gprs gtp echo-timer dynamic enable

To enable the dynamic echo timer on the gateway GPRS support node (GGSN), use the **gprs gtp echo-timer dynamic enable** command in global configuration mode. To disable the dynamic echo timer, use the **no** form of this command.

gprs gtp echo-timer dynamic enable

no gprs gtp echo-timer dynamic enable

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

For a GPRS tunneling protocol (GTP) path to be active, the serving GPRS support node (SGSN) needs to be active. To determine that an SGSN is active, the GGSN and SGSN exchange echo messages. Although the GGSN supports different methods of echo message timing, the basic echo flow begins when the GGSN sends an echo request message to the SGSN. The SGSN sends a corresponding echo response message back to the GGSN.

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

The GGSN supports two different methods of echo timing—the default echo timer and the dynamic echo timer.

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

Default echo timer

The dynamic echo timer is based on the default echo timer in the GGSN. A description of the default echo timer follows as a means of comparison.

The default echo timer configuration uses the following commands:

- **gprs gtp n3-requests**—Specifies maximum number of times that the GGSN attempts to send a echo-request message. The default is 5 times.
- **gprs gtp path-echo-interval**—Specifies the number of seconds that the GGSN waits before sending an echo-request message. The default is 60 seconds.
- **gprs gtp t3-response**—Specifies the number of seconds that the GGSN waits before resending an echo-request message after the path echo interval has expired and the echo response has not been received. The default is 1 second.

If the GGSN receives the echo response within the path echo interval (as specified in the **gprs gtp path-echo-interval** command; default is 60 seconds), it sends another echo request message after 60 seconds (or whatever time was configured in the **gprs gtp path-echo-interval** command). This message flow continues as long as the GGSN receives an echo response message within the specified path echo interval.

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

For example, if N3 is set to the default of 5, and T3 is set to the default of 1 second, the GGSN will resend 4 echo request messages (the initial request + 4 retries = 5). The T3 time increments for each additional echo request by a factor of 2 seconds. So, the GGSN resends a message in 2 seconds, 4 seconds, 8 seconds, and 16 seconds. If the GGSN fails to receive an echo response message within the time period of the N3-requests counter, it clears the GTP path and deletes all the PDP contexts.

For the above example, the total elapsed time from when the first request message is sent, to when the GTP path is cleared, is: 60 + 2 + 4 + 8 + 16 = 90 seconds,

where 60 is the initial value of the path echo interval, and the remaining four time periods are the increments of the T3 timer for the subsequent retries.

Dynamic echo timer

The dynamic echo timer method is different from the default echo timer method on the GGSN because it uses a calculated round-trip time (RTT), as well as a configurable factor or multiplier to be applied to the RTT statistic.

The dynamic echo timer configuration uses the following commands:

- **gprs gtp echo-timer dynamic enable**—Enables the dynamic echo timer on the GGSN.
- **gprs gtp echo-timer dynamic minimum**—Specifies the minimum time period (in seconds) for the dynamic echo timer. If the RTT is less than this value, the GGSN uses the value set in this command.
- **gprs gtp echo-timer dynamic smooth-factor**—Configures the multiplier that the dynamic echo timer uses when calculating the time to wait to send retries, when it has not received a response from the SGSN within the path echo interval.

- **gprs gtp n3-requests**—Specifies the maximum number of times that the GGSN attempts to send an echo-request message. The default is 5 times.
- **gprs gtp path-echo-interval**—Specifies the number of seconds within which the GGSN expects to receive an echo response. This is the period of time that the GGSN waits before sending another echo-request message. The default is 60 seconds.

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

If the GGSN fails to receive an echo response message within the path echo interval, the GGSN goes into retransmission, or path failure mode. During path failure mode, the GGSN uses a value referred to as the T-dynamic. The T-dynamic is the greater of either the dynamic minimum, or the RTT statistic multiplied by the smooth factor.

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

For example, if the RTT is 6 seconds, N3 is set to 5, and the smooth factor is set to 3, the GGSN will resend 4 echo request messages in path failure mode. The T-dynamic value is 18 (RTT x smooth factor), so the GGSN sends a retry echo request message in 36 seconds, 72 seconds, 144 seconds, and 288 seconds. If the GGSN fails to receive an echo response message in this time period, it clears the GTP path and deletes all PDP contexts. The total elapsed time from when the first request message is sent to when the GTP path is cleared is: 60 + 36 + 72 + 144 + 288 = 600 seconds,

where 60 is the initial value of the path echo interval, and the remaining 4 time periods are the increments of the T-dynamic for the subsequent retries.

Examples

The following example turns on the dynamic echo timer, sets the minimum value to 5 seconds, and configures a smooth factor of 3:

```
gprs gtp echo-timer dynamic enable
gprs gtp echo-timer dynamic minimum 5
gprs gtp echo-timer dynamic smooth-factor 3
```

Related Commands

Command	Description
gprs gtp echo-timer dynamic minimum	Specifies the minimum time period used by the dynamic echo timer.
gprs gtp echo-timer dynamic smooth-factor	Configures the multiplier that the GGSN uses to calculate the time to wait to send retries of the dynamic echo timer.
gprs gtp n3-requests	Specifies the maximum number of times that the GGSN attempts to send a signaling request.
gprs gtp path-echo-interval	Specifies the number of seconds that the GGSN waits before sending an echo-request message.

gprs gtp echo-timer dynamic minimum

To specify the minimum time period used by the dynamic echo timer, use the **gprs gtp echo-timer dynamic minimum** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs gtp echo-timer dynamic minimum *number*

no gprs gtp echo-timer dynamic minimum *number*

Syntax Description

number	Minimum time period (between 1 and 60 seconds) of the dynamic echo timer. Value must be an integer. The default value is 5 seconds.

Defaults

5 seconds

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use this command to specify the minimum time period (in seconds) used by the dynamic echo timer, also referred to as the T-dynamic. If the gateway GPRS support node's (GGSN's) current calculation of the round-trip time (RTT) statistic, multiplied by the smooth factor, is less than the configured dynamic minimum value, then the GGSN uses the configured minimum as the T-dynamic.

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

If the GGSN fails to receive an echo response message from the serving GPRS support node (SGSN) within the path echo interval, the GGSN goes into retransmission, or path failure mode. During path failure mode, the GGSN uses a value referred to as the T-dynamic. The T-dynamic is the greater of either the dynamic minimum, or the RTT statistic multiplied by the smooth factor.

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

Note For more information about the dynamic echo timer on the GGSN, see the "Usage Guidelines" section for the **gprs gtp echo-timer dynamic enable** command.

Examples

The following example turns on the dynamic echo timer, sets the minimum value to 6 seconds, and configures a smooth factor of 2:

```
gprs gtp echo-timer dynamic enable
gprs gtp echo-timer dynamic minimum 6
gprs gtp echo-timer dynamic smooth-factor 2
```

Related Commands

Command	Description
gprs gtp echo-timer dynamic enable	Enables the dynamic echo timer on the GGSN.
gprs gtp echo-timer dynamic smooth-factor	Configures the multiplier that the GGSN uses to calculate the time to wait to send retries of the dynamic echo timer.
gprs gtp n3-requests	Specifies the maximum number of times that the GGSN attempts to send a signaling request.
gprs gtp path-echo-interval	Specifies the number of seconds that the GGSN waits before sending an echo-request message to the SGSN.

gprs gtp echo-timer dynamic smooth-factor

To configure the multiplier that the gateway GPRS support node (GGSN) uses to calculate the time to wait to send retries of the dynamic echo timer, use the **gprs gtp echo-timer dynamic smooth-factor** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs gtp echo-timer dynamic smooth-factor *number*

no gprs gtp echo-timer dynamic smooth-factor *number*

Syntax Description

number	Integer (between 1 and 100) used by the GGSN as a multiplier for the round-trip time (RTT) statistic, to calculate the T-dynamic. The default is 2.

Defaults

2

Command Modes

Global configuration

Command History

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

Usage Guidelines

The dynamic echo timer uses the smooth factor to calculate what is known as the T-dynamic. The T-dynamic is calculated by multiplying the RTT (or the value configured in the **gprs gtp echo-timer dynamic minimum**, whichever is greater) times the smooth-factor.

Note See the "Usage Guidelines" section for the **gprs gtp echo-timer dynamic enable** command for a detailed explanation of how the dynamic echo timer works.

Examples

The following example turns on the dynamic echo timer, sets the minimum value to 1 second, and configures a smooth factor of 2:

```
gprs gtp echo-timer dynamic enable
gprs gtp echo-timer dynamic minimum 1
gprs gtp echo-timer dynamic smooth-factor 2
```

Related Commands

Command	Description
gprs gtp echo-timer dynamic enable	Enables the dynamic echo timer on the GGSN.
gprs gtp echo-timer dynamic minimum	Specifies the minimum time period used by the dynamic echo timer.
gprs gtp n3-requests	Specifies the maximum number of times that the GGSN attempts to send a signaling request.
gprs gtp path-echo-interval	Specifies the number of seconds that the GGSN waits before sending an echo-request message to the SGSN.
gprs gtp t3-response	Specifies the initial time that the GGSN waits before resending a signaling request message when a response to a request has not been received

gprs gtp error-indication-throttle

To specify the maximum number of error indication messages that the gateway GPRS support node (GGSN) sends out in one second, use the **gprs gtp error-indication-throttle** command in global configuration mode. To return to the default value, issue the **no** form of this command.

gprs gtp error-indication-throttle window-size *size*

no gprs gtp error-indication-throttle

Syntax Description

size	Integer (between 0 and 256) that specifies the maximum number of error indication messages that the GGSN sends in one second.

Defaults

Error indication throttling is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

GPRS tunneling protocol (GTP) error indication messages are sent by the GGSN to the serving GPRS support node (SGSN) when the SGSN sends data for packet data protocol (PDP) context the GGSN cannot locate. The error indication message informs the SGSN that the PDP context cannot be located so that the SGSN can clean up the PDP context on its end.

Use the **gprs gtp error-indication-throttle** command to specify the maximum number of error indication messages that are sent by the GGSN in one second. This provides a way to implement flow control for transmission of GTP error messages. This command sets the initial value of a counter which is decremented each time an error indication message is sent. When the counter reaches zero, the GGSN stops transmitting error indication messages. The GGSN resets this counter to the configured throttle value after one second.

If you do not issue the command, error indication throttling is not enabled. To restore the default value (error indication throttling is disabled) use the **no** form of this command.

Examples

The following example shows a throttle value of 150:

```
gprs gtp error-indication-throttle window-size 150
```

gprs gtp ip udp ignore checksum

To configure the GGSN to ignore user datagram protocol (UDP) checksums (in order to support CEF switching on the GGSN), use the **gprs gtp ip udp ignore checksum** global configuration command. To disable the ignoring of UDP checksums on the GGSN, use the **no** form of this command.

gprs gtp ip udp ignore checksum

no gprs gtp ip udp ignore checksum

Syntax Description

This command has no arguments or keywords.

Defaults

In releases prior to Cisco IOS Release 12.3(14)XU, UDP checksums are verified by default.

With Cisco IOS Release 12.3(14)XU and later, UDP checksums are ignored by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was incorporated in Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was incorporated in Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was incorporated in Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was incorporated in Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was incorporated in Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was incorporated in Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU and the default was changed to have the GGSN ignore UDP checksums.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

UDP checksum verification can prohibit operation of CEF switching processing on the GGSN if the checksum should have a non-zero result. Therefore, if you want to enable CEF switching on the GGSN, ensure that the GGSN is configured to ignore UPD checksums (the default).

If UDP checksum verification remains enabled on the GGSN and a non-zero result occurs, the GTP T-PDUs will be process switched, even if you have configured the GGSN for CEF switching.

The **gprs gtp ip udp ignore checksum** command does not apply if you are only using process switching on the GGSN.

Note When downgrading to an image prior to Cisco IOS Release 12.3(14)YU when using the default for the **gprs gtp ip udp ignore checksum** command (UDP checksums are ignored), you will need to manually configure the GGSN to ignore UPD checksums. In releases prior to Cisco IOS Release 12.3(14)YU, UDP checksums are verified by the GGSN by default.

For more information about switching processes, refer to the *Cisco IOS Switching Services Configuration Guide*.

Examples

The following example disables UDP checksum verification on the GGSN:

```
gprs gtp ip udp ignore checksum
```

Related Commands

Command	Description
ip cef	Enables CEF on the route processor card.

gprs gtp map signalling tos

To specify an IP type of service (ToS) mapping for GPRS tunneling protocol (GTP) signaling packets, use the **gprs gtp map signalling tos** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs gtp map signalling tos *tos-value*

no gprs gtp map signalling tos *tos-value*

Syntax Description

tos-value	Value between 0 and 7 that specifies the IP ToS mapping. The default value is 5.

Defaults

ToS value 5

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs gtp map signalling tos** command to specify the IP ToS mapping for GTP signaling packets transmitted by the gateway GPRS support node (GGSN). The higher the value, the higher the class of service provided to the packets.

Examples

The following example specifies a IP ToS mapping value of 3:

```
gprs gtp map signalling tos 3
```

Related Commands

Command	Description
gprs canonical-qos map tos	Specifies a QoS mapping from the canonical QoS classes to an IP ToS category.
gprs charging container volume-threshold	Specifies the maximum number of bytes that the GGSN maintains in a user's charging container before closing the charging container and updating the CDR.
gprs charging map data tos	Specifies an IP ToS mapping for GGSN charging data packets.
gprs charging packet-queue-size	Specifies the maximum number of unacknowledged charging data transfer requests that the GGSN maintains in its queue.
gprs charging message transfer-response number-responded	Specifies the number of seconds that the GGSN waits before it transfers charging data to the charging gateway.

gprs gtp n3-buffer-size

To specify the size of the receive buffer that the gateway GPRS support node (GGSN) uses to receive GPRS tunneling protocol (GTP) signaling messages and packets sent through the tunneling protocol, use the **gprs gtp n3-buffer-size** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs gtp n3-buffer-size *bytes*

no gprs gtp n3-buffer-size

Syntax Description

bytes	Number of bytes (between 2048 and 65535) that specifies the size of the N3 buffer. The default is 8192 bytes.

Defaults

8192 bytes

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs gtp n3-buffer-size** command to specify the size of the GTP N3 buffer on the GGSN. The N3 buffer is a receive buffer that the GGSN uses to receive GTP signaling messages and packets sent through the tunneling protocol. The recommended value for the N3 buffer size is 8192 bytes (the default size).

Examples

The following example specifies a buffer size of 2084 bytes:

```
gprs gtp n3-buffer-size 2048
```

gprs gtp n3-requests

To specify the maximum number of times that the gateway GPRS support node (GGSN) attempts to send a signaling request to a serving GPRS support node (SGSN), use the **gprs gtp n3-requests** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs gtp n3-requests *requests*

no gprs gtp n3-requests *requests*

Syntax Description

requests	A number between 1 and 65535 that specifies the number of times that a request is attempted. The default is 5 requests.

Defaults

5 requests

Command Modes

Global configuration

Command History

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

Usage Guidelines

The value of the **gprs gtp n3-requests** command is used for all signaling requests on the GGSN.

The GGSN supports two different methods of echo timing—the default echo timer and the dynamic echo timer. The **gprs gtp n3-requests** command is used by the GGSN to perform either type of echo processing.

Examples

The following example shows the GGSN attempting to send a signaling request 3 times:

```
gprs gtp n3-requests 3
```

Related Commands

Command	Description
gprs gtp echo-timer dynamic enable	Enables the dynamic echo timer on the GGSN.
gprs gtp n3-buffer-size	Specifies the size of the receive buffer that the GGSN uses to receive GTP signaling messages and packets sent through the tunneling protocol.
gprs gtp path-echo-interval	Specifies the number of seconds that the GGSN waits before sending an echo-request message to the SGSN.
gprs gtp t3-response	Specifies the initial time that the GGSN waits before resending a signaling request message when a response to a request has not been received.

gprs gtp path-echo-interval

To specify the number of seconds that the gateway GPRS support node (GGSN) waits before sending an echo-request message to the serving GPRS support node (SGSN) or charging gateway, use the **gprs gtp path-echo-interval** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs gtp path-echo-interval *interval*

no gprs gtp path-echo-interval *interval*

Syntax Description

interval	Number of seconds that the GGSN waits before sending an echo-request message. Specify a value between 60 and 65535 seconds. The value 0 disables the echo-request feature. The default is 60 seconds.

Defaults

60 seconds

Command Modes

Global configuration

Command History

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

Usage Guidelines

The GGSN supports two different methods of echo timing—the default echo timer and the dynamic echo timer. The **gprs gtp path-echo-interval** command is used on the GGSN to perform either type of echo processing.

Use the **gprs gtp path-echo-interval** command to specify the interval that the GGSN waits before sending an echo-request message to the SGSN or charging gateway to check for GPRS tunneling protocol (GTP) path failure.

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

Examples

The following example shows the GGSN waiting 90 seconds before sending an echo-request message:

```
gprs gtp path echo-interval 90
```

Related Commands

Command	Description
gprs gtp echo-timer dynamic enable	Enables the dynamic echo timer on the GGSN.
gprs gtp n3-requests	Specifies the maximum number of times that the GGSN attempts to send a signaling request to an SGSN.
gprs gtp t3-response	Specifies the initial time that the GGSN waits before resending a signaling request message when a response to a request has not been received.

gprs gtp path history

To configure the maximum number of path entries for which the gateway GRPS serving node (GGSN) stores statistics after the path is deleted, use the **gprs gtp path history** command in global configuration mode.

gprs gtp path history *number*

no gprs gtp path history

Syntax Description

number	Number of path entries for which to store statistics in history when the path is deleted. A valid value is between 1 and 1000.

Defaults

100 entries.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs gtp path history** command to configure the number of path entries for which the GGSN stores statistics after the path is deleted.

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

Examples

The following example configures the GGSN to store statistics for up to 250 entries:

```
gprs gtp path history 250
```

Related Commands

Command	Description
show gprs gtp path history	Displays summary details of past GTP path entries stored in history.
show gprs gtp path statistics remote-address	Displays the details of counters for a current path, or the details of counters maintained in history for a deleted path.

gprs gtp path sgsn

To suppress echo requests per SGSN and/or UDP port, use the **gprs gtp path sgsn** command in global configuration mode. To remove this configuration, use the **no** form of this command.

gprs gtp path sgsn *start-ip-address* [*end-ip-address*] [*UDP port*] **echo 0**

no gprs gtp path sgsn *start-ip-address* [*end-ip-address*] [*UDP port*] **echo 0**

Syntax Description

start-ip-address	Specifies the first IP address of the range.
end-ip-address	Specifies the last IP address of the range.
udp port	Specifies the corresponding UDP port.
echo 0	Disables echo requests.

Command Default

There are no default behaviors or values.

Command Modes

Global configuration

Command History

Release	Modification
12.(4)15XQ	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Echo requests can be disabled per SGSN and/or UDP port. This feature enables operators to selectively disable charging for GSNs that might not have the capability to respond to echo requests from the GGSN entirely, or only those echo requests received on certain UDP ports, while keeping the echo requests intact for the other SGSNs.

When a new path is created, the GGSN checks to see if the path parameters, namely the destination address and port, matches any of the conditions configured when suppressing echo requests. If the parameters match, the GGSN sets the path echo interval to 0 for that path. Otherwise, the global path echo interval configuration is used to send echo requests.

Examples

The following example disables echo requests for one SGSN:

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

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

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

gprs gtp pdp-context timeout idle

To specify the time, in seconds, that a gateway GPRS support node (GGSN) allows a session to remain idle at any access point before purging the packet data protocol (PDP) context, use the **gprs gtp pdp-context timeout idle** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs gtp pdp-context timeout idle *seconds* [**uplink**]

no gprs gtp pdp-context timeout idle

Syntax Description

seconds	Time, in seconds, that the GGSN allows a PDP context to remain idle on any access point before terminating the context. Specify a value between 30 and 4294967 seconds.
uplink	(Optional) Enables the session idle timer in the uplink direction only. When the **uplink** keyword option is not specified, the session idle timer is enabled in both directions (uplink and downlink).

Defaults

259200 seconds (72 hours)

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(8)XU1	This command was integrated into Cisco IOS Release 12.3(8)XU1 and the **uplink** keyword option was added.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

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

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

On the GGSN, the session idle timer can be configured globally and at the access point name (APN). The value configured at the APN level using the **gtp pdp-context timeout idle** access-point configuration command overrides the value configured globally using the **gprs gtp pdp-context timeout idle** global configuration command. The value configured in the user profile on the RADIUS server overrides the value configured at the APN.

Note The session idle timer started for a PDP context is reset by Transport Protocol Data Unit (TPDU) traffic and GPRS tunneling protocol (GTP) signaling messages for that PDP context. For example, if an Update PDP Context request is received, the session idle timer is reset for that PDP context.

You can disable the session idle timer for a particular user by configuring 0 as the session idle time duration in the user profile on the RADIUS server. If a user is authenticated by RADIUS, the session idle time cannot be disabled.

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

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

Examples

The following example shows configuring the GGSN to wait 18000 seconds before ending an idle PDP context:

```
gprs gtp pdp-context timeout idle 18000
```

Related Commands

Command	Description
gprs gtp pdp-context timeout session	Specifies the time, in seconds, that the GGSN allows a session to be active on any access point before terminating the session.
gprs idle-pdp-context purge-time	Specifies the time, in hours, that the GGSN waits before purging idle mobile sessions.
gtp pdp-context timeout idle	Specifies the time, in seconds, that a GGSN allows a session to be idle at a particular APN before terminating the session.
gtp pdp-context timeout session	Specifies the time, in seconds, that a GGSN allows a session to be active at a particular APN before terminating the session.
session idle-time	Specifies the time, in hours, that the GGSN waits before purging idle mobile sessions for an access point.
show gprs gtp pdp-context	Displays a list of the currently active PDP contexts (mobile sessions).

gprs gtp pdp-context timeout session

To specify the time, in seconds, that the gateway GPRS support node (GGSN) allows a session to exist at any access point before terminating the session, use the **gprs gtp pdp-context timeout session** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs gtp pdp-context timeout session *seconds*

no gprs gtp pdp-context timeout session

Syntax Description

seconds	Time, in seconds, that the GGSN allows a session to exist at any access point. Specify a value between 30 and 4294967 seconds.

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

When enabled using the **gprs radius attribute session-timeout** command, the GGSN supports the RADIUS Session-Timeout (Attribute 27). The GGSN stores the attribute timeout value received in access-accept packets sent by the authentication, authorization, and accounting (AAA) server and when the duration of a session exceeds the duration configured as absolute session timer, the GGSN terminates the session and all packet data protocol (PDP) contexts belonging to the session (those with the same International Mobile Subscriber Identity [IMSI] or mobile station [MS] address).

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

Note The active session timeout feature requires that the **gprs radius attribute session-timeout** command has been enabled.

On the GGSN, the absolute session timer can be configured globally and at the access point name (APN). The value configured at the APN level using the **gtp pdp-context timeout session** access-point configuration command overrides the value configured globally using the **gprs gtp pdp-context timeout session** global configuration command. The value configured in the user profile on the RADIUS server overrides the value configured at the APN.

Examples

The following example shows configuring the GGSN to end any session that exceeds 86400 seconds in duration:

```
gprs gtp pdp-context timeout session 86400
```

Related Commands

Command	Description
gprs gtp pdp-context timeout idle	Specifies the time, in seconds, that a GGSN allows a session to be idle at any access point before terminating the session.
gprs idle-pdp-context purge-timer	Specifies the time, in hours, that the GGSN waits before purging idle mobile sessions.
gtp pdp-context timeout idle	Specifies the time, in seconds, that a GGSN allows a session to be idle at a particular APN before terminating the session.
gtp pdp-context timeout session	Specifies the time, in seconds, that a GGSN allows a session to be active at a particular APN before terminating the session.
session idle-time	Specifies the time, in hours, that the GGSN waits before purging idle mobile sessions for an access point.
show gprs gtp pdp-context	Displays a list of the currently active PDP contexts (mobile sessions).

gprs gtp ppp vtemplate

To associate the virtual template interface that defines the PPP characteristics with support for the PPP packet data protocol (PDP) type over GPRS tunneling protocol (GTP) on the gateway GPRS support node (GGSN), use the **gprs gtp ppp vtemplate** command in global configuration mode. To remove specification of the PPP virtual template interface for GTP on the GGSN, use the **no** form of this command.

gprs gtp ppp vtemplate *number*

no gprs gtp ppp vtemplate

Syntax Description

number	Integer identifier of the virtual template interface over which the PPP characteristics are defined on the GGSN. This number must match the number configured in the corresponding **interface virtual-template** command.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Before you configure the **gprs gtp ppp vtemplate** command, you must configure the virtual template interface with the necessary PPP characteristics. The number that you configure for the virtual template interface that defines the PPP characteristics, must correspond to the number that you specify in the **gprs gtp ppp vtemplate** command.

Examples

The following example configures two virtual template interfaces on the GGSN, one for GTP encapsulation and one for PPP, and specifies the PPP virtual template interface for GTP on the GGSN.

Note The virtual template interface for PPP is a different virtual template interface than the GPRS/UMTS virtual template interface for GTP encapsulation.

The first section of commands configures the GPRS virtual template interface for GTP:

```
interface Virtual-Template 1
 ip unnumber loopback 1
 no ip directed-broadcast
 encapsulation gtp
 no ip route-cache
 gprs access-point-list gprs
```

The following example configures a virtual template interface for PPP and associates the virtual template for support of the PPP PDP type over GTP on the GGSN:

```
interface Virtual-Template 2
 ip unnumbered FastEthernet 1/0
 no ip directed-broadcast
 no peer default ip address
 ppp authentication chap
 ppp timeout retry 30

gprs gtp ppp vtemplate 2
```

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.

gprs gtp ppp-regeneration vtemplate

To associate the virtual template interface that is configured for PPP encapsulation with support for regenerated PPP sessions on the GGSN, use the **gprs gtp ppp-regeneration vtemplate** global configuration command. To remove specification of the PPP virtual template interface for regenerated PPP sessions on the GGSN, use the **no** form of this command.

gprs gtp ppp-regeneration vtemplate *number*

no gprs gtp ppp-regeneration vtemplate

Syntax Description

number	Integer identifier of the virtual template interface which defines PPP encapsulation on the GGSN. This number must match the number configured in the corresponding **interface virtual-template** command.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Before you configure the **gprs gtp ppp-regeneration vtemplate** command, you must configure the virtual template interface for PPP encapsulation using the **encapsulation ppp** command. In addition, you must also configure the **ip address negotiated** command and the **no peer neighbor-route** command at the virtual template interface for PPP encapsulation.

The number that you configure for the virtual template interface to support PPP encapsulation, must correspond to the number that you specify in the **gprs gtp ppp-regeneration vtemplate** command.

Examples

The following example configures two virtual template interfaces on the GGSN, one for GTP encapsulation for communication between the GGSN and the SGSN, and one for PPP regeneration. The virtual template interface for PPP regeneration supports the creation of PPP sessions from the GGSN over Layer 2 Tunneling Protocol (L2TP) tunnels to an L2TP network server (LNS).

Note The virtual template interface for PPP regeneration is a different virtual template interface than the GPRS virtual template interface for PPP PDP type support and for GTP encapsulation.

The first section of commands configures the GPRS virtual template interface for GTP:

```
interface Virtual-Template 1
 ip unnumber loopback 1
 no ip directed-broadcast
 encapsulation gtp
 no ip route-cache
 gprs access-point-list gprs
```

The following example configures a virtual template interface for PPP regeneration:

```
interface Virtual-Template 11
 ip address negotiated
 no peer neighbor-route
 encapsulation ppp
```

Note The **encapsulation ppp** configuration will not display in a show running configuration because it is the default encapsulation.

The following example specifies virtual template interface 11 for PPP regeneration on the GGSN:

```
gprs gtp ppp-regeneration vtemplate 11
```

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.

gprs gtp response-message pco ipcp nack

To configure IP control protocol (IPCP) options returned in the protocol control option (PCO) information element (IE) by the gateway GPRS support node (GGSN) in the Create packet data protocol (PDP) Context responses, use the **gprs gtp response-message pco ipcp** global configuration field. To return to the default values, use the **no** form of the command.

gprs gtp response-message pco ipcp {**nack** | **message-length**}

no gprs gtp response-message pco ipcp {**nack** | **message-length**}

Syntax Description

nack	Specifies for the GGSN to return an IPCP Conf-Nack (Code 03) in the GTP PCO IE of the Create PDP Context response when returning IPCP options for which the granted values (non-zero) differ from those requested. (IPCP Conf-Reject [Code 04) is returned for those options for which the returned address values are zero).
message-length	Configures an extra field that indicates the message length to be added to the header in the PCO IE of the Create PDP Context response when returning IPCP options.

Defaults

The GGSN sends an IPCP Conf-Ack (Code 02) in the PCO IE of the Create PDP Context response for the the requested IPCP address options supported by the GGSN. The values being returned might be the same as or differ from those requested, or be zero. For unsupported options, an IPCP Conf-Reject is returned.

The GGSN does not add an extra fieldthat indicates the message length to the PCO IE, when returning IPCP options.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)XB	This command was introduced.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB and the **message-length** keyword option was added.

Usage Guidelines

Use the **gprs gtp response-message pco ipcp** command to configure IPCP options returned by the GGSN in the PCO IE of a Create PDP Context response.

Use the **gprs gtp response-message pco ipcp** command, with the **nack** keyword option specified, to configure the GGSN to return an IPCP Conf-Nack in the PCO IE of a Create PDP Context response when returning IPCP options for which the granted values differ from those requested (non-zero values).

When the **gprs gtp response-message pco ipcp nack** command is configured, and the PCO IE of the Create PDP Context request contains IPCP options, the PCO IE in the create PDP response includes the following, depending on the whether options are supported by (and values are acceptable to) the GGSN:

- IPCP Conf-Ack—One or (zero) IPCP Conf-Ack for the IPCP options for which the requested values are acceptable by the GGSN.
- IPCP Conf-Nack—One or (zero) IPCP Conf-Nack containing the IPCP options for which the granted values differ from those requested.
- IPCP Conf-Reject—One (or zero) IPCP Conf-Reject containing the requested options which are not supported by the GGSN, or, if supported, for which no values can be granted.

Use the **gprs gtp response-message pco ipcp** command, with the **message-length** keyword option specified, to configured the GGSN to add a message length field to the PCO IE in the Create PDP Context response, when returning IPCP options.

Examples

The following configures the GGSN to include an extra field in the header of the PCO IE when returning IPCP options that indicates the message length in Create PDP Context responses.

```
gprs gtp response-message pco ipcp message-length
```

Related Commands

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

gprs gtp response-message wait-accounting

To configure the gateway GPRS support node (GGSN) to wait for a RADIUS accounting response before sending a Create packet data protocol (PDP) Context response to the serving GPRS support node (SGSN) for Create PDP Context requests received across all access points, use the **gprs gtp response-message wait-accounting** command in global configuration mode. To configure the GGSN to send a Create PDP Context response to the SGSN after sending a RADIUS start accounting message to the RADIUS server (without waiting for a response from the RADIUS accounting server), use the **no** form of this command.

gprs gtp response-message wait-accounting

no gprs gtp response-message wait-accounting

Syntax Description

This command has no arguments or keywords.

Defaults

The GGSN sends a Create PDP Context response to the SGSN after sending a RADIUS start accounting message to the RADIUS accounting server. The GGSN does not wait for a RADIUS accounting response from the RADIUS accounting server.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs gtp response-message wait-accounting** command to configure the GGSN to wait for a RADIUS accounting response from the RADIUS accounting server before sending a Create PDP Context response to the SGSN for Create PDP Context requests received across all access points.

If the GGSN does not receive a response from the RADIUS accounting server when you have configured the **gprs gtp response-message wait-accounting** command, it rejects the PDP context request.

When broadcast accounting is used (accounting requests are sent to multiple RADIUS servers), if a RADIUS server responds with an accounting response, the GGSN sends a Create PDP Context response and does not wait for the other RADIUS servers to respond.

The GGSN supports configuration of RADIUS response message waiting at both the global and access-point configuration levels. You can minimize your configuration by specifying the configuration that you want to support across most access point names (APNs), at the global configuration level. Then, at the access-point configuration level, you can selectively modify the behavior that you want to support at a particular APN. Therefore, at the APN configuration level, you can override the global configuration of RADIUS response message waiting.

To configure the GGSN to wait for a RADIUS accounting response as the default behavior for all APNs, use the **gprs gtp response-message wait-accounting** global configuration command. To disable this behavior for a particular APN, use the **no response-message wait-accounting** access-point configuration command.

To verify whether RADIUS response message waiting is enabled or disabled at an APN, you can use the **show gprs access-point** command and observe the value reported in the wait_accounting output field.

Examples

The following example globally configures the GGSN to wait for a RADIUS accounting response from the RADIUS accounting server before sending an Activate PDP Context response to the SGSN, for PDP context requests received across all access points except access-point 1. RADIUS response message waiting has been overridden at access-point 1 using the **no gtp response-message wait-accounting** command.

Note This example shows only a partial configuration of the GGSN, to highlight the commands for implementing RADIUS response message waiting. Additional configuration statements are required to complete a full configuration of the GGSN.

```
aaa new-model
!
aaa group server radius foo
 server 10.2.3.4
 server 10.6.7.8
!
aaa authentication ppp foo group foo
aaa authorization network default group radius
aaa accounting exec default start-stop group foo
!
gprs access-point-list gprs
 access-point 1
  access-mode non-transparent
  access-point-name www.pdn1.com
  aaa-group authentication foo
  no gtp response-message wait-accounting
  exit
 access-point 2
  access-mode non-transparent
  access-point-name www.pdn2.com
  aaa-group authentication foo
!
gprs gtp response-message wait-accounting
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

Related Commands

Command	Description
gtp response-message wait-accounting	Configures the GGSN to wait for a RADIUS accounting response before sending a Create PDP Context response to the SGSN, for Create PDP Context requests received at a particular APN.
show gprs access-point	Displays information about access points on the GGSN.

gprs gtp t3-response

To specify the initial time that the gateway GPRS support node (GGSN) waits before resending a signaling request message when a response to a request has not been received, use the **gprs gtp t3-response** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs gtp t3-response *response-interval*

no gprs gtp t3-response

Syntax Description

response-interval	A value between 1 and 65535 that specifies the length of the T3 response interval, in seconds. The default is 1 second.

Defaults

1 second

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **gprs gtp t3-response** command is used by the GGSN to process Delete packet data protocol (PDP) Context requests and to perform the default method of echo timing.

For delete PDP context requests, the **gprs gtp t3-response** command is used by the GGSN to specify how long the GGSN waits before sending a retry of the delete PDP context request when a response is not received from the serving GPRS support node (SGSN), until the **gprs gtp n3-requests** limit is reached.

The GGSN supports two echo timer implementations—the default echo timer and the dynamic echo timer. The **gprs gtp t3-response** command is also used on the GGSN to perform the default type of echo processing, when the dynamic echo timer is not enabled.

If the GGSN receives the echo response within the path echo interval (as specified in the **gprs gtp path-echo-interval** command; default is 60 seconds), it sends another echo request message after 60 seconds (or whatever time was configured in the **gprs gtp path-echo-interval** command). This message flow continues as long as the GGSN receives an echo response message within the specified path echo interval.

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

For example, if N3 is set to the default of 5, and T3 is set to the default of 1 second, the GGSN will resend 4 echo request messages (the initial request + 4 retries = 5). The T3 time increments for each additional echo request, by a factor of 2 seconds. So, the GGSN resends a message in 2 seconds, 4 seconds, 8 seconds, and 16 seconds. If the GGSN fails to receive an echo response message from the SGSN within the time period of the N3-requests counter, it clears the GPRS tunneling protocol (GTP) path and deletes all the PDP contexts.

For the above example, the total elapsed time from when the first request message is sent, to when the GTP path is cleared, is: 60 + 2 + 4 + 8 + 16 = 90 seconds,

where 60 is the initial value of the path echo interval, and the remaining 4 time periods are the increments of the T3 timer for the subsequent retries.

Examples

The following example shows a T3 interval response interval of 524 seconds:

```
gprs gtp t3-response 524
```

Related Commands

Command	Description
gprs gtp n3-requests	Specifies the maximum number of times that the GGSN attempts to send a signaling request to an SGSN.
gprs gtp path-echo-interval	Specifies the number of seconds that the GGSN waits before sending an echo request message to the SGSN.

gprs gtp update qos-fail delete

To configure the GGSN to delete a PDP context if a GGSN-initiated QoS update fails, and no GGSN-initiated Update PDP Context Request failure action has been configured at the APN, use the **gprs gtp update qos-fail delete** command in global configuration mode. To return to the default value, use the **no** form of the command.

gprs gtp update qos-fail delete

no gprs gtp update qos-fail delete

Syntax Description

This command has no arguments or keywords.

Defaults

PDP contexts are not deleted.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use this command to configure the GGSN to generate a Delete PDP Context request when a GGSN-initiated Update PDP Context Request for a QoS update fails.

The Acct Stop record generated by the GGSN indicates the update failure.

This configuration applies when the Update PDP Context Response from the SGSN, initiated for a QoS change, times out after n3 tries or the Cause value is a value other than “Request Accepted.”

Note The GGSN-initiated Update PDP Context Request failure action defined at the APN overrides this global configuration.

Examples

The following is an example:

```
Router(config)# gprs gtp update qos-fail delete
```

Related Commands

Command	Description
gtp update qos-fail delete	Configures the GGSN to delete PDP contexts for an APN when GGSN-initiated QoS updates fail.

gprs idle-pdp-context purge-timer

To specify the time, in hours, that the gateway GPRS support node (GGSN) waits before purging idle mobile sessions, use the **gprs idle-pdp-context purge-timer** command in global configuration mode. To return to the default value, use the **no** form of this command**.**

gprs idle-pdp-context purge-timer *hours*

no gprs idle-pdp-context purge-timer

Syntax Description

hours	Value between 0 and 255 that specifies the number of hours that the GGSN waits before purging idle sessions. The value 0 disables the purge timer. The default is 72 hours.

Defaults

72 hours

Command Modes

Global configuration

Command History

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

Usage Guidelines

To specify the time that the GGSN waits before purging idle mobile sessions, use the **gprs idle-pdp-context purge-timer** command. To disable this feature, specify a purge-timer value of 0.

You can override the value of the global purge timer using the **session idle-time** access-point configuration command.

Note With GGSN Release 5.0 and later, you can also configure the session idle timer globally using the **gprs gtp pdp-context timeout idle** access-point configuration command, however, the two methods cannot be configured at the same time.

Examples

The following example specifies for the GGSN to wait 60 hours before purging idle sessions:

```
gprs idle-pdp-context purge-timer 60
```

Related Commands

Command	Description
gprs gtp pdp-context timeout idle	Specifies the number of seconds that a GGSN allows a session to be idle before terminating the session.
gprs gtp pdp-context timeout session	Specifies the number of seconds that the GGSN allows a session to be active before terminating the session.
gtp pdp-context timeout idle	Specifies the number of seconds that a GGSN allows a session to be idle at a particular APN before terminating the session.
gtp pdp-context timeout session	Specifies the number of seconds that a GGSN allows a session to be active at a particular APN before terminating the session.
session idle-time	Specifies the time that the GGSN waits before purging idle mobile sessions for the current access point.

gprs iscsi

To configure the GGSN to use an iSCSI target interface profile for record storage, use the **gprs iscsi** command in global configuration mode. To remove this configuration, use the **no** form of this command.

gprs iscsi *target_profile_name*

no gprs iscsi *target_profile_name*

Syntax Description

target_profile_name	Name of the iSCSI target interface profile. The profile name specified must be the same as the one configured using the **ip iscsi target-profile** command.

Command Default

iSCSI storage is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Multiple iSCSI profiles can be configured on the GGSN, however, only one target can be defined per profile, and the GGSN can be configured to use only one profile at a time using the **gprs iscsi** global configuration command.

Examples

The following example configures the GGSN to use an iSCSI target interface profile named “targetA” to store and retrieve G-CDRs:

```
gprs iscsi targetA
```

Related Commands

Command	Description
ip iscsi target-profile	Creates an iSCSI target interface profile for an SCSI target (or modifies an existing one), and enters iSCSI interface configuration mode.

gprs maximum-pdp-context-allowed

To specify the maximum number of packet data protocol (PDP) contexts (mobile sessions) that can be activated on the gateway GPRS support node (GGSN), use the **gprs maximum-pdp-context-allowed** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs maximum-pdp-context-allowed *pdp-contexts*

no gprs maximum-pdp-context-allowed

Syntax Description

pdp-contexts	Integer between 1 and 4294967295 that specifies the number of active PDP contexts allowed. The default is 10000 PDP contexts.

Defaults

10000 PDP contexts

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was integrated into Cisco IOS Release 12.2(4)MX, and the default value was changed from 1000 to 10000.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs maximum-pdp-context-allowed** command to specify the maximum number of PDP contexts allowed on the GGSN. When the maximum allowable number of PDP contexts is reached, the GGSN refuses new PDP contexts (mobile sessions) until sessions are available.

The practical upper limit for the maximum number of PDP contexts supported on a GGSN is dependent on the memory and platform in use and the GGSN configuration (for example, whether or not a method of PPP has been configured to forward packets beyond the terminal equipment and mobile termination, whether Dynamic Feedback Protocol [DFP] is being used or the memory protection feature is enabled, and the rate of PDP context creation to be supported).

Note DFP weighs PPP PDPs against IP PDPs with one PPP PDP equal to 8 IP PDPs.

Cisco 7200 Series Router

The following list shows the maximum number of PDP contexts supported on the GGSN according to the memory and Cisco 7206 router in use when a method of PPP has not been configured:

- Cisco 7206 VXR NPE-300 with 256 Mb of RAM—80,000 IP PDP contexts.
- Cisco 7206 VXR NPE-400 router with 512 Mb of RAM—135,000 IP PDP contexts.

Catalyst 6500 Series Switch / Cisco 7600 Series Router

The Cisco Multi-processor WAN Application Module (MWAM) can support up to 60,000 IP PDP contexts per GGSN instance with a maximum number of 300,000 IP PDP contexts per MWAM on which five GGSNs are configured.

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

Note If you use dynamic feedback protocol (DFP) with GPRS tunneling protocol (GTP) load balancing, you must also specify a maximum number of PDP contexts for each GGSN, using the **gprs maximum-pdp-context-allowed** command. Do not accept the default value of 10000 PDP contexts. Significantly lower values can impact performance in a GTP load-balancing environment.

DFP weighs PPP PDPs against IP PDPs, with one PPP PDP equal to 8 IP PDPs. Therefore, when using DFP, be aware that the configured maximum number of PDP contexts affects the GGSN weight. The lower the maximum number of PDP contexts, the lower the weight when all other parameters remain the same.

Note For more information about configuring GTP load balancing, see the *IOS Server Load Balancing*, documentation located at Cisco.com.

Examples

In the following example 15000 PDP contexts are allowed on the GGSN:

```
gprs maximum-pdp-context-allowed 15000
```

Related Commands

Command	Description
gprs idle-pdp-context purge-timer	Specifies the time that the GGSN waits before purging idle mobile sessions.

gprs mcc mnc

To configure the mobile country code (MCC) and mobile network code (MNC) that the gateway GPRS support node (GGSN) uses to determine if a Create packet data protocol (PDP) Context request is from a roamer, use the **gprs mcc mnc** command in global configuration mode. To return to the default values, use the **no** form of this command.

gprs mcc *mcc-num* **mnc** *mnc-num* **[trusted]**

no gprs mcc *mcc-num* **mnc** *mnc-num* **[trusted]**

Syntax Description

mcc *mcc-num*	3-digit decimal number for the MCC. The valid range for the MCC is 000 to 999. The default value is 000, which is not a valid code.
mnc *mnc-num*	2- or 3-digit decimal number for the MNC. The valid range for the MNC is 00 to 999. The default value is 000, which is not a valid code.
trusted	Specifies that the MCC and MNC defined are those of a trusted PLMN. Up to 5 trusted PLMNs can configured as trusted.

Defaults

000—For both the MCC and MNC. A valid code must be a non-zero value.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs mcc mnc** command as part of the configuration required on the GGSN to support creation of call detail records (CDRs) for roaming mobile subscribers, or to block roamers from being able to Create PDP Context requests.

The MCC and MNC together identify a GPRS/UMTS public land mobile network (PLMN). The values you configure using the **gprs mcc mnc** command without the **trusted** keyword option specified are those of the home PLMN ID - the PLMN to which the GGSN belongs. Only one home PLMN can be defined for a GGSN at a time. The GGSN uses the values that you configure in this command to compare with the international mobile subscriber identity (IMSI) in a Create PDP Context request.

The GGSN automatically specifies values of 000 for the MCC and MNC. However, you must configure non-zero values for both the MCC and MNC before you can enable the GGSN to create charging CDRs for roamers.

To properly issue the **gprs mcc mnc** command, you must specify both the **mcc** keyword with its argument and the **mnc** keyword with its argument. You cannot issue the command without specifying both keywords.

It is important that you configure the **gprs mcc mnc** and **gprs charging roamers** commands in their proper order. After you configure the MCC and MNC values, use the **gprs charging roamers** command to enable charging for roamers on the GGSN. You can change the MCC and MNC values by reissuing the **gprs mcc mnc** command.

Using the **gprs mcc mnc** command, you can also configure up to 5 “trusted” PLMNs by specifying the **trusted** keyword. A Create PDP Context request from a mobile subscriber in a trusted PLMN is treated the same as a Create PDP Context request from a mobile subscriber in the home PLMN.

To verify your configuration of these codes on the GGSN, use the **show gprs charging parameters** command.

Note To see a list of some established MCC and MNC codes, see the “Table of MCC and MNC Codes” appendix in the *Cisco GGSN Configuration Guide*. To find more information about MCC and MNC codes, see the ITU E.212 recommendation, *Identification Plan for Land Mobile Stations*.

Examples

The following example replaces the default values of 000 on the GGSN, and specifies an MCC code of 310 for the USA and an MNC code of 15 for the Bell South service provider:

```
gprs mcc 310 mnc 15
```

Related Commands

Command	Description
block-foreign-ms	Restricts GPRS access based on the mobile user’s home PLMN.
gprs charging roamers	Enables charging for roamers on the GGSN.
show gprs charging parameters	Displays information about the current GGSN charging configuration.

gprs memory threshold

To prevent the gateway GPRS support node (GGSN) from draining processor memory during abnormal conditions (such as charging gateways [CGs] being down), use the **gprs memory threshold** command in global configuration mode to configure a memory threshold, that when reached, activates the memory protection feature on the GGSN.

gprs memory threshold *threshold*

no gprs memory threshold

Syntax Description

threshold	Memory threshold, that when fallen below enables the memory protection feature on the GGSN. Valid range is 0 to 1024.

Defaults

The default is 10% of the total memory available at the time GGSN services are enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

By default, the memory threshold is 10% of the total memory available at the time GGSN services are enabled using the **gprs ggsn service** global configuration command. You can use the **gprs memory threshold** global configuration command to configure the threshold according to the router and memory size.

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

- Rejects new Create packet data protocol (PDP) Context requests with the cause value "No Resource."
- Drops any existing PDPs for which an update is received with the cause value "Management Intervention."
- Drops any PDPs for which a volume trigger has occurred.

Examples

The following example sets the memory threshold to 50 KB:

```
gprs memory threshold 512
```

gprs ms-address exclude-range

To specify the IP address range(s) used by the GPRS/UMTS network, and thereby excluded from the mobile station (MS) IP address range, use the **gprs ms-address exclude-range** command in global configuration mode. To remove the specified range(s), use the **no** form of this command.

gprs ms-address exclude-range *start-ip end-ip*

no gprs ms-address exclude-range *start-ip end-ip*

Syntax Description

start-ip	IP address at the beginning of the range.
end-ip	IP address at the end of the range.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

An MS cannot have the same IP address as another GPRS network entity. Use the **gprs ms-address exclude-range** command to reserve certain IP address ranges for use by the GPRS/UMTS network, and to disallow these address ranges from use by an MS.

The **gprs ms-address exclude range** command verification is performed only for IP PDPs and does not apply to MS addresses assigned to virtual private networks (VPNs) or for PPP Regen or PPP PDP types.

During processing of a Create packet data protocol (PDP) Context request, the gateway GPRS support node (GGSN) verifies whether the IP address of an MS falls within the specified excluded range. If there is an overlap of the MS IP address with an excluded range, then the Create PDP Context request is rejected. This measure prevents duplicate IP addressing in the network.

You can configure up to 100 IP address ranges. A range can be one or more addresses. However, you can configure only one IP address range per command entry. To exclude a single IP address, you can repeat the IP address in the *start-ip* and *end-ip* arguments. IP addresses are 32-bit values.

Examples

Example 1

The following example specifies the IP address ranges used by the GPRS/UMTS network (which are thereby excluded from the MS IP address range):

```
gprs ms-address exclude-range 10.0.0.1 10.20.40.50
gprs ms-address exclude-range 172.16.150.200 172.30.200.255
gprs ms-address exclude-range 192.168.100.100 192.168.200.255
```

Example 2

The following example excludes an MS from using the IP address 10.10.10.1:

```
gprs ms-address exclude-range 10.10.10.1 10.10.10.1
```

Related Commands

Command	Description
show gprs ms-address exclude-range	Displays the IP address range(s) configured on the GGSN for the GPRS/UMTS network.

gprs plmn ip address

To specify the IP address range of a public land mobile network (PLMN), use the **gprs plmn ip address** command in global configuration mode.

gprs plmn ip address *start_ip end_ip* [**sgsn**]

no gprs plmn ip address *start_ip end_ip* [**sgsn**]

Syntax Description

start_ip	IP address at the beginning of the range.
end_ip	IP address at the end of the range.
sgsn	(Optional) Specifies that only the PLMN IP address ranges defined with the **sgsn** keyword specified be used to determine if an serving GPRS support node (SGSN) is located in a PLMN other than the gateway GPRS support node (GGSN).

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs plmn ip address** global configuration command to specify the IP address range of the PLMN.

The **gprs plmn ip address** command defines addresses that belong to a PLMN. To indicate that the addresses are SGSN addresses within the PLMN, issue the **gprs plmn ip address** command with the **sgsn** keyword option specified. This option is used by the charging for roamers feature (**gprs charging roamers** command).

When using the **gprs plmn ip address** command with the GGSN charging for roamers feature, depending on how the PLMN IP address ranges have been defined using the **gprs plmn ip address** *start_ip end_ip* [**sgsn**] command, the charging for roamers feature operates as follows:

- If no PLMN IP address ranges are configured using the **gprs plmn ip address** *start_ip end_ip* [**sgsn**] command, the GGSN generates CDRs for all initiated PDP contexts regardless of whether the GGSN and SGSN are located within the same PLMN.
- If a list of PLMN IP address ranges has been configured using the **gprs plmn ip address** *start_ip end_ip* [**sgsn**] command, and one or more of those ranges has been defined using the **sgsn** keyword, the GGSN uses those ranges defined with the **sgsn** keyword to determine whether an SGSN is located within the same PLMN.

  With this configuration, the following scenarios outline how the charging for roamers feature will function:

  - Mobile station 1 (MS1) is subscribed to PLMN1 and attaches to an SGSN in PLMN2. From PLMN2, MS1 initiates a packet data protocol (PDP) context with the GGSN in PLMN1. In this case, MS1 is a roamer, and the GGSN generates a call detail record (CDR) because it determines that the SGSN is located in a different PLMN.
  - MS1 is subscribed to PLMN1 and attaches to an SGSN in PLMN2. From PLMN2, MS1 initiates a PDP context with the GGSN in PLMN2. In this case, MS1 is not a roamer because the SGSN and GGSN are in the same PLMN. The GGSN does not create a CDR.

Configuration Guidelines

To enable charging for roamers on the GGSN, you should first define a set of IP address ranges for a PLMN using the **gprs plmn ip address** command.

It is important that you configure the **gprs plmn ip address** and **gprs charging roamers** commands in their proper order. After you configure the IP address range for a PLMN, use the **gprs charging roamers** command to enable charging for roamers on the GGSN. You can change the IP address range by reissuing the **gprs plmn ip address** command.

To verify your configuration, use the **show gprs charging parameters** command to see if the charging for roamers feature is enabled. To verify your PLMN IP address ranges, use the **show gprs plmn ip address** command.

Examples

The following example specifies the IP address range of a PLMN:

```
gprs plmn ip address 10.0.0.1 10.20.40.50
```

Related Commands

Command	Description
gprs charging roamers	Enables charging for roamers on the GGSN.
show gprs plmn ip address	Displays a list of IP address ranges defined for the PLMN.

gprs pcscf

To configure a group of P-CSCF addresses and enter P-CSCF group configuration mode, use the **gprs pcscf** command in global configuration mode. To disable the P-CSCF server group, issue the **no** form of this command.

gprs pcscf *group-name*

no gprs pcscf *group-name*

Syntax Description

group-name	Specifies the name of a P-CSCF server group and enters P-CSCF group configuration mode.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs pcscf** command to define a P-CSCF server group for P-CSCF Discovery and enter P-CSCF group configuration mode.

The GGSN can be configured to return a list of preconfigured Proxy Call Session Control Function (P-CSCF) server addresses for an APN when it receives a Create PDP Context request that contains a "P-CSCF Address Request" field in the PCO.

The MS sets the P-CSCF Address Request field of the PCO in the Activate PDP Context request. This request is forwarded to the GGSN in the Create PDP Context request from the SGSN. Upon receiving, the GGSN returns all the P-CSCF addresses configured for the APN in the "P-CSCF Address" field of the PCO.

If a Create PDP Context Request does not contain the P-CSCF address request field in the PCO, or if no P-CSCF addresses are preconfigured, the Create PDP Context Response will not return any P-CSCF addresses. An error message will not be generated and the Create PDP Context Request will be processed.

To configure the P-CSCF Discovery support, you must preconfigure P-CSCF server groups on the GGSN using the **gprs pcscf** command and configure P-CSCF server groups for an APN using the **pcscf** access-point configuration command.

Note The order of the addresses returned in the "P-CSCF Address Field" of the PCO is the same as the order in which they are defined in the P-CSCF server group and the groups are associated with the APN.

Examples

The following example configures a P-CSCF group identified as “groupA”:

```
gprs pcscf groupA
```

Related Commands

Command	Description
pcscf	Assigns a P-CSCF server group to an APN.
server	Specifies the IP address of a P-CSCF server you want to include in the P-CSCF server group.
show gprs access-point	Displays information about access points on the GGSN.
show gprs pcscf	Displays a summary of the P-CSCF groups configured on the GGSN.

gprs qos bandwidth-pool

Command	Description
pcscf	Assigns a P-CSCF server group to an APN.
server	Specifies the IP address of a P-CSCF server you want to include in the P-CSCF server group.
show gprs access-point	Displays information about access points on the GGSN.
show gprs pcscf	Displays a summary of the P-CSCF groups configured on the GGSN.

To create or modify a Call Admission Control (CAC) bandwidth pool that can be attached to one or more APNs, use the **gprs qos bandwidth-pool** command in global configuration mode. To delete the bandwidth pool, use the **no** form of this command.

gprs qos bandwidth-pool *pool-name*

no gprs qos bandwidth-pool *pool-name*

Syntax Description

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

Defaults

No bandwidth pools are configured.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The CAC feature ensures that required network resources are available for real-time data traffic (such as voice, video, etc.). The CAC feature consists of two functions: maximum quality of service (QoS) authorization using CAC maximum QoS policies and bandwidth management.

The CAC bandwidth management function ensures that there is sufficient bandwidth for real-time packet data protocol (PDP) contexts during the PDP context activation and modification process.

The CAC feature uses user-defined bandwidth pools to negotiate and reserve bandwidth. In these pools, you define the total bandwidth allocated to that pool and then allocate a percentage of that bandwidth to each traffic class.

In the following example, bandwidth pool (pool A) has been created with 100000 kbps allocated to it. Additionally, a percentage of that 100000 kbps of bandwidth has been allocated to each traffic class, creating four "traffic class-based" bandwidth pools.

```
gprs bandwidth-pool A
  bandwidth 100000
  traffic-class conversational percent 40
  traffic-class streaming percent 30
  traffic-class interactive percent 20
  traffic-class background percent 10
```

Note The CAC feature requires that Universal Mobile Telecommunications System (UMTS) QoS is enabled on the GGSN. For more information on configuring UMTS QoS on the GGSN, see the *GGSN Release 6.0 Configuration Guide*.

Once a bandwidth pool is allocated for a traffic class, it cannot be borrowed by the other sub pools allocated for the different traffic classes. The request is only admitted within the bandwidth pool to which the traffic class belongs.

Use the **gprs qos bandwidth-pool** command to create or modify a CAC bandwidth pool and apply the bandwidth pool to one or more APNs using the **bandwidth-pool** access point configuration command.

Examples

The following example creates a bandwidth pool named "pool a":

```
gprs qos bandwidth pool a
```

Related Commands

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

gprs qos cac-policy

To create or modify a Call Admission Control (CAC) maximum quality of service (QoS) policy that can be attached to one or more access point names (APNs), and enter CAC maximum QoS policy configuration mode, use the **gprs qos cac-policy** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs qos cac-policy *policy-name*

no gprs qos cac-policy *policy-name*

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The CAC feature on the gateway GPRS support node (GGSN) ensures that required network resources are available for real-time data traffic such as voice and video. CAC is applied at the APN and consists of two functions: maximum QoS authorization and bandwidth management.

The CAC maximum QoS authorization function ensures that the QoS requested by a Create packet data protocol (PDP) Context does not exceed the maximum QoS configured within an APN. Using a *CAC maximum QoS policy*, you define certain QoS parameters within a policy and attach the policy to an APN. The CAC maximum QoS policy limits the QoS requested by the PDP during its creation and modification process.

Use the **gprs qos cac-policy** command to create or modify a CAC maximum QoS policy and apply the policy to an APN using the **cac-policy** access point configuration command.

Note The CAC feature requires that Universal Mobile Telecommunications System (UMTS) QoS has been configured. For information on configuring UMTS QoS, see the *GGSN Release 6.0 Configuration Guide*.

Once you have entered policy configuration mode using the **gprs qos cac-policy** command, you can configure the following QoS parameters in a policy and apply the policy to an APN:

- Maximum number of active PDP contexts (**maximum pdp-context** command)
- Maximum bit rate (**mbr traffic-class** command)
- Guaranteed bit rate (**gbr traffic-class** command)
- Maximum traffic class (**maximum traffic-class** command)
- Traffic handling priority (**maximum traffic-class** command with **priority** option)
- Delay class (**maximum delay-class** command)
- Peak throughput class (**maximum peak-throughput** command)

Examples

The following example creates a CAC maximum QoS policy named "policy a":

```
gprs qos cac-policy a
```

Related Commands

Command	Description
cac-policy	Enables the maximum QoS policy function of the CAC feature and applies a policy to an APN.
gbr traffic-class	Specifies the maximum guaranteed bit rate (GBR) that can be allowed in uplink and downlink directions for real-time classes (conversational and streaming) at an APN.
maximum delay-class	Defines the maximum delay class for R97/R98 (GPRS) QoS that can be accepted.
maximum peak-throughput	Defines the maximum peak throughput for R97/R98 (GPRS) QoS that can be accepted.
maximum pdp-context	Specifies the maximum number PDP contexts that can be created for a particular APN.
maximum traffic-class	Defines the highest traffic class that can be accepted.
mbr traffic-class	Specifies the maximum bit rate (MBR) that can be allowed for each traffic class in both directions (downlink and uplink).

gprs qos default-response requested

To specify that the gateway GPRS support node (GGSN) sets its default quality of service (QoS) values in the response message exactly as requested in the Create packet data protocol (PDP) Context request message, use the **gprs qos default-response requested** command in global configuration mode. To return to the default QoS, use the **no** form of this command.

gprs qos default-response requested

no gprs qos default-response requested

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled. The GGSN sets its QoS default to the best-effort class.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **gprs qos default-response requested** command is useful only when canonical QoS is not configured on the GGSN. Canonical QoS is enabled using the **gprs qos map canonical-qos** command.

When canonical QoS is not enabled, and the **gprs qos default-response requested** command has not been configured on the GGSN, the GGSN always sets its QoS values to best-effort in the response message.

Examples

The following example enables the GGSN to set its QoS values in the response message according to the QoS values requested in the Create PDP Context request message:

```
gprs qos default-response requested
```

Related Commands

Command	Description
gprs qos map canonical-qos	Enables mapping of GPRS QoS categories to a canonical QoS method that includes best-effort, normal, and premium QoS classes.

gprs qos map canonical-qos

To enable mapping of general packet radio service (GPRS) quality of service (QoS) categories to a canonical QoS method that includes best-effort, normal, and premium QoS classes, use the **gprs qos map canonical-qos** command in global configuration mode. To disable canonical mapping, use the **no** form of this command.

gprs qos map canonical-qos

no gprs qos map canonical-qos

Syntax Description

This command has no arguments or keywords.

Defaults

Canonical QoS mapping is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **qprs qos map canonical-qos** command to map GPRS QoS into the following canonical categories: best effort, normal, and premium.

Examples

The following example shows canonical QoS mapping enabled:

```
qos map canonical-qos
```

Related Commands

Command	Description
gprs canonical-qos best-effort bandwidth-factor	Specifies the bandwidth factor to be applied to the canonical best-effort QoS class.
gprs canonical-qos gsn-resource-factor	Specifies a value that is used by the GGSN to calculate the QoS level provided to mobile users.
gprs canonical-qos map tos	Specifies a QoS mapping from the canonical QoS classes to an IP ToS category.
gprs canonical-qos premium mean-throughput-deviation	Specifies a mean throughput deviation factor that the GGSN uses to calculate the allowable data throughput for QoS.

gprs qos map delay

To enable mapping of general packet radio service (GPRS) quality of service (QoS) categories to delay QoS classes, use the **gprs qos map delay** command in global configuration mode. To disable delay mapping, use the **no** form of this command.

gprs qos map delay

no gprs qos map delay

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs qos map delay** command to enable QoS delay mapping on the gateway GPRS support node (GGSN). To map the QoS delay classes (class 1, class 2, class 3, and best effort) to IP type of service (ToS) categories, use the **gprs delay-qos map tos** command.

Examples

The following example enables delay QoS mapping:

```
gprs qos map delay
```

Related Commands

Command	Description
gprs delay-qos map tos	Specifies a QoS mapping from the delay QoS classes to an IP ToS category.
gprs qos default-response requested	Configures the GGSN to set its default QoS mapping values in a Create PDP Context response which has no QoS mapping selected.

gprs qos map umts

To enable universal mobile telecommunication system (UMTS) quality of service (QoS) on the gateway GPRS support node (GGSN), use the **gprs qos map umts** command in global configuration mode. To disable this mapping and return to the default QoS mapping, use the **no** form of this command.

gprs qos map umts

no gprs qos map umts

Syntax Description

This command has no arguments or keywords.

Defaults

UMTS QoS mapping is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs qos map umts** command to enable UMTS QoS mapping.

Examples

The following example enables UMTS traffic QoS mapping:

```
gprs qos map umts
```

Related Commands

Command	Description
gprs umts-qos map traffic-class	Specifies a QoS mapping from the UMTS traffic classes to a DiffServ PHB group.
gprs umts-qos map diffserv-phb	Assigns a DSCP to a DiffServ PHB group.
gprs umts-qos dscp unmodified	Specifies that the subscriber datagram be forwarded through the GTP path without modifying its DSCP.

Command	Description
show gprs qos status	Displays QoS statistics for the GGSN.
show gprs umts-qos map traffic-class	Displays UMTS QoS mapping information.

gprs radius attribute chap-challenge

To specify that the CHAP challenge always be included in the Challenge Attribute field (and not in the Authenticator field) in an Access-Request to the Remote Access Dial-In User Service (RADIUS) server, use **gprs radius attribute chap-challenge global configuration** command in global configuration mode. To disable, use the **no** form of this command.

gprs radius attribute chap-challenge

no gprs radius attribute chap-challenge

Syntax Description

This command has no arguments or keywords.

Defaults

If the CHAP challenge length is 16 bytes, it is sent in the Authenticator field of an Access-Request. If it is greater than 16 bytes, it is sent in the Challenge Attribute field.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs radius attribute chap-challenge** command when configuring RADIUS security on the GGSN.

When the **gprs radius attribute chap-challenge** command is configured, the CHAP challenge is always sent in the Challenge Attribute field of an Access-Request to the RADIUS server and not in the Authenticator field. When the command is not configured, the CHAP challenge is sent in the Authenticator field unless the challenge exceeds 16 bytes, in which case, it is sent in the Challenge Attribute field of the Access-Request.

Examples

The following example configures the CHAP challenge to always be sent in an Access Request to the RADIUS server:

```
gprs radius attribute chap-challenge
```

Related Commands

show gprs gtp pdp-context	Displays a list of the currently active PDP contexts (mobile sessions).

gprs radius attribute quota-server ocs-address

To configure the GGSN to send the Online Charging Server (OCS) IP address (received in an Access-Accept response from a RADIUS server) in the csg:quota server attribute in Accounting-Start messages, use **gprs radius attribute quota-server ocs-address** global configuration command in global configuration mode. To disable this configuration, use the **no** form of this command.

gprs radius attribute quota-server ocs-address

no gprs radius attribute quota-server ocs-address

Syntax Description

This command has no arguments or keywords.

Defaults

The GGSN sends its own IP address in the csg:quota server field.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)XB2	This command was introduced.
12.4(9)XG	This command was integrated into Cisco IOS Release 12.4(9)XG.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **gprs radius attribute quota-server ocs-address** command to configure the GGSN to send the IP address and port of an external OCS (that has been received in the conditional "csg:quota_server" attribute in an Access-Accept response for a prepaid subscriber from the RADIUS server), in Accounting-Start messages to the CSG.

When the **gprs radius attribute quota-server ocs-address** command has been configured, the CSG can interface directly with an external OCS to which it has a GTP' interface. This external OCS will function as the quota server for the prepaid users, providing an alternate online billing solution than the one provided by the GGSN, interacting with Diameter/DCCA, functioning as the quota server for prepaid users.

When the **gprs radius attribute quota-server ocs-address** command is configure, the GGSN functions as the quota server for just postpaid users. The GGSN does not generate enhance G-CDRs for prepaid users, however, it does continue to generate G-CDRs for them.

For more information about the GGSN support for OCS address selection, see the Configuring Enhance Service-Aware Billing" chapter of the *GGSN Configuration Guide*.

Examples

The following configures the GGSN to send the IP address of an external OCS in the csg:quota server attribute in Accounting-Start messages for prepaid users:

```
gprs radius attribute quota-server ocs-address
```

Related Commands

show gprs gtp pdp-context	Displays a list of the currently active PDP contexts (mobile sessions).

gprs radius attribute session-timeout

To specify that the Session-Timeout (Attribute 27) field be included in a Remote Access Dial-In User Service (RADIUS) request, use the **gprs radius attribute session-timeout** command in global configuration mode. To disable, use the **no** form of this command.

gprs radius attribute session-timeout

no gprs radius attribute session-timeout

Syntax Description

This command has no arguments or keywords.

Defaults

Attribute 27 is not included.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs radius attribute session-timeout** command to configure the Session-Timeout (Attribute 27) field be included in a Remote Access Dial-In User Service (RADIUS) request.

The GGSN stores the attribute value received in Access-Accept packets sent by the AAA server and terminates the PDP context upon expiration of the time. You can configure the number of seconds the GGSN allows a session to be active before terminating the session at the global level (**gprs gtp pdp-context timeout session** command) and at the access-point level (**gtp pdp-context timeout session** command.

Examples

The following example configures Attribute 27 to always be sent in an Access Request to the RADIUS server:

```
gprs radius attribute session-timeout
```

Related Commands

Command	Description
gprs gtp pdp-context timeout session	Specifies the time, in seconds, that the GGSN allows a session to be active at any access point before terminating the session.
gtp pdp-context timeout session	Specifies the time, in seconds, that a GGSN allows a session to be active at a particular APN before terminating the session.

gprs radius msisdn first-byte

To specify that the first byte of the mobile station ISDN (MSISDN) information element (IE) is included in a RADIUS request, use the **gprs radius msisdn first-byte** command in global configuration mode. To remove the first byte from the MSISDN IE in a RADIUS request, use the **no** form of this command.

gprs radius msisdn first-byte

no gprs radius msisdn first-byte

Syntax Description

This command has no arguments or keywords.

Defaults

The first byte is not included.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs radius msisdn first-byte** command when configuring RADIUS security on the gateway GPRS support node (GGSN).

The first octet of an MSISDN IE using E.164 addressing is 91 in hexadecimal, that is, 10010001. In this 91 code, the 1 is the extension bit, 001 is the international number, and 0001 indicates E.164 numbering.

Examples

The following example specifies that the first byte of the MSISDN IE is included in a RADIUS request:

```
gprs radius msisdn first-byte
```

gprs redundancy

To enable GPRS tunneling protocol session redundancy (GTP-SR) on a gateway GPRS support node (GGSN), use the **gprs redundancy** command in global configuration mode. To disable GTP-SR, use the **no** form of this command.

gprs redundancy

no gprs redundancy

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs redundancy** command to enable GTP-SR on a GGSN.

Cisco GGSN Release 5.1 and later supports Active/Standby, 1-to-1 inter-device GTP-SR. GTP-SR enables two GGSNs to appear as one network entity and ensures that continuous service is provided to mobile subscribers in the event one of the GGSNs fails.

In a GTP-SR implementation, the Active GGSN establishes and terminates packet data protocol (PDP) sessions and sends required stateful data to the Standby GGSN. To stay current on the states of active PDP sessions, the Standby GGSN receives the stateful data sent by the Active GGSN. As soon as the Standby GGSN detects that the Active GGSN has failed, it becomes active and assumes the responsibilities of the Active GGSN.

Before GTP-SR can be enabled on two redundant GGSNs, a GTP-SR inter-device infrastructure must be configured. For information on configuring a inter-device infrastructure, see the "Configuring GTP Session Redundancy" chapter of the *Cisco GGSN Release 6.0 Configuration Guide*.

Examples

The following example enables GTP-SR on a GGSN:

```
gprs redundancy
```

Related Commands

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

gprs redundancy charging sync-window cdr rec-seqnum

To configure the window size used to determine when the call detail record (CDR) record sequence number needs to be synchronized to the Standby gateway GPRS support node (GGSN), use the **gprs redundancy charging sync-window cdr rec-seqnum** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs redundancy charging sync-window cdr rec-seqnum size

no gprs redundancy charging sync-window cdr rec-seqnum size

Syntax Description

size	Configures the window size used to determine when the CDR record sequence number needs to be synchronized.Valid range is 1 to 20.

Defaults

10

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs redundancy charging sync-window cdr rec-seqnum** command to configure the window size used to determine when the record sequence number needs to be synchronized.

The record sequence number is used by the charging gateway to detect duplicate CDRs associated with a PDP context. To minimize the amount of data being synchronized to the Standby GGSN, the record sequence number is not synchronized each time a CDR is closed. Instead, a window threshold for the record sequence number is synchronized each time a CDR closes. The current value of the record sequence number and the record number last synchronized for a PDP context is checked, and if the difference is the value configured for the window size using the **gprs redundancy charging sync-window cdr rec-seqnum** global configuration command, the current record sequence number is synchronized to the Standby GGSN.

When a Standby GGSN becomes the Active GGSN, it starts from the last value synchronized, plus the window size.

Examples

The following example configures a window size of 15:

```
gprs redundancy charging sync-window cdr rec-seqnum 15
```

Related Commands

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

gprs redundancy charging sync-window gtpp seqnum

To configure the window size used to determine when the GTP' sequence number needs to be synchronized to the Standby gateway GPRS support node (GGSN), use the **gprs redundancy charging sync-window gtpp seqnum** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs redundancy charging sync-window gtpp seqnum *size*

no gprs redundancy charging sync-window gtpp seqnum *size*

Syntax Description

size	Configures the window size used to determine when the GTP' sequence number needs to be synchronized. Valid range is 5 to 65535. **Note** Since a GGSN can transmit 128 GTP packets without any acknowledgement, we recommend that you configure the window size to be greater than 128.

Defaults

10000

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs redundancy charging sync-window gtpp seqnum** command to configure the window size used to determine when the GTP' sequence number needs to be synchronized.

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

To minimize the amount of data being synchronized to the Standby GGSN, the GTP' sequence number is not synchronized each time a CDR is closed. Instead, a window threshold for the GTP' sequence number is synchronized each time a CDR message is sent. The current value of the GTP' sequence number and the gtpp sequence number last synchronized for a PDP context is checked and if the difference is the value configured for the window size (using the **gprs redundancy charging sync-window gtpp seqnum** global configuration command), the current GTP prime sequence number is synchronized to the Standby GGSN.

When a Standby GGSN becomes the Active GGSN, it starts from the last value synchronized plus the window size.

Examples

The following example configures the window size for the GTP' sequence number synchronization to be 120:

```
gprs redundancy charging sync-window gtpp seqnum 120
```

Related Commands

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

gprs service-aware

To enable service-aware billing on the gateway GPRS support node (GGSN), use the **gprs service-aware** command in global configuration mode. To disable the support, use the **no** form of this command

gprs service-aware

no gprs service-aware

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs service-aware** global configuration command to enable service-aware billing on the on the GGSN.

Note Service-aware billing must be enabled before configuring other enhanced service-aware billing features on the GGSN. These features include the GGSN-to-CSG interface, the GGSN-to-Diameter/DCCA interface, and support of enhanced service-level G-CDRs.

Examples

The following configuration example enables service-aware billing on a GGSN:

```
gprs service-aware
```

Related Commands

Command	Description
service-aware	Enables service-aware billing for a particular access point.

gprs service-mode

To configure the global service-mode state of a gateway GPRS support node (GGSN), use the **gprs service-mode** command in global configuration mode.

gprs service-mode {operational | maintenance}

no gprs service-mode {operational | maintenance}

Syntax Description

operational	Specifies that the service-mode state of the GGSN is operational.
maintenance	Specifies that the service-mode state of the GGSN is maintenance.

Defaults

Operational.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs service-mode** command to place the global service-mode state of a GGSN in maintenance mode.

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

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

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

Examples

The following example places a GGSN in maintenance mode:

```
gprs service-mode maintenance
```

Related Commands

Command	Description
service-mode	Configures the service-mode state of an APN.
gprs service-mode test imsi	Configures a test user for which you can Create PDP Contexts to test an APN configuration.
show gprs service-mode	Displays the current global service mode state of the GGSN and the last time it was changed.

gprs service-mode test imsi

To configure a test user for which you can Create PDP Contexts to test an APN configuration, use the **gprs service-mode test imsi** command in global configuration mode. To remove the test user configuration, use the **no** form of this command.

gprs service-mode test imsi *imsi-value*

no gprs service-mode test imsi *imsi-value*

Syntax Description

imsi-value	International Mobile Subscriber Identity (IMSI) value for which PDP contexts are to be created.

Defaults

No test user is configured on the GGSN.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs service-mode test imsi** command to configure a test user for which Create PDP Contexts will be created to test configurations.

Only one test user can be configured per GGSN.

Note PDP context creation from a test user is only supported while a GGSN is in operational mode.

Examples

The following example creates a test user with the IMSI 211F111130000000:

```
gprs service-mode test imsi 211F111130000000
```

Related Commands

Command	Description
gprs service-mode	Configures the service-mode state of a GGSN.
service-mode	Configures the service-mode state of an APN.
show gprs service-mode	Displays the current global service mode state of the GGSN and the last time it was changed.

gprs slb mode

To define the Cisco IOS SLB operation mode for gateway GPRS support node (GGSN)-IOS SLB messaging, use the **gprs slb mode** command in global configuration mode.

gprs slb mode {dispatched | directed}

Syntax Description

dispatched	Specifies that the Cisco IOS SLB is operating in dispatched mode.
directed	Specifies that the Cisco IOS SLB is operating in directed server NAT mode.

Defaults

Dispatched

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs slb mode** command to defined the Cisco IOS SLB mode of operation when configuring GGSN-IOS SLB messaging.

GGSN-IOS SLB Messaging CAC Failure Notification Support

When configuring support for GGSN-IOS SLB messaging CAC failure notifications, if Cisco IOS SLB is operating in dispatched mode, the virtual server that forwarded the Create PDP Context request to the GGSN is known to the GGSN, and the GGSN can send the CAC failure notification directly to that server. Therefore, only the **gprs slb notify** command is required to enable GGSN-SLB messaging on the GGSN.

However, if the Cisco IOS SLB is functioning in directed server NAT mode, the virtual server is not known to the GGSN. Therefore, a list of virtual servers that the GGSN should notify when a CAC failure occurs must be defined on the GGSN using the **gprs slb vserver** global configuration command and the Cisco IOS SLB mode of operation must be defined using the **gprs slb mode** global configuration command.

Note When configuring support for GGSN-IOS SLB messaging CAC failure notifications when the Cisco IOS SLB is functioning in directed server NAT mode, the **gprs slb mode** and **gprs slb vserver** global configuration commands are required.

GGSN-IOS SLB Messaging Delete Notification Support

When configuring support for GGSN-IOS SLB messaging delete notifications (GTP IMSI sticky database support), the Cisco IOS SLB operation mode must be defined using the **gprs slb mode** command and a list of virtual servers that the GGSN should send delete notifications must be defined on the GGSN using the **gprs slb vserver** global configuration command.

For complete information on configuring GGSN-IOS SLB messaging, refer to the “Configuring Messaging from the GGSN to the Cisco IOS SLB” section of the “Configuring Load Balancing on the GGSN” chapter for the *GGSN Configuration Guide*.

Examples

The following example defines Cisco IOS SLB to be in directed server NAT mode:

```
gprs slb mode directed
```

Related Commands

Command	Description
clear gprs slb statistics	Clears Cisco IOS SLB statistics.
gprs slb notify	Configures the GGSN to send notifications to the Cisco IOS SLB when a specific condition exists that affects a session forwarded by the Cisco IOS SLB.
gprs slb vserver	Configures the Cisco IOS SLB virtual servers to be notified by the GGSN when the specific condition defined using the **gprs slb notify** command occurs.
show gprs slb detail	Displays Cisco IOS SLB related information, such as the operation mode, virtual servers addresses, and statistics.
show gprs slb mode	Displays the Cisco IOS SLB mode of operation defined on the GGSN.
show gprs slb statistics	Displays Cisco IOS SLB statistics.
show gprs slb vservers	Displays the list of defined Cisco IOS SLB virtual servers.

gprs slb notify

To enable the gateway GPRS support node (GGSN) to notify the Cisco IOS Server Load Balancing (SLB) when a specific condition occurs, use the **gprs slb notify** global configuration command. To disable GGSN-IOS SLB messaging, issue the **no** form of this command.

gprs slb notify {cac-failure | session-deletion}

no gprs slb notify {cac-failure | session-deletion}

Syntax Description

cac-failure	Specifies that the GGSN notify the Cisco IOS SLB when a universal mobile telecommunications system (UMTS) quality of server (QoS) call admission control (CAC) or canonical QoS failure has caused a Create packet data protocol (PDP) Context request to be rejected.
session-deletion	Configures the GGSN to send a delete notification message to the Cisco IOS SLB when the last PDP context associated with an international mobile subscriber identity (IMSI) is deleted.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into the Cisco IOS Release 12.3(14)YU and the **session-deletion** keyword option was added.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs slb notify** command to enable GGSN-IOS SLB messaging.

The GGSN-IOS SLB messaging function enables you to configure the GGSN to notify the Cisco IOS SLB when a certain condition exists that affects a session forwarded by the Cisco IOS SLB. The notification also instructs the Cisco IOS SLB on how to react to the condition.

There are two types of GGSN-IOS SLB notifications that can be configured using the **gprs slb notify** command—CAC failure notifications and delete notifications (for GTP IMSI sticky database support).

CAC Failure Notifications

When support for CAC failure notifications is configured on the GGSN and the Cisco IOS SLB, when a Create PDP Context request is rejected by the GGSN because of a CAC failure, the GGSN notifies the Cisco IOS SLB that the failure has occurred, and instructs the Cisco IOS SLB to reassign the session to another GGSN in the server farm.

Note If the Cisco IOS SLB is functioning in directed server NAT mode, a list of virtual servers must be defined on the GGSN using the **gprs slb vserver** global configuration command, and the Cisco IOS SLB mode of operation must be defined using the **gprs slb mode** global configuration command.

Delete Notifications (GTP IMSI Sticky Database Support)

When support for delete notifications is configured on the GGSN and the Cisco IOS SLB, a sticky database entry is created on the Cisco IOS SLB when the first Create PDP Context request from a subscriber is received. When the last PDP context of that IMSI is deleted on the GGSN, the GGSN sends a delete notification to the Cisco IOS SLB that instructs the Cisco IOS SLB to remove the sticky entry from the database.

Note This configuration requires that the **virtual** virtual server configuration command be configured with the **service gtp** keywords specified.

For complete information on configuring GGSN-IOS SLB messaging, refer to the “Configuring Messaging from the GGSN to the Cisco IOS SLB” section of the “Configuring Load Balancing on the GGSN” chapter for the *GGSN Configuration Guide*.

Examples

Example 1

The following example configures the GGSN to notify the Cisco IOS SLB when a Create PDP Context request has been rejected because of a UMTS QoS CAC failure and the Cisco IOS SLB is functioning in dispatched mode.

On the GGSN:

```
gprs slb notify cac-failure
```

On the Cisco IOS SLB:

```
gtp notification cac 4
```

Example 2

The following example configures the GGSN to notify the Cisco IOS SLB when a Create PDP Context request has been rejected because of a UMTS QoS CAC failure and the Cisco IOS SLB is functioning in directed server NAT mode.

On the GGSN:

```
gprs slb mode directed
gprs slb notify cac-failure
gprs slb vserver 10.10.10.10
```

On the Cisco IOS SLB:

```
gtp notification cac 4
```

Example 3

The following example configures the GGSN to notify the Cisco IOS SLB (functioning in directed server NAT mode) when the last PDP context associated with a IMSI is deleted:

On the GGSN:

```
gprs slb mode directed
gprs slb notify session-deletion
gprs slb vserver 10.10.10.10
```

On the Cisco IOS SLB:

```
sticky gtp imsi group 1
```

Example 4

The following example configures the GGSN to notify the Cisco IOS SLB (functioning in dispatched mode) when the last PDP context associated with a IMSI is deleted:

On the GGSN:

```
gprs slb mode dispatched
gprs slb notify session-deletion
gprs slb vserver 10.10.10.10
```

On the Cisco IOS SLB:

```
sticky gtp imsi group 1
```

Related Commands

Command	Description
clear gprs slb statistics	Clears Cisco IOS SLB statistics.
gprs slb mode	Defines the Cisco IOS SLB operation mode.
gprs slb vserver	Configures the Cisco IOS SLB virtual servers to be notified by the GGSN when the specific condition defined using the **gprs slb notify** command occurs.
show gprs slb detail	Displays Cisco IOS SLB related information, such as the operation mode, virtual servers addresses, and statistics.
show gprs slb mode	Displays the Cisco IOS SLB mode of operation defined on the GGSN.
show gprs slb statistics	Displays Cisco IOS SLB statistics.
show gprs slb vservers	Displays the list of defined Cisco IOS SLB virtual servers.

gprs slb vserver

To configure the Cisco IOS SLB virtual server(s) to be notified by the gateway GPRS support node (GGSN) when the specfic type of condition defined using the **gprs slb notify** command occurs, use the **gprs slb vserver** command in global configuration mode. To remove a virtual server from the list, use the **no** form of this command.

gprs slb vserver *ip_address* [**next-hop ip** *ip-address* [**vrf** *name*]]

no slb vserver *ip_address* [**next-hop ip** *ip-address* [**vrf** *name*]]

Syntax Description

ip_address	IP address of the virtual server.
next-hop ip *ip-address*	(Optional) IP address of the next-hop that can be used to reach the virtual server.
vrf *name*	(Optional) Specifies VPN routing and forwarding instance.

Defaults

No virtual servers are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU and the **next hop** and **vrf** keyword options were added.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gprs slb vserver** global configuration command to defined a list of Cisco IOS SLB virtual servers to be notified by a GGSN when GGSN-IOS SLB messaging is enabled.

For example, if Cisco IOS SLB is functioning in directed server NAT mode, the GGSN will send the notification to all the vservers in the list. However, only the vserver that is processing the PDP context will react to the notification. The other vservers will ignore the notification.

This command is used in conjunction with the **gprs slb notify** and the **gprs slb mode** global configuration commands.

Note This command is not required when configuring support for GGSN-IOS SLB messaging CAC failure notifications when the Cisco IOS SLB is functioning in dispatched mode.

For complete information on configuring GGSN-IOS SLB messaging, refer to the "Configuring Messaging from the GGSN to the Cisco IOS SLB" section of the "Configuring Load Balancing on the GGSN" chapter for the *GGSN Configuration Guide*.

Examples

Example 1

The following example adds a GTP server with the IP address 172.10.10.10 to the list of virtual servers to be notified by the GGSN:

```
gprs slb vserver 172.10.10.10
```

Related Commands

Command	Description
clear gprs slb statistics	Clears Cisco IOS SLB statistics.
gprs slb mode	Defines the Cisco IOS SLB operation mode.
gprs slb notify	Configures the GGSN to send notifications to the Cisco IOS SLB when a certain condition exists that affects a session forwarded by the Cisco IOS SLB.
show gprs slb detail	Displays Cisco IOS SLB related information, such as the operation mode, virtual servers addresses, and statistics.
show gprs slb mode	Displays the Cisco IOS SLB mode of operation defined on the GGSN.
show gprs slb statistics	Displays Cisco IOS SLB statistics.
show gprs slb vservers	Displays the list of defined Cisco IOS SLB virtual servers.

gprs throughput interval

To configure the intervals at which the throughput data is collected for APNs, use the **gprs throughput interval** command in global configuration mode. To return to the default value, use the **no** form of this command.

gprs throughput interval *interval1 interval2*

no gprs throughput interval *interval1 interval2*

Syntax Description

interval	Number of seconds that the GGSN waits before collecting throughput data.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs throughput interval** command to configure the intervals at which the GGSN will collect throughput data for APNs.

Examples

The following example configures the GGSN to collect throughput data every 5 minutes (300 seconds):

```
gprs throughput interval 300
```

Related Commands

Command	Description
show gprs access-point throughput statistics	Displays throughput statistics for access points on a GGSN.

gprs umts-qos dscp unmodified

To specify that the subscriber datagram be forwarded through the GTP path without modifying its DSCP, use the **gprs umts-qos dscp unmodified** command in global configuration mode. To remove this specification and enable the DSCP to be re-marked with the DSCP assigned to the traffic class during the PDP context creation, use the **no** form of this command.

gprs umts-qos dscp unmodified [**up** | **down** | **all**]

no gprs umts-qos dscp unmodified [**up** | **down** | **all**]

Syntax Description

up	(Optional) Specifies subscriber datagram DSCPs in the uplink GTP path.
down	(Optional) Specifies subscriber datagram DSCPs in the downlink GTP path.
all	(Optional) Specifies subscriber datagram DSCPs in all GTP paths.

Defaults

The DSCP in the subscriber datagram is re-marked with the DSCP assigned to the traffic class during the PDP context creation.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs umts-qos dscp unmodified** command to configure the GGSN to forward subscriber datagram DSCPs through the GTP path without modifying the DSCP.

Examples

The following example sets subscriber datagrams in the uplink GTP path to retain their DSCPs:

```
gprs umts-qos dscp unmodified up
```

Related Commands

Command	Description
gprs qos map umts	Enables UMTS QoS on the GGSN.
gprs umts-qos map traffic-class	Specifies a QoS mapping from the UMTS traffic classes to a differentiated services (DiffServ) per-hop behavior (PHB) group.
gprs umts-qos map diffserv-phb	Assigns a differentiated services code point (DSCP) to a DiffServ PHB group.
show gprs qos status	Displays QoS statistics for the GGSN.
show gprs umts-qos map traffic-class	Displays UMTS QoS mapping information.

gprs umts-qos map diffserv-phb

To assign a differentiated services code point (DSCP) to a DiffServ PHB group, use the **gprs umts-qos map diffserv-phb** command in global configuration mode. To set the specified DSCP to the default DiffServ PHB group, use the **no** form of this command.

gprs umts-qos map diffserv-phb *diffserv-phb-group* [*dscp1*] [*dscp2*] [*dscp3*]

no gprs umts-qos map diffserv-phb

Syntax Description

diffserv-phb-group	Specifies the DiffServ PHB group. The PHB groups are: • signalling-class • ef-class • af1-class • af2-class • af3-class • af4-class • best-effort
dscp1	Required for all classes. Specifies one of 64 DSCP values from 0 to 63. The DSCP value corresponds to drop precedence 1.
dscp2	(Optional for AF classes only) Specifies one of 64 DSCP values from 0 to 63. The DSCP value corresponds to drop precedence 2.
dscp3	(Optional for AF classes only) Specifies one of 64 DSCP values from 0 to 63. The DSCP value corresponds to drop precedence 3.

Defaults

The default DSCP value associated with the PHB class is used.

Command Modes

Global configuration

Command History

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

Usage Guidelines

For the Assured Forwarding (AF) PHB group, you can specify up to three DSCP values for each drop precedence. The signalling, EF, and best-effort classes do not have drop precedence, so only the first DSCP value is used. If you enter a value for the *dscp2* or *dscp3* arguments for these classes, it is ignored.

Drop precedence indicates the order in which a packet will be dropped when there is congestion on the network.

Table 1 shows the default DSCP values for each PHB group.

Table 2 Default DSCP Values per PHB Group

PHB	DSCP
Signalling	5?
EF	101110 (46)
AF11	001010 (10)
AF12	001100 (12)
AF13	001110 (14)
AF21	010010 (18)
AF22	010100 (20)
AF23	010110 (22)
AF31	011010 (26)
AF32	011100 (28)
AF33	011110 (30)
AF41	100010 (34)
AF42	100100 (36)
AF43	100110 (38)
Best effort	000000 (0)

Examples

The following example assigns a DSCP value of 31 to the EF class and three DSCP values to AF class2 of 51, 52, and 53:

```
gprs umts-qos map diffserv-phb ef-class 31
gprs umts-qos map diffserv-phb af-class2 51 52 53
```

Related Commands

Command	Description
gprs qos map umts	Enables UMTS QoS on the GGSN.
gprs umts-qos map traffic-class	Specifies a QoS mapping from the UMTS traffic classes to a differentiated services (DiffServ) per-hop behavior (PHB) group.
gprs umts-qos dscp unmodified	Specifies that the subscriber datagram be forwarded through the GTP path without modifying its DSCP.
show gprs qos status	Displays QoS statistics for the GGSN.
show gprs umts-qos map traffic-class	Displays UMTS QoS mapping information.

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.

gprs umts-qos map traffic-class

To specify a QoS mapping from the UMTS traffic classes to a differentiated services (DiffServ) per-hop behavior (PHB) group, use the **gprs umts-qos map traffic-class** command in global configuration mode. To remove a QoS mapping and set the specified traffic class to the default mapping, use the **no** form of this command.

gprs umts-qos map traffic-class *traffic-class diffserv-phb-group*

no gprs umts-qos map traffic-class

Syntax Description

traffic-class	Specifies the traffic class. The UMTS traffic classes are: • signalling • conversational • streaming • interactive • background
diffserv-phb-group	Specifies the DiffServ PHB group. The PHB groups are: • signalling-class • ef-class • af1-class • af2-class • af3-class • af4-class • best-effort

Defaults

You must enable UMTS QoS using the **gprs qos map umts** command before entering this command.

Note Use the **gprs umts-qos map traffic-class** command only if you want to use mapping values other than the defaults.

The default mapping values for the UMTS traffic classes are as follows:

- signalling traffic class to the signalling-class DiffServ PHB group
- conversational traffic class to the ef-class DiffServ PHB group
- streaming traffic class to the af2-class DiffServ PHB group
- interactive traffic class to the af3-class DiffServ PHB group
- background traffic class to the best-effort DiffServ PHB group

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **gprs umts-qos map traffic-class** command to specify a mapping between various QoS UMTS traffic categories and the DiffServ PHB groups.

Examples

The following example specifies a QoS mapping from the UMTS traffic class conversational to the DiffServ PHB group af-class1:

```
gprs umts-qos map traffic-class conversational af1-class
```

Related Commands

Command	Description
gprs qos map umts	Enables UMTS QoS on the GGSN.
gprs umts-qos map diffserv-phb	Assigns a differentiated services code point (DSCP) to a DiffServ PHB group.
gprs umts-qos dscp unmodified	Specifies that the subscriber datagram be forwarded through the GTP path without modifying its DSCP.
show gprs qos status	Displays QoS statistics for the GGSN.
show gprs umts-qos map traffic-class	Displays UMTS QoS mapping information.

gtp pdp-context single pdp-session

To configure the gateway GPRS support node (GGSN) to delete the primary PDP context, and any associated secondary PDP contexts, of a *hanging* PDP session upon receiving a new create request from the same MS that shares the same IP address of the hanging PDP context, use the **gtp pdp-context single pdp-session** command in global configuration mode. To return to the default value, use the **no** form of this command.

gtp pdp-context single pdp-session [**mandatory**]

[**no**] **gtp pdp-context single pdp-session** [**mandatory**]

Syntax Description

mandatory	Specifies that the primary PDP context and any associated secondary PDP contexts be deleted regardless of the RADIUS user profile configuration.

Defaults

Create PDP Context requests that share the IP address of an existing PDP context for the same MS are rejected.

Command Modes

Access-point configuration

Command History

Release	Modification
12.3(8)XU2	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **gtp pdp-context single pdp-session** command to configure the GGSN to delete the primary PDP context, and any associated secondary PDP contexts, of a *hanging* PDP session upon receiving a new create request from the same MS that shares the same IP address of the hanging PDP context.

A hanging PDP context is a PDP context on the GGSN whose corresponding PDP context on the SGSN has already been deleted for some reason.

When this condition occurs and the **gtp pdp-context single pdp-session** command is not configured, if on the same APN, the same MS sends a new Create PDP Context request that has a different NSAPI but has been assigned the same IP address used by the hanging PDP context, the GGSN rejects the new Create PDP Context request.

When the **gtp pdp-context single pdp-session** is configured on an APN, the single PDP session per MS feature is enabled and applies to all users for whom the “gtp-pdp-session=single-session” Cisco VSA has been defined in their RADIUS user profile. If the command is not configured, the feature is not enabled and does not apply to any user regardless of their RADIUS user profile configuration. If the command is configured with the **mandatory** keyword option specified, the feature is enabled and applies to all users on that APN regardless of their RADIUS user profile configuration.

Note This feature is supported on the Cisco 7200 series platform.

Examples

The following example configures the GGSN to delete the primary PDP context, and associated secondary PDP contexts, of a *hanging* PDP context when it receives a new Create PDP Context request that shares the same IP address:

```
gtp pdp-context single pdp-session
```

Related Commands

Command	Description
show gprs access-point	Displays information about access points on the GGSN.
show gprs pdp-context tid	Displays PDP contexts by tunnel ID. This value corresponds to the IMSI plus NSAPI and can be up to 16 numeric digits.

gtp pdp-context timeout idle

To specify the time, in seconds, that a gateway GPRS support node (GGSN) allows a session to be idle at a particular access point before terminating the session, use the **gtp pdp-context timeout idle** access-point configuration command in global configuration mode. To return to the default value, use the **no** form of this command.

gtp pdp-context timeout idle *interval* [**uplink**]

no gtp pdp-context timeout idle

Syntax Description

interval	Time, in seconds, that the GGSN allows a session to be idle at a particular access point before terminating the session. Specify a value between 30 and 4294967 seconds. The value 0 disables the session timeout feature.
uplink	(Optional) Enables the session idle timer in the uplink direction only. When the **uplink** keyword option is not specified, the session idle timer is enabled in both directions (uplink and downlink).

Defaults

259200 seconds (72 hours)

Command Modes

Access-point configuration

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(8)XU1	This command was integrated into Cisco IOS Release 12.3(8)XU1 and the **uplink** keyword option was added.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

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

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

On the GGSN, the session idle timer can be configured globally and at the APN. The value configured at the APN level using the **gtp pdp-context timeout idle** access-point configuration command overrides the value configured globally using the **gprs gtp pdp-context timeout idle** global configuration command. The value configured in the user profile on the RADIUS server overrides the value configured at the APN.

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

You can disable the session idle timer for a particular user by configuring 0 as the session idle time duration in the user profile on the RADIUS server. If a user is authenticated by RADIUS, the session idle time cannot be disabled.

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

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

Examples

The following example shows configuring the GGSN to wait 18000 seconds before ending an idle session:

```
gtp pdp-context timeout idle 18000
```

Related Commands

Command	Description
gprs gtp pdp-context timeout idle	Specifies the time, in seconds, that a GGSN allows a session to be idle before terminating the session.
gprs gtp pdp-context timeout session	Specifies the time, in seconds, that the GGSN allows a session to be active before terminating the session.
gprs idle-pdp-context purge-timer	Specifies the time, in hours, that the GGSN waits before purging idle mobile sessions.
gtp pdp-context timeout session	Specifies the time, in seconds, that a GGSN allows a session to be active at a particular APN before terminating the session.
session idle-time	Specifies the time, in hours, that the GGSN waits before purging idle mobile sessions for an access point.
show gprs gtp pdp-context	Displays a list of the currently active PDP contexts (mobile sessions).

gtp pdp-context timeout session

To specify the time, in seconds, that a gateway GPRS support node (GGSN) allows a session to exist at a particular access point before terminating the session, use the **gprs gtp pdp-context timeout session** command in access-point configuration mode. To return to the default value, use the **no** form of this command.

gtp pdp-context timeout session *seconds*

no gtp pdp-context timeout session *seconds*

Syntax Description

seconds	Time, in seconds, that the GGSN allows a session to exist at a particular access point. Specify a value between 30 and 4294967 seconds.

Defaults

Disabled

Command Modes

Access-point configuration

Command History

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

Usage Guidelines

When enabled using the **gprs radius attribute session-timeout** command, the GGSN supports the RADIUS Session-Timeout (Attribute 27). The GGSN stores the attribute timeout value received in access-accept packets sent by the AAA server and when the duration of a session exceeds the duration configured as absolute session timer, the GGSN terminates the session and all PDP contexts belonging to the session (those with the same IMSI or MS address).

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

Note The active session timeout feature requires that the **gprs radius attribute session-timeout** command has been enabled.

On the GGSN, the absolute session timer can be configured globally and at the APN. The value configured at the APN level using the **gtp pdp-context timeout session** access-point configuration command overrides the value configured globally using the **gprs gtp pdp-context timeout session** global configuration command. The value configured in the user profile on the RADIUS server overrides the value configured at the APN.

Examples

The following example shows configuring the GGSN to wait 86400 seconds before ending a session:

```
gtp pdp-context timeout session 86400
```

Related Commands

Command	Description
gprs gtp pdp-context timeout idle	Specifies the time, in seconds, that a GGSN allows a session to be idle at any access point before terminating the session.
gprs gtp pdp-context timeout session	Specifies the time, in seconds, that the GGSN allows a session to be active at any access point before terminating the session.
gprs idle-pdp-context purge-timer	Specifies the time, in hours, that the GGSN waits before purging idle mobile sessions.
gtp pdp-context timeout idle	Specifies the time, in seconds, that a GGSN allows a session to be idle at a particular APN before terminating the session.
session idle-time	Specifies the time, in hours, that the GGSN waits before purging idle mobile sessions for an access point.
show gprs gtp pdp-context	Displays a list of the currently active PDP contexts (mobile sessions).

gtp response-message wait-accounting

To configure the gateway GPRS support node (GGSN) to wait for a RADIUS accounting response before sending a Create PDP Context response to the SGSN, for Create PDP Context requests received at a particular APN, use the **gtp response-message wait-accounting** command in access-point configuration mode. To configure the GGSN to send a Create PDP Context response to the SGSN after sending a RADIUS start accounting message to the RADIUS server (without waiting for a response from the RADIUS accounting server), use the **no** form of this command.

gtp response-message wait-accounting

no gtp response-message wait-accounting

Syntax Description

This command has no arguments or keywords.

Defaults

The GGSN sends a Create PDP Context response to the SGSN after sending a RADIUS start accounting message to the RADIUS accounting server. The GGSN does not wait for a RADIUS accounting response from the RADIUS accounting server.

Command Modes

Access-point configuration

Command History

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

Usage Guidelines

Use the **gtp response-message wait-accounting** command to configure the GGSN to wait for a RADIUS accounting response from the RADIUS accounting server, before sending a Create PDP Context response to the SGSN.

If the GGSN does not receive a response from the RADIUS accounting server when you have configured the **gtp response-message wait-accounting** command, then the GGSN rejects the PDP context request.

The GGSN supports configuration of RADIUS response message waiting at both the global and access-point configuration levels. You can minimize your configuration by specifying the configuration that you want to support across most APNs, at the global configuration level. Then, at the access-point configuration level, you can selectively modify the behavior that you want to support at a particular APN. Therefore, at the APN configuration level, you can override the global configuration of RADIUS response message waiting.

To configure the GGSN to wait for a RADIUS accounting response as the default behavior for all APNs, use the **gprs gtp response-message wait-accounting** global configuration command. To disable this behavior for a particular APN, use the **no gtp response-message wait-accounting** access-point configuration command.

To verify whether RADIUS response message waiting is enabled or disabled at an APN, you can use the **show gprs access-point** command and observe the value reported in the wait_accounting output field.

Examples

The following examples show only a partial configuration of the GGSN, to highlight those commands related to implementing RADIUS response message waiting. Additional configuration statements are required to complete a full configuration of the GGSN.

Example 1

The following example configures the GGSN to wait for an accounting response from the RADIUS server before sending a Create PDP Context response to the SGSN, for PDP context requests at access-point 1:

```
aaa new-model
!
aaa group server radius foo
 server 10.2.3.4
 server 10.6.7.8
!
aaa authentication ppp foo group foo
aaa authorization network default group radius
aaa accounting exec default start-stop group foo
!
gprs access-point-list gprs
 access-point 1
  access-mode non-transparent
  access-point-name www.pdn1.com
  aaa-group authentication foo
  gtp response-message wait-accounting
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

Example 2

The following example globally configures the GGSN to wait for a RADIUS accounting response from the RADIUS server before sending a Create PDP Context response to the SGSN. The GGSN waits for a response for PDP context requests received across all access points, except access-point 1. RADIUS response message waiting has been overridden at access-point 1 using the **no gtp response-message wait-accounting** command:

```
aaa new-model
!
aaa group server radius foo
 server 10.2.3.4
 server 10.6.7.8
!
aaa authentication ppp foo group foo
aaa authorization network default group radius
aaa accounting exec default start-stop group foo
```

```
!
gprs access-point-list gprs
 access-point 1
  access-mode non-transparent
  access-point-name www.pdn1.com
  aaa-group authentication foo
  no gtp response-message wait-accounting
  exit
 access-point 2
  access-mode non-transparent
  access-point-name www.pdn2.com
  aaa-group authentication foo
!
gprs gtp response-message wait-accounting
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

Related Commands

Command	Description
gprs gtp response-message wait-accounting	Configures the GGSN to wait for a RADIUS accounting response before sending an activate PDP context request to the SGSN, for Create PDP Context requests received across all access points.
show gprs access-point	Displays information about access points on the GGSN.

gtp update qos-fail delete

To configure the GGSN to delete a PDP context for this APN if a GGSN-initiated QoS update fails, use the **gtp update qos-fail delete** command in global configuration mode. To return to the default value, use the **no** form of the command.

gtp update qos-fail delete

no gtp update qos-fail delete

Syntax Description

This command has no arguments or keywords.

Defaults

PDP contexts are not deleted.

Command Modes

Access point configuration

Command History

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

Usage Guidelines

Use this command to configure the GGSN to generate a Delete PDP Context request when a GGSN-initiated Update PDP Context Request for a QoS update fails.

The Acct Stop record generated by the GGSN indicates the update failure.

This configuration applies when the Update PDP Context Response from the SGSN, initiated for a QoS change, times out after n3 tries or the Cause value is a value other than “Request Accepted.”

Note If this command is not configured, the action configured globally using the **gprs gtp update qos-fail delete** command is used.

Examples

The following is an example:

```
Router(access-point-config)#gtp update qos-fail dele
```

Related Commands

Command	Description
gprs gtp update qos-fail delete	Configures the GGSN to delete PDP contexts when GGSN-initiated QoS updates fail.

interface

To specify the logical interface, by name, that the quota server will use to communicate with the Content Services Gateway (CSG), use the **interface** command in quota server configuration mode. To remove the interface, use the **no** form of this command

interface *interface-name*

no interface *interface-name*

Syntax Description

interface-name	Name of the interface that the quota server will use to communicate with the CSG.

Defaults

No default behavior or values.

Command Modes

Quota server configuration

Command History

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

Usage Guidelines

Use the **interface** quota server configuration mode command to specify the logical interface the quota server will use to communicate with the CSG.

We recommend that a loopback interface be used as the quota server interface.

If the path to the CSG is up, using the **no** form of this command will bring the path down. Therefore, ensure that you use the command carefully. It must be configured for proper quota server-to-CSG interworking.

Examples

The following configuration specifies the logical interface “loopback1” as the interface that the quota server will use to communicate with the CSG:

```
ggsn quota-server qs1
 interface loopback1
```

Related Commands .

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

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

ip (iSCSI interface)

To specify the IP address of an iSCSI target in the target profile on the GGSN, use the **ip** command in iSCSI interface configuration mode. To remove the IP address configuration, use the **no** form of the command.

ip *ip_address*

no ip *ip_address*

Syntax Description

ip_address	IP address of the SCSI target.

Command Default

No default behavior or values.

Command Modes

iSCSI interface configuration

Command History

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

Usage Guidelines

Use the **ip** command to specify the IP address of the iSCSI target in an iSCSI target interface profile on the GGSN.

Only one target can be defined per profile.

Examples

The following example configures an iSCSI target interface profile with the name “targetA” to a SCSI target with the IP address “10.0.0.1.”

```
gprs iscsi targetA
  name iqn.2002-10.edu.abc.iol.iscsi.draft20-target:1
  ip 10.0.0.1
  port 3260
```

Related Commands

Command	Description
gprs iscsi	Configures the GGSN to use the specified iSCSI profile for record storage.
gprs iscsi target	Creates an iSCSI interface profile for an iSCSI target (or modifies an existing one), and enters iSCSI interface configuration mode.

Command	Description
name	Defines the name of the target.
port	Specifies the number of the TCP port on which to listen for iSCSI traffic.

ip iscsi target-profile

To create an iSCSI interface profile for an iSCSI target (or modify an existing profile) on the GGSN, and enter iSCSI interface configuration mode, use the **ip iscsi target-profile** command in global configuration mode. To remove the iSCSI interface profile, use the **no** form of the command.

ip iscsi target-profile *target_profile_name*

no ip iscsi target-profile *target_profile_name*

Syntax Description

target_profile_name	Name of the profile.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **ip iscsi target-profile** command to configure an iSCSI target profile on the GGSN. The iSCSI profile enables the GGSN to read/write to a remote iSCSI device (target) on a SAN via an iSCSI interface.

Multiple iSCSI profiles can be configured on the GGSN, however, only one target can be defined per profile, and only one profile at a time can be associated with the GGSN to use the iSCSI interface using the **gprs iscsi** global configuration command.

Note PSD and iSCSI cannot be configured on a GGSN at the same time, therefore, with GGSN Release 8.0 and later, PSD is not supported.

When in iSCSI target interface configuration mode, the following subconfigurations are supported:

- **default**—Sets a command to its defaults
- **exit**—Exits iSCSI target submode
- **ip**—IP address of target (Required)
- **name**—iSCSI target name (Required)
- **no**—Negate a command or set its defaults
- **port**—TCP port of target (Required)
- **record-store**—Record store

- **source-interface**—iSCSI source interface for packets to target
- **target-portal**—Target portal group
- **vrf**—VRF name associated with this target interface profile

Examples

The following example configures an iSCSI interface profile with the name “targetA” to use to store and retrieve charging DTRs (which can contain multiple G-CDRs) when a charging gateway is not available:

```
ip iscsi target-profile targetA
  name iqn.2002-10.edu.abc.iol.iscsi.draft20-target:1
  ip 10.0.0.1
  port 3260
```

Related Commands

Command	Description
gprs iscsi	Configures the GGSN to use the specified iSCSI profile for record storage.
ip	Specifies the IP address of the target on the SAN.
name	Specifies the name of a SCSI target in the iSCSI profile on the GGSN.
port	Specifies the number of the TCP port on which to listen for iSCSI traffic.

ip local pool

To configure a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface, use the **ip local pool** command in global configuration mode. To remove a range of addresses from a pool (the longer of the **no** forms of this command), or to delete an address pool (the shorter of the **no** forms of this command), use one of the **no** forms of this command.

ip local pool {**default** | *poolname*} [*low-ip-address* [*high-ip-address*]] [**group** *group-name*] [**cache-size** *size*] [**recycle delay** *seconds*]

no ip local pool *poolname low-ip-address* [*high-ip-address*]

no ip local pool {**default** | *poolname*}

Syntax Description

default	Creates a default local IP address pool that is used if no other pool is named.
poolname	Name of the local IP address pool.
low-IP-address [*high-IP-address*]	(Optional) First and, optionally, last address in an IP address range.
group *group-name*	(Optional) Creates a pool group.
cache-size *size*	(Optional) Sets the number of IP address entries on the free list that the system checks before assigning a new IP address. Returned IP addresses are placed at the end of the free list. Before assigning a new IP address to a user, the system checks the number of entries from the end of the list (as defined by the **cache-size** *size* option) to verify that there are no returned IP addresses for that user. The range for the cache size is 0 to 100. The default cache size is 20.
recycle delay *seconds*	(Optional) Indicates the time (in seconds) to hold an IP address in the local pool before making it available for reuse.

Defaults

No address pools are configured. Any pool created without the optional **group** keyword is a member of the base system group.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
11.3AA	This command was enhanced to allow address ranges to be added and removed.
12.1(5)DC	This command was enhanced to allow pool groups to be created.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and support was added for the Cisco 6400 node route processor 25v (NRP-25v) and Cisco 7400 platforms.
12.4(15)T	The **recycle delay** keyword and *seconds* argument were added.

Usage Guidelines

Use the **ip local pool** command to create one or more local address pools from which IP addresses are assigned when a peer connects. You may also add another range of IP addresses to an existing pool. To use a named IP address pool on an interface, use the **peer default ip address pool** interface configuration command. A pool name can also be assigned to a specific user using authentication, authorization, and accounting (AAA) RADIUS and TACACS functions.

If no named local IP address pool is created, a default address pool is used on all point-to-point interfaces after the **ip address-pool local** global configuration command is issued. If no explicit IP address pool is assigned, but pool use is requested by use of the **ip address-pool local** command, the special pool named "default" is used.

The optional **group** keyword and associated group name allows the association of an IP address pool with a named group. Any IP address pool created *without* the **group** keyword automatically becomes a member of a *base* system group.

The optional **recycle delay** keyword and its associated time indicates the time in seconds to hold the IP address from the pool before making it available for reuse.

An IP address pool name can be associated with only one group. Subsequent use of the same pool name, within a pool group, is treated as an extension of that pool, and any attempt to associate an existing local IP address pool name with a different pool group is rejected. Therefore, each use of a pool name is an implicit selection of the associated pool group.

Note To reduce the chances of inadvertent generation of duplicate addresses, the system allows creation of the special pool named "default" only in the base system group, that is, no group name can be specified with the pool name "default."

All IP address pools within a pool group are checked to prevent overlapping addresses; however, no checks are made between any group pool member and a pool not in a group. The specification of a named pool within a pool group allows the existence of overlapping IP addresses with pools in other groups, and with pools in the base system group, but not among pools within a group. Otherwise, processing of the IP address pools is not altered by their membership in a group. In particular, these pool names can be specified in **peer** commands and returned in RADIUS and AAA functions with no special processing.

IP address pools can be associated with Virtual Private Networks (VPNs). This association permits flexible IP address pool specifications that are compatible with a VPN and a VPN routing and forwarding (VRF) instance.

The IP address pools can also be used with the **translate** commands for one-step vty-async connections and in certain AAA or TACACS+ authorization functions. Refer to the chapter "Configuring Protocol Translation and Virtual Asynchronous Devices" in the *Cisco IOS Terminal Services Configuration Guide* and the "System Management" part of the *Cisco IOS Configuration Fundamentals Configuration Guide* for more information.

IP address pools are displayed with the **show ip local pool** EXEC command.

Examples

The following example creates a local IP address pool named "pool2," which contains all IP addresses in the range 172.16.23.0 to 172.16.23.255:

```
ip local pool pool2 172.16.23.0 172.16.23.255
```

The following example configures a pool of 1024 IP addresses:

```
no ip local pool default
ip local pool default 10.1.1.0 10.1.4.255
```

Note Although not required, it is good practice to precede local pool definitions with a **no** form of the command to remove any existing pool, because the specification of an existing pool name is taken as a request to extend that pool with the new IP addresses. If the intention is to extend the pool, the **no** form of the command is not applicable.

The following example configures multiple ranges of IP addresses into one pool:

```
ip local pool default 10.1.1.0 10.1.9.255
ip local pool default 10.2.1.0 10.2.9.255
```

The following examples show how to configure two pool groups and IP address pools in the base system group:

```
ip local pool p1-g1 10.1.1.1 10.1.1.50 group grp1
ip local pool p2-g1 10.1.1.100 10.1.1.110 group grp1
ip local pool p1-g2 10.1.1.1 10.1.1.40 group grp2
ip local pool lp1 10.1.1.1 10.1.1.10
ip local pool p3-g1 10.1.2.1 10.1.2.30 group grp1
ip local pool p2-g2 10.1.1.50 10.1.1.70 group grp2
ip local pool lp2 10.1.2.1 10.1.2.10
```

In the example:

- Group grp1 consists of pools p1-g1, p2-g1, and p3-g1.
- Group grp2 consists of pools p1-g2 and p2-g2.
- Pools lp1 and lp2 are not associated with a group and are therefore members of the base system group.

Note that IP address 10.1.1.1 overlaps groups grp1, grp2, and the base system group. Also note that there is no overlap within any group including the base system group, which is unnamed.

The following examples show configurations of IP address pools and groups for use by a VPN and VRF:

```
ip local pool p1-vpn1 10.1.1.1 10.1.1.50 group vpn1
ip local pool p2-vpn1 10.1.1.100 10.1.1.110 group vpn1
ip local pool p1-vpn2 10.1.1.1 10.1.1.40 group vpn2
ip local pool lp1 10.1.1.1 10.1.1.10
ip local pool p3-vpn1 10.1.2.1 10.1.2.30 group vpn1
ip local pool p2-vpn2 10.1.1.50 10.1.1.70 group vpn2
ip local pool lp2 10.1.2.1 10.1.2.10
```

The examples show configuration of two pool groups, including pools in the base system group, as follows:

- Group vpn1 consists of pools p1-vpn1, p2-vpn1, and p3-vpn1.
- Group vpn2 consists of pools p1-vpn2 and p2-vpn2.
- Pools lp1 and lp2 are not associated with a group and are therefore members of the base system group.

Note that IP address 10.1.1.1 overlaps groups vpn1, vpn2, and the base system group. Also note that there is no overlap within any group including the base system group, which is unnamed.

The VPN needs a configuration that selects the proper group by selecting the proper pool based on remote user data. Thus, each user in a given VPN can select an address space using the pool and associated group appropriate for that VPN. Duplicate addresses in other VPNs (other group names) are not a concern, because the address space of a VPN is specific to that VPN.

In the example, a user in group vpn1 is associated with some combination of the pools p1-vpn1, p2-vpn1, and p3-vpn1, and is allocated addresses from that address space. Addresses are returned to the same pool from which they were allocated.

The following example configures a recycle delay of 30 seconds to hold IP addresses in the pool before making them available for reuse:

```
ip local pool default 10.1.1.0 10.1.9.255 recycle delay 30
```

Related Commands

Command	Description
debug ip peer	Displays additional output when IP address pool groups are defined.
ip address-pool	Enables an address pooling mechanism used to supply IP addresses to dial in asynchronous, synchronous, or ISDN point-to-point interfaces.
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.
show ip local pool	Displays statistics for any defined IP address pools.
translate lat	Translates a LAT connection request automatically to another outgoing protocol connection type.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection type.

ip vrf forwarding

To associate a Virtual Private Network (VPN) routing/forwarding instance (VRF) with a Diameter peer, use the **ip vrf forwarding** command in Diameter peer configuration mode. To remove the VRF configuration, use the **no** form of this command

ip vrf forwarding *name*

no ip vrf forward

Syntax Description

name	Name assigned to a VRF.

Defaults

The default is the global routing table.

Command Modes

Diameter peer configuration

Command History

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

Usage Guidelines

Use the **ip vrf** forwarding command to associate a VRF with a Diameter peer.

Examples

The following example shows how to link a VRF to Diameter peer “dcca1”:

```
Router(config)# diameter peer dcca1
Router(config-dia-peer)# ip vrf forwarding vpn1
```

Related Commands .

Command	Description
address ipv4	Configures the IP address of the Diameter peer host.
destination host	Configures the Fully Qualified Domain Name (FQDN) of the Diameter peer
destination realm	Configures the destination realm (domain name) in which the Diameter host is located.
diameter peer	Defines the Diameter peer (server) and enters diameter peer configuration mode.
security	Configures the security protocol to use for the Diameter peer-to-peer connection.
source interface	Configures the interface to use to connect to the Diameter peer.
timer	Configures Diameter base protocol timers for peer-to-peer communication.
transport	Configures the transport protocol to use to connect with the Diameter peer.

ip-access-group

To specify access permissions between an MS and a PDN through the gateway GPRS support node (GGSN) at a particular access point, use the **ip-access-group** command in access-point configuration mode. To disable the input access list, use the **no** form of this command.

ip-access-group *access-list-number* {**in** | **out**}

no ip-access-group *access-list-number* {**in** | **out**}

Syntax Description

access-list-number	Number of an access list that has been set up using the **access-list** command.
in	The specified access list controls access from the PDN to the mobile station.
out	The specified access list controls access from the mobile station to the PDN.

Defaults

No access list is enforced.

Command Modes

Access-point configuration

Command History

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

Usage Guidelines

Use the **ip-access-group** command to specify an access list that indicates whether users are given or denied permission to access the mobile station from the PDN through the GGSN using a specified access point.

Examples

The following example grants access-list 101 inbound access to the mobile station from the PDN through the GGSN:

```
access-list 101 permit ip 10.0.0.2 0.255.255.255 any
interface virtual-template 1
 ip unnumber loopback 1
 no ip directed-broadcast
 encapsulation gtp
 gprs access-point-list abc
!
gprs access-point-list abc
 access-point 1
  access-point-name gprs.somewhere.com
  dhcp-server 10.100.0.3
  ip-access-group 101 in
  exit
!
```

ip-address-pool

To specify a dynamic address allocation method using IP address pools for the current access point, use the **ip-address-pool** command in access-point configuration mode. To return to the default value, use the **no** form of this command.

ip-address-pool {**dhcp-proxy-client** | **radius-client** | **local** *pool-name* | **disable**}

no ip-address-pool {**dhcp-proxy-client** | **radius-client** | **local** *pool-name* | **disable**}

Syntax Description

dhcp-proxy-client	The access-point IP address pool is allocated using a DHCP server.
radius-client	The access-point IP address pool is allocated using a RADIUS server.
local	The access-point IP address pool is allocated using a locally configured address pool.
disable	Disables dynamic address allocation for this access point.

Defaults

The global setting specified with the **gprs default ip-address-pool** command is used. The default value for the global configuration command is that IP address pools are disabled.

Command Modes

Access-point configuration

Command History

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

Usage Guidelines

You can specify an IP allocation method for an access point in two ways:

- Enter access-point configuration mode and use the **ip-address-pool** command to specify an IP address allocation method for the current access point.
- Specify a global value for the IP address pool by issuing the **gprs default ip-address-pool** command. In that case, you do not need to specify an address-pool method for the specific access point.

If you specify **dhcp-proxy-client** as the method for allocating IP addresses, then you must configure a DHCP server for IP address allocation. You can do this at the global configuration level using the **gprs default-dhcp server** command, or at the access point level using the **dhcp-server** command.

If you specify **radius-client** as the method for allocating IP addresses, then you must configure a RADIUS server for IP address allocation, configure AAA on the GGSN, and configure AAA server groups globally on the GGSN or at the access point. For more information about configuring RADIUS on the GGSN, refer to the Usage Guidelines section for the **aaa-group** and **gprs default aaa-group** commands.

Note Configuring a local IP address pool under an APN (using the **ip-address-pool local** access-point configuration command) improves the PDP context activation rate as the number of PDP contexts increases.

Examples

The following example configures DHCP as the IP address pool allocation method for access-point 1 and specifies that the other access points use the global default, which is specified as RADIUS:

```
aaa new-model
!
aaa group server radius foo
 server 10.2.3.4
 server 10.6.7.8
aaa group server radius foo1
 server 10.10.0.1
!
aaa authentication ppp foo group foo
aaa authentication ppp foo group foo1
aaa authorization network default group radius
aaa accounting exec default start-stop group foo
aaa accounting network foo1 start-stop group foo1
!
interface Loopback0
 ip address 10.88.0.1 255.255.255.255
!
interface virtual-template 1
 ip unnumber Loopback0
 no ip directed-broadcast
 encapsulation gtp
 gprs access-point-list abc
!
gprs access-point-list abc
 access-point 1
  access-point-name gprs.pdn1.com
  ip address-pool dhcp-proxy-client
  aggregate auto
  dhcp-server 10.100.0.3
  dhcp-gateway-address 10.88.0.1
  exit
!
```

```
 access-point 2
  access-point-name gprs.pdn2.com
  access-mode non-transparent
  aaa-group authentication foo
  exit
!
gprs default ip-address-pool radius-client
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.10.0.1 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

Related Commands

Command	Description
dhcp-server	Specifies a primary (and backup) DHCP server to allocate IP addresses to MS users entering a particular PDN access point.
gprs default dhcp-server	Specifies a default DHCP server from which the GGSN obtains IP address leases for mobile users.
gprs default ip-address-pool	Specifies a dynamic address allocation method using IP address pools for the GGSN.
aaa-group	Specifies an AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN.
gprs default aaa-group	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN

ip probe path

To enable route probe support on an APN, use the **ip probe path** command in access-point configuration mode. To return to the default, use the **no** form of this command.

ip probe path *ip_address* **protocol udp [port** *port* **ttl** *ttl***]**

no ip probe path *ip_address* **protocol udp [port** *port* **ttl** *ttl***]**

Syntax Description

ip_address	IP address to which the GGSN is to send a probe packet for each PDP context successfully created.
protocol udp	Specifies UDP.
port *port*	(Optional) UDP destination port.
ttl *ttl_value*	(Optional) IP time-to-live (TTL) value for outgoing packet.

Defaults

Disabled

Command Modes

Access-point configuration

Command History

Release	Modification
12.3(2)XB1	This command was introduced.
12.3(8)XU	This command was incorporated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **ip probe path** access-point configuration command to enable the GGSN to send a probe packet to a specific destination for each PDP context that is successfully established.

An example of how to use this feature is when a firewall load balancer (FWLB) is being used in the network. If the **ip probe path** command is configured, when a PDP context is established, the GGSN sends a probe packet the FWLB. This enables the FWLB to create an entry for the PDP context even if there is no upstream packet from the MS. Once an entry is created, the FWLB can forward any downstream packet from the network for the MS to the appropriate GGSN without depending on the MS to send the packet first.

Note If an APN is mapped to a VRF, the route probe packet will go through the VRF routing table.

ipv6 (access point)

To configure an access point to support IPv6 packet data protocol (PDP) contexts, exclusively or in addition to IPv4 PDP contexts, use the **ipv6** command in access point configuration mode. To disable the support of IPv6 PDPs on the access point, use the **no** form of this command.

ipv6 [**enable** | **exclusive**]

no ipv6 [**enable** | **exclusive**]

Syntax Description

enable	Configures an access point to support both IPv6 PDP and IPv4 PDP contexts.
exclusive	Configures an access point to allow only IPv6 PDP contexts.

Defaults

IPv6 is disabled (by default, only IPv4 PDPs are supported on an access point).

Command Modes

Access point configuration

Command History

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

Usage Guidelines

Use the **ipv6 enable** command to configure an access point to support both IPv6 and IPv4 PDP contexts, or, optionally, specify the **exclusive** keyword option to configure the access point to support only IPv6 PDP contexts. (If an access point is configured to support IPv6 PDPs exclusively, IPv4 PDPs are rejected by the access point).

Note IPv6 support on a gateway GPRS support node (GGSN) access point requires that a tunnel for IPv6 traffic has been configured on the supervisor engine. Tunneling encapsulates IPv6 packets in IPv4 packets for delivery across an IPv4 infrastructure. By using tunnels, you can communicate with isolated IPv6 networks without upgrading the IPv4 infrastructure between them. For information on tunneling IPv6 traffic, refer to the *Cisco IOS IPv6 Configuration Guide*.

Note On the GGSN, VPN routing and forwarding (VRF) is not supported for IPv6 PDPs. Therefore, if an access point on which VRF is enabled is configured to support IPv6 PDPs (via the **ipv6** command), the IPv4 PDPs are routed in the VRF, but the IPv6 PDPs are routed in the global routing table.

Examples

The following example enables the support of both IPv4 and IPv6 PDP on access point 1.

```
Router(config)# access-point 1
Router(access-point-config)# ipv6 enable
```

Related Commands

Command	Description
ipv6 base-template	Specifies the base virtual template interface (containing IPv6 routing advertisements (RA) parameters), that the access point copies when creating a virtual subinterface for an IPv6 PDP context.
ipv6 dns primary	Specifies the address of an IPv6 DNS (primary and secondary) to be sent in IPv6 to create PDP context responses on an access point.
ipv6 ipv6-access-group	Specifies IPv6 access permissions on an access point.
ipv6 ipv6-address-pool	Configures a dynamic IPv6 prefix allocation method on an access point.
ipv6 redirect	Redirects IPv6 traffic to an IPv6 external device.
ipv6 security verify	Enables the GGSN to verify the IPv6 source address of an upstream TPDU against the address previously assigned to an MS,

ipv6 base-vtemplate

To specify the base virtual template interface (containing IPv6 routing advertisements [RA] parameters), that an accesss point copies when creating a virtual subinterface for an IPv6 packet data protocol (PDP) context, use the **ipv6 base-vtemplate** command in access point configuration mode. To remove the configuration, use the **no** form of this command.

ipv6 base-vtemplate *number*

no ipv6 base-vtemplate *number*

Syntax Description

number	Virtual template index number.

Defaults

No default behavior or values.

Command Modes

Access point configuration

Command History

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

Usage Guidelines

A virtual-access subinterface is created for each IPv6 PDP session established on the gateway GPRS support node (GGSN). The configurations for the virtual-access, such as routing advertisement timers, are cloned from the base vtemplate interface associated with an access point.

Use the **ipv6 base-vtemplate** command to associate a base virtual-template interface to an access point.

When a Create PDP Context request is receive, a virtual access subinterface is cloned from the base virtual template associated with the access point; and after the IPv6 virtual access subinterface is created, an IPv6 address is allocated as defined by the configuration under the access point. The Create PDP Context response is sent back only after the virtual-access subinterface is created, and authentication and address allocation are successfully completed.

Examples

The following example specifies access point 1 to use virtual template interface 10 as the base virtual template:

```
Router(config)# access-point 1
Router(access-point-config)# ipv6 base-vtemplate 10
```

Related Commands

Command	Description
ipv6	Configures an access point to support IPv6 PDP contexts, exclusively or in addition to IPv4 PDP contexts.
ipv6 dns primary	Specifies the address of an IPv6 DNS (primary and secondary) to be sent in IPv6 Create PDP Context responses on an access point.
ipv6 ipv6-access-group	Specifies IPv6 access permissions on an access point.
ipv6 ipv6-address-pool	Configures a dynamic IPv6 prefix allocation method on an access point.
ipv6 redirect	Redirects IPv6 traffic to an IPv6 external device.
ipv6 security verify	Enables the GGSN to verify the IPv6 source address of an upstream TPDU against the address previously assigned to an MS,

ipv6 dns primary

To specify the address of a primary (and backup) Domain Name System (DNS) to be sent in IPv6 Create packet data protocol (PDP) Context response on an access point, use the **ipv6 dns primary** command in access point configuration mode. To remove the IPv6 DNS address configuration from the access point configuration, use the **no** form of this command.

ipv6 dns primary *ipv6-address* [**secondary** *ipv6-address*]

no ipv6 dns primary *ipv6-address* [**secondary** *ipv6-address*]

Syntax Description

ipv6-address	IPv6 address of the primary IPv6 DNS.
secondary *ipv6-address*	(Optional) Specifies the IPv6 address of the backup IPv6 DNS.

Defaults

No default behavior or values.

Command Modes

Access point configuration

Command History

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

Usage Guidelines

Use the **ipv6 dns primary** command to specify the address of the primary (and backup) IPv6 DNS at the access point level.

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

The DNS address can come from the RADIUS server or local access point name (APN) configuration. The criterion for selecting the DNS address depends on the IP address allocation scheme configured under the APN.

Depending on the configuration, the criterion for selecting the IPv6 DNS address is as follows:

7. RADIUS-based IP address allocation scheme—A DNS address returned from the RADIUS server (in Access-Accept responses) is used. If the RADIUS server does not return a DNS address, the local APN configuration is used.
8. Static IP addresses—A local APN configuration is used.

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

Examples

The following example specifies a primary IPv6 DNS and a secondary IPv6 DNS for access point 2:

```
access-point 2
 access-point-name xyz.com
 ipv6 enable
 ipv6 base-vtemplate
 ipv6 dns primary 3001::99 secondary 4001::99
 exit
```

Related Commands

Command	Description
ipv6	Configures an access point to support IPv6 PDP contexts, exclusively or in addition to IPv4 PDP contexts.
ipv6 base-template	Specifies the base virtual template interface (containing IPv6 routing advertisements [RA] parameters), that the access point copies when creating a virtual subinterfaces for an IPv6 PDP context.
ipv6 ipv6-access-group	Specifies IPv6 access permissions on an access point.
ipv6 ipv6-address-pool	Configures a dynamic IPv6 prefix allocation method on an access point.
ipv6 redirect	Redirects IPv6 traffic to an IPv6 external device.
ipv6 security verify	Enables the GGSN to verify the IPv6 source address of an upstream TPDU against the address previously assigned to an MS,

ipv6 ipv6-access-group

To specify IPv6 access permissions (uplink and downlink) at an access point, use the **ipv6 ipv6-access-group** command in access point configuration mode. To disable the access list, use the **no** form of this command.

ipv6 ipv6-access-group *access-list-name* [**up** | **down**]

no ipv6 ipv6-access-group *access-list-name* [**up** | **down**]

Syntax Description

access-list-name	Name of the access list configuration to apply to IPv6 payload packets.
up	Applies the filter to uplink packets.
down	Applies the filter to downlink packets.

Defaults

No access list is enforced.

Command Modes

Access point configuration

Command History

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

Usage Guidelines

Use the **ipv6 ipv6-access-group** command to specify an access list that indicates whether IPv6 users are given or denied permission using a specified access point.

Examples

The following example grants access-list IPv6acl inbound access to the mobile station from the PDN through the GGSN:

```
!
gprs access-point-list abc
 access-point 1
  access-point-name gprs.somewhere.com
  ipv6 ipv6-access-group IPv6acl up
  exit
!
```

Related Commands

Command	Description
ipv6	Configures an access point to support IPv6 PDP contexts, exclusively or in addition to IPv4 PDP contexts.
ipv6 access-list	Defines an IPv6 access list and places the router in IPv6 access list configuration mode.
ipv6 base-template	Specifies the base virtual template interface (containing IPv6 routing advertisements [RA] parameters), that the access point copies when creating a virtual subinterfaces for an IPv6 PDP context.
ipv6 dns primary	Specifies the address of an IPv6 DNS (primary and secondary) to be sent in an IPv6 Create PDP Context response on an access point.
ipv6 ipv6-address-pool	Configures a dynamic IPv6 prefix allocation method on an access point.
ipv6 redirect	Redirects IPv6 traffic to an IPv6 external device.
ipv6 security verify	Enables the GGSN to verify the IPv6 source address of an upstream TPDU against the address previously assigned to an MS,

ipv6 ipv6-address-pool

To configure a dynamic IPv6 prefix allocation method on an access point, use the **ipv6 ipv6-address-pool** command in access point configuration mode. To disable a dynamic prefix address allocation, use the **no** form of this command.

ipv6 ipv6-address-pool {**local** *pool-name* | **radius-client**}

no ipv6 ipv6-address-pool {**local** *pool-name* | **radius-client**}

Syntax Description

local *pool-name*	IPv6 prefixes are allocated from a locally configured IPv6 prefix pool.
radius-client	IPv6 prefixes are allocated from a RADIUS server.

Defaults

Disabled—a dynamic IPv6 prefix allocation method is not configured.

Command Modes

Access point configuration

Command History

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

Usage Guidelines

The IPv6 prefix can be obtained from a locally configured prefix pool, or a RADIUS server.

Use the **ipv6 ipv6-address-pool** command to configure the dynamic IPv6 prefix allocation method that you want an access point to use.

Note DHCPv6 is not support for IPv6 PDPs as an address allocation scheme.

Examples

The following example configures an access point to use a locally configured IPv6 prefix address pool named “localv6”:

```
Router(access-point-config)# ipv6 ipv6-address-pool local localv6
```

Related Commands

Command	Description
ipv6	Configures an access point to support IPv6 PDP contexts, exclusively or in addition to IPv4 PDP contexts.
ipv6 base-template	Specifies the base virtual template interface (containing IPv6 routing advertisements [RA] parameters), that the access point copies when creating a virtual subinterface for an IPv6 PDP context.
ipv6 dns primary	Specifies the address of an IPv6 DNS (primary and secondary) to be sent in an IPv6 Create PDP Context response on an access point.
ipv6 ipv6-access-group	Specifies IPv6 access permissions on an access point.
ipv6 local pool	Configures a local IPv6 prefix pool.
ipv6 redirect	Redirects IPv6 traffic to an IPv6 external device.
ipv6 security verify	Enables the GGSN to verify the IPv6 source address of an upstream TPDU against the address previously assigned to an MS,

ipv6 redirect

To redirect IPv6 traffic to an external IPv6 device, use the **ipv6 redirect** command in access point configuration mode. To disable the redirection of IPv6 traffic, use the **no** form of this command

ipv6 redirect [all | intermobile] *destination-ipv6-address*

no ipv6 redirect [all | intermobile] *destination-ipv6-address*

Syntax Description

all	Configures the gateway GPRS support node (GGSN) to redirect all IPv6 traffic to an external IPv6 device on an access point.
intermobile	Configures the GGSN to redirect mobile-to-mobile IPv6 traffic to an external IPv6 device.
destination-ipv6-address	IP address of the IPv6 external device to which you want to redirect IPv6 traffic.

Defaults

IPv6 traffic is not redirected.

Command Modes

Access point configuration

Command History

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

Usage Guidelines

Use the **ipv6 redirect** command to redirect IPv6 traffic on an access point to an external device (such as an external firewall) for verification.

Use the **ipv6 redirect** command with the **all** keyword specified, to redirect all IPv6 packets to a specified destination regardless of whether the destination address belongs to a mobile station (MS) on the same GGSN or not.

Use the **ipv6 redirect** command with the **intermobile** keyword specified, to redirect IPv6 mobile-to-mobile traffic to an external device (such as an external firewall) for verification. Only IPv6 packets for which the destination address belongs to an MS that is active on the same GGSN can be redirected. If the receiving MS does not have a packate data protocol (PDP) context in the same GGSN on which the sending MS PDP context is created, the packets are dropped.

Note On the Cisco 7600 series router platform, the traffic redirection feature requires that policy based routing (PBR) is configured on the Multilayer Switch Feature Card (MSFC) and incoming VLAN interface from the Cisco Service and Application Module for IP (SAMI), and that the next hop to route the packets is set using the set **ip next-hop** command.

Examples

The following example redirects all IPv6 traffic to an external device with the IPv6 address 3001::99.

```
ipv6 redirect all 3001::99
```

The following example redirects mobile-to-mobile IPv6 traffic to an external device with the IPv6 address 3001::99.

```
ipv6 redirect intermobile 3001::99
```

Related Commands

Command	Description
ipv6	Configures an access point to support IPv6 PDP contexts, exclusively or in addition to IPv4 PDP contexts.
ipv6 base-template	Specifies the base virtual template interface (containing IPv6 routing advertisements (RA) parameters), that the access point copies when creating a virtual sub-interfaces for an IPv6 PDP context.
ipv6 dns primary	Specifies the address of an IPv6 DNS (primary and secondary) to be sent in IPv6 create PDP context responses on an access point.
ipv6 ipv6-access-group	Specifies IPv6 access permissions on an access point.
ipv6 ipv6-address-pool	Configures a dynamic IPv6 prefix allocation method on an access point.
ipv6 security verify	Enables the GGSN to verify the IPv6 source address of an upstream TPDU against the address previously assigned to an MS,

ipv6 security verify source

To enable the gateway GPRS support node (GGSN) to verify the source address of an upstream transport protocol data unit (TPDU) against the address previously assigned to an IPv6 mobile station (MS), use the **ipv6 security verify source** command in access point configuration mode. To disable IPv6 source verification, use the **no** form of this command.

ipv6 security verify source

ipv6 no security verify source

Syntax Description

This command has no arguments or keywords.

Defaults

The GGSN does not verify source addresses.

Command Modes

Access point configuration

Command History

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

Usage Guidelines

Use the **ipv6 security verify source** command to configure the GGSN to verify the source address of an upstream TPDU against the address previously assigned to the IPv6 MS.

When the **ipv6 security verify source** command is configured on an access point, the GGSN verifies the source address of a TPDU before GPRS tunneling protocol (GTP) will accept and forward it. If the GGSN determines that the address differs from the address previously assigned to the MS, it drops the TPDU and counts it as an illegal packet in its PDP context and access point.

Configuring the **ipv6 security verify source** command in access point configuration mode protects the GGSN from faked user identities.

Note While the GGSN supports security source address verification only, the destination field is viewable with security.

Examples

The following example enables the verification of source IPv6 addresses received in upstream TPDUs:

```
ipv6 security verify source
```

Related Commands

Command	Description
ipv6	Configures an access point to support IPv6 PDP contexts, exclusively or in addition to IPv4 PDP contexts.
ipv6 base-template	Specifies the base virtual template interface (containing IPv6 routing advertisements [RA] parameters), that the access point copies when creating a virtual subinterface for an IPv6 PDP context.
ipv6 dns primary	Specifies the address of an IPv6 DNS (primary and secondary) to be sent in IPv6 create PDP context responses on an access point.
ipv6 ipv6-access-group	Specifies IPv6 access permissions on an access point.
ipv6 ipv6-address-pool	Configures a dynamic IPv6 prefix allocation method on an access point.
ipv6 redirect	Redirects IPv6 traffic to an IPv6 external device.

limit duration

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

limit duration *number* **[reset]**

no limit duration *number* **[reset]**

Syntax Description

duration-value	A value, in minutes, between 5 and 4294967295 that specifies the time duration limit. The default is 1,048,576 bytes (1 MB).
reset	(Optional) Keyword to specify that the time trigger be reset if the CDR is closed by any other trigger. If the **reset** keyword is not specified, the time trigger will not be reset when the volume trigger expires (**limit volume** command), but it will be reset when any other trigger expires.

Defaults

Disabled

Command Modes

Charging profile configuration

Command History

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

Usage Guidelines

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

For the box-level charging profile (profile 0 configured using the charging related global configuration commands), all triggers are reset by the expiration of another trigger. However, for charging profiles 1 through 15, the **reset** keyword option must be set for the **limit duration** and **limit volume** charging profile configuration commands for the expiration of any trigger to reset all other triggers.

If the **reset** keyword option is not specified when configuring the time trigger, the time trigger will not be reset when the volume trigger expires (**limit volume** command), but it will be reset when any other trigger expires.

Related Commands.

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

limit sgsn-change

To specify as a trigger condition in a charging profile, the maximum number of SGSN changes that can occur before closing and updating the G-CDR for a particular PDP context, use the **limit sgsn-change** command in charging profile configuration mode. To return to the default value, use the **no** form of this command.

limit sgsn-change *number*

no limit sgsn-change *number*

Syntax Description

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

Defaults

Disabled

Command Modes

Charging profile configuration

Command History

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

Usage Guidelines

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

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

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

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

Related Commands.

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

limit volume

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

limit volume *threshold-value* **[reset]**

no limit volume *threshold-value* **[reset]**

Syntax Description

threshold-value	A value between 1 and 4294967295 that specifies the container threshold value, in bytes. The default is 1,048,576 bytes (1 MB).
reset	(Optional) Keyword to specify that the volume trigger be reset if the CDR is closed by any other trigger. If the **reset** keyword is not specified, the volume trigger will not be reset when the time trigger expires (**limit duration** command), but it will be reset when any other trigger expires.

Defaults

1,048,576 bytes (1 MB)

Command Modes

Charging profile configuration

Command History

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

Usage Guidelines

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

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

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

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

For the box-level charging profile (profile 0 configured using the charging related global configuration commands), all triggers are reset by the expiration of another trigger. However, for charging profiles 1 through 15, the **reset** keyword option must be set for the **limit duration** and **limit volume** charging profile configuration commands for the expiration of any trigger to reset all other triggers. If the **reset** keyword is not specified when configuring the volume trigger, the volume trigger will not be reset when the time trigger expires (**limit duration** command), but it will be reset when any other trigger expires.

Related Commands.

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

match flow pdp

To specify PDP flows as the match criterion in a class map, use the **match flow pdp** command in class map configuration mode. To remove PDP flow as a match criterion, use the **no** form of this command.

match flow pdp

no match flow pdp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Class map configuration

Command History

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

Usage Guidelines

The **match flow pdp** class map configuration command enables the ability to configure session-based policing (per-PDP policing) for downlink traffic on a GGSN.

Note When defining a class map for PDP flow classification, do not specify the **match-any** keyword option.

Note The Per-PDP policing feature requires that UMTS QoS has been configured.

Note If you are using trust DSCP policy map configuration, ensure that you configure only one class map with **match flow pdp** in the policy map. Simultaneous multiple flows for policing, with different DSCPs for a PDP, are not supported.

To configure the Per-PDP policing feature on a GGSN, you must complete the following tasks:

1. Create a class for PDP flows using the **class-map** command.

```
GGSN(config)# class-map class-pdp
GGSN(config-cmap)# Match flow pdp
GGSN(config-cmap)# exit
```

2. Create a policy map using the **policy-map** command and assign a class to the map using the **class** command.

```
GGSN(config)# policy-map policy-gprs
GGSN(config-pmap)# class class-pdp
```

3. In the policy map, configure the Traffic Policing feature using the **police** policy map class configuration command.

```
GGSN(config-pmap-c)# police rate pdp [burst bytes] [peak-rate pdp [peak-burst bytes]]
conform-action action exceed-action action [violate-action action]
GGSN(config-pmap-c)# exit
GGSN(config-pmap)# exit
```

4. Attach a service policy to an APN using the **service-policy** access-point configuration command.

```
GGSN(config)# access-point 1
GGSN(access-point-config) service-policy in policy-gprs
```

Examples

The following example specifies PDP flows as the match criterion in a class map named “class-pdp”:

```
class-map class-pdp
  match flow pdp
```

Related Commands

Command	Description
police rate	Configures traffic policing using the police rate.
service-policy	Attaches a service policy to an APN, to be used as the service policy for PDP flows of that APN.

maximum delay-class

To define in a Call Admission Control (CAC) maximum QoS policy, the maximum delay class for R97/R98 QoS that can be accepted at an APN, use the **maximum delay-class** command in CAC maximum QoS policy configuration mode. To return to the default value, use the **no** form of this command.

maximum delay-class *value* [**reject**]

no maximum delay-class *value* **[reject]**

Syntax Description

value	Specifies the maximum delay class that can be accepted at an APN. Valid values are 1 to 4.
reject	(Optional) Specifies that if the maximum delay class is higher than the configured value, the Create PDP Context is rejected. If this keyword is not specified, the delay class is downgraded to the value of the configured delay class. This keyword option is ignored for update PDP context requests.

Defaults

PDP contexts for which the maximum delay-class is higher than the configured value are downgraded to the configured value.

Command Modes

CAC maximum QoS policy configuration

Command History

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

Usage Guidelines

Use the **maximum delay-class** CAC maximum QoS policy configuration command to specify the maximum delay class that can be accepted at an APN.

By default, PDP contexts for which the maximum delay-class is higher than the configured value are downgraded to the configured value.

If the **reject** keyword has been specified, if the maximum delay class requested is higher than the configured delay class, the Create PDP Context is rejected.

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

Examples

The following example defines 3 as the maximum delay class for GPRS QoS that can be accepted at an APN:

```
maximum delay-class 3
```

Related Commands

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

maximum pdp-context

To specify in a Call Admission Control maximum QoS policy, the maximum number of PDP contexts that can be created for a particular APN, use the **maximum pdp-context** command in CAC maximum QoS policy configuration mode. To return to the default value, use the **no** form of this command.

maximum pdp-context *number1* [**threshold** *number2*]

no maximum pdp-context *number1* [**threshold** *number2*]

Syntax Description

number1	Specifies the maximum number of PDP contexts that can be created in an APN.
threshold *number2*	(Optional) Specifies the threshold, that after reached, only PDP contexts with allocation/retention priority 1 are accepted.

Defaults

No default behavior or values.

Command Modes

CAC maximum QoS policy configuration

Command History

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

Usage Guidelines

Use the **maximum pdp-context** CAC maximum QoS policy configuration command to configure the maximum number of PDP contexts that can be created for a particular APN.

The maximum number of PDP contexts defined for an APN using the **maximum pdp-context** command cannot exceed the maximum number of PDP contexts defined by the **gprs maximum-pdp-context-allowed** global configuration command.

When the optional **threshold** keyword is specified, when the total number of PDP contexts exceeds the configured number, only PDP contexts with Allocation/Retention Priority 1 are accepted. Create PDP contexts with other priorities (2/3) are rejected. If the optional **threshold** keyword is not specified, when the total number of PDP contexts reaches the configured maximum number, all subsequent Create PDP Contexts are rejected.

The **maximum pdp-context** command configuration is checked before all other QoS parameters defined in a policy: maximum bit rate, guaranteed bit rate, highest traffic class, highest traffic handling priority, highest delay class, and highest peak throughput class.

Examples

In the following example, 15000 is specified as the maximum number of PDP contexts that can be created for a particular APN:

```
maximum pdp-context 15000
```

Related Commands

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

maximum peak-throughput

To define in a Call Admission Control (CAC) maximum QoS policy, the maximum peak throughput for R97/R98 QoS that can be accepted at an APN, use the **maximum peak-throughput** command in CAC maximum QoS policy configuration mode. To return to the default value, use the **no** form of this command.

maximum peak-throughput *value* [**reject**]

no maximum peak-throughput *value* [**reject**]

Syntax Description

value	Specifies the maximum peak throughput that can be accepted at an APN. Valid values are between 1 and 9.
reject	(Optional) Specifies that if the maximum peak throughput is higher than the configured value, the Create PDP Context is rejected. If this keyword is not specified, the peak throughput is downgraded to the value of the configured peak throughput value. This option is ignored for update PDP context requests.

Defaults

PDP contexts for which the peak throughput is higher than the configured value are downgraded to the configured value.

Command Modes

CAC maximum QoS policy configuration

Command History

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

Usage Guidelines

Use the **maximum peak-throughput** CAC maximum QoS policy configuration command to specify the maximum peak throughput that can be accepted at an APN.

By default, PDP contexts for which the peak throughput is higher than the configured value are downgraded to the configured value.

If the **reject** keyword has been specified, if the maximum peak throughput requested is higher than the configured peak throughput, the Create PDP Context is rejected.

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

Examples

The following example defines 7 as the maximum peak-throughput GPRS QoS that can be accepted at an APN:

```
maximum peak-throughput 7
```

Related Commands

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

maximum traffic-class

To define in a Call Admission Control (CAC) maximum QoS policy, the highest traffic class that can be accepted at an APN, use the **maximum traffic-class** command in CAC maximum QoS policy configuration mode. To return to the default value, use the **no** form of this command.

maximum traffic-class *traffic-class-name* [**priority** *value*]

no maximum traffic-class *traffic-class-name* [**priority** *value*]

Syntax Description

traffic-class-name	Specifies the highest traffic class that can be accepted at an APN. Valid values are conversational, streaming, interactive, or background.
priority	(Optional) Specifies the highest traffic handling priority for the interactive traffic class.

Defaults

All traffic classes are accepted.

Command Modes

CAC maximum QoS policy configuration

Command History

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

Usage Guidelines

Use the **maximum traffic-class** CAC maximum QoS policy configuration command to define the highest traffic class that can be accepted at an APN. If the traffic class requested in a Create PDP Context request is higher than the configured class, the request is rejected.

The GGSN does not downgrade the traffic class of a PDP context unless the highest traffic class configured is changed after a PDP context is created and the GGSN receives an update PDP context request with a traffic class higher than the newly configured value. If this condition occurs, the GGSN downgrades the traffic class to the value of the newly configured maximum traffic class.

By default, all traffic classes are accepted.

Use the optional **priority** keyword to define the highest traffic handling priority for the interactive traffic class. If the requested traffic handling priority exceeds the highest one, it will be downgraded to the configured one. If the interactive traffic class is configured without the **priority** keyword option, then PDPs with any traffic handling priority are allowed. If the traffic class is not interactive, the **priority** keyword is ignored.

Examples

The following example configures streaming as the highest traffic class accepted at an APN:

```
maximum traffic-class streaming
```

The following example configures interactive as the highest traffic class accepted at an APN:

```
maximum traffic-class interactive
```

The following example configures interactive as the highest traffic class with traffic handling priority 2 accepted at an APN:

```
maximum traffic-class interactive priority 2
```

Related Commands

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

mbr traffic-class

To define in a Call Admission Control (CAC) maximum QoS policy, the maximum bit rate (MBR) that can be allowed for each traffic class, use the **mbr traffic-class** command in CAC maximum QoS policy configuration mode. To return to the default value, use the **no** form of this command.

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

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

Syntax Description

traffic-class-name	Specifies the UMTS traffic class to which the MBR applies. Valid values are Conversational, Streaming, Interactive, or Background.
bitrate	Maximum bit rate in kilobits per second. Valid value is between 1 and 16000. **Note** Although the valid command range for both the uplink and downlink direction is 1 to 16000, the maximum rate that can be acheived in the uplink direction is 8640. Additionally, a value greater than 8640 in the downlink direction is supported for GTPv1 PDPs only.
uplink	Specifies MBR applies to a traffic-class for uplink traffic.
downlink	Specifies MBR applies to a traffic-class for downlink traffic.
reject	(Optional) Specifies that when the MBR exceeds the configured value, the Create PDP Contexts is rejected. This option is ignored for update PDP context requests.

Defaults

Any MBR is accepted.

Command Modes

CAC maximum QoS policy configuration

Command History

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

Usage Guidelines

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

When the **reject** optional keyword is specified, if the requested MBR exceeds the configured value, Create PDP Contexts are rejected. If the **reject** keyword is not specified, the MBR is downgraded to the configured value.

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

Examples

The following example defines 1000 kbps as the uplink MBR supported and 2000 kbps as the maximum downlink MBR:

```
mbr traffic-class interactive 1000 uplink
mbr traffic-class interactive 1000 downlink
```

Related Commands

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

msisdn suppression

To specify that the gateway GPRS support node (GGSN) overrides the mobile station integrated services digital network (MSISDN) number with a pre-configured value in its authentication requests to a RADIUS server, use the **msisdn suppression** command in access-point configuration mode. To enable the GGSN to send the MSISDN number in authentication requests to a RADIUS server, use the **no** form of the command.

msisdn suppression [*value*]

no msisdn suppression [*value*]

Syntax Description

value	(Optional) String (up to 20 characters long) that the GGSN sends in place of the MSISDN number in authentication requests to a RADIUS server. Valid characters for the string are any of those accepted by the MSISDN encoding specifications, including the integers 0–9, and characters a, b, c, * and #. The default value is that no string is sent.

Defaults

The MSISDN number is suppressed, and no ID string is sent to the RADIUS server in place of the MSISDN number.

Command Modes

Access point configuration

Command History

Release	Modification
12.2(2)	This command was introduced.
12.2(4)MX2	This command was integrated into Cisco IOS Release 12.2(4)MX2.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Certain countries have privacy laws which prohibit service providers from identifying the MSISDN number of mobile stations in authentication requests. Use the **msisdn suppression** command to specify a value that the GGSN sends in place of the MSISDN number in its authentication requests to a RADIUS server. If no value is configured, then no number is sent to the RADIUS server.

To use the **msisdn suppression** command, you must configure a RADIUS server either globally or at the access point and specify non-transparent access mode.

Examples

The following example will override the MSISDN ID sent in the create request and will not send any ID to the RADIUS server:

```
gprs access-point-list abc
   access-point 1
     radius-server 192.168.1.1
     access-mode non-transparent
     msisdn suppression
```

Related Commands

Command	Description
access-mode	Specifies whether the GGSN requests user authentication at the access point to a PDN.
aaa-group	Specifies an AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN.
gprs default aaa-group	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN.

n3-requests

To specify the maximum number of times that the quota server attempts to send a signaling request to the CSG, use the **n3-requests** command in quota server configuration mode. To return to the default value, use the **no** form of this command.

n3-requests *number*

no n3-requests

Syntax Description

number	Number between 1 and 65535 that specifies the number of times a request is attempted.

Defaults

5 requests.

Command Modes

Quota server configuration

Command History

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

Usage Guidelines

Use the **n3-requests** command to configure the maximum number of times the quota server will attempt to send a signaling request to the CSG.

Examples

The following example configures the quota server to attempt to send a signaling request no more than 3 times:

```
ggsn quota-server qs1
 interface loopback1
 echo-interval 90
 n3-requests 3
```

Related Commands .

Command	Description
csg-group	Associates the quota server to a CSG group that is to be used for quota server-to-CSG communication.
echo-interval	Specifies the number of seconds that the quota server waits before sending an echo-request message to the CSG.
ggsn quota-server	Configures the quota server process that interfaces with the CSG for enhanced service-aware billing.

Command	Description
interface	Specifies the logical interface, by name, that the quota server will use to communicate with the CSG.
t3-response	Specifies the initial time that the quota server waits before resending a signaling request message when a response to a request has not been received.
show ggsn quota-server	Displays quota server parameters or statistics about the quota server message and error counts.

name

To specify the name of a iSCSI target in the target profile on the GGSN, use the **name** command in iSCSI interface configuration mode. To remove the IP address configuration, use the **no** form of the command.

name *target_name*

no name *target_name*

Syntax Description

target_name	Name of the SCSI target.

Command Default

No default behavior or values.

Command Modes

iSCSI interface configuration

Command History

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

Usage Guidelines

Use the **name** command to specify the name of the SCSI target in an iSCSI target interface profile on the GGSN.

Examples

The following example configures an iSCSI target interface profile with the name targetA to a SCSI target named “eftcompany.com.”

```
ip iscsi target-profile targetA
  name iqn.2002-10.edu.abc.iol.iscsi.draft20-target:1
  ip 10.0.0.1
  port 3260
```

Related Commands

Command	Description
gprs iscsi	Configures the GGSN to use the specified iSCSI profile for record storage.
ip	Specifies the IP address of the target on the SAN.
ip iscsi target-profile	Creates an iSCSI interface profile for an SCSI target (or modifies an existing one), and enters iSCSI interface configuration mode.
port	Specifies the number of the TCP port on which to listen for iSCSI traffic.

nbns primary

To specify a primary (and backup) NBNS to be sent in create PDP responses at the access point, use the **nbns primary** command in access-point configuration mode. To remove the NBNS from the access-point configuration, use the **no** form of this command

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Access-point configuration

Command History

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

Usage Guidelines

Use the **nbns primary** command to specify the primary (and backup) NBNS at the access point level.

This feature is benefits address allocation schemes where there is no mechanism to obtain these address. Also, for a RADIUS-based allocation scheme, it prevents the operator from having to configure a NBNS and DNS under each user profile.

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

1. DHCP-based IP address allocation scheme (local and external)—NBNS address returned from the DHCP server is sent to the MS. If the DHCP server does not return an NBNS address, the local APN configuration is used.
2. RADIUS-based IP address allocation scheme—NBNS address returned from the RADIUS server (in Access-Accept responses) is used. If the RADIUS server does not return an NBNS address, the local APN configuration is used.

3. Local IP Address Pool-based IP address allocation scheme—Local APN configuration is used.
4. Static IP Addresses—Local APN configuration is used.

Note The GGSN sends DNS addresses in the create PDP response only if the MS is requesting the DNS address in the PCO IE.

Examples

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

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

Related Commands

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

network-behind-mobile

To enable an access point to support routing behind the mobile station (MS), use the **network-behind-mobile** command in access-point configuration mode. To disable support for routing behind the MS, use the **no** form of this command.

network-behind-mobile

no network-behind-mobile

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Access-point configuration

Command History

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

Usage Guidelines

Use the network-behind-mobile access-point configuration command to enable an access point to support routing behind the MS. The routing behind the MS feature enables the routing of packets to IP addresses that do not belong to the PDP context (the MS), but exist behind it. The network address of the destination can be different than the MS address.

Before enabling routing behind the MS, the following requirements must be met:

- The MS must use RADIUS for authentication and authorization.
- At minimum, one Framed-Route, attribute 22 as defined in Internet Engineering Task Force (IETF) standard RFC 2865, must be configured in the RADIUS server for each MS that wants to use this feature.

  When configured, the Framed-Route attribute is automatically downloaded to the GGSN during the authentication and authorization phase of the PDP context creation. If routing behind the MS is not enabled, the GGSN ignores the Framed-Route attribute. If multiple Framed-Route attributes have been configured for an MS, the GGSN uses the first attribute configured. When the MS session is no longer active, the route is deleted.

- For PDP Regen or PPP with L2TP sessions, the Framed-Route attribute must be configure in the RADIUS server of the LNS.
- For PPP Regen sessions, if the **security verify source** command is configure, the Framed-Route attribute must also be configured in the user profile in the GGSN RADIUS server.Packets routed behind the MS share the same 3GPP QoS settings of the MS.
- Static routes are not configured. Configuring static routes and the routing behind the mobile station feature (Framed Route, attribute 22) at the same time is not supported.

Examples

The following example shows how to enable support for routing behind the MS at access point 200:

```
gprs access-point-list abc
 access-point 200
  network-behind-mobile
```

Related Commands

Command	Description
security verify	Specifies the verification of source and/or destination addresses.
show gprs gtp pdp-context	Displays a list of the currently active PDP contexts (mobile sessions).
show gprs gtp statistics	Displays the current GTP statistics for the GGSN.
show ip route	Displays the current state of the routing table.
show pdp	Displays a list of the currently active PDP contexts (mobile sessions).

pcscf

To assign a P-CSCF server group to be used for an access point name (APN) for P-CSCF Discovery, use the **pcscf** command in access-point configuration mode. To remove the P-CSCF server group association, issue the **no** form of this command.

pcscf *group-name*

no pcscf *group-name*

Syntax Description

group-name	Specifies the name of a P-CSCF server group to be used for P-CSCF Discovery for an APN.

Defaults

No default behavior or values.

Command Modes

Access-point configuration

Command History

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

Usage Guidelines

Use the **pcscf** command to define a P-CSCF server group to be used by an APN for the P-CSCF Discovery support.

Note The order of the addresses returned in the “P-CSCF Address Field” of the PCO is the same as the order in which they are defined in the P-CSCF server group and the groups are associated with the APN.

Examples

The following example configures a P-CSCF group identified as “groupA” for an APN:

```
pcscf groupA
```

Related Commands

Command	Description
gprs pcscf	Configures a P-CSCF server group on the GGSN and enters P-CSCF group configuration mode.
server	Specifies the IP address of a P-CSCF server you want to include in the P-CSCF server group.
show gprs access-point	Displays information about access points on the GGSN.
show gprs pcscf	Displays a summary of the P-CSCF groups configured on the GGSN.

police rate

To configure PDP traffic policing using the police rate, use the **police rate** command in policy-map class configuration mode or policy-map class police configuration mode. To remove PDP traffic policing from the configuration, use the **no** form of this command.

police rate pdp [burst *bytes*] **[peak-rate pdp** [**peak-burst** *bytes*]] **conform-action** *action* **exceed-action** *action* **[violate-action** *action*]

no police rate pdp [burst *bytes*] **[peak-rate pdp** [**peak-burst** *bytes*]] **conform -action** *action* **exceed-action** *action* **[violate-action** *action*]

Syntax Description

burst *bytes*	(Optional) Committed burst size, in bytes. The size varies according to the interface and platform in use. Valid rage is 1000 to 512000000. The default is 1500.
peak-rate pdp	(Optional) Specifies that the peak rate of sessions be considered when policing PDP traffic.
peak-burst *bytes*	(Optional) Peak burst size, in bytes. The size varies according to the interface and platform in use. Valid range is 1000 to 512000000. The default is 2500.
conform-action	Action to take on packets when rate is less than conform burst.
exceed-action	Action to take on packets when rate exceeds conform burst.
violate action	Action to take on packets when rate violates conform burst.
action	(Optional) Action to take on packets. Specify one of the following keywords: • **drop**—Drops the packet. • **set-dscp-transmit new-dscp**—Sets the IP differentiated services code point (DSCP) value and sends the packet with the new IP DSCP value setting. • **set-prec-transmit new-prec**—Sets the IP precedence and sends the packet with the new IP precedence value setting. • **transmit**—Sends the packet with no alteration.

Defaults

Disabled.

Command Modes

Policy map class configuration

Command History

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

Usage Guidelines

Per-PDP policing (session-based policing) is a GGSN Traffic Conditioner (3G TS 23.107) function that can be used to limit the maximum rate of traffic received on the Gi interface for a particular PDP context.

The policing function enforces the CAC-negotiated data rates for a PDP context. The GGSN can be configured to either drop non-conforming traffic or mark non-conforming traffic for preferential dropping if congestion should occur.

The policing parameters used depends on the PDP context. Specifically,

- For GTPv1 PDPs with R99 QoS profiles, the MBR and GBR parameters from the CAC-negotiated QoS profile are used. For non real time traffic, only the MBR parameter is used.
- For GTPv1 PDPs with R98 QoS profiles and GTPv0 PDPs, the peak throughput parameter from the CAC-negotiated QoS policy is used.

Before configuring per-PDP policing, note the following:

- UMTS QoS mapping must be enabled on the GGSN.
- Cisco Express Forwarding (CEF) must be enabled on Gi interface.
- Per-PDP policing is supported for downlink traffic at the Gi interface only.
- The initial packets of a PDP context are not policed.
- Hiearchical policing is not supported.
- If flow-based policing is configured in a policy map that is attached to an APN, the **show policy-map apn** command displays the total number of packets received before policing and does not display the policing counters.
- A service policy that has been applied to an APN cannot be modified. To modify a service policy, remove the service policy from the APN, modify it, and then re-apply it.
- Multiple class maps, each with **match flow pdp** configured and a different differentiated services code point (DSCP), are supported in a policy map only if the DSCP is trusted (the **gprs umts-qos dscp unmodified** global configuration command has not been configured on the GGSN).

To clear policing counters displayed by the **show policy-map apn** command, issue the **clear gprs access-point statistics** *access-point-index* access-point configuration command.

Examples

The following is an example:

```
class-map match-all class-pdp
 match flow pdp
!
! Configures a policy-map and attaches this class map into it.

policy-map policy-gprs
 class class-pdp
  police rate pdp
    conform-action set-dscp-transmit 15
    exceed-action set-dscp-transmit 15
    violate-action drop

! Attaches the policy-map to the apn.

gprs access-point-list gprs
  access-point 1
   access-point-name static
   service-policy input policy-gprs
   !
```

Related Commands

Command	Description
match flow pdp	Specifies PDP flows as the match criterion in a class map.
service-policy	Attaches a service policy to an APN, to be used as the service policy for PDP flows of that APN.

port

To configure the port number on which the CSG listens for quota server traffic, use the **port** command in CSG group configuration mode. To deconfigure the port, use the **no** form of this command

port *port-number*

no port

Syntax Description

port-number	Number of the port on which the CSG listens for quota server traffic.

Defaults

3386

Command Modes

CSG group configuration

Command History

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

Usage Guidelines

Use the **port** command to configure the port number on which the CSG listens for quota server traffic.

The CSG always sends traffic to the quota server on port 3386. By default, it also listens for traffic from the quota server on port 3386, however, it can be configured to listen to a different port using the **port** CSG group configuration command.

Examples

The following configuration example configures the CSG to listen for traffic from a quota server on port 4444:

```
ggsn csg-group csg1
  virtual-address 5.5.5.14
  port 4444
```

Related Commands

Command	Description
ggsn csg-group	Configures a CSG group on the GGSN for quota server-to-CSG communication.
real-address	Configures the IP address of a real CSG for source checking on inbound messages from a CSG.

Command	Description
show ggsn csg	Displays the parameters used by the CSG group or the number of path and quota management messages sent and received by the quota server.
virtual-address	Configures a virtual IP address to which the quota server will send all requests.

port (iSCSI interface)

To specify the number of the port on which to listen for iSCSI traffic in the iSCSI target interface profile on the GGSN, use the **port** command in iSCSI interface configuration mode. To remove the port number, use the **no** form of the command.

port *port_number*

no port *port_number*

Syntax Description

port_number	Number of the port on which to use for iSCSI traffic.

Command Default

No default behavior or values.

Command Modes

iSCSI interface configuration

Command History

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

Usage Guidelines

Use the **port** command to configure the port on which to listen for iSCSI traffic in the iSCSI target interface profile on the GGSN. Port 3260 is recommended.

Examples

The following example configures an iSCSI taret interface profile with the name targetA to a iSCSI target with which the GGSN will communicate using port number 3260.

```
ip iscsi target-profile targetA
  name iqn.2002-10.edu.abc.iol.iscsi.draft20-target:1
  ip 10.0.0.1
  port 3260
```

Related Commands

Command	Description
gprs iscsi	Configures the GGSN to use the specified iSCSI profile for record storage.
ip	Specifies the IP address of the target on the SAN.
ip iscsi target-profile	Creates an iSCSI interface profile for an SCSI target (or modifies an existing one), and enters iSCSI interface configuration mode.
name	Defines the name of the target.

ppp-regeneration

To enable an access point to support PPP regeneration, use the **ppp-regeneration** command in access point configuration mode. To disable support for PPP regeneration at an access point, use the **no** form of this command.

ppp-regeneration [**max-session** *number*] [**setup-time** *seconds*] [**verify-domain** | **fixed-domain**] [**allow-duplicate**]

no ppp-regeneration [**max-session** *number*] [**setup-time** *seconds*] [**verify-domain** | **fixed-domain**] [**allow-duplicate**]

Syntax Description

max-session *number*	Maximum number of PPP regenerated sessions allowed at the access point. The default value 65535.
setup-time *seconds*	Maximum amount of time, in seconds, within which a PPP regenerated session must be established. Valid value is between 1 and 65535. The default value is 60 seconds.
verify-domain	Configures the gateway GPRS support node (GGSN) to verify that the domain name from the acces point name (APN) information element (IE) and the Protocol Configuration Option (PCO) IE are the same before creating an L2TP tunnel to the user.
fixed-domain	
allow-duplicate	Configures the GGSN to not check for duplicate IP addresses for PPP regenerated packet data protocol (PDP) contexts.

Defaults

The default **max-session** value is 65535 seconds.

The default **setup-time** is 60 seconds.

The default for the **verify-domain** option is to create an L2TP tunnel to the user to the domain specified in the PCO IE without verifying against the APN.

The default for the **allow-duplicate** option is to disallow duplicate IP addresses.

Command Modes

Access point configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was integrated into Cisco IOS Release 12.2(8)YD and the default value changed from being device dependent to 65535.
12.2(8)YW	This command was integrated into Cisco IOS Release 12.2(8)YW.
12.3(2)XB	This command was integrated into Cisco IOS Release 12.3(2)XB.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.

Release	Modification
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ and the **fixed-domain** keyword option was added.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.
12.4(9)XG	This command was integrated into Cisco IOS Release 12.4(9)XG and the **allow-duplicate** keyword option was added.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.

Usage Guidelines

Use the **ppp-regeneration** command to enable an access point to support PPP regeneration and to specify parameters for PPP regeneration sessions on the GGSN.

Note The **ppp-regeneration** command configuration applies to IPv4 PDPs only.

Note PPP regeneration support at an access point requires Cisco Express Forwarding (CEF) to be enabled by using the **ip cef** command.

The maximum **setup-time** value should allow for the total amount of time required to create the PPP virtual access (VA) and to establish a PPP session. If the setup time is reached before the PPP IP Control Protocol (IPCP) is up, the GGSN tears down the L2TP session, PPP VA, and PDP context.

The type of PPP method configured to forward packets beyond the terminal equipment and mobile termination affects the maximum number of PDP contexts supported on the GGSN. For more information, see the "Configuring PPP Support on the GGSN" chapter of the *Cisco IOS Mobile Wireless Configuration Guide*.

When PPP regeneration is being used, use the **ppp-regeneration verify-domain** command in access point configuration mode to configure the GGSN to verify the domain sent in the PCO IE in a Create PDP Context request against the domain in the APN IE sent out by the user before selecting an L2TP tunnel to the user. If there is a mismatch between the user-supplied domain name and the APN, the Create PDP Context request is rejected with the cause value "Service not supported."

Examples

The following example shows a partial GGSN configuration for PPP regeneration, in which PPP regeneration is enabled at access point 1. The example specifies a maximum of 100 PPP regeneration sessions, with a limit of 30 seconds for creating PPP VA and establishing a PPP session:

```
gprs access-point-list abc
 access-point 1
  access-point-name gprs.corporate.com
  ppp-regeneration max-session 100 setup-time 30
  ppp-regeneration verify domain
  exit
```

Related Commands

Command	Description
gprs gtp ppp-regeneration vtemplate	Associates the virtual template interface that is configured for PPP encapsulation with support for regenerated PPP sessions on the GGSN.
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.

radius attribute acct-session-id charging-id

To specify that the gateway GPRS support node (GGSN) include only the charging ID in the Acct-Session-ID (attribute 44) in accounting requests at an APN, use the **radius attribute acct-session-id charging-id** command in access-point configuration mode. To disable this configuration, use the **no** form of this command.

radius attribute acct-session-id charging-id

no radius attribute acct-session-id charging-id

Syntax Description

This command has no arguments or keywords.

Defaults

The default is to send the GGSN address and charging ID in the Acct-Session-ID in accounting requests to a RADIUS server.

Command Modes

Access point configuration

Command History

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

Usage Guidelines

Use the **radius attribute acct-session-id charging-id** command to send only the charging ID in Acct-Session-ID (attribute 44) in its authentication and accounting requests to a RADIUS server.

Examples

The following example specifies that only the charging ID be sent in the Acct-Session-ID in accounting requests to the RADIUS server:

```
gprs access-point-list abc
   access-point 1
     radius attribute acct-session-id charging-id
```

Related Commands

Command	Description
access-mode	Specifies whether the GGSN requests user authentication at the access point to a PDN.
aaa-group	Specifies an AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN.

Command	Description
gprs default aaa-group	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN.
show gprs access-point	Displays information about access points on the GGSN.

radius attribute nas-id

To specify that the gateway GPRS support node (GGSN) include the NAS-Identifier (attribute 32) in access requests at an APN, use the **radius attribute nas-id** command in access-point configuration mode. To disable this configuration, use the **no** form of this command.

radius attribute nas-id *word*

no radius attribute nas-id

Syntax Description

word	Text string sent in attribute 32 that identifies the NAS originating in the access-request packets.

Defaults

The default is to not send the NAS-Identifier in access requests.

Command Modes

Access point configuration

Command History

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

Usage Guidelines

Use the **radius attribute nas-id** command to include the NAS-Identifier in access requests at an APN.

This command overrides the configuration of the **radius-server attribute 32 include-in-access-req format** global configuration command.

Examples

The following example configures the GGSN to send the NAS-Identifier in access requests at the APN:

```
gprs access-point-list abc
   access-point 1
     radius attribute nas-id GGSNGATEWAY1
```

Related Commands

Command	Description
access-mode	Specifies whether the GGSN requests user authentication at the access point to a PDN.
aaa-group	Specifies an AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN.

Command	Description
gprs default aaa-group	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN.
show gprs access-point	Displays information about access points on the GGSN.

radius attribute suppress imsi

To specify that the gateway GPRS support node (GGSN) suppress the Third Generation Partnership Project (3GPP) vendor-specific attribute (VSA) 3GGP-IMSI number in its authentication and accounting requests to a RADIUS server, use the **radius attribute suppress imsi** command in access-point configuration mode. To enable the GGSN to send the 3GPP VSA 3GPP-IMSI number in authentication and accounting requests to a RADIUS server, use the **no** form of the command.

radius attribute suppress imsi

no radius attribute suppress imsi

Syntax Description

This command has no arguments or keywords.

Defaults

The default is to send the 3GPP VSA 3GPP-IMSI number in authentication and accounting requests to a RADIUS server.

Command Modes

Access point configuration

Command History

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

Usage Guidelines

Use the **radius attribute suppress imsi** command to have GGSN suppress the 3GPP VSA 3GPP-IMSI number in its authentication and accounting requests to a RADIUS server.

Examples

The following example will not send the 3GPP VSA 3GPP-IMSI to the RADIUS server:

```
gprs access-point-list abc
   access-point 1
     radius attribute suppress imsi
```

Related Commands

Command	Description
access-mode	Specifies whether the GGSN requests user authentication at the access point to a PDN.
aaa-group	Specifies an AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN.
gprs default aaa-group	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN.
show gprs access-point	Displays information about access points on the GGSN.

radius attribute suppress qos

To specify that the gateway GPRS support node (GGSN) suppress the 3GPP VSA 3GPP-GPRS-QoS-Profile in its authentication and accounting requests to a RADIUS server, use the **radius attribute suppress qos** command in access-point configuration mode. To enable the GGSN to send the 3GPP VSA 3GPP-GPRS-QoS-Profile in authentication and accounting requests to a RADIUS server, use the **no** form of the command.

radius attribute suppress qos

no radius attribute suppress qos

Syntax Description

This command has no arguments or keywords.

Defaults

The default is to send the 3GPP VSA 3GPP-GPRS-QoS-Profile in authentication and accounting requests to a RADIUS server.

Command Modes

Access point configuration

Command History

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

Usage Guidelines

Use the **radius attribute suppress qos** command to have GGSN suppress the 3GPP VSA 3GPP-GPRS-QoS-Profile in its authentication and accounting requests to a RADIUS server.

Examples

The following example will not send the 3GPP VSA 3GPP-GPRS-QoS-Profile to the RADIUS server:

```
gprs access-point-list abc
   access-point 1
     radius attribute suppress qos
```

Related Commands

Command	Description
access-mode	Specifies whether the GGSN requests user authentication at the access point to a PDN.
aaa-group	Specifies an AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN.
gprs default aaa-group	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN.
show gprs access-point	Displays information about access points on the GGSN.

radius attribute suppress sgsn-address

To specify that the gateway GPRS support node (GGSN) suppress the 3GPP VSA 3GPP-SGSN-Address in its authentication and accounting requests to a RADIUS server, use the **radius attribute suppress sgsn-address** command in access-point configuration mode. To enable the GGSN to send the 3GPP VSA 3GPP-SGSN-Address in authentication and accounting requests to a RADIUS server, use the **no** form of the command.

radius attribute suppress sgsn-address

no radius attribute suppress sgsn-address

Syntax Description

This command has no arguments or keywords.

Defaults

The default is to send the 3GPP VSA 3GPP-SGSN-Address in authentication and accounting requests to a RADIUS server.

Command Modes

Access point configuration

Command History

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

Usage Guidelines

Use the **radius attribute suppress sgsn-address** command to have GGSN suppress the 3GPP VSA 3GPP-SGSN-Address in its authentication and accounting requests to a RADIUS server.

Examples

The following example will not send the 3GPP VSA 3GPP-SGSN-Address to the RADIUS server:

```
gprs access-point-list abc
   access-point 1
     radius attribute suppress sgsn-address
```

Related Commands

Command	Description
access-mode	Specifies whether the GGSN requests user authentication at the access point to a PDN.
aaa-group	Specifies an AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN.
gprs default aaa-group	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN.
show gprs access-point	Displays information about access points on the GGSN.

radius attribute user-name msisdn

To specify that the gateway GPRS support node (GGSN) include the MSISDN in the User-Name (attribute 1) in access requests at an APN, use the **radius attribute user-name msisdn** command in access-point configuration mode. To disable this configuration, use the **no** form of this command.

radius attribute user-name msisdn

no radius attribute user-name msisdn

Syntax Description

This command has no arguments or keywords.

Defaults

The default is to send the user name in the attribute 1.

Command Modes

Access point configuration

Command History

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

Usage Guidelines

Use the **radius attribute user-name msisdn** command to have GGSN send the MSISDN in the User-Name (attribute 1) instead of the user name in authentication and accounting requests to a RADIUS server.

Examples

The following example will send the MSISDN in access requests to the RADIUS server:

```
gprs access-point-list abc
   access-point 1
     radius attribute user-name msisdn
```

Related Commands

Command	Description
access-mode	Specifies whether the GGSN requests user authentication at the access point to a PDN.
aaa-group	Specifies an AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN.

Command	Description
gprs default aaa-group	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN.
show gprs access-point	Displays information about access points on the GGSN.

real-address

To configure the IP address of a real Content Services Gateway (CSG) for source checking on inbound messages from a CSG, use the **real-address** command in CSG group configuration mode.
To deconfigure the IP address of a real CSG, use the **no** form of this command

real-address *ip-address*

no real-address

Syntax Description

ip-address	IP address of a real CSG.

Defaults

No default behavior or values.

Command Modes

CSG group configuration

Command History

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

Usage Guidelines

Use the **real-address** CSG group configuration command to configure the IP address of a real CSG.

Configuring the IP address of a real CSG provides an additional security check against the source of messages. When configured, source address checking is performed on inbound message from the CSG.

For redundancy, you can configure up to two real IP addresses of CSGs in a CSG server group.

Using the **no** form of this command will remove the IP address from the list of IP addresses of a CSG server group.

Examples

The following configuration example configures two real IP addresses in CSG group csg1:

```
ggsn csg-group csg1
  virtual-address 5.5.5.14
  port 4444
  real-address 5.1.1.1
  real-address 5.1.1.2
```

Related Commands

Command	Description
ggsn csg-group	Configures a CSG group on the GGSN for quota server-to-CSG communication.
port	Configures the port number on which the CSG listens for quota server traffic.

Command	Description
show ggsn csg	Displays the parameters used by the CSG group or the number of path and quota management messages sent and received by the quota server.
virtual-address	Configures a virtual IP address to which the quota server will send all requests.

redirect all ip

To redirect all traffic to an external device, use the **redirect all ip** command in access-point configuration mode. To disable the redirection of all traffic, use the **no** form of this command.

redirect all ip *ip-address*

no redirect all ip *ip-address*

Syntax Description

ip-address	IP address of the external device to which you want to redirect traffic.

Defaults

Disabled

Command Modes

Access-point configuration

Command History

Release	Modification
12.3(2)XB2	This command was introduced.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **redirect all ip** access-point command to redirect all traffic to an external device (such as an external firewall) for verification.

Using the Redirect All Traffic feature, you can:

- Redirect all packets to a specified destination regardless of whether the destination address belongs to a mobile station (MS) on the same GGSN or not.

  If redirecting traffic using the Mobile-to-Mobile Redirect feature, only packets for which the destination address belongs to an MS that is active on the same GGSN can be redirected. If the receiving MS has no PDP context in the GGSN where the sending MS PDP context is created, the packets are dropped.
- Redirect all traffic to a specific destination when aggregate routes are configured.

Note On the Catalyst 6500 series switch / Cisco 7600 series platform, the traffic redirection feature requires that policy based routing (PBR) is configured on the MSFC2 and incoming VLAN interface from the Cisco MWAM, and that the next hop to route the packets is set using the **set ip next-hop** command.

Examples

The following example redirects all traffic to 5.5.5.13:

```
redirect all ip 5.5.5.13
```

Related Commands

Command	Description
security verify	Specifies the verification of source and/or destination addresses.

redirect intermobile ip

To redirect mobile-to-mobile traffic to an external device, use the **redirect intermobile ip** command in access-point configuration mode. To disable the redirection of mobile-to-mobile traffic, use the **no** form of this command.

redirect intermobile ip *ip-address*

no redirect intermobile ip *ip-address*

Syntax Description

ip-address	IP address of the external device to which you want to redirect mobile-to-mobile traffic.

Defaults

Disabled

Command Modes

Access-point configuration

Command History

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

Usage Guidelines

Use the **redirect intermobile ip** access-point command to redirect mobile-to-mobile traffic to an external device (such as an external firewall) for verification.

Redirection of intermobile traffic does not occur on an ingress APN unless the TPDUs are exiting the same APN. In addition, redirection of TPDUs tunneled by L2TP from the ingress APN to the LNS of the PDN does not occur.

On the Catalyst 6500 series switch / Cisco 7600 series internet router platform, the mobile-to-mobile redirection feature requires that policy based routing (PBR) is configured on the MSFC2 and incoming VLAN interface from the Cisco MWAM, and that the next hop to route the packets that match the criteria is set using the **set ip next-hop** command.

Examples

The following example redirects mobile-to-mobile traffic to 5.5.5.13:

```
redirect intermobile ip 5.5.5.13
```

Related Commands

Command	Description
gprs plmn ip address	Specifies the IP address range of a PLMN.
security verify	Specifies the verification of source and/or destination addresses.

security

To configure the security protocol to use for the Diameter peer-to-peer connection, use the **security** command in Diameter peer configuration mode. To remove a security protocol, use the **no** form of this command

security ipsec

no security

Syntax Description

ipsec	Defines IPSec as the security protocol to use for securing messages between peers.

Defaults

IPSec.

Command Modes

Diameter peer configuration

Command History

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

Usage Guidelines

Use the **security** command to define the security protocol to use for the Diameter peer-to-peer connection.

When the security protocol is changed dynamically, the connection to the peer is torn down and reestablished after Diameter peer configuration mode is exited.

Examples

The following configuration example defines IPSec as the security protocol to use for a peer-to-peer connection with Diameter peer “dcca1”:

```
Diameter peer dcca1
 address ipv4 10.10.10.1
 transport tcp port 4000
 security ipsec
```

Related Commands .

Command	Description
address ipv4	Configures the IP address of the Diameter peer host.
destination host	Configures the Fully Qualified Domain Name (FQDN) of the Diameter peer
destination realm	Configures the destination realm (domain name) in which the Diameter host is located.

Command	Description
diameter peer	Defines the Diameter peer (server) and enters diameter peer configuration mode.
ip vrf forwarding	Defines the VRF associated with the Diameter peer.
source interface	Configures the interface to use to connect to the Diameter peer.
timer	Configures Diameter base protocol timers for peer-to-peer communication.
transport	Configures the transport protocol to use to connect with the Diameter peer.

security verify

To enable the gateway GPRS support node (GGSN) to verify the IP verification of IP addresses in TPDUs, use the **security verify** command in access-point configuration mode. To disable the verification of IP addresses, use the **no** form of this command.

security verify {**source** | **destination**}

no security verify {**source** | **destination**}

Syntax Description

source	Specifies that the source IP address of an upstream TPDU be verified against the address previously assigned an MS.
destination	Specifies that the destination address of upstream TPDU received off a GTP tunnel be verified against the global list of PLMN addresses specified by the **gprs plmn ip address** global configuration command.

Defaults

Disabled

Command Modes

Access-point configuration

Command History

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

Usage Guidelines

Use the **security verify source** access point configuration command to configure the GGSN to verify the source IP address of an upstream TPDU against the address previously assigned to an MS.

When the **security verify source** command is configured on an APN, the GGSN verifies the source address of a TPDU before GTP will accept and forward it. If the GGSN determines that the address differs from that previously assigned to the MS, it drops the TPDU and accounts it as an illegal packet in its PDP context and APN. Configuring the **security verify source access point** configuration command protects the GGSN from faked user identities.

Use the **security verify destination** access point configuration command to have the GGSN verify the destination addresses of upstream TPDUs against global lists of PLMN addresses specified using the **gprs plmn ip address** command. If the GGSN determines that a destination address of a TPDU is within the range of a list of addresses, it drops the TPDU. If it determines that the TPDU contains a destination address that does not fall within the range of a list, it forwards the TPDU to its final destination.

Examples

The following example enables the verification of source IP addresses received in upstream TPDUs:

```
security verify source
```

Related Commands

Command	Description
redirect intermobile ip	Specifies the redirection of mobile-to-mobile traffic.
gprs plmn ip address	Specifies the IP address range of a PLMN.
show gprs access-point	Displays information about access points on the GGSN.

server (psd)2

To define a Persistent Storage Device (PSD) server (backup or retrieve-only), use the **server** command in data-store configuration mode. To remove the PSD server configuration, use the **no** form of this command.

server *psd-ip-address* [**retrieve-only**]

no slb vserver *psd-ip-address* [**retrieve-only**]

Syntax Description

ip_address	IP address of the PSD.
retrieve-only	Specifies that the GGSN will only retrieve G-CDRs from the PSD.

Defaults

No default behavior or values.

Command Modes

PSD group configuration

Command History

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

Usage Guidelines

Use the **server** data-store configuration command to define a PSD server or servers.

PSD servers can be configured as a “backup” or “retrieve-only” PSD.

The backup PSD server is a local PSD (within the same chassis) to which the GGSN writes G-CDRs if no charging gateway is available. When a charging gateway becomes available, the GGSN can be configured to automatically retrieve G-CDRs (using the **auto-retrieve** data-store configuration command) from the PSDs, or the G-CDRs can be manually retrieved via FTP.

Note The backup PSD server shares the same operational mode properties as the charging gateways.

In a GTP-SR implementation, a “retrieve-only” PSD must also be configured using the **server** data-store configuration command with the **retrieve-only** keyword option specified. A retrieve-only PSD defined for one GGSN also functions as a backup PSD for an alternate GGSN of a redundant pair. If a failover should occur, the newly active GGSN collects the G-CDRs from its retrieve-only PSD and forwards them to the charging gateway.

For example, if you have a redundantly configured GGSNs in chassis A and chassis B, each with their own PSDs (PSD A and PSD B), when the GGSN in chassis A is active, it writes to its local PSD, PSD A. PSD A is also defined as the retrieve-only PSD for the GGSN in chassis B.

If the active GGSN on chassis A becomes inactive, the standby GGSN in chassis B becomes active and begins writing to its backup PSD, PSD B. PSD B is also defined as the retrieve-only PSD for the GGSN in chassis A.

When PSD A on chassis A becomes available again, the GGSN on chassis B automatically initiates a retrieval of G-CDRs from PSD A on Chassis A (if the **auto-retrieval** command has been configured) or the G-CDRs are manually retrieved.

Note You can configure one backup PSD (local) and one retrieve-only PSD (remote) per PSD server group. One server group can be defined per GGSN.

Note If a retrieve-only PSD is configured without the **auto-retrieve** command configured as well, the GGSN will not initiate a start retrieve when a retrieving event occurs.

Examples

The following example defines the PSD to which the GGSN will backup G-CDRs as well as retrieve G-CDRs:

```
server 172.10.10.10
```

The following example defines a PSD with the IP address 192.10.10.1 as the “retrieve-only” PSD for a GGSN:

```
server 192.10.10.1 retrieve only
```

Related Commands

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

server (p-cscf)

To define a Proxy Call Session Control Function (P-CSCF) server in a P-CSCF server group, use the **server** command in P-CSCF group configuration mode. To remove the P-CSCF server configuration, use the **no** form of this command.

server [**ipv6**] *ip-address*

no server [**ipv6**] *ip-address*

Syntax Description

ipv6	(Optional) Specifies an IPv6 server to be a member of the P-CSCF group.
ip_address	IP address of the P-CSCF.

Defaults

No default behavior or values.

Command Modes

P-CSCF group configuration

Command History

Release	Modification
12.4(2)XB	This command was introduced.
12.4(9)XG	This command was integrated into Cisco IOS Release 12.4(9)XG and the **ipv6** keyword option was added.
12.4(15)XQ	This command was integrated into Cisco IOS Release 12.4(15)XQ.

Usage Guidelines

Use the **server** P-CSCF command in group configuration mode to define a P-CSCF server or servers in a P-CSCF server group.

The order of the addresses returned in the “P-CSCF Address Field” of the Protocol Configuration Option (PCO) is the same as the order in which they are defined in the P-CSCF server group and the groups are associated with the access point name (APN).

If no P-CSCF addresses are preconfigured, the Create PDP Context Response will not return any P-CSCF addresses. An error message will not be generated and the Create PDP Context Request will be processed.

Note Up to 10 P-CSCF servers can be defined in a P-CSCF server group. Both IPv6 and IPv4 P-CSCF servers can be defined in a server group. The packet data protocol (PDP) type dictates to which server the IP addresses are sent.

Examples

The following example defines an P-CSCF server with the IP address 172.10.10.10 to a P-CSCF server group:

```
gprs pcscf groupA
 server 172.10.10.10
```

Related Commands

Command	Description
gprs pcscf	Configures a P-CSCF server group on the GGSN and enters P-CSCF group configuration mode.
pcscf	Assigns a P-CSCF server group to an APN.
server	Specifies the IP address of a P-CSCF server that you want to include in the P-CSCF server group.
show gprs access-point	Displays information about access points on the GGSN.
show gprs pcscf	Displays a summary of the P-CSCF groups configured on the GGSN.

service-aware

To enable service-aware billing for a particular access point, use the **service-aware** command in access-point configuration mode. To disable the support on an access point, use the **no** form of this command.

service-aware

no service-aware

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Access-point configuration

Command History

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

Usage Guidelines

Use the **service-aware** command to enable service-aware billing for a particular access point.

When service-aware billing is enabled for an APN, using the **gprs gtp response-message wait-accounting** global configuration command, the GGSN must be configured to wait for a RADIUS accounting response before sending a Create PDP Context response to an SGSN for a Create PDP Context request.

Examples

The following configuration example enables service-aware billing for access-point 1:

```
interface virtual-template 1
 gprs access-point-list abc
!
gprs access-point-list abc
 access-point 1
  service-aware
```

Related Commands

Command	Description
gprs service-aware	Enables service-aware billing on the GGSN.

service-mode

To configure the service-mode state of an APN, use the **service-mode** command in access-point configuration mode. To return to the default value, use the **no** form of this command.

service-mode {operational | maintenance}

Syntax Description

operational	Specifies that the service-mode state of the APN is operational.
maintenance	Specifies that the service-mode state of the APN is maintenance.

Defaults

Operational

Command Modes

Access-point configuration

Command History

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

Usage Guidelines

Use the **service-mode** access-point configuration command to perform APN-related tasks (such as adding a new APN or modifying an existing APN) without affecting sessions for other APNs in the GGSN.

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

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

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

Note

When the GGSN is in global maintenance mode (**gprs service-mode maintenance** command), all APNs are in maintenance mode as well.

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

Examples

The following example changes the service-mode state of an APN to maintenance mode:

```
service-mode maintenance
```

Related Commands

Command	Description
gprs service-mode	Configures the service-mode state of a GGSN.
gprs service-mode test imsi	Configures a test user for which you can Create PDP Contexts to test an APN configuration.
show gprs access-point	Displays information about access points on the GGSN.
show gprs service-mode	Displays the current global service mode state of the GGSN and the last time it was changed.

service-policy

To attach a service policy to an APN, to be used as the service policy for PDP flows of that APN, use the **service-policy** command in access-point configuration mode. To remove a service policy, use the **no** form of this command.

service-policy input *policy-map-name*

no service-policy input *policy-map-name*

Syntax Description

input	Applies the specified policy map to incoming T-PDUs.
policy-map-name	The name of a service policy map (created using the **policy-map** command) to be attached. The name can be a maximum of 40 alphanumeric characters.

Defaults

No service policy is attached to an APN.

Command Modes

Access-point configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)XU	This command was integrated into Cisco IOS Release 12.3(8)XU.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.

Usage Guidelines

Use the **service-policy** access-point configuration command to attach a policy map to an APN when configuring the Per-PDP policing feature on the GGSN. Before attaching a policy map to an APN, the policy map must be configured using the **policy-map** command.

Note The Per-PDP policing feature requires that UMTS QoS has been configured.

Note Do not use flow-based policing with multiple DSCP-based classifications if trust DSCP is configured.

Note If you are using trust DSCP policy map configuration, ensure that you configure only one class map with **match flow pdp** in the policy map. Simultaneous multiple flows for policing, with different DSCPs for a PDP, are not supported.

Service policies cannot be attached to or removed from an APN when there are active PDP contexts on that APN. To modify a service policy, you must first disassociate it from the APN using the **no service-policy** access point configuration command.

Caution If you remove the global policy map configuration (using the **no policy-map** global configuration command), service policies associated with APNs will also be removed without any warning.

To configure the Per-PDP policing feature on a GGSN, you must complete the following tasks:

1. Create a class for PDP flows using the **class-map** command.

```
GGSN(config)# Class-map class-pdp
GGSN(config-cmap)# Match flow pdp
GGSN(config-cmap)# exit
```

2. Create a policy map using the **policy-map** command and assign a class to the map using the **class** command.

```
GGSN(config)# Policy-map policy-gprs
GGSN(config-pmap)# Class class-pdp
```

3. In the policy map, configure the Traffic Policing feature using the **police rate** policy map class configuration command.

```
GGSN(config-pmap-c)# police rate pdp [burst bytes] [peak-rate pdp [peak-burst bytes]]
conform-action action exceed-action action [violate-action action]
GGSN(config-pmap-c)# exit
GGSN(config-pmap)# exit
```

4. Attach a service policy to an APN using the **service-policy** access-point configuration command.

```
GGSN(config)# Access-point 1
GGSN(access-point-config) Service-policy in policy-gprs
```

Examples

The following example attaches service policy “policy-gprs” to access-point 1:

```
access-point 1
 service-policy in policy-gprs
```

Related Commands

Command	Description
match flow pdp	Specifies PDP flows as the match criterion in a class map.
police rate	Configures traffic policing using the police rate.

session idle-time

To specify the time, in hours, that the gateway GPRS support node (GGSN) waits before purging idle mobile sessions for the current access point, use the **session idle-time** command in access-point configuration mode. To disable the idle timer at the access point, use the **no** form of this command.

session idle-time *number*

no session idle-time

Syntax Description

number	Number of hours between 1 and 168.

Defaults

No session idle timer is configured on the access point.

Command Modes

Access-point configuration

Command History

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

Usage Guidelines

The GGSN implements the idle timer in 3 ways. These implementations are listed in the order in which the GGSN processes them.

- Radius server—If the access-point is configured for non-transparent access mode and the Radius server returns a session timeout attribute, then the GGSN uses the session idle timeout value from the Radius server.
- Access-point—If the access-point is configured for transparent access mode, or is in non-transparent access mode and the Radius server does not return a session idle timeout value, the GGSN uses the value that you specified for the **session idle-time** command.
- Global timer—If the GGSN does not get a session idle timeout value from the Radius server or the access-point, it uses the value that you specified in the **gprs idle-pdp-context purge-timer** command.

The **session idle-time** command value overrides the value configured in the **gprs idle-pdp-context purge-timer** command for that access-point.

When the session reaches the timeout value, the PDP context is deleted.

Note With GGSN Release 5.0 and later, you can also configure the session idle timer for an access-point using the **gtp pdp-context timeout idle** access-point configuration command, however, the two methods cannot be configured at the same time.

Use the **show gprs gtp pdp-context tid** command to view the session idle-time value. The value is shown in the "gtp pdp idle time" field.

Examples

The following example specifies that the GGSN waits for 5 hours before purging idle time sessions for access-point 1. The GGSN waits for 60 hours before purging idle time sessions for all access points *except* access-point 1:

```
gprs access-point-list abc
 access-point 1
  access-point-name gprs.pdn1.com
  session idle-time 5

gprs idle-pdp-context purge-timer 60
```

Related Commands

Command	Description
gprs gtp pdp-context timeout idle	Specifies the time, in seconds, that a GGSN allows a session to be idle before terminating the session.
gprs gtp pdp-context timeout session	Specifies the time, in seconds, that the GGSN allows a session to be active before terminating the session.
gtp pdp-context timeout idle	Specifies the time, in seconds, that the GGSN allows a session to be idle at a particular APN before terminating the session.
gtp pdp-context timeout session	Specifies the time, in seconds, that a GGSN allows a session to be active at a particular APN before terminating the session.
gprs idle-pdp-context purge-timer	Specifies the time that the GGSN waits before purging idle mobile sessions.
show gprs gtp pdp-context	Displays a list of the currently active PDP contexts (mobile sessions).

session-failover

To enable sessions to failover over to an alternate Diameter server (via Credit Control Session Failover [CCSF] AVP support) when a credit control answer (CCA) message from the DCCA server does not contain a value for the CCSF AVP, use the **session-failover** command in DCCA client profile configuration mode. To return to the default value, use the **no** form of this command

session-failover

no session-failover

Syntax Description

This command has no arguments or keywords.

Defaults

Session failover is not supported.

Command Modes

DCCA client profile configuration

Command History

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

Usage Guidelines

Use the **session-failover** command to configure session failover support locally by enabling the CCSF AVP. The CCSF AVP indicates whether a Diameter session should be failed over to an alternate Diameter server or not.

A value returned by a Diameter server in a CCA overrides the default configured locally.

When session failover is disabled, the Credit Control (CC) session will not be moved to an alternate DCCA server if a failure should occur. If support of the CCSF AVP is enabled, the CC session will be moved to an alternate destination if a failover should occur.

Examples

The following configuration example enables the CCSF AVP in CCRs for a DCCA client:

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

Related Commands

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