

PDG Service Configuration Mode Commands

The PDG Service Configuration Mode is used to specify the properties required for the UEs in the WLAN (Wireless Local Access Network) to interface with the Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG).

Command Modes

Exec > Global Configuration > Context Configuration > PDG Service Configuration

configure > context *context_name* **> pdg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdg-service)#
```

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands chapter.

- aaa attribute, on page 1
- associate sgtp-service, on page 2
- certificate-selection, on page 3
- bind, on page 4
- ip gnp-qos-dscp, on page 6
- ip qos-dscp, on page 9
- ip source-violation, on page 11
- max-tunnels-per-ue, on page 13
- plmn id, on page 13
- setup-timeout, on page 14

aaa attribute

Sets the attributes that the system uses in AAA messages.

Product PDG/TTG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PDG Service Configuration

configure > context *context_name* **> pdg-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pdg-service)#`

Syntax Description

```
aaa attribute { 3gpp-negotiated-qos-profile string }
no aaa attribute
```

3gpp-negotiated-qos-profile *string*

Specifies the 3GPP negotiated QoS profile to use in AAA messages during IMS emergency call handling as an alphanumeric string of 1 through 31 characters.

no aaa attribute

Removes a previously configured AAA attribute.

Usage Guidelines Specifies the 3GPP negotiated QoS profile to use in AAA messages during IMS emergency call handling.

Example

The following command specifies the 3GPP negotiated QoS profile to use during IMS emergency call handling:

```
aaa attribute 3gpp-negotiated-qos-profile 100
```

associate sgtp-service

Identifies the SGTP service to be associated with the PDG service to enable TTG functionality on the PDG/TTG. TTG functionality supports GTP-C (GTP control plane) messaging and GTP-U (GTP user data plane) messaging between the TTG and the GGSN over the Gn' interface.

Important This command can be used before the associated service instance is created and configured but care should be used to match the service names.

Product PDG/TTG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PDG Service Configuration

configure > context *context_name* **> pdg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdg-service)#
```

Syntax Description

`[ no ] associate sgtp-service` *`sgtp_service_name`* **`[ context`** *`sgtp_context_name`* **`]`**

no

Removes the service association definition from the configuration.

sgtp-service *sgtp_service_name*

Specifies which SGTP service configuration, by naming the SGTP service instance, to associate with this PDG service.

sgtp_service_name is an alphanumeric string of 1 through 63 characters with no spaces.

context *sgpt_context_name*

Defines the context in which the SGTP service was created. If no context is specified, the current context is used.

sgtp_context_name is an alphanumeric string of 1 through 63 characters with no spaces.

Usage Guidelines

Use this command to associate the SGTP service to be associated with the PDG service to enable TTG functionality on the PDG/TTG.

Example

The following command associates SGTP service *sgtp_service_1* with this PDG service:

```
associate sgtp-service sgtp_service_1 context sgtp_context_1
```

certificate-selection

Configures the PDG/TTG to select the trusted certificate (and the private key for calculating the AUTH payload) to be included in the first IKE_AUTH message from the PDG/TTG based on the APN (Access Point Name). The selected certificate is associated with the APN included in the IDr payload of the first IKE_AUTH message from the UE.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDG Service Configuration

configure > context *context_name* **> pdg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdg-service)#
```

Syntax Description

```
[ no ] certificate-selection apn-based
default certificate-selection
```

certificate-selection apn-based

Selects a trusted certificate for the first IKE-AUTH message based on the APN.

no certificate-selection

Disables APN-based certificate selection and resumes sending a certificate bound to a crypto template.

default certificate-selection

Sets the default certificate selection method to a certificate bound to a crypto template.

Usage Guidelines

Configures the PDG/TTG to select the trusted certificate to be included in the first IKE_AUTH message based on the APN.

Example

Use the following example to enable APN-based certificate selection:

```
certificate-selection apn-based
```

bind

Binds the PDG service IP address to a crypto template and specifies the maximum number of sessions the PDG service supports.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDG Service Configuration

configure > **context** *context_name* > **pdg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdg-service)#
```

Syntax Description

[no] bind address *ipv4_address* **{ crypto-template** *string* **} mode { ttg | pdg } [max-sessions** *number* **]**

no

Removes a previously configured binding.

bind address *ipv4_address*

Specifies the IPv4 address of the PDG service with which the UE attempts to establish an IKEv2/IPSec tunnel. This address must be a valid IP address within the context.

