv6 routing advertisements [RA] parameters), that the access point copies when creating a virtual subinterface for an IPv6 PDP context.
ipv6 dns primary	Specifies the address of an IPv6 DNS (primary and secondary) to be sent in IPv6 create PDP context responses on an access point.
ipv6 ipv6-access-group	Specifies IPv6 access permissions on an access point.
ipv6 ipv6-address-pool	Configures a dynamic IPv6 prefix allocation method on an access point.
ipv6 redirect	Redirects IPv6 traffic to an IPv6 external device.

limit duration

To specify as a trigger condition in a charging profile, the time duration limit that when exceeded causes the gateway GPRS support node (GGSN) to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context, use the **limit duration** command in charging profile configuration mode. To return to the default value, use the **no** form of this command.

limit duration *number* **[reset]**

no limit duration *number* **[reset]**

Syntax Description

duration-value	A value, in minutes, between 5 and 4294967295 that specifies the time duration limit. The default is 1,048,576 bytes (1 MB).
reset	(Optional) Keyword to specify that the time trigger be reset if the CDR is closed by any other trigger. If the **reset** keyword is not specified, the time trigger will not be reset when the volume trigger expires (**limit volume** command), but it will be reset when any other trigger expires.

Defaults

Disabled

Command Modes

Charging profile configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **limit duration** charging profile configuration command to specify the time limit, that when exceeded, causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a PDP context.

For the box-level charging profile (profile 0 configured using the charging related global configuration commands), all triggers are reset by the expiration of another trigger. However, for charging profiles 1 through 15, the **reset** keyword option must be set for the **limit duration** and **limit volume** charging profile configuration commands for the expiration of any trigger to reset all other triggers.

If the **reset** keyword option is not specified when configuring the time trigger, the time trigger will not be reset when the volume trigger expires (**limit volume** command), but it will be reset when any other trigger expires.

Related Commands.

Command	Description
category	Identifies the subscriber category to which a charging profile applies.s
cdr suppression	Specifies that CDRs be suppressed as a charging characteristic in a charging profile.
charging profile	Associates a default charging profile to an access point.
content dcca profile	Defines a DCCA client profile in a GGSN charging profile.
content postpaid time	Specifies as a trigger condition for postpaid users in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
content postpaid validity	Specifies as a trigger condition in a charging profile, the amount of time quota granted to a postpaid user is valid.
content postpaid volume	Specifies as a trigger condition for postpaid users in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
content rulebase	Associates a default rule-base ID with a charging profile.
description	Specifies the name or a brief description of a charging profile.
gprs charging characteristics reject	Specifies that Create PDP Context requests for which no charging profile can be selected be rejected by the GGSN.
gprs charging container time-trigger	Specifies a global time limit, that when exceeded by a PDP context causes the GGSN to close and update the G-CDR for that particular PDP context.
gprs charging profile	Creates a new charging profile (or modifies an existing one), and enters charging profile configuration mode.
limit sgsn-change	Specifies, as a trigger condition in a charging profile, the maximum number of SGSN changes that can occur before closing and updating the G-CDR for a particular PDP context.
limit volume	Specifies, as a trigger condition in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
tariff-time	Specifies that a charging profile use the tariff changes configured using the **gprs charging tariff-time** global configuration command.

limit sgsn-change

To specify as a trigger condition in a charging profile, the maximum number of SGSN changes that can occur before closing and updating the G-CDR for a particular PDP context, use the **limit sgsn-change** command in charging profile configuration mode. To return to the default value, use the **no** form of this command.

limit sgsn-change *number*

no limit sgsn-change *number*

Syntax Description

number	Integer from 0 to 15. The default value is disabled.

Defaults

Disabled

Command Modes

Charging profile configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

A value of 0 means that a G-CDR is closed each time that a new SGSN begins handling the PDP context.

The command specifies the number of changes, not the number of SGSNs to be supported. The number of SGSNs supported is equal to 1 more than the change limit. For example, if the SGSN change limit is 2, the maximum number of SGSNs in the list before the GGSN closes the G-CDR is 3.

When you enable the **gprs charging cdr-option no-partial-cdr-generation** command, the GGSN creates any subsequent G-CDRs for the same PDP context request with the same fields in all G-CDRs and maintains sequence numbering.

If an SGSN change limit trigger is not configured when **gprs charging cdr-option no-partial-cdr-generation command** is configured, and a G-CDR is closed due to any other trigger (such as tariff times or QoS changes), the GGSN copies the last SGSN (the current SGSN) in the list in the new G-CDR. However, for charging releases prior to Release 4, by default, when the **gprs charging cdr-option no-partial-cdr-generation** command is configured and there is an SGSN change limit trigger configured either using the **gprs charging container sgsn-change-limit** global configuration or the **limit sgsn-change** charging profile configuration command, the CDR will not contain any SGSN address if it closed because of a non-SGSN-change trigger and there is no SGSN change. Therefore, to ensure that all CDR parameters are copied, including the SGSN list, specify the **all** keyword option when issuing the **gprs charging cdr-option no-partial-cdr-generation**.

Related Commands.

Command	Description
category	Identifies the subscriber category to which a charging profile applies.s
cdr suppression	Specifies that CDRs be suppressed as a charging characteristic in a charging profile.
charging profile	Associates a default charging profile to an access point.
content dcca profile	Defines a DCCA client profile in a GGSN charging profile.
content postpaid time	Specifies as a trigger condition for postpaid users in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
content postpaid validity	Specifies as a trigger condition in a charging profile, the amount of time quota granted to a postpaid user is valid.
content postpaid volume	Specifies as a trigger condition for postpaid users in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
content rulebase	Associates a default rule-base ID with a charging profile.
description	Specifies the name or a brief description of a charging profile.
gprs charging characteristics reject	Specifies that Create PDP Context requests for which no charging profile can be selected be rejected by the GGSN.
gprs charging container time-trigger	Specifies a global time limit, that when exceeded by a PDP context causes the GGSN to close and update the G-CDR for that particular PDP context.
gprs charging profile	Creates a new charging profile (or modifies an existing one), and enters charging profile configuration mode.
limit duration	Specifies, as a trigger condition in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
limit volume	Specifies, as a trigger condition in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
tariff-time	Specifies that a charging profile use the tariff changes configured using the **gprs charging tariff-time** global configuration command.

limit volume

To specify as a trigger condition in a charging profile, the maximum number of bytes that the gateway GPRS support node (GGSN) maintains across all containers for a particular PDP context before closing and updating the G-CDR, use the **limit volume** command in charging profile configuration mode. To return to the default value, use the **no** form of this command.

limit volume *threshold-value* **[reset]**

no limit volume *threshold-value* **[reset]**

Syntax Description

threshold-value	A value between 1 and 4294967295 that specifies the container threshold value, in bytes. The default is 1,048,576 bytes (1 MB).
reset	(Optional) Keyword to specify that the volume trigger be reset if the CDR is closed by any other trigger. If the **reset** keyword is not specified, the volume trigger will not be reset when the time trigger expires (**limit duration** command), but it will be reset when any other trigger expires.

Defaults

1,048,576 bytes (1 MB)

Command Modes

Charging profile configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

While a PDP context (mobile session) is active, charging events are generated based on various actions. One way that users can be charged is based on the amount of data transmitted between the PDN and the mobile station. Data volume is recorded in each of the containers of a G-CDR record. Service providers can use this recorded data volume to bill users by volume usage.

Use the **limit volume** charging profile configuration command to control the maximum amount of data volume that can be reported in each G-CDR from an active PDP context before the G-CDR is eligible for an update to the charging gateway for subsequent billing. The GGSN opens another partial G-CDR for that PDP context while it remains in session on the GGSN.

For example, consider that a volume threshold setting of 1 MB is configured on the GGSN. The GGSN opens a container in a G-CDR for a new PDP context. A trigger occurs for the PDP context, and at that time the GGSN has registered transmission of 500 KB of data for the PDP context. The trigger causes the GGSN to close the container for the PDP context, which has occurred before the volume limit is reached (500 KB of data transmitted, and 1 MB allowed).

As transmission for the PDP context continues, the GGSN opens a new container in the G-CDR. The GGSN now has up to 500 KB more data that can be processed for that PDP context before reaching the volume threshold limit for the G-CDR. When the volume threshold is reached across all containers for the PDP context (that is, the sum of all of the byte counts across all containers for the PDP context reaches 1 MB), the GGSN closes the G-CDR with a volume limit cause so that the G-CDR can be sent to the charging gateway. The GGSN opens another partial G-CDR for the PDP context while it remains in session.

For the box-level charging profile (profile 0 configured using the charging related global configuration commands), all triggers are reset by the expiration of another trigger. However, for charging profiles 1 through 15, the **reset** keyword option must be set for the **limit duration** and **limit volume** charging profile configuration commands for the expiration of any trigger to reset all other triggers. If the **reset** keyword is not specified when configuring the volume trigger, the volume trigger will not be reset when the time trigger expires (**limit duration** command), but it will be reset when any other trigger expires.

Related Commands.

Command	Description
category	Identifies the subscriber category to which a charging profile applies.s
cdr suppression	Specifies that CDRs be suppressed as a charging characteristic in a charging profile.
charging profile	Associates a default charging profile to an access point.
content dcca profile	Defines a DCCA client profile in a GGSN charging profile.
content postpaid time	Specifies as a trigger condition for postpaid users in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
content postpaid validity	Specifies as a trigger condition in a charging profile, the amount of time quota granted to a postpaid user is valid.
content postpaid volume	Specifies as a trigger condition for postpaid users in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
content rulebase	Associates a default rule-base ID with a charging profile.
description	Specifies the name or a brief description of a charging profile.
gprs charging characteristics reject	Specifies that Create PDP Context requests for which no charging profile can be selected be rejected by the GGSN.
gprs charging container time-trigger	Specifies a global time limit, that when exceeded by a PDP context causes the GGSN to close and update the G-CDR for that particular PDP context.
gprs charging profile	Creates a new charging profile (or modifies an existing one), and enters charging profile configuration mode.
limit duration	Specifies, as a trigger condition in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
limit sgsn-change	Specifies, as a trigger condition in a charging profile, the maximum number of SGSN changes that can occur before closing and updating the G-CDR for a particular PDP context.
tariff-time	Specifies that a charging profile use the tariff changes configured using the **gprs charging tariff-time** global configuration command.

match flow pdp

To specify PDP flows as the match criterion in a class map, use the **match flow pdp** command in class map configuration mode. To remove PDP flow as a match criterion, use the **no** form of this command.

match flow pdp

no match flow pdp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Class map configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The **match flow pdp** class map configuration command enables the ability to configure session-based policing (per-PDP policing) for downlink traffic on a GGSN.

Note When defining a class map for PDP flow classification, do not specify the **match-any** keyword option.

Note The Per-PDP policing feature requires that UMTS QoS has been configured.

Note If you are using trust DSCP policy map configuration, ensure that you configure only one class map with **match flow pdp** in the policy map. Simultaneous multiple flows for policing, with different DSCPs for a PDP, are not supported.

To configure the Per-PDP policing feature on a GGSN, you must complete the following tasks:

1. Create a class for PDP flows using the **class-map** command.

```
GGSN(config)# class-map class-pdp
GGSN(config-cmap)# Match flow pdp
GGSN(config-cmap)# exit
```

2. Create a policy map using the **policy-map** command and assign a class to the map using the **class** command.

```
GGSN(config)# policy-map policy-gprs
GGSN(config-pmap)# class class-pdp
```

3. In the policy map, configure the Traffic Policing feature using the **police** policy map class configuration command.

```
GGSN(config-pmap-c)# police rate pdp [burst bytes] [peak-rate pdp [peak-burst bytes]]
conform-action action exceed-action action [violate-action action]
GGSN(config-pmap-c)# exit
GGSN(config-pmap)# exit
```

4. Attach a service policy to an APN using the **service-policy** access-point configuration command.

```
GGSN(config)# access-point 1
GGSN(access-point-config) service-policy in policy-gprs
```

Examples

The following example specifies PDP flows as the match criterion in a class map named “class-pdp”:

```
class-map class-pdp
  match flow pdp
```

Related Commands

Command	Description
police rate	Configures traffic policing using the police rate.
service-policy	Attaches a service policy to an APN, to be used as the service policy for PDP flows of that APN.

maximum delay-class

To define in a Call Admission Control (CAC) maximum QoS policy, the maximum delay class for R97/R98 QoS that can be accepted at an APN, use the **maximum delay-class** command in CAC maximum QoS policy configuration mode. To return to the default value, use the **no** form of this command.

maximum delay-class *value* [**reject**]

no maximum delay-class *value* **[reject]**

Syntax Description

value	Specifies the maximum delay class that can be accepted at an APN. Valid values are 1 to 4.
reject	(Optional) Specifies that if the maximum delay class is higher than the configured value, the Create PDP Context is rejected. If this keyword is not specified, the delay class is downgraded to the value of the configured delay class. This keyword option is ignored for update PDP context requests.

Defaults

PDP contexts for which the maximum delay-class is higher than the configured value are downgraded to the configured value.

Command Modes

CAC maximum QoS policy configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **maximum delay-class** CAC maximum QoS policy configuration command to specify the maximum delay class that can be accepted at an APN.

By default, PDP contexts for which the maximum delay-class is higher than the configured value are downgraded to the configured value.

If the **reject** keyword has been specified, if the maximum delay class requested is higher than the configured delay class, the Create PDP Context is rejected.

If the **reject** keyword is not specified and the delay class in a create or update PDP context request is greater than the configured value, the requested delay class is downgraded to the configured value.

Examples

The following example defines 3 as the maximum delay class for GPRS QoS that can be accepted at an APN:

```
maximum delay-class 3
```

Related Commands

Command	Description
cac-policy	Enables the maximum QoS policy function of the CAC feature and applies a policy to an APN.
gbr traffic-class	Specifies the maximum guaranteed bit rate (GBR) that can be allowed in uplink and downlink directions for real-time classes (conversational and streaming) at an APN.
gprs qos cac-policy	Creates or modifies a CAC maximum QoS policy.
maximum delay-class	Defines the maximum delay class for R97/R98 (GPRS) QoS that can be accepted.
maximum peak-throughput	Defines the maximum peak throughput for R97/R98 (GPRS) QoS that can be accepted.
maximum pdp-context	Specifies the maximum PDP contexts that can be created for a particular APN.
maximum traffic-class	Defines the highest traffic class that can be accepted.
mbr traffic-class	Specifies the maximum bit rate (MBR) that can be allowed for each traffic class in both directions (downlink and uplink).

maximum pdp-context

To specify in a Call Admission Control maximum QoS policy, the maximum number of PDP contexts that can be created for a particular APN, use the **maximum pdp-context** command in CAC maximum QoS policy configuration mode. To return to the default value, use the **no** form of this command.

maximum pdp-context *number1* [**threshold** *number2*]

no maximum pdp-context *number1* [**threshold** *number2*]

Syntax Description

number1	Specifies the maximum number of PDP contexts that can be created in an APN.
threshold *number2*	(Optional) Specifies the threshold, that after reached, only PDP contexts with allocation/retention priority 1 are accepted.

Defaults

No default behavior or values.

Command Modes

CAC maximum QoS policy configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **maximum pdp-context** CAC maximum QoS policy configuration command to configure the maximum number of PDP contexts that can be created for a particular APN.

The maximum number of PDP contexts defined for an APN using the **maximum pdp-context** command cannot exceed the maximum number of PDP contexts defined by the **gprs maximum-pdp-context-allowed** global configuration command.

When the optional **threshold** keyword is specified, when the total number of PDP contexts exceeds the configured number, only PDP contexts with Allocation/Retention Priority 1 are accepted. Create PDP contexts with other priorities (2/3) are rejected. If the optional **threshold** keyword is not specified, when the total number of PDP contexts reaches the configured maximum number, all subsequent Create PDP Contexts are rejected.

The **maximum pdp-context** command configuration is checked before all other QoS parameters defined in a policy: maximum bit rate, guaranteed bit rate, highest traffic class, highest traffic handling priority, highest delay class, and highest peak throughput class.

Examples

In the following example, 15000 is specified as the maximum number of PDP contexts that can be created for a particular APN:

```
maximum pdp-context 15000
```

Related Commands

Command	Description
cac-policy	Enables the maximum QoS policy function of the CAC feature and applies a policy to an APN.
gbr traffic-class	Specifies the maximum guaranteed bit rate (GBR) that can be allowed in uplink and downlink directions for real-time classes (conversational and streaming) at an APN.
gprs qos cac-policy	Creates or modifies a CAC maximum QoS policy.
maximum delay-class	Defines the maximum delay class for R97/R98 (GPRS) QoS that can be accepted.
maximum peak-throughput	Defines the maximum peak throughput for R97/R98 (GPRS) QoS that can be accepted.
maximum pdp-context	Specifies the maximum PDP contexts that can be created for a particular APN.
maximum traffic-class	Defines the highest traffic class that can be accepted.
mbr traffic-class	Specifies the maximum bit rate (MBR) that can be allowed for each traffic class in both directions (downlink and uplink).

maximum peak-throughput

To define in a Call Admission Control (CAC) maximum QoS policy, the maximum peak throughput for R97/R98 QoS that can be accepted at an APN, use the **maximum peak-throughput** command in CAC maximum QoS policy configuration mode. To return to the default value, use the **no** form of this command.

maximum peak-throughput *value* [**reject**]

no maximum peak-throughput *value* **[reject]**

Syntax Description

value	Specifies the maximum peak throughput that can be accepted at an APN. Valid values are between 1 and 9.
reject	(Optional) Specifies that if the maximum peak throughput is higher than the configured value, the Create PDP Context is rejected. If this keyword is not specified, the peak throughput is downgraded to the value of the configured peak throughput value. This option is ignored for update PDP context requests.

Defaults

PDP contexts for which the peak throughput is higher than the configured value are downgraded to the configured value.

Command Modes

CAC maximum QoS policy configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **maximum peak-throughput** CAC maximum QoS policy configuration command to specify the maximum peak throughput that can be accepted at an APN.

By default, PDP contexts for which the peak throughput is higher than the configured value are downgraded to the configured value.

If the **reject** keyword has been specified, if the maximum peak throughput requested is higher than the configured peak throughput, the Create PDP Context is rejected.

If the **reject** keyword is not specified and the peak throughput in a create or update PDP context request is greater than the configured value, the requested peak throughput is downgraded to the configured value.

Examples

The following example defines 7 as the maximum peak-throughput GPRS QoS that can be accepted at an APN:

```
maximum peak-throughput 7
```

Related Commands

Command	Description
cac-policy	Enables the maximum QoS policy function of the CAC feature and applies a policy to an APN.
gbr traffic-class	Specifies the maximum guaranteed bit rate (GBR) that can be allowed in uplink and downlink directions for real-time classes (conversational and streaming) at an APN.
gprs qos cac-policy	Creates or modifies a CAC maximum QoS policy.
maximum delay-class	Defines the maximum delay class for R97/R98 (GPRS) QoS that can be accepted.
maximum peak-throughput	Defines the maximum peak throughput for R97/R98 (GPRS) QoS that can be accepted.
maximum pdp-context	Specifies the maximum PDP contexts that can be created for a particular APN.
maximum traffic-class	Defines the highest traffic class that can be accepted.
mbr traffic-class	Specifies the maximum bit rate (MBR) that can be allowed for each traffic class in both directions (downlink and uplink).

maximum traffic-class

To define in a Call Admission Control (CAC) maximum QoS policy, the highest traffic class that can be accepted at an APN, use the **maximum traffic-class** command in CAC maximum QoS policy configuration mode. To return to the default value, use the **no** form of this command.

maximum traffic-class *traffic-class-name* **[priority** *value***]**

no maximum traffic-class *traffic-class-name* **[priority** *value***]**

Syntax Description

traffic-class-name	Specifies the highest traffic class that can be accepted at an APN. Valid values are conversational, streaming, interactive, or background.
priority	(Optional) Specifies the highest traffic handling priority for the interactive traffic class.

Defaults

All traffic classes are accepted.

Command Modes

CAC maximum QoS policy configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **maximum traffic-class** CAC maximum QoS policy configuration command to define the highest traffic class that can be accepted at an APN. If the traffic class requested in a Create PDP Context request is higher than the configured class, the request is rejected.

The GGSN does not downgrade the traffic class of a PDP context unless the highest traffic class configured is changed after a PDP context is created and the GGSN receives an update PDP context request with a traffic class higher than the newly configured value. If this condition occurs, the GGSN downgrades the traffic class to the value of the newly configured maximum traffic class.

By default, all traffic classes are accepted.

Use the optional **priority** keyword to define the highest traffic handling priority for the interactive traffic class. If the requested traffic handling priority exceeds the highest one, it will be downgraded to the configured one. If the interactive traffic class is configured without the **priority** keyword option, then PDPs with any traffic handling priority are allowed. If the traffic class is not interactive, the **priority** keyword is ignored.

Examples

The following example configures streaming as the highest traffic class accepted at an APN:

```
maximum traffic-class streaming
```

The following example configures interactive as the highest traffic class accepted at an APN:

```
maximum traffic-class interactive
```

The following example configures interactive as the highest traffic class with traffic handling priority 2 accepted at an APN:

```
maximum traffic-class interactive priority 2
```

Related Commands

Command	Description
cac-policy	Enables the maximum QoS policy function of the CAC feature and applies a policy to an APN.
gbr traffic-class	Specifies the maximum guaranteed bit rate (GBR) that can be allowed in uplink and downlink directions for real-time classes (conversational and streaming) at an APN.
gprs qos cac-policy	Creates or modifies a CAC maximum QoS policy.
maximum delay-class	Defines the maximum delay class for R97/R98 (GPRS) QoS that can be accepted.
maximum peak-throughput	Defines the maximum peak throughput for R97/R98 (GPRS) QoS that can be accepted.
maximum pdp-context	Specifies the maximum PDP contexts that can be created for a particular APN.
maximum traffic-class	Defines the highest traffic class that can be accepted.
mbr traffic-class	Specifies the maximum bit rate (MBR) that can be allowed for each traffic class in both directions (downlink and uplink).

mbr traffic-class

To define in a Call Admission Control (CAC) maximum QoS policy, the maximum bit rate (MBR) that can be allowed for each traffic class, use the **mbr traffic-class** command in CAC maximum QoS policy configuration mode. To return to the default value, use the **no** form of this command.

mbr traffic-class *traffic-class-name bitrate* **{uplink | downlink} [reject]**

no mbr traffic-class *traffic-class-name bitrate* **{uplink | downlink} [reject]**

Syntax Description

traffic-class-name	Specifies the UMTS traffic class to which the MBR applies. Valid values are Conversational, Streaming, Interactive, or Background.
bitrate	Maximum bit rate in kilobits per second. Valid value is between 1 and 16000. **Note** Although the valid command range for both the uplink and downlink direction is 1 to 16000, the maximum rate that can be acheived in the uplink direction is 8640. Additionally, a value greater than 8640 in the downlink direction is supported for GTPv1 PDPs only.
uplink	Specifies MBR applies to a traffic-class for uplink traffic.
downlink	Specifies MBR applies to a traffic-class for downlink traffic.
reject	(Optional) Specifies that when the MBR exceeds the configured value, the Create PDP Contexts is rejected. This option is ignored for update PDP context requests.

Defaults

Any MBR is accepted.

Command Modes

CAC maximum QoS policy configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into the Cisco IOS Release 12.3(14)YU, and to support High Speed Downlink Packet Access (HSDPA), the maximum data transmission rate in the downlink direction was increased to 16000 kilobits.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **mbr traffic-class** CAC maximum QoS policy configuration command to define the highest MBR that can be accepted for real-time traffic on an APN.

When the **reject** optional keyword is specified, if the requested MBR exceeds the configured value, Create PDP Contexts are rejected. If the **reject** keyword is not specified, the MBR is downgraded to the configured value.

If the **reject** keyword is not specified and the MBR in a create or update PDP context request is greater than the configured value, the requested MBR is downgraded to the configured value.

Examples

The following example defines 1000 kbps as the uplink MBR supported and 2000 kbps as the maximum downlink MBR:

```
mbr traffic-class interactive 1000 uplink
mbr traffic-class interactive 1000 downlink
```

Related Commands

Command	Description
cac-policy	Enables the maximum QoS policy function of the CAC feature and applies a policy to an APN.
gbr traffic-class	Specifies the maximum guaranteed bit rate (GBR) that can be allowed in uplink and downlink directions for real-time classes (conversational and streaming) at an APN.
gprs qos cac-policy	Creates or modifies a CAC maximum QoS policy.
maximum delay-class	Defines the maximum delay class for R97/R98 (GPRS) QoS that can be accepted.
maximum peak-throughput	Defines the maximum peak throughput for R97/R98 (GPRS) QoS that can be accepted.
maximum pdp-context	Specifies the maximum PDP contexts that can be created for a particular APN.
maximum traffic-class	Defines the highest traffic class that can be accepted.
mbr traffic-class	Specifies the maximum bit rate (MBR) that can be allowed for each traffic class in both directions (downlink and uplink).

msisdn suppression

To specify that the gateway GPRS support node (GGSN) overrides the mobile station integrated services digital network (MSISDN) number with a pre-configured value in its authentication requests to a RADIUS server, use the **msisdn suppression** command in access-point configuration mode. To enable the GGSN to send the MSISDN number in authentication requests to a RADIUS server, use the **no** form of the command.

msisdn suppression [*value*]

no msisdn suppression [*value*]

Syntax Description

value	(Optional) String (up to 20 characters long) that the GGSN sends in place of the MSISDN number in authentication requests to a RADIUS server. Valid characters for the string are any of those accepted by the MSISDN encoding specifications, including the integers 0–9, and characters a, b, c, * and #. The default value is that no string is sent.

Defaults

The MSISDN number is suppressed, and no ID string is sent to the RADIUS server in place of the MSISDN number.

Command Modes

Access point configuration

Command History

Release	Modification
12.2(2)	This command was introduced.
12.2(4)MX2	This command was integrated into Cisco IOS Release 12.2(4)MX2.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

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.

Examples

The following example will override the MSISDN ID sent in the create request and will not send any ID to the RADIUS server:

```
gprs access-point-list abc
   access-point 1
     radius-server 192.168.1.1
     access-mode non-transparent
     msisdn suppression
```

Related Commands

Command	Description
access-mode	Specifies whether the GGSN requests user authentication at the access point to a PDN.
aaa-group	Specifies an AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN.
gprs default aaa-group	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN.

n3-requests

To specify the maximum number of times that the quota server attempts to send a signaling request to the CSG, use the **n3-requests** command in quota server configuration mode. To return to the default value, use the **no** form of this command.

n3-requests *number*

no n3-requests

Syntax Description

number	Number between 1 and 65535 that specifies the number of times a request is attempted.

Defaults

5 requests.

Command Modes

Quota server configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **n3-requests** command to configure the maximum number of times the quota server will attempt to send a signaling request to the CSG.

Examples

The following example configures the quota server to attempt to send a signaling request no more than 3 times:

```
ggsn quota-server qs1
 interface loopback1
 echo-interval 90
 n3-requests 3
```

Related Commands .

Command	Description
csg-group	Associates the quota server to a CSG group that is to be used for quota server-to-CSG communication.
echo-interval	Specifies the number of seconds that the quota server waits before sending an echo-request message to the CSG.
ggsn quota-server	Configures the quota server process that interfaces with the CSG for enhanced service-aware billing.

Command	Description
interface	Specifies the logical interface, by name, that the quota server will use to communicate with the CSG.
t3-response	Specifies the initial time that the quota server waits before resending a signaling request message when a response to a request has not been received.
show ggsn quota-server	Displays quota server parameters or statistics about the quota server message and error counts.

name

To specify the name of a iSCSI target in the target profile on the GGSN, use the **name** command in iSCSI interface configuration mode. To remove the IP address configuration, use the **no** form of the command.

name *target_name*

no name *target_name*

Syntax Description

target_name	Name of the SCSI target.

Command Default

No default behavior or values.

Command Modes

iSCSI interface configuration

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **name** command to specify the name of the SCSI target in an iSCSI target interface profile on the GGSN.

Examples

The following example configures an iSCSI target interface profile with the name targetA to a SCSI target named “eftcompany.com.”

```
ip iscsi target-profile targetA
  name iqn.2002-10.edu.abc.iol.iscsi.draft20-target:1
  ip 10.0.0.1
  port 3260
```

Related Commands

Command	Description
gprs iscsi	Configures the GGSN to use the specified iSCSI profile for record storage.
ip	Specifies the IP address of the target on the SAN.
ip iscsi target-profile	Creates an iSCSI interface profile for an SCSI target (or modifies an existing one), and enters iSCSI interface configuration mode.
port	Specifies the number of the TCP port on which to listen for iSCSI traffic.

nbns primary

To specify a primary (and backup) NBNS to be sent in create PDP responses at the access point, use the **nbns primary** command in access-point configuration mode. To remove the NBNS from the access-point configuration, use the **no** form of this command

nbns primary *ip-address* [**secondary** *ip-address*]

Syntax Description

ip-address	IP address of the primary NBNS.
secondary *ip-address*	(Optional) Specifies the IP address of the backup NBNS.

Defaults

No default behavior or values.

Command Modes

Access-point configuration

Command History

Release	Modification
12.3(2)XB	This command was introduced.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **nbns primary** command to specify the primary (and backup) NBNS at the access point level.

This feature is benefits address allocation schemes where there is no mechanism to obtain these address. Also, for a RADIUS-based allocation scheme, it prevents the operator from having to configure a NBNS and DNS under each user profile.

The NBNS address can come from three possible sources: DHCP server, RADIUS server, or local APN configuration. The criterion for selecting the NBNS address depends on the IP address allocation scheme configured under the APN. Depending on the configuration, the criterion for selecting the DNS and NBNS addresses is as follows:

1. DHCP-based IP address allocation scheme (local and external)—NBNS address returned from the DHCP server is sent to the MS. If the DHCP server does not return an NBNS address, the local APN configuration is used.
2. RADIUS-based IP address allocation scheme—NBNS address returned from the RADIUS server (in Access-Accept responses) is used. If the RADIUS server does not return an NBNS address, the local APN configuration is used.

3. Local IP Address Pool-based IP address allocation scheme—Local APN configuration is used.
4. Static IP Addresses—Local APN configuration is used.

Note The GGSN sends DNS addresses in the create PDP response only if the MS is requesting the DNS address in the PCO IE.

Examples

The following example specifies a primary and secondary NBNS at the access point level:

```
access-point 2
 access-point-name xyz.com
 nbns primary 10.60.0.1 secondary 10.60.0.2
 exit
```

Related Commands

Command	Description
ip-address-pool	Specifies a dynamic address allocation method using IP address pools for the current access point.
dns primary	Specifies a primary (and backup) DNS at the access point level.

network-behind-mobile

To enable an access point to support routing behind the mobile station (MS), use the **network-behind-mobile** command in access-point configuration mode. To disable support for routing behind the MS, use the **no** form of this command.

network-behind-mobile

no network-behind-mobile

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Access-point configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the network-behind-mobile access-point configuration command to enable an access point to support routing behind the MS. The routing behind the MS feature enables the routing of packets to IP addresses that do not belong to the PDP context (the MS), but exist behind it. The network address of the destination can be different than the MS address.

Before enabling routing behind the MS, the following requirements must be met:

- The MS must use RADIUS for authentication and authorization.
- At minimum, one Framed-Route, attribute 22 as defined in Internet Engineering Task Force (IETF) standard RFC 2865, must be configured in the RADIUS server for each MS that wants to use this feature.

  When configured, the Framed-Route attribute is automatically downloaded to the GGSN during the authentication and authorization phase of the PDP context creation. If routing behind the MS is not enabled, the GGSN ignores the Framed-Route attribute. If multiple Framed-Route attributes have been configured for an MS, the GGSN uses the first attribute configured. When the MS session is no longer active, the route is deleted.

- For PDP Regen or PPP with L2TP sessions, the Framed-Route attribute must be configure in the RADIUS server of the LNS.
- For PPP Regen sessions, if the **security verify source** command is configure, the Framed-Route attribute must also be configured in the user profile in the GGSN RADIUS server.Packets routed behind the MS share the same 3GPP QoS settings of the MS.
- Static routes are not configured. Configuring static routes and the routing behind the mobile station feature (Framed Route, attribute 22) at the same time is not supported.

Examples

The following example shows how to enable support for routing behind the MS at access point 200:

```
gprs access-point-list abc
 access-point 200
  network-behind-mobile
```

Related Commands

Command	Description
security verify	Specifies the verification of source and/or destination addresses.
show gprs gtp pdp-context	Displays a list of the currently active PDP contexts (mobile sessions).
show gprs gtp statistics	Displays the current GTP statistics for the GGSN.
show ip route	Displays the current state of the routing table.
show pdp	Displays a list of the currently active PDP contexts (mobile sessions).

pcscf

To assign a P-CSCF server group to be used for an access point name (APN) for P-CSCF Discovery, use the **pcscf** command in access-point configuration mode. To remove the P-CSCF server group association, issue the **no** form of this command.

pcscf *group-name*

no pcscf *group-name*

Syntax Description

group-name	Specifies the name of a P-CSCF server group to be used for P-CSCF Discovery for an APN.

Defaults

No default behavior or values.

Command Modes

Access-point configuration

Command History

Release	Modification
12.4(2)XB	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

Use the **pcscf** command to define a P-CSCF server group to be used by an APN for the P-CSCF Discovery support.

Note The order of the addresses returned in the "P-CSCF Address Field" of the PCO is the same as the order in which they are defined in the P-CSCF server group and the groups are associated with the APN.

Examples

The following example configures a P-CSCF group identified as "groupA" for an APN:

```
pcscf groupA
```

Related Commands

Command	Description
gprs pcscf	Configures a P-CSCF server group on the GGSN and enters P-CSCF group configuration mode.
server	Specifies the IP address of a P-CSCF server you want to include in the P-CSCF server group.
show gprs access-point	Displays information about access points on the GGSN.
show gprs pcscf	Displays a summary of the P-CSCF groups configured on the GGSN.

police rate

To configure PDP traffic policing using the police rate, use the **police rate** command in policy-map class configuration mode or policy-map class police configuration mode. To remove PDP traffic policing from the configuration, use the **no** form of this command.

police rate pdp [burst *bytes*] **[peak-rate pdp** [**peak-burst** *bytes*]] **conform-action** *action* **exceed-action** *action* **[violate-action** *action***]**

no police rate pdp [burst *bytes*] **[peak-rate pdp** [**peak-burst** *bytes*]] **conform -action** *action* **exceed-action** *action* **[violate-action** *action***]**

Syntax Description

burst *bytes*	(Optional) Committed burst size, in bytes. The size varies according to the interface and platform in use. Valid rage is 1000 to 512000000. The default is 1500.
peak-rate pdp	(Optional) Specifies that the peak rate of sessions be considered when policing PDP traffic.
peak-burst *bytes*	(Optional) Peak burst size, in bytes. The size varies according to the interface and platform in use. Valid range is 1000 to 512000000. The default is 2500.
conform-action	Action to take on packets when rate is less than conform burst.
exceed-action	Action to take on packets when rate exceeds conform burst.
violate action	Action to take on packets when rate violates conform burst.
action	(Optional) Action to take on packets. Specify one of the following keywords: • **drop**—Drops the packet. • **set-dscp-transmit new-dscp**—Sets the IP differentiated services code point (DSCP) value and sends the packet with the new IP DSCP value setting. • **set-prec-transmit new-prec**—Sets the IP precedence and sends the packet with the new IP precedence value setting. • **transmit**—Sends the packet with no alteration.

Defaults

Disabled.

Command Modes

Policy map class configuration

Command History

Release	Modification
12.3(8)XU	This command was integrated into the Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.

Usage Guidelines

Per-PDP policing (session-based policing) is a GGSN Traffic Conditioner (3G TS 23.107) function that can be used to limit the maximum rate of traffic received on the Gi interface for a particular PDP context.

The policing function enforces the CAC-negotiated data rates for a PDP context. The GGSN can be configured to either drop non-conforming traffic or mark non-conforming traffic for preferential dropping if congestion should occur.

The policing parameters used depends on the PDP context. Specifically,

- For GTPv1 PDPs with R99 QoS profiles, the MBR and GBR parameters from the CAC-negotiated QoS profile are used. For non real time traffic, only the MBR parameter is used.
- For GTPv1 PDPs with R98 QoS profiles and GTPv0 PDPs, the peak throughput parameter from the CAC-negotiated QoS policy is used.

Before configuring per-PDP policing, note the following:

- UMTS QoS mapping must be enabled on the GGSN.
- Cisco Express Forwarding (CEF) must be enabled on Gi interface.
- Per-PDP policing is supported for downlink traffic at the Gi interface only.
- The initial packets of a PDP context are not policed.
- Hiearchical policing is not supported.
- If flow-based policing is configured in a policy map that is attached to an APN, the **show policy-map apn** command displays the total number of packets received before policing and does not display the policing counters.
- A service policy that has been applied to an APN cannot be modified. To modify a service policy, remove the service policy from the APN, modify it, and then re-apply it.
- Multiple class maps, each with **match flow pdp** configured and a different differentiated services code point (DSCP), are supported in a policy map only if the DSCP is trusted (the **gprs umts-qos dscp unmodified** global configuration command has not been configured on the GGSN).

To clear policing counters displayed by the **show policy-map apn** command, issue the **clear gprs access-point statistics** *access-point-index* access-point configuration command.

Examples

The following is an example:

```
class-map match-all class-pdp
 match flow pdp
!
! Configures a policy-map and attaches this class map into it.

policy-map policy-gprs
 class class-pdp
  police rate pdp
    conform-action set-dscp-transmit 15
    exceed-action set-dscp-transmit 15
    violate-action drop

! Attaches the policy-map to the apn.

gprs access-point-list gprs
  access-point 1
   access-point-name static
   service-policy input policy-gprs
   !
```

Related Commands

Command	Description
match flow pdp	Specifies PDP flows as the match criterion in a class map.
service-policy	Attaches a service policy to an APN, to be used as the service policy for PDP flows of that APN.

port

To configure the port number on which the CSG listens for quota server traffic, use the **port** command in CSG group configuration mode. To deconfigure the port, use the **no** form of this command

port *port-number*

no port

Syntax Description

port-number	Number of the port on which the CSG listens for quota server traffic.

Defaults

3386

Command Modes

CSG group configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **port** command to configure the port number on which the CSG listens for quota server traffic.

The CSG always sends traffic to the quota server on port 3386. By default, it also listens for traffic from the quota server on port 3386, however, it can be configured to listen to a different port using the **port** CSG group configuration command.

Examples

The following configuration example configures the CSG to listen for traffic from a quota server on port 4444:

```
ggsn csg-group csg1
  virtual-address 5.5.5.14
  port 4444
```

Related Commands

Command	Description
ggsn csg-group	Configures a CSG group on the GGSN for quota server-to-CSG communication.
real-address	Configures the IP address of a real CSG for source checking on inbound messages from a CSG.

Command	Description
show ggsn csg	Displays the parameters used by the CSG group or the number of path and quota management messages sent and received by the quota server.
virtual-address	Configures a virtual IP address to which the quota server will send all requests.

port (iSCSI interface)

To specify the number of the port on which to listen for iSCSI traffic in the iSCSI target interface profile on the GGSN, use the **port** command in iSCSI interface configuration mode. To remove the port number, use the **no** form of the command.

port *port_number*

no port *port_number*

Syntax Description

port_number	Number of the port on which to use for iSCSI traffic.

Command Default

No default behavior or values.

Command Modes

iSCSI interface configuration

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **port** command to configure the port on which to listen for iSCSI traffic in the iSCSI target interface profile on the GGSN. Port 3260 is recommended.

Examples

The following example configures an iSCSI taret interface profile with the name targetA to a iSCSI target with which the GGSN will communicate using port number 3260.

```
ip iscsi target-profile targetA
  name iqn.2002-10.edu.abc.iol.iscsi.draft20-target:1
  ip 10.0.0.1
  port 3260
```

Related Commands

Command	Description
gprs iscsi	Configures the GGSN to use the specified iSCSI profile for record storage.
ip	Specifies the IP address of the target on the SAN.
ip iscsi target-profile	Creates an iSCSI interface profile for an SCSI target (or modifies an existing one), and enters iSCSI interface configuration mode.
name	Defines the name of the target.

ppp-regeneration

To enable an access point to support PPP regeneration, use the **ppp-regeneration** command in access point configuration mode. To disable support for PPP regeneration at an access point, use the **no** form of this command.

ppp-regeneration [**max-session** *number*] [**setup-time** *seconds*] [**verify-domain** | **fixed-domain**] **[allow-duplicate**]

no ppp-regeneration [**max-session** *number*] [**setup-time** *seconds*] [**verify-domain** | **fixed-domain**] **[allow-duplicate**]

Syntax Description

max-session *number*	Maximum number of PPP regenerated sessions allowed at the access point. The default value 65535.
setup-time *seconds*	Maximum amount of time, in seconds, within which a PPP regenerated session must be established. Valid value is between 1 and 65535. The default value is 60 seconds.
verify-domain	Configures the gateway GPRS support node (GGSN) to verify that the domain name from the acces point name (APN) information element (IE) and the Protocol Configuration Option (PCO) IE are the same before creating an L2TP tunnel to the user.
fixed-domain	
allow-duplicate	Configures the GGSN to not check for duplicate IP addresses for PPP regenerated packet data protocol (PDP) contexts.

Defaults

The default **max-session** value is 65535 seconds.

The default **setup-time** is 60 seconds.

The default for the **verify-domain** option is to create an L2TP tunnel to the user to the domain specified in the PCO IE without verifying against the APN.

The default for the **allow-duplicate** option is to disallow duplicate IP addresses.

Command Modes

Access point configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD and the default value changed from being device dependent to 65535.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.

Release	Modification
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ and the **fixed-domain** keyword option was added.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.
12.4(9)XG	This command was integrated into Cisco IOS Release 12.4(9)XG and the **allow-duplicate** keyword option was added.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.

Usage Guidelines

Use the **ppp-regeneration** command to enable an access point to support PPP regeneration and to specify parameters for PPP regeneration sessions on the GGSN.

Note The **ppp-regeneration** command configuration applies to IPv4 PDPs only.

Note PPP regeneration support at an access point requires Cisco Express Forwarding (CEF) to be enabled by using the **ip cef** command.

The maximum **setup-time** value should allow for the total amount of time required to create the PPP virtual access (VA) and to establish a PPP session. If the setup time is reached before the PPP IP Control Protocol (IPCP) is up, the GGSN tears down the L2TP session, PPP VA, and PDP context.

The type of PPP method configured to forward packets beyond the terminal equipment and mobile termination affects the maximum number of PDP contexts supported on the GGSN. For more information, see the "Configuring PPP Support on the GGSN" chapter of the *Cisco IOS Mobile Wireless Configuration Guide*.

When PPP regeneration is being used, use the **ppp-regeneration verify-domain** command in access point configuration mode to configure the GGSN to verify the domain sent in the PCO IE in a Create PDP Context request against the domain in the APN IE sent out by the user before selecting an L2TP tunnel to the user. If there is a mismatch between the user-supplied domain name and the APN, the Create PDP Context request is rejected with the cause value "Service not supported."

Examples

The following example shows a partial GGSN configuration for PPP regeneration, in which PPP regeneration is enabled at access point 1. The example specifies a maximum of 100 PPP regeneration sessions, with a limit of 30 seconds for creating PPP VA and establishing a PPP session:

```
gprs access-point-list abc
 access-point 1
  access-point-name gprs.corporate.com
  ppp-regeneration max-session 100 setup-time 30
  ppp-regeneration verify domain
  exit
```

Related Commands

Command	Description
gprs gtp ppp-regeneration vtemplate	Associates the virtual template interface that is configured for PPP encapsulation with support for regenerated PPP sessions on the GGSN.
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.

radius attribute acct-session-id charging-id

To specify that the gateway GPRS support node (GGSN) include only the charging ID in the Acct-Session-ID (attribute 44) in accounting requests at an APN, use the **radius attribute acct-session-id charging-id** command in access-point configuration mode. To disable this configuration, use the **no** form of this command.

radius attribute acct-session-id charging-id

no radius attribute acct-session-id charging-id

Syntax Description

This command has no arguments or keywords.

Defaults

The default is to send the GGSN address and charging ID in the Acct-Session-ID in accounting requests to a RADIUS server.

Command Modes

Access point configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **radius attribute acct-session-id charging-id** command to send only the charging ID in Acct-Session-ID (attribute 44) in its authentication and accounting requests to a RADIUS server.

Examples

The following example specifies that only the charging ID be sent in the Acct-Session-ID in accounting requests to the RADIUS server:

```
gprs access-point-list abc
   access-point 1
     radius attribute acct-session-id charging-id
```

Related Commands

Command	Description
access-mode	Specifies whether the GGSN requests user authentication at the access point to a PDN.
aaa-group	Specifies an AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN.

Command	Description
gprs default aaa-group	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN.
show gprs access-point	Displays information about access points on the GGSN.

radius attribute nas-id

To specify that the gateway GPRS support node (GGSN) include the NAS-Identifier (attribute 32) in access requests at an APN, use the **radius attribute nas-id** command in access-point configuration mode. To disable this configuration, use the **no** form of this command.

radius attribute nas-id *word*

no radius attribute nas-id

Syntax Description

word	Text string sent in attribute 32 that identifies the NAS originating in the access-request packets.

Defaults

The default is to not send the NAS-Identifier in access requests.

Command Modes

Access point configuration

Command History

Release	Modification
12.3(2)XB	This command was introduced.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **radius attribute nas-id** command to include the NAS-Identifier in access requests at an APN.

This command overrides the configuration of the **radius-server attribute 32 include-in-access-req format** global configuration command.

Examples

The following example configures the GGSN to send the NAS-Identifier in access requests at the APN:

```
gprs access-point-list abc
   access-point 1
     radius attribute nas-id GGSNGATEWAY1
```

Related Commands

Command	Description
access-mode	Specifies whether the GGSN requests user authentication at the access point to a PDN.
aaa-group	Specifies an AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN.

Command	Description
gprs default aaa-group	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN.
show gprs access-point	Displays information about access points on the GGSN.

radius attribute suppress imsi

To specify that the gateway GPRS support node (GGSN) suppress the Third Generation Partnership Project (3GPP) vendor-specific attribute (VSA) 3GGP-IMSI number in its authentication and accounting requests to a RADIUS server, use the **radius attribute suppress imsi** command in access-point configuration mode. To enable the GGSN to send the 3GPP VSA 3GPP-IMSI number in authentication and accounting requests to a RADIUS server, use the **no** form of the command.

radius attribute suppress imsi

no radius attribute suppress imsi

Syntax Description

This command has no arguments or keywords.

Defaults

The default is to send the 3GPP VSA 3GPP-IMSI number in authentication and accounting requests to a RADIUS server.

Command Modes

Access point configuration

Command History

Release	Modification
12.2(8)YD	This command was introduced.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **radius attribute suppress imsi** command to have GGSN suppress the 3GPP VSA 3GPP-IMSI number in its authentication and accounting requests to a RADIUS server.

Examples

The following example will not send the 3GPP VSA 3GPP-IMSI to the RADIUS server:

```
gprs access-point-list abc
   access-point 1
     radius attribute suppress imsi
```

Related Commands

Command	Description
access-mode	Specifies whether the GGSN requests user authentication at the access point to a PDN.
aaa-group	Specifies an AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN.
gprs default aaa-group	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN.
show gprs access-point	Displays information about access points on the GGSN.

radius attribute suppress qos

To specify that the gateway GPRS support node (GGSN) suppress the 3GPP VSA 3GPP-GPRS-QoS-Profile in its authentication and accounting requests to a RADIUS server, use the **radius attribute suppress qos** command in access-point configuration mode. To enable the GGSN to send the 3GPP VSA 3GPP-GPRS-QoS-Profile in authentication and accounting requests to a RADIUS server, use the **no** form of the command.

radius attribute suppress qos

no radius attribute suppress qos

Syntax Description

This command has no arguments or keywords.

Defaults

The default is to send the 3GPP VSA 3GPP-GPRS-QoS-Profile in authentication and accounting requests to a RADIUS server.

Command Modes

Access point configuration

Command History

Release	Modification
12.2(8)B	This command was introduced.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **radius attribute suppress qos** command to have GGSN suppress the 3GPP VSA 3GPP-GPRS-QoS-Profile in its authentication and accounting requests to a RADIUS server.

Examples

The following example will not send the 3GPP VSA 3GPP-GPRS-QoS-Profile to the RADIUS server:

```
gprs access-point-list abc
   access-point 1
     radius attribute suppress qos
```

Related Commands

Command	Description
access-mode	Specifies whether the GGSN requests user authentication at the access point to a PDN.
aaa-group	Specifies an AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN.
gprs default aaa-group	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN.
show gprs access-point	Displays information about access points on the GGSN.

radius attribute suppress sgsn-address

To specify that the gateway GPRS support node (GGSN) suppress the 3GPP VSA 3GPP-SGSN-Address in its authentication and accounting requests to a RADIUS server, use the **radius attribute suppress sgsn-address** command in access-point configuration mode. To enable the GGSN to send the 3GPP VSA 3GPP-SGSN-Address in authentication and accounting requests to a RADIUS server, use the **no** form of the command.

radius attribute suppress sgsn-address

no radius attribute suppress sgsn-address

Syntax Description

This command has no arguments or keywords.

