



Cisco IOS Mobile Wireless Commands

This book documents all of the Cisco IOS software commands in Cisco IOS Release 12.2(8)YD for the Gateway GPRS Support Node (GGSN) and GTP Director Module (GDM), in alphabetical order.

To locate the group of commands that are applicable to a particular technology area, such as General Packet Radio Service (GPRS), see the chapter, [“Cisco IOS GGSN Command Set”](#) in the [“Mobile Wireless Commands by Technology”](#) section on page 291.

aaa-accounting

To enable or disable accounting for a particular access point on the GGSN, use the **aaa-accounting** access-point configuration command.

aaa-accounting { **enable** | **disable** }

Syntax Description	enable	disable
	Enables accounting on the APN. When you configure an APN for non-transparent access, this is the default value.	Disables accounting on the APN. When you configure an APN for transparent access, this is the default value.

Defaults	enable	disable
	For non-transparent APNs	For transparent APNs

Command Modes	Access-point 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.

Usage Guidelines	The Cisco Systems GGSN has different defaults for enabling and disabling accounting services for transparent and non-transparent access points:
	<ul style="list-style-type: none"> If you configure an APN for non-transparent access using the access-mode command, the GGSN automatically enables accounting with authentication at the APN. If you configure an APN for transparent access, which is the default access mode, the GGSN automatically disables accounting at the APN. <p>Therefore, if you have configured a transparent access APN and you want to provide accounting at that APN, you need to configure the aaa-accounting enable command at the APN.</p> <p>However, for accounting to occur, you also must complete the configuration by specifying the following other configuration elements on the GGSN:</p> <ul style="list-style-type: none"> Enable AAA services using the aaa new-model global configuration command. Define a server group with the IP addresses of the RADIUS servers in that group using the aaa group server global configuration command. Configure the following AAA services: <ul style="list-style-type: none"> AAA authentication using the aaa authentication global configuration command AAA authorization using the aaa authorization global configuration command

- AAA accounting using the **aaa accounting** global configuration command as shown in [Example 2](#).
- Assign the type of services that the AAA server group should provide. If you only want the server group to support accounting services, then you need to configure the server for accounting only. You can assign the AAA services to the AAA server groups either at the GPRS global configuration level using the **gprs default aaa-group** command, or at the APN using the **aaa-group** command.
- Configure the RADIUS servers using the **radius-server host** command.

**Note**

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

To selectively disable accounting at specific APNs where you do not want that service, use the **aaa-accounting disable** access-point configuration command.

You can verify whether AAA accounting is enabled or disabled at an APN using the **show gprs access-point** command.

There is not a **no** form of this command.

Examples**Example 1**

The following configuration example disables accounting at access-point 1:

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

Example 2

The following configuration example enables accounting on transparent access-point 4. Accounting is disabled on access-point 5 because it is configured for transparent mode and the **aaa-accounting enable** command is not explicitly configured.

Accounting is automatically enabled on access-point 1 because it has been configured for non-transparent access mode. Accounting is explicitly disabled at access-point 3, because accounting is automatically enabled for non-transparent access mode.

An example of some of the AAA and RADIUS global configuration commands are also shown:

```
aaa new-model
!
aaa group server radius foo
  server 10.2.3.4
  server 10.6.7.8
aaa group server radius foo1
  server 10.10.0.1
aaa group server radius foo2
  server 10.2.3.4
  server 10.10.0.1
aaa group server foo3
  server 10.6.7.8
  server 10.10.0.1
```

```

!
aaa authentication ppp foo group foo
aaa authentication ppp foo2 group foo2
aaa authorization network default group radius
aaa accounting exec default start-stop group foo
aaa accounting network foo1 start-stop group foo1
aaa accounting network foo2 start-stop group foo2
!
gprs access-point-list gprs
  access-point 1
    access-mode non-transparent
    access-point-name www.pdn1.com
    aaa-group authentication foo
  !
  access-point 3
    access-point-name www.pdn2.com
    access-mode non-transparent
    aaa-accounting disable
    aaa-group authentication foo
  !
  access-point 4
    access-point-name www.pdn3.com
    aaa-accounting enable
    aaa-group accounting foo1
  !
  access-point 5
    access-point-name www.pdn4.com
  !
gprs default aaa-group authentication foo2
gprs default aaa-group accounting foo3
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.10.0.1 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel

```

Related Commands

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

aaa-group

To specify a AAA server group and assign the type of AAA services to be supported by the server group for a particular access point on the GGSN, use the **aaa-group** access-point configuration command. To remove a AAA server group, use the **no** form of this command.