This is a mandatory parameter.

crypto-template *string*

Specifies the name of the crypto template to be bound to the PDG service. This is the name of the IPSec policy to be used as a template for PDG/TTG subscriber session IPSec policies. The crypto template includes most of the IPSec and IKEv2 parameters for keepalive, lifetime, NAT-T, and cryptographic and authentication algorithms. There must be one crypto template per PDG service.

This is a mandatory parameter.

string is an alphanumeric string of 0 through 127 characters.

mode { ttg | pdg }

Default: There is no default value.

Specifies whether the PDG service provides TTG or PDG functionality, as follows:

- In TTG mode, PDN connectivity is provided through the GGSN. PDG functionality is provided by the combined TTG and GGSN.
- In PDG mode, PDN connectivity and PDG functionality are provided directly through the PDG service.

This is a mandatory parameter.



Important PDG mode is not supported in this software release.

Dependencies:

When you configure the PDG service to be in TTG mode, you must also configure the SGTP service using the **associate sgtp-service** command, as the TTG needs to connect with the GGSN to complete the PDG functionality.

The following behaviors occur when the PDG service operates in TTG mode:

- If the SGTP service associated with PDG service is not configured, the PDG service is not started.
- If the SGTP service associated with PDG service is not started, the PDG service is not started.
- If the SGTP service associated with PDG service is stopped, the PDG service is stopped.
- If the SGTP service associated with PDG service is re-started, the PDG service is re-started.
- If the SGTP service is not yet configured, whenever the SGTP service is started, the PDG service is started.

Note that starting or stopping the PDG service has no impact on the SGTP service.

max-sessions *number*

Specifies the maximum number of sessions to be supported by the PDG service as an integer from 0 through 1000000. Default: 1000000

If the max-sessions value is changed on an existing system, the new value takes effect immediately if it is higher than the current value. If the new value is lower than the current value, existing sessions remain established, but no new sessions are permitted until usage falls below the newly-configured value.

Usage Guidelines

Use this command in PDG Service Configuration Mode to bind the IP address used as the connection point for establishing IKEv2/IPSec sessions to a crypto template. You can also use it to define the maximum number of sessions the PDG service supports.

Example

The following command binds a PDG service with an IP address of *209.165.200.228* to the crypto template *crypto_template_1*, sets the mode to TTG, and sets the maximum number of sessions to *500000*:

```
bind address 209.165.200.228 crypto-template crypto_template_1 mode ttg
max-sessions 500000
```

ip gnp-qos-dscp

Configures the quality of service (QoS) differentiated service code point (DSCP) used when sending data packets over the Gn' interface in the uplink direction.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDG Service Configuration