Defaults

The default is to send the 3GPP VSA 3GPP-SGSN-Address in authentication and accounting requests to a RADIUS server.

Command Modes

Access point configuration

Command History

Release	Modification
12.2(8)B	This command was introduced.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **radius attribute suppress sgsn-address** command to have GGSN suppress the 3GPP VSA 3GPP-SGSN-Address in its authentication and accounting requests to a RADIUS server.

Examples

The following example will not send the 3GPP VSA 3GPP-SGSN-Address to the RADIUS server:

```
gprs access-point-list abc
   access-point 1
     radius attribute suppress sgsn-address
```

Related Commands

Command	Description
access-mode	Specifies whether the GGSN requests user authentication at the access point to a PDN.
aaa-group	Specifies an AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN.
gprs default aaa-group	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN.
show gprs access-point	Displays information about access points on the GGSN.

radius attribute user-name msisdn

To specify that the gateway GPRS support node (GGSN) include the MSISDN in the User-Name (attribute 1) in access requests at an APN, use the **radius attribute user-name msisdn** command in access-point configuration mode. To disable this configuration, use the **no** form of this command.

radius attribute user-name msisdn

no radius attribute user-name msisdn

Syntax Description

This command has no arguments or keywords.

Defaults

The default is to send the user name in the attribute 1.

Command Modes

Access point configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **radius attribute user-name msisdn** command to have GGSN send the MSISDN in the User-Name (attribute 1) instead of the user name in authentication and accounting requests to a RADIUS server.

Examples

The following example will send the MSISDN in access requests to the RADIUS server:

```
gprs access-point-list abc
   access-point 1
     radius attribute user-name msisdn
```

Related Commands

Command	Description
access-mode	Specifies whether the GGSN requests user authentication at the access point to a PDN.
aaa-group	Specifies an AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN.

Command	Description
gprs default aaa-group	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN.
show gprs access-point	Displays information about access points on the GGSN.

real-address

To configure the IP address of a real Content Services Gateway (CSG) for source checking on inbound messages from a CSG, use the **real-address** command in CSG group configuration mode.
To deconfigure the IP address of a real CSG, use the **no** form of this command

real-address *ip-address*

no real-address

Syntax Description

ip-address	IP address of a real CSG.

Defaults

No default behavior or values.

Command Modes

CSG group configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **real-address** CSG group configuration command to configure the IP address of a real CSG.

Configuring the IP address of a real CSG provides an additional security check against the source of messages. When configured, source address checking is performed on inbound message from the CSG.

For redundancy, you can configure up to two real IP addresses of CSGs in a CSG server group.

Using the **no** form of this command will remove the IP address from the list of IP addresses of a CSG server group.

Examples

The following configuration example configures two real IP addresses in CSG group csg1:

```
ggsn csg-group csg1
  virtual-address 5.5.5.14
  port 4444
  real-address 5.1.1.1
  real-address 5.1.1.2
```

Related Commands

Command	Description
ggsn csg-group	Configures a CSG group on the GGSN for quota server-to-CSG communication.
port	Configures the port number on which the CSG listens for quota server traffic.

Command	Description
show ggsn csg	Displays the parameters used by the CSG group or the number of path and quota management messages sent and received by the quota server.
virtual-address	Configures a virtual IP address to which the quota server will send all requests.

redirect all ip

To redirect all traffic to an external device, use the **redirect all ip** command in access-point configuration mode. To disable the redirection of all traffic, use the **no** form of this command.

redirect all ip *ip-address*

no redirect all ip *ip-address*

Syntax Description

ip-address	IP address of the external device to which you want to redirect traffic.

Defaults

Disabled

Command Modes

Access-point configuration

Command History

Release	Modification
12.3(2)XB2	This command was introduced.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **redirect all ip** access-point command to redirect all traffic to an external device (such as an external firewall) for verification.

Using the Redirect All Traffic feature, you can:

- Redirect all packets to a specified destination regardless of whether the destination address belongs to a mobile station (MS) on the same GGSN or not.

  If redirecting traffic using the Mobile-to-Mobile Redirect feature, only packets for which the destination address belongs to an MS that is active on the same GGSN can be redirected. If the receiving MS has no PDP context in the GGSN where the sending MS PDP context is created, the packets are dropped.
- Redirect all traffic to a specific destination when aggregate routes are configured.

Note On the Catalyst 6500 series switch / Cisco 7600 series platform, the traffic redirection feature requires that policy based routing (PBR) is configured on the MSFC2 and incoming VLAN interface from the Cisco MWAM, and that the next hop to route the packets is set using the **set ip next-hop** command.

Examples

The following example redirects all traffic to 5.5.5.13:

```
redirect all ip 5.5.5.13
```

Related Commands

Command	Description
security verify	Specifies the verification of source and/or destination addresses.

redirect intermobile ip

To redirect mobile-to-mobile traffic to an external device, use the **redirect intermobile ip** command in access-point configuration mode. To disable the redirection of mobile-to-mobile traffic, use the **no** form of this command.

redirect intermobile ip *ip-address*

no redirect intermobile ip *ip-address*

Syntax Description

ip-address	IP address of the external device to which you want to redirect mobile-to-mobile traffic.

Defaults

Disabled

Command Modes

Access-point configuration

Command History

Release	Modification
12.2(8)B	This command was introduced.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **redirect intermobile ip** access-point command to redirect mobile-to-mobile traffic to an external device (such as an external firewall) for verification.

Redirection of intermobile traffic does not occur on an ingress APN unless the TPDUs are exiting the same APN. In addition, redirection of TPDUs tunneled by L2TP from the ingress APN to the LNS of the PDN does not occur.

On the Catalyst 6500 series switch / Cisco 7600 series internet router platform, the mobile-to-mobile redirection feature requires that policy based routing (PBR) is configured on the MSFC2 and incoming VLAN interface from the Cisco MWAM, and that the next hop to route the packets that match the criteria is set using the **set ip next-hop** command.

Examples

The following example redirects mobile-to-mobile traffic to 5.5.5.13:

```
redirect intermobile ip 5.5.5.13
```

Related Commands

Command	Description
gprs plmn ip address	Specifies the IP address range of a PLMN.
security verify	Specifies the verification of source and/or destination addresses.

security

To configure the security protocol to use for the Diameter peer-to-peer connection, use the **security** command in Diameter peer configuration mode. To remove a security protocol, use the **no** form of this command

security ipsec

no security

Syntax Description

ipsec	Defines IPSec as the security protocol to use for securing messages between peers.

Defaults

IPSec.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **security** command to define the security protocol to use for the Diameter peer-to-peer connection.

When the security protocol is changed dynamically, the connection to the peer is torn down and reestablished after Diameter peer configuration mode is exited.

Examples

The following configuration example defines IPSec as the security protocol to use for a peer-to-peer connection with Diameter peer “dcca1”:

```
Diameter peer dcca1
 address ipv4 10.10.10.1
 transport tcp port 4000
 security ipsec
```

Related Commands .

Command	Description
address ipv4	Configures the IP address of the Diameter peer host.
destination host	Configures the Fully Qualified Domain Name (FQDN) of the Diameter peer
destination realm	Configures the destination realm (domain name) in which the Diameter host is located.

Command	Description
diameter peer	Defines the Diameter peer (server) and enters diameter peer configuration mode.
ip vrf forwarding	Defines the VRF associated with the Diameter peer.
source interface	Configures the interface to use to connect to the Diameter peer.
timer	Configures Diameter base protocol timers for peer-to-peer communication.
transport	Configures the transport protocol to use to connect with the Diameter peer.

security verify

To enable the gateway GPRS support node (GGSN) to verify the IP verification of IP addresses in TPDUs, use the **security verify** command in access-point configuration mode. To disable the verification of IP addresses, use the **no** form of this command.

security verify {**source** | **destination**}

no security verify {**source** | **destination**}

Syntax Description

source	Specifies that the source IP address of an upstream TPDU be verified against the address previously assigned an MS.
destination	Specifies that the destination address of upstream TPDU received off a GTP tunnel be verified against the global list of PLMN addresses specified by the **gprs plmn ip address** global configuration command.

Defaults

Disabled

Command Modes

Access-point configuration

Command History

Release	Modification
12.2(8)B	This command was introduced.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **security verify source** access point configuration command to configure the GGSN to verify the source IP address of an upstream TPDU against the address previously assigned to an MS.

When the **security verify source** command is configured on an APN, the GGSN verifies the source address of a TPDU before GTP will accept and forward it. If the GGSN determines that the address differs from that previously assigned to the MS, it drops the TPDU and accounts it as an illegal packet in its PDP context and APN. Configuring the **security verify source access point** configuration command protects the GGSN from faked user identities.

Use the **security verify destination** access point configuration command to have the GGSN verify the destination addresses of upstream TPDUs against global lists of PLMN addresses specified using the **gprs plmn ip address** command. If the GGSN determines that a destination address of a TPDU is within the range of a list of addresses, it drops the TPDU. If it determines that the TPDU contains a destination address that does not fall within the range of a list, it forwards the TPDU to its final destination.

Examples

The following example enables the verification of source IP addresses received in upstream TPDUs:

```
security verify source
```

Related Commands

Command	Description
redirect intermobile ip	Specifies the redirection of mobile-to-mobile traffic.
gprs plmn ip address	Specifies the IP address range of a PLMN.
show gprs access-point	Displays information about access points on the GGSN.

server (psd)2

To define a Persistent Storage Device (PSD) server (backup or retrieve-only), use the **server** command in data-store configuration mode. To remove the PSD server configuration, use the **no** form of this command.

server *psd-ip-address* [**retrieve-only**]

no slb vserver *psd-ip-address* [**retrieve-only**]

Syntax Description

ip_address	IP address of the PSD.
retrieve-only	Specifies that the GGSN will only retrieve G-CDRs from the PSD.

Defaults

No default behavior or values.

Command Modes

PSD group configuration

Command History

Release	Modification
12.3(14)YU	This command was introduced.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

Use the **server** data-store configuration command to define a PSD server or servers.

PSD servers can be configured as a “backup” or “retrieve-only” PSD.

The backup PSD server is a local PSD (within the same chassis) to which the GGSN writes G-CDRs if no charging gateway is available. When a charging gateway becomes available, the GGSN can be configured to automatically retrieve G-CDRs (using the **auto-retrieve** data-store configuration command) from the PSDs, or the G-CDRs can be manually retrieved via FTP.

Note The backup PSD server shares the same operational mode properties as the charging gateways.

In a GTP-SR implementation, a “retrieve-only” PSD must also be configured using the **server** data-store configuration command with the **retrieve-only** keyword option specified. A retrieve-only PSD defined for one GGSN also functions as a backup PSD for an alternate GGSN of a redundant pair. If a failover should occur, the newly active GGSN collects the G-CDRs from its retrieve-only PSD and forwards them to the charging gateway.

For example, if you have a redundantly configured GGSNs in chassis A and chassis B, each with their own PSDs (PSD A and PSD B), when the GGSN in chassis A is active, it writes to its local PSD, PSD A. PSD A is also defined as the retrieve-only PSD for the GGSN in chassis B.

If the active GGSN on chassis A becomes inactive, the standby GGSN in chassis B becomes active and begins writing to its backup PSD, PSD B. PSD B is also defined as the retrieve-only PSD for the GGSN in chassis A.

When PSD A on chassis A becomes available again, the GGSN on chassis B automatically initiates a retrieval of G-CDRs from PSD A on Chassis A (if the **auto-retrieval** command has been configured) or the G-CDRs are manually retrieved.

Note You can configure one backup PSD (local) and one retrieve-only PSD (remote) per PSD server group. One server group can be defined per GGSN.

Note If a retrieve-only PSD is configured without the **auto-retrieve** command configured as well, the GGSN will not initiate a start retrieve when a retrieving event occurs.

Examples

The following example defines the PSD to which the GGSN will backup G-CDRs as well as retrieve G-CDRs:

```
server 172.10.10.10
```

The following example defines a PSD with the IP address 192.10.10.1 as the “retrieve-only” PSD for a GGSN:

```
server 192.10.10.1 retrieve only
```

Related Commands

Command	Description
auto-retrieve	Configures the GGSN to automatically initiate a retrieval of G-CDRs from PSDs defined in a PSD server group.
clear data-store statistics	Clears PSD-related statistics.
data-store	Configures a PSD server group on the GGSN to use for GGSN-to-PSD communication.
show data-store	Displays the status of the PSD client and PSD server-related information.
show data-store statistics	Displays statistics related to the PSD client.

server (p-cscf)

To define a Proxy Call Session Control Function (P-CSCF) server in a P-CSCF server group, use the **server** command in P-CSCF group configuration mode. To remove the P-CSCF server configuration, use the **no** form of this command.

server [**ipv6**] *ip-address*

no server [**ipv6**] *ip-address*

Syntax Description

ipv6	(Optional) Specifies an IPv6 server to be a member of the P-CSCF group.
ip_address	IP address of the P-CSCF.

Defaults

No default behavior or values.

Command Modes

P-CSCF group configuration

Command History

Release	Modification
12.4(2)XB	This command was introduced.
12.4(9)XG	This command was integrated into Cisco IOS Release 12.4(9)XG and the **ipv6** keyword option was added.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.

Usage Guidelines

Use the **server** P-CSCF command in group configuration mode to define a P-CSCF server or servers in a P-CSCF server group.

The order of the addresses returned in the "P-CSCF Address Field" of the Protocol Configuration Option (PCO) is the same as the order in which they are defined in the P-CSCF server group and the groups are associated with the access point name (APN).

If no P-CSCF addresses are preconfigured, the Create PDP Context Response will not return any P-CSCF addresses. An error message will not be generated and the Create PDP Context Request will be processed.

Note Up to 10 P-CSCF servers can be defined in a P-CSCF server group. Both IPv6 and IPv4 P-CSCF servers can be defined in a server group. The packet data protocol (PDP) type dictates to which server the IP addresses are sent.

Examples

The following example defines an P-CSCF server with the IP address 172.10.10.10 to a P-CSCF server group:

```
gprs pcscf groupA
 server 172.10.10.10
```

Related Commands

Command	Description
gprs pcscf	Configures a P-CSCF server group on the GGSN and enters P-CSCF group configuration mode.
pcscf	Assigns a P-CSCF server group to an APN.
server	Specifies the IP address of a P-CSCF server that you want to include in the P-CSCF server group.
show gprs access-point	Displays information about access points on the GGSN.
show gprs pcscf	Displays a summary of the P-CSCF groups configured on the GGSN.

service-aware

To enable service-aware billing for a particular access point, use the **service-aware** command in access-point configuration mode. To disable the support on an access point, use the **no** form of this command.

service-aware

no service-aware

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Access-point configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **service-aware** command to enable service-aware billing for a particular access point.

When service-aware billing is enabled for an APN, using the **gprs gtp response-message wait-accounting** global configuration command, the GGSN must be configured to wait for a RADIUS accounting response before sending a Create PDP Context response to an SGSN for a Create PDP Context request.

Examples

The following configuration example enables service-aware billing for access-point 1:

```
interface virtual-template 1
 gprs access-point-list abc
!
gprs access-point-list abc
 access-point 1
  service-aware
```

Related Commands

Command	Description
gprs service-aware	Enables service-aware billing on the GGSN.

service-mode

To configure the service-mode state of an APN, use the **service-mode** command in access-point configuration mode. To return to the default value, use the **no** form of this command.

service-mode {operational | maintenance}

Syntax Description

operational	Specifies that the service-mode state of the APN is operational.
maintenance	Specifies that the service-mode state of the APN is maintenance.

Defaults

Operational

Command Modes

Access-point configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **service-mode** access-point configuration command to perform APN-related tasks (such as adding a new APN or modifying an existing APN) without affecting sessions for other APNs in the GGSN.

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

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

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

Note When the GGSN is in global maintenance mode (**gprs service-mode maintenance** command), all APNs are in maintenance mode as well.

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

Examples

The following example changes the service-mode state of an APN to maintenance mode:

```
service-mode maintenance
```

Related Commands

Command	Description
gprs service-mode	Configures the service-mode state of a GGSN.
gprs service-mode test imsi	Configures a test user for which you can Create PDP Contexts to test an APN configuration.
show gprs access-point	Displays information about access points on the GGSN.
show gprs service-mode	Displays the current global service mode state of the GGSN and the last time it was changed.

service-policy

To attach a service policy to an APN, to be used as the service policy for PDP flows of that APN, use the **service-policy** command in access-point configuration mode. To remove a service policy, use the **no** form of this command.

service-policy input *policy-map-name*

no service-policy input *policy-map-name*

Syntax Description

input	Applies the specified policy map to incoming T-PDUs.
policy-map-name	The name of a service policy map (created using the **policy-map** command) to be attached. The name can be a maximum of 40 alphanumeric characters.

Defaults

No service policy is attached to an APN.

Command Modes

Access-point configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **service-policy** access-point configuration command to attach a policy map to an APN when configuring the Per-PDP policing feature on the GGSN. Before attaching a policy map to an APN, the policy map must be configured using the **policy-map** command.

Note The Per-PDP policing feature requires that UMTS QoS has been configured.

Note Do not use flow-based policing with multiple DSCP-based classifications if trust DSCP is configured.

Note If you are using trust DSCP policy map configuration, ensure that you configure only one class map with **match flow pdp** in the policy map. Simultaneous multiple flows for policing, with different DSCPs for a PDP, are not supported.

Service policies cannot be attached to or removed from an APN when there are active PDP contexts on that APN. To modify a service policy, you must first disassociate it from the APN using the **no service-policy** access point configuration command.

Caution If you remove the global policy map configuration (using the **no policy-map** global configuration command), service policies associated with APNs will also be removed without any warning.

To configure the Per-PDP policing feature on a GGSN, you must complete the following tasks:

1. Create a class for PDP flows using the **class-map** command.

```
GGSN(config)# Class-map class-pdp
GGSN(config-cmap)# Match flow pdp
GGSN(config-cmap)# exit
```

2. Create a policy map using the **policy-map** command and assign a class to the map using the **class** command.

```
GGSN(config)# Policy-map policy-gprs
GGSN(config-pmap)# Class class-pdp
```

3. In the policy map, configure the Traffic Policing feature using the **police rate** policy map class configuration command.

```
GGSN(config-pmap-c)# police rate pdp [burst bytes] [peak-rate pdp [peak-burst bytes]]
conform-action action exceed-action action [violate-action action]
GGSN(config-pmap-c)# exit
GGSN(config-pmap)# exit
```

4. Attach a service policy to an APN using the **service-policy** access-point configuration command.

```
GGSN(config)# Access-point 1
GGSN(access-point-config) Service-policy in policy-gprs
```

Examples

The following example attaches service policy “policy-gprs” to access-point 1:

```
access-point 1
 service-policy in policy-gprs
```

Related Commands

Command	Description
match flow pdp	Specifies PDP flows as the match criterion in a class map.
police rate	Configures traffic policing using the police rate.

session idle-time

To specify the time, in hours, that the gateway GPRS support node (GGSN) waits before purging idle mobile sessions for the current access point, use the **session idle-time** command in access-point configuration mode. To disable the idle timer at the access point, use the **no** form of this command.

session idle-time *number*

no session idle-time

Syntax Description

number	Number of hours between 1 and 168.

Defaults

No session idle timer is configured on the access point.

Command Modes

Access-point configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The GGSN implements the idle timer in 3 ways. These implementations are listed in the order in which the GGSN processes them.

- Radius server—If the access-point is configured for non-transparent access mode and the Radius server returns a session timeout attribute, then the GGSN uses the session idle timeout value from the Radius server.
- Access-point—If the access-point is configured for transparent access mode, or is in non-transparent access mode and the Radius server does not return a session idle timeout value, the GGSN uses the value that you specified for the **session idle-time** command.
- Global timer—If the GGSN does not get a session idle timeout value from the Radius server or the access-point, it uses the value that you specified in the **gprs idle-pdp-context purge-timer** command.

The **session idle-time** command value overrides the value configured in the **gprs idle-pdp-context purge-timer** command for that access-point.

When the session reaches the timeout value, the PDP context is deleted.

Note With GGSN Release 5.0 and later, you can also configure the session idle timer for an access-point using the **gtp pdp-context timeout idle** access-point configuration command, however, the two methods cannot be configured at the same time.

Use the **show gprs gtp pdp-context tid** command to view the session idle-time value. The value is shown in the "gtp pdp idle time" field.

Examples

The following example specifies that the GGSN waits for 5 hours before purging idle time sessions for access-point 1. The GGSN waits for 60 hours before purging idle time sessions for all access points *except* access-point 1:

```
gprs access-point-list abc
 access-point 1
  access-point-name gprs.pdn1.com
  session idle-time 5

gprs idle-pdp-context purge-timer 60
```

Related Commands

Command	Description
gprs gtp pdp-context timeout idle	Specifies the time, in seconds, that a GGSN allows a session to be idle before terminating the session.
gprs gtp pdp-context timeout session	Specifies the time, in seconds, that the GGSN allows a session to be active before terminating the session.
gtp pdp-context timeout idle	Specifies the time, in seconds, that the GGSN allows a session to be idle at a particular APN before terminating the session.
gtp pdp-context timeout session	Specifies the time, in seconds, that a GGSN allows a session to be active at a particular APN before terminating the session.
gprs idle-pdp-context purge-timer	Specifies the time that the GGSN waits before purging idle mobile sessions.
show gprs gtp pdp-context	Displays a list of the currently active PDP contexts (mobile sessions).

session-failover

To enable sessions to failover over to an alternate Diameter server (via Credit Control Session Failover [CCSF] AVP support) when a credit control answer (CCA) message from the DCCA server does not contain a value for the CCSF AVP, use the **session-failover** command in DCCA client profile configuration mode. To return to the default value, use the **no** form of this command

session-failover

no session-failover

Syntax Description

This command has no arguments or keywords.

Defaults

Session failover is not supported.

Command Modes

DCCA client profile configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **session-failover** command to configure session failover support locally by enabling the CCSF AVP. The CCSF AVP indicates whether a Diameter session should be failed over to an alternate Diameter server or not.

A value returned by a Diameter server in a CCA overrides the default configured locally.

When session failover is disabled, the Credit Control (CC) session will not be moved to an alternate DCCA server if a failure should occur. If support of the CCSF AVP is enabled, the CC session will be moved to an alternate destination if a failover should occur.

Examples

The following configuration example enables the CCSF AVP in CCRs for a DCCA client:

```
gprs dcca profile dcca-profile1
  authorization dcca-method
  tx-timeout 12
  ccfh continue
  session-failover
```

Related Commands

Command	Description
authorization	Defines a method of authorization (AAA method list), in the DCCA client profile, that specifies the Diameter server groups.
ccfh	Configures the Credit Control Failure Handling (CCFH) AVP locally to use for a credit-control session when the Credit Control Answer (CCA) sent by the DCCA server does not contain CCFH value.
content dcca profile	Defines the DCCA client profile in a GGSN charging profile.
destination-realm	Configures the destination realm to be sent in CCR initial requests to a DCCA server.
gprs dcca profile	Defines a DCCA client profile on the GGSN and enters DCCA client profile configuration mode.
trigger	Specifies that SGSN and QoS changes will trigger a DCCA client to request quota-reauthorization
tx-timeout	Configures a TX timeout value used by the DCCA client to monitor the communication of Credit Control Requests (CCRs) with a Diameter server.

show aaa servers sg

To display counters (information about the number of packets sent to and received from authentication, authorization, and accounting [AAA] servers) for all the servers that are members of a specific server group, use the **show aaa servers sg** command in privileged EXEC mode.

show aaa servers sg *sg-name*

Syntax Description

sg-name	Name of the server group for which you want to display counters for each server in the group.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)XG	This command was introduced.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **show aaa servers sg** command to display counters for all the servers in a specified server group.

The command displays information about packets sent and received for all AAA transaction types.

Examples

The following example displays information about each RADIUS servers that are a member of the "group1" server group:

```
router# show aaa servers sg group1

RADIUS: id 3, priority 0, host 1.1.1.1, auth-port 1645, acct-port 1646
     State: current UP, duration 159574s, previous duration 0s
     Dead: total time 0s, count 0
     Authen: request 0, timeouts 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
     Author: request 0, timeouts 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
     Account: request 0, timeouts 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
     Elapsed time since counters last cleared: 1d20h19m

RADIUS: id 4, priority 0, host 2.2.2.2, auth-port 1645, acct-port 1646
     State: current UP, duration 159574s, previous duration 0s
     Dead: total time 0s, count 0
     Authen: request 0, timeouts 0
```

```
                Response: unexpected 0, server error 0, incorrect 0, time 0ms
                Transaction: success 0, failure 0
        Author: request 0, timeouts 0
                Response: unexpected 0, server error 0, incorrect 0, time 0ms
                Transaction: success 0, failure 0
        Account: request 0, timeouts 0
                Response: unexpected 0, server error 0, incorrect 0, time 0ms
                Transaction: success 0, failure 0
        Elapsed time since counters last cleared: 1d20h19m

RADIUS: id 5, priority 0, host 3.3.3.3, auth-port 1645, acct-port 1646
        State: current UP, duration 159575s, previous duration 0s
        Dead: total time 0s, count 0
        Authen: request 0, timeouts 0
                Response: unexpected 0, server error 0, incorrect 0, time 0ms
                Transaction: success 0, failure 0
        Author: request 0, timeouts 0
                Response: unexpected 0, server error 0, incorrect 0, time 0ms
                Transaction: success 0, failure 0
        Account: request 0, timeouts 0
                Response: unexpected 0, server error 0, incorrect 0, time 0ms
                Transaction: success 0, failure 0
        Elapsed time since counters last cleared: 1d20h19m
```

Table 3 describes the fields shown in the display.

Table 3 show aaa servers sg Field Descriptions

Field	Description
id	An identifier that uniquely identifies the server on the router.
priority	The priority by which the server will be tried within the server group.
host	The IP address of the AAA server.
auth-port	The port on the AAA server that is used for authentication and authorization requests.
acct-port	The port on the AAA server that is used for accounting requests.
State	Indicates the assumed state of the AAA server. The following states are possible: • UP—Indicates that the server is currently considered alive and attempts will be made to communicate with it. • DEAD—Indicates that the server is currently presumed dead and, in the case of failovers, this server will be skipped unless it is the last server in the group. • duration—Is the amount of time the server is assumed to be in the current state, either UP or DEAD. • previous duration—Is the amount of time the server was considered to be in the previous state.
Dead	Indicates the number of times that this server has been marked dead, and the cumulative amount of time, in seconds, that it spent in that state.

Table 3 show aaa servers sg Field Descriptions

Field	Description
Authen	Provides information about authentication packets that were sent to and received from a server, and authentication transactions that were successful or that failed. The following information may be reported in this field: • request—Number of authentication requests that were sent to the AAA server. • timeouts—Number of timeouts (no responses) that were observed, when a transmission was sent to this server. • Response—Provides statistics about responses that were observed from the server and includes the following reports: – unexpected—Number of unexpected responses. A response is considered unexpected when it is received after the timeout period for the packet has expired. This may happen if the link to the server is severely congested, for example. An unexpected response can also be produced when a server generates a response for no apparent reason. – server error—Number of server errors. This category is a catchall for error packets that do not any of the previous categories. – incorrect—Number of incorrect responses. A response is considered incorrect if it is of the wrong format expected by the protocol. This frequently happens when an incorrect server key is configured on the router. • Transaction—These fields provide information about AAA transactions related to the server. A transaction is defined as a request for authentication, authorization, or accounting information that is sent by the AAA module, or by an AAA client (such as PPP) to an AAA protocol (RADIUS or TACACS+), which may involve multiple packet transmissions and retransmissions. Transactions may require packet retransmissions to one or more servers in a single server group, to verify success or failure. Success or failure is reported to AAA by the RADIUS and TACACS+ protocols, as follows – success—Incremented when a transaction is successful. – failure—Incremented when a transaction fails (for example, packet retransmissions to another server in the server group failed due to failover or did not succeed. (A negative response to an Access Request, such as Access Reject, is considered to be a successful transaction).
Author	The fields in this category are similar to those in the Authen fields. An important difference, however, is that because authorization information is carried in authentication packets for the RADIUS protocol, these fields are not incremented when using RADIUS.

Table 3 show aaa servers sg Field Descriptions

Field	Description
Account	The fields in this category are similar to those in the Authen fields, but provide accounting transaction and packet statistics.
Elapsed time since counters last cleared	Displays the amount of time in days, hours, and minutes, that has passed since the counters were last cleared.

Related Commands

Command	Description
clear aaa counters server sg	Clears and resets the counters to zero for all servers in a specific server group.

show data-store

To display the status of the Persistent Storage Device (PSD) client and PSD server-related information, use the **show data-store** command in privileged EXEC mode.

show data-store

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)YU	This command was introduced.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

Use the **show data-store** command to display the status of the PSD client and PSD server information.

Examples

The following is sample output of the **show data-store** command:

```
router# show data-store

--------------------------------------------------------------------------------
  Server       Retrieve  Link    Current      Operating    Disk       Data
IP address       Only    State    Status        Mode       State     Present
--------------------------------------------------------------------------------
172.17.17.17      YES     DOWN      IDLE           -      AVAILABLE     YES
192.10.5.1        NO      UP        IDLE        STANDBY   AVAILABLE     NO
--------------------------------------------------------------------------------
Auto retrieval                    :ENABLED
Client                            :GGSN Charging
```

Table 4 describes the fields shown in the display.

Table 4 show data-store Field Descriptions

Field	Description
Server IP Address	IP address of the PSD.
Retrieve Only	Whether or not the PSD is a “retrieve-only” PSD. Possible values are YES or NO.
Link State	Status of link between the GGSN and PSD. Possible values are UP or DOWN.

Table 4 show data-store Field Descriptions (continued)

Field	Description
Current Status	Whether or not activity is occurring on the link. Possible values are: • IDLE—PSD server is available. When a PSD moves from a Writing to Idle state, the pending write requests are copied and sent to the active charging gateway. • WRITING—G-CDRs are in the process of being backed up to the PSD. Once the PSD disk state is full, the PSD moves to an Idle state. • RETRIEVING—G-CDRs are being retrieved and forwarded to the active charging gateway. Once all records are retrieved, the PSD state moves to idle.
Operating Mode	Operational state of the PSD. Possible values are: • UNDEFINED—PSD is configured on the GGSN but no connection established. • STANDBY—PSD is configured and connection is established, but the PSD is in Standby mode (no writing or retrieving activity is occurring). • ACTIVE—G-CDRs are being backed up to the PSD. In this state, aggregation characteristics and throttles that normally apply to the charging gateways are applied to the PSD.
Disk State	Whether or not disk space is available on the PSD. Possible values are AVAILABLE or FULL.
Data Present	Whether or not data currently exists on a disk. Possible values are YES or NO.
Auto retrieval	Whether or not the auto-retrieval feature has been configured for a PSD server group.
Client	PSD client.

Related Commands

Command	Description
auto-retrieve	Configures the GGSN to automatically initiate a retrieval of G-CDRs from PSDs defined in a PSD server group.
clear data-store statistics	Clears PSD-related statistics.
data-store	Configures a PSD server group on the GGSN to use for GGSN-to-PSD communication.
show data-store statistics	Displays PSD client statistics.

show data-store statistics

To display statistics related to the Persistent Storage Device (PSD) client, including the number of requests sent and DRT responses received, use the **show data-store statistics** command in privileged EXEC mode.

show data-store statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)YU	This command was introduced.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

Use the **show data-store statistics** command to display statistics related to the PSD client (for example, number of Read/Write requests sent and responses received).

Examples

The following is sample output of the **show data-store** command:

```
router# show data-store statistics

Requests sent:
         FIFO Write. . . . . . . . . . . . . . . . . . . . = 0
         FIFO Read . . . . . . . . . . . . . . . . . . . . = 12
         FIFO Read/Write retransmissions . . . . . . . . . = 12

DRT Responses rcvd:
         Retrieved msgs forwarded. . . . . . . . . . . . . = 8
         Disk full transitions. . . . . . . . . . . . . .  = 0
```

Table 5 describes the fields shown in the display.

Table 5 show data-store statistics Field Descriptions

Field	Description
Requests sent: FIFO Write	First-in, first-our Write requests sent.
Requests sent: FIFO Read	First-in, first-our Read requests sent.
Requests sent: FIFO Read/Write retransmissions	First-in, first-our Read/Write requests sent.

Table 5 show data-store statistics Field Descriptions (continued)

Field	Description
DRT Responses rcvd: Retrieved msgs forwarded	
DRT Responses rcvd:Disc full transitions	

Related Commands

Command	Description
auto-retrieve	Configures the GGSN to automatically initiate a retrieval of G-CDRs from PSDs defined in a PSD server group.
clear data-store statistics	Clears PSD-related statistics.
data-store	Configures a PSD server group on the GGSN to use for GGSN-to-PSD communication.
show data-store	Displays the status of the PSD client and PSD server-related information.

show diameter peer

To display information about the state of a Diameter peer, including various counters, use the **show diameter peer** command in privilege EXEC mode.

show diameter peer [*name* **| all]**

Syntax Description

name	Name of the Diameter peer for which you want to display state information.
all	Displays information for all Diameter peers.

Defaults

No default behavior or values.

Command Modes

Privilege EXEC

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Examples

The following configuration example displays information about the state of Diameter peer “peerA”:

```
show diameter peer peerA
 Peer information for peerA
---------------------------------------
Peer name :peerA
Peer type :Server
Peer transport protocol :TCP
Peer listening port :3688
Peer security protocol :IPSEC
Peer connection timer value :30 seconds
Peer watch dog timer value :35 seconds.
Peer vrf name :default
Peer connection status :UP.
```

Table 18 describes the fields shown in the display.

Table 6 show diameter peer Field Descriptions

Field	Description
Peer Name	Name of the Diameter peer.
Peer Type	Type of Diameter peer. Possible values are Server and Client.
Peer transport protocol	Transport protocol used to connect to peer.
Peer listening port	Port being used listen for peer communication.

Table 6 show diameter peer Field Descriptions (continued)

Field	Description
Peer security protocol	Security protocol being used for peer-to-peer communication. Possible value is IPSEC.
Peer connection timer	Timeout period for attempting to connect to the peer after a connection has been dropped.
Peer watch dog timer	Maximum period of time this node will wait for the Diameter peer to respond to a watchdog packet.
Peer vrf name	Name of VRF associated with the Diameter peer.
Peer connection status	Status of the connection to the peer. Possible values are UP or DOWN.

show ggsn csg

To display the parameters configured for a Content Services Group (CSG) group or the number of path and quota management messages sent and received by a quota server, use the **show ggsn csg** command in privilege EXEC mode.

show ggsn csg [parameters | statistics]

Syntax Description

parameters	Displays the parameters configured for a CSG group.
statistics	Displays the number of path and quota management messages sent and received by a quota server.

Defaults

No default behavior or values.

Command Modes

Privilege EXEC

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Examples

Example 1 displays the parameters used by the CSG group. Example 2 displays the number of path and management messages sent and received by the quota server.

Example 1

```
ggsn1#show ggsn csg parameters
GGSN CSG parameters:
  Group name:           csg1
  virtual/alias address:5.5.5.14
  Port on CSG:          3386
  Path state:           UP
  Peal addresses:       5.1.1.1 5.1.1.2
  Active real's address:5.1.1.2
```

Example 2

```
ggsn1#show ggsn csg statistics
GGSN CSG path statistics:
  Outbound msg count:  224
  Outbound byte count: 1344
  Inbound msg count:   222
  Inbound byte count:  1554
GGSN CSG path msg statistics:
  Service Auth Req:     0
  Service Auth Resp:    0
  Service Reauth Req:   0
  Service Stop:         0
```

```
  Quota Return:          0
  Quota Return Req:      0
  Quota Push Resp:       0
  Service Stop Req:      0
  Quota Push:            0
  Quota Push resp:       0
  GTP' Acknowledgements:0
ggsn1#
```

Related Commands

Command	Description
ggsn csg-group	Configures a CSG group on the GGSN for quota server-to-CSG communication.
port	Configures the port number on which the CSG listens for quota server traffic.
real-address	Configures the IP address of a real CSG for source checking on inbound messages from a CSG.
virtual-address	Configures a virtual IP address to which the quota server will send all requests.

show ggsn quota-server

To display quota server parameters or quota server-related statistics, use the **show ggsn quota-server** command in privilege EXEC mode.

show ggsn quota-server [parameters | statistics]

Syntax Description

parameters	Displays the quota server configuration.
statistics	Displays quota server-related message and error counts.

Defaults

No default behavior or values.

Command Modes

Privilege EXEC

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show ggsn quota-server** command to display the quota server configuration or quota server-related statistics on messages and error counts.

Quota server-related statistics can be cleared using the **clear ggsn quota-server statistics** command.

Examples

Example 1 displays the quota server configuration on a GGSN. Example 2 displays quota server-related statistics.

Example 1

```
ggsn1#show ggsn quota-server parameters
GGSN Quota Server parameters:
  Server name:  qs
  Interface:    Loopback1
  IP address:   10.1.1.1
  Table ID:     0
  Port on QS:   3386
  Echo interval:60 secs
  N3 number:    5
  T3 time:      1 secs
  CSG group:    csg1
```

Example 2

```
ggsn1#show ggsn quota-server statistics
GGSN Quota Server statistics
Quota management statistics:
  Requests rcvd:  35
```

```
  Responses rcvd: 16
  Requests sent:  16
  Responses sent: 27
Overall path management statistics:
  Requests rcvd:  5717
  Responses rcvd: 5818
  Requests sent:  5825
  Responses sent: 5717
Error statistics:
  Negative responses rcvd:0
  Requests unreplied:     0
  Seqnum failures:        0
  Dropped msgs:           10
  Unknown msgs:           0
  Unknown responses:      0
  Msgs with IE error:     0
  Bad source address msgs:0
  Version not supported:  0
  Mandatory TLV missing:  0
  Mandatory TLV incorrect:2
  Invalid Msg format:     0
  No response:            1
```

Related Commands .

Command	Description
clear ggsn quota-server statistics	Clears the quota server-related statistics displayed using the **show ggsn quota-server statistics** command.
csg-group	Associates the quota server to a CSG group that is to be used for quota server-to-CSG communication.
echo-interval	Specifies the number of seconds that the quota server waits before sending an echo-request message to the CSG.
ggsn quota-server	Configures the quota server process that interfaces with the CSG for enhanced service-aware billing.
interface	Specifies the logical interface, by name, that the quota server will use to communicate with the CSG.
n3-requests	Specifies the maximum number of times that the quota server attempts to send a signaling request to the CSG.
t3-response	Specifies the initial time that the quota server waits before resending a signaling request message when a response to a request has not been received.

show gprs

To display statistics for a gateway GPRS support node (GGSN), use the **show gprs** command in privileged EXEC mode.

show gprs

Syntax Description

access-point-index	Index number of an access point. Statistics for that access point are shown.
all	Statistics for all access points on the GGSN are shown.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **show gprs** command to display statistics collected for the GGSN during the interval defined using the **gprs interval** global configuration command.

Examples

The following example displays statistics for the GGSN:

```
Router#show gprs
 Collection interval - 3 min, Last collected at - 1 min back
   upstream data volume in octets: 0
   downstream data volume in octets: 0
   upstream packet count: 0
   downstream packet count: 0
 Collection interval - 4 min, Last collected at - 2 min back
   upstream data volume in octets: 0
   downstream data volume in octets: 0
   upstream packet count: 0
   downstream packet count: 0
Router#
```

Related Commands

Command	Description
gprs interval	Configures the interval at which the GGSN collects data for APNs.

show gprs access-point

To display information about access points on the gateway GPRS support node (GGSN), use the **show gprs access-point** command in privileged EXEC mode.

show gprs access-point {access-point-index [**address-allocation]** | **all**}

Syntax Description

access-point-index	Integer (from 1 to 65535) that identifies a GGSN access point. Information about that access point is shown.
address-allocation	Tunnel ID (TID) and dynamically allocated mobile station (MS) addresses (by either a DHCP or RADIUS server) are shown for packet data protocol (PDP) contexts on the specified access point.
all	Information about all access points on the GGSN is shown.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Release	Modification
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX. • The following output fields were added to the display: – accounting – aggregate – apn_accounting_server_group – apn_authentication_server_group – apn-type – apn_username – apn_password – Block Roamer Mode – GPRS vaccess interface – VPN – wait_accounting • The following output fields were removed from the display: – apn_charging_gw – apn_backup_charging_gw – apn_radius_server • Several output field results were changed from binary 0 and 1 to Yes and No. • The following output fields were added to the **all** version of this command: – Access-type – ppp-regeneration (max-session, setup time) – VRF Name
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD and the Block Roamer Mode output field was changed to Block Foreign-MS Mode output field.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW. • The following output fields were added to the display: – input ACL – output ACL – backup – RADIUS attribute suppress MSISDN – RADIUS attribute suppress IMSI – RADIUS attribute suppress SGSN Address – RADIUS attribute suppress QoS • The format of the apn_username: , apn_password: display fields was changed to apn_username: apn_password:.

Release	Modification
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(2)XU. The following fields were added to the display: • cac policy • idle timeout • input bandwidth pool • input service-policy • output bandwidth pool • Service Mode • session timeout
12.3(8)XU2	This command was integrated into Cisco IOS Release 12.3(2)XU2 and the **single pdp-session** field was the display.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU and the following field was added to the display: • apn_type: Virtual pre-authenticate
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB and the following field was added to the display: • P-CSCF group name
12.4(9)XG	This command was integrated into Cisco IOS Release 12.4(9)XG and the following fields were added to the **show gprs access-point** *access-point-index* display: • IPV6 enable • IPV6 base template • IPV6 uplink access list • IPV6 downline access list • IPV6 dynamic_address_pool • IPV6 local prefix pool • IPV6 primary dns • IPV6secondary dns
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ and the following field was added to the display: • Delete PDP upon update failure • Interim periodic accounting

Usage Guidelines

Use the access-point-index argument to specify a particular access point number for which you want to obtain information.

Use the **address-allocation** keyword to obtain information about dynamically allocated MS addresses and lease terms per access point.

Use the **all** keyword to obtain information about all access points in an abbreviated format.

Examples

Example 1

The following is sample output from the **show gprs access-point** command for access point 1, which is a real access point:

```
Router# show gprs access-point 1

    apn_index 1          apn_name = gprs.corporate.com
    apn_mode: transparent
    apn-type: Real
    accounting: Disable
    interim accounting: Disable
    interim periodic: Disable
    wait_accounting: Disable
    interim periodic accounting:
    input ACL: None, output ACL: None
    dynamic_address_pool: dhcp-proxy-client
    apn_dhcp_server: 10.99.100.5     backup: 10.99.100.4
    apn_dhcp_gateway_addr: 10.27.1.1
    apn_authentication_server_group: abc
    apn_accounting_server_group: abc1
    apn_username:  apn_password:
    subscribe_required: No
    deactivate_pdp_context_on violation: Yes
    Block Foreign-MS Mode: Disable
    VPN: Disable  (VRF Name : None)
    GPRS vaccess interface: Virtual-Access2
    RADIUS attribute suppress MSISDN: Disabled
    RADIUS attribute suppress IMSI: Disabled
    RADIUS attribute suppress SGSN Address: Disabled
    RADIUS attribute suppress QoS: Disabled
    number of ip_address_allocated 0
    session timeout: 0
    idle timeout: 0
    Security features
     Verify mobile source addr: enable
     Verify mobile destination addr: enable

    Traffic redirection:
     Mobile-to-mobile: destination 1.1.1.1

    Total number of PDP in this APN :0

    aggregate:
    In APN:    Disable

    In Global: Disable

    primary dns: 0.0.0.0
    secondary dns: 0.0.0.0
    primary nbns: 0.0.0.0
    secondary nbns: 0.0.0.0
    Service Mode: Operational
```

```
cac policy: p1
input bandwidth pool: pool1
output bandwidth pool: pool2
input service-policy: pdp-class-pdp
single pdp-session: Mandatory

P-CSCF group name: GroupA
IPV6 enable
Delete PDP upon update failure
IPV6 base vtemplate : 10
IPv6 uplink access list: NONE
IPV6 downlink access list : NONE
IPV6 dynamic_address_pool : local
IPV6 local prefix pool : localv6
IPV6 primary dns : 2001:1:2:3::123
IPV6 secondary dns: 3001:1:2:3::123

DHCP address release sent by GGSN    0
```

Table 7 describes the fields show in the example.

Table 7 show gprs access-point Field Descriptions

Field	Description
apn_index	Number assigned to the access point.
apn_name	Access point name.
apn_mode	Current setting for the **access-mode** command: • Transparent—Users are allowed access without authorization or authentication. • Non-transparent—Users must be authenticated by the GGSN acting as a proxy for the authentication.
apn-type	Current setting for the **access-type** command: • Real—APN type that corresponds to a physical interface to an external network on the GGSN. • Virtual—APN type that is not associated with any specific physical target network. • Virtual pre-authenticate—Pre-authentication-based APN type that uses AAA-based user profiles to return the target APN to which the Create PDP Context request is next routed.
charging service mode	Indicates whether the charging functions of a GGSN are in operational or maintenance mode.
Delete PDP upon update failure	Current setting for the **gtp update qos-fail delete** command: • Enabled—The GGSN deletes a PDP context if a GGSN-initiated QoS update fails. • Disabled—The GGSN does not delete a PDP context if a GGSN-initiated QoS update fails.

Table 7 show gprs access-point Field Descriptions (continued)

Field	Description
accounting	Current status of accounting services at the APN: • Enable—Accounting services are enabled at the APN. This is the default for non-transparent access APNs. • Disable—Accounting services are disabled at the APN. This is the default for transparent access APNs. You can configure an APN for accounting services by using the **aaa-accounting** command in access point configuration mode.
interim accounting	Indicates whether the ability to send interim accounting records to an accounting server after a routing area update or QoS change has been made is configured by using the **aaa-accounting interim update** command. The possible values are enabled or disabled.
interim periodic	Indicates the time interval at which the periodic accounting records are sent by the GGSN. The possible values are Disabled' and Enabled (with periodic interval value in minutes) or Enabled with (use Attribute 85).
wait_accounting	Current status of RADIUS accounting response message waiting at the APN: • Enable—GGSN waits for an accounting response message from the RADIUS server before sending an Activate PDP Context request to the SGSN. • Disable—GGSN sends an Activate PDP Context request to the SGSN after sending an accounting request to the RADIUS server. The GGSN does not wait for a RADIUS accounting response. You can configure RADIUS accounting response message waiting by using the **gprs gtp response-message wait-accounting** command in global configuration mode, or the **response-message wait-accounting** command in access point configuration mode.
input ACL	IP access list for inbound packets (Gi to Gn interfaces).
output ACL	IP access list for outbound packets (Gn to Gi interfaces).
dynamic_address_pool	Current setting for the **ip-address-pool** command.
apn_dhcp_server	IP address of the DHCP server, if configured.
backup	IP address of the backup DHCP server, if configured.
apn_dhcp_gateway_addr	IP address of the DHCP gateway, if an address has been configured.
apn_authentication_server_group	Name of the AAA server group that is providing authentication services.
apn_accounting_server_group	Name of the AAA server group that is providing accounting services.
apn_username	Username specified in the **anonymous user** command. If the **anonymous user** command is not configured, this field will be blank.

Table 7 show gprs access-point Field Descriptions (continued)

Field	Description
apn_password	Password specified in the **anonymous user** command. If the **anonymous user** command is not configured, this field will be blank.
subscribe_required	Current setting for the **subscription-required** command: • No—No subscription is required. • Yes—Subscription is required for access point users. The GGSN looks for the "subscription verified" selection mode in the Create PDP Context request to establish the session.
deactivate_pdp_context_on violation	Current setting for the **access-violation** command: • No—User packets are discarded. • Yes—Mobile sessions are terminated when there is an access violation.
Block Foreign-MS Mode	Current setting for the **block-foreign-ms** command: • Enable—Blocking for foreign MSs is configured. • Disable—Blocking for foreign MSs is not configured.
VPN	Indicates whether a Virtual Private Network (VPN) is enabled or disabled at the access point. **Note** VRF is not supported for IPv6 PDPs. Therefore, if the **ipv6** command is configured on an APN on which VRF is enabled, the IPv4 PDPs are routed in VRF, but the IPv6 PDPs are routed in the global routing table.
GPRS vaccess interface	Name of the virtual access interface associated with the VPN. If no VPN is configured at the access point, the name of the virtual access interface for the GGSN virtual template is shown, which is always Virtual-Access1.
RADIUS attribute suppress MSISDN	Current setting for the **msisdn suppression** command: • Enabled—GGSN overrides or suppresses the Mobile Subscriber ISDN (MSISDN) number in its RADIUS authentication. • Disabled—GGSN does not override or suppress the MSISDN number in its RADIUS authentication.
RADIUS attribute suppress IMSI	Current setting for the **radius attribute suppress imsi** command: • Enabled—GGSN suppresses the 3GPP-IMSI number in its authentication and accounting requests to a RADIUS server. • Disabled—GGSN does not suppress the 3GPP-IMSI number in its authentication and accounting requests to a RADIUS server.