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

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

Syntax Description

authentication	Assigns the selected server group for authentication services on the APN.
accounting	Assigns the selected server group for accounting services only on the APN.
<i>server-group</i>	Specifies the name of a AAA server group to be used for AAA services on the APN.
Note	The name of the AAA server group that you specify must correspond to a server group that you configure using the aaa group server command.

Defaults

No default behavior or values.

Command Modes

Access-point configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was 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.

Usage Guidelines

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

- You can selectively implement groups of servers for authentication and accounting at different APNs.
- You can configure different server groups for authentication services and accounting services in the same APN.
- You can control which RADIUS services you want to enable at a particular APN, such as AAA accounting.

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

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

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

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

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

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

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

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

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

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


Note

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

Examples

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

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

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

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

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

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

```
aaa new-model
!
aaa group server radius foo
  server 10.2.3.4
  server 10.6.7.8
aaa group server radius foo1
  server 10.10.0.1
aaa group server radius foo2
  server 10.2.3.4
  server 10.10.0.1
aaa group server foo3
  server 10.6.7.8
  server 10.10.0.1
!
aaa authentication ppp foo group foo
aaa authentication ppp foo2 group foo2
aaa authorization network default group radius
aaa accounting exec default start-stop group foo
aaa accounting network foo1 start-stop group foo1
aaa accounting network foo2 start-stop group foo2
aaa accounting network foo3 start-stop group foo3
!
gprs access-point-list gprs
  access-point 1
    access-mode non-transparent
    access-point-name www.pdn1.com
    aaa-group authentication foo
  !
  access-point 2
    access-mode non-transparent
    access-point-name www.pdn2.com
  !
  access-point 4
    access-point-name www.pdn4.com
    aaa-accounting enable
    aaa-group accounting foo1
  !
  access-point 5
    access-point-name www.pdn5.com
  !
```

```

gprs default aaa-group authentication foo2
gprs default aaa-group accounting foo3
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.10.0.1 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel

```

Related Commands

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

access-mode

To specify whether the GGSN requests user authentication at the access point to a PDN, use the **access-mode** access-point configuration command. To remove an access mode and return to the default value, use the **no** form of this command.

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

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

Syntax Description

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

Defaults

transparent

Command Modes

Access-point configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated in Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was incorporated in Cisco IOS Release 12.2(4)MX.
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.

Usage Guidelines

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

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

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

Examples

Example 1

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

```
interface virtual-template 1
  gprs access-point-list abc
```

```

!
gprs access-point-list abc
  access-point 1
    access-point-name gprs.pdn.com
    access-mode non-transparent

```

Example 2

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

```

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

```



Note

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

Related Commands

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

access-point

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

access-point *access-point-index*

no access-point *access-point-index*

Syntax Description	
	<i>access-point-index</i> Integer from 1 to 65535 that identifies a GPRS access point.

Defaults	
	No default behavior or values.

Command Modes	
	Access-point list configuration

Command History	Release	Modification
	12.1(1)GA	This command was introduced.
	12.1(5)T	This command was integrated in Cisco IOS Release 12.1(5)T.
	12.2(4)MX	This command was incorporated in Cisco IOS Release 12.2(4)MX.
	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.

Usage Guidelines	
	Use the access-point command to create an access point to a PDN.
	To configure an access point, first set up an access-point list using the gprs access-point-list command and then add the access point to the access-point list.
	You can specify access point numbers in any sequence.



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

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

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

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

access-point-name

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

access-point-name *apn-name*

no access-point-name *apn-name*

Syntax Description	<i>apn-name</i>	Specifies the network or domain name of the private data network that can be accessed through the current access point.
--------------------	-----------------	---

Defaults There is no default value for this command.

Command Modes Access-point configuration

Command History	Release	Modification
	12.1(1)GA	This command was introduced.
	12.1(5)T	This command was integrated in Cisco IOS Release 12.1(5)T.
	12.2(4)MX	This command was incorporated in Cisco IOS Release 12.2(4)MX.
	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.