configure > **context** *context_name* > **pdg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdg-service)#
```

Syntax Description

[no] ip gnp-qos-dscp { background *dscp* **| conversational***dscp* **| interactive** *dscp* **| streaming** *dscp* **| interactive [traffic-handling-priority** *traffic_priority* **] { allocation-retention-priority** *allocation_retention_priority* **} } +**
default ip gnp-qos-dscp

no

Disables the overriding of the ToS (Type of Service) field and enables the pass-through option.

background *dscp*

Specifies the DSCP marking to be used for packets of sessions subscribed to the 3GPP background class, in which the data transfer is not time-critical (for example, in e-mail exchanges). This traffic class is the lowest QoS.

dscp: Sets the DSCP for the specified traffic class. See the *dscp* section below.

conversational *dscp*

Specifies the DSCP marking to be used for packets of sessions subscribed to the 3GPP conversational class, in which there is a constant flow of traffic in both the uplink and downlink direction. This traffic class is the highest QoS.

dscp: Sets the DSCP for the specified traffic pattern. See the dscp section below.

interactive [traffic-handling-priority *traffic_priority*]

Specifies the DSCP marking to be used for packets of sessions subscribed to three possible traffic priorities in the 3GPP interactive class, in which there is an intermittent flow of packets in the uplink and downlink direction. This traffic class has a higher QoS than the background class, but not as high as the streaming class.

traffic_priority is the 3GPP traffic handling priority and can be the integers 1, 2 or 3.

allocation-retention-priority *allocation_retention_priority*

Specifies the DSCP for the interactive class if the allocation priority is present in the QoS profile.

allocation-retention-priority can be the integers 1, 2, or 3.

DSCP uses the values in the following table based on the traffic handling priority and allocation/retention priority if the allocation priority is present in the QOS profile.

Allocation Priority	1	2	3
Traffic Handling Priority			
1	ef	ef	ef
2	af21	af21	af21
3	af21	af21	af21



Important If you only configure DCSP marking for interactive traffic classes without specifying ARP, it may not properly take effect. The CLI allows this scenario for backward compatibility however, it is recommended that you configure all three values.

streaming *dscp*

Specifies the DSCP marking to be used for packets of sessions subscribed to the 3GPP streaming class, in which there is a constant flow of data in either in the uplink or downlink direction. This traffic class has a higher QoS than the interactive class, but not as high as the conversational class.

dscp: Set the DSCP for the specified traffic pattern. See the dscp section below.

dscp

Default:

- background: be
- interactive
- Traffic Priority 1: ef
- Traffic Priority 1: af21
- Traffic Priority 1: af21
- streaming: af11
- conversational: ef

Specifies the DSCP for the specified traffic pattern. *dscp* can be configured to any one of the following:

- af11: Assured Forwarding 11 per-hop-behavior (PHB)
- af33: Assured Forwarding 33 PHB

- af12: Assured Forwarding 12 PHB
- af13: Assured Forwarding 13 PHB
- af21: Assured Forwarding 21 PHB
- af22: Assured Forwarding 22 PHB
- af23: Assured Forwarding 23 PHB
- af31: Assured Forwarding 31 PHB
- af32: Assured Forwarding 32 PHB
- af41: Assured Forwarding 41 PHB
- af42: Assured Forwarding 42 PHB
- af43: Assured Forwarding 43 PHB
- be: Best effort forwarding PHB
- ef: Expedited forwarding PHB

+

More than one of the above keywords can be entered within a single command.

Usage Guidelines

DSCP levels can be assigned to specific traffic patterns in order to ensure that data packets are delivered according to the precedence with which they're tagged. The diffserv markings are applied to the IP header of every subscriber data packet transmitted over the Gn' interface(s).

The four traffic patterns have the following order of precedence: background (lowest), interactive, streaming, and conversational (highest). Data packets falling under the category of each of the traffic patterns are tagged with a DSCP that further indicate their precedence as shown in the following tables:

Drop Precedence	Class			
	Class 1	Class 2	Class 3	Class 4
Low	af11	af21	af31	af41
Medium	af12	af22	af32	af41
High	af13	af23	af33	af43

Precedence (low to high)	DSCP
1	Best Effort (be)
2	Class 1
3	Class 2
4	Class 3
5	Class 4
6	Express Forwarding (ef)

The DSCP level can be configured for multiple traffic patterns within a single instance of this command.

Example

The following command configures the DSCP level for the streaming traffic pattern to be ef:**ip gnp-qos-dscp streaming ef**

The following command configures the DSCP levels for the conversational, streaming, interactive and background traffic patterns to be ef, af22, and af41, respectively:**ip gnp-qos-dscp conversational ef streaming ef interactive af22 background af41**

ip qos-dscp

Configures the quality of service (QoS) differentiated service code point (DSCP) used when sending data packets over the Wu interface in the downlink direction.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDG Service Configuration

configure > context *context_name* **> pdg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdg-service)#
```