Table 7 show gprs access-point Field Descriptions (continued)

Field	Description
RADIUS attribute suppress SGSN Address	Current setting for the **radius attribute suppress sgsn-address** command: • Enabled—GGSN suppresses the 3rd Generation Partnership Program (3GPP) Vendor-Specific Attribute (VSA) 3GPP-SGSN-Address subattribute in its RADIUS authentication and accounting requests. • Disabled—GGSN does not suppress the 3GPP VSA 3GPP-SGSN-Address subattribute in its RADIUS authentication and accounting requests.
RADIUS attribute suppress QoS	Current setting for the **radius attribute suppress qos** command: • Enabled—GGSN suppresses the 3GPP VSA 3GPP-QoS-Profile subattribute in its RADIUS authentication and accounting requests. • Disabled—GGSN does not suppress the 3GPP VSA 3GPP-QoS-Profile subattribute in its RADIUS authentication and accounting requests.
number of ip_address_allocated	Number of IP addresses allocated to MS users.
session timeout	Amount of time that the GGSN waits before purging mobile sessions for the access point configured by using the **gtp pdp-context timeout session** command in access point configuration mode.
idle_timeout	Number of seconds the GGSN allows a PDP context to be idle before terminating the context as configured by using the **gprs gtp pdp-context timeout idle** global configuration command.
Verify mobile source addr	Current setting for the **security verify source** command: • Enabled—GGSN verifies the source IP address of upstream Transport Protocol Data Unit (TPDUs) against addresses previously assigned to MSs. • Disabled—GGSN does not verify the source IP address of upstream TPDUs against addresses previously assigned to MSs.
Verify mobile destination addr	Current setting for the **security verify destination** command: • Enabled—GGSN verifies the destination address of upstream TPDUs against the global list of Public Land Mobile Network (PLMN) addresses specified using the **gprs plmn ip address** command. • Disabled—GGSN does not verify the destination address of upstream TPDUs against the global list of PLMN addresses specified using the **gprs plmn ip address** command.
Mobile-to-Mobile	Current setting for the **redirect intermobile ip** command.
Total number of PDP in this APN	Number of active PDP contexts for this access point.

Table 7 show gprs access-point Field Descriptions (continued)

Field	Description
aggregate	Route aggregation configuration information on the GGSN. The output display includes the "In APN" field for configuration information for the access point, and the "In global" field for global configuration on the GGSN. The output field may contain the following information: • IP network address and mask for which PDP requests on the access point will be collectively routed over the virtual template interface on the GGSN. IP address and mask information appears if an aggregate range has been configured on the GGSN. • auto—Indicates that the GGSN uses the allocated IP mask from the DHCP (IPv4 PDPs) or RADIUS server to perform route aggregation on the APN. The keyword auto appears when the APN has been configured with the **aggregate auto** command in access point configuration mode. This value applies only to the APN. • Disable—Indicates that route aggregation is not configured at either the APN or global level.
primary dns	IP address of the primary DNS to be sent in Create PDP Context responses at the access point.
secondary dns	IP address of the secondary (backup) DNS to be sent in Create PDP Context responses at the access point
primary nbns	IP address of the primary NetBIOS Name Service (NBNS) to be sent in Create PDP Context responses at the access point.
secondary nbns	IP address of the secondary (backup) NBNS to be sent in Create PDP Context response at the access point.
Service Mode	Indicates whether a GGSN is in operational mode or maintenance mode.
cac policy	Name of the CAC maximum QoS policy applied to the APN, if any.
input bandwidth pool	Name of the bandwidth pool, if any, applied to the output (Gn) interface in the downlink direction.
output bandwidth pool	Name of the bandwidth pool, if any, applied to the output (Gi) interface in the uplink direction.
input service-policy	Service policy attached to the APN using the **service-policy** access point configuration command.

Table 7 show gprs access-point Field Descriptions (continued)

Field	Description
single pdp-session	Whether the GGSN has been configured to delete the primary PDP context, and any associated secondary PDP contexts, of a *hanging* PDP session upon receiving a new Create PDP Context request from the same MS that shares the same IP address of the hanging PDP context. Possible values are: • Enabled—The feature is enabled on the APN and applies to all users for whom the "gtp-pdp-session=single-session" Cisco VSA has been defined in their RADIUS user profile. • Disabled—The feature is disabled on the access point and does not apply to any user regardless of the RADIUS user profile configuration. • Mandatory—The feature is enabled on the APN and applies to all users on that APN regardless of the RADIUS user profile configuration.
P-CSCF group name	Name of the P-CSCF server group(s) used by this APN for P-CSCF Discovery.
IPV6 enable	Current setting for the **ipv6** command: • Enabled—Access point is configured to allow both IPv4 and IPv6 PDP contexts. • Exclusive—Access point is configured to allow only IPv6 PDP contexts.
IPV6 base template	Virtual template interface, which contains IPv6 routing advertisements (RAs) parameters, for an APN to copy to create virtual subinterfaces for IPv6 PDP contexts.
IPV6 uplink access list	IPv6 access list for inbound packets.
IPV6 downlink access list	IPv6 access list for outbound packets.
IPV6 dynamic_address_pool	Current setting for the **ipv6 ipv6-address-pool** command.
IPV6 local prefix pool	Local IPv6 prefix pool.
IPV6 primary dns	IPv6 address of the primary IPv6 DNS to be sent in Create PDP Context responses at the access point.
IPV6 secondary dns	IPv6 address of the secondary (backup) IPv6 DNS to be sent in Create PDP Context responses at the access point
VRF name	Name assigned to the VPN Routing and Forwarding instance. A value of None appears when VRF is not enabled at the access point.

Example 2

The following is sample output from the **show gprs access-point address-allocation** command:

```
router# show gprs access-point 8 address-allocation

TID                     PDP_ADDRESS

1111111100000099        10.88.105.227
1111111100000191        10.88.105.7
1111111100000192        10.88.105.70
1111111100000297        10.88.106.162
1111111100000298        10.88.106.169
1111111100000299        10.88.106.161
1111111100000391        10.88.106.150
1111111100000392        10.88.106.25
1111111100000442        10.88.106.196
1111111100000443        10.88.106.197
1111111100000886        10.88.108.153
1111111100000887        10.88.108.158
2222222200000000        10.88.111.255
```

Table 8 describes the fields show in the display.

Table 8 show gprs access-point address-allocation Field Descriptions

Field	Description
TID	Tunnel ID for the Create PDP Context request on the APN.
PDP_ADDRESS	IP address assigned to the Create PDP Context request on the APN.

Example 3

The following is sample output of the **show gprs access-point all** command:

```
router# show gprs access-point all

There are 3 Access-Points configured

Index   Mode            Access-type    AccessPointName      VRF Name
-------------------------------------------------------------------------
1       transparent        Real        corporate_1.com       corporate_1.com
        ppp-regeneration (max-session: 10000, setup-time: 60)
-------------------------------------------------------------------------
2       non-transparent    Real        corporate_2.com
-------------------------------------------------------------------------
3       transparent        Virtual     corporate_3.com
-------------------------------------------------------------------------
```

Table 9 describes the fields show in the display.

Table 9 show gprs access-point all Field Descriptions

Field	Description
Index	Integer assigned to the access point in the GGSN configuration. The index number is used to reference an APN in GGSN commands.
Mode	Authorization configured on the access point. The possible values are: • transparent—Users who access the PDN through the access point associated with the current virtual template are allowed access without authorization or authentication. • non-transparent—Users who access the PDN through the current virtual template must be authenticated by the GGSN acting as a proxy for the authentication.
Access-type	Type of access point. The possible values are: • Real—APN type that corresponds to an external physical network on the GGSN. This is the default value. • Virtual—APN type that is not associated with any specific physical target network on the GGSN. Virtual APNs are used to simply HLR provisioning in the PLMN.
AccessPointName	Access point network ID, which is commonly an Internet domain name.
VRF Name	Name of the VPN routing and forwarding instance associated with the APN.
ppp-regeneration (max-session, setup-time)	PPP regeneration session parameters configured at the access point: • max-session—Maximum number of PPP regenerated sessions allowed at the access point. • setup-time—Maximum amount of time (between 1 and 65535 seconds) within which a PPP regenerated session must be established.

Related Commands

Command	Description
access-point	Specifies an access point number and enters access point configuration mode.

show gprs access-point statistics

To display data volume and packet data protocol (PDP) activation and deactivation statistics for access points on the gateway GPRS support node (GGSN), use the **show gprs access-point statistics** command in privileged EXEC mode.

To display data volume and PDP activation and deactivation statistics for access points on the gateway GPRS support node (GGSN), use the **show gprs access-point statistics** command in privileged EXEC mode.

show gprs access-point statistics {*access-point-index* | **all**}

Syntax Description

access-point-index	Index number of an access point. Statistics for that access point are shown.
all	Statistics for all access points on the GGSN are shown.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU and the following new output fields were added: • DHCP address requests sent by GGSN • DHCP address requests successful • DHCP address release sent by GGSN • downstream packet count • upstream packet count
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Release	Modification
12.4(9)XG	This command was integrated into Cisco IOS Release 12.4(9)XG and the following IPv6-related fields were added to the **show gprs access-point statistics access-point-index** command display: • ms init ipv6 pdp activation • successful ms init ipv6 pdp activation • dynamic ipv6 PDP activation • successful dynamic ipv6 activation • ms init ipv6 pdp deactivation • successful ms init ipv6 pdp deactivation • ggsn init ipv6 pdp deactivation • successful ggsn init ipv6 pdp deactivation • network init ipv6 pdp deactivation • successful network init ipv6 pdp deactivation • upstream ipv6 data bytes • upstream ipv6 data pak • downstream ipv6 data bytes • downstream ipv6 pak
12.4(15)XQ	This command was integrated into Cisco IOS Relesae 12.4(15)XQ and the following fields were added to the display: • PDP update initiated by GGSN • Successful PDP update initiated by GGSN • Total number of successful COA requests • Number of times direct tunnel enabled

Usage Guidelines

Use the **show gprs access-point statistics** command to display data volume and PDP activation and deactivation statistics for access points on the GGSN.

Use the *access-point-index* argument to specify a particular access point number for which you want to obtain information.

Use the **all** keyword to obtain information about all access points in an abbreviated format.

Examples

The following example displays PDP context activation and deactivation statistics for all access points on the GGSN:

```
router# show gprs access-point statistics 3
   PDP activation initiated by MS:                          11
   PDP update initiated by GGSN                              0
   Successful PDP update initiated by GGSN                   0
   Successful PDP activation initiated by MS:                8
   *Dynamic PDP activation initiated by MS:                 11
   Successful dynamic activation initiated by MS:            8
   PDP deactivation initiated by MS:                         0
   Successful PDP deactivation initiated by MS:              0
   Network initiated PDP activation:                         0
   Successful network initiated PDP activation:              0
   PDP deactivation initiated by GGSN:                       4
   Successful PDP deactivation initiated by GGSN:            3
   upstream data volume in octets:                           0
   *downstream data volume in octets:                        0
   upstream packet count:                                    0
   downstream packet count:                                  0
   *DHCP address requests sent by GGSN:                      0
   *DHCP address requests successful:                        0
   *DHCP address release sent by GGSN:                       0

   ms init ipv6 pdp activation                              11
   successful ms init ipv6 pdp activation                    8
   dynamic ipv6 pdp activation                              11
   successful dynamic v6 pdp activation                      8
   ms init ipv6 pdp deactivation                             0
   successful ms init v6 pdp deactivation                    0
   ggsn init ipv6 pdp deactivation                           4
   successful ggsn init v6 pdp deactivation                  3
   network init ipv6 pdp deactivation                        0
   successful network init ipv6 pdp deactivation             0

   upstream ipv6 data bytes                                192
   upstream ipv6 data pak                                    3
   downstream ipv6 data bytes                             3552
   downstream ipv6 data pak                                 48

   Total number of successful COA requests                   0
   Number of times direct tunnel enabled                     0
```

Table 10 show gprs access-point statistics Field Descriptions

Field	Description
active PDP	Number of IPv4 PDP contexts that are currently established on the GGSN.
downstream data volume in octets	Number of bytes of data received by the GGSN from the PDN, or network.
downstream packet count	Downstream traffic byte counts.
DHCP address release sent by GGSN	Number of DHCP release packets sent by a DHCP server to the GGSN.
DHCP address requests sent by GGSN	Number of DHCP request packets sent to a DHCP server by the GGSN.
DHCP address requests successful	Number of DHCP requests that were successful.

Table 10 show gprs access-point statistics Field Descriptions (continued)

Field	Description
Dest addr violation	Number of IPv4 packets (and bytes) dropped by the GGSN because of a source address violation. This field displays only when the **security verify destination** command is configured. This field does not apply to APNs using VRF. In addition, verification of destination addresses does not apply to GTP-PPP regeneration or GTP-PPP with L2TP.
Dynamic PDP activation initiated by MS	Number of Create PDP Context Request messages received by the GGSN from an MS without a PDP address. (Duplicate requests are not counted.)
downstream ipv6 data bytes	Number of bytes of IPv6 data received by the GGSN from the PDN, or network.
downstream ipv6 pak	Downstream IPv6 traffic byte counts.
dynamic ipv6 PDP activation	Number of IPv6 Create PDP Context requests received by the GGSN from an MS requesting dynamic IPv6 address allocation.
ggsn init ipv6 pdp deactivation	Number of IPv6 PDP context deactivation requests initiated by the GGSN.
upstream ipv6 data bytes	Number of bytes of IPv6 data received by the GGSN from the SGSN.
upstream ipv6 data pak	Upstream IPv6 traffic byte counts.
ms init ipv6 pdp activation	Number of IPv6 Create PDP Context requests received by the GGSN that were initiated by the MS.
ms init ipv6 pdp deactivation	Number of IPv6 Delete PDP Context requests received by the GGSN that were initiated by the MS.
Number of times direct tunnel enabled	Number of direct tunnel PDPs established.
network init ipv6 pdp deactivation	Number of IPv6 Create PDP Context Request messages received by the GGSN that were network-initiated.
successful dynamic ipv6 activation	Number of successful IPv6 PDP context creations initiated by mobile user that used dynamic ipv6 address allocation.
successful ggsn init ipv6 pdp deactivation	Number of IPv6 PDP contexts that were successfully deactivated by a GGSN-initiated request.
successful ms init ipv6 pdp activation	Number of successful IPv6 PDP context creations initiated by a SGSN-initiated request.
successful ms init ipv6 pdp deactivation	Number of IPv6 PDP contexts that were successfully deactivated by a SGSN-initiated request.
successful network init ipv6 pdp activation	Number of IPv6 PDP contexts that were successfully activated by a network-initiated request.
successful network init ipv6 pdp deactivation	Number of IPv6 PDP contexts that were successfully deactivated by a network-initiated request.

Table 10 show gprs access-point statistics Field Descriptions (continued)

Field	Description
Network initiated PDP activation	Number of Create PDP Context Request messages received by the GGSN from network initiation.
PDP activation initiated by MS	Number of Create PDP Context Request messages received by the GGSN from an SGSN. (Duplicate requests are not counted.)
PDP deactivation initiated by GGSN	Number of Delete PDP Context Request messages sent by the GGSN to an SGSN.
PDP deactivation initiated by MS	Number of Delete PDP Context Request messages received by the GGSN from an SGSN. (Duplicate messages are not counted.)
PDP update initiated by GGSN	Number of Update PDP Context Requests that were initiated by the GGSN.
ppp-regeneration (max-session, setup-time)	PPP regeneration session parameters configured at the access point: max-session—Maximum number of PPP regenerated sessions allowed at the access point. setup-time—Maximum amount of time (between 1 and 65535 seconds) within which a PPP regenerated session must be established.
Redirected mobile-to-mobile traffic	Number of IPv4 packets (and bytes) dropped at the APN from which they exit because mobile-to-mobile traffic has been redirected. This field displays only when the **redirect intermobile ip** command is configured.
Src addr violation	Number of IPv4 packets (and bytes) dropped because of source address violation. This field displays only when the **security verify source** command is configured.
Successful dynamic activation initiated by MS	Number of Create PDP Context Response messages sent by the GGSN with a cause value of “GTP_RES_REQACCEPTED”, indicating that the PDP address has been dynamically assigned.
Successful network initiated PDP activation	Number of PDP contexts activated on the GGSN that were initiated by the network.
Successful PDP activation initiated by MS	Number of Create PDP Context Response messages sent by the GGSN with a cause value of “GTP_RES_REQACCEPTED.”
Successful PDP deactivation initiated by GGSN	Number of Delete PDP Context Response messages received by the GGSN from an SGSN.
Successful PDP deactivation initiated by MS	Number of Delete PDP Context Response messages sent by the GGSN to an SGSN with a cause value of “GTP_RES_REQACCEPTED”.
Successful PDP update initiated by GGSN	Number of Update PDP Context Requests initiated by the GGSN that were successful.
Total number of successful CoA requests	Number of CoA requests, containing new QoS, that were successful.
upstream data volume in octets	Number of bytes of data received by the GGSN from the SGSN.
upstream packet count	Upstream traffic byte counts.

Related Commands

Command	Description
clear gprs access-point statistics	Clears statistics counters for a specific access point or for all access points on the GGSN.
show gprs access-point	Displays information about access points on the GGSN.

show gprs access-point throughput statistics

To display throughput statistics for access points on a gateway GPRS support node (GGSN), use the **show gprs access-point throughput statistics** command in privileged EXEC mode.

show gprs access-point throughput statistics {*access-point-index* | **all**}

Syntax Description

access-point-index	Index number of an access point. Statistics for that access point are shown.
all	Statistics for all access points on the GGSN are shown.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs access-point throughput statistics** command to display throughput statistics for access points on the GGSN.

Use the *access-point-index* argument to specify a particular access point number for which you want to obtain information.

Use the **all** keyword to obtain information about all access points in an abbreviated format.

Examples

The following example displays throughput statistics for access point 1:

```
GGSN# show gprs access-point throughput statistics 1

Collection interval - 1 min, Last collected at - 1 min back
    upstream data volume in octets:     0
    downstream data volume in octets:   0
    upstream packet count:              0
    downstream packet count:            0

  Collection interval - 2 min, Last collected at - 2 min back
    upstream data volume in octets:     0
    downstream data volume in octets:   0
    upstream packet count:              0
    downstream packet count:            0
```

Related Commands

Command	Description
clear gprs access-point statistics	Clears statistics counters for a specific access point or for all access points on the GGSN.
gprs throughput interval	Configures the interval at which the GGSN collects throughput data for APNs.
show gprs access-point	Displays information about access points on the GGSN.

show gprs bandwidth-pool status

To display a list of configured CAC bandwidth pools, along with their status, use the **show gprs bandwidth-pool status** command in privileged EXEC mode.

show gprs bandwidth-pool status *pool-name*

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs bandwidth-pool status** command to display a list of configured bandwidth pools and their status.

Examples

The following is sample output of the **show gprs bandwidth-pool status** command:

```
GGSN#show gprs bandwith-pool status bwpool1

BW Name:bwpool1
Total BW:1000000
Available BW:0
=====================================================================
conversational                Total BW:400000      Available BW:400000
streaming                     Total BW:300000      Available BW:300000
interactive                   Total BW:200000      Available BW:200000
background                    Total BW:100000      Available BW:100000
```

Table 8 describes the fields shown in the display.

Table 11 show gprs bandwidth-pool status Field Descriptions

Field	Description
BW Name	Name of the bandwidth pool as defined using the **gprs bandwidth-pool** global configuration command and each sub traffic class -based pools defined using the **traffic-class** bandwidth pool configuration command.
Total BW	Total amount of bandwidth, in kilobits per second, allocated to a bandwidth pool using the **bandwidth** bandwidth pool configuration command. Also, the total bandwidth allocated to a sub traffic class-based pool, defined as a percentage or absolute value using the **traffic-class** bandwidth pool configuration command.
Available BW	Remaining amount of bandwidth, in kilobits per second, for a bandwidth pool and the remaining available bandwidth (in percentage or absolute value) for each sub traffic class-based pool.
conversational	Amount of the bandwidth pool bandwidth, in kilobits per second or as a percentage, allocated to the Conversational traffic class and the bandwidth currently available.
streaming	Amount of the bandwidth pool bandwidth, in kilobits per second or as a percentage, allocated to the Streaming traffic class and the bandwidth currently available.
interactive	Amount of the bandwidth pool bandwidth, in kilobits per second or as a percentage, allocated to the Interactive traffic class and the bandwidth currently available.
background	Amount of the bandwidth pool bandwidth, in kilobits per second or as a percentage, allocated to the Background traffic class and the bandwidth currently available.

Related Commands

Command	Description
bandwidth	Defines the total bandwidth, in kilobits per second, for a bandwidth pool.
bandwidth-pool	Applies a bandwidth pool to an APN.
gprs qos bandwidth-pool	Creates or modifies a bandwidth pool.
traffic-class	Allocates bandwidth pool bandwidth to a specific traffic class.

show gprs charging parameters

To display information about the current gateway GPRS support note (GGSN) charging configuration, use the **show gprs charging parameters** command in privileged EXEC mode.

show gprs charging parameters

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX. The following output fields were added to the display: • Charging CDR Option Local Record Sequence Number • Charging CDR Option No Partial CDR Generation • Charging CDR Option Node ID • Charging CDR Option Packet Count • Charging Change Condition Limit • Charging Send Buffer Size • Charging GTP' Port Number • Charging MCC Code • Charging MNC Code • Charging Roamers CDR Only • Charging HPLMN Matching Criteria • Charging SGSN Limit The following output fields were removed from the display: • Charging MCC Code • Charging MNC Code • Charging HPLMN Matching Criteria
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.

Release	Modification
12.2(8)YW	This command was integrated into the Cisco IOS Release 12.2(8)YW. • The Charging Path Protocol field was changed from binary 0 and 1 to udp and tcp. • The Charging qos-info output field was changed to Charging release. • The following output fields were added to the display: – Charging Time Limit – Charging qos-info – Charging Transfer Format. – GTP' use short header
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU and the following fields were added to the display: • Access Point Name • ChCh Selection Mode • Default Tertiary Charging Gateway Address • Dynamic Address • External Charging ID • PDP Type • Served PDP Address • Service Mode • SGSN PLMN ID
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into the Cisco IOS Release 12.3(14)YU and the following fields were added to the display: • Access Point Name Virtual • Camel Charging Info • IMEISV • MS Time Zone • Radio Access Technology • User Location Information
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.
12.4(9)XG	This command was integrated into Cisco IOS Release 12.4(9)XG.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ and the following fields were added to the display: • GGSN's iSCSI profile • Charging Source Interface

Usage Guidelines

Use the **show gprs charging parameters** command to display the currently active charging parameters for the GGSN.

Examples

The following is sample output of the **show gprs charging parameters** command:

```
Router# show gprs charging parameters

GPRS Charging Protocol Parameters
        ================================

* Default Charging Gateway Address:             <172.17.1.2>
* Default Backup Charging Gateway Address:      UNDEFINED.
* Default Tertiary Charging Gateway Address:UNDEFINED.
* Backup data store (PSD) Address:          UNDEFINED
* Retrieve only data store (PSD) Address    UNDEFINED
* GGSN's iSCSI profile:                     TARGET_LINUX
* Current Active Charging Gateway Address:  <172.17.1.2>
* Current Backup Charging Gateway Address:  UNDEFINED.
* Charging Server Switch-Over Timer:        <60> seconds.
* Charging Path Protocol:                   udp
* GTP' use short header:                    DISABLED
* Charging Message Options:
   Transfer Request:
 - Packet Transfer Command IE:              DISABLED.
   Transfer Response:
 - Number Responded:                        DISABLED.
* Charging MAP DATA TOS:                    <3>
* Charging Transfer Interval:               <105> seconds.
* Charging Transfer Threshold:              <1048576> bytes.
* Charging CDR Aggregation Limit:           <255> CDRs per msg.
* Charging Packet Queue Size:               <128> messages.
* Charging Gateway Path Request Timer:      <0> Minutes.
* Charging Change Condition Limit:          <5>
* Charging SGSN Limit:                      DISABLED.
* Charging Time Limit:                      <0>
* Charging Send Buffer Size:                <1460>
* Charging Port Number:                     <3386>
* Charging Roamers CDR Only:                DISABLED.
* Charging CDR Option:
- Local Record Sequence Number:             DISABLED.
 - APN Selection Mode:                      DISABLED.
 - ChCh Selection Mode:                     DISABLED.
 - Radio Access Type - RAT:                 DISABLED.
 - User Location Information:               ENABLED.
 - MS Time Zone:                            ENABLED.
 - IMEISV:                                  DISABLED.
 - CAMEL Charging Info:                     ENABLED.
 - SGSN PLMN ID:                            DISABLED.
 - Dynamic Address:                         ENABLED.
 - Served PDP Address:                      ENABLED.
 - PDP Type:                                ENABLED.
 - Access Point Name:                       ENABLED.
 - Network Initiated PDP:                   ENABLED.
 - No Partial CDR Generation:               DISABLED.
 - Node ID:                                 DISABLED.
 - Packet Count:                            DISABLED.
 - Served MSISDN:                           DISABLED.
 - Private Echo:                            DISABLED.
* Charging release:                         5
* Charging Tariff Time Changes:
- NO Tariff Time Changes
```

```
* Charging Service Mode:                    OPERATIONAL
* Charging Source Interface                 loopbackX
* Backup data store (PSD) Address:          172.28.28.28
* Retrieve only data store (PSD) Address    192.13.13.13
```

Table 12 describes the fields shown in the display.

Table 12 show gprs charging parameters Field Descriptions

Field	Description
Backup data store (PSD) Address	IP address of the local Persistent Storage Device (PSD) to which G-CDRs are backed up if a charging gateway is unavailable.
Charging CDR Aggregation Limit	Maximum number of CDRs that the GGSN aggregates in a charging data transfer message to the charging gateway. You can configure this limit using the **gprs charging cdr-aggregation-limit** command.
Charging CDR Option: Access Point Name Charging CDR Option: Access Point Name Virtual	Status indicating if the GGSN provides the APN or virtual APN parameter in G-CDRs. Possible values are enabled or disabled. You can enable the GGSN to provide the APN or virtual PAN parameter in G-CDRs using the **gprs charging cdr-option apn** and **gprs charging cdr-option apn virtual** commands.
Charging CDR Option: APN Selection Mode	Status indicating if the GGSN provides the reason code for APN selection in G-CDRs. The possible values are enabled or disabled. You can enable the GGSN to provide the APN selection mode in G-CDRs using the **gprs charging cdr-option apn-selection-mode** command.
Charging CDR Option: CAMEL Charging Info	Status indicating if the GGSN includes a copy of the tag and length of the Customized Application for Mobile Enhanced Logic (CAMEL) from the S-CDR in G-CDRs. You can enable the GGSN to include a copy of the tag and length of the CAMEL in G-CDRs using the **gprs charging cdr-option camel-charge-info** command.
Charging CDR Option: ChCh Selection Mode	Status indicating if the GGSN includes the charging characteristics selection mode parameter in G-CDRs. Possible values are enabled or disabled.
Charging CDR Option: Dynamic Address	Status indicating if the GGSN includes the dynamic address flag parameter in G-CDRs. Possible values are enabled or disabled. You can enable the GGSN to provide the APN parameter in G-CDRs using the **gprs charging cdr-option dynamic-address** command.

Table 12 show gprs charging parameters Field Descriptions (continued)

Field	Description
Charging CDR Option: IMEISV	Status indicating if the GGSN includes the International Mobile Equipment Identity IMEI software version (IMEISIV) in G-CDRs. You can enable the GGSN to include the IMEISIV IE in G-CDRs using the **gprs charging cdr-option imeisv** command.
Charging CDR Option: Local Record Sequence Number	Status indicating if the GGSN uses the local record sequence field in G-CDRs. The possible values are enabled or disabled. You can enable the GGSN to use the local record sequence field in G-CDRs using the **gprs charging cdr-option local-record-sequence-number** command.
Charging CDR Option: MS Time Zone	Status indicating if the GGSN includes the MS time zone (MSTZ) in G-CDRs. You can enable the GGSN to provide MSTZ in G-CDRs using the **gprs charging cdr-option ms-time-zone** command.
Charging CDR Option: Network Initiated PDP	Status indicating if the GGSN includes the NIP parameter in G-CDRs. The possible values are enabled or disabled. You can enable the GGSN to use the local record sequence field in G-CDRs using the **gprs charging cdr-option nip** command.
Charging CDR Option: No Partial CDR Generation	Status indicating if the GGSN can create partial CDRs. The possible values are enabled or disabled. You can disable partial CDR generation by the GGSN using the **gprs charging cdr-option no-partial-cdr-generation** command.
Charging CDR Option: Node ID	Status indicating if the GGSN specifies the name of the node that generated the CDR in the node ID field of the G-CDR. The possible values are enabled or disabled. You can enable the GGSN to use the node ID field in G-CDRs using the **gprs charging cdr-option node-id** command.
Charging CDR Option: Packet Count	Status indicating if the GGSN provides uplink and downlink packet counts in the optional record extension field of a G-CDR. The possible values are ON or OFF. You can enable the GGSN to provide packet counts using the **gprs charging cdr-option packet-count** command.
Charging CDR Option: PDP Type	Status indicating if the GGSN includes the PDP type parameter in G-CDRs. The possible values are enabled or disabled. You can enable the GGSN to provide packet counts using the **gprs charging cdr-option pdp-type** command.

Table 12 show gprs charging parameters Field Descriptions (continued)

Field	Description
Charging CDR Option: Private Echo	Status indicating if the GGSN uses private echo signaling for flow control. The possible values are enabled or disabled. You can enable private echo signaling using the **gprs charging flow-control private-echo** command.
Charging CDR Option: Radio Access Type-RAT	Status indicating if the GGSN includes the radio access technology (RAT) IE in G-CDRs. You can enable the GGSN to provide the RAT IE in G-CDRs using the **gprs charging cdr-option rat-type** command.
Charging CDR Option: Served MSISDN	Status indicating if the GGSN provides the mobile station integrated services digital network number from the Create PDP Context request in a G-CDR. The possible values are enabled or disabled. You can enable the GGSN to provide the MSISDN number using the **gprs charging cdr-option served-msisdn** command.
Charging CDR Option: Served PDP Address	Status indicating if the GGSN provides the PDP address from the Create PDP Context request in a G-CDR. Possible values are enabled or disabled. You can enable this feature using the **gprs charging cdr-option pdp-address** command.
Charging CDR Option: SGSN PLMN ID	Status indicating if the GGSN includes the SGSN PLMN identifier in G-CDRs. The possible values are enabled or disabled. You can enable the GGSN to include the SGSN PLMN identifier using the **gprs charging cdr-option sgsn-plmn** command.
Charging CDR Option: User Location Information	Status indicating if the GGSN includes the user location information (ULI) IE in G-CDRs. You can configure the GGSN to include the ULI IE in G-CDRs using the **gprs charging cdr-option user-loc-info** command.
Charging Change Condition Limit	Maximum number of charging containers in each G-CDR. You can configure the change condition limit using the **gprs charging container change-limit** command.
Charging Gateway Path Request Timer	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. You can configure the path request timer using the **gprs charging cg-path-requests** command.

Table 12 show gprs charging parameters Field Descriptions (continued)

Field	Description
Charging Gateway Priority Switchover	Whether or not the GGSN switches over to a charging gateway of higher priority when that gateway becomes active. The possible values are ENABLED (the GGSN switches over to a charging gateway of higher priority when that gateway becomes active) or DISABLED (the GGSN does not switch over to gateways of higher priority when such a gateway becomes active). You can enable the GGSN to switch over to a higher priority charging gateway using the **gprs charging switchover priority** command.
Charging MAP DATA TOS	Type of service (ToS) priority currently configured for GGSN charging packets. Value (between 0 and 5) is set in the precedence bits of the IP header of charging packets. You can configure the ToS mapping using the **gprs charging map data tos** command.
Charging Message Options: Number Responded	Status indicating if the GGSN uses the Number of Requests Responded field instead of the Length field in the Requests Responded IE of Data Record Transfer Response messages. The possible values are enabled or disabled. You can enable the GGSN to use the Number of Requests Responded field using the **gprs charging message transfer-response number-responded** command.
Charging Message Options: Packet Transfer Command IE	Status indicating if the GGSN includes the Packet Transfer Command IE in the Data Record Transfer Request messages. The possible values are enabled or disabled. You can enable the GGSN to include the Packet Transfer Command IE in the Data Record Transfer Request messages using the **gprs charging message transfer-request command-ie** command.
Charging Message Options: Send Possibly Duplicated CDR	Status indicating if the GGSN retransmits Data Record Transfer Request messages (sent to a previously active charging gateway) with the value of the Packet Transfer Request IE set to Send Possibly Duplicate Data Record Packet (2). The possible values are enabled or disabled. To configure the GGSN to retransmit Data Record Transfer Request messages with the value of the Packet Transfer Request IE set to 2, use the **gprs charging message transfer-request possibly-duplicate** command.

Table 12 show gprs charging parameters Field Descriptions (continued)

Field	Description
Charging Message Options: Transfer Request	Whether the GGSN includes the Packet Transfer Command IE in the Data Record Transfer Response messages. The possible values are ENABLED (the GGSN includes the Packet Transfer Command IE) or DISABLED (the GGSN does not include the IE).
Charging Messages Options: Transfer Response	Whether the GGSN is using the Number of Requests Responded field instead or the Length field in the Requests Responded IE of Data Record Transfer Response messages. The possible values are ENABLED (the GGSN uses the Number of Requests Responded field) or DISABLED (the GGSN uses the Length field).
Charging Packet Queue Size	Maximum number of unacknowledged charging data transfer requests that the GGSN maintains in its queue. You can configure the maximum queue size using the **gprs charging packet-queue-size** command.
Charging Path Protocol	Protocol in use between the GGSN and the charging gateway. The possible values are udp or tcp. You can configure the charging path protocol using the **gprs charging path-protocol** command.
Charging Port Number	Destination port of the charging gateway. You can configure the destination port using the **gprs charging port** command.
Charging release	Charging release with which the GGSN is to comply when presenting G-CDRs. Possible values are 98, 99, 4, or 5. You can configure the charging release using the **gprs charging release** command.
Charging Roamers CDR Only	Status of the charging for roamers feature on the GGSN. The possible values are enabled or disabled. You can configure the GGSN to support creation of CDRs for roaming subscribers using the **gprs charging roamers** command.
Charging Send Buffer Size	Size (in bytes) of the buffer that contains the GTP' PDU and signaling messages on the GGSN. You can configure the buffer size using the **gprs charging send-buffer** command.
Charging Server Switch-Over Timer	Amount of time (in seconds) that the GGSN waits before sending charging data to the backup charging gateway, after the active charging gateway fails. You can configure this period of time using the **gprs charging server-switch-timer** command.

Table 12 show gprs charging parameters Field Descriptions (continued)

Field	Description
Charging SGSN Limit	Maximum number of SGSN changes that can occur before the GGSN closes a G-CDR for a particular PDP context.
Charging Source Interface	Loopback interface being used for charging traffic.
Charging Tariff Time Changes	Time of day when GGSN charging tariffs change. You can configure this time using the **gprs charging tariff-time** command.
Charging Transfer Interval	Amount of time (in seconds) that the GGSN waits before checking and sending any closed CDRs to the charging gateway. You can configure this period of time using the **gprs charging transfer interval** command.
Charging Transfer Threshold	Maximum size (in bytes) that the GGSN maintains in a charging container before closing it and updating the CDR. You can configure the container volume using the **gprs charging container volume-threshold** command.
Current Active Charging Gateway Address	IP address of the charging gateway to which the GGSN is currently sending charging data. You can configure the primary charging gateway using the **gprs default charging-gateway** command.
Current Backup Charging Gateway Address	IP address of the backup charging gateway to which the GGSN will send charging data if the current active charging gateway becomes unavailable. You can configure the backup charging gateway using the **gprs default charging-gateway** command.
Default Backup Charging Gateway Address	IP address of the default secondary (backup) charging gateway. You can configure the default backup charging gateway using the **gprs default charging-gateway** command.
Default Tertiary Charging Gateway Address	IP address of the default tertiary (backup) charging gateway. You can configure the default backup charging gateway using the **gprs default charging-gateway** command.
Default Charging Gateway Address	IP address of the default primary charging gateway. You can configure the default primary charging gateway using the **gprs default charging-gateway** command.
GGSN's iSCSI profile	Name of the iSCSI target interface profile configured on the GGSN.

Table 12 show gprs charging parameters Field Descriptions (continued)

Field	Description
GTP' use short header	Whether the GGSN is using the GTP short header (6-byte header). The possible values are ENABLED (the GGSN is using the GTP short header) or DISABLED (the GGSN is using the GTP long header). You can configure the GGSN to use the GTP short header using the **gprs charging header short** command.
Retrieve only data store (PSD) Address	IP address of the remote Persistent Storage Device (PSD) from which G-CDRs are only retrieved.

Related Commands

Command	Description
show gprs charging statistics	Displays cumulative charging statistics for the GGSN.

show gprs charging statistics

To display cumulative charging statistics for the gateway GPRS support node (GGSN), use the **show gprs charging statistics** command in privileged EXEC mode.

show gprs charging statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX, and the statistics were changed to be cumulative since the last restart of the GGSN and the keyword options were removed.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs charging statistics** command to display cumulative charging statistics since the last restart of the GGSN.

Examples

The following is sample output of the **show gprs charging statistics** command:

```
router# show gprs charging statistics all
            GPRS Charging Protocol Statistics
            =================================

   * Total Number of CDRs for Charging:              <200>
   * Total Number of Containers for Charging:        <104>
   * Total Number of CDR_Output_Msgs sent:           <22>

   -- Charging Gateway Statistics --
   * Charging Gateway Down Count:                    <1>
   * Last Charging Gateway Down Time = 2001/11/29 15:23:0
```

Table 10 describes the fields shown in the display.

Table 13 show gprs charging statistics Field Descriptions

Field	Description
Total Number of CDRs for Charging	Cumulative number of open and closed G-CDRs on the GGSN since the last startup of the GGSN.
Total Number of Containers for Charging	Cumulative number of all open and closed charging containers for all G-CDRs on the GGSN since the last startup of the GGSN.
Total Number of CDR_Output_Msgs sent	Cumulative number of G-CDR output messages that the GGSN sent to the charging gateway and received acknowledgment for since the last startup of the GGSN.
Charging Gateway Down Count	Number of times that the charging gateway has transitioned its state (from up or unknown, to down) since the last startup of the GGSN.
Last Charging Gateway Down Time	Recorded system time when the charging gateway was last in a down state. This statistics only appears if a charging gateway has been down.

Related Commands

Command	Description
show gprs charging parameters	Displays information about the current GGSN charging configuration.
show gprs charging status	Displays current charging statistics for the GGSN.

show gprs charging status

To display current charging statistics for the gateway GPRS support node (GGSN), use the **show gprs charging status** command in privileged EXEC mode.

show gprs charging status {**tid** *tunnel_id* | **access-point** *access-point-index* | **all**}

Syntax Description

tid *tunnel_id*	Specifies a tunnel ID for which you want to display charging statistics.
access-point *access-point-index*	Specifies the index of the access point for which you want to display charging statistics.
all	Requests display of all charging statistics.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD and the Number of partial CDRs output field was changed to the Number of closed CDRs buffered.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB and the sgsn_plmn_id field was added to the display.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs charging status** command to display current charging statistics for the GGSN since the last G-CDR was sent.

Examples

Example 1

The following is sample output of the **show gprs charging status tid** command:

```
router# show gprs charging status tid 1102334415151515
                    GPRS Charging Protocol Status for TID
                    =====================================

            * Number of CDRs :                              <1>
```

```
* Number of closed CDRs buffered:                <0>
* Number of Containers:                          <0>

         ** Detail fields of CDR entry **
            =========================
- served_imsi = 0x112 3344151515F5
- sgsn_plmn_id = 0x21F354
- ggsn_address = 10.10.10.1
- charging_id = 68960026
- SGSN change list (total=[1]): [4.4.4.4]
- apn = www.gprs_companya.fr
- pdp_type: - pdp_type_org = 1
- pdp_type_num = 33
- dynamic_addr_flag = 1
- pdp_type.chrg_data_vol_list:
- rec_opening_time = 2003/5/9 10:2:12 <tz_offset:0>
- duration = 0 - cause_rec_closing = 0
- rec_seq_number = 0
```

Table 11 describes the fields shown in the display.

Table 14 show gprs charging status tid Field Descriptions

Field	Description
Number of CDRs	Number of currently open and closed G-CDRs on the GGSN for the specified TID, since the last G-CDR was successfully sent to the charging gateway.
Number of closed CDRs buffered	Number of currently closed G-CDRs that the GGSN has not yet sent to the charging gateway for the specified TID.
Number of Containers	Number of all currently open and closed charging containers for the specified TID, since the last G-CDR was successfully sent to the charging gateway.

Example 2

The following is sample output of the **show gprs charging status access-point** command:

```
router# show gprs charging status access-point 1

                GPRS Charging Protocol Status for APN
                =====================================

* Number of CDRs:                               <96>
* Number of closed CDRs buffered:               <0>
* Number of Containers:                         <0>
```

Table 12 describes the fields shown in the display.

Table 15 show gprs charging status access-point Field Descriptions

Field	Description
Number of CDRs	Number of currently open and closed G-CDRs on the GGSN for the specified access point, since the last G-CDR was successfully sent to the charging gateway.

Table 15 show gprs charging status access-point Field Descriptions (continued)

Field	Description
Number of closed CDRs buffered	Number of currently closed G-CDRs that the GGSN has not yet sent to the charging gateway for the specified access point.
Number of Containers	Number of all currently open and closed charging containers for the specified access point, since the last G-CDR was successfully sent to the charging gateway.

Example 3

The following is sample output of the **show gprs charging status all** command:

```
router# show gprs charging status all
            GPRS Charging Protocol Status
            =============================

   * Number of APNs :                                <1>
   * Number of CDRs :                                <96>
   * Number of closed CDRs buffered:                 <0>
   * Number of Containers buffered:                  <0>
   * Number of pending unack. CDR_Output_Msgs:       <1>
```

Table 13 describes the fields shown in the display.

Table 16 show gprs charging status Field Descriptions

Field	Description
Number of APNs	Number of access points for which charging data has currently been collected. This statistic appears in the **all** version of this command only.
Number of CDRs	Number of currently open and closed G-CDRs on the GGSN since the last G-CDR was successfully sent to the charging gateway. For the **tid** and **access-point** versions of this command, this is the number of currently open and closed G-CDRs for the specified TID or access point.
Number of closed CDRs buffered	Number of currently closed G-CDRs that the GGSN has not yet sent to the charging gateway. For the **tid** and **access-point** versions of this command, this is the number of currently closed G-CDRs for the specified TID or access-point that have not yet been sent to the charging gateway.
Number of Containers buffered	Number of all currently open and closed charging containers since the last G-CDR was successfully sent to the charging gateway.
Number of pending unack. CDR_Output_Msgs	Number of G-CDR output messages sent by the GGSN that are not acknowledged by the charging gateway.

Related Commands

Command	Description
show gprs charging parameters	Displays information about the current GGSN charging configuration.
show gprs charging statistics	Displays cumulative charging statistics for the GGSN.

show gprs gtp ms

To display the currently active MSs on the gateway GPRS support node (GGSN), use the **show gprs gtp ms** command in privileged EXEC mode.

show gprs gtp ms {**imsi** *imsi*| **access-point** *access-point-index* | **all**}

Syntax Description

imsi *imsi*	Displays MSs by International Mobile Subscriber Identity (IMSI). The IMSI can be up to 15 numeric digits. You can obtain the IMSI from the output for the **show gprs gtp ms all** command or the **show gprs gtp pdp-context tid** command.
access-point *access-point-index*	Displays MSs by access point.
all	Displays all MSs.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)YW	This command was introduced.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB. • The MS Addr field was updated to reflect the virtual interface identifier for PPP PDP contexts and the status of PPP PDP with L2TP contexts. • The SGSN MCC/MNC field was added
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs gtp ms** command to display information about the mobile stations that are currently active on the GGSN. You can display the MS information according to access-point or IMSI. You can also display information for all MSs.

Examples

The following example displays information for all MSs:

```
router# show gprs gtp ms all
IMSI               SGSN MCCMNC     MS ADDRESS      APN
112233445565437    12345           10.3.0.1        gprsa.apn.com

223456788765437    67891           10.2.0.1 (Vi5)  gprsb.apn.com
```

The following example displays information for all MSs on access-point 1:

```
router# show gprs gtp ms access-point 1
IMSI                    SGSN MCCMNC    MS ADDRESS      APN
112233445565437         12345          10.3.0.1        gprsa.apn.com
```

The following example displays information for all MSs on IMSI 110406080002045:

```
router# show gprs gtp ms imsi 110406080002045
IMSI               SGSN MCCMNC     MS ADDRESS      APN
110406080002045    12345           10.10.10.2      gprsc.apn.com

 number of pdp:2
 reference count:1
```

Table 14 describes the fields shown in the display.

Table 17 show gprs gtp ms Field Descriptions

Field	Description
IMSI	International mobile subscriber identity for the MSs.
MS ADDRESS	The IP address for the MSs. **Note** For PPP PDP contexts, this field will also display the virtual interface identifier. For PPP PDP with L2TP contexts, this field will also display the state of the PDP context. Possible states are Pending, Forwarded, or Terminating.
APN	Access point name.
number of pdp	Number of PDP contexts on the MSs.
reference count	Internal data structure field. It is used only for internal troubleshooting purposes.
SGSN MCCMNC	MCC/MNC of the SGSN.

Related Commands

Command	Description
show gprs gtp pdp-context	Displays a list of the currently active PDP contexts (mobile sessions).
show gprs gtp status	Displays information about the current status of the GTP on the GGSN (such as activated PDP contexts, throughput, and QoS statistics).

show gprs gtp parameters

To display information about the current GPRS Tunneling Protocol (GTP) configuration on the gateway GPRS support node (GGSN), use the **show gprs gtp parameters** command in privileged EXEC mode.

show gprs gtp parameters

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX. The following output fields were added to the display: • Charging MCC Code • Charging MNC Code • Charging HPLMN Matching Criteria • GTP dynamic echo-timer minimum • GTP dynamic echo-timer smooth factor The following output field was removed: • GTP max hold time for old sgsn PDUs T3_tunnel
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD and the following output field was removed from the display: • GPRS HPLMN Matching Criteria
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU and the following output fields were removed from the display: • GPRS MCC Code • GPRS MNC Code
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.

Usage Guidelines

Use the **show gprs gtp parameters** command to display the current GTP parameters configured on the GGSN.

Examples

The following is sample output of the **show gprs gtp parameters** command:

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

Table 15 describes the fields shown in the display.

Table 18 show gprs gtp parameters Field Descriptions

Field	Description
GTP buffer size for receiving N3_buffer	Current size of the receive buffer (in bytes) that the GGSN uses to receive GTP signaling messages and packets sent through the tunneling protocol. You can configure the N3 buffer using the **gprs gtp n3-buffer-size** command.
GTP dynamic echo-timer minimum	Current minimum time period (in seconds) used by the dynamic echo timer. You can configure the minimum value using the **gprs gtp echo-timer dynamic minimum** command.
GTP dynamic echo-timer smooth factor	Current multiplier used by the GGSN to calculate the T-dynamic for the dynamic echo timer. You can configure the smooth factor using the **gprs gtp echo-timer dynamic smooth-factor** command.
GTP max pdp context	Current maximum number of PDP contexts (mobile sessions) that can be activated on the GGSN. You can configure the maximum number of PDP context requests using the **gprs maximum-pdp-context-allowed** command.
GTP max retry N3_request	Maximum number of times that the GGSN attempts to send a signaling request to an SGSN. You can configure the maximum number of signaling requests made by the GGSN using the **gprs gtp n3-requests** command.

Table 18 show gprs gtp parameters Field Descriptions (continued)

Field	Description
GTP path echo interval	Interval, in seconds, that the GGSN waits before sending an echo-request message to the SGSN. You can configure the path echo interval using the **gprs gtp path-echo-interval** command.
GTP signal max wait time T3_response	Interval, in seconds, that the GGSN waits before responding to a signaling request message. You can configure the maximum interval using the **gprs gtp t3-response** command.

Related Commands

Command	Description
show gprs gtp statistics	Displays the current GTP statistics for the GGSN (such as IE, GTP signaling, and GTP PDU statistics).
show gprs gtp status	Displays information about the current status of the GTP on the GGSN (such as activated PDP contexts, throughput, and QoS statistics).

show gprs gtp path

To display information about one or more GTP paths between the gateway GPRS support node (GGSN) and other GPRS/UMTS devices, use the **show gprs gtp path** command in privileged EXEC mode.

show gprs gtp path {**all** | **remote-address** *ip-address* [**remote-port** *remote-port*] | **version** *gtp-version*}

Syntax Description

all	Displays information for all GTP paths.
remote-address *ip-address*	Displays GTP path information for a specified remote IP address. Optionally, displays GTP path information for a specified remote IP address and port number.
remote-port *remote_port_num*	(Optional) Displays GTP path information for a specified remote IP address and port number.
version *gtp-version*	Displays the of GTP paths by the GTP version (0 or 1).

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.
12.4(9)XG	This command was integrated into Cisco IOS Release 12.4(9)XG.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.

Usage Guidelines

Use the **show gprs gtp path** command to display information for one or more GTP paths from the GGSN.

Examples

Example 1

The following example shows the output for all GTP paths on the GGSN:

```
GGSN# show gprs gtp path  all
Total number of path:1

Local address           Remote address          GTP version    Dynamic echo
timer
33.33.33.1(3386)        11.0.0.1(3386)          0              Disabled

  Collection interval - 5 min, Last collected at - 3 min back
    upstream data volume in octets:     480
    downstream data volume in octets:   0
    upstream packet count:              4
    downstream packet count:            0

  Collection interval - 10 min, Last collected at - 8 min back
    upstream data volume in octets:     120
    downstream data volume in octets:   0
    upstream packet count:              1
    downstream packet count:            0
```

Table 22 describes the fields shown in the display.

Table 19 show gprs gtp path Field Descriptions

Field	Description
Total number of path	Total number of GTP paths currently established.
Local address	IP address and port number for the local end of the GTP path.
Remote address	IP address and port number for the remote end of the GTP path, such as the address of the SGSN.
GTP version	Version of the GTP protocol (version 0 or 1) supported by the path.
Dynamic echo timer	Current setting (in seconds) for the dynamic echo timer. “Disabled” appears when the dynamic echo timer is not in use.

show gprs gtp path statistics history

To display statistics (such as the local address and remote port of the path, the GTP version, and the time that the path was deleted) for GTP path entries stored in history, use the **show gprs gtp path statistics history** command in privileged EXEC mode.

show gprs gtp path statistics history *number*

Syntax Description

number	Number of path entries for which to display statistics.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)XG	This command was introduced.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQand the following fields were added to the display: • Total Update requests sent • Total Update responses rcvd • Number of times DT enabled
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **show gprs gtp path statistics history** command to display statistics for the path entries stored in the path history table. The statistics includes information such as the local address, remote address, GTP version of the path, and the time at which the path was deleted.

The first group of statistics in the list are those of the most recently-deleted path.

The maximum number of path entries stored in the history table is configured by using the **gprs gtp path history** global configuration command.

Examples

The following is sample output from the **show gprs gtp path statistics history** command:

```
Router#show gprs gtp path statistics history
Path: IP address: 172.21.21.21, Remote port: 2152
GPRS GTP Path Statistics:
  Unexpected Data Message            0          Received PDU message               0
  Total Data dropped                 0          Sent PDU message                   0
  Received PDU bytes                 0          Number of short messages           0
  Sent PDU bytes                     0          Number of unknown message          0
  Unexpected signaling message       0          Roaming trusted PDPs               0
  Roaming non-trusted PDPs           0          Non-roaming PDPs                   0
  Source Violations                  0          Unsupported extension hdr recd     0
  Path failures                      0          Path fail due to local delete      0
  Total packets dropped              0          Signaling messages dropped         0
  Signaling msg received             2          Signaling msg sent                 3
  Number of PDPs created             0          Number of PDPs deleted             0
  Number of PPP PDPs created         0          Number of PPP PDPs deleted         0
```

```
  Single PDP cleared                0          Creates received as update          0
  Local delete: version upgrade     0          Local delete due to no sgsn         0
  Local delete: version fallback    0          Create collide with delete          0
  Version changes                   0          Retransmit for create               0
  IPv6 PDP activation rejected      0          IPv6 PDPs created                   0
  IPv6 PDPs deleted                 0          IPv6 signaling msg rcvd             0
  IPv6 signaling msg sent           0          IPv6 pdus received                  0
  IPv6 pdus sent                    0          IPv6 bytes received                 0
  IPv6 bytes sent                   0          Total update requests sent          0
  Total update responses rcvd       0          Number of times DT enabled          0

Path: IP address: 172.21.21.21, Remote port: 2123
GPRS GTP Path Statistics:
  Unexpected Data Message           0          Received PDU message                0
  Total Data dropped                0          Sent PDU message                    0
  Received PDU bytes                0          Number of short messages            0
  Sent PDU bytes                    0          Number of unknown message           0
  Unexpected signaling message      0          Roaming trusted PDPs                0
  Roaming non-trusted PDPs          0          Non-roaming PDPs                    0
  Source Violations                 0          Unsupported extension hdr recd      0
  Path failures                     0          Path fail due to local delete       0
  Total packets dropped             0          Signaling messages dropped          0
  Signaling msg received            6          Signaling msg sent                 12
  Number of PDPs created            0          Number of PDPs deleted              0
  Number of PPP PDPs created        0          Number of PPP PDPs deleted          0
  Single PDP cleared                0          Creates received as update          0
  Local delete: version upgrade     0          Local delete due to no sgsn         0
  Local delete: version fallback    0          Create collide with delete          0
  Version changes                   0          Retransmit for create               3
  IPv6 PDP activation rejected      0          IPv6 PDPs created                   0
  IPv6 PDPs deleted                 0          IPv6 signaling msg rcvd             0
  IPv6 signaling msg sent           0          IPv6 pdus received                  0
  IPv6 pdus sent                    0          IPv6 bytes received                 0
  IPv6 bytes sent                   0          Total update requests sent          0
  Total update responses rcvd       0          Number of times DT enabled          0

Path: IP address: 172.10.1.1, Remote port: 2152
GPRS GTP Path Statistics:
  Unexpected Data Message           0          Received PDU message                0
  Total Data dropped                0          Sent PDU message                    0
  Received PDU bytes                0          Number of short messages            0
  Sent PDU bytes                    0          Number of unknown message           0
  Unexpected signaling message      0          Roaming trusted PDPs                0
  Roaming non-trusted PDPs          0          Non-roaming PDPs                    0
  Source Violations                 0          Unsupported extension hdr recd      0
  Path failures                     0          Path fail due to local delete       0
  Total packets dropped             0          Signaling messages dropped          0
  Signaling msg received            1          Signaling msg sent                  2
  Number of PDPs created            1          Number of PDPs deleted              1
  Number of PPP PDPs created        0          Number of PPP PDPs deleted          0
  Single PDP cleared                0          Creates received as update          0
  Local delete: version upgrade     0          Local delete due to no sgsn         0
  Local delete: version fallback    0          Create collide with delete          0
  Version changes                   0          Retransmit for create               0
  IPv6 PDP activation rejected      0          IPv6 PDPs created                   0
  IPv6 PDPs deleted                 0          IPv6 signaling msg rcvd             0
  IPv6 signaling msg sent           0          IPv6 pdus received                  0
  IPv6 pdus sent                    0          IPv6 bytes received                 0
  IPv6 bytes sent                   0          Total update requests sent          0
  Total update responses rcvd       0          Number of times DT enabled          0

Path: IP address: 172.10.1.1, Remote port: 2123
GPRS GTP Path Statistics:
  Unexpected Data Message           0          Received PDU message                0
```

```
  Total Data dropped                0          Sent PDU message                  0
  Received PDU bytes                0          Number of short messages          0
  Sent PDU bytes                    0          Number of unknown message         0
  Unexpected signaling message      0          Roaming trusted PDPs              0
  Roaming non-trusted PDPs          0          Non-roaming PDPs                  0
  Source Violations                 0          Unsupported extension hdr recd    0
  Path failures                     0          Path fail due to local delete     0
  Total packets dropped             0          Signaling messages dropped        0
  Signaling msg received            0          Signaling msg sent                0
  Number of PDPs created            0          Number of PDPs deleted            0
  Number of PPP PDPs created        0          Number of PPP PDPs deleted        0
  Single PDP cleared                0          Creates received as update        0
  Local delete: version upgrade     0          Local delete due to no sgsn       0
  Local delete: version fallback    0          Create collide with delete        0
  Version changes                   0          Retransmit for create             0
  IPv6 PDP activation rejected      0          IPv6 PDPs created                 0
  IPv6 PDPs deleted                 0          IPv6 signaling msg rcvd           0
  IPv6 signaling msg sent           0          IPv6 pdus received                0
  IPv6 pdus sent                    0          IPv6 bytes received               0
  IPv6 bytes sent                   0          Total update requests sent        0
  Total update responses rcvd       0          Number of times DT enabled        0

Router#
```

Table 20 describes the fields shown in the display.

Table 20 show gprs gtp path statistics history Command Field Descriptions

Field	Description
Creates collide with delete	Number of create PDP context requests that collided with a delete PDP context request.
Creates received as update	Number of create PDP context requests received as an update PDP context request.
IPv6 bytes received	Number of IPv6 bytes received.
IPv6 bytes sent	Number of IPv6 bytes sent.
IPv6 PDP activation rejected	Number of activate IPv6 PDP context request rejected.
IPv6 PDPs created	Number of IPv6 PDP contexts created.
IPv6 PDPs deleted	Number of IPv6 PDP contexts deleted.
IPv6 pdus received	Number of IPv6 PDUs received.
IPv6 pdus sent	Number of IPv6 PDUs sent.
IPv6 signaling msg rcvd	Number of IPv6 signaling messages received.
IPv6 signaling msg sent	Number of IPv6 signaling messages sent.
Local delete due to no sgsn	Number of PDPs deleted locally because of no SGSN.
Local delete: version fallback	Number of PDPs deleted because of a version fallback.
Local delete: version upgrade	Number of PDPs deleted because of a version upgrade.

Table 20 show gprs gtp path statistics history Command Field Descriptions (continued)

Non-roaming PDPs	Number of non-roaming PDPs.
Number of PDPs created	Number of IPv4 PDP contexts created.
Number of PDPs deleted	Number of IPv4 PDP contexts deleted.
Number of PPP PDPs created	Number of PPP PDP contexts created.
Number of PPP PDPs deleted	Number of PPP PDP contexts deleted.
Number of short messages	Number of GTP messages received which are too short.
Number of times DT enabled	Number of times direct tunnel was enabled for a PDP context.
Number of unknown messages	Number of unknown GTP messages received.
Path failures	Number of path failures.
Path fail due to local delete	Number of path failure due to a local delete PDP context request.
Received PDU bytes	Number of IPv4 PDU bytes transmitted.
Received PDU message	Number of IPv4 PDU messages received.
Retransmit for create	Number of retransmitted create PDP context requests received.
Roaming non-trusted PDPs	Number of roaming PDPs not in a trusted PLMN.
Roaming trusted PDPs	Number of roaming PDPs in a trusted PLMN.
Sent PDU bytes	Number of IPv4 PDU bytes transmitted.
Sent PDU message	Number of IPv4 PDU messages transmitted.
Signaling messages dropped	Number of GTP signaling messages dropped.
Signaling msg received	Number of signaling messages received.
Signaling msg sent	Number of signaling messages sent.
Single PDP cleared	Number of hanging single PDP contexts cleared on the GGSN.
Source Violations	Number of PDPs terminated due to an access violation.
Total Data dropped	Total data dropped.
Total Update requests sent	Total number of GGSN-initiated Update PDP Context Requests sent.
Total Update responses rcvd	Total number responses to GGSN-initiated Update PDP Context Requests.

Table 20 show gprs gtp path statistics history Command Field Descriptions (continued)

Total packets dropped	Total number of packets dropped.
Unexpected Data Message	Number of GTP PDUs received for nonexistent PDP contexts.
Unexpected signaling message	Number of unexpected GTP signaling messages received.
Unsupported extension hdr recd	Number of create PDP context requests received with unsupported extension headers when GGSN comprehension is required.
Version changes	Number of GTP version changes that have occurred on the SGSN path

Related Commands

Command	Description
gprs gtp path history	Configures the maximum number of path entries for which the GGSN stores statistics after the path is deleted.
show gprs gtp path statistics remote-address	Displays the statistics for a specific GTP path.

show gprs gtp path statistics remote-address

To display statistics for a specific path, use the **show gprs gtp path statistics remote-address** command in privileged EXEC mode.

show gprs gtp path statistics r**emote-address** *ip-address* [**remote-port** *port-num*]

Syntax Description

remote-address *ip-address*	IP address of the SGSN for which you want to view path details.
remote-port *port-num*	Port number on the SGSN of the entry for which you want to view details.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)XG	This command was introduced.
12.4(9)XG2	This command was integrated into Cisco IOS Release 12.4(9)XG2 and the following fields were added to the display: • Local delete: no req to sgsn • Local delete: no wait sgsn
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ and the following fields were added to the display: • Number of time DT enabled • Total Update requests sent • Total Update responses rcvd
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **show gprs gtp path statistics remote-address** command to display statistics for a specific GTP path. These details include the local address and remote address of the path, the GTP version used, and the time at which the path was deleted.

If a remote port is not specified, statistics for all entries of the path are displayed.

If the path specified does not currently exist, the statistics stored in the path history table will be searched and displayed if the entry exists in history.

Examples

The following is sample output from the **show gprs gtp path statistics remote-address** command:

```
router#show gprs gtp path statistics remote-address 172.10.10.10
Path: IP address: 172.10.10.10, Remote port: 2123

GPRS GTP Path Statistics:
  Unexpected Data Message        0       Received PDU message            0
  Total Data dropped             0       Sent PDU message                0
  Received PDU bytes             0       Number of short messages        0
```

```
  Sent PDU bytes                  0       Number of unknown message        0
  Unexpected signaling message    0       Roaming trusted PDPs             0
  Roaming non-trusted PDPs        0       Non-roaming PDPs                 0
  Source Violations               0       Unsupported extension hdr recd   0
  Path failures                   0       Path fail due to local delete    0
  Total packets dropped           0       Signaling messages dropped       0
  Signaling msg received          26504   Signaling msg sent               26504
  Number of PDPs created          26504   Number of PDPs deleted           35
  Number of PPP PDPs created      0       Number of PPP PDPs deleted       0
  Number of times DT enabled   0       Single PDP cleared             0
  Creates received as update      0       Local delete: version upgrade     0
  Local delete due to no sgsn     0       Local delete: version fallback    0
  Create collide with delete      0       Local delete: no wait sgsn        0
  Local delete: no req to sgsn    0       Version changes                   0
  Retransmit for create           0       IPv6 PDP activation rejected      0
  IPv6 PDPs created               0       IPv6 PDPs deleted                 0
  IPv6 signaling msg rcvd         0       IPv6 signaling msg sent           0
  IPv6 pdus received              0       IPv6 pdus sent                    0
  IPv6 bytes received             0       IPv6 bytes sent                   0
  Total Update requests sent      2       Total Update responses rcvd       1

Path: IP address: 10.102.5.92, Remote port: 2152
GPRS GTP Path Statistics:
  Unexpected Data Message         0       Received PDU message              0
  Total Data dropped              0       Sent PDU message                  0
  Received PDU bytes              0       Number of short messages          0
  Sent PDU bytes                  0       Number of unknown message         0
  Unexpected signaling message    0       Roaming trusted PDPs              0
  Roaming non-trusted PDPs        0       Non-roaming PDPs                 0
  Source Violations               0       Unsupported extension hdr recd   0
  Path failures                   0       Path fail due to local delete    0
  Total packets dropped           0       Signaling messages dropped       0
  Signaling msg received          26504   Signaling msg sent               26504
  Number of PDPs created          26504   Number of PDPs deleted           35
  Number of PPP PDPs created      0       Number of PPP PDPs deleted       0
  Number of times DT enabled   0       Single PDP cleared             0
  Creates received as update      0       Local delete: version upgrade     0
  Local delete due to no sgsn     0       Local delete: version fallback    0
  Create collide with delete      0       Local delete: no wait sgsn        0
  Local delete: no req to sgsn    0       Version changes                   0
  Retransmit for create           0       IPv6 PDP activation rejected      0
  IPv6 PDPs created               0       IPv6 PDPs deleted                 0
  IPv6 signaling msg rcvd         0       IPv6 signaling msg sent           0
  IPv6 pdus received              0       IPv6 pdus sent                    0
  IPv6 bytes received             0       IPv6 bytes sent                   0
  Total Update requests sent      2       Total Update responses rcvd       1
router#
```

Table 21 describes the fields shown in the display.

Table 21 show gprs gtp path statistics remote-address Command Field Descriptions

Field	Description
Creates collide with delete	Number of create PDP context requests that collided with a delete PDP context request.
Creates received as update	Number of create PDP context requests received as an update PDP context request.
IPv6 bytes received	Number of IPv6 bytes received.
IPv6 bytes sent	Number of IPv6 bytes sent.

Table 21 show gprs gtp path statistics remote-address Command Field Descriptions

IPv6 PDP activation rejected	Number of activate IPv6 PDP context request rejected.
IPv6 PDPs created	Number of IPv6 PDP contexts created.
IPv6 PDPs deleted	Number of IPv6 PDP contexts deleted.
IPv6 pdus received	Number of IPv6 PDUs received.
IPv6 pdus sent	Number of IPv6 PDUs sent.
IPv6 signaling msg rcvd	Number of IPv6 signaling messages received.
IPv6 signaling msg sent	Number of IPv6 signaling messages sent.
Local delete due to no sgsn	Number of PDPs deleted locally because of no SGSN.
Local delete: version fallback	Number of PDPs deleted because of a version fallback.
Local delete: version upgrade	Number of PDPs deleted because of a version upgrade.
Local delete: no req to sgsn	Number of PDPs deleted when the GGSN is configured to delete PDP contexts locally without sending a delete PDP context request to the SGSN.
Local delete: no wait sgsn	Number of PDPs deleted when the GGSN is configured to not wait for the SGSN to respond to its delete PDP context request before deleting the PDP context.
Non-roaming PDPs	Number of non-roaming PDPs.
Number of times DT enabled	Number of direct tunnel PDP contexts created.
Number of PDPs created	Number of IPv4 PDP contexts created.
Number of PDPs deleted	Number of IPv4 PDP contexts deleted.
Number of PPP PDPs created	Number of PPP PDP contexts created.
Number of PPP PDPs deleted	Number of PPP PDP contexts deleted.
Number of short messages	Number of GTP messages received which are too short.
Number of unknown messages	Number of unknown GTP messages received.
Path failures	Number of path failures.
Path fail due to local delete	Number of path failure due to a local delete PDP context request.
Received PDU bytes	Number of IPv4 PDU bytes transmitted.
Received PDU message	Number of IPv4 PDU messages received.
Retransmit for create	Number of retransmitted create PDP context requests received.
Roaming non-trusted PDPs	Number of roaming PDPs not in a trusted PLMN.
Roaming trusted PDPs	Number of roaming PDPs in a trusted PLMN.
Sent PDU bytes	Number of IPv4 PDU bytes transmitted.
Sent PDU message	Number of IPv4 PDU messages transmitted.
Signaling messages dropped	Number of GTP signaling message dropped.
Signaling msg received	Number of signaling messages received.
Signaling msg sent	Number of signaling messages sent.
Single PDP cleared	Number of hanging single PDP contexts cleared on the GGSN.
Source Violations	Number of PDPs terminated due to a access violation.

Table 21 show gprs gtp path statistics remote-address Command Field Descriptions

Total Data dropped	Total data dropped.
Total packets dropped	Total number of packets dropped.
Total Update requests sent	Total number of GGSN-initiated Update PDP Context Requests sent.
Total Update responses rcvd	Total number responses to GGSN-initiated Update PDP Context Requests.
Unexpected Data Message	Number of GTP PDUs received for nonexistent PDP contexts.
Unexpected signaling message	Number of unexpected GTP signaling messages received.
Unsupported extension hdr recd	Number of create PDP context requests received with unsupported extension headers when GGSN comprehension is required.
Version changes	Number of GTP version changes that have occurred on the SGSN path.

Related Commands

Command	Description
gprs gtp path history	Configures the maximum number of path entries for which the GGSN stores statistics after the path is deleted.
show gprs gtp path statistics history	Displays summary of the counters for past GTP path entries stored in history.

show gprs gtp path throughput

To display throughput information for one or more GTP paths between a gateway GPRS support node (GGSN) and other GPRS/UMTS devices, use the **show gprs gtp path throughput** command in privileged EXEC mode.

show gprs gtp path throughput {**all** | **remote-address** *ip-address* [**remote-port** *remote-port*] | **version** *gtp-version*}

Syntax Description

all	Displays information for all GTP paths.
remote-address *ip-address*	Displays GTP path throughput information for a specified remote IP address. Optionally, displays GTP path throughput information for a specified remote IP address and port number.
remote-port *remote_port_num*	(Optional) Displays GTP path throughput information for a specified remote IP address and port number.
version *gtp-version*	Displays the throughput of GTP paths by the GTP version (0 or 1).

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs gtp path throughput** command to display throughput information for one or more GTP paths from the GGSN.

Examples

Example 1

The following example shows the output for all GTP paths on the GGSN:

```
GGSN# show gprs gtp path throughput all
Total number of path:1

Local address           Remote address          GTP version    Dynamic echo
timer
33.33.33.1(3386)        11.0.0.1(3386)          0              Disabled

  Collection interval - 5 min, Last collected at - 3 min back
    upstream data volume in octets:     480
    downstream data volume in octets:   0
    upstream packet count:              4
    downstream packet count:            0

  Collection interval - 10 min, Last collected at - 8 min back
    upstream data volume in octets:     120
    downstream data volume in octets:   0
    upstream packet count:              1
    downstream packet count:            0
```

Table 17 describes the fields shown in the display.

Table 22 show gprs gtp path throughput Field Descriptions

Field	Description
Total number of path	Total number of GTP paths currently established.
Local address	IP address and port number for the local end of the GTP path.
Remote address	IP address and port number for the remote end of the GTP path, such as the address of the SGSN.
GTP version	Version of the GTP protocol (version 0 or 1) supported by the path.
Dynamic echo timer	Current setting (in seconds) for the dynamic echo timer. “Disabled” appears when the dynamic echo timer is not in use.

show gprs gtp pdp-context

To display a list of the currently active PDP contexts (mobile sessions), use the **show gprs gtp pdp-context** command in privileged EXEC mode.

show gprs gtp pdp-context {**tid** *tunnel_id* **[service [all | id** *id_string***]]** | **ms-address** *ip_address* [**access-point** *access-point-index*] | **imsi** *imsi* [**nsapi** *nsapi* [**tft**]] | **path** *ip-address* [*remote-port-num*] | **access-point** *access-point-index* | **pdp-type** {**ip** | **ppp**} | **qos-umts-class** {**background** | **conversational** | **interactive** | **streaming**} | **qos-precedence** {**low** | **normal** | **high**} | **qos-delay** {**class1** | **class2** | **class3** | **classbesteffort**} | **version** *gtp-version***}** | **msisdn** [*msisdn*] | **all**}

Syntax Description

tid *tunnel_id* **[service [all | id** *id_string***]]**	Displays PDP contexts by tunnel ID. This value corresponds to the IMSI plus NSAPI and can be up to 16 numeric digits. Optionally, displays the service category in a PDP context.
ms-address *ip_address*	Displays PDP contexts for the specified mobile station IP address (in dotted-decimal format).
apn-index *access-point-index*	(Optional) Displays PDP contexts for the specified mobile station IP address at a particular access point. This option is required to display mobile stations that are accessing a private VPN.
imsi *imsi*	Displays PDP contexts by International Mobile Subscriber Identity (IMSI). The IMSI value can be up to 15 numeric digits.
nsapi *nsapi* [**tft**]	(Optional) Displays a particular PDP context by Network Service Access Point Identifier (NSAPI) for the specified IMSI. Optionally, displays the traffic flow template (TFT) filters associated with the NSAPI.
path *ip-address* [*remote_port_num*]	Displays PDP contexts by path. Optionally, displays PDP contexts by remote IP address and port number.
access-point *access-point-index*	Displays PDP contexts by access point. Possible values are 1 to 65535.
pdp-type {**ip** | **ppp**}	Displays PDP contexts that are transmitted using either IP or PPP.
qos-umts-class	Displays PDPs by UMTS QoS traffic class. You can specify the following traffic classes: **background**, **conversational**, **interactive**, and **streaming**. This option is available when UMTS QoS is enabled.
qos-precedence	Displays PDP contexts for a specified GPRS QoS precedence type. You can specify the following precedence types: **low**, **normal**, and **high**. This option is available when GPRS QoS canonical QoS is enabled.
qos-delay	Displays PDP contexts for a specified GPRS quality of service delay class type. You can specify the following delay class types: **class1**, **class2**, **class3**, and **classbesteffort**. This option is available when GPRS QoS delayed-based QoS is enabled.
version *gtp-version*	Displays PDP contexts by GTP version. The possible values are 0 or 1.
msisdn [*msisdn*]	Displays all PDP contexts with MSISDN information. Optionally, displays particular PDPs filtered by the longest prefix match of the specified MSISDN.
all	Displays all PDP contexts.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(1)	The MS International PSTN/ISDN Number (MSISDN) field was added to the output display.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX. • The **pdp-type ppp** and **qos-delay** options were added to the command. • The following fields were added to the output display of the **tid** version of this command: – cef_down_byte – cef_down_pkt – cef_drop – cef_up_byte – cef_up_pkt – gtp pdp idle time • The Network Init Information section was added to the output display of the **tid** version of this command with the following new fields: – Buf.Bytes – MNRG Flag – NIP State – PDU Discard Flag – SGSN Addr • The following fields were removed from the output display of the **tid** version of this command: – fast_up_pkt – fast_up_byte – fast_down_pkt – fast_down_byte – fast_drop • The “dynamic?” and “Dynamic” fields were removed from the output display of the **all** and **tid** versions of this command, and were replaced by the Source field.

Release	Modification
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD and the following fields were added to the output display of the **tid** version of this command: • primary dns • secondary dns • primary nbns • secondary nbns
12.2(8)YW	This command was integrated into the 12.2(8)YW. • The the option of displaying PDP contexts by remote IP address and port number was added. • The delay Qos class(req.) output field was added to the display of the **tid** version of this command when the mapping of GPRS QoS categories to delay QoS classes is enabled. • The **ms-address**, **imsi**, **qos-umts-class** and **version** options were added to the command. • The ggsn_addr_signal field was changed to the sgsn_addr_data in the output display of the **tid** version of this command. • The following fields were added to the output display of the **tid** version of this command: – control teid local – control teid remote – data teid local – data teid remote – primary pdp – nsapi
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB and the MS Addr field updated to reflect the virtual interface identifier for PPP PDP and PPP Regen contexts and the status of PPP PDP with L2TP contexts.

Release	Modification
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU. • The following fields were added to the output display of the **tid** version of this command: – charging characteristics – charging characteristics received – Framed_route – idle timeout – mask – roamer – session timeout – visitor • The gtp pdp idle time field were removed from the output display of the **tid** version of this command. • An overflow indicator (+) was added to the following fields of the output display of the **tid** version of this command: – cef_down_pkt – cef_up_pkt – rcv_pkt_count – send_pkt_count
12.3(8)XU2	This command was integrated into Cisco IOS Release 12.3(8)XU2 and the single pdp-session field was added to the output display of the **tid** version of this command.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.

Release	Modification
12.3(14)YQ	This command was integrated into the Cisco IOS Release 12.3(14)YQ. • The option of display the service category in a PDP context was added was added. • The following fields were added to the **tid** version of this command when the **service** keyword option is specified: – Diameter Credit Control – Current Billing Status – Reason to convert to postpaid – DCCA profile name and Source – Rule base id and Source – ServiceID – State – Quota(octets) – Time – flags – Last pushed quota - Tariff Time Change - Time Quota - Volume Quota - Validity Time - Quota ConsumptionTime - Quota Holding time - Time Quota Threshold - Volume Quota Threshold - Trigger Flags – Last received quota - Tariff_time_change - Time_quota - Volume_quota - Validity_time - Quota ConsumptionTime - Quota Holding_Time - Time Quota Threshold - Volume Quota Threshold - Trigger Flags

Release	Modification
12.3(14)YU	This command was integrated into the Cisco IOS Release 12.3(14)YU and the **msisdn** [*msisdn*] keyword option was added. Additionally, the QoS for charging field was removed from the **show gprs gtp pdp-context tid** command display and when a PDP is created via a virtual APN, the following field has been added to the **show gprs gtp pdp-context tid** command display: • virtual-apn: *virtual-apn-name*
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs gtp pdp-context** command to display the currently active PDP contexts on the GGSN. You can display PDP contexts by tunnel ID, by IMSI, by access point, by PDP type, and by GPRS QoS precedence, UMTS QoS traffic class, or you can display all PDP contexts.

Several versions of the **show gprs gtp pdp-context** command display similar output. The examples provided show these two different types of output.

Interpreting the Effective Bandwidth

Example 2 provides sample output from the **show gprs gtp pdp-context tid** command, which includes the field called effective bandwidth (in bps). The effective bandwidth is determined according to the GPRS QoS canonical QoS class (premium, normal, or best effort) for the PDP context; it does not represent the actual bandwidth in use by the PDP context. The potential number of supported PDP contexts for that class of QoS can then be calculated according to the total amount of bandwidth (GSN resource) available to the GGSN.

For more information about GPRS QoS canonical QoS and resources on the GGSN, see the "Configuring QoS on the GGSN" chapter in the *Cisco IOS Mobile Wireless Configuration Guide*.

Examples

Example 1

The following is sample output of the **show gprs gtp pdp-context all** command:

```
router# show gprs gtp pdp-context all
TID              MS Addr          Source  SGSN Addr       APN
1234567890123456 10.11.1.1        Radius  10.4.4.11       www.pdn1.com
2345678901234567 Forwarded (Vi5)  IPCP    10.4.4.11       www.pdn2.com
3456789012345678 10.21.1.1 (Vi7)  IPCP    10.1.4.11       www.pdn3.com
4567890123456789 10.31.1.1 (Vi9)  IPCP    10.1.4.11       www.pdn4.com
5678901234567890 10.41.1.1        Static  10.4.4.11       www.pdn5.com
```

Note The same output fields shown in Example 1 also appear when you use the **access-point**, **path**, **pdp-type**, **qos-delay**, or **qos-precedence** keyword options of the **show gprs gtp pdp-context** command.

Table 18 describes the fields shown in the display.

Table 23 show gprs gtp pdp-context all Field Descriptions

Field	Description
APN	Access point name where the PDP context is active.
MS Addr	IP address of the mobile station. **Note** For PPP PDP and PPP Regen contexts, this field will also display the virtual interface identifier. For PPP PDP with L2TP contexts, this field will also display the state of the PDP context. Possible states are Pending, Forwarded, or Terminating.
SGSN Addr	IP address of the SGSN that is processing the packets.
Source	Source of IP addressing for the MS. The possible values are: • DHCP—Dynamic address allocation using DHCP. • IPCP—Dynamic address allocation for PPP PDP types, or for IP PDP types with PPP regeneration, using PPP IP Control Protocol. • Local—Dynamic address allocation using a local pool. • Pending—Waiting for dynamic address allocation. Dynamic address source is unknown. • Radius—Dynamic address allocation using RADIUS. • Static—IP address is not dynamically assigned.
TID	Tunnel ID for the PDP context.

Example 2

The following is sample output from the **show gprs gtp pdp-context tid** command for a PDP context created by GTP version 1 and GPRS QoS canonical QoS is configured:

```
router#show gprs gtp pdp-context tid 1111111111111111
TID              MS Addr         Source  SGSN Addr       APN
1111111111111111 10.1.1.1        Radius  10.8.8.1        dns.com

    current time :Mar 18 2002 11:24:36
    user_name (IMSI):1111111111111111   MS address:10.1.1.1
    MS International PSTN/ISDN Number (MSISDN):ABC
    sgsn_addr_signal:10.8.8.1           sgsn_addr_data:10.8.0.1
    control teid local: 0x63493E0C
    control teid remove: 0x00000121
    data teid local:  0x63483E10
    data teid remote:  0x00000121
    primary pdp: Y      nsapi: 0
    signal_sequence: 0                  seq_tpdu_up:     0
    seq_tpdu_down:   0
    upstream_signal_flow:  1            upstream_data_flow:  2
    downstream_signal_flow:14           downstream_data_flow:12
```

```
RAupdate_flow:          0
pdp_create_time:  Mar 18 2002 09:58:39
last_access_time: Mar 18 2002 09:58:39
mnrgflag:          0                tos mask map:00
session timeout: 0
idle timeout: 0
gprs qos_req:091101                canonical Qos class(req.):01
gprs qos_neg:25131F                canonical Qos class(neg.):01
effective bandwidth:0.0
rcv_pkt_count:     0               rcv_byte_count:  0
send_pkt_count:    0               send_byte_count: 0
cef_up_pkt:        0               cef_up_byte:    0
cef_down_pkt:      0               cef_down_byte:  0
cef_drop:           0              out-sequence pkt: 0
Src addr violation:             2 paks,     1024 bytes
Dest addr violation:            2 paks,     1024 bytes
Redirected mobile-to-mobile traffic:  2 paks,     1024 bytes
charging_id:        29160231
visitor: No        roamer: No
charging characteristics: 0
charging characteristics received: 0
pdp reference count:2
primary dns:        2.2.2.2
secondary dns:      4.4.4.4
primary nbns:       3.3.3.3
secondary nbns:     5.5.5.5
ntwk_init_pdp:      0
Framed_route 5.5.5.0 mask 255.255.255.0
single pdp-session: Enabled
absolute session start time: NOT SET
virtual apn: pre-auth-virtual

** Network Init Information **
MNRG Flag: 0                PDU Discard Flag: 0
SGSN Addr: 172.16.44.1      NIP State:        NIP_STATE_WAIT_PDP_ACTIVATION
Buf.Bytes: 500
```

Table 19 describes the fields shown in the display.

Note The Network Init Information section of the output appears only while network-initiated PDP contexts are being processed by the GGSN.

Note The same output fields shown in Example 2 also appear when you use the **imsi** keyword option of the **show gprs gtp pdp-context** command.

Note If the PDP context is created via a virtual APN, the “virtual-apn: *virtual-apn name*” field displays.

Table 19 describes the fields shown in the display.

Table 24 show gprs gtp pdp-context tid Field Descriptions

Field	Description
APN	Access point name where the PDP context is active.
canonical Qos class (neg.)	Negotiated canonical quality of service class for the PDP context, with the following values: • 01—Best effort • 02—Normal • 03—Premium This field displays when GPRS QoS canonical QoS is enabled on the GGSN.
canonical Qos class (req.)	Requested GPRS canonical QoS class by the PDP context, with the following values: • 01—Best effort • 02—Normal • 03—Premium This field displays when GPRS QoS canonical QoS is enabled on the GGSN.
cef_down_byte	Total number of G-PDU bytes CEF switched on the downlink, from the GGSN to the SGSN.
cef_down_pkt	Total number of G-PDU packets CEF switched on the downlink, from the GGSN to the SGSN. The plus (+) sign is an overflow indicator.
cef_drop	Total number of G-PDU packets dropped during CEF switching.
cef_up_byte	Total number of G-PDU bytes CEF switched on the uplink, from the SGSN to the GGSN.
cef_up_pkt	Total number of G-PDU packets CEF switched on the uplink, from the SGSN to the GGSN. The plus (+) sign is an overflow indicator.
charging characteristics	Number of the charging profile selected for the PDP context.
charging characteristics received	Charging characteristics IE received from the SGSN. The value of the charging characteristics received field is the decimal value of the two octets, with the first octet being the more significant byte than the second. The profile index, which is used to select the charging profile, is the integer obtained by dividing the charging characteristics received value by 256.
charging_id	Unique 4-octet value generated by the GGSN for the PDP context. The value 0 is reserved.
control teid local	Uplink tunnel endpoint identifier (TEID) chosen by the GGSN for control plane messages. This field displays for PDP contexts created with GTP version 1.

Table 24 show gprs gtp pdp-context tid Field Descriptions (continued)

Field	Description
control teid remote	Downlink TEID chosen by the SGSN for control plane messages. This field displays for PDP contexts created with GTP version 1.
current time	Date and time of the show command output.
data teid local	Uplink TEID chosen by the GGSN for G-PDUs. This field displays for PDP contexts created with GTP version 1.
data teid remote	Downlink TEID chosen by the SGSN for PDUs. This field displays for PDP contexts created with GTP version 1.
Dest addr violation	Number of packets (and bytes) dropped by the GGSN because of a source address violation. This field displays only when the **security verify destination** command is configured. **Note** This field does not apply to APNs using VRF. In addition, verification of destination addresses does not apply to GTP-PPP regeneration or GTP-PPP with L2TP.
downstream_data_flow	Flow label of downlink G-PDUs.
downstream_signal_flow	Flow label of downlink signaling messages.
effective bandwidth	Estimated number of bits per second allocated by the GGSN for this PDP context. The effective bandwidth is determined according to the QoS class (premium, normal, or best effort) for the PDP context. The potential number of supported PDP contexts for that class of QoS can be calculated according to the total amount of bandwidth (GSN resource) available to the GGSN. This field displays when canonical QoS is enabled on the GGSN. **Note** The effective bandwidth does not represent actual bandwidth usage.
Framed_route	Framed-Route, attribute 22, for the PDP context, downloaded from the RADIUS server during authentication and authorization.

Table 24 show gprs gtp pdp-context tid Field Descriptions (continued)

Field	Description
gprs qos_neg	Negotiated quality of service for the PDP context. The field is in the format *vwxyzz*, which represents the following QoS classes (as defined in the GSM specifications for quality of service profiles): • *v*—Delay class • *w*—Reliability class • *x*—Peak throughput class • *y*—Precedence class • *zz*—Mean throughput class **Note** To determine the GPRS QoS attributes shown in this output, you must convert the value to binary and interpret the values to find the corresponding class attributes. Some of the bits represent "don't care" bits and are not interpreted as part of the final value. For more information about how to interpret this value, see the "Interpreting the Requested and Negotiated GPRS QoS" section of the "Configuring QoS" chapter in the *Cisco IOS Mobile Wireless Configuration Guide*.
gprs qos_req	Requested quality of service by the PDP context. The field is in the format *vwxyzz*, which represents the following QoS classes (as defined in the GSM specifications for GPRS QoS profiles): • *v*—Delay class • *w*—Reliability class • *x*—Peak throughput class • *y*—Precedence class • *zz*—Mean throughput class **Note** See the Note in the description of the gprs qos_neg output field above.
idle timeout	Number of seconds the GGSN waits before purging idle PDP contexts.
last_access_time	Time when the PDP context for this TID was last accessed. The date format is MMM DD YYYY. The time format is hours:minutes:seconds. When a signaling packet or data packet for a PDP context arrives on the GGSN, the last_access_time is reset to the current date and time. If the last_access_time exceeds the purge timer for idle PDP contexts, then the PDP context is purged by the GGSN.
mask	Framed-Route subnet.
mnrgflag	Mobile not reachable flag, with the following values: • 0—flag is off. • 1—flag is on, indicating that the MS is not reachable

Table 24 show gprs gtp pdp-context tid Field Descriptions (continued)

Field	Description
MS_ADDR and MS Address	IP address of the mobile station. **Note** For PPP PDP and PPP Regen contexts, this field will also display the virtual interface identifier. For PPP PDP with L2TP contexts, this field will also display the state of the PDP context. Possible states are Pending, Forwarded, or Terminating.
MS International PSTN/ISDN Number (MSISDN)	Integrated Services Digital Network (ISDN) number of the mobile station.
nsapi	Network Service Access Point Identifier (NSAPI). This field displays for PDP contexts created with GTP version 1.
ntwk_init_pdp	Network initiated PDP context indicator, with the following values: • 0—Not a network initiated PDP context. This indicates a mobile initiated PDP context. • 1—Network initiated PDP context
out-sequence pkt	
pdp_create_time	Time when the PDP context for this TID was created. The date format is MMM DD YYYY. The time format is hours:minutes:seconds.
pdp reference count	Number of subsystems on the GGSN that are aware of the PDP context. For example, if both the charging and GTP subsystems are aware of the PDP context, then the pdp reference counter shows a value of 2.
primary dns	IP address of the primary DNS server.
primary nbns	IP address of the primary NetBIOS Name Service (NBNS).
primary pdp	Whether the PDP is primary or secondary. Possible values are Y (PDP is primary) or N (PDP is secondary). This field displays for PDP contexts created with GTP version 1.
RAupdate_flow	Flow Label Data II information element in GTP header. This IE contains the flow label for data transmission between old and new SGSNs for a particular PDP context. This IE is requested by the new SGSN.
rcv_byte_count	Total number of G-PDU bytes received. For the GGSN, this is the total byte count on the uplink.
rcv_pkt_count	Total packet count of received G-PDUs. For the GGSN, this is the total byte count on the uplink. The plus (+) sign is an overflow indicator.
Redirected mobile-to-mobile traffic	Number of packets (and bytes) dropped at the APN from which they exit because mobile-to-mobile traffic has been redirected. This field displays only when the **redirect intermobile ip** command is configured.

Table 24 show gprs gtp pdp-context tid Field Descriptions (continued)

Field	Description
roamer	Whether the PDP context is that of a roaming mobile subscriber (subscriber whose SGSN PLMN ID differs from the GGSN's). The possible values are yes or no.
secondary dns	IP address of the secondary DNS server.
secondary nbns	IP address of the secondary NBNS.
send_byte_count	Total number of G-PDU bytes sent by the GSN (GGSN or SGSN D-node).
send_pkt_count	Total number of G-PDU packets sent by the GSN (GGSN or SGSN D-node). The plus (+) sign is an overflow indicator.
seq_tpdu_down	Last sequence number used in the downlink T-PDU. This number wraps to 0 after 65535.
seq_tpdu_up	Last sequence number used in the uplink T-PDU. This number wraps to 0 after 65535.
session timeout	Number of seconds that the GGSN allows a session to remain active before purging all PDP contexts with the same IMSI or MS address.
sgsn_addr_signal	IP address of the SGSN that is processing the packets.
sgsn_addr_data	IP address of the SGSN that is processing tunnel packet data units (TPDUs).
signal_sequence	Last sequence number used in the GTP signaling message.
single PDP-session	Whether the GGSN has been configured to delete the primary PDP context, and any associated secondary PDP contexts, of a *hanging* PDP session upon receiving a new create request from the same MS that shares the same IP address of the hanging PDP context.
Source	Source of IP addressing for the MS. The possible values are: • DHCP—Dynamic address allocation using DHCP. • IPCP—Dynamic address allocation for PPP PDP types, or for IP PDP types with PPP regeneration, using PPP IP Control Protocol. • Local—Dynamic address allocation using a local pool. • Pending—Waiting for dynamic address allocation. Dynamic address source is unknown. • Radius—Dynamic address allocation using RADIUS. • Static—IP address is not dynamically assigned.
Src addr violation	Number of packets (and bytes) dropped because of source address violation. This field displays only when the **security verify source** command is configured.
TID	Tunnel ID for the PDP context.
tos mask map	ToS value in IP header of this PDP context.
umts qos_req	Requested UMTS quality of service by the PDP context. This field displays when UMTS QoS is enabled on the GGSN.

Table 24 show gprs gtp pdp-context tid Field Descriptions (continued)

Field	Description
umts qos_neg	Negotiated UMTS quality of service for the PDP context. This field displays when UMTS QoS is enabled on the GGSN.
upstream_data_flow	Flow label of uplink G-PDUs.
upstream_signal_flow	Flow label of uplink signaling messages.
user_name (IMSI)	International mobile subscriber identity for the PDP context.
virtual APN	Virtual access point name where the PDP context is active.
visitor	Whether the PDP context is that of a visiting mobile subscriber (subscriber whose IMSI contains a foreign PLMN ID).). The possible values are yes or no.

Table 20 describes the fields shown in the Network Init Information section of the output.

Table 25 show gprs gtp pdp-context tid Network Init Information Field Descriptions

Field	Description
Buf.Bytes	Number of bytes currently buffered for this network-initiated PDP context.
last_access_time	Time when the PDP context for this TID was last accessed. The date format is MMM DD YYYY. The time format is hours:minutes:seconds. When a signaling packet or data packet for a PDP context arrives on the GGSN, the last_access_time is reset to the current date and time. If the last_access_time exceeds the purge timer for idle PDP contexts, then the PDP context is purged by the GGSN.
MNRG Flag	Mobile not reachable flag, with the following values: • 0—flag is off. • 1—flag is on, indicating that the MS is not reachable
NIP State	State information for the network initiated PDP process on the GGSN.

Table 25 show gprs gtp pdp-context tid Network Init Information Field Descriptions

Field	Description
PDU Discard Flag	Discarded PDU indicator for a network initiated PDP context, with the following values: • 0—PDUs are not discarded. This indicates that PDUs for a network initiated PDP context are being sent to the SGSN. • 1—PDUs are being discarded by the GGSN. PDUs are discarded by the GGSN when a network initiated PDP context procedure is unsuccessful. This occurs when the SGSN sends a rejection of the PDP context request to the GGSN with a Cause value of either "MS Refuses" or "MS is not GPRS Responding." When the flag is set to 1, the GGSN ignores PDUs destined for that MS for the specified PDU discard period. The default period is 300 seconds (5 minutes). You can configure the PDU discard time using the **gprs ntwk-init-pdp pdu-discard-period** command.
SGSN Addr	IP address of the SGSN that is associated with the network-initiated procedure for this PDP context (used for paging).

Example 3

The following is sample output from the **show gprs gtp pdp-context tid service id** command:

```
ggsn1#show gprs gtp pdp tid 1111000000000050 service id 1
Diameter Credit Control:Enabled
Current Billing status:Prepaid
Reason to convert to postpaid:N/A
DCCA profile name:1, Source:charging profile
Rule base id:ABC,  Source:AAA server
ServiceID  State         Quota(octets)         Time     flags

 1        AUTHORIZED        80000              6000     SGSN:

Last pushed quota
-----------------
Tariff Time Change:    1110585600  Time Quota:            6000
Volume Quota:          80000       Validity Time:         500
Quota ConsumptionTime: 45          Quota Holding time:    35
Time Quota Threshold:  4000        Volume Quota Threshold:50000
Trigger Flags:         1

Last received quota
-------------------
Tariff_time_change:    1110585600  Time_quota:           6000
Volume quota:          80000       Validity_time:        500
Quota ConsumptionTime: 45          Quota Holding_Time:   35
Time Quota Threshold:  4000        Volume Quota Threshold:50000
Trigger Flags:         1
```

Example 4

The following is sample output from the **show gprs gtp pdp-context msisdn** command:

```
ggsn1#show gprs gtp pdp-context msisdn

TID              MS Addr         Source  SGSN Addr       MSISDN              APN
2123456708000010 55.10.0.2       LOCAL   10.1.1.70       408525823010        ippdpl
2123456809000010 55.10.0.3       LOCAL   10.1.1.70       408525823011        ippdpl
2123456707000010 55.10.0.4       LOCAL   10.1.1.70       408525823110        ippdpl
2123456789990010 55.10.0.5       LOCAL   10.1.1.70       408525823210        ippdpl
```

Note All PDP contexts are displayed

The following is sample output from the **show gprs gtp pdp-context msisdn** command with an msisdn specified:

```
ggsn1#show gprs gtp pdp-context msisdn 4085258230

TID              MS Addr         Source  SGSN Addr       MSISDN              APN
2123456708000010 55.10.0.2       LOCAL   10.1.1.70       408525823010        ippdpl
2123456809000010 55.10.0.3       LOCAL   10.1.1.70       408525823011        ippdpl
```

Note All PDP contexts whose MSISDN matches the prefix 4085258230 are displayed

Table 21 describes the fields shown in the display.

Table 26 show gprs gtp pdp-context msisdn Field Descriptions

Field	Description
TID	Tunnel ID for the PDP context request on the APN.
MS Addr	The IP address for the MS.
Source	Source of IP addressing for the MS. The possible values are: • DHCP—Dynamic address allocation using DHCP. • IPCP—Dynamic address allocation for PPP PDP types, or for IP PDP types with PPP regeneration, using PPP IP Control Protocol. • Local—Dynamic address allocation using a local pool. • Pending—Waiting for dynamic address allocation. Dynamic address source is unknown. • Radius—Dynamic address allocation using RADIUS. • Static—IP address is not dynamically assigned.
SGSN Addr	IP address of the SGSN that is processing the packets.
MSISDN	Integrated Services Digital Network (ISDN) number of the mobile station.
APN	Access point name.

Related Commands

Command	Description
show gprs access-point	Displays information about access points on the GGSN.
show gprs gtp status	Displays information about the current status of the GTP on the GGSN (such as activated PDP contexts, throughput, and QoS statistics).

show gprs gtp statistics

To display the current GPRS tunneling protocol (GTP) statistics for the gateway GPRS support node (GGSN) (such as IE, GTP signaling, and GTP PDU statistics), use the **show gprs gtp statistics** command in privileged EXEC mode.

show gprs gtp statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(2)GB	This command was integrated into Cisco IOS Release 12.1(2)GB and the following fields were added to the output display: • total created_pdp • total deleted_pdp
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX, and the following fields were added to the output display: • ntwk_init_pdp_act_rej • ppp_regen_pending • ppp_regen_pending_peak • ppp_regen_total_drop • ppp_regen_no_resource • total created_ppp_pdp • total ntwkInit created pdp
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into the Cisco IOS Release 12.2(8)YW and the following fields were added to the output display: • tft_semantic_error • tft_syntactic_error • packet_filter_semantic_error • packet_filter_syntactic_error • total deleted_ppp_pdp
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.

Release	Modification
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU and the following fields were added to the output display: • insert_download_route_fail • network_behind_ms APNs • pdp_wo_tft_exist • save_download_route_fail • total_download_route • total_insert_download_route • unsupported_comp_exthdr
12.3(8)XU2	This command was integrated into Cisco IOS Release 12.3(8)XU2 and the single pdp-session cleared output field was added.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB and the following fields were added to the output display: • create_as_update • create_collide_with_delete • no_sgsn_local_del_pdp • path_fail_local_del_pdp • rcv_retransmit_create_req • version_changes • ver_upgrade_local_del • ver_faillback_local_del
12.4(9)XG	This command was integrated into Cisco IOS Release 12.4(9)XG and the following IPv6-related fields were added to the display: • created ipv6 pdp • created ipv6 pdpmcb • deleted ipv6 pdp • deleted ipv6 pdpmcb • rejected ipv6 pdp • rcvd ipv6 data bytes • rcvd ipv6 pdu • rcvd ipv6 signal msg • sent ipv6 data bytes • sent ipv6 pdu • sent ipv6 signal msg

Release	Modification
12.4(9)XG2	This command was integrated into Cisco IOS Release 12.4(9)XG2 and the following fields were added to the display: • no_req_sgsn_local_del_pdp • no_wait_sgsn_local_del_pdp
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ and the following fields were added to the display: • Number of times DT enabled • total COA msg received • total COA msgs discarded • total COA triggered update • total EI rcvd on DT PDPs • total error indication sent • total error indication rcvd • total error indication rcvd DT PDPs • total update responses rcv • total update fail DT pdps

Usage Guidelines

Use the **show gprs gtp statistics** command to display the GTP statistics for the GGSN. The counter values displayed by this command represent totals accumulated since the last time the statistical counters were cleared using the **clear gprs gtp statistics** command.

Examples

The following is sample output of the **show gprs gtp statistics** command:

```
router# show gprs gtp statistics
 GPRS GTP Statistics:
  version_not_support              0       msg_too_short               0
  unknown_msg                      0       unexpected_sig_msg          0
  unexpected_data_msg              0       unsupported_comp_exthdr     0
  mandatory_ie_missing             0       mandatory_ie_incorrect      0
  optional_ie_invalid              0       ie_unknown                  0
  ie_out_of_order                  0       ie_unexpected               2
  ie_duplicated                    0       optional_ie_incorrect       0
  pdp_activation_rejected          1       tft_semantic_error          0
  tft_syntactic_error                      pkt_ftr_semantic_error      0
  pkt_ftr_syntactic_error          0       pdp_wo_tft_exist            0
  non_existent 1 path_failure      0
  total_dropped                    0       signalling_msg_dropped      0
  data_msg_dropped 0 no_resource   0
  get_pak_buffer_failure           0       rcv_signalling_msg         11
  snd_signalling_msg              11       rcv_pdu_msg                53
  snd_pdu_msg                     79       rcv_pdu_bytes             865
  snd_pdu_bytes                 3319       total created_pdp           4
  total deleted_pdp                3       total created_ppp_pdp       3
  total deleted_ppp_pdp            3       ppp_regen_pending           0
  ppp_regen_pending_peak           0       ppp_regen_total_drop        0
  ppp_regen_no_resource            0       ntwk_init_pdp_act_rej       0
  total ntwkInit created pdp       0       single pdp-session cleared  0
```

```
  total ntwkInit update pdp       2       total update responses rcv  2
  total COA msg received          2       total COA msgs discarded    0
  total COA triggered update      2       total err indications rcvd    0
  total err indications sent      0       Number of times DT enabled    0
  total EI rcvd on DT PDPs        0       total update fail DT pdps     0
  created ipv6 pdp                0       rejected ipv6 pdp             0
  deleted ipv6 pdp                0       created ipv6 pdpmcb           0
  deleted ipv6 pdpmcb             0
  rcvd ipv6 pdu                   0       sent ipv6 pdu                10
  rcvd ipv6 data bytes            0       sent ipv6 data bytes       1000

 GPRS Network behind mobile Statistics:
  network_behind_ms APNs          1       total_download_route          0
  save_download_route_fail        0       insert_download_route_fail    0
  total_insert_download_route     0

 Debug info:
  path_fail_local_del_pdp         0       ver_upgrade_local_del         0
  no_sgsn_local_del_pdp           0       ver_fallback_local_del        0
  no_wait_sgsn_local_del_pdp      0       no_req_sgsn_local_del_pdp     0
  create_collide_with_delete      0       version_changes               0
  rcv_retransmit_create_req         0       create_as_update                0
router#

router#show gprs gtp statistics | in DT
  total err indications sent      0       Number of times DT enabled    0
  total EI rcvd on DT PDPs 0 total update fail DT pdps 0
```

Table 27 describes the fields shown in the display:

Table 27 show gprs gtp statistics Field Descriptions

Field	Description
created ipv6 pdp	Number of IPv6 PDP contexts created since system startup.
created ipv6 pdpmcb	
data_msg_dropped	Number of GTP PDUs dropped.
Debug info: create_as_update	Number of create PDP context requests treated as update.
Debug info: create_collide_with_delete	Number of create PDP context requests that collided with delete PDP context requests.
Debug info: no_sgsn_local_del_pdp	Number of PDPs deletes because an SGSN could not be found.
Debug info: path_fail_local_del_pdp	Number of PDPs deletes because a path failure occurred.
Debug info: rcv_retransmit_create_req	Number of create PDP context requests for which retransmit requests were received.
Debug info: ver_faillback_local_del	Number of PDP deletes due to version fallback.
Debug info: ver_upgrade_local_del	Number of PDP deletes due to version upgrade
Debug info: verson_changes	Number of PDPs locally deleted due to change in version.
deleted ipv6 pdp	Number of IPv6 PDP contexts deleted since system startup.

Table 27 show gprs gtp statistics Field Descriptions (continued)

Field	Description
deleted ipv6 pdpmcb	
get_pak_buffer_failure	Number of times the GGSN has failed to obtain a GTP packet.
ie_duplicated	Number of GTP messages received with a duplicated information element.
ie_out_of_order	Number of GTP messages received with an information element (IE) out of order.
ie_unexpected	Number of GTP messages received with an information element that not expected in the GTP message, but is defined in GTP. GTP messages with unexpected IEs are processed as if the IE was not present.
ie_unknown	Number of GTP messages received with an information element of an unknown type.
insert_download_route_fail	Number of routes downloaded from the RADIUS server that failed to be inserted into the routing table because they conflicted with others.
mandatory_ie_incorrect	Number of GTP messages received with an incorrect mandatory information element—for example, with an information element that has an incorrect length.
mandatory_ie_missing	Number of GTP messages received with a missing mandatory information element.
msg_too_short	Number of GTP messages received that are too short to hold the GTP header for the supported GTP version.
network_behind_ms APNs	Number of APNs configured to support routing behind the MS.
no_resource	Number of times a resource was not available for transmitting GTP messages. For example, the router may be out of memory.
no_req_sgsn_local_del_pdp	Number of PDPs contexts deleted locally without the GGSN sending a delete PDP context request to the SGSN.[1]
no_sgsn_local_del_pdp	Number of PDPs deleted locally because of no SGSN.
no_wait_sgsn_local_del_pdp	Number of PDPs contexts without waiting for a response from the SGSN.[1]
non-existent	Number of create/update PDP requests received on non-existing PDP contexts.
ntwk_init_pdp_act_rej	Number of rejected PDP context requests that were initiated by the network (PDN).
Number of times DT enabled	
optional_ie_incorrect	Number of GTP messages received with an optional IE that is incorrect, which prevents the GGSN from processing the GTP message correctly.
optional_ie_invalid	Number of GTP messages received with an information element that contains a value that is not within the defined range for that IE. GTP messages with invalid optional IEs are processed as if the IE was not present.

Table 27 show gprs gtp statistics Field Descriptions (continued)

Field	Description
packet_filter_semantic_error	Number of GTP messages received with an IE element with packet filter semantic errors. A semantic error is when the defined format of the information element (IE) is valid but the content of the IE is inconsistent or invalid.
packet_filter_syntactic_error	Number of GTP messages received with an IE element with packet filter syntactic errors. A syntactic error is when the coding of the IE is invalid.
path_failure	Number of path failures on the GPRS Support Node (GSN).
pdp_activation_rejected	Number of times a request to activate a PDP context was rejected.
pdp_wo_tft_exist	Number of Create PDP Context requests received without traffic flow template information element.
ppp_regen_no_resource	Total number of rejected responses to create PDP context and delete PDP context requests due to unavailable resource on the GGSN for PPP regeneration.
ppp_regen_pending	Number of pending PPP regeneration sessions.
ppp_regen_pending_peak	Maximum number of pending PPP regeneration sessions since the statistic was cleared.
ppp_regen_total_drop	Total number of create PDP context and delete PDP context requests that were dropped due to the threshold limit being reached for maximum number of PPP regeneration sessions allowed on the GGSN.
rcvd ipv6 data bytes	Number of bytes received in IPv6 PDUs.
rcvd ipv6 pdu	Number of IPv6 PDU messages received.
rcvd ipv6 signal msg	Number of IPv6 GTP signaling messages received.
rcv_pdu_bytes	Number of bytes received in PDUs.
rcv_pdu_msg	Number of PDU messages received.
rcv_signaling_msg	Number of GTP signaling messages received.
rejected ipv6 pdp	Number of IPv6 PDP context rejected since system startup.
save_download_route_fail	Number of times a downloaded route could not be saved because there was not enough memory.
sent ipv6 data bytes	Number of IPv6 PDU bytes sent.
sent ipv6 pdu	Number of IPv6 PDU messages sent.
sent ipv6 signal msg	Number of IPv6 GTP signaling messages sent.
signalling_msg_dropped	Number of GTP signaling messages dropped.
single pdp-session cleared	Number of hanging single PDP contexts cleared on the GGSN.
snd_pdu_bytes	Number of PDU bytes sent.
snd_pdu_msg	Number of PDU messages sent.
snd_signalling_msg	Number of GTP signaling messages sent.
tft_semantic_error	Number of GTP messages received with an IE element with traffic flow template (TFT) semantic errors. A semantic error is when the defined format of the information element (IE) is valid but the content of the IE is inconsistent or invalid.

Table 27 show gprs gtp statistics Field Descriptions (continued)

Field	Description
tft_syntactic_error	Number of GTP messages received with an IE element with TFT syntactic errors. A syntactic error is when the coding of the IE is invalid.
total COA msg received	Number of CoA messages received on the GGSN.
total COA msg discarded	Number of CoA messages discarded because of error.
total COA triggered deleted	Number of Delete PDP Context Requests initiated because of a COA trigger.
total COA triggered update	Number of Update PDP Context Requests initiated because of a COA trigger.
total created DT PDPs	Number of direct tunnel PDP contexts established.
total created_pdp	Number of PDP contexts created since system startup (supports Special Mobile Group (SMG)-28 standards level and later)
total created_ppp_pdp	Number of PDP contexts created for PPP PDP PDU types.
total deleted_pdp	Number of PDP contexts deleted since system startup (supports SMG-28 standards level and later)
total deleted_ppp_pdp	Number of PDP contexts created for PPP PDP PDU types deleted since system startup.
total_download_route	Number of routes downloaded from the RADIUS server.
total_dropped	Number of GTP messages dropped.
total EI rcvd on DT PDPs	Number of error indications sent from the RNC received on the GGSN for direct tunnel PDPs.
total error indication rcvd	Number of error indications received on the GGSN.
total error indication sent	Number of error indications sent.
total_insert_download_route	Total number of routes downloaded from the RADIUS server that have been inserted into the routing table by the GGSN.
total ntwkInit created pdp	Number of PDP context requests activated by the GGSN that were initiated by the network (PDN).
total netwkInit update pdp	Number of Update PDP Context Requests sent by the GGSN.
total update fail DT PDPs	Number of direct tunnel PDP contexts deleted because a successful Update PDP Context Response was not received.
total update responses rcv	Number of update request responses received.
unexpected_data_msg	Number of GTP PDUs received for nonexistent PDP contexts.
unexpected_sig_msg	Number of unexpected GTP signaling messages received—for example, a message received on the wrong end of the tunnel or a response message received for a request that was not sent by the GGSN.
unknown_msg	Number of unknown GTP messages received.
unsupported_comp_exthdr	Number of Create PDP Context requests received with unsupported extension headers when GGSN comprehension is required.
version_not_support	Number of GTP messages received from devices running an unsupported version of the GTP.

1. This field displays only when an APN is in maintenance mode (the **service-mode maintenance** access-point configuration command).

Related Commands

Command	Description
clear gprs gtp statistics	Clears the current GGSN GTP statistics.
clear gprs statistics all	Clears all GGSN counters and statistics (both global and per-APN).
show gprs gtp path statistics	Display information about one or more GTP paths between the GGSN and other GPRS/UMTS devices.

show gprs gtp status

To display information about the current status of the GPRS Tunneling Protocol (GTP) on the gateway GPRS support node (GGSN) (such as activated PDP contexts, throughput, and QoS statistics), use the **show gprs gtp status** command in privileged EXEC mode.

show gprs gtp status

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX, and the following output fields were added: • activated_ppp_pdp • activated_ppp_regen_pdp • ntwk_init_pdp • qos_delay1_pdp • qos_delay2_pdp • qos_delay3_pdp • qos_delaybesteffort_pdp
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into the Cisco IOS Release 12.2(8)YW and the following output fields were added: • activated gtpv0 pdp • activated gtpv1 pdp • activated ms
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU and the QoS information was removed.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.

Release	Modification
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ and the following output fields were added to YQ1: • Prepaid PDPs • Postpaid PDPs
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.
12.4(9)XG	This command was integrated into Cisco IOS Release 12.4(9)XG and the following fields were added to the output display: • activated ipv6 ms • activated gtpv0 ipv6 pdp • activated gtpv1 ipv6 pdp • gtp ipv6 swidbs
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ and the following field was added to the display: • gtp direct tunnel PDPs • gtp's va swidbs

Usage Guidelines

Use the **show gprs gtp status** command to display information about the status of GTP running on the GGSN.

Examples

The following example shows output from the **show gprs gtp status** command:

```
router#show gprs gtp status
 GPRS GTP Status:
   activated gtpv0 pdp     2
   activated gtpv1 pdp     7
   activated ms            9
   activated ipv6 ms       2
   activated gtpv0 v6 pdp  1
   activated gtpv1 v6 pdp  1
   activated ppp regen pdp 1
   activated ppp pdp       2
   gtp's va hwidbs         2
   gtp's va swidbs         1
   gtp ipv6 swidbs         2
   gtp direct tunnel PDPs  7
 Service-aware Status:
   Prepaid PDPs            0
   Postpaid PDPs           0
router#
```

Table 28 describes the fields shown in the display.

Table 28 show gprs gtp status Field Descriptions

Field	Description
activated gtpv0 pdp	Number of IPv4 PDP contexts created with GTP version 0.
activated gtpv0 ipv6 pdp	Number of IPv6 PDP contexts created with GTP version 0.
activated gtpv1 pdp	Number of IPv4 PDP contexts created with GTP version 1.
activated gtpv1 ipv6 pdp	Number of IPv6 PDP contexts created with GTP version 1.
activated ipv6 ms	Number of active IPv6 mobile stations (MS).
activated ms	Number of active IPv4 MSs.
activated_ppp_pdp	Number of point-to-point protocol IPv4 PDP contexts currently active.
activated_ppp_regen_pdp	Number of IPv4 point-to-point protocol PDP contexts created on the GGSN.
gtp direct tunnel PDPs	Number of direct tunnel PDPs currently active.
gtp ipv6 swidb	Number of virtual access created for IPv6 PDP contexts.
gtp's ppp va hwidbs	Number of virtual access created for IPv4 PPP PDP contexts.
gtp's va swidbs	Number of virtual access created for
ntwk_init_pdp	Current number of active IPv4 PDP contexts that are initiated by the network to an MS.
Prepaid PDPs	Current number of active prepaid IPv4 PDP contexts.
Postpaid PDPs	Current number of active postpaid IPv4 PDP contexts.

Related Commands

Command	Description
show gprs gtp statistics	Displays the current GTP statistics for the GGSN.

show gprs memory threshold statistics

To display information about the number of PDP contexts that have been deleted or the number of Create PDP Context requests that have been rejected because of the memory threshold has been exceeded, use the **show gprs memory threshold statistics** command in privileged EXEC mode:

show gprs memory threshold statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs memory threshold statistics** command to obtain information about the number of PDP contexts that have been deleted or the number of Create PDP Context requests that have been rejected because the memory threshold has been exceeded.

Examples

The following example shows output from the **show gprs memory threshold statistics** command:

```
GGSN# show gprs memory threshold statistics
Memory Threshold Statistics
    ================================================
    GGSN memory threshold status :NOT IN THRESHOLD

    Number of times reached :       0
    Number of PDPs rejected :       0
    Number of PDPs dropped due to
              duration limit :      0
              volume limit :        0
              update request :      0

    Time when last memory threshold was reached :NEVER
```

Table 24 describes the fields shown in the display.

Table 29 show gprs memory threshold statistics Field Descriptions

Field	Description
GGSN memory threshold status	Current status of the GGSN memory threshold. Possible values are “in threshold” and “not in threshold.”
Number of times reached	Number of times the GGSN memory threshold has been reached since last startup.
Number of PDPs rejected	Number of Create PDP Contexts rejected because the GGSN exceeded its memory threshold.
Number of PDPs dropped due to: duration limit	Number of existing PDP contexts dropped while in memory threshold because of the generation of a CDR with the duration limt trigger configured using the **limit duration** charging profile configuration command.
Number of PDPs dropped due to: volume limit	Number of existing PDP contexts dropped while in memory threshold because of the generation of a CDR with the volume limit trigger configured using the **limit volume** charging profile configuration command.
Number of PDPs dropped due to: update request	Number of existing PDP contexts dropped while in memory threshold because of a PDP context update message.
Time when the last memory threshold was reached	Last time the GGSN memory threshold was exceeded.

show gprs ms-address exclude-range

To display the IP address range(s) configured on the gateway GPRS support node (GGSN) for the GPRS/UMTS network, use the **show gprs ms-address exclude-range** command in privileged EXEC mode.

show gprs ms-address exclude-range

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs ms-address exclude-range** command to display the IP address range(s) configured on the GGSN for the GPRS network.

IP addresses are 32-bit values.

Examples

The following is sample output of the **show gprs ms-address exclude-range** command:

```
router# show gprs ms-address exclude-range
Start IP         End IP
10.0.0.1         10.10.10.10
```

Table 25 describes the fields shown in the display.

Table 30 show gprs ms-address exclude-range Field Descriptions

Field	Description
Start IP	IP address at the beginning of the range.
End IP	IP address at the end of the range.

Related Commands

Command	Description
gprs ms-address exclude-range	Specifies the IP address range(s) used by the GPRS network and thereby excluded from the mobile station (MS) IP address range.

show gprs pcscf

To display a summary of the P-CSCF server group(s) configured on the GGSN for P-CSCF Discovery, use the **show gprs pcscf** command in privileged EXEC mode.

show gprs pcscf

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(2)XB	This command was introduced.
12.4(9)XG	This command was integrated into Cisco IOS Release 12.4(9)XG and the command has been modified to display IPv6 servers that are a part of a P-CSCF server group.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.

Usage Guidelines

Use the **show gprs pcscf** command to display a summary of the P-CSCF server group(s) configured on the GGSN.

Examples

The following example shows the output for the **show gprs pcscf** command:

```
router#show gprs pcscf
P-CSCF Group name:groupA
List of IP addresses in the group:
172.76.82.77
192.3.3.3

P-CSCF Group name:groupB
List of IP addresses in the group:
172.76.82.77
192.4.4.4

P-CSCF Group name:groupC
List of IP addresses in the group:
2001:999::9
```

Related Commands

Command	Description
gprs pcscf	Configures a P-CSCF server group on the GGSN and enters P-CSCF group configuration mode.
pcscf	Assigns a P-CSCF server group to an APN.
server	Specifies the IP address of a P-CSCF server you want to include in the P-CSCF server group.
show gprs access-point	Displays information about access points on the GGSN.

show gprs plmn

To display the mobile country code (MCC) and mobile network code (MNC) of the home and trusted PLMNs, use the **show gprs plmn** command in privileged EXEC mode.

show gprs plmn

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs plmn** command to display the configured MCCs and MNCs of the home and trusted PLMNs.

Examples

The following is sample output of the **show gprs plmn ip address** command:

```
GGSN# show gprs plmn
Home PLMN
  MCC = 302  MNC = 678
Trusted PLMN
  MCC = 346  MNC = 123
  MCC = 234  MNC = 67
  MCC = 123  MNC = 45
  MCC = 100  MNC = 35
```

Related Commands

Command	Description
gprs mcc mnc	Configure MCC and MNC that the GGSN uses to determine if a Create PDP Context request is from a roamer.

show gprs plmn ip address

To display the IP address range(s) configured for a PLMN, use the **show gprs plmn ip address** command in privileged EXEC mode.

show gprs plmn ip address

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)YW	This command was introduced.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs plmn ip address** command to display the IP address range(s) configured for a PLMN.

IP addresses are 32-bit values.

Examples

The following is sample output of the **show gprs plmn ip address** command:

```
router# show gprs plmn ip address
PLMN Start IP    End IP           Range Type
9.9.9.9          9.9.9.9
10.2.25.1        10.2.25.255
16.0.0.9         16.0.0.9
99.100.0.1       99.100.0.255
101.0.1.1        101.0.1.1        sgsn
105.0.1.1        105.0.1.1        sgsn
106.0.1.1        106.0.1.1        sgsn
110.12.0.2       110.12.0.2
110.13.0.2       110.13.0.2
```

Table 25 describes the fields shown in the display.

Table 31 show gprs plmn ip address Field Descriptions

Field	Description
PLMN Start IP	IP address at the beginning of the range.
End IP	IP address at the end of the range.

Related Commands

Command	Description
gprs plmn ip address	Specifies the PLMN IP address range(s) used by the GGSN.

show gprs qos status

To display the number of PDP contexts currently active on the gateway GPRS support node (GGSN) for a particular QoS class, use the **show gprs qos status** command in privileged EXEC mode.

show gprs qos status

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)YW	This command was introduced.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs qos status** command to display the number of PDP contexts currently active on the GGSN for a particular QoS class.

Examples

Example 1

The following example shows output from the **show gprs qos status** command for UMTS QoS:

```
router# show gprs qos status
GPRS QoS Status:
  type:UMTS
  conversational_pdp      100   streaming_pdp     150
  interactive_pdp         1345  background_pdp    2000
```

Table 27 describes the fields shown in the display.

Table 32 show gprs qos status Field Descriptions

Field	Description
type	Type of QoS. Possible QoS types are: • Canonical—Configured using the **gprs qos map canonical-qos** command. • Delay—Configured using the **gprs qos map delay** command. • UMTS—Configured using the **gprs qos map umts** command. • None—No QoS is configured on the GGSN.
conversational_pdp	Current number of PDP contexts that have a conversational UMTS QoS traffic class.
streaming_pdp	Current number of PDP contexts that have a streaming UMTS QoS traffic class.
interactive_pdp	Current number of PDP contexts that have a interactive UMTS QoS traffic class.
background_pdp	Current number of PDP contexts that have a background UMTS QoS traffic class.

Example 2

The following example displays output from the **show gprs qos status** command for canonical QoS:

```
router# show gprs qos status
GPRS QoS Status:
type:Canonical
 gsn_used_bandwidth:1110.000        total gsn_resource:1048576
 mean_throughput_premium:0.000
 mean_throughput_normal:1110.000    mean_throughput_besteffort 0.000
 qos_high_pdp:0                     qos_normal_pdp:1
 qos_low_pdp :0                     qos_premium mean-throughput-deviation 0.100
```

Table 28 describes the fields shown in the display.

Table 33 show gprs qos status Field Descriptions

Field	Description
gsn_used_bandwidth	Currently used bandwidth, in bits per second. Represents the cumulative bandwidth for all active PDP context requests currently using canonical QoS. This field only appears when canonical QoS is enabled.
mean_throughput_besteffort	Total mean throughput for best effort QoS users, in bits per second. Represents the cumulative throughput for all active PDP context requests classified in the best effort canonical QoS class. This field only appears when canonical QoS is enabled.

Table 33 show gprs qos status Field Descriptions

Field	Description
mean_throughput_normal	Total mean throughput for normal QoS users, in bits per second. Represents the cumulative throughput for all active PDP context requests classified in the normal canonical QoS class. This field only appears when canonical QoS is enabled.
mean_throughput_premium:	Total mean throughput for premium QoS users, in bits per second. Represents the cumulative throughput for all active PDP context requests classified in the premium canonical QoS class. This field only appears when canonical QoS is enabled.
qos_high_pdp	Current number of active PDP contexts that are classified in the premium canonical QoS class. This field only appears when canonical QoS is enabled.
qos_low_pdp	Current number of PDP contexts that are classified in the best effort canonical QoS class. This field only appears when canonical QoS is enabled.
qos_normal_pdp	Current number of PDP contexts that are classified in the normal canonical QoS class. This field only appears when canonical QoS is enabled.
qos_premium mean-throughput-deviation	Current mean throughput deviation for QoS. This field only appears when canonical QoS is enabled.
total gsn_resource	Currently available GSN resources. This field only appears when canonical QoS is enabled.
type	Type of QoS. Possible QoS types are: • Canonical—Configured using the **gprs qos map canonical-qos** command. • Delay—Configured using the **gprs qos map delay** command. • UMTS—Configured using the **gprs qos map umts** command. • None—No QoS is configured on the GGSN.

Example 3

The following example displays output from the **show gprs qos status** command for delay QoS:

```
router# show gprs qos status
GPRS QoS Status:
type:Delay
qos_delay1_pdp:0            qos_delay2_pdp: 0
qos_delay3_pdp:0            qos_delaybesteffort_pdp    0
```

Table 29 describes the fields shown in the display.

Table 34 show gprs qos status Field Descriptions

Field	Description
type	Type of QoS. Possible QoS types are: • Canonical—Configured using the **gprs qos map canonical-qos** command. • Delay—Configured using the **gprs qos map delay** command. • UMTS—Configured using the **gprs qos map umts** command. • None—No QoS is configured on the GGSN.
qos_delay1_pdp	Current number of active PDP contexts that are classified in the class 1 delay QoS class. This field only appears when delay QoS is enabled.
qos_delay2_pdp	Current number of active PDP contexts that are classified in the class 2 delay QoS class. This field only appears when delay QoS is enabled.
qos_delay3_pdp	Current number of active PDP contexts that are classifed in the class 3 delay QoS class. This field only appears when delay QoS is enabled.
qos_delaybesteffort_pdp	Current number of active PDP contexts that are classified in the best effort delay QoS class. This field only appears when delay QoS is enabled.

Example 4

The following example shows output from the **show gprs qos status** command when no QoS has been configured on the GGSN:

```
router# show gprs qos status
GPRS QoS Status:
type:None
```

Related Commands

Command	Description
gprs qos map canonical-qos	Enables mapping of GPRS QoS categories to a canonical QoS method that includes best-effort, normal, and premium QoS classes.
gprs qos map delay	Enables Delay QoS on the GGSN.
gprs qos map umts	Enables UMTS QoS on the GGSN.

show gprs redundancy

To display statistics related to GTP-SR, use the **show gprs redundancy** command in privileged EXEC mode.

show gprs redundancy [**statistics**]

Syntax Description

statistics	Displays GTP-SR statistics.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(11)YJ	This command was introduced.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs redundancy** command to display GTP-SR related event queues and/or statistics.

Examples

The following example shows the output for the **show gprs redundancy statistics** command:

```
GGSN#show gprs redundancy statistics

tb10-7600-5-2#show  gprs redundancy statistics
GPRS Redundancy Statistics
  Last cleared:never

  CheckPointed-From-Active Statistics

    Total Number of Messages:                 9
      Number of Context Setup messages:       0
      Number of Context Modify messages:      0
      Number of Context Remove messages:      0
      Number of Path Setup messages:          0
      Number of Path Modify messages:         0
      Number of Path Remove messages:         0
      Number of CGF Ready messages:           1
      Number of CGF Modify messages:          0
      Number of CGF Remove messages:          0
      Number of Internal State messages:      8
```

The following example shows the output for the **show gprs redundancy** command:

```
GGSN#show gprs redundancy
GPRS redundancy is enabled and Unit-Status is Standby

Redundancy Transport Infrastructure status
  Redundancy Infrastructure state:             STANDBY HOT
  Peer Redundancy Infrastructure state:        ACTIVE

  GGSN Redundancy system up since:             00:01:16 UTC Mar 1 2002
  Time of last switchover:                     never
  Total Number of Switchovers:                 0

GPRS Redundancy Statistics
  Last cleared:never

  CheckPointed-From-Active Statistics

    Total Number of Messages:                  9
      Number of Context Setup messages:        0
      Number of Context Modify messages:       0
      Number of Context Remove messages:       0
      Number of Path Setup messages:           0
      Number of Path Modify messages:          0
      Number of Path Remove messages:          0
      Number of CGF Ready messages:            1
      Number of CGF Modify messages:           0
      Number of CGF Remove messages:           0
      Number of Internal State messages:       8
```

Table 30 describes the fields shown in the display.

Table 35 show gprs redundancy Field Descriptions

Field	Description
Redundancy Transport Infrastructure state	Current state of the local redundancy infrastructure.
Peer Redundancy Infrastructure state	Current state of the redundancy infrastructure on the peer GGSN. Possible values are ACTIVE or STANDBY.
GGSN Redundancy system up since	Time at which the GTP-SR system was established.
Time of last switchover	Time the last switchover occurred.
Total Number of Switchovers	Total number of times a switchover has occurred since GTP-SR system has been up.
Last cleared	Time GTP-SR statistics were last cleared.
Total number of Messages	Total number of GTP-SR related messages received.
Number of Context Setup messages	Number of Create PDP Context messages received.
Number of Context Modify messages	Number of modify PDP context messages received.
Number of Context Remove messages	Number of delete PDP context messages received.
Number of Path Setup messages	Number of SGSN-to-GGSN path setup messages received.
Number of Path Modify messages	Number of SGSN-to-GGSN path modify messages received.
Number of Path Remove messages	Number of SGSN-to-GGSN path deletion messages received.

Table 35 show gprs redundancy Field Descriptions (continued)

Field	Description
Number of CGF Ready messages	Number of GGSN-to-CG functionality ready messages received.
Number of CGF Modify messages	Number of GGSN-to-CG path change messages received.
Number of CGF Remove messages	Number of GGSN-to-CG path deletion messages received.
Number of Internal State messages	Number of internal state messages.

Related Commands

Command	Description
clear gprs redundancy statistics	Clears statistics related to GTP-SR.
gprs redundancy	Enables GTP-SR on a GGSN.
gprs redundancy charging sync-window cdr rec-seqnum	Configures the window size used to determine when the CDR record sequence number needs to be synchronized to the Standby GGSN.
gprs redundancy charging sync-window gtpp seqnum	Configures the window size used to determine when the GTP' sequence number needs to be synchronized to the Standby GGSN.

show gprs service-aware statistics

To view statistics related to the service-aware features of the gateway GPRS support node (GGSN), such as packets sent to, and received from, the Diameter server or CSG, use the **show gprs service-aware statistics** command in privileged EXEC mode:

show gprs service-aware statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privilege EXEC

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs service-aware statistics** command to display the statistics related to service-aware features for the GGSN.

The counter values displayed by this command represent totals accumulated since the last time the statistical counters were cleared using the **clear gprs service-aware statistics** command.

Examples

The following is sample output of the **show gprs service-aware statistics** command:

```
router#show gprs service-aware statistics
GGSN service-aware statistics:
  num service aware apn 1
  total_ggsn_event           4          total_ggsn_failure         0
  total_csg_event            23999      total_csg_failure          0
  total_dcca_event           23996      total_dcca_failure         5
  total_category_created     23996      total_category_deleted     4
  total_sync_object_created  6000       total_sync_object_deleted  6000
  category_fsm_return_error  0          total_quota_push_ack       23995
  total_service_auth         0          total_service_reauth       0
  total_service_stop         4          total_quota_return         0
  total_quota_granted        23995      total_terminate_category   0
  total_blacklisted_category 1          total_unknown_category     0
  total_RAR_event            0          total_rating_change        0
  total_delete_pdp           0          total_convert_to_postpaid  0
  report_final_convert_to_postpaid 0    total_send_dummy_quota     0
  category_wait_csg_timeout  0          sync_timeout_ser_stop      1
  sync_timeout_qr            0          sync_timeout_other         0

GGSN service-aware pdp session statistics:
  total_prepaid_users        5994       total_postpaid_users         10
  reject_due_to_dcca_failure 0          reject_due_to_csg_failure    0
  reject_due_to_other_reason 0
```

Table 31 describes the fields shown in the display.

Table 36 show gprs service-aware statistics Field Descriptions

Field	Description
num service aware apn	Number of APNS that are service-aware (i.e., for which credit-control will be performed using a Diameter server).
total_ggsn_event	Number of PDP-level events received, such as GTP update event or sending an accounting-stop message.
total_ggsn_failure	Number of internal failures associated with creating, accessing, or manipulating various category-related dtat structures.
total_csg_event	Number of CSG-related events received by various categories, such as Quota Push Ack, Service-Auth, or Service-Reauth.
total_csg_failure	Number of CSG-related errors received, such as GTP' NACK.
total_dcca_event	Number of DCCA-server related events received by various categories, such as Quota Grants, Blacklists, or Authorization Denied.
total_dcca_failure	Number of times the DCCA server has not responded during a specified time period.
total_category_created	Number of categories created across all PDP contexts.
total_category_deleted	Number of categories deleted across all PDP contexts.
total_sync_object_created	Number of sync objects created, to which to send multiple messages associated with an event.
total_sync_object_deleted	Number of sync objects deleted. A sync object is required when a DCCA procdure such as Quota-Push needs to be performed for multiple categories in a single CCR/CCA.

Table 36 show gprs service-aware statistics Field Descriptions (continued)

Field	Description
category_fsm_return_error	Number of internal erros while executing the category state machine.
total_quota_push_ack	Number of Quota Push acknowledgements received from the CSG.
total_service_auth	Number of Service-Auth requests received from the CSG.
total_service_reauth	Number of Service-Reauth requests received from the CSG.
total_service_stop	Number of Service-Stop responses received from the CSG.
total_quota_return	Number of Quota-Return messages received from the CSG.
total_quota_granted	Number of times quota has been granted by the DCCA server for various categories.
total_terminate_category	Number of times the DCCA server has terminated the service because authorization was denied or the user's credit was exhausted.
total_blacklisted_category	Number of times the DCCA server blacklisted a category.
total_unknown_category	Number of times the DCCA server has responded with a DIAMETER_RATING_FAILED message.
total_RAR_event	Number of times an update PDP context request has been received by category.
total_rating_change	Number of times an update PDP context event has been received by category.
total_delete_pdp	Not currently used.
total_convert_to_postpaid	Number of times a CC session has been converted to postpaid session because of an unresponsive DCCA server.
report_final_convert_to_postpaid	Number of times a session was converted to a postpaid session because of an invalid answer from the DCCA server.
total_send_dummy_quota	Number of times dummy quota has been granted because of a slow DCCA server (for example, a server that didn't respond in the required Tx time interval).
category_wait_csg_timeout	Number of times a category timeout occurred on service stop.
sync_timeout_ser_stop	Sync_object timeout on service stop.
sync_timeout_qr	Sync_object timeout on quota return.
sync_timeout_other	Sync_object timeout on other reasons.
total_prepaid_users	Number of service-aware users treated as pre-paid users.
total_postpaid_users	Number of service-aware users treated as post-paid users.
reject_due_to_dcca_failure	Number of times a PDP context has been rejected because of a failure to communicate with a DCCA server.
reject_due_to_csg_failure	Number of times a PDP context has been rejected because of a failure to communicate with a CSG server.
reject_due_to_other_reason	Number of times a PDP contect has been rejected for other reasons.

Related Commands

Command	Description
clear gprs service-aware statistics	Displays information about access points on the GGSN.

show gprs slb detail

To display all Cisco IOS SLB-related information, such as operation mode, virtual server addresses, SLB notifications, and statistics, use the **show gprs slb detail** command in privileged EXEC mode.

show gprs slb detail

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU and the Subscriber exit field was added to the output.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB and the following fields were removed from the display: • SLB Notifications sent – CAC failure – Subscriber ext The following fields were added to the SLB Statistics section of the display: • CAC-failure notifications sent • Session-deletion notifications sent • PDP status notifications sent • PDP status negative response sent • PDP status requests received

Usage Guidelines

Use the **show gprs slb detail** command to display to all Cisco IOS SLB-related information, including statistics associated with GTP SLB sticky database support.

Examples

The following example shows the output for the **show gprs slb detail** command:

```
GGSN#show gprs slb detail
SLB Operation Mode:dispatched
SLB vservers:
  10.10.195.1
SLB Statistics:
  CAC-failure notifications sent:             0
  Session-deletion notifications sent:        0
  PDP status notifications sent:              0
  PDP status negative response sent:          0
  PDP status requests received:               0
GGSN#
```

Table 32 describes the fields shown in the display.

Table 37 show gprs slb detail Field Descriptions

Field	Description
CAC-failure notifications sent	Number of times the GGSN has notified the Cisco IOS SLB that a Call Admission Control (CAC) or canonical QoS failure has occurred.
PPP status negative response sent	Number of responses sent to the IOS SLB after the sticky object idle timer has expired that indicate that the PDP context associated with the sticky object has ended.
PPP status notifications sent	Number of status notifications sent to the IOS SLB after the idle timer on associated sticky object has expired that indicate whether a PDP context is active or has ended.
PPP status requests received	Number of IOS SLB requests received by the GGSN.
Session-deletion notifications sent	Number of times the GGSN has notified the Cisco IOS SLB that the last PDP context associated with an IMSI has been deleted.
SLB Operation Mode:	Mode of operation in which the Cisco IOS SLB is functioning. Possible values are dispatched and directed.
SLB vservers	IP addresses of the virtual servers to be notified by the GGSN when the specific type of condition defined using the **gprs slb notify** command occurs.

Related Commands

Command	Description
clear gprs slb statistics	Clears Cisco IOS SLB statistics.
gprs slb mode	Defines the Cisco IOS SLB operation mode.
gprs slb notify	Enables the GGSN to notify the Cisco IOS SLB when a specific type of condition occurs.
gprs slb vserver	Configures the Cisco IOS SLB virtual servers to be notified by the GGSN when the specific type of condition defined using the **gprs slb notify** command occurs.
show gprs slb mode	Displays the Cisco IOS SLB mode of operation.
show gprs slb statistics	Displays Cisco IOS SLB statistics.
show gprs slb vservers	Displays the list of defined Cisco IOS SLB virtual servers.

show gprs slb mode

To display the Cisco IOS SLB mode of operation defined on the gateway GPRS support node (GGSN), use the **show gprs slb mode** command in privileged EXEC mode.

show gprs slb mode

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs slb mode** command to display the Cisco IOS SLB operation mode defined on the GGSN.

Examples

The following example shows that the Cisco IOS SLB operation mode is defi ned as dispatch mode:

```
GGSN#show gprs slb mode
SLB Operation Mode:dispatched
```

Related Commands

Command	Description
clear gprs slb statistics	Clears Cisco IOS SLB statistics.
gprs slb mode	Defines the Cisco IOS SLB operation mode.
gprs slb notify	Enables the GGSN to provide feedback to the Cisco IOS SLB when a specific condition occurs.
gprs slb vserver	Configures the Cisco IOS SLB virtual servers to be notified by the GGSN when the specific type of condition defined by the **gprs slb notify** command occurs.
show gprs slb detail	Displays Cisco IOS SLB related information, such as the operation mode, virtual servers addresses, and statistics.

Command	Description
show gprs slb statistics	Displays Cisco IOS SLB statistics.
show gprs slb vservers	Displays the list of defined Cisco IOS SLB virtual servers.

show gprs slb statistics

To display Cisco IOS SLB statistics, use the **show gprs slb mode** command in privileged EXEC mode.

show gprs slb statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into the Cisco IOS Release 12.3(14)YU and the Subscriber exit field was added to the output.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB and the following fields were removed from the display: • SLB Notifications sent – CAC failure – Subscriber exit The following fields were added to the SLB Statistics section of the display: • CAC-failure notifications sent • Session-deletion notifications sent • PDP status notifications sent • PDP status negative response sent • PDP status requests received

Usage Guidelines

Use the **show gprs slb statistics** command to display IOS SLB statistics, including statistics associated with GTP SLB sticky database support.

Examples

The following example displays IOS SLB-related statistics on the GGSN:

```
GGSN#show gprs slb statistics
SLB Statistics:
    CAC-failure notifications sent:             0
    Session-deletion notifications sent:        0
    PDP status notifications sent:              0
    PDP status negative response sent:          0
    PDP status requests received:               0
```

Table 33 describes the fields shown in the display.

Table 38 show gprs slb statistics Field Descriptions

Field	Description
CAC-failure notifications sent	Number of times the GGSN has notified the Cisco IOS SLB that a Call Admission Control (CAC) or canonical QoS failure has occurred.
PPP status negative response sent	Number of responses sent to the IOS SLB after the sticky object idle timer has expired that indicate that the PDP context associated with the sticky object has ended.
PPP status notifications sent	Number of status notifications sent to the IOS SLB after the idle timer on associated sticky object has expired that indicate whether a PDP context is active or has ended.
PPP status requests received	Number of IOS SLB requests received by the GGSN.
Session-deletion notifications sent	Number of times the GGSN has notified the IOS SLB that the last PDP context associated with an IMSI has been deleted.

Related Commands

Command	Description
clear gprs slb statistics	Clears Cisco IOS SLB statistics.
gprs slb mode	Defines the Cisco IOS SLB operation mode.
gprs slb notify	Enables the GGSN to notify the Cisco IOS SLB when a specific type of condition occurs.
gprs slb vserver	Configures the Cisco IOS SLB virtual servers to be notified by the GGSN when the specific type of condition defined using the **gprs slb notify** command occurs.
show gprs slb detail	Displays Cisco IOS SLB related information, such as the operation mode, virtual servers addresses, and statistics.
show gprs slb mode	Displays the Cisco IOS SLB mode of operation defined on the GGSN.
show gprs slb vservers	Displays the list of defined Cisco IOS SLB virtual servers.

show gprs slb vservers

To display a list of Cisco IOS SLB virtual servers to be notified by the gateway GPRS support node (GGSN) when the specific type of condition defined using the **gprs slb notify** command occurs, use the **show gprs slb vservers** command in privileged EXEC mode.

show gprs slb vservers

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs slb vservers** command to display a list of Cisco IOS SLB virtual servers to be used for GGSN-SLB messaging.

Examples

The following example shows a list of virtual servers that were defined using the **gprs slb vservers global** configuration command:

```
GGSN#show gprs slb vservers
SLB vservers:
10.10.10.10
11.11.11.11
```

Related Commands

Command	Description
clear gprs slb statistics	Clears Cisco IOS SLB statistics.
gprs slb mode	Defines the Cisco IOS SLB operation mode.
gprs slb notify	Enables the GGSN to notify the Cisco IOS SLB when a specific type of condition occurs.
gprs slb vserver	Configures the Cisco IOS SLB virtual servers to be notified by the GGSN when the specific type of condition defined by the **gprs slb notify** command occurs.

Command	Description
show gprs slb detail	Displays Cisco IOS SLB related information, such as the operation mode, virtual servers addresses, and statistics.
show gprs slb mode	Displays the Cisco IOS SLB mode of operation defined on the GGSN.
show gprs slb statistics	Displays Cisco IOS SLB statistics.

show gprs service-mode

To display the current service mode of the gateway GPRS support node (GGSN) and the last time the service mode was changed, issue the **show gprs service-mode** command in privileged EXEC mode.

show gprs service-mode

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs service-mode** command to display the current service mode of a GGSN and the last time the service mode was changed.

Examples

Example 1

The following example shows output from the **show gprs service-mode** command when no service-mode change has occurred:

```
GGSN# show gprs service-mode
Service mode:operational
GGSN#
```

Example 2

The following example shows output from the **show gprs service-mode** command when a service-mode change has occurred:

```
GGSN# show gprs service-mode
Service mode:maintenance last change at: 23:49:21 UTC Mon January 20, 2004
GGSN#
```

Related Commands

Command	Description
gprs charging service-mode	Configures the service-mode state of a GGSN's charging functions.
gprs service-mode	Configures the service-mode state of a GGSN.
service-mode	Configures the service-mode state of an APN.

show gprs umts-qos map traffic-class

To display UMTS QoS mapping information, use the **show gprs umts-qos map traffic-class** command in privileged EXEC mode.

show gprs umts-qos map traffic-class {**all | signalling | conversational | streaming | interactive | background**}

Syntax Description

all	Displays information for all UMTS QoS traffic classes.
signalling	Displays information for the UMTS QoS traffic class signalling.
conversational	Displays information for the UMTS QoS traffic class conversational.
streaming	Displays information for the UMTS QoS traffic class streaming.
interactive	Displays information for the UMTS QoS traffic class interactive.
background	Displays information for the UMTS QoS traffic class background.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)YW	This command was introduced.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs umts-qos map traffic-class** command to display information about UMTS QoS mapping.

Examples

The following example shows output from the **show gprs umts-qos map traffic-class** command for all UMTS QoS traffic classes:

```
router# show gprs umts-qos map traffic-class all
Traffic Class       Diffserv PHB Group       Diffserv Code Point

signaling           Signaling Class          40

conversational      EF Class                 46

streaming           AF2 Class                18,20,22
```

```
interactive         AF3 Class               26,28,30

background          Best Effort             0
```

Table 34 describes the fields shown in the display.

Table 39 show gprs umts-qos map traffic-class Field Descriptions

Field	Description
Traffic Class	Type of UMTS QoS traffic class as specified in the **gprs umts-qos map traffic-class** command. The UMTS QoS traffic classes are: • signaling • conversational • streaming • interactive • background
Diffserv PHB Group	Type of DiffServ PHB group as specified in the **gprs umts-qos map diffserv-phb** command. Possible DiffServ PHB groups are: • signalling-class • ef-class • af1-class • af2-class • af3-class • af4-class • best-effort
Diffserv Code Point	Number of DSCPs as specified in the **gprs umts-qos map diffserv-phb** command.

Related Commands

Command	Description
gprs umts-qos map traffic-class	Specifies a QoS mapping from the UMTS traffic classes to a differentiated services (DiffServ) per-hop behavior (PHB) group
gprs umts-qos map diffserv-phb	Assigns a differentiated services code point (DSCP) to a DiffServ PHB group.

show gprs umts-qos police pdp-context tid

To display policing statistics for a PDP context, use the **show gprs umts-qos police pdp tid** command in privileged EXEC mode.

show gprs umts-qos police pdp-context tid *tid*

Syntax Description

tid	Specifies the tunnel ID for which you want to display policing statistics.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs umts-qos police pdp-context tid** command to display policing information for a PDP context.

Examples

The following example shows output from the **show gprs umts-qos police pdp-context tid** command for a PDP context:

```
GGSN#sh gprs umts-qos police pdp-context tid 1203000000000010
DOWNLINK POLICING STATISTICS
Flow id:1
      police:
          rate 5184000 , bc 1500 bytes
         peak-rate 7424000, be 1800 bytes
        conformed 2 packets, 200 bytes; actions:
          set-dscp-transmit 15
        exceeded 0 packets, 0 bytes; actions:
          set-dscp-transmit 15
        violated 0 packets, 0 bytes; actions:
          drop

   Flow id:Identifier used in communication with IOS QoS regarding a
            particular flow.

   rate :Average rate in bits per second.

   bc :Normal burst size in bytes
```

```
peak-rate :peak rate in bits per second

be :Excess burst size in bytes.
```

Related Commands

Command	Description
police rate	Configures traffic policing using the police rate.
service-policy	Attaches a service policy to an APN, to be used as the service policy for PDP flows of that APN.

show gprs umts-qos profile pdp tid

To display requested and negotiated QoS information for a PDP context, use the **show gprs umts-qos profile pdp tid** command in privileged EXEC mode.

show gprs umts-qos profile pdp tid *tid*

Syntax Description

tid	Specifies the tunnel ID for which you want to display policing statistics.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show gprs umts-qos profile pdp tid** command to display requested and negotiated QoS information for a PDP context.

Examples

The following example shows output from the **show gprs umts-qos profile pdp tid** command for R97/R98 QoS:

```
show gprs umts-qos profile pdp tid 1203000000000010
Requested QoS Profile               Negotiated QoS Profile
=================                   =================
Delay Class:2                       Delay Class:2
Reliability:1                       Reliability:1
Peak Throughput:1                   Peak Throughput:1
Precedence:1                        Precedence:1
Mean Throughput:1                   Mean Throughtput:1
```

The following example shows output from the **show gprs umts-qos profile pdp tid** command for R99 QoS:

```
Requested QoS Profile               Negotiated QoS Profile
================                    =================
Allocation/Retention:1              Allocaion/Retention:1
Delay Class:2                       Delay Class:2
Reliability:1                       Reliability:1
Peak Throughput:1                   Peak Throughput:1
Precedence:1                        Precedence:1
Mean Throughput:1                   Mean Throughtput:1
```

```
Traffic Class:conversational
Delivery Order:2
Delivery of Err:2
Max SDU Size(bytes):1520
MBR for Uplink(kbps):20
MBR for Downlink(kbps):20
Residual BER:1
SDU Error Ratio:1*10^-2
Transfer Delay(ms):10
Handling Priority:1
GBR for Uplink(kbps):10
GBR for Downlink(kbps):5
Source Statistics Des:Speech
```

```
Traffic Class:conversational
Delivery Order:2
Delivery of Err:2
Max SDU Size(bytes):1520
MBR for Uplink(kbps):20
MBR for Downlink(kbps):20
Residual BER:1
SDU Error Ratio:1*10^-2
Transfer Delay(ms):10
Handling Priority:1
GBR for Uplink(kbps):10
GBR for Downlink(kbps):5
Source Statistics Des:Speech
```

show ip iscsi name

To display the name of an iSCSI initiator, use the **show ip iscsi name** command in privileged EXEC mode.

show ip iscsi name

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **show ip iscsi name** command to display the name of an iSCSI initiator.

Examples

The following example shows output from the **show ip iscsi session** command:

```
Router#show ip iscsi name
iSCSI initiator name: iqn.1987-07.com.cisco:wtbg-sup-09-3
Router#
```

Related Commands

Command	Description
show ip iscsi session	Displays information about the iSCSI sessions on the GGSN.
show ip iscsi target	Displays information about iSCSI targets.

show ip iscsi session

To display the status of iSCSI sessions on the GGSN, use the **show ip iscsi session** command in privileged EXEC mode.

show ip iscsi session [*session_id*] [**detail**]

Syntax Description

session_id	(Optional) Identification number of the session.
detail	(Optional) Displays detailed information about the iSCSI session.

Syntax Description

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **show ip iscsi session** command to display iSCSI sessions.

Examples

The following example shows output from the **show ip iscsi session** command:

```
Router#show ip iscsi session 12
ID TARGET STATE CONNECTIONS
------------------------------------------------------------
12 LINUX Logged In 1

Router#show ip iscsi session
ID TARGET STATE CONNECTIONS
------------------------------------------------------------
12 LINUX Logged In 1

Router#show ip iscsi session detail
ID: 12
Profile: LINUX
State: Logged In
Connections: 1
First Burst Length: 16384
Max Burst Length: 16384
Max Recv Data Segment: 32768
Max Xmit Data Segment: 8192
Initial R2T: Yes
Immediate data: Yes
Data PDU in order: Yes
Data PDU in order: Yes

Router#show ip iscsi session 12 detail
ID: 12
```

```
Profile: LINUX
State: Logged In
Connections: 1
First Burst Length: 16384
Max Burst Length: 16384
Max Recv Data Segment: 32768
Max Xmit Data Segment: 8192
Initial R2T: Yes
Immediate data: Yes
Data PDU in order: Yes
Data PDU in order: Yes

Router#
```

show ip iscsi stats

To display iSCSI statistics, use the **show ip iscsi stats** command in privileged EXEC mode.

show ip iscsi stats [**detail**]

Syntax Description

detail	(Optional) Displays detailed information about the iSCSI statistics.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **show ip iscsi stats** command to display iSCSI statistics.

Examples

The following example shows output from the **show ip iscsi stats** command:

```
Router#show ip iscsi stats
 iSCSI Stats:
  Login Requests - 2, Login Responses - 2
  Logout Requests - 0, Logout Responses - 0
  Login Timeouts - 0, Logout Timeouts - 0
  SCSI Commands - 27, SCSI Responses - 27
  Data In PDUs - 25, Data Out PDUs - 0
  Immed Data - 1, Unsolicited Data - 0
  NOP Ins - 35, NOP Outs - 35
  Async Requests - 0, Async Req Logout - 0
  Async Drop Conn - 0, Async Drop Conns - 0
  R2t Requests - 0, Rejects - 0

 System Stats:
  TX Queue Overflow - 0, RX Queue Overflow - 0
  Connection Resets - 0, Tasks aborted - 0

 SCSI Stats:
  Total Requests - 27
  Test Unit Ready Requests - 1, Test Unit Ready Failures - 0
  Report Luns Requests - 1, Report Luns Failures - 0
  Lun Inquiry Requests - 5, Lun Inquiry Failures - 0
  Read Capacity Requests - 5, Read Capacity Failures - 0
  Read Requests - 14, Read Failures - 0
  Write Requests - 1, Write Failures - 0
  Blocks Read- 49, Blocks Written - 8
```

```
Router#show ip iscsi stats detail
 iSCSI Stats:
  Login Requests - 2, Login Responses - 2
  Logout Requests - 0, Logout Responses - 0
  Login Timeouts - 0, Logout Timeouts - 0
  SCSI Commands - 27, SCSI Responses - 27
  Data In PDUs - 25, Data Out PDUs - 0
  Immed Data - 1, Unsolicited Data - 0
  NOP Ins - 36, NOP Outs - 36
  Async Requests - 0, Async Req Logout - 0
  Async Drop Conn - 0, Async Drop Conns - 0
  R2t Requests - 0, Rejects - 0

 System Stats:
  TX Queue Overflow - 0, RX Queue Overflow - 0
  Connection Resets - 0, Tasks aborted - 0

 SCSI Stats:
  Total Requests - 27
  Test Unit Ready Requests - 1, Test Unit Ready Failures - 0
  Report Luns Requests - 1, Report Luns Failures - 0
  Lun Inquiry Requests - 5, Lun Inquiry Failures - 0
  Read Capacity Requests - 5, Read Capacity Failures - 0
  Read Requests - 14, Read Failures - 0
  Write Requests - 1, Write Failures - 0
  Blocks Read- 49, Blocks Written - 8
```

Related Commands

Command	Description
clear ip iscsi stats	Clears iSCSI statistics.

show ip iscsi target

To display details about an iSCSI target, use the **show ip iscsi target** command in privileged EXEC mode.

show ip iscsi target

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **show ip iscsi target** command to display information about an iSCSI target.

Examples

The following example shows output from the **show ip iscsi target** command:

```
Router#show ip iscsi target
Target Profile= TARGET_LINUX IN_USE
  Target: name= iqn.2002-10.edu.unh.iol.iscsi.draft20-target:1
  Target: ip= 10.76.43.233, port= 3260, portal group= 0
  vrf= , sync read offset= 100, batch write= 100
  write interval= 5 sec, file size= 100 MB #
```

Related Commands

Command	Description
show ip iscsi session	Displays iSCSI sessions.
show ip iscsi stats	Display iSCSI statistics.

show policy-map apn

To display statistical and configuration information for all input and output policies attached to an APN, use the **show policy-map apn** command in privileged EXEC mode.

show policy-map apn *access-point-index*

Syntax Description

access-point-index	Integer (from 1 to 65535) that identifies an access point. Information about that access point is shown.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **show policy-map apn** command to display statistical and configuration information for all input and output policies attached to an APN.

Examples

This section provides sample outputs of the **show policy-map apn** command. The output you see might vary slightly from the ones shown below.

Example 1: Non Flow-Based Policing

The example provides sample output of the **show policy-map apn** command for non flow-based policing for access point 1, to which a service policy called "policy-non-flow" is attached (configured as shown below).

```
! Configures a class map with dscp based classification

class-map match-all class-dscp
 match ip dscp default

! Configures a policy with this class map

policy-map policy-nonflow
 class class-dscp
 police rate pdp
    conform-action transmit
    exceed-action set-dscp-transmit 15
```

```
    violate-action drop

! Attaches the policy to an APN

gprs access-point-list gprs
  access-point 1
    access-point-name static
    service-policy input policy-nonflow
    !

 GGSN#show policy-map apn 1
 APN 1

  Service-policy input:policy-nonflow

    Class-map:class-dscp (match-all)
      3 packets, 300 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match:ip dscp default
      police:
          rate 8000 bps, burst 1000 bytes
          peak-rate 10000 bps, peak-burst 1400 bytes
        conformed 3 packets, 300 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          set-dscp-transmit 15
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
     Class-map:class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match:any
```

With the above configuration, the **show gprs umts-qos police pdp-context tid** command does not display any information for the configuration is not per-PDP based.

```
GGSN#show gprs umts-qos police pdp-context tid 1203000000000010
No Policing Statistics Available
```

Example 2: Flow-Based Policing

The example provides sample output of the **show policy-map apn** command for flow-based policing for access point 1, to which a service policy called "policy-non-flow" is attached (configured as shown below).

```
! Configures a class map with flow based classification.

class-map match-all class-pdp
 match flow pdp
!
! Configures a policy-map and attch this class map into it.

policy-map policy-gprs
 class class-pdp
  police rate pdp
    conform-action set-dscp-transmit 15
    exceed-action set-dscp-transmit 15
    violate-action drop
!
```

Note With non flow-based policing, the police rate is not provided using the police rate command but is taken dynamically from the configure maximum and guaranteed bit rates.

```
! Attaches the policy-map to the apn.

gprs access-point-list gprs
  access-point 1
   access-point-name static
   service-policy input policy-gprs
   !

GGSN#show policy-map apn 1
 APN 1

  Service-policy input:policy-gprs

    Class-map:class-pdp (match-all)
      3 packets, 300 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match:flow pdp
      police:
          rate pdp, bc 1500 bytes
         peak-rate pdp, be 1800 bytes
        conformed 0 packets, 0 bytes; actions:
          set-dscp-transmit 15
        exceeded 0 packets, 0 bytes; actions:
          set-dscp-transmit 15
        violated 0 packets, 0 bytes; actions:
          drop

    Class-map:class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match:any
```

The **show policy-map** command displays the aggregated traffic count. To display the policing counters, issues the **show gprs umts-qos police pdp-context tid** command:

```
GGSN#show gprs umts-qos police pdp-context tid 1203000000000010
DOWNLINK POLICING STATISTICS
Flow id:1
      police:
          rate 5184000 , bc 1500 bytes
         peak-rate 7424000, be 1800 bytes
        conformed 2 packets, 200 bytes; actions:
          set-dscp-transmit 15
        exceeded 0 packets, 0 bytes; actions:
          set-dscp-transmit 15
        violated 0 packets, 0 bytes; actions:
          drop
```

Example 3: Flow and DSCP-Based Policing

In the following example, a policy map is created with both flow-based and DSCP-based classication. In this configuration, per-PDP policing occurs when both conditions are met. For example, if a packet is received by the GGSN for a PDP with a different DSCP value than the one configured in the class-map, policing does not occur.

```
! Configures a class map with match flow + DSCP based classification.
!
class-map match-all class-flow-dscp
 match ip dscp default
 match flow pdp
!
! Configure a policy-map with this class map
!
policy-map policy-flow-dscp
 class class-flow-dscp
  police rate pdp
    conform-action transmit
    exceed-action set-dscp-transmit 15
    violate-action drop

! Attaches the policy to an apn.

gprs access-point-list gprs
  access-point 1
   access-point-name static
   service-policy input policy-flow-dscp
   !
```

Note Data with DSCP value 0 has been processed.

```
GGSN#show policy-map apn 1
 APN 1

  Service-policy input:policy-flow-dscp

    Class-map:class-flow-dscp (match-all)
      4 packets, 456 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match:ip dscp default
      Match:flow pdp
      police:
          rate pdp, bc 1500 bytes
       peak-rate pdp, be 1800 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          set-dscp-transmit 15
        violated 0 packets, 0 bytes; actions:
          drop

    Class-map:class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match:any
```

```
GGSN#show gprs umts-qos police pdp-context tid 1203000000000010
DOWNLINK POLICING STATISTICS
Flow id:1
      police:
          rate 5184000 , bc 1500 bytes
         peak-rate 7424000, be 1800 bytes
        conformed 3 packets, 342 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          set-dscp-transmit 15
        violated 0 packets, 0 bytes; actions:
          drop
```

A packet with a different DSCP value does not get policed.

Related Commands

Command	Description
match flow	Specifies PDP flows as the match criterion in a class map.
police rate	Configures traffic policing using the police rate.
service-policy	Attaches a service policy to an APN, to be used as the service policy for PDP flows of that APN.
show gprs umts-qos police pdp-context tid	Displays policing statistics for a PDP context.

show record-storage-module stats

To display current record storage module (RSM) statistics, use the **show record-storage-module stats** command in privileged EXEC mode.

show record-storage-module stats

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **show record-storage-module stats** command to display RSM statistics.

Examples

The following example shows output from the **show record-storage-module stats** command:

```
Router#show record-storage-module stats
RSM Appl Stats:
 requests:
  open= 1, read= 0, write= 0
  ping= 0, close= 0
 request fail:
  open= 0, read= 0, write= 0
  ping= 0, close= 0 | ta
 alloc fail:
  appl info= 0, appl msg= 0, appl req= 0,
  data buffer= 0, drive= 0
 RSM Clear:
    Statistics = 1

Router#
```

Related Commands

Command	Description
clear record-storage-module stats	Clears current RSM-related statistics.

show record-storage-module target-info

To display the number of record storage module (RSM) disks available their current status, use the **show record-storage-module target-info** command in privileged EXEC mode.

show record-storage-module target-info [all | target-profile *profile_name***] [detail]**

Syntax Description

all	Displays statistics for all targets for which there are profiles.
target-profile *profile_name*	Displays statistics for a specific profile.
detail	Displays detailed information about the RSM drives.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **show record-storage-module target-info** command to display RSM statistics by profile.

Examples

The following example shows output from the **show record-storage-module target-info** command:

```
Router#show record-storage-module target-info all detail
  Target profile = TARGET_LINUX
  Application name = GGSN, Target State = Active, Disk = Usable
  Application id = 2, iSCSI handle = 2
  Number of drives = 5, Read drive = sda3, Write drive = sda3
  Active drives:
   Drive = sda3
   File system id = 19
   Descriptors: read = -1, write = -1, master = -1
   Current File: bytes written = 0, bytes read = 0
   Master file in memory:
   Drive full = No
   Write: dir = 1, file = 1
   Read: dir = 1, file = 1, offset = 62675
   Salvage file = 0, CRC = 0x91C816C0
  Failed drives:
   Drive = sda0
   Reason = Unexpected IFS error (Invalid DOS media or no media in slot)
   Drive = sda1
   Reason = Unexpected IFS error (Invalid DOS media or no media in slot)
   Drive = sda2
   Reason = Unexpected IFS error (Invalid DOS media or no media in slot)
   Drive = sda4
   Reason = Unexpected IFS error (Invalid DOS media or no media in slot)
```

show tech-support

To display GPRS/UMTS protocol-specific information about the router when reporting a problem, use the **show tech-support** command in privileged EXEC mode and specify the **ggsn** keyword option.

show tech-support [**ggsn**]

Syntax Description

ggsn	(Optional) Displays show command output specific to GPRS/UMTS.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU and the **ggsn** keyword option was added.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The output of **show tech-support ggsn** includes the ggsn-specific output displayed by the following commands:

- **show gprs charging parameters**
- **show gprs charging statistics**
- **show gprs charging status all**
- **show gprs gtp parameters**
- **show gprs gtp statistics**
- **show gprs gtp status**
- **show gprs memory threshold statistics**
- **show gprs qos status**
- **show running-config**
- **show version**

Examples

The following example shows the output of the **show tech-support ggsn** command:

```
GGSN#  show tech-support ggsn

------------------ show version ------------------

Cisco IOS Software, 7200 Software (C7200-G8IS-M), Experimental Version
12.3(20040128:223808) [r50 104]
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Sun 01-Feb-04 05:22 by user

ROM: System Bootstrap, Version 12.2(4r)B2, RELEASE SOFTWARE (fc2)
BOOTLDR: 7200 Software (C7200-KBOOT-M), Version 12.1(8a)E, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)

ggsn uptime is 1 day, 21 hours, 4 minutes
System returned to ROM by reload at 19:48:49 EST Fri Jan 30 2004
System image file is "tftp://9.1.0.1/gota/c7200-g8is-mz"
Last reload reason: Reload command

Cisco 7206VXR (NPE400) processor (revision A) with 491520K/32768K bytes of memory.
Processor board ID 29550562
R7000 CPU at 350MHz, Implementation 39, Rev 3.3, 256KB L2, 4096KB L3 Cache
6 slot VXR midplane, Version 2.7

Last reset from s/w nmi

PCI bus mb0_mb1 has 600 bandwidth points
PCI bus mb2 has 40 bandwidth points

4 Ethernet interfaces
3 FastEthernet interfaces
125K bytes of NVRAM.

46976K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
8192K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x0

------------------ show running-config ------------------

Building configuration...

Current configuration : 6770 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service udp-small-servers
service tcp-small-servers
service gprs ggsn
!
hostname ggsn
!
boot-start-marker
boot-end-marker
!
logging queue-limit 100
no logging buffered
enable secret 5 <removed>
enable password <removed>
!
clock timezone EST -4
```

```
aaa new-model
!
aaa group server radius mwg
!
aaa group server radius list1
 server 10.76.82.75 auth-port 1645 acct-port 1646
!
aaa authentication ppp default local
aaa authentication ppp list1 local
aaa authorization network default local
aaa authorization network list1 local
aaa authorization configuration list1 group radius
aaa accounting update periodic 10
aaa accounting network default start-stop group radius
aaa accounting network list1 start-stop group radius
aaa session-id common
ip subnet-zero
!
ip cef
no ip domain lookup
ip host PAGENT-SECURITY-V3 39.26.7.9 17.99.0.0
!
ip dhcp pool TEST
   network 100.0.0.0 255.0.0.0
!
ip vrf vpn1
 rd 100:1
!
ip address-pool dhcp-proxy-client
vpdn enable
!
ipv6 unicast-routing
!
interface Tunnel0
 description to handle vrf traffic from APN1 on GGSN MWAM 1
 ip unnumbered Loopback3
 tunnel source Loopback3
 tunnel destination 20.20.120.20
!
interface Tunnel1
 no ip address
 shutdown
 tunnel source 17.1.101.1
 tunnel destination 13.1.101.1
!
interface Tunnel2
 no ip address
 shutdown
 tunnel source 17.1.102.1
 tunnel destination 13.1.102.1
!
interface Loopback0
 ip address 100.0.0.1 255.255.255.255
 no ip route-cache
 no ip mroute-cache
 shutdown
!
interface Loopback1
 ip address 33.44.55.66 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 shutdown
!
interface Loopback2
```

```
 ip address 35.0.0.1 255.0.0.0
 no ip route-cache
 no ip mroute-cache
 shutdown
!
interface Loopback3
 description interface for ggsn mwam 1
 ip address 20.20.120.21 255.255.255.255
 no ip route-cache
 no ip mroute-cache
 shutdown
!
interface FastEthernet0/0
 ip address 9.3.66.3 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
 no cdp enable
!
interface FastEthernet0/1
 ip address 20.20.51.31 255.255.255.0
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 1.1.1.1 255.255.255.0
 shutdown
 duplex half
!
interface Ethernet2/0
 ip address 10.3.12.1 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet2/1
 ip address 11.3.12.1 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet2/2
 ip address 12.3.12.1 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet2/3
 ip address 10.10.10.2 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Virtual-Template1
```

```
 ip address 72.72.72.1 255.255.0.0
 encapsulation gtp
 gprs access-point-list 1
!
interface Virtual-Template2
 ip unnumbered Loopback0
 no peer default ip address
!
interface Virtual-Template3
 description VT for PPP and PPP L2TP
 ip unnumbered Loopback1
 peer default ip address pool mypool
 no keepalive
!
ip local pool pdsn-pool 6.6.10.1 6.6.10.255
ip local pool pdsn-pool 6.6.11.1 6.6.26.255
ip local pool pdsn-pool 6.6.27.1 6.6.42.255
ip local pool pdsn-pool 6.6.43.1 6.6.58.255
ip local pool pdsn-pool 6.6.59.1 6.6.64.255
ip local pool pdsn-pool 6.6.65.1 6.6.80.255
ip local pool pdsn-pool 55.55.10.1 55.55.25.253
ip local pool ha-pool 24.24.1.1 24.24.16.255
ip local pool mypool 85.0.0.0 85.0.0.255
ip local pool mypool 85.1.0.0 85.1.255.255
ip local pool mypool 85.2.0.0 85.2.255.255
ip local pool mypool 85.3.0.0 85.3.255.255
ip local pool pooltest 180.180.1.1 180.180.1.10
ip default-gateway 9.15.0.1
ip classless
ip route 7.7.7.1 255.255.255.255 Ethernet2/3
ip route 9.1.0.1 255.255.255.255 9.3.0.1
ip route 9.100.0.1 255.255.255.255 9.15.0.1
ip route 20.20.120.20 255.255.255.255 FastEthernet0/1
no ip http server
!
access-list 112 deny   tcp any any
access-list 120 permit ip any host 10.1.102.1
access-list 150 permit icmp any 60.0.0.0 0.0.0.255
access-list 150 permit icmp 60.0.0.0 0.0.0.255 any
dialer-list 1 protocol ip permit
ipv6 router rip TEST2
  poison-reverse
!
gprs maximum-pdp-context-allowed 45000
gprs qos map umts
gprs access-point-list 1
  access-point 1
   access-point-name gprs.cisco.com
   aaa-group authentication list1
   aggregate 1.1.0.0 255.255.0.0
   access-violation deactivate-pdp-context
   !
  access-point 2
   access-point-name ppp.com
   ppp-regeneration
   !
  !
!
gprs gtp path-echo-interval 0
gprs gtp ip udp ignore checksum
gprs gtp ppp vtemplate 3
gprs gtp ppp-regeneration vtemplate 2
gprs default ip-address-pool radius-client
gprs default charging-gateway 12.3.11.1  13.3.11.1
```

```
gprs default map-converting-gsn 10.3.11.1
!
gprs charging server-switch-timer 0
gprs charging cdr-aggregation-limit 1
!
radius-server host 10.76.82.75 auth-port 1645 acct-port 1646
radius-server key <removed>
!
control-plane
!
mgcp modem passthrough voip mode ca
no mgcp timer receive-rtcp
!
dial-peer cor custom
!
!
gatekeeper
 shutdown
!
alias exec pdp sh gprs gtp pdp all
alias exec pdptid show gprs gtp pdp tid
alias exec pdptid1 show gprs gtp pdp tid  1111111111111111
alias exec pdptid2 show gprs gtp pdp tid 2222222222222222
alias exec pdpclear clear gprs gtp pdp all
!
line con 0
 exec-timeout 0 0
 password <removed>
 logging synchronous
 login authentication console
 transport preferred all
 transport output all
 stopbits 1
line aux 0
 transport preferred all
 transport output all
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password <removed>
 transport preferred all
 transport input all
 transport output all
line vty 5 15
 transport preferred all
 transport input all
 transport output all
!
no scheduler max-task-time
!
end

------------------ show gprs gtp status ------------------

GPRS GTP Status:
  activated gtpv0 pdp     0
  activated gtpv1 pdp     0
  activated ms            0
  network init pdp        0
  activated ppp regen pdp 0
  activated ppp pdp       0
  gtp's ppp va hwidbs     0

------------------ show gprs gtp parameters ------------------
```

```
    GTP path echo interval                          = 0
    GTP signal max wait time T3_response            = 1
    GTP max retry N3_request                        = 5
    GTP dynamic echo-timer minimum                  = 5
    GTP dynamic echo-timer smooth factor            = 2
    GTP buffer size for receiving N3_buffer         = 8192
    GTP max pdp context                             = 45000

------------------ show gprs gtp statistics ------------------

GGSN# show gprs gtp statistics
GPRS GTP Statistics:
 version_not_support        0           msg_too_short              0
 unknown_msg                0           unexpected_sig_msg         0
 unexpected_data_msg        0           unsupported_comp_exthdr    0
 mandatory_ie_missing       0           mandatory_ie_incorrect     0
 optional_ie_invalid        0           ie_unknown                 0
 ie_out_of_order            0           ie_unexpected              0
 ie_duplicated              0           optional_ie_incorrect      0
 pdp_activation_rejected    2           tft_semantic_error         0
 tft_syntactic_error        0           pkt_ftr_semantic_error     0
 pkt_ftr_syntactic_error    0           non_existent               0
 path_failure               0           total_dropped              0
 signalling_msg_dropped     0           data_msg_dropped           0
 no_resource                0           get_pak_buffer_failure     0
 rcv_signalling_msg         7           snd_signalling_msg         7
 rcv_pdu_msg                0           snd_pdu_msg                0
 rcv_pdu_bytes              0           snd_pdu_bytes              0
 total created_pdp          3           total deleted_pdp          2
 total created_ppp_pdp      0           total deleted_ppp_pdp      0
 ppp_regen_pending          0           ppp_regen_pending_peak     0
 ppp_regen_total_drop       0           ppp_regen_no_resource      0
 ntwk_init_pdp_act_rej      0           total ntwkInit created pdp 0

GPRS Network behind mobile Statistics:
  network_behind_ms APNs      1          total_download_route       5
  save_download_route_fail    0          insert_download_route_fail 2
  total_insert_download_route 3

------------------ show gprs charging status all ------------------

        GPRS Charging Protocol Status
        =================================

* Number of APNs :                              <0>
* Number of CDRs :                              <0>
* Number of closed CDRs buffered:               <0>
* Number of Containers buffered:                <0>
* Number of pending unack. CDR_Output_Msgs:     <0>

------------------ show gprs charging parameters ------------------

        GPRS Charging Protocol Parameters
        =================================

* Default Charging Gateway Address:        <12.3.11.1>
* Default Backup Charging Gateway Address: <13.3.11.1>
* Default Tertiary Charging Gateway Address: UNDEFINED.
* Current Active Charging Gateway Address: <12.3.11.1>
* Current Backup Charging Gateway Address: <13.3.11.1>
* Charging Server Switch-Over Timer:       <0> seconds.
* Charging Path Protocol:                  udp
* GTP' use short header:                   DISABLED
```

```
* Charging Message Options:
   Transfer Request:
 - Packet Transfer Command IE:             DISABLED.
   Transfer Response:
 - Number Responded:                       DISABLED.
* Charging MAP DATA TOS:                   <3>
* Charging Transfer Interval:              <105> seconds.
* Charging Transfer Threshold:             <1048576> bytes.
* Charging CDR Aggregation Limit:          <1> CDRs per msg.
* Charging Packet Queue Size:              <128> messages.
* Charging Gateway Path Request Timer:     <0> Minutes.
* Charging Change Condition Limit:         <5>
* Charging SGSN Limit:                     DISABLED.
* Charging Time Limit:                     <0>
* Charging Send Buffer Size:               <1460>
* Charging Port Number:                    <3386>
* Charging Roamers CDR Only:               DISABLED.
* Charging CDR Option:
 - Local Record Sequence Number:           DISABLED.
 - APN Selection Mode:                     DISABLED.
 - ChCh Selection Mode:                    DISABLED.
 - IMS Signaling Context:                  DISABLED.
 - External Charging ID:                   DISABLED.
 - SGSN PLMN ID:                           DISABLED.
 - Dynamic Address:                        ENABLED.
 - Served PDP Address:                     ENABLED.
 - PDP Type:                               ENABLED.
 - Access Point Name:                      ENABLED.
 - Network Initiated PDP:                  ENABLED.
 - No Partial CDR Generation:              DISABLED.
 - Node ID:                                DISABLED.
 - Packet Count:                           DISABLED.
 - Served MSISDN:                          DISABLED.
 - Private Echo:                           DISABLED.
* Charging release:                        99
* Charging Tariff Time Changes:
- NO Tariff Time Changes
* Charging Service Mode:                   OPERATIONAL

------------------ show gprs charging statistics ------------------

        GPRS Charging Protocol Statistics
        =================================

* Total Number of CDRs for Charging:              <0>
* Total Number of Containers for Charging:        <0>
* Total Number of CDR_Output_Msgs sent:           <0>

-- Charging Gateway Statistics --
* Charging Gateway Down Count:                    <0>
```

```
------------------ show gprs qos status ------------------

GPRS QoS Status:
  type: UMTS
  conversational_pdp         0  streaming_pdp     0
  interactive_pdp            0  background_pdp    0

------------------ show gprs memory threshold statistics --

Memory Threshold Statistics
================================================
GGSN memory threshold status :NOT IN THRESHOLD

Number of times reached :       0
Number of PDPs rejected :       0
Number of PDPs dropped due to
          duration limit :      0
          volume limit :        0
          update request :      0

Time when last memory threshold was reached :NEVER
```

source interface

To configure the interface to use to connect to a Diameter peer, use the **source interface** command in Diameter peer configuration mode. To remove the interface configuration, use the **no** form of this command

source interface *interface_name*

no source interface

Syntax Description

interface_name	Name of the interface that the GGSN will use to communicate a Diameter peer.

Defaults

No default behavior or values.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **source interface** command to specify the interface to use for a Diameter peer-to-peer connection. The DCCA client process on the GGSN will use this source address and port to initiate the TCP connection to the peer.

Examples

The following configuration example fastEthernet0 as the source interface to use for the peer-to-peer connection:

```
Diameter peer dcca1
 address ipv4 10.10.10.1
 transport tcp port 4000
 security ipsec
 source interface fastEthernet0
```

Related Commands .

Command	Description
address ipv4	Configures the IP address of the Diameter peer host.
destination host	Configures the Fully Qualified Domain Name (FQDN) of the Diameter peer
destination realm	Configures the destination realm (domain name) in which the Diameter host is located.
diameter peer	Defines the Diameter peer (server) and enters diameter peer configuration mode.

Command	Description
ip vrf forwarding	Defines the VRF associated with the Diameter peer.
security	Configures the security protocol to use for the Diameter peer-to-peer connection.
timer	Configures Diameter base protocol timers for peer-to-peer communication.
transport	Configures the transport protocol to use to connect with the Diameter peer.

subscription-required

To specify that the gateway GPRS support node (GGSN) checks the value of the selection mode in a PDP context request to determine if a subscription is required to access a PDN through a particular access point, use the **subscription-required** command in access-point configuration mode. To specify that no subscription is required, use the **no** form of this command.

subscription-required

no subscription-required

Syntax Description

This command has no arguments or keywords.

Defaults

No subscription is required

Command Modes

Access-point configuration.

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **subscription-required** command to specify that the GGSN checks the value of the selection mode in a PDP context request to determine if a subscription is required for user access to PDNs through the current access point. When you configure the **subscription-required** command at the APN, the GGSN looks for the "subscription verified" selection mode in the PDP context request to establish the session. If the GGSN finds that the selection mode is designated as subscription not verified in the PDP context request, then the GGSN rejects the PDP context request.

The subscription must be set up by the service provider, and subscription information must be passed with the mobile user's PDP context requests.

Examples

The following example specifies that the GGSN checks for subscription verification in the selection mode before establishing a session at the access-point:

```
access-point 1
 access-point-name gprs.somewhere.com
 dhcp-server 10.100.0.3
 dhcp-gateway-address 10.88.0.1
 subscription-required
 exit
```

t3-response

To specify the initial time that the quota server waits before resending a signaling request message when a response to a request has not been received, use the **t3-response** command in quota server configuration mode. To return to the default value, use the **no** form of this command

t3-response *response-interval*

no t3-response

Syntax Description

response-interval	Value between 1 and 65535 that specifies the length of the T3 response interval, in seconds.

Defaults

1 second.

Command Modes

Quota server configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

The **t3-response** command is used by the GGSN to process delete PDP context requests and to perform the default method of echo timing.

For delete PDP context requests, the **t3-response** command is used to specify how long the quota server waits before sending a retry of the delete PDP context request when a response is not received from the CSG, until the n3-requests limit is reached.

Examples

The following example configures a T3 interval response interval of 524 seconds:

```
ggsn quota-server qs1
 interface loopback1
 echo-interval 90
 n3-requests 3
 t3-response 524
```

Related Commands .

Command	Description
clear ggsn quota-server statistics	Clears the quota server-related statistics displayed using the **show ggsn quota-server statistics** command.
csg-group	Associates the quota server to a CSG group that is to be used for quota server-to-CSG communication.

Command	Description
echo-interval	Specifies the number of seconds that the quota server waits before sending an echo-request message to the CSG.
ggsn quota-server	Configures the quota server process that interfaces with the CSG for enhanced service-aware billing.
interface	Specifies the logical interface, by name, that the quota server will use to communicate with the CSG.
n3-requests	Specifies the maximum number of times that the quota server attempts to send a signaling request to the CSG.
show ggsn quota-server	Displays quota server parameters or statistics about the message and error counts.

tariff-time

To specify that a charging profile use the tariff changes configured using the **gprs charging tariff-time** global configuration command, use the **tariff-time** command in charging profile configuration mode. To return to the default value, use the **no** form of this command.

tariff-time

no tariff-time

Syntax Description

This command has no arguments or keywords.

Defaults

No tariff-time changes

Command Modes

Charging profile configuration.

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **tariff-time** charging profile configuration command to specify that the time configured for tariff changes on the GGSN (using the **gprs charging tariff-time** global configuration command) apply to a charging profile created using the **gprs charging profile** global configuration or **charging profile** access-point configuration commands.

Examples

The following example specifies that tariff-changes apply to a charging profile:

```
charging profile 10
 tarrif-time
 exit
```

Related Commands..

Command	Description
category	Identifies the subscriber category to which a charging profile applies.s
cdr suppression	Specifies that CDRs be suppressed as a charging characteristic in a charging profile.
charging profile	Associates a default charging profile to an access point.
content dcca profile	Defines a DCCA client profile in a GGSN charging profile.

Command	Description
content postpaid time	Specifies as a trigger condition for postpaid users in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
content postpaid validity	Specifies as a trigger condition in a charging profile, the amount of time quota granted to a postpaid user is valid.
content postpaid volume	Specifies as a trigger condition for postpaid users in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.
content rulebase	Associates a default rule-base ID with a charging profile.
description	Specifies the name or a brief description of a charging profile.
gprs charging characteristics reject	Specifies that Create PDP Context requests for which no charging profile can be selected be rejected by the GGSN.
gprs charging container time-trigger	Specifies a global time limit, that when exceeded by a PDP context causes the GGSN to close and update the G-CDR for that particular PDP context.
gprs charging profile	Creates a new charging profile (or modifies an existing one), and enters charging profile configuration mode.
limit duration	Specifies as a trigger condition in a charging profile, the time duration limit that when exceeded causes the GGSN to collect upstream and downstream traffic byte counts and close and update the G-CDR for a particular PDP context.
limit sgsn-change	Specifies as a trigger condition in a charging profile, the maximum number of SGSN changes that can occur before closing and updating the G-CDR for a particular PDP context.
limit volume	Specifies as a trigger condition in a charging profile, the maximum number of bytes that the GGSN maintains across all containers for a particular PDP context before closing and updating the G-CDR.

timer

To configure Diameter base protocol timers for peer-to-peer communication, use the **timer** command in Diameter peer configuration mode. To remove the timer configurations, use the **no** form of this command

timer {connection | transaction | watchdog} *seconds*

no timer {connection | transaction | watchdog}

Syntax Description

connection	Sets the maximum amount of time the GGSN attempts to reconnect to a Diameter peer after a connection to the peer has been brought down due to a transport failure. A value of 0 configures the GGSN to not try to reconnect.
transaction	Sets the maximum amount of time the GGSN waits for a Diameter peer to respond before trying another peer.
watchdog	Sets the maximum amount of time the GGSN waits for a Diameter peer to respond to a watchdog packet. When the watchdog timer expires, a DWR is sent to the Diameter peer and the watchdog timer is reset. If a DWA is not received before the next expiration of the watchdog timer, a transport failure to the Diameter peer has occurred.
seconds	Maximum amount of time, in seconds, of the timer. Valid range, in seconds, is 1 to 1000.

Defaults

30 seconds.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **timer** Diameter peer configuration command to configure Diameter base timers for a Diameter node.

When configuring timers, note that the value for the transaction timer, should be larger than the TX-timeout value, and, on the SGSN, the values configured for the number GTP N3 requests and T3 retransmissions must be larger than the sum of all possible server timers (RADIUS, DCCA, and CSG). Specifically, the SGSN N3*T3 must be greater than 2 x RADIUS timeout + *N* x DCCA timeout + CSG timeout where:

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

Examples

The following example configures the frequency of connection attempts with a Diameter peer to 120 seconds.

```
Diameter peer dcca1
 address ipv4 10.10.10.1
 transport tcp port 4000
 security ipsec
 source interface fastEthernet0
 timer connection 120
```

Related Commands .

Command	Description
address ipv4	Configures the IP address of the Diameter peer host.
destination host	Configures the Fully Qualified Domain Name (FQDN) of the Diameter peer
destination realm	Configures the destination realm (domain name) in which the Diameter host is located.
diameter peer	Defines the Diameter peer (server) and enters diameter peer configuration mode.
ip vrf forwarding	Defines the VRF associated with the Diameter peer.
security	Configures the security protocol to use for the Diameter peer-to-peer connection.
source interface	Configures the interface to use to connect to the Diameter peer.
transport	Configures the transport protocol to use to connect with the Diameter peer.

traffic-class

To allocate bandwidth from a bandwidth pool to a specific traffic class, use the **traffic-class** command in bandwidth pool configuration mode. To return to the default value, use the **no** form of this command.

traffic-class *traffic-class-name* **[percent]** *value*

no traffic-class *traffic-class-name* **[percent]** *value*

Syntax Description

traffic-class-name	Specifies the traffic class for which you are allocating bandwidth. Valid values are conversational, streaming, interactive, or background.
percent	(Optional) Specifies that the bandwidth be allocated as a percentage rather than absolute value.
value	Specifies the bandwith in either a percentage (1 to 100% when used with the optional **percent** keyword), or absolute value in kilobits per second (0 to 4292967295). Note that the same unit (percentage or absolute value) must be used for all traffic classes.

Defaults

No bandwidth reservation is configured for any of the traffic classes, therefore, all PDPs are accepted.

Command Modes

Bandwidth pool configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **traffic-class** bandwidth pool configuration command to allocate bandwidth to a specific traffic class.

Note Before allocating the bandwidth in a bandwidth pool to a specific traffic class, the pool must be created using the **gprs qos bandwidth-pool** global configuration command.

The bandwidth can be allocated as a percentage or absolute value, however, the bandwidth unit must be consistent for all traffic classes (percentage and absolute value cannot be mixed within the same bandwidth pool).

If a traffic class is configured with 0 (absolute value) as the allocated bandwidth, the total bandwidth available for that traffic class is 0 kbps. Therefore, if a Create PDP Context request with that traffic class is received, it is rejected by the GGSN.

Note Bandwidth reservation can be configured for real-time (conversational and streaming) and non real-time (interactive and background) class PDPs, however, bandwidth checking is performed only for real-time PDP contexts. All Create PDP Context requests for non real-time PDPs are allowed.

Examples

The following example reserves 15% of the total available bandwidth to the Background class of PDPs:

```
traffic-class background percent 15%
```

Related Commands

Command	Description
bandwidth	Defines the total bandwidth, in kilobits per second, for a bandwidth pool. Valid values are 1 to 4292967295.
bandwidth-pool	Applies a bandwidth pool to an APN.
gprs qos bandwidth-pool	Creates or modifies a bandwidth pool.
traffic-class	Allocates bandwidth pool bandwidth to a specific traffic class.

transport

To configure the transport protocol to use to connect with a Diameter peer, use the **transport** command in Diameter peer configuration mode. To remove the configuration, use the **no** form of this command

transport {tcp | sctp} port *port-number*

no transport

Syntax Description

tcp	Defines TCP as the transport protocol to use to connect to the Diameter peer.
sctp	Defines SCTP as the transport protocol to use to connect to the Diameter peer. **Note** SCTP is not supported as the transport protocol in GGSN Release 5.2.
port *port-number*	Port on the Diameter peer to use for peer-to-peer connection. The default is 3868.

Defaults

No default behavior or values.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **transport** command to define the protocol to use to connect to a Diameter peer.

When the **no** form of this command is issued, all session that are bound to the peer cannot use the connection any longer. If there are any pending messages in the connection queue, the applications that sent the messages will be notified so that they can try alternate peers.

Examples

The following configuration example configures TCP as the transport protocol between Diameter peers and port 4000 as the port to use for peer-to-peer communication:

```
Diameter peer dcca1
 address ipv4 10.10.10.1
 transport tcp port 4000
```

Related Commands .

Command	Description
address ipv4	Configures the IP address of the Diameter peer host.
destination host	Configures the Fully Qualified Domain Name (FQDN) of the Diameter peer

Command	Description
destination realm	Configures the destination realm (domain name) in which the Diameter host is located.
diameter peer	Defines the Diameter peer (server) and enters diameter peer configuration mode.
ip vrf forwarding	Defines the VRF associated with the Diameter peer.
security	Configures the security protocol to use for the Diameter peer-to-peer connection.
source interface	Configures the interface to use to connect to the Diameter peer.
timer	Configures Diameter base protocol timers for peer-to-peer communication.

trigger

To configure a condition that, when it occurs, triggers a DCCA client to request quota-reauthorization for a service-aware prepaid PDP context, use the **trigger** command in DCCA profile configuration mode. To remove the configuration, use the **no** form of this command.

trigger {sgsn-change | qos-change | rat | plmn-id}

no trigger {sgsn-change | qos-change | rat | plmn-id}

Syntax Description

sgsn-change	Configures the DCCA client to request quota-reauthorization if SGSN changes occur.
qos-change	Configures the DCCA client to request quota-reauthorization if a QoS changes should occur.
rat	Configures a radio access technology (RAT) change change to trigger a quota-reauthorization request. The RAT indicates whether the SGSN serves the user equipment (UE) UMTS or GSM/EDGE RAN (GERAN).
plmn-id	Configures a public land mobile network (PLMN) ID change change to trigger a quota-reauthorization request.

Defaults

No default behavior or values.

Command Modes

DCCA profile configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.
12.4(9)XG	This command was integrated into Cisco IOS Release 12.4(9)XG and the **rat** and **plmn-id** keyword options were added.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.

Usage Guidelines

Use the **trigger** command to configure changes that trigger the GGSN to request quota reauthorization for service-aware prepaid PDP contexts.

Modifying this command will not affect existing PDP contexts using a DCCA client.

Note This command is not supported by a vendor-specific DCCA client.

Examples

The following configuration example configures serveral conditions in a DCCA profile, “dcca-profile1” for prepaid PDP contexts, that when the condition occurs, triggers quota reauthorization:

```
gprs dcca profile dcca-profile1
  tx-timeout 100
  ccfh continue
  authorization dcca-net
  destination-realm cisco.com
  trigger sgsn-change
  trigger qos-change
  trigger rat-change
  trigger plmn-change
```

Related Commands .

Command	Description
authorization	Defines a method of authorization (AAA method list), in the DCCA client profile, that specifies the Diameter server groups.
ccfh	Configures the Credit Control Failure Handling (CCFH) AVP locally to use for a credit-control session when the Credit Control Answer (CCA) sent by the DCCA server does not contain CCFH value.
content dcca profile	Defines the DCCA client profile in a GGSN charging profile.
destination-realm	Configures the destination realm to be sent in CCR initial requests to a DCCA server.
gprs dcca profile	Defines a DCCA client profile on the GGSN and enters DCCA client profile configuration mode.
session-failover	Configures Credit Control Session Failover (CCSF) AVP support when a credit control answer (CCA) message from the DCCA server does not contain a value for the CCSF AVP.
tx-timeout	Configures a TX timeout value used by the DCCA client to monitor the communication of Credit Control Requests (CCRs) with a Diameter server.

tx-timeout

To configure a TX timeout value used by the DCCA client to monitor the communication of Credit Control Requests (CCRs) with a Diameter server, use the **tx-timeout** command in DCCA client profile configuration mode. To return to the default values, use the **no** form of this command

tx-timeout *value*

no tx-timeout

Syntax Description

value	Amount of time, in seconds, a CRR can wait for a response from the Diameter sever before the DCCA client takes action. Valid range is 0 to 1000 seconds.

Defaults

10 seconds.

Command Modes

DCCA client profile configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Typically, the Diameter base detects transport failures that occur with a Diameter server. For prepaid services, the time it takes for a response from the network is crucial, therefore the DCCA client can be configured to react faster than the Diameter base if necessary.

The Tx timer is used by the DCCA client to supervise the communication with the Diameter server. The timer is started with each initial and updated CCR. If the time configured for the timer elapses, the DCCA client takes an action on the PDP context depending on the current value of the Credit Control Fault Handling (CCFH) AVP for the credit control (CC) session.

When a response to all pending CCRs is received, the Tx timer is stopped.

Examples

The following configuration example sets the Tx time for a DCCA client to 25 seconds:

```
gprs dcca profile dcca-profile1
  authorization dcca-method
  tx-timeout 25
```

Related Commands

Command	Description
authorization	Defines a method of authorization (AAA method list), in the DCCA client profile, that specifies the Diameter server groups.
ccfh	Configures the Credit Control Failure Handling (CCFH) AVP locally to use for a credit-control session when the Credit Control Answer (CCA) sent by the DCCA server does not contain CCFH value.
content dcca profile	Defines the DCCA client profile in a GGSN charging profile.
gprs dcca profile	Defines a DCCA client profile on the GGSN and enters DCCA client profile configuration mode.
session-failover	Configures Credit Control Session Failover (CCSF) AVP support when a credit control answer (CCA) message from the DCCA server does not contain a value for the CCSF AVP

virtual-address

To configure a virtual IP address to which a quota server sends all CSG requests, use the **virtual-address** command in CSG group configuration mode. To deconfigure the virtual IP address, use the **no** form of this command

virtual-address *ip-address*

no virtual-address *ip-address*

Syntax Description

ip-address	Virtual IP address of the CSG group.

Defaults

No default behavior or values.

Command Modes

CSG group configuration

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **virtual-address** to configure the virtual IP address of a CSG group.

The virtual IP address is the address to which the quota server will send all requests, and is required before a path between the quota server and the CSG can come up.

Caution Issuing the **no** form of this command will bring down a quota server-to-CSG path if is up.

Examples

The following configuration example configures CSG group csg1 to use the virtual IP address 5.5.5.14:

```
ggsn csg-group csg1
  virtual-address 5.5.5.14
  port 4444
  real-address 5.1.1.1
  real-address 5.1.1.2
```

Related Commands

Command	Description
ggsn csg-group	Configures a CSG group on the GGSN for quota server-to-CSG communication.
port	Configures the port number on which the CSG listens for quota server traffic.

Command	Description
real-address	Configures the IP address of a real CSG for source checking on inbound messages from a CSG.
show ggsn csg	Displays the parameters used by the CSG group or the number of path and quota management messages sent and received by the quota server.

vrf

To configure VPN routing and forwarding (VRF) at a gateway GPRS support node (GGSN) access point and associate an access point with a particular VRF instance, use the **vrf** command in access-point configuration mode.

vrf *vrf-name*

Syntax Description

vrf-name	Name of the corresponding VRF instance with which the access point is associated.

Defaults

No default behavior or values.

Command Modes

Access-point configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **vrf** command to configure VRF at a GGSN access point and associate an access point with a particular VRF instance.

Note With GGSN Release 5.0 and later, you can assign mutliple APNs to the same VRF.

Note Multiple VRFs can be associated with the same VRF instance.

The *vrf-name* should match the name configured in an **ip vrf** global configuration command, and also the **ip vrf forwarding** command at the Gi interface.

To support VRF, you must also enable Cisco Express Forwarding (CEF) switching on the router using the **ip cef** global configuration command.

If you are also configuring DHCP services at the APN, then you must also configure the **dhcp-server** *ip-address* **vrf** command.

Note Memory constraints might occur if you define a large number of access points to support VRF.

Note VRF is not supported on the Catalyst 6500/Cisco 7600 Supervisor / MSFC2. Therefore, to support VRF on the Catalyst 6500/Cisco 7600 platform, you must tunnel VRF encapsulated traffic through the Supervisor / MSFC2 via a GRE tunnel. For more information, see the *Cisco GGSN Release 5.1 Configuration Guide*.

Examples

The following example shows a VRF configuration for vpn3 (without tunneling) using the **ip vrf** global configuration command. Because the **ip vrf** command establishes both VRF and CEF routing tables, notice that **ip cef** also is configured at the global configuration level to enable CEF switching at all of the interfaces.

The following other configuration elements must also associate the same VRF named vpn3:

- FastEthernet0/0 is configured as the Gi interface using the **ip vrf forwarding** interface configuration command.
- Access-point 2 implements VRF using the **vrf** command access-point configuration command.

The DHCP server at access-point 2 also is configured to support VRF. Notice that access-point 1 uses the same DHCP server, but is not supporting the VRF address space. The IP addresses for access-point 1 will apply to the global routing table:

```
aaa new-model
!
aaa group server radius foo
 server 10.2.3.4
 server 10.6.7.8
!
aaa authentication ppp foo group foo
aaa authorization network default group radius
aaa accounting exec default start-stop group foo
!
ip cef
!
ip vrf vpn3
 rd 300:3
!
interface Loopback1
 ip address 10.30.30.30 255.255.255.255
!
interface Loopback2
 ip vrf forwarding vpn3
 ip address 10.27.27.27 255.255.255.255
!
interface FastEthernet0/0
 ip vrf forwarding vpn3
 ip address 10.50.0.1 255.255.0.0
 duplex half
!
interface FastEthernet1/0
 ip address 10.70.0.1 255.255.0.0
 duplex half
!
interface loopback 1
 ip address 10.8.0.1 255.255.255.0
!
```

```
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list gprs
!
ip route 10.10.0.1 255.255.255.255 Virtual-Template1
ip route vrf vpn3 10.100.0.5 255.255.255.0 fa0/0 10.50.0.2
ip route 10.200.0.5 255.255.255.0 fa1/0 10.70.0.2
!
no ip http server
!
gprs access-point-list gprs
 access-point 1
  access-point-name gprs.pdn.com
  ip-address-pool dhcp-proxy-client
  dhcp-server 10.200.0.5
  dhcp-gateway-address 10.30.30.30
  network-request-activation
  exit
  !
 access-point 2
  access-point-name gprs.pdn2.com
  access-mode non-transparent
  ip-address-pool dhcp-proxy-client
  dhcp-server 10.100.0.5 10.100.0.6 vrf
  dhcp-gateway-address 10.27.27.27
  aaa-group authentication foo
  vrf vpn3
  exit
!
gprs default ip-address-pool dhcp-proxy-client
gprs gtp ip udp ignore checksum
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

Related Commands

Command	Description
dhcp-server	Specifies a primary (and backup) DHCP server to allocate IP addresses to MS users entering a particular PDN access point.
ip cef	Enables CEF on the RP card.
ip vrf	Configures a VRF routing table.
ip vrf forwarding	Associates a VRF with an interface or subinterface.
rd	Creates routing and forwarding tables for a VRF and and specifies the default route distinguisher for a VPN.

Debug Commands

The commands in this section are for troubleshooting the GGSN. For information about other debug commands, see the *Cisco IOS Debug Command Reference*.

Caution Because debugging output is assigned high priority in the CPU process, it can diminish the performance of the router or even render it unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

This chapter contains the following section and commands:

TID/IMSI/MSISDN-Based Conditionally Triggered Debugging

When the TID/IMSI/MSISDN-based conditionally triggered debugging feature is enabled, the GGSN generates debugging messages for PDP contexts that match a particular tunnel ID (TID), International Mobile Subscriber Identity (IMSI) value, or Mobile Station ISDN number (MSISDN) entering or leaving the GGSN. The GGSN will not generate debugging output for PDP contexts containing a different TID, IMSI, or MSISDN value.

Normally, the GGSN will generate debugging messages for every PDP context, resulting in a large number of messages that consume system resources and can make it difficult to find the specific information you need. By limiting the number of debugging messages, you can receive messages related to only to PDP contexts you want to troubleshoot.

Usage Guidelines for TID/IMSI/MSISDN-Based Conditional Debugging

Use the following guidelines when configuring TID/IMSI/MSISDN-based conditional debugging on a GGSN.

1. Before enabling a **debug gprs** command, first enable TID/IMSI/MSISDN-based debugging using the **debug condition calling** command. Ensure that the TID/IMSI or MSISDN string match the ones from the Create Request.

   For examples:

   For a create request with TID 12345678090000B0, you would enter:

   ```
   GGSN# debug condition calling 12345678090000B0
   Condition 1 set
   GGSN#
   ```

   For a create request with IMSI 21436579000000, you would enter:

   ```
   GGSN# debug condition calling 21436579000000
   Condition 2 set
   GGSN#
   ```

   For a create request with MSISDN 1112223344, you would enter:

   ```
   GGSN# debug condition calling msisdn-1112223344
   Condition 3 set
   GGSN#
   ```

   To verify the set conditions, enter:

   ```
   GGSN# show debug condition all
   Condition 1: calling 12345678090000B0 (0 flags triggered)
   Condition 2: calling 21436579000000 (0 flags triggered)
   Condition 3: calling 1112223344 (0 flags triggered)
   GGSN#
   ```

2. After turning on TID, IMSI, or MSISDN-based debugging, turn on GPRS debugging by entering the **debug gprs gtp** and/or **debug gprs charging** commands.

   Once this step is completed, when PDP Context Create Requests are received, the GGSN will display debug messages for those create requests with either a matching TID, IMSI, or MSISDN.

3. Because the **no debug all** command does not disable conditional debug flags, to ensure that you do not receive a flood of debugging messages when disabling debugging, turn off GPRS debug flags first using the **no debug all** command as follows:

```
GGSN# no debug all
All possible debugging has been turned off
GGSN#

GGSN# show debug condition all
Condition 1: calling 12345678090000B0 (1 flags triggered)
Condition 2: calling 21436579000000 (1 flags triggered)
Condition 3: calling 1112223344 (1 flags triggered)

GGSN#
```

4. Disable the conditional debug flags using the **no debug condition all** command:

```
GGSN# no debug condition all
Removing all conditions may cause a flood of debugging messages to result, unless
specified debugging flags are first removed.

Proceed with the removal of all conditions [yes/no] y
2 conditions have been removed
```

5. Verify that the conditional debug flags have been removed using the **show debug condition all** command:

```
GGSN# show debug condition all
% No conditions found
```

debug aaa coa

To display debug information for CoA processing, use the **debug aaa coa** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug aaa coa

no debug aaa coa

Syntax Description

This command has no keywords or arguments

Defaults

Debugging for POD packets is not enabled.

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **debug aaa coa** to display debug information for CoA processing.

Examples

The following is an example of debug information for CoA processing:

```
SAMI 5/3:  *Mar 4 23:51:02.820: COA: 10.10.10.10 request queued
SAMI 5/3:  *Mar 4 23:51:02.820: ++++++ CoA Attribute List ++++++
SAMI 5/3:  *Mar 4 23:51:02.820: 410414A8 0 00000009 string-session-id(337) 15
080808012521869
SAMI 5/3: *Mar 4 23:51:02.820: 4189D04C 0 00000009 qos-profile(507) 28
25621F9301FEFE245E1414003200
SAMI 5/3: *Mar 4 23:51:02.820:
SAMI 5/3: *Mar 4 23:51:02.820: COA: Sending ACK from port 1700 to 10.10.10.10/1700
```

debug condition calling

To limit output for some debug commands based on specified conditions, use the **debug condition** command in privileged EXEC mode. To remove the specified condition, use the **no** form of this command.

debug condition {**username** *username* | **called** *dial-string* | **caller** *dial-string* | **vcid** *vc-id* | **ip** *ip-address* | **calling** [*tid* | *imsi* | **msisdn**-*msisdn*]}

no debug condition {*condition-id* | **all**}

Syntax Description

username *username*	Generates debugging messages for interfaces with the specified username.
called *dial-string*	Generates debugging messages for interfaces with the called party number.
caller *dial-string*	Generates debugging messages for interfaces with the calling party number.
vcid *vc-id*	Generates debugging messages for the VC ID specified.
ip *ip-address*	Generates debugging messages for the IP address specified.
calling [*tid* | *imsi string* | **msisdn**-*msisdn* **]**	Displays events related to GTP processing on the GGSN based on tunnel identifier (TID), international mobile system identifier (IMSI), or Mobile Station ISDN number (MSISDN) in a PDP Context Create Request message.
condition-id	Removes the condition indicated.
all	Removes all conditional debugging conditions.

Defaults

No default behavior or values.

Command History

Release	Modification
12.3(2)XB	This command was introduced on the GGSN.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into the Cisco IOS Release 12.3(14)YU and the **msisdn** keyword option was added.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Ensure that you enable TID/IMSI/MSISDN-based conditional debugging using the **debug condition calling** command before configuring the **debug gprs gtp** and **debug gprs charging**. In addition, ensure that you disable the **debug gprs gtp** and **debug gprs charging** commands using the **no debug all** command before disabling conditional debugging using the **no debug condition** command. This will prevent a flood of debug messages when you disable conditional debugging.

For more information on using the GGSN TID/IMSI/MSISDN-based conditional debugging, see "TID/IMSI/MSISDN-Based Conditionally Triggered Debugging" section on page 610.

Examples

Example 1

The following examples configure a conditional debug session based on a TID 12345678090000B0, IMSI 21436579000000, and MSISDN 408525823010:

```
GGSN# debug condition calling 12345678090000B0
Condition 1 set
GGSN#

GGSN# debug condition calling 21436579000000
Condition 2 set
GGSN#

GGSN# debug condition calling msisdn 408525823010
Condition 3 set
GGSN#
```

Example 2

The following example stops all conditional debugging:

```
Router# no debug conditional all
All possible debugging has been turned off
Router#
```

debug data-store

To display persistant storage device (PSD)-related debugging messages for the gateway GPRS support node (GGSN), use the **debug data-store** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug data-store

no debug data-store

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)YU	This command was introduced.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command displays PSD-related debugging messages for the GGSN.

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network flows and fewer users. Debugging during these periods reduces the effect these commands have on other users on the system.

Examples

The following example configures a debugging session to check PSD-related parameters:

```
Router# debug data-store
```

debug data-store detail

To display extended details for persistent storage device (PSD)-related debugging information, use the **debug data-store detail** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug data-store detail

no debug data-store detail

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)YU	This command was introduced.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command displays PSD-related debugging messages for the GGSN.

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network flows and fewer users. Debugging during these periods reduces the effect these commands have on other users on the system.

Examples

The following example configures a detailed PSD-related debugging session:

```
Router# debug data-store details
```

Related Commands

Command	Description
auto-retrieve	Configures the GGSN to automatically initiate a retrieval of G-CDRs from PSDs defined in a PSD server group.
clear data-store statistics	Clears PSD-related statistics.
show data-store	Displays the status of the PSD client and PSD server-related information.
show data-store statistics	Displays statistics related to the PSD client.

debug diameter

To display information about Diameter processing on the gateway GPRS support node (GGSN), use the **debug diameter** command in privilege EXEC mode.

debug diameter {dcca | connection | error | packet | event | fsm | failover | all}

Syntax Description

dcca	Displays Diameter Credit Control Application-related information.
connection	Displays Diameter peer connection information.
error	Displays errors related to Diameter processing.
packet	Displays Diameter packets.
event	Displays Diameter-related events.
fsm	Displays Diameter-related fault state machine messages.
failover	Displays information about DCCA server failovers.
all	Displays all Diameter-related information.

Defaults

No default behavior or values.

Command Modes

Privilege EXEC

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

This command is useful for system operators and development engineers if problems are encountered with Diameter processing.

Examples

The following configuration example displays Diameter-related events:

```
debug diameter event
```

debug ggsn quota-server

To display debug information related to quota server processing on the gateway GPRS support node (GGSN), use the **debug ggsn quota-server** command in privilege EXEC mode.

debug ggsn quota-server [details | packets [dump] | events | parsing | errors]

Syntax Description

details	Displays extended details about quota server operations on the GGSN.
packets	Displays packets sent between the quota server process on the GGSN and the CSG. Optionally, displays output in hexadecimal notation.
events	Displays events related to quota server processing on the GGSN.
parsing	Displays details about GTP TLV parsing between the quota server and the Content Services Gateway.
errors	Displays errors related to quota server processing on the GGSN

Defaults

No default behavior or values.

Command Modes

Privilege EXEC

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

This command is useful for system operators and development engineers if problems are encountered with communication between the GGSN quota server process and the CSG.

Examples

The following example enables the display of events related to quota server processing on the GGSN:

```
Router# debug ggsn quota-server events
```

The following example enables the display of packets sent between the quota server process on the GGSN and the CSG:

```
Router# debug ggsn quota-server packets
```

The following example enables the display of detailed quota server processing debug output:

```
Router# debug ggsn quota-server details
```

debug gprs category fsm event

To display debug information related to service-aware gateway GPRS support node (GGSN) category events, and state transactions, use the **debug gprs category fsm event** command in privilege EXEC mode.

debug gprs category fsm event

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privilege EXEC

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

This command is useful for system operators and development engineers if problems are encountered with eGGSN processing.

Examples

The following example enables the display of eGGSN events and state transactions:

```
Router# debug ggsn eggsn category fsm event
```

debug gprs dcca

To display troubleshooting information about DCCA processing on the gateway GPRS support node (GGSN), use the **debug gprs dcca** command in privilege EXEC mode.

debug gprs dcca

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privilege EXEC

Command History

Release	Modification
12.3(14)YQ	This command was introduced.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

This command is useful for system operators and development engineers if Diameter protocol problems are encountered on the GGSN.

Examples

The following configuration example displays information specific to DCCA processing:

```
debug gprs dcca
```

debug gprs dfp

To display debug messages for GPRS DFP weight calculation, use the **debug gprs dfp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug gprs dfp

no debug gprs dfp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command History

Release	Modification
12.1(9)E	This command was introduced.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

See the following caution before using **debug** commands:

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network flows and fewer users. Debugging during these periods reduces the effect these commands have on other users on the system.

This command displays debug messages for GPRS DFP weight calculation. To display debug messages for the DFP agent subsystem, use the **debug ip dfp agent** command.

Examples

The following example configures a debug session to check all GPRS DFP weight calculation:

```
Router# debug gprs dfp
GPRS DFP debugging is on
Router#
```

The following example stops all debugging:

```
Router# no debug all
All possible debugging has been turned off
Router#
```

debug gprs dhcp

To display information about Dynamic Host Configuration Protocol (DHCP) processing on the gateway GPRS support node (GGSN), use the **debug gprs dhcp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug gprs dhcp

no debug gprs dhcp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

This command is useful for system operators and development engineers if problems are encountered with DHCP processing on the GGSN. To display standard debug messages between the DHCP client on the router and a DHCP server, you can also use the **debug dhcp** or **debug dhcp detail** commands with the **debug gprs dhcp** command.

Caution Because the **debug gprs dhcp** command generates a significant amount of output, use it only when traffic on the GPRS network is low, so other activity on the system is not adversely affected.

Examples

The following example shows sample output for DHCP processing on the GGSN:

```
Router# debug gprs dhcp
2d13h: GPRS:DHCP req:TID 1111111100000099, Req 1
2d13h: GPRS:Requesting IP address for pdp 1111111100000099 from server 172.16.0.8 tableid
0
2d13h: GPRS:DHCP ip allocation pass (10.88.17.43) for pdp 1111111100000099
2d13h: GPRS:Using DHCP ip address 10.88.17.43 for pdp 1111111100000099
```

The following example shows sample output for standard debug messaging for DHCP processing on the router between the DHCP client and a DHCP server:

```
2d13h: DHCP: proxy allocate request
2d13h: DHCP: new entry. add to queue
2d13h: DHCP: SDiscover attempt # 1 for entry:
2d13h: DHCP: SDiscover: sending 283 byte length DHCP packet
2d13h: DHCP: SDiscover with directed serv 172.16.0.8, 283 bytes
2d13h: DHCP: XID MATCH in dhcpc_for_us()
2d13h: DHCP: Received a BOOTREP pkt
2d13h: DHCP: offer received from 172.16.0.8
2d13h: DHCP: SRequest attempt # 1 for entry:
2d13h: DHCP: SRequest- Server ID option: 172.16.0.8
2d13h: DHCP: SRequest- Requested IP addr option: 10.88.17.43
2d13h: DHCP: SRequest placed lease len option: 604800
2d13h: DHCP: SRequest: 301 bytes
2d13h: DHCP: SRequest: 301 bytes
2d13h: DHCP: XID MATCH in dhcpc_for_us()
2d13h: DHCP: Received a BOOTREP pkt
2d13h: DHCP Proxy Client Pooling: ***Allocated IP address: 10.88.17.43
```

Related Commands

Command	Description
debug dhcp	Displays debug messages between the DHCP client on the router and a DHCP server.

debug gprs gtp

To display information about the GPRS Tunneling Protocol (GTP), use the **debug gprs gtp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug gprs gtp {**events** | **messages** | **packets**}

no debug gprs gtp {**events** | **messages** | **packets**}

Syntax Description

events	Displays events related to GTP processing on the GGSN.
messages	Displays GTP signaling messages that are sent between the SGSN and GGSN.
packets	Displays GTP packets that are sent between the SGSN and GGSN.

Defaults

No default behavior or values.

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX, and the **ppp** {**details** | **events**} option was added.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

This command is useful for system operators and development engineers if problems are encountered with communication between the GGSN and the SGSN using GTP.

Caution Because the **debug gprs gtp** command generates a significant amount of output, use it only when traffic on the GPRS network is low, so other activity on the system is not adversely affected.

Examples

The following example enables the display of events related to GTP processing on the GGSN:

```
Router# debug gprs gtp events
```

The following example enables the display of GTP signaling messages:

```
Router# debug gprs gtp messages
```

The following example enables the display of GTP packets sent between the SGSN and GGSN:

```
Router# debug gprs gtp packets
```

The following example enables the display of GTP PPP events between the SGSN and GGSN:

```
Router# debug gprs gtp ppp events
```

The following example enables the display of detailed GTP PPP debug output along with GTP PPP events between the SGSN and GGSN:

```
Router# debug gprs gtp ppp details
Router# debug gprs gtp ppp events
```

debug gprs gtp parsing

To display information about the parsing of GPRS Tunneling Protocol (GTP) information elements (IEs) in signaling requests, use the **debug gprs gtp parsing** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug gprs gtp parsing

no debug gprs gtp parsing

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

This command is useful for system operators and development engineers to verify parsing of GTP IEs in signaling requests that are received by GDM or by the GGSN. If the packet is parsed successfully, you will receive a message along with the TID for the packet as shown in the following example:

```
GPRS:TID:7300000000000000:Packet Parsed successfully
```

The **debug gprs gtp parsing** command can be used to verify GDM or GGSN processing of IEs.

Caution Because the **debug gprs gtp parsing** command generates a significant amount of output, use it only when traffic on the GPRS network is low, so other activity on the system is not adversely affected.

Examples

The following example enables the display of debug messages that occur while GDM or the GGSN parses GTP IEs:

```
Router# debug gprs gtp parsing
```

debug gprs gtp ppp

To display information about PPP PDP type processing on the gateway GPRS support node (GGSN), use the **debug gprs gtp ppp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug gprs gtp ppp {**events** | **details**}

no debug gprs gtp ppp {**events** | **details**}

Syntax Description

events	Displays messages specific to certain conditions that are occurring during PPP PDP type processing.
details	Displays more extensive and lower-level messages related to PPP PDP type processing.

Defaults

No default behavior or values.

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

This command is useful for system operators and development engineers if problems are encountered with PPP PDP type processing on the GGSN.

You can enable both forms of the **debug gprs gtp ppp** command at the same time, as separate command line entries. The **events** keyword generates output specific to certain conditions that are occurring, which helps qualify the output being received using the **details** option.

Caution Because the **debug gprs gtp ppp** command generates a significant amount of output, use it only when traffic on the GPRS network is low, so other activity on the system is not adversely affected.

Examples

The following debug examples provide sample output for a Create PDP Context request and clear PDP context using PPP PDP type on the GGSN. The examples show output while both debug events and details are enabled on the GGSN.

Example 1

The following example displays details and events output related to PPP PDP context processing for a Create PDP Context requested received by the GGSN:

```
Router# debug gprs gtp ppp events
GTP PPP events display debugging is on
Router# debug gprs gtp ppp details
GTP PPP details display debugging is on
7200b#
3d23h: GPRS:
3d23h: GTP-PPP Fa1/0: Create new gtp_ppp_info
3d23h: GPRS:
3d23h: GTP-PPP: domain gprs.cisco.com not in any VPDN group
3d23h: GPRS:
3d23h: GTP-PPP: aaa-group accounting not configured under APN gprs.cisco.com
3d23h: GPRS:GTP-PPP: Don't cache internally generated pak's header
3d23h: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
3d23h: GPRS:
3d23h: GTP-PPP Vi2: gtp_ppp_cstate_react changing states
3d23h: GPRS:GTP-PPP: pdp_entry 0x62F442A4, recv ppp data pak
3d23h: GPRS:GTP-PPP Vi2: proc_udp_input pak's linktype = 30
3d23h: GPRS:GTP-PPP: pdp_entry 0x62F442A4, recv ppp data pak
3d23h: GPRS:GTP-PPP Vi2: proc_udp_input pak's linktype = 30
3d23h: GPRS:GTP-PPP: pdp_entry 0x62F442A4, recv ppp data pak
3d23h: GPRS:GTP-PPP Vi2: proc_udp_input pak's linktype = 30
3d23h: GPRS:
3d23h: GTP-PPP: Vi2: Concat names user00 & gprs.cisco.com
3d23h: GPRS:
3d23h: GTP-PPP: New username after concat: user00@gprs.cisco.com
3d23h: GPRS:
3d23h: GTP-PPP: Vi2: Concat names user00@gprs.cisco.com & gprs.cisco.com
3d23h: GPRS:
3d23h: GTP-PPP: New username after concat: user00@gprs.cisco.com
3d23h: GPRS:GTP-PPP: pdp_entry 0x62F442A4, recv ppp data pak
3d23h: GPRS:GTP-PPP Vi2: proc_udp_input pak's linktype = 30
3d23h: GPRS:GTP-PPP: pdp_entry 0x62F442A4, recv ppp data pak
3d23h: GPRS:GTP-PPP Vi2: proc_udp_input pak's linktype = 30
3d23h: GPRS:GTP-PPP: pdp_entry 0x62F442A4, recv ppp data pak
3d23h: GPRS:GTP-PPP Vi2: proc_udp_input pak's linktype = 30
3d23h: GPRS:GTP-PPP: pdp_entry 0x62F442A4, recv ppp data pak
3d23h: GPRS:GTP-PPP Vi2: proc_udp_input pak's linktype = 30
3d23h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, changed state to
up
3d23h: GPRS:GTP-PPP: pdp_entry 0x62F442A4, recv ppp data pak
3d23h: GPRS:GTP-PPP Vi2: proc_udp_input pak's linktype = 30
3d23h: GPRS:GTP-PPP: pdp_entry 0x62F442A4, recv ppp data pak
3d23h: GPRS:GTP-PPP Vi2: proc_udp_input pak's linktype = 30
3d23h: GPRS:
3d23h: GTP-PPP Vi2: gtp_ppp_protocol_up is notified about intf UP
3d23h: GPRS:
3d23h: GTP-PPP Vi2: PDP w/ MS addr 98.102.0.1 inserted into IP radix tree
```

Example 2

The following example displays both details and events related to PPP PDP type processing after clearing PDP contexts on the GGSN:

```
Router# clear gprs gtp pdp-context all
3d23h: GPRS:GTP-PPP: pdp_entry 0x62F442A4, recv ppp data pak
3d23h: GPRS:GTP-PPP Vi2: proc_udp_input pak's linktype = 30
3d23h: GPRS:GTP-PPP: pdp_entry 0x62F442A4, recv ppp data pak
3d23h: GPRS:GTP-PPP Vi2: proc_udp_input pak's linktype = 30
3d23h: GPRS:
3d23h: GTP-PPP Vi2: gtp_ppp_pdp_terminate shutting down the vaccess
```

```
3d23h: GPRS:
3d23h: GTP-PPP Vi2: gtp_ppp_pdp_shut_va shutting down intf
3d23h: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to down
3d23h: GPRS:
3d23h: GTP-PPP Vi2: gtp_ppp_cstate_react changing states
3d23h: GPRS:
3d23h: GTP-PPP Vi2: gtp_ppp_free_va resetting intf vectors
3d23h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, changed state to
down
```

debug gprs gtp ppp-regeneration

To display information about PPP regeneration processing on the GGSN, use the **debug gprs gtp ppp-regeneration** privileged EXEC command. To disable debugging output, use the **no** form of this command.

debug gprs gtp ppp-regeneration {**events** | **details**}

no debug gprs gtp ppp-regeneration {**events** | **details**}

Syntax Description

events	Displays messages specific to certain conditions that are occurring during PPP regeneration processing.
details	Displays more extensive and lower-level messages related to PPP regeneration processing.

Defaults

No default behavior or values.

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

This command is useful for system operators and development engineers if problems are encountered with communication between GDM and a GGSN.

You can enable both forms of the **debug gprs gtp ppp-regeneration** command at the same time, as separate command line entries. The **events** keyword generates output specific to certain conditions that are occurring, which helps qualify the output being received using the **details** option.

Caution Because the **debug gprs gtp ppp-regeneration** command generates a significant amount of output, use it only when traffic on the GPRS network is low, so other activity on the system is not adversely affected.

Examples

The following debug examples provide sample output for a create PDP context request and clear PDP context using PPP regeneration on the GGSN. The examples show output while both debug events and details are enabled on the GGSN.

Example 1

The following example displays details and events output related to PPP regeneration processing for a create PDP context requested received by the GGSN:

```
Router# debug gprs gtp ppp-regeneration details
GTP PPP regeneration details display debugging is on
Router# debug gprs gtp ppp-regeneration events
GTP PPP regeneration events display debugging is on
06:24:02: PPP-REGEN state counters: pending counter is 0
06:24:02:               State[IDLE] counter is 0
06:24:02:               State[AUTHORIZING] counter is 0
06:24:02:               State[VPDN CONNECTING] counter is 0
06:24:02:               State[PPP NEGOTIATING] counter is 0
06:24:02:               State[PPP CONNECTED] counter is 0
06:24:02:               State[PPP TERMINATING] counter is 0
06:24:02: PPP-REGEN state counters: pending counter is 1
06:24:02:               State[IDLE] counter is 1
06:24:02:               State[AUTHORIZING] counter is 0
06:24:02:               State[VPDN CONNECTING] counter is 0
06:24:02:               State[PPP NEGOTIATING] counter is 0
06:24:02:               State[PPP CONNECTED] counter is 0
06:24:02:               State[PPP TERMINATING] counter is 0
06:24:02: GPRS:1011111111500001:Authen: PAP username: tomy1@corporate_1.com
06:24:02: GPRS:1011111111500001:Session timer started
06:24:02: GPRS:Processing PPP regen reqQ
06:24:02: GPRS:1011111111500001:Processing Initiate PPP  regen from reqQ
06:24:02: GPRS:1011111111500001:got event [REQUEST PPP REGEN] in state [IDLE]
06:24:02: PPP-REGEN state counters: pending counter is 1
06:24:02:               State[IDLE] counter is 0
06:24:02:               State[AUTHORIZING] counter is 1
06:24:02:               State[VPDN CONNECTING] counter is 0
06:24:02:               State[PPP NEGOTIATING] counter is 0
06:24:02:               State[PPP CONNECTED] counter is 0
06:24:02:               State[PPP TERMINATING] counter is 0
06:24:02: GPRS:1011111111500001:state [IDLE->AUTHORIZING] on event [REQUEST PPP REGEN]
06:24:02: GPRS:1011111111500001:Got VPN authorization info
06:24:02: GPRS:1011111111500001:got event [AUTHOR SUCCESS] in state [AUTHORIZING]
06:24:02: PPP-REGEN state counters: pending counter is 1
06:24:02:               State[IDLE] counter is 0
06:24:02:               State[AUTHORIZING] counter is 0
06:24:02:               State[VPDN CONNECTING] counter is 1
06:24:02:               State[PPP NEGOTIATING] counter is 0
06:24:02:               State[PPP CONNECTED] counter is 0
06:24:02:               State[PPP TERMINATING] counter is 0
06:24:02: GPRS:1011111111500001:state [AUTHORIZING->VPDN CONNECTING] on event [AUTHOR
SUCCESS]
06:24:02: GPRS:1011111111500001:Author succeeded, establishing the tunnel
06:24:02: GPRS:1011111111500001:Create/Clone vaccess to negotiate PPP
06:24:02: GPRS:1011111111500001:no need to set NS ppp_config
06:24:02: GPRS:1011111111500001:MS no static IP addr. Get one via IPCP
06:24:02: GPRS:1011111111500001:VPDN to inform PPP regen: CONNECTED
06:24:02: GPRS:1011111111500001:got event [VPDN CONNECTED] in state [VPDN CONNECTING]
06:24:02: PPP-REGEN state counters: pending counter is 1
06:24:02:               State[IDLE] counter is 0
06:24:02:               State[AUTHORIZING] counter is 0
06:24:02:               State[VPDN CONNECTING] counter is 0
06:24:02:               State[PPP NEGOTIATING] counter is 1
06:24:02:               State[PPP CONNECTED] counter is 0
06:24:02:               State[PPP TERMINATING] counter is 0
06:24:02: GPRS:1011111111500001:state [VPDN CONNECTING->PPP NEGOTIATING] on event [VPDN
CONNECTED]
06:24:02: GPRS:1011111111500001:Start PPP negotiations on vaccess
06:24:02: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
```

```
06:24:02: GPRS:1011111111500001:IPCP is up
06:24:02: GPRS:1011111111500001:LNS allocates 10.100.1.1 for MS
06:24:02: GPRS:1011111111500001:IP addr 10.100.1.1 is negotiated for MS
06:24:02: GPRS:1011111111500001:PPP connected
06:24:02: GPRS:1011111111500001:got event [PPP NEGOTIATED] in state [PPP NEGOTIATING]
06:24:02: PPP-REGEN state counters: pending counter is 0
06:24:02:               State[IDLE] counter is 0
06:24:02:               State[AUTHORIZING] counter is 0
06:24:02:               State[VPDN CONNECTING] counter is 0
06:24:02:               State[PPP NEGOTIATING] counter is 0
06:24:02:               State[PPP CONNECTED] counter is 1
06:24:02:               State[PPP TERMINATING] counter is 0
06:24:02: GPRS:1011111111500001:state [PPP NEGOTIATING->PPP CONNECTED] on event [PPP
NEGOTIATED]
06:24:02: GPRS:1011111111500001:PPP succeeded negotiation, session established
06:24:02: GPRS:1011111111500001:Session timer stopped
06:24:03: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, changed state
to up
```

Example 2

The following example displays both details and events related to PPP regeneration processing after clearing PDP contexts on the GGSN:

```
Router# clear gprs gtp pdp-context all
06:28:05: PPP-REGEN state counters: pending counter is 0
06:28:05:               State[IDLE] counter is 0
06:28:05:               State[AUTHORIZING] counter is 0
06:28:05:               State[VPDN CONNECTING] counter is 0
06:28:05:               State[PPP NEGOTIATING] counter is 0
06:28:05:               State[PPP CONNECTED] counter is 1
06:28:05:               State[PPP TERMINATING] counter is 0
06:28:05: GPRS:1011111111500001:PPP regen current state PPP CONNECTED
06:28:05: GPRS:1011111111500001:GTP disconnecting the PPP regen session
06:28:05: GPRS:Processing PPP regen reqQ
06:28:05: GPRS:1011111111500001:Processing Disconnect PPP  regen from reqQ
06:28:05: GPRS:1011111111500001:got event [CANCEL REGEN'ED PPP] in state [PPP CONNECTED]
06:28:05: PPP-REGEN state counters: pending counter is 1
06:28:05:               State[IDLE] counter is 0
06:28:05:               State[AUTHORIZING] counter is 0
06:28:05:               State[VPDN CONNECTING] counter is 0
06:28:05:               State[PPP NEGOTIATING] counter is 0
06:28:05:               State[PPP CONNECTED] counter is 0
06:28:05:               State[PPP TERMINATING] counter is 1
06:28:05: GPRS:1011111111500001:state [PPP CONNECTED->PPP TERMINATING] on event [CANCEL
REGEN'ED PPP]
06:28:05: GPRS:1011111111500001:Cancel request after VPND tunnel is up
06:28:05: PPP-REGEN state counters: pending counter is 1
06:28:05:               State[IDLE] counter is 0
06:28:05:               State[AUTHORIZING] counter is 0
06:28:05:               State[VPDN CONNECTING] counter is 0
06:28:05:               State[PPP NEGOTIATING] counter is 0
06:28:05:               State[PPP CONNECTED] counter is 0
06:28:05:               State[PPP TERMINATING] counter is 1
06:28:05: GPRS:1011111111500001:PPP down
06:28:05: GPRS:1011111111500001:got event [PPP FAILED] in state [PPP TERMINATING]
06:28:05: PPP-REGEN state counters: pending counter is 1
06:28:05:               State[IDLE] counter is 1
06:28:05:               State[AUTHORIZING] counter is 0
06:28:05:               State[VPDN CONNECTING] counter is 0
06:28:05:               State[PPP NEGOTIATING] counter is 0
06:28:05:               State[PPP CONNECTED] counter is 0
06:28:05:               State[PPP TERMINATING] counter is 0
```

```
06:28:05: GPRS:1011111111500001:state [PPP TERMINATING->IDLE] on event [PPP FAILED]
06:28:05: GPRS:1011111111500001:LCP went down
06:28:05: GPRS:1011111111500001:VPDN disconnect
06:28:05: GPRS:1011111111500001:got event [CLEANUP CONTEXT] in state [IDLE]
06:28:05: GPRS:1011111111500001:state [IDLE->IDLE] on event [CLEANUP CONTEXT]
06:28:05: GPRS:1011111111500001:Freeing context structure
06:28:05: GPRS:1011111111500001:VPDN handle invalid, no need to free it
06:28:05: GPRS:1011111111500001:remove PPP regen context from Vi2
06:28:05: GPRS:1011111111500001:Session timer stopped
06:28:05: PPP-REGEN state counters: pending counter is 0
06:28:05:               State[IDLE] counter is 0
06:28:05:               State[AUTHORIZING] counter is 0
06:28:05:               State[VPDN CONNECTING] counter is 0
06:28:05:               State[PPP NEGOTIATING] counter is 0
06:28:05:               State[PPP CONNECTED] counter is 0
06:28:05:               State[PPP TERMINATING] counter is 0
06:28:05: GPRS:1011111111500001:PPP regen context 0x633F196C released
06:28:05: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to down
06:28:06: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, changed state
to down
```

debug gprs iscsi

To display information about the GPRS iSCSI processing, use the **debug gprs iscsi** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug gprs gtp {**errors** | **events** | **messages**}

no debug gprs gtp {**errors** | **events** | **messages**}

Syntax Description

errors	Displays error messages related to GPRS iSCSI processing on the GGSN.
events	Displays events related to GPRS iSCSI processing on the GGSN.
messages	Displays signaling messages related to GPRS iSCSI.

Defaults

No default behavior or values.

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

This command is useful for system operators and development engineers if problems are encountered with communication between the GGSN and the SAN using iSCSI.

Examples

The following example displays GPRS iSCSI debugging:

```
Router#
SAMI 9/3: GPRS:Fn is ggsn_iscsi_send_leftover_dtrs_to_cgw
SAMI 9/3: GPRS:Fn is ggsn_iscsi_send_leftover_dtrs_to_cgw
SAMI 9/3: GPRS:ISCSI: data_len = 246, error code = 0
SAMI 9/3: GPRS:GGSN_ISCSI_MSG
SAMI 9/3: GPRS:ISCSI_READ_ACK_RCVD
SAMI 9/3: GPRS:
 ISCSI: Retrieved DTR Val is iscsi_hdr.dtr_typ_val 2
SAMI 9/3: GPRS:ISCSI: dtr_typ_val = 2 fn:send_retrieved_dtr_to_cgw
SAMI 9/3: GPRS:ISCSI: SAN has sent the record for a read request
SAMI 9/3: GPRS:ISCSI: ISCSI_DYNAMIC send_retrieved_dtr_to_cgw
SAMI 9/3: GPRS:ISCSI: gtp_msg_send_iscsi_retrieved_drt_req is called
SAMI 9/3: GPRS:retrieved cdr from ISCSI
SAMI 9/3: GPRS:Fn is gtp_msg_send_iscsi_retrieved_drt_req, pak val is 4AE35EE4
pak-datagramstart is 7C53FA18 pak->datagramsize is 232

SAMI 9/3: GPRS:ISCSI: data_len = 246, error code = 0
SAMI 9/3: GPRS:GGSN_ISCSI_MSG
SAMI 9/3: GPRS:ISCSI_READ_ACK_RCVD
SAMI 9/3: GPRS:
 ISCSI: Retrieved DTR Val is iscsi_hdr.dtr_typ_val 2
SAMI 9/3: GPRS:ISCSI: dtr_typ_val = 2 fn:send_retrieved_dtr_to_cgw
SAMI 9/3: GPRS:ISCSI: SAN has sent the record for a read request
SAMI 9/3: GPRS:ISCSI: ISCSI_DYNAMIC send_retrieved_dtr_to_cgw
```

```
SAMI 9/3: GPRS:ISCSI: gtp_msg_send_iscsi_retrieved_drt_req is called
SAMI 9/3: GPRS:retrieved cdr from ISCSI
SAMI 9/3: GPRS:Fn is gtp_msg_send_iscsi_retrieved_drt_req, pak val is 41056464
pak-datagramstart is 7C003058 pak->datagramsize is 232

SAMI 9/3: GPRS:ISCSI: data_len = 246, error code = 0
SAMI 9/3: GPRS:GGSN_ISCSI_MSG
SAMI 9/3: GPRS:ISCSI_READ_ACK_RCVD
SAMI 9/3: GPRS:
 ISCSI: Retrieved DTR Val is iscsi_hdr.dtr_typ_val 2
SAMI 9/3: GPRS:ISCSI: dtr_typ_val = 2 fn:send_retrieved_dtr_to_cgw
SAMI 9/3: GPRS:ISCSI: SAN has sent the record for a read request
SAMI 9/3: GPRS:ISCSI: ISCSI_DYNAMIC send_retrieved_dtr_to_cgw
SAMI 9/3: GPRS:ISCSI: gtp_msg_send_iscsi_retrieved_drt_req is called
SAMI 9/3: GPRS:retrieved cdr from ISCSI
SAMI 9/3: GPRS:Fn is gtp_msg_send_iscsi_retrieved_drt_req, pak val is 415563FC
pak-datagramstart is 7C53FD58 pak->datagramsize is 232

SAMI 9/3: GPRS:ISCSI: data_len = 246, error code = 0
SAMI 9/3: GPRS:GGSN_ISCSI_MSG
SAMI 9/3: GPRS:ISCSI_READ_ACK_RCVD
SAMI 9/3: GPRS:
 ISCSI: Retrieved DTR Val is iscsi_hdr.dtr_typ_val 2
SAMI 9/3: GPRS:ISCSI: dtr_typ_val = 2 fn:send_retrieved_dtr_to_cgw
SAMI 9/3: GPRS:ISCSI: SAN has sent the record for a read request
SAMI 9/3: GPRS:ISCSI: ISCSI_DYNAMIC send_retrieved_dtr_to_cgw
SAMI 9/3: GPRS:ISCSI: gtp_msg_send_iscsi_retrieved_drt_req is called
SAMI 9/3: GPRS:retrieved cdr from ISCSI
SAMI 9/3: GPRS:Fn is gtp_msg_send_iscsi_retrieved_drt_req, pak val is 41056BDC
pak-datagramstart is 7C003D58 pak->datagramsize is 232

SAMI 9/3: GPRS:Fn is ggsn_iscsi_send_leftover_dtrs_to_cgw
SAMI 9/3: GPRS:Fn is ggsn_iscsi_send_leftover_dtrs_to_cgw
SAMI 9/3: GPRS:ISCSI: data_len = 1162, error code = 0
SAMI 9/3: GPRS:GGSN_ISCSI_MSG
SAMI 9/3: GPRS:ISCSI_READ_ACK_RCVD
SAMI 9/3: GPRS:
 ISCSI: Retrieved DTR Val is iscsi_hdr.dtr_typ_val 1
SAMI 9/3: GPRS:ISCSI: dtr_typ_val = 1 fn:send_retrieved_dtr_to_cgw
SAMI 9/3: GPRS:ISCSI: SAN has sent the record for a read request
SAMI 9/3: GPRS:ISCSI: ISCSI_PENDING send_retrieved_dtr_to_cgw cgw_down_flags  300
SAMI 9/3: GPRS:ISCSI: gtp_msg_send_iscsi_retrieved_drt_req is called
SAMI 9/3: GPRS:retrieved cdr from ISCSI
SAMI 9/3: GPRS:Fn is gtp_msg_send_iscsi_retrieved_drt_req, pak val is 4AE3B10C
pak-datagramstart is 7C5512D8 pak->datagramsize is 1132

SAMI 9/3: GPRS:Fn is ggsn_iscsi_send_leftover_dtrs_to_cgw
SAMI 9/3: GPRS:Fn is ggsn_iscsi_send_leftover_dtrs_to_cgw
SAMI 9/3: GPRS:ISCSI: data_len = 0, error code = 3
SAMI 9/3: GPRS:ISCSI retrieved empty record 3
SAMI 9/3: GPRS:GGSN_ISCSI_MSG
SAMI 9/3: GPRS:ISCSI_READ_ACK_RCVD
SAMI 9/3: GPRS:Empty iSCSI record was rcvd, so send leftover DTRs to CG
SAMI 9/3: GPRS:Fn is ggsn_iscsi_send_leftover_dtrs_to_cgw
SAMI 9/3: GPRS:ISCSI: data_len = 0, error code = 3
SAMI 9/3: GPRS:ISCSI retrieved empty record 3
SAMI 9/3: GPRS:GGSN_ISCSI_MSG
SAMI 9/3: GPRS:ISCSI_READ_ACK_RCVD
SAMI 9/3: GPRS:Empty iSCSI record was rcvd, so send leftover DTRs to CG
SAMI 9/3: GPRS:Fn is ggsn_iscsi_send_leftover_dtrs_to_cgw
SAMI 9/3: GPRS:ISCSI: data_len = 0, error code = 3
SAMI 9/3: GPRS:ISCSI retrieved empty record 3
SAMI 9/3: GPRS:GGSN_ISCSI_MSG
SAMI 9/3: GPRS:ISCSI_READ_ACK_RCVD
```

```
SAMI 9/3: GPRS:Empty iSCSI record was rcvd, so send leftover DTRs to CG
SAMI 9/3: GPRS:Fn is ggsn_iscsi_send_leftover_dtrs_to_cgw
SAMI 9/3: GPRS:ISCSI: data_len = 0, error code = 3
SAMI 9/3: GPRS:ISCSI retrieved empty record 3
SAMI 9/3: GPRS:GGSN_ISCSI_MSG
SAMI 9/3: GPRS:ISCSI_READ_ACK_RCVD
SAMI 9/3: GPRS:Empty iSCSI record was rcvd, so send leftover DTRs to CG
SAMI 9/3: GPRS:Fn is ggsn_iscsi_send_leftover_dtrs_to_cgw
SAMI 9/3: GPRS:ISCSI: data_len = 0, error code = 3
SAMI 9/3: GPRS:ISCSI retrieved empty record 3
SAMI 9/3: GPRS:GGSN_ISCSI_MSG
SAMI 9/3: GPRS:ISCSI_READ_ACK_RCVD
SAMI 9/3: GPRS:Empty iSCSI record was rcvd, so send leftover DTRs to CG
SAMI 9/3: GPRS:Fn is ggsn_iscsi_send_leftover_dtrs_to_cgw
SAMI 9/3: GPRS:ISCSI: data_len = 0, error code = 3
SAMI 9/3: GPRS:ISCSI retrieved empty record 3
SAMI 9/3: GPRS:GGSN_ISCSI_MSG
SAMI 9/3: GPRS:ISCSI_READ_ACK_RCVD
SAMI 9/3: GPRS:Empty iSCSI record was rcvd, so send leftover DTRs to CG
SAMI 9/3: GPRS:Fn is ggsn_iscsi_send_leftover_dtrs_to_cgw
SAMI 9/3: GPRS:Fn is ggsn_iscsi_send_leftover_dtrs_to_cgw
Router#
```

debug gprs radius

To display information about Remote Access Dial-In User Service (RADIUS) processing on the gateway GPRS support node (GGSN), use the **debug gprs radius** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug gprs radius

no debug gprs radius

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

This command is useful for system operators and development engineers if problems are encountered with communication between a RADIUS server and the GGSN.

Caution Because the **debug gprs radius** command generates a significant amount of output, use it only when traffic on the GPRS network is low, so other activity on the system is not adversely affected.

Examples

The following example enables the display of debug messages related to RADIUS processing on the GGSN:

```
Router# debug gprs radius
```

debug gprs redundancy

To display debug messages, errors, events, or packets related to GTP session redundancy (GTP-SR), use the **debug gprs redundancy** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug gprs redundancy [**debug** | **errors** | **events** | **packets**]

no debug gprs redundancy [**debug** | **errors** | **events** | **packets**]

Syntax Description

debug	Displays debug messages related to GTP-SR.
errors	Displays errors related to GTP-SR.
events	Displays events related to GTP-SR.
packets	Displays packets related to GTP-SR packets.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)YJ	This command was introduced.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

This command displays debug level messages, errors, events, or packets for GTP-SR. It is useful for system operators and development engineers if problems are encountered with communication between the two GGSNs configured as an redundant pair and on which GTP-SR is enabled.

Examples

The following example enables the display of events related to GTP-SR processing on the GGSN:

```
Router# debug gprs redundancy
```

Related Commands

Command	Description
clear gprs redundancy statistics	Clears statistics related to GTP-SR.
gprs redundancy	Enables GTP-SR on a GGSN.
gprs redundancy charging sync-window cdr rec-seqnum	Configures the window size used to determine when the CDR record sequence number needs to be synchronized to the Standby GGSN.

Command	Description
gprs redundancy charging sync-window gtpp seqnum	Configures the window size used to determine when the GTP' sequence number needs to be synchronized to the Standby GGSN.
show gprs redundancy	Displays statistics related to GTP-SR.

debug ip iscsi

To display information about the iSCSI processing on the GGSN, use the **debug ip iscsi** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip iscsi {**all** | **error** | **event | packet**} [**detail**]

no debug ip iscsi {**all** | **error** | **event | packet**} [**detail**]

Syntax Description

all	Displays all iSCSI debug information.
error	Displays error messages related to iSCSI processing on the GGSN.
event	Displays events related to iSCSI processing on the GGSN.
packet	Displays iSCSI packets that are sent between the GGSN and SAN.
detail	(Optional) Displays detailed packet and event information.

Defaults

No default behavior or values.

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

This command is useful for system operators and development engineers if problems are encountered with communication between the GGSN and the SAN using iSCSI.

Examples

The following example displays iSCSI debugging at the time of login:

```
===============
Router#debug ip iscsi all
iSCSI All debugging is on

Router#show debug
iSCSI:
  iSCSI Events debugging is on
  iSCSI Events Detailed debugging is on
  iSCSI Packets debugging is on
  iSCSI Packets Detailed debugging is on
  iSCSI Error debugging is on

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#gprs iscsi LINUX
Router(config)#end
Router#
SAMI 9/3: iSCSI Event: iSCSI Connection Event (0), State Change from(0) -> To(1)
SAMI 9/3: iSCSI Event: Socket Connect Success
SAMI 9/3: iSCSI Event: iSCSI Connection Event (4), State Change from(1) -> To(2)
SAMI 9/3: iSCSI Event: Send CONN Up Msg to RX
```

```
SAMI 9/3: INTR->TGT (HEADER + DATA):
493DEE20:                   43810000 00000092          C.......
493DEE30: 30303030 31000000 00000000 00000000  00001...........
493DEE40: 00000001 00000000 00000000 00000000  ................
493DEE50: 00000000 00000000 496E6974 6961746F  ........Initiato
493DEE60: 724E616D 653D6971 6E2E3139 38372D30  rName=iqn.1987-0
493DEE70: 372E636F 6D2E6369 73636F3A 6D777462  7.com.cisco:mwtb
493DEE80: 6732352D 7375702D 30392D33 00546172  g25-sup-09-3.Tar
493DEE90: 6765744E 616D653D 69716E2E 32303032  getName=iqn.2002
493DEEA0: 2D31302E 6564752E 756E682E 696F6C2E  -10.edu.unh.iol.
493DEEB0: 69736373 692E6472 61667432 302D7461  iscsi.draft20-ta
493DEEC0: 72676574 3A310053 65737369 6F6E5479  rget:1.SessionTy
493DEED0: 70653D4E 6F726D61 6C004175 74684D65  pe=Normal.AuthMe
493DEEE0: 74686F64 3D4E6F6E 65000000           thod=None...
SAMI 9/3: iSCSI Event: Starting Login Timer (5)
SAMI 9/3: iSCSI Event: New Connection Event - 0
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 23810000 00000027 30303030 31000000  #......'00001...
4B5A7260: 00000000 00000000 00000001 00000001  ................
4B5A7270: 00000005 00000000 00000000 00000000  ................
4B5A7280:
SAMI 9/3: TGT->INTR:Data:
493E6E50:                   41757468 4D657468          AuthMeth
493E6E60: 6F643D4E 6F6E6500 54617267 6574506F  od=None.TargetPo
493E6E70: 7274616C 47726F75 70546167 3D310000  rtalGroupTag=1..
493E6E80:
SAMI 9/3: iSCSI Event: Data-In: Read (40) bytes of Data Segment
SAMI 9/3: INTR->TGT (HEADER + DATA):
493DEE20:                   43870000 00000133          C......3
493DEE30: 30303030 31000000 00000000 00000000  00001...........
493DEE40: 00000001 00000002 00000000 00000000  ................
493DEE50: 00000000 00000000 48656164 65724469  ........HeaderDi
493DEE60: 67657374 3D4E6F6E 65004461 74614469  gest=None.DataDi
493DEE70: 67657374 3D4E6F6E 65004D61 78526563  gest=None.MaxRec
493DEE80: 76446174 61536567 6D656E74 4C656E67  vDataSegmentLeng
493DEE90: 74683D33 32373638 00446566 61756C74  th=32768.Default
493DEEA0: 54696D65 32576169 743D3500 44656661  Time2Wait=5.Defa
493DEEB0: 756C7454 696D6532 52657461 696E3D35  ultTime2Retain=5
493DEEC0: 0049464D 61726B65 723D4E6F 004F464D  .IFMarker=No.OFM
493DEED0: 61726B65 723D4E6F 00457272 6F725265  arker=No.ErrorRe
493DEEE0: 636F7665 72794C65 76656C3D 3000496E  coveryLevel=0.In
493DEEF0: 69746961 6C523254 3D596573 00496D6D  itialR2T=Yes.Imm
493DEF00: 65646961 74654461 74613D59 6573004D  ediateData=Yes.M
493DEF10: 61784275 7273744C 656E6774 683D3136  axBurstLength=16
493DEF20: 33383400 46697273 74427572 73744C65  384.FirstBurstLe
493DEF30: 6E677468 3D313633 3834004D 61784F75  ngth=16384.MaxOu
493DEF40: 74737461 6E64696E 67523254 3D31004D  tstandingR2T=1.M
493DEF50: 6178436F 6E6E6563 74696F6E 733D3100  axConnections=1.
493DEF60: 44617461 50445549 6E4F7264 65723D59  DataPDUInOrder=Y
493DEF70: 65730044 61746153 65717565 6E636549  es.DataSequenceI
493DEF80: 6E4F7264 65723D59 65730000           nOrder=Yes..
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 23870000 000000C2 30303030 31000F53  #......B00001..S
4B5A7260: 00000000 00000000 00000002 00000001  ................
4B5A7270: 00000005 00000000 00000000 00000000  ................
4B5A7280:
SAMI 9/3: TGT->INTR:Data:
493E6E50:                   48656164 65724469          HeaderDi
493E6E60: 67657374 3D4E6F6E 65004461 74614469  gest=None.DataDi
493E6E70: 67657374 3D4E6F6E 65004465 6661756C  gest=None.Defaul
493E6E80: 7454696D 65325761 69743D35 00446566  tTime2Wait=5.Def
493E6E90: 61756C74 54696D65 32526574 61696E3D  aultTime2Retain=
493E6EA0: 35004572 726F7252 65636F76 6572794C  5.ErrorRecoveryL
493E6EB0: 6576656C 3D300049 6D6D6564 69617465  evel=0.Immediate
```

```
493E6EC0: 44617461 3D596573 004D6178 4F757473  Data=Yes.MaxOuts
493E6ED0: 74616E64 696E6752 32543D31 004D6178  tandingR2T=1.Max
493E6EE0: 436F6E6E 65637469 6F6E733D 31004669  Connections=1.Fi
493E6EF0: 72737442 75727374 4C656E67 74683D31  rstBurstLength=1
493E6F00: 36333834 004D6178 42757273 744C656E  6384.MaxBurstLen
493E6F10: 6774683D 31363338 34000000           gth=16384...
SAMI 9/3: iSCSI Event: Data-In: Read (196) bytes of Data Segment
SAMI 9/3: iSCSI Event: iSCSI Connection Event (6), State Change from(2) -> To(3)
SAMI 9/3: iSCSI Event: Starting Full Feature Phase Timer (5)
SAMI 9/3: iSCSI Event: iSCSI Session Event (0), State Change from(0) -> To(1)
SAMI 9/3: iSCSI Event-Det: handle scsi cmd req
SAMI 9/3: iSCSI Event-Det: run pending queue
SAMI 9/3: iSCSI Event-Det: send scsi command
SAMI 9/3: INTR->TGT HEAD:
493DEE20:                   01C00000 00000000          .@......
493DEE30: 00000000 00000000 00000001 00000000  ................
493DEE40: 00000001 00000003 00000000 00000000  ................
493DEE50: 00000000 00000000                    ........
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 21800000 00000000 00000000 00000000  !...............
4B5A7260: 00000001 00000000 00000003 00000002  ................
4B5A7270: 00000006 00000000 00000000 00000000  ................
4B5A7280:
SAMI 9/3: SCSI Event: Test unit ready command successful
SAMI 9/3: iSCSI Event-Det: handle scsi cmd req
SAMI 9/3: iSCSI Event-Det: run pending queue
SAMI 9/3: iSCSI Event-Det: send scsi command
SAMI 9/3: INTR->TGT HEAD:
493DEE20:                   01C00000 00000000          .@......
493DEE30: 00000000 00000000 00000002 000000FF  ................
493DEE40: 00000002 00000004 A0000000 00000000  ........ ........
493DEE50: 00FF0000 00000000                    ........
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 25800000 00000030 00000000 00000000  %......0........
4B5A7260: 00000002 FFFFFFFF 00000000 00000003  ................
4B5A7270: 00000006 00000000 00000000 00000000  ................
4B5A7280:
SAMI 9/3: iSCSI Event: recv_data for itt 2, cmnd 0xA0, bufflen 255, offset 0 exp offset 0,
flags 0x80 datasn 0

SAMI 9/3: TGT->INTR:Data:
414F59E0: 00000028 00000000 00000000 00000000  ...(............
414F59F0: 00010000 00000000 00020000 00000000  ................
414F5A00: 00030000 00000000 00040000 00000000  ................
414F5A10:
SAMI 9/3: iSCSI Event: Data-In: Read (48) bytes of Data Segment
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 21820000 00000000 00000000 00000000  !...............
4B5A7260: 00000002 00000000 00000004 00000003  ................
4B5A7270: 00000007 00000001 00000000 000000CF  ...............O
4B5A7280:
SAMI 9/3: iSCSI Event-Det: handle scsi cmd req
SAMI 9/3: iSCSI Event-Det: run pending queue
SAMI 9/3: iSCSI Event-Det: send scsi command
SAMI 9/3: INTR->TGT HEAD:
493DEE20:                   01C00000 00000000          .@......
493DEE30: 00000000 00000000 00000003 000000FF  ................
493DEE40: 00000003 00000005 12000000 FF000000  ................
493DEE50: 00000000 00000000                    ........
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 25800000 000000FF 00000000 00000000  %...............
4B5A7260: 00000003 FFFFFFFF 00000000 00000004  ................
4B5A7270: 00000007 00000000 00000000 00000000  ................
4B5A7280:
```

```
SAMI 9/3: iSCSI Event: recv_data for itt 3, cmnd 0x12, bufflen 255, offset 0 exp offset 0,
flags 0x80 datasn 0

SAMI 9/3: TGT->INTR:Data:
493D6960:          00000402 1F008000 554E482D      ........UNH-
493D6970: 494F4C20 66696C65 2D6D6F64 65207461  IOL file-mode ta
493D6980: 72676574 312E3220 00000000 00000000  rget1.2 ........
493D6990: 00000000 00000000 00000000 00000000  ................
493D69A0: 00000000 00000000 00000000 00000000  ................
493D69B0: 00000000 00000000 00000000 00000000  ................
493D69C0: 00000000 00000000 00000000 00000000  ................
493D69D0: 00000000 00000000 00000000 00000000  ................
493D69E0: 00000000 00000000 00000000 00000000  ................
493D69F0: 00000000 00000000 00000000 00000000  ................
493D6A00: 00000000 00000000 00000000 00000000  ................
493D6A10: 00000000 00000000 00000000 00000000  ................
493D6A20: 00000000 00000000 00000000 00000000  ................
493D6A30: 00000000 00000000 00000000 00000000  ................
493D6A40: 00000000 00000000 00000000 00000000  ................
493D6A50: 00000000 00000000 00000000 00000000  ................
493D6A60: 00000000                             ....
SAMI 9/3: iSCSI Event: Data-In: Read (256) bytes of Data Segment
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 21800000 00000000 00000000 00000000  !...............
4B5A7260: 00000003 00000000 00000005 00000004  ................
4B5A7270: 00000008 00000001 00000000 00000000  ................
4B5A7280:
SAMI 9/3: SCSI Event: Processing inquire LUN response
SAMI 9/3: SCSI Event: Calling Device Add - 414F59E0
SAMI 9/3: SCSI Event: scsi add device
SAMI 9/3: SCSI Event: lun_in_inquiry 1
SAMI 9/3: iSCSI Event-Det: handle scsi cmd req
SAMI 9/3: iSCSI Event-Det: run pending queue
SAMI 9/3: iSCSI Event-Det: send scsi command
SAMI 9/3: INTR->TGT HEAD:
493DEE20:                   01C00000 00000000          .@......
493DEE30: 00010000 00000000 00000004 000000FF  ................
493DEE40: 00000004 00000006 12000000 FF000000  ................
493DEE50: 00000000 00000000                    ........
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 25800000 000000FF 00000000 00000000  %...............
4B5A7260: 00000004 FFFFFFFF 00000000 00000005  ................
4B5A7270: 00000008 00000000 00000000 00000000  ................
4B5A7280:
SAMI 9/3: iSCSI Event: recv_data for itt 4, cmnd 0x12, bufflen 255, offset 0 exp offset 0,
flags 0x80 datasn 0

SAMI 9/3: TGT->INTR:Data:
493A3D40: 00000402 1F008000 554E482D 494F4C20  ........UNH-IOL
493A3D50: 66696C65 2D6D6F64 65207461 72676574  file-mode target
493A3D60: 312E3220 00000000 00000000 00000000  1.2 ............
493A3D70: 00000000 00000000 00000000 00000000  ................
493A3D80: 00000000 00000000 00000000 00000000  ................
493A3D90: 00000000 00000000 00000000 00000000  ................
493A3DA0: 00000000 00000000 00000000 00000000  ................
493A3DB0: 00000000 00000000 00000000 00000000  ................
493A3DC0: 00000000 00000000 00000000 00000000  ................
493A3DD0: 00000000 00000000 00000000 00000000  ................
493A3DE0: 00000000 00000000 00000000 00000000  ................
493A3DF0: 00000000 00000000 00000000 00000000  ................
493A3E00: 00000000 00000000 00000000 00000000  ................
493A3E10: 00000000 00000000 00000000 00000000  ................
493A3E20: 00000000 00000000 00000000 00000000  ................
493A3E30: 00000000 00000000 00000000 00000000  ................
```

```
493A3E40:
SAMI 9/3: iSCSI Event: Data-In: Read (256) bytes of Data Segment
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 21800000 00000000 00000000 00000000  !...............
4B5A7260: 00000004 00000000 00000006 00000005  ................
4B5A7270: 00000009 00000001 00000000 00000000  ................
4B5A7280:
SAMI 9/3: SCSI Event: Processing inquire LUN response
SAMI 9/3: SCSI Event: Calling Device Add - 41E1B98C
SAMI 9/3: SCSI Event: scsi add device
SAMI 9/3: SCSI Event: lun_in_inquiry 2
SAMI 9/3: iSCSI Event-Det: handle scsi cmd req
SAMI 9/3: iSCSI Event-Det: run pending queue
SAMI 9/3: iSCSI Event-Det: send scsi command
SAMI 9/3: INTR->TGT HEAD:
493DEE20:                   01C00000 00000000          .@......
493DEE30: 00020000 00000000 00000005 000000FF  ................
493DEE40: 00000005 00000007 12000000 FF000000  ................
493DEE50: 00000000 00000000                    ........
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 25800000 000000FF 00000000 00000000  %...............
4B5A7260: 00000005 FFFFFFFF 00000000 00000006  ................
4B5A7270: 00000009 00000000 00000000 00000000  ................
4B5A7280:
SAMI 9/3: iSCSI Event: recv_data for itt 5, cmnd 0x12, bufflen 255, offset 0 exp offset 0,
flags 0x80 datasn 0

SAMI 9/3: TGT->INTR:Data:
4B643390:          00000402 1F008000 554E482D      ........UNH-
4B6433A0: 494F4C20 66696C65 2D6D6F64 65207461  IOL file-mode ta
4B6433B0: 72676574 312E3220 00000000 00000000  rget1.2 ........
4B6433C0: 00000000 00000000 00000000 00000000  ................
4B6433D0: 00000000 00000000 00000000 00000000  ................
4B6433E0: 00000000 00000000 00000000 00000000  ................
4B6433F0: 00000000 00000000 00000000 00000000  ................
4B643400: 00000000 00000000 00000000 00000000  ................
4B643410: 00000000 00000000 00000000 00000000  ................
4B643420: 00000000 00000000 00000000 00000000  ................
4B643430: 00000000 00000000 00000000 00000000  ................
4B643440: 00000000 00000000 00000000 00000000  ................
4B643450: 00000000 00000000 00000000 00000000  ................
4B643460: 00000000 00000000 00000000 00000000  ................
4B643470: 00000000 00000000 00000000 00000000  ................
4B643480: 00000000 00000000 00000000 00000000  ................
4B643490: 00000000                             ....
SAMI 9/3: iSCSI Event: Data-In: Read (256) bytes of Data Segment
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 21800000 00000000 00000000 00000000  !...............
4B5A7260: 00000005 00000000 00000007 00000006  ................
4B5A7270: 0000000A 00000001 00000000 00000000  ................
4B5A7280:
SAMI 9/3: SCSI Event: Processing inquire LUN response
SAMI 9/3: SCSI Event: Calling Device Add - 4B63DC5C
SAMI 9/3: SCSI Event: scsi add device
SAMI 9/3: SCSI Event: lun_in_inquiry 3
SAMI 9/3: iSCSI Event-Det: handle scsi cmd req
SAMI 9/3: iSCSI Event-Det: run pending queue
SAMI 9/3: iSCSI Event-Det: send scsi command
SAMI 9/3: INTR->TGT HEAD:
493DEE20:                   01C00000 00000000          .@......
493DEE30: 00030000 00000000 00000006 000000FF  ................
493DEE40: 00000006 00000008 12000000 FF000000  ................
493DEE50: 00000000 00000000                    ........
SAMI 9/3: TGT->INTR:Header:
```

```
4B5A7250: 25800000 000000FF 00000000 00000000  %...............
4B5A7260: 00000006 FFFFFFFF 00000000 00000007  ................
4B5A7270: 0000000A 00000000 00000000 00000000  ................
4B5A7280:
SAMI 9/3: iSCSI Event: recv_data for itt 6, cmnd 0x12, bufflen 255, offset 0 exp offset 0,
flags 0x80 datasn 0

SAMI 9/3: TGT->INTR:Data:
4198DBD0: 00000402 1F008000 554E482D 494F4C20  ........UNH-IOL
4198DBE0: 66696C65 2D6D6F64 65207461 72676574  file-mode target
4198DBF0: 312E3220 00000000 00000000 00000000  1.2 ............
4198DC00: 00000000 00000000 00000000 00000000  ................
4198DC10: 00000000 00000000 00000000 00000000  ................
4198DC20: 00000000 00000000 00000000 00000000  ................
4198DC30: 00000000 00000000 00000000 00000000  ................
4198DC40: 00000000 00000000 00000000 00000000  ................
4198DC50: 00000000 00000000 00000000 00000000  ................
4198DC60: 00000000 00000000 00000000 00000000  ................
4198DC70: 00000000 00000000 00000000 00000000  ................
4198DC80: 00000000 00000000 00000000 00000000  ................
4198DC90: 00000000 00000000 00000000 00000000  ................
4198DCA0: 00000000 00000000 00000000 00000000  ................
4198DCB0: 00000000 00000000 00000000 00000000  ................
4198DCC0: 00000000 00000000 00000000 00000000  ................
4198DCD0:
SAMI 9/3: iSCSI Event: Data-In: Read (256) bytes of Data Segment
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 21800000 00000000 0000
Router#0000 00000000  !................
4B5A7260: 00000006 00000000 00000008 00000007  ................
4B5A7270: 0000000B 00000001 00000000 00000000  ................
4B5A7280:
SAMI 9/3: SCSI Event: Processing inquire LUN response
SAMI 9/3: SCSI Event: Calling Device Add - 4B63C60C
SAMI 9/3: SCSI Event: scsi add device
SAMI 9/3: SCSI Event: lun_in_inquiry 4
SAMI 9/3: iSCSI Event-Det: handle scsi cmd req
SAMI 9/3: iSCSI Event-Det: run pending queue
SAMI 9/3: iSCSI Event-Det: send scsi command
SAMI 9/3: INTR->TGT HEAD:
493DEE20:                   01C00000 00000000          .@......
493DEE30: 00040000 00000000 00000007 000000FF  ................
493DEE40: 00000007 00000009 12000000 FF000000  ................
493DEE50: 00000000 00000000                    ........
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 25800000 000000FF 00000000 00000000  %...............
4B5A7260: 00000007 FFFFFFFF 00000000 00000008  ................
4B5A7270: 0000000B 00000000 00000000 00000000  ................
4B5A7280:
SAMI 9/3: iSCSI Event: recv_data for itt 7, cmnd 0x12, bufflen 255, offset 0 exp offset 0,
flags 0x80 datasn 0

SAMI 9/3: TGT->INTR:Data:
4B63C720: 00000402 1F008000 554E482D 494F4C20  ........UNH-IOL
4B63C730: 66696C65 2D6D6F64 65207461 72676574  file-mode target
4B63C740: 312E3220 00000000 00000000 00000000  1.2 ............
4B63C750: 00000000 00000000 00000000 00000000  ................
4B63C760: 00000000 00000000 00000000 00000000  ................
4B63C770: 00000000 00000000 00000000 00000000  ................
4B63C780: 00000000 00000000 00000000 00000000  ................
4B63C790: 00000000 00000000 00000000 00000000  ................
4B63C7A0: 00000000 00000000 00000000 00000000  ................
4B63C7B0: 00000000 00000000 00000000 00000000  ................
4B63C7C0: 00000000 00000000 00000000 00000000  ................
```

```
4B63C7D0: 00000000 00000000 00000000 00000000  ................
4B63C7E0: 00000000 00000000 00000000 00000000  ................
4B63C7F0: 00000000 00000000 00000000 00000000  ................
4B63C800: 00000000 00000000 00000000 00000000  ................
4B63C810: 00000000 00000000 00000000 00000000  ................
4B63C820:
SAMI 9/3: iSCSI Event: Data-In: Read (256) bytes of Data Segment
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 21800000 00000000 00000000 00000000  !...............
4B5A7260: 00000007 00000000 00000009 00000008  ................
4B5A7270: 0000000C 00000001 00000000 00000000  ................
4B5A7280:
SAMI 9/3: SCSI Event: Processing inquire LUN response
SAMI 9/3: SCSI Event: Calling Device Add - 493A3378
SAMI 9/3: SCSI Event: scsi add device
SAMI 9/3: SCSI Event: max= 5 lun_in_inquiry= 5
SAMI 9/3: iSCSI Event-Det: handle scsi cmd req
SAMI 9/3: iSCSI Event-Det: run pending queue
SAMI 9/3: iSCSI Event-Det: send scsi command
SAMI 9/3: INTR->TGT HEAD:
493DEE20:                   01C00000 00000000          .@......
493DEE30: 00000000 00000000 00000008 000000FF  ................
493DEE40: 00000008 0000000A 25000000 00000000  ........%.......
493DEE50: 00000000 00000000                     ........
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 25800000 00000008 00000000 00000000  %...............
4B5A7260: 00000008 FFFFFFFF 00000000 00000009  ................
4B5A7270: 0000000C 00000000 00000000 00000000  ................
4B5A7280:
SAMI 9/3: iSCSI Event: recv_data for itt 8, cmnd 0x25, bufflen 255, offset 0 exp offset 0,
flags 0x80 datasn 0

SAMI 9/3: TGT->INTR:Data:
493D65D0:                   003FFFFF 00000200          .?......
493D65E0:
SAMI 9/3: iSCSI Event: Data-In: Read (8) bytes of Data Segment
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 21820000 00000000 00000000 00000000  !...............
4B5A7260: 00000008 00000000 0000000A 00000009  ................
4B5A7270: 0000000D 00000001 00000000 000000F7  ................w
4B5A7280:
SAMI 9/3: SCSI Event: Processing read capacity response
SAMI 9/3: SCSI Event: max= 5 lun= 1
SAMI 9/3: iSCSI Event-Det: handle scsi cmd req
SAMI 9/3: iSCSI Event-Det: run pending queue
SAMI 9/3: iSCSI Event-Det: send scsi command
SAMI 9/3: INTR->TGT HEAD:
493DEE20:                   01C00000 00000000          .@......
493DEE30: 00010000 00000000 00000009 000000FF  ................
493DEE40: 00000009 0000000B 25000000 00000000  ........%.......
493DEE50: 00000000 00000000                     ........
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 25800000 00000008 00000000 00000000  %...............
4B5A7260: 00000009 FFFFFFFF 00000000 0000000A  ................
4B5A7270: 0000000D 00000000 00000000 00000000  ................
4B5A7280:
SAMI 9/3: iSCSI Event: recv_data for itt 9, cmnd 0x25, bufflen 255, offset 0 exp offset 0,
flags 0x80 datasn 0

SAMI 9/3: TGT->INTR:Data:
41637830:                           003FFFFF              .?..
41637840: 00000200                              ....
SAMI 9/3: iSCSI Event: Data-In: Read (8) bytes of Data Segment
SAMI 9/3: TGT->INTR:Header:
```

```
4B5A7250: 21820000 00000000 00000000 00000000  !...............
4B5A7260: 00000009 00000000 0000000B 0000000A  ................
4B5A7270: 0000000E 00000001 00000000 000000F7  ...............w
4B5A7280:
SAMI 9/3: SCSI Event: Processing read capacity response
SAMI 9/3: SCSI Event: max= 5 lun= 2
SAMI 9/3: iSCSI Event-Det: handle scsi cmd req
SAMI 9/3: iSCSI Event-Det: run pending queue
SAMI 9/3: iSCSI Event-Det: send scsi command
SAMI 9/3: INTR->TGT HEAD:
493DEE20:                   01C00000 00000000          .@......
493DEE30: 00020000 00000000 0000000A 000000FF  ................
493DEE40: 0000000A 0000000C 25000000 00000000  ........%.......
493DEE50: 00000000 00000000                     ........
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 25800000 00000008 00000000 00000000  %...............
4B5A7260: 0000000A FFFFFFFF 00000000 0000000B  ................
4B5A7270: 0000000E 00000000 00000000 00000000  ................
4B5A7280:
SAMI 9/3: iSCSI Event: recv_data for itt 10, cmnd 0x25, bufflen 255, offset 0 exp offset
0, flags 0x80 datasn 0

SAMI 9/3: TGT->INTR:Data:
4ADE19D0:                           003FFFFF              .?..
4ADE19E0: 00000200                                  ....
SAMI 9/3: iSCSI Event: Data-In: Read (8) bytes of Data Segment
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 21820000 00000000 00000000 00000000  !...............
4B5A7260: 0000000A 00000000 0000000C 0000000B  ................
4B5A7270: 0000000F 00000001 00000000 000000F7  ...............w
4B5A7280:
SAMI 9/3: SCSI Event: Processing read capacity response
SAMI 9/3: SCSI Event: max= 5 lun= 3
SAMI 9/3: iSCSI Event-Det: handle scsi cmd req
SAMI 9/3: iSCSI Event-Det: run pending queue
SAMI 9/3: iSCSI Event-Det: send scsi command
SAMI 9/3: INTR->TGT HEAD:
493DEE20:                   01C00000 00000000          .@......
493DEE30: 00030000 00000000 0000000B 000000FF  ................
493DEE40: 0000000B 0000000D 25000000 00000000  ........%.......
493DEE50: 00000000 00000000                     ........
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 25800000 00000008 00000000 00000000  %...............
4B5A7260: 0000000B FFFFFFFF 00000000 0000000C  ................
4B5A7270: 0000000F 00
Router#000000 00000000 00000000  ................
4B5A7280:
SAMI 9/3: iSCSI Event: recv_data for itt 11, cmnd 0x25, bufflen 255, offset 0 exp offset
0, flags 0x80 datasn 0

SAMI 9/3: TGT->INTR:Data:
4ADE1B10: 003FFFFF 00000200                    .?......
SAMI 9/3: iSCSI Event: Data-In: Read (8) bytes of Data Segment
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 21820000 00000000 00000000 00000000  !...............
4B5A7260: 0000000B 00000000 0000000D 0000000C  ................
4B5A7270: 00000010 00000001 00000000 000000F7  ...............w
4B5A7280:
SAMI 9/3: SCSI Event: Processing read capacity response
SAMI 9/3: SCSI Event: max= 5 lun= 4
SAMI 9/3: iSCSI Event-Det: handle scsi cmd req
SAMI 9/3: iSCSI Event-Det: run pending queue
SAMI 9/3: iSCSI Event-Det: send scsi command
SAMI 9/3: INTR->TGT HEAD:
```

```
493DEE20:                   01C00000 00000000          .@......
493DEE30: 00040000 00000000 0000000C 000000FF  ................
493DEE40: 0000000C 0000000E 25000000 00000000  ........%.......
493DEE50: 00000000 00000000                     ........
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 25800000 00000008 00000000 00000000  %...............
4B5A7260: 0000000C FFFFFFFF 00000000 0000000D  ................
4B5A7270: 00000010 00000000 00000000 00000000  ................
4B5A7280:
SAMI 9/3: iSCSI Event: recv_data for itt 12, cmnd 0x25, bufflen 255, offset 0 exp offset
0, flags 0x80 datasn 0

SAMI 9/3: TGT->INTR:Data:
4B642580:                           0003FFFF              ....
4B642590: 00000200                              ....
SAMI 9/3: iSCSI Event: Data-In: Read (8) bytes of Data Segment
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 21820000 00000000 00000000 00000000  !...............
4B5A7260: 0000000C 00000000 0000000E 0000000D  ................
4B5A7270: 00000011 00000001 00000000 000000F7  ................w
4B5A7280:
SAMI 9/3: SCSI Event: Processing read capacity response
SAMI 9/3: SCSI Event: Max= 5 lun= 5
SAMI 9/3: SCSI Event: device discovery completed
SAMI 9/3: SCSI Event:
Creating File System on sda0
SAMI 9/3: SCSI Event: Read command, lba(0), nblocks(1)
SAMI 9/3: iSCSI Event-Det: handle scsi cmd req
SAMI 9/3: iSCSI Event-Det: run pending queue
SAMI 9/3: iSCSI Event-Det: send scsi command
SAMI 9/3: INTR->TGT HEAD:
493DEE20:                   01C00000 00000000          .@......
493DEE30: 00000000 00000000 0000000D 00000200  ................
493DEE40: 0000000D 0000000F 28000000 00000000  ........(.......
493DEE50: 01000000 00000000                     ........
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 25800000 00000200 00000000 00000000  %...............
4B5A7260: 0000000D FFFFFFFF 00000000 0000000E  ................
4B5A7270: 00000011 00000000 00000000 00000000  ................
4B5A7280:
SAMI 9/3: iSCSI Event: recv_data for itt 13, cmnd 0x28, bufflen 512, offset 0 exp offset
0, flags 0x80 datasn 0

SAMI 9/3: TGT->INTR:Data:
4B5A8B00: 00000000 00000000 00000000 00000000  ................
4B5A8B10: 00000000 00000000 00000000 00000000  ................
4B5A8B20: 00000000 00000000 00000000 00000000  ................
4B5A8B30: 00000000 00000000 00000000 00000000  ................
4B5A8B40: 00000000 00000000 00000000 00000000  ................
4B5A8B50: 00000000 00000000 00000000 00000000  ................
4B5A8B60: 00000000 00000000 00000000 00000000  ................
4B5A8B70: 00000000 00000000 00000000 00000000  ................
4B5A8B80: 00000000 00000000 00000000 00000000  ................
4B5A8B90: 00000000 00000000 00000000 00000000  ................
4B5A8BA0: 00000000 00000000 00000000 00000000  ................
4B5A8BB0: 00000000 00000000 00000000 00000000  ................
4B5A8BC0: 00000000 00000000 00000000 00000000  ................
4B5A8BD0: 00000000 00000000 00000000 00000000  ................
4B5A8BE0: 00000000 00000000 00000000 00000000  ................
4B5A8BF0: 00000000 00000000 00000000 00000000  ................
4B5A8C00: 00000000 00000000 00000000 00000000  ................
4B5A8C10: 00000000 00000000 00000000 00000000  ................
4B5A8C20: 00000000 00000000 00000000 00000000  ................
4B5A8C30: 00000000 00000000 00000000 00000000  ................
```

```
4B5A8C40: 00000000 00000000 00000000 00000000  ................
4B5A8C50: 00000000 00000000 00000000 00000000  ................
4B5A8C60: 00000000 00000000 00000000 00000000  ................
4B5A8C70: 00000000 00000000 00000000 00000000  ................
4B5A8C80: 00000000 00000000 00000000 00000000  ................
4B5A8C90: 00000000 00000000 00000000 00000000  ................
4B5A8CA0: 00000000 00000000 00000000 00000000  ................
4B5A8CB0: 00000000 00000000 E6F06A79 00000000  ........fpjy....
4B5A8CC0: 00000000 00000000 00000000 00000000  ................
4B5A8CD0: 00000000 00000000 00000000 00000000  ................
4B5A8CE0: 00000000 00000000 00000000 00000000  ................
4B5A8CF0: 00000000 00000000 00000000 000055AA  ..............U*
4B5A8D00:
SAMI 9/3: iSCSI Event: Data-In: Read (512) bytes of Data Segment
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 21800000 00000000 00000000 00000000  !...............
4B5A7260: 0000000D 00000000 0000000F 0000000E  ................
4B5A7270: 00000012 00000001 00000000 00000000  ................
4B5A7280:
SAMI 9/3: SCSI Event:
Creating File System on sda1
SAMI 9/3: SCSI Event: Read command, lba(0), nblocks(1)
SAMI 9/3: iSCSI Event-Det: handle scsi cmd req
SAMI 9/3: iSCSI Event-Det: run pending queue
SAMI 9/3: iSCSI Event-Det: send scsi command
SAMI 9/3: INTR->TGT HEAD:
493DEE20:                   01C00000 00000000          .@......
493DEE30: 00010000 00000000 0000000E 00000200  ................
493DEE40: 0000000E 00000010 28000000 00000000  ........(.......
493DEE50: 01000000 00000000                    ........
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 25800000 00000200 00000000 00000000  %...............
4B5A7260: 0000000E FFFFFFFF 00000000 0000000F  ................
4B5A7270: 00000012 00000000 00000000 00000000  ................
4B5A7280:
SAMI 9/3: iSCSI Event: recv_data for itt 14, cmnd 0x28, bufflen 512, offset 0 exp offset
0, flags 0x80 datasn 0

SAMI 9/3: TGT->INTR:Data:
4B5A8B00: 33C08ED0 BC007CFB 5007501F FCBE1B7C  3@.P<.|{P.P.|>.|
4B5A8B10: BF1B0650 57B9E501 F3A4CBBD BE07B104  ?..PW9e.s$K=>.1.
4B5A8B20: 386E007C 09751383 C510E2F4 CD188BF5  8n.|.u..E.btM..u
4B5A8B30: 83C61049 7419382C 74F6A0B5 07B4078B  .F.It.8,tv 5.4..
4B5A8B40: F0AC3C00 74FCBB07 00B40ECD 10EBF288  p,<.t|;..4.M.kr.
4B5A8B50: 4E10E846 00732AFE 4610807E 040B740B  N.hF.s*~F..~..t.
4B5A8B60: 807E040C 7405A0B6 0775D280 46020683  .~..t. 6.uR.F...
4B5A8B70: 46080683 560A00E8 21007305 A0B607EB  F...V..h!.s. 6.k
4B5A8B80: BC813EFE 7D55AA74 0B807E10 0074C8A0  <.>~}U*t..~..tH
4B5A8B90: B707EBA9 8BFC1E57 8BF5CBBF 05008A56  7.k).|.W.uK?...V
4B5A8BA0: 00B408CD 1372238A C1243F98 8ADE8AFC  .4.M.r#.A$?..^.|
4B5A8BB0: 43F7E38B D186D6B1 06D2EE42 F7E23956  Cwc.Q.V1.RnBwb9V
4B5A8BC0: 0A772372 05394608 731CB801 02BB007C  .w#r.9F.s.8..;.|
4B5A8BD0: 8B4E028B 5600CD13 73514F74 4E32E48A  .N..V.M.sQOtN2d.
4B5A8BE0: 5600CD13 EBE48A56 0060BBAA 55B441CD  V.M.kd.V.`;*U4AM
4B5A8BF0: 13723681 FB55AA75 30F6C101 742B6160  .r6.{U*u0vA.t+a`
4B5A8C00: 6A006A00 FF760AFF 76086A00 68007C6A  j.j..v..v.j.h.|j
4B5A8C10: 016A10B4 428BF4CD 13616173 0E4F740B  .j.4B.tM.aas.Ot.
4B5A8C20: 32E48A56 00CD13EB D661F9C3 496E7661  2d.V.M.kVayCInva
4B5A8C30: 6C696420 70617274 6974696F 6E207461  lid partition ta
4B5A8C40: 626C6500 4572726F 72206C6F 6164696E  ble.Error loadin
4B5A8C50: 67206F70 65726174 696E6720 73797374  g operating syst
4B5A8C60: 656D004D 69737369 6E67206F 70657261  em.Missing opera
4B5A8C70: 74696E67 20737973 74656D00 00000000  ting system.....
4B5A8C80: 00000000 00000000 00000000 00000000  ................
```

```
4B5A8C90: 00000000 00000000 00000000 00000000  ................
4B5A8CA0: 00000000 00000000 00000000 00000000  ................
4B5A8CB0: 00000000 002C4463 656289D3 00000000  .....,Dceb.S....
4B5A8CC0: 00000000 00000000 00000000 00000000  ................
4B5A8CD0: 00000000 00000000 00000000 00000000  ................
4B5A8CE0: 00000000 00000000 00000000 00000000  ................
4B5A8CF0: 00000000 00000000 00000000 000055AA  ..............U*
4B5A8D00:
SAMI 9/3: iSCSI Event: Data-In: Read (512) bytes of Data Segment
SAMI 9/3: TGT->INTR:Header:
4B5A7250:
SAMI 9/3: %SYS-5-CONFIG_I: Configured from console by console
SAMI 9/3: %RSM-4-UNEXPECTED: Error: Drive sda4 unusable (Invalid DOS media or no media in
slot) -Process= "RSM Process", ipl= 0, pid= 193,  -Traceback= 0x446E45DC 0x442AD9BC
0x442AB94C 0x442A6318 0x442A648C 0x442AB41C 0x442A3B28 0x45602878 0x45605C50
SAMI 9/3: %GPRSISCSIFLTMG-4-GPRS_ISCSI_OPEN_SUCCESS: Succeeded to establish connection
with SAN with session id 13
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 20800000 00000000 00000000 00000000   ................
4B5A7260: FFFFFFFF 0000001C 0000001E 0000001C  ................
4B5A7270: 00000020 00000000 00000000 00000000  ... ............
4B5A7280:
SAMI 9/3: INTR->TGT (HEADER + DATA):
4B5A5B50: 40800000 00000000 00000000 00000000  @...............
4B5A5B60: FFFFFFFF 0000001C 0000001C 0000001E  ................
4B5A5B70: 00000000 00000000 00000000 00000000  ................
4B5A5B80:
SAMI 9/3: iSCSI Event-Det: Connection timer event (0)
SAMI 9/3: iSCSI Event: FFP Timeout Event Active Tasks(0)
SAMI 9/3: iSCSI Event: Starting Full Feature Phase Timer (5)
SAMI 9/3: INTR->TGT (HEADER + DATA):
4B5A5B50: 40800000 00000000 00000000 00000000  @...............
4B5A5B60: 0000001C FFFFFFFF 0000001C 0000001E  ................
4B5A5B70: 00000000 00000000 00000000 00000000  ................
4B5A5B80:
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 20800000 00000000 00000000 00000000   ................
4B5A7260: 0000001C FFFFFFFF 0000001E 0000001C  ................
4B5A7270: 00000020 00000000 00000000 00000000  ... ............
4B5A7280:
SAMI 9/3: iSCSI Event-Det: Connection timer event (0)
SAMI 9/3: iSCSI Event: FFP Timeout Event Active Tasks(0)
SAMI 9/3: iSCSI Event: Starting Full Feature Phase Timer (5)
SAMI 9/3: INTR->TGT (HEADER + DATA):
4B5A5B50: 40800000 00000000 00000000 00000000  @...............
4B5A5B60: 0000001D FFFFFFFF 0000001C 0000001F  ................
4B5A5B70: 00000000 00000000 00000000 00000000  ................
4B5A5B80:
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 20800000 00000000 00000000 00000000   ................
4B5A7260: 0000001D FFFFFFFF 0000001F 0000001C  ................
4B5A7270: 00000020 00000000 00000000 00000000  ... ............
4B5A7280:
SAMI 9/3: iSCSI Event-Det: Connection timer event (0)
SAMI 9/3: iSCSI Event: FFP Timeout Event Active Tasks(0)
SAMI 9/3: iSCSI Event: Starting Full Feature Phase Timer (5)
SAMI 9/3: INTR->TGT (HEADER + DATA):
4B5A5B50: 40800000 00000000 00000000 00000000  @...............
4B5A5B60: 0000001E FFFFFFFF 0000001C 00000020  ................
4B5A5B70: 00000000 00000000 00000000 00000000  ................
4B5A5B80:
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 20800000 00000000 00000000 00000000   ................
4B5A7260: 0000001E FFFFFFFF 00000020 0000001C  ........... ....
```

```
4B5A7270: 00000020 00000000 00000000 00000000  ... ............
4B5A7280:
SAMI 9/3: iSCSI Event-Det: Connection timer event (0)
SAMI 9/3: iSCSI Event: FFP Timeout Event Active Tasks(0)
SAMI 9/3: iSCSI Event: Starting Full Feature Phase Timer (5)
SAMI 9/3: INTR->TGT (HEADER + DATA):
4B5A5B50: 40800000 00000000 00000000 00000000  @...............
4B5A5B60: 0000001F FFFFFFFF 0000001C 00000021  ...............!
4B5A5B70: 00000000 00000000 00000000 00000000  ................
4B5A5B80:
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 20800000 00000000 00000000 00000000   ...............
4B5A7260: 0000001F FFFFFFFF 00000021 0000001C  ...........!....
4B5A7270: 00000020 00000000 00000000 00000000  ... ............
4B5A7280:
SAMI 9/3: iSCSI Event-Det: Connection timer event (0)
SAMI 9/3: iSCSI Event: FFP Timeout Event Active Tasks(0)
SAMI 9/3: iSCSI Event: Starting Full Feature Phase Timer (5)
SAMI 9/3: INTR->TGT (HEADER + DATA):
4B5A5B50: 40800000 00000000 00000000 00000000  @...............
4B5A5B60: 00000020 FFFFFFFF 0000001C 00000022  ... ...........".
4B5A5B70: 00000000 00000000 00000000 00000000  ................
4B5A5B80:
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 20800000 00000000 00000000 00000000   ...............
4B5A7260: 00000020 FFFFFFFF 00000022 0000001C  ... .......".....
4B5A7270: 00000020 00000000 00000000 00000000  ... ............
4B5A7280:
SAMI 9/3: iSCSI Event-Det: Connection timer event (0)
SAMI 9/3: iSCSI Event: FFP Timeout Event Active Tasks(0)
SAMI 9/3: iSCSI Event: Starting Full Feature Phase Timer (5)
SAMI 9/3: INTR->TGT (HEADER + DATA):
4B5A5B50: 40800000 00000000 00000000 00000000  @...............
4B5A5B60: 00000021 FFFFFFFF 0000001C 00000023  ...!...........#
4B5A5B70: 00000000 00000000 00000000 00000000  ................
4B5A5B80:
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 20800000 00000000 00000000 00000000   ...............
4B5A7260: 00000021 FFFFFFFF 00000023 0000001C  ...!.......#....
4B5A7270: 00000020 00000000 00000000 00000000  ... ............
4B5A7280:
SAMI 9/3: iSCSI Event-Det: Connection timer event (0)
SAMI 9/3: iSCSI Event: FFP Timeout Event Active Tasks(0)
SAMI 9/3: iSCSI Event: Starting Full Feature Phase Timer (5)
SAMI 9/3: INTR->TGT (HEADER + DATA):
4B5A5B50: 40800000 00000000 00000000 00000000  @...............
4B5A5B60: 00000022 FFFFFFFF 0000001C 00000024  ..."...........$
4B5A5B70: 00000000 00000000 00000000 00000000  ................
4B5A5B80:
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 20800000 00000000 00000000 00000000   ...............
4B5A7260: 00000022 FFFFFFFF 00000024 0000001C  ..."....... $....
4B5A7270: 00000020 00000000 00000000 00000000  ... ............
4B5A7280:
SAMI 9/3: iSCSI Event-Det: Connection timer event (0)
SAMI 9/3: iSCSI Event: FFP Timeout Event Active Tasks(0)
SAMI 9/3: iSCSI Event: Starting Full Feature Phase Timer (5)
SAMI 9/3: INTR->TGT (HEADER + DATA):
4B5A5B50: 40800000 00000000 00000000 00000000  @...............
4B5A5B60: 00000023 FFFFFFFF 0000001C 00000025  ...#...........%
4B5A5B70: 00000000 00000000 00000000 00000000  ................
Router#
4B5A5B80:
SAMI 9/3: TGT->INTR:Header:
```

```
4B5A7250: 20800000 00000000 00000000 00000000   ................
4B5A7260: 00000023 FFFFFFFF 00000025 0000001C  ...#.......%....
4B5A7270: 00000020 00000000 00000000 00000000  ... ............
4B5A7280:
SAMI 9/3: iSCSI Event-Det: Connection timer event (0)
SAMI 9/3: iSCSI Event: FFP Timeout Event Active Tasks(0)
SAMI 9/3: iSCSI Event: Starting Full Feature Phase Timer (5)
SAMI 9/3: INTR->TGT (HEADER + DATA):
4B5A5B50: 40800000 00000000 00000000 00000000  @...............
4B5A5B60: 00000024 FFFFFFFF 0000001C 00000026  ...$...........&
4B5A5B70: 00000000 00000000 00000000 00000000  ................
4B5A5B80:
SAMI 9/3: TGT->INTR:Header:
4B5
Router#
Router#
Router#A7250: 20800000 00000000 00000000 00000000   ................
4B5A7260: 00000024 FFFFFFFF 00000026 0000001C  ...$.......&....
4B5A7270: 00000020 00000000 00000000 00000000  ... ............
4B5A7280:
Router#
Router#
SAMI 9/3: iSCSI Event-Det: Connection timer event (0)
SAMI 9/3: iSCSI Event: FFP Timeout Event Active Tasks(0)
SAMI 9/3: iSCSI Event: Starting Full Feature Phase Timer (5)
SAMI 9/3: INTR->TGT (HEADER + DATA):
4B5A5B50: 40800000 00000000 00000000 00000000  @...............
4B5A5B60: 00000025 FFFFFFFF 0000001C 00000027  ...%...........'
4B5A5B70: 00000000 00000000 00000000 00000000  ................
4B5A5B80:
SAMI 9/3: TGT->INTR:Header:
4B5A7250: 20800000 00000000 00000000 00000000   ................
4B5A7260: 00000025 FFFFFFFF 00000027 0000001C  ...%.......'....
4B5A7270:un al 00000020 00000000 00000000 00000000  ... ............
4B5A7280:                                                        l
All possible debugging has been turned off
Router#sh ip iscsi session
ID        TARGET             STATE                CONNECTIONS
-----------------------------------------------------------------
13        LINUX              Logged In            1

================================================
```

debug record-storage-module

To display debugging information related to the record storage module (RSM), use the **debug record-storage-module** command in privileged EXEC model. To disable debugging output, use the **no** form of this command.

debug record-storage-module [**all** | **dsm** | **error** | **event**]

no debug record-storage-module [**all** | **dsm** | **error** | **event**]

Syntax Description

all	Displays all RSM flags.
dsm	Displays data store manager debug information.
error	Displays RSM-related errors.
event	Displays RSM-related events.

Defaults

No default behavior or values.

Command History

Release	Modification
12.4(15)XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

This command is useful for system operators and development engineers if problems are encountered with communication between the GGSN and the SCSI target.

Examples

The following example displays RSM-related debugging at the time of the write process:

```
Router#
SAMI 9/3: %GPRSFLTMG-4-CHARGING: GSN: 32.0.0.2, TID: 0000000000000000, APN: NULL, Reason:
3, GSN GTP' Transfer Failure
Router#
SAMI 9/3: RSM-Event-Det: Write by appl GGSN for profile LINUX
SAMI 9/3: RSM-FUNC: Write Handler
SAMI 9/3: RSM-DSM-DET: Allocate write buffer
SAMI 9/3: RSM-DSM-DET: rem_len= 260966, bytes= 1178
SAMI 9/3: RSM-DSM: Write to file now
SAMI 9/3: RSM-DSM-DET: sda3:/root/00000001/00000001.dat exists
SAMI 9/3: RSM-DSM: Size of sda3:/root/00000001/00000001.dat is 780686
SAMI 9/3: RSM-DSM-DET: Write to sda3:/root/00000001/00000001.dat
SAMI 9/3: RSM-DSM-DET: sda3:/root/00000001/00000001.dat size is 781864 bytes
SAMI 9/3: RSM-DSM-DET: Call the write response handler
Router#show debug
Record Storage Module:
  RSM DSM debugging is on
  RSM DSM DETAIL debugging is on
  RSM EVENT DETAIL debugging is on
  RSM EVENT debugging is on
  RSM ERROR debugging is on
```

The following example displays RSM-related debugging at the time of the read process:

```
Router#
SAMI 9/3: RSM-Event-Det: Read by appl GGSN for profile LINUX
SAMI 9/3: RSM-DSM-DET: Allocate read buffer
SAMI 9/3: RSM-DSM-DET: Data buffer empty, read from disk
SAMI 9/3: RSM-DSM: Read from file sda3:/root/00000001/00000001.dat
SAMI 9/3: RSM-DSM-DET: Read fd is illegal in drive sda3
SAMI 9/3: RSM-DSM-DET: sda3:/root/00000001/00000001.dat exists
SAMI 9/3: RSM-DSM-DET: Read from off = 778460
SAMI 9/3: RSM-FUNC: Read in buffer
SAMI 9/3: RSM-DSM-DET: Read 262144 byte from sda3:/root/00000001/00000001.dat
SAMI 9/3: RSM-DSM-DET: Complete Record, next rec offset= 262
SAMI 9/3: RSM-Event-Det: Read record= 246 bytes
SAMI 9/3: RSM-Event-Det: Read by appl GGSN for profile LINUX
SAMI 9/3: RSM-DSM-DET: Complete Record, next rec offset= 524
SAMI 9/3: RSM-Event-Det: Read record= 246 bytes
SAMI 9/3: RSM-Event-Det: Read by appl GGSN for profile LINUX
SAMI 9/3: RSM-DSM-DET: Complete Record, next rec offset= 786
SAMI 9/3: RSM-Event-Det: Read record= 246 bytes
SAMI 9/3: RSM-Event-Det: Read by appl GGSN for profile LINUX
SAMI 9/3: RSM-DSM-DET: Complete Record, next rec offset= 1048
SAMI 9/3: RSM-Event-Det: Read record= 246 bytes
SAMI 9/3: RSM-Event-Det: Read by appl GGSN for profile LINUX
SAMI 9/3: RSM-DSM-DET: Complete Record, next rec offset= 2226
SAMI 9/3: RSM-Event-Det: Read record= 1162 bytes
SAMI 9/3: RSM-Event-Det: Read by appl GGSN for profile LINUX
SAMI 9/3: RSM-DSM-DET: Complete Record, next rec offset= 3404
SAMI 9/3: RSM-Event-Det: Read record= 1162 bytes
SAMI 9/3: RSM-Event-Det: Read by appl GGSN for profile LINUX
SAMI 9/3: RSM-DSM-DET: Next Record is not in buffer
SAMI 9/3: RSM-FUNC: Copy partial record to next buffer
SAMI 9/3: RSM-DSM-DET: copy= 0 bytes from offset= 3404 to offset= 2016
SAMI 9/3: RSM-DSM-DET: Data buffer empty, read from disk
SAMI 9/3: RSM-DSM: Read from file sda3:/root/00000001/00000001.dat
SAMI 9/3: RSM-FUNC: Read in buffer
SAMI 9/3: RSM-DSM-DET: Read 262144 byte from sda3:/root/00000001/00000001.dat
SAMI 9/3: RSM-DSM-DET: Chk if more data exists
SAMI 9/3: RSM-DSM-DET: Get next read file
SAMI 9/3: RSM-DSM-DET: sda3:/root/00000001/00000002.dat (File not found)
SAMI 9/3: RSM-DSM-DET: Get next read dir
SAMI 9/3: RSM-DSM-DET: sda3:/root/00000002/ does not exist
SAMI 9/3: RSM-DSM: Check next read drive sda3
SAMI 9/3: RSM-DSM: file sda3:/root/00000001/00000001.dat is the file currently read
SAMI 9/3: RSM-Error: Disk is empty
SAMI 9/3: RSM-DSM: Zero bytes read
SAMI 9/3: RSM-DSM-DET: Bytes in write buffer = 0
SAMI 9/3: RSM-Event: Disk is empty-No more records to Read
SAMI 9/3: RSM-Event-Det: Read record= 0 bytes
SAMI 9/3: RSM-Event-Det: Read by appl GGSN for profile LINUX
SAMI 9/3: RSM-DSM-DET: Bytes in write buffer = 0
SAMI 9/3: RSM-Event: Disk is empty-No more records to Read
SAMI 9/3: RSM-Event-Det: Read record= 0 bytes
SAMI 9/3: RSM-Event-Det: Read by appl GGSN for profile LINUX
SAMI 9/3: RSM-DSM-DET: Bytes in write buffer = 0
SAMI 9/3: RSM-Event: Disk is empty-No more records to Read
SAMI 9/3: RSM-Event-Det: Read record= 0 bytes
SAMI 9/3: RSM-Event-Det: Read by appl GGSN for profile LINUX
SAMI 9/3: RSM-DSM-DET: Bytes in write buffer = 0
SAMI 9/3: RSM-Event: Disk is empty-No more records to Read
SAMI 9/3: RSM-Event-Det: Read record= 0 bytes
SAMI 9/3: RSM-Event-Det: Read by appl GGSN for profile LINUX
SAMI 9/3: RSM-DSM-DET: Bytes in write buffer = 0
SAMI 9/3: RSM-Event: Disk is empty-No more records to Read
```

```
SAMI 9/3: RSM-Event-Det: Read record= 0 bytes
SAMI 9/3: RSM-Event-Det: Read by appl GGSN for profile LINUX
SAMI 9/3: RSM-DSM-DET: Bytes in write buffer = 0
SAMI 9/3: RSM-Event: Disk is empty-No more records to Read
SAMI 9/3: RSM-Event-Det: Read record= 0 bytes
```