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

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

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

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

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

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

access-type

To specify whether an access point is real or virtual on the GGSN, use the **access-type** access-point configuration command. To return to the default value, use the **no** form of this command.

access-type { virtual | real }

no access-type { virtual | real }

Syntax Description	virtual	real
	Specifies an APN type that is not associated with any specific physical target network on the GGSN.	Specifies an APN type that corresponds to an external physical network to a PDN on the GGSN. This is the default value.

Defaults **real**

Command Modes Access-point configuration

Command History	Release	Modification
	12.2(4)MX	This command was introduced.
	12.2(8)YD	This command was 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.

Usage Guidelines Use the **access-type** command to specify whether an access point is real or virtual on the GGSN. You only need to configure this command for virtual access types.

Virtual access types are used to configure virtual APN support on the Cisco Systems GGSN to minimize provisioning issues in other GPRS network entities that require configuration of APN information. Using the virtual APN feature on the Cisco Systems GGSN, HLR subscription data can simply provide the name of the virtual APN. User's can still request access to specific target networks that are accessible by the GGSN without requiring each of those destination APNs to be provisioned at the HLR.

The default keyword, **real**, identifies a physical target network that the GGSN can reach. Real APNs must always be configured on the GGSN to reach external networks. Virtual APNs can be configured in addition to real access points to ease provisioning in the GPRS PLMN.

No other access-point configuration commands are applicable if the access type is virtual.

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

```
access-point 1
  access-point-name corporate
  access-type virtual
exit
access-point 2
  access-point-name corporatea.com
```

```
ip-address-pool dhcp-client  
dhcp-server 10.21.21.1
```

Related Commands

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

access-violation deactivate-pdp-context

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

access-violation deactivate-pdp-context

no access-violation deactivate-pdp-context

Syntax Description This command has no arguments or keywords.

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

Command Modes Access-point configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated in Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was incorporated in Cisco IOS Release 12.2(4)MX.
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 and the discard-packets option was removed.

Usage Guidelines

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

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

Examples

The following example shows deactivation of a user's access in addition to discarding the user packets:

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


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

aggregate

To configure the GGSN to create an aggregate route in its IP routing table, when receiving PDP requests from MSs on the specified network, for a particular access point on the GGSN, use the **aggregate** access-point configuration command. To remove an aggregate route, use the **no** form of this command.

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Access-point configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was 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.

Usage Guidelines

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

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

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

To configure the GGSN to automatically aggregate routes that are returned by a DHCP or RADIUS server, use the **aggregate auto** command at the APN. Automatic route aggregation can be configured at the access-point configuration level only on the GGSN. The **gprs default aggregate** global configuration command does not support the **auto** option; therefore, you cannot configure automatic route aggregation globally on the GGSN.

You can specify multiple **aggregate** commands at each access point to support multiple network aggregates. However, if you use the **aggregate auto** command at the APN, you cannot specify any other aggregate route ranges at the APN. If you need to handle other static route cases at the APN, then you will have to use the **gprs default aggregate** global configuration command.

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

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

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

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

**Note**

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

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

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

**Note**

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

Examples**Example 1**

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

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

**Note**

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

Example 2

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

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

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

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

```

    dhcp-gateway-address 10.88.0.1
    exit
!
gprs default aggregate 10.80.0.0 255.255.255.0

```

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

```

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

```

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

```

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

Gateway of last resort is not set

    10.80.0.0/16 is subnetted, 1 subnets
C       10.80.0.0 is directly connected, Loopback0
    10.113.0.0/16 is subnetted, 1 subnets
C       10.113.0.0 is directly connected, Virtual-Access1
    172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
C       172.16.43.192/28 is directly connected, FastEthernet0/0
S       172.16.43.0/24 is directly connected, FastEthernet0/0
S       172.16.43.35/32 is directly connected, Ethernet2/3
    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
U       10.88.0.0/24 [1/0] via 0.0.0.0, Virtual-Access1
C       10.88.0.0/16 is directly connected, Loopback2

```

Related Commands

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

anonymous user

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

anonymous user *username* [*password*]

no anonymous user *username* [*password*]

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Access-point configuration

Command History

Release	Modification
12.2(4)MX	This command was introduced.
12.2(8)YD	This command was 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.

Usage Guidelines

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

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

Examples

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

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

block-foreign-ms

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

block-foreign-ms

no block-foreign-ms

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Access-point configuration

Command History	Release	Modification
	12.2(8)YD	This command was introduced.
	12.2(8)YW	This command was incorporated in Cisco IOS Release 12.2(8)YW.

Usage Guidelines The **block-foreign-ms** command enables the GGSN to block foreign MSs from accessing the GGSN. When you use this command, the GGSN determines if an MS is inside or outside of the PLMN based on the mobile country code (MCC) and mobile network code (MNC). The MCC and MNC are specified using the **gprs mcc mnc** command.



Note

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

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

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

Related Commands	Command	Description
	gprs mcc mnc	Configures the mobile country code and mobile network code that the GGSN uses to determine whether a create PDP context request is from a foreign MS.

clear gprs access-point statistics

To clear statistics counters for a specific access point or for all access points on the GGSN, use the **clear gprs access-point statistics** privileged EXEC command.

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

Syntax Description		
	<i>access-point-index</i>	Index number of an access point. Information about that access point is cleared.
	all	Information about all access points on the GGSN is cleared.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)MX	This command was introduced.
	12.2(8)YD	This command was 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.

Usage Guidelines This command clears the statistics that are displayed by the **show gprs access-point statistics** command.

Examples The following example clears the statistics at access point 2:

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

The following example clears the statistics for all access points:

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

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

clear gprs charging cdr

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

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

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

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(1)GA	This command was introduced.
	12.1(5)T	This command was integrated in Cisco IOS Release 12.1(5)T.
	12.2(4)MX	This command was incorporated in Cisco IOS Release 12.2(4)MX and the partial-record keyword was added.
	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.

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

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

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

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

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

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

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

Examples

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

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

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

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

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

Related Commands

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

clear gprs gtp pdp-context

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

```
clear gprs gtp pdp-context { tid tunnel-id | imsi imsi_value | path ip-address [remote_port_num] | access-point access-point-index | all }
```

Syntax Description	Parameter	Description
	tid <i>tunnel-id</i>	Tunnel ID (TID) for which PDP contexts are to be cleared.
	imsi <i>imsi_value</i>	International Mobile Subscriber Identity (IMSI) value for which PDP contexts are to be cleared.
	path <i>ip-address</i> [<i>remote_port_num</i>]	Remote SGSN IP address for which all PDP contexts associated with the SGSN are to be cleared. Optionally, the remote SGSN IP address and remote port number for which all PDP contexts are to be cleared.
	access-point <i>access-point-index</i>	Access-point index for which PDP contexts are to be cleared.
	all	Clear all currently active PDP contexts.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(1)GA	This command was introduced.
	12.1(5)T	This command was integrated in Cisco IOS Release 12.1(5)T.
	12.2(4)MX	This command was incorporated in Cisco IOS Release 12.2(4)MX.
	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.

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

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

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

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

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

Examples

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

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

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

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

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

clear gprs gtp statistics

To clear the current GPRS GTP statistics, use the **clear gprs gtp statistics** privileged EXEC configuration command.

clear gprs gtp statistics

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(1)GA	This command was introduced.
	12.1(5)T	This command was integrated in Cisco IOS Release 12.1(5)T.
	12.2(4)MX	This command was incorporated in Cisco IOS Release 12.2(4)MX.
	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.

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



Note

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

Examples The following example clears the GPRS GTP statistics:

```
router# clear gprs gtp statistics
```

clear gprs gtp-director statistics

To clear the current counters for GTP Director Module (GDM) statistics, use the **clear gprs gtp-director statistics** privileged EXEC configuration command.

clear gprs gtp-director statistics

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(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.

Usage Guidelines Use the **clear gprs gtp-director statistics** command to clear all of the counters that are displayed by the **show gprs gtp-director statistics** command.

Examples The following example clears the GDM counters:

```
router# clear gprs gtp-director statistics
```

Related Commands	Command	Description
	show gprs gtp-director statistics	Displays the current statistics for requests received and processed by GDM.

dhcp-gateway-address

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

dhcp-gateway-address *ip-address*

no dhcp-gateway-address *ip-address*

Syntax Description	<i>ip-address</i>	The IP address of the DHCP gateway to be used in DHCP requests for users who connect through the specified access point.
--------------------	-------------------	--

Defaults When you do not configure a **dhcp-gateway-address**, the GGSN uses the virtual template interface address as the DHCP gateway address.

Command Modes Access-point configuration

Command History	Release	Modification
	12.1(1)GA	This command was introduced.
	12.1(5)T	This command was integrated in Cisco IOS Release 12.1(5)T.
	12.2(4)MX	This command was incorporated in Cisco IOS Release 12.2(4)MX.
	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.

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

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

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

Examples

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

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

Related Commands

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

dhcp-server

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

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

```
no dhcp-server {ip-address} [ip-address] [vrf]
```

Syntax Description		
<i>ip-address</i>	IP address of a DHCP server. The first <i>ip-address</i> argument specifies the IP address of the primary DHCP server. The second (optional) <i>ip-address</i> argument specifies the IP address of a backup DHCP server.	
vrf	DHCP server uses the VPN routing and forwarding (VRF) table that is associated with the APN.	

Defaults Global routing table

Command Modes Access-point configuration

Command History	Release	Modification
	12.1(1)GA	This command was introduced.
	12.1(5)T	This command was integrated in Cisco IOS Release 12.1(5)T.
	12.2(4)MX	This command was incorporated in Cisco IOS Release 12.2(4)MX, with the following changes: <ul style="list-style-type: none"> The vrf keyword was added. The <i>name</i> argument, as an option for a hostname in place of the IP address of a host, has been removed.
	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.

Usage Guidelines To configure DHCP on the GGSN, you must configure either the **gprs default ip-address-pool** global configuration command, or the **ip-address-pool** access-point configuration command with the **dhcp-proxy-client** keyword option.

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

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

The DHCP server can be specified in two ways:

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

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

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

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

Examples

Example 1

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

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

Example 2

The following example shows a VRF configuration for vpn3 (without tunneling) using the **ip vrf** global configuration command. Because the **ip vrf** command establishes both VRF and CEF routing tables, notice that **ip cef** also is configured at the global configuration level to enable CEF switching at all of the interfaces.

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

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

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

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

```
ip vrf vpn3
 rd 300:3
!
interface Loopback1
 ip address 10.30.30.30 255.255.255.255
!
interface Loopback2
 ip vrf forwarding vpn3
 ip address 10.27.27.27 255.255.255.255
!
interface FastEthernet0/0
 ip vrf forwarding vpn3
 ip address 10.50.0.1 255.255.0.0
 duplex half
!
interface FastEthernet1/0
 ip address 10.70.0.1 255.255.0.0
 duplex half
!
interface loopback 1
 ip address 10.8.0.1 255.255.255.0
!
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list gprs
!
ip route 10.10.0.1 255.255.255.255 Virtual-Template1
ip route vrf vpn3 10.100.0.5 255.255.255.0 fa0/0 10.50.0.2
ip route 10.200.0.5 255.255.255.0 fa1/0 10.70.0.2
!
no ip http server
!
gprs access-point-list gprs
 access-point 1
  access-point-name gprs.pdn.com
  ip-address-pool dhcp-proxy-client
  dhcp-server 10.200.0.5
  dhcp-gateway-address 10.30.30.30
  network-request-activation
  exit
!
 access-point 2
  access-point-name gprs.pdn2.com
  access-mode non-transparent
  ip-address-pool dhcp-proxy-client
  dhcp-server 10.100.0.5 10.100.0.6 vrf
  dhcp-gateway-address 10.27.27.27
  aaa-group authentication foo
  vrf vpn3
  exit
!
gprs default ip-address-pool dhcp-proxy-client
gprs gtp ip udp ignore checksum
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

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

encapsulation gtp

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

encapsulation gtp

no encapsulation gtp

Syntax Description This command has no arguments or keywords.

Defaults PPP encapsulation

Command Modes Interface configuration

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated in Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was incorporated in Cisco IOS Release 12.2(4)MX.
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.

Usage Guidelines Use the **encapsulation gtp** command to specify the GTP as the encapsulation type for a virtual template. This is a mandatory setting for both the GGSN and GDM.

Examples The following example specifies the GPRS tunneling protocol (GTP) as the encapsulation type:

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

gprs access-point-list

To configure an access point list that you use to define PDN access points on the GGSN, use the **gprs access-point-list** global configuration command. To remove an existing access-point list, use the **no** form of this command.

gprs access-point-list *list_name*

no gprs access-point-list *list_name*

Syntax Description	<i>list_name</i>	The name of the access-point list.
--------------------	------------------	------------------------------------

Defaults	No access-point list is defined
----------	---------------------------------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.1(1)GA	This command was introduced.
	12.1(5)T	This command was integrated in Cisco IOS Release 12.1(5)T.
	12.2(4)MX	This command was incorporated in Cisco IOS Release 12.2(4)MX.
	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.

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

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