Syntax Description

```
ip qos-dscp { qci { 1 { dscp-pt } | 2 { dscp-pt } | 3 { dscp-pt } | 4 { dscp-pt } | 5
 { allocation-retention-priority 1..3 | dscp-pt } | 6 { allocation-retention-priority 1..3
 | dscp-pt } | 7 { allocation-retention-priority 1..3dscp | dscp-pt } | 8 {
allocation-retention-priority 1..3 | dscp-pt } | 9 { dscp-pt } + }
no ip qos-dscp { qci { 1 | 2 | 3 | 4 | 5 { allocation-retention-priority 1..3 | dscp-pt
 } | 6 { allocation-retention-priority 1..3 | dscp-pt } | 7 { allocation-retention-priority
 1..3 | dscp-pt } | 8 { allocation-retention-priority 1..3 | dscp-pt } | 9 {+
```

allocation-retention-priority

Specifies the DSCP for interactive class if the allocation priority is present in the QOS profile.

allocation-retention-priority can be the integers 1, 2, or 3.

DSCP values use the following matrix to map based on traffic handling priority and Alloc/Retention priority if the allocation priority is present in the QOS profile.

The following table shows the DSCP value matrix for *allocation-retention-priority*.

Table 1: Default DSCP Value Matrix

	Allocation Priority 1	Allocation Priority 2	Allocation Prior
Traffic Handling Priority			
1	ef	ef	ef
2	af21	af21	af21

	Allocation Priority 1	Allocation Priority 2	Allocation Priority 3
3	af21	af21	af21

qci

Configures the QCI attribute of QoS. Here the *qci_val* is the QCI for which the negotiate limit is being set, it ranges from 1 to 9.

dscp

Default QCI:

- 1: ef
- 2: ef
- 3: af11
- 4: af11
- 5: ef
- 6: ef
- 7: af21
- 8: af21
- 9: be

Specifies the DSCP for the specified traffic pattern. *dscp* can be configured to any one of the following:

• **af11:** Assured Forwarding 11 per-hop-behavior (PHB)	• **af32:** Assured Forwarding 32 PHB
• **af12:** Assured Forwarding 12 PHB	• **af33:** Assured Forwarding 33 PHB
• **af13:** Assured Forwarding 13 PHB	• **af41:** Assured Forwarding 41 PHB
• **af21:** Assured Forwarding 21 PHB	• **af42:** Assured Forwarding 42 PHB
• **af22:** Assured Forwarding 22 PHB	• **af43:** Assured Forwarding 43 PHB
• **af23:** Assured Forwarding 23 PHB	• **be:** Best effort forwarding PHB
• **af31:** Assured Forwarding 31 PHB	• **ef:** Expedited forwarding PHB

+

More than one of the above keywords can be entered within a single command.

Usage Guidelines

You can assign DSCP to specific traffic patterns to ensure that data packets are delivered according to the precedence with which they are tagged. The diffserv markings are applied to the outer IP header of every GTP data packet. The diffserv marking of the inner IP header is not modified.

The traffic patterns are defined by QCI (1 to 9). Data packets falling under the category of each of the traffic patterns are tagged with a DSCP that further indicate their precedence as shown in the following tables:

Table 2: Class structure for assured forwarding (af) levels

Drop Precedence	Class			
	Class 1	Class 2	Class 3	Class 4
Low	af11	af21	af31	af41
Medium	af12	af22	af32	af41
High	af13	af23	af33	af43

Table 3: DSCP Precedence

Precedence (low to high)	DSCP
0	Best Effort (be)
1	Class 1
2	Class 2
3	Class 3
4	Class 4
5	Express Forwarding (ef)

The DSCP level can be configured for multiple traffic patterns within a single instance of this command.

The no ip qos command can be issued to remove a QOS setting and return it to it's default setting.

Example

The following command configures the DSCP level for QCI to be Expedited Forwarding,**ef**:

