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-nam*e 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.
   -
     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.