```
! Virtual Template configuration
interface virtual-template 1
 ip unnumber loopback 1
 no ip directed-broadcast
 encapsulation gtp
 gprs access-point-list abc
!
! Access point list configuration
gprs access-point-list abc
 access-point 1
  access-point-name gprs.somewhere.com
  exit
!
 access-point 2
  access-point-name xyz.com
  exit
```

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

gprs canonical-qos best-effort bandwidth-factor

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

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

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

Syntax Description	<i>bandwidth-factor</i>	Integer from 1 to 4000000 that specifies the desired bandwidth factor (in bits per second). The default is 10 bits per second.
---------------------------	-------------------------	--

Defaults	10 bits per second
-----------------	--------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated in Cisco IOS Release 12.1(5)T.	
12.2(4)MX	This command was incorporated in Cisco IOS Release 12.2(4)MX.	
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.	

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



Note

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

Examples	The following example configures a bandwidth factor of 20: <pre>gprs canonical-qos best-effort bandwidth-factor 20</pre>
-----------------	---

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

gprs canonical-qos gsn-resource-factor

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

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

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

Syntax Description	<i>resource-factor</i>	Integer between 1 and 4294967295 representing an amount of resource that the GGSN calculates internally for canonical QoS processing. The default value is 3145728000.
---------------------------	------------------------	--

Defaults	3,145,728,000
-----------------	---------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.1(1)GA	This command was introduced.
	12.1(5)T	This command was integrated in Cisco IOS Release 12.1(5)T.
	12.2(4)MX	This command was incorporated in Cisco IOS Release 12.2(4)MX and the default value was changed from 1,048,576 to 3,145,728,000 bits per second.
	12.2(8)YD	This command was 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.

Usage Guidelines	The default value for this command was chosen to support 10000 PDP contexts with a premium QoS class. If a greater throughput is required for GPRS user data, increase the resource factor value. However, selecting a high value may result in exceeding the actual processing capacity of the GGSN.
-------------------------	---

Examples	The following example configures a resource factor of 1048576: <pre>gprs canonical-qos gsn-resource-factor 1048576</pre>
-----------------	---

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

gprs canonical-qos map tos

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

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

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

Syntax Description

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

Defaults

When canonical QoS is enabled on the GGSN, the default IP ToS precedence values are assigned according to the canonical QoS class as follows:

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

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated in Cisco IOS Release 12.1(5)T.
12.2(4)MX	This command was incorporated in Cisco IOS Release 12.2(4)MX.
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.

Usage Guidelines

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

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

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

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

Examples

The following example specifies a QoS mapping from the canonical QoS classes to a premium ToS category of five, a normal ToS category of three, and a best-effort ToS category of two:

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

Related Commands

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

gprs canonical-qos premium mean-throughput-deviation

To specify a mean throughput deviation factor that the GGSN uses to calculate the allowable data throughput for the premium QoS class, use the **gprs canonical-qos premium mean-throughput-deviation** global configuration command. To return to the default value, use the **no** form of this command.

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

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

Syntax Description	<i>deviation_factor</i>	Value that specifies the deviation factor. This value can range from 1 to 1000. The default value is 100.
---------------------------	-------------------------	---

Defaults	100
-----------------	-----

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.1(1)GA	This command was introduced.
12.1(5)T	This command was integrated in Cisco IOS Release 12.1(5)T.	
12.2(4)MX	This command was incorporated in Cisco IOS Release 12.2(4)MX.	
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.	

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

$$EB = \text{Min}[p, m + a(p - m)]$$

Where

EB = the effective bandwidth

p = peak throughput from the GPRS QoS profile in PDP context requests

m = mean throughput from the GPRS QoS profile in PDP context requests

a = the deviation factor divided by 1000 (a/1000)

Examples The following example configures a mean throughput deviation of 1000:

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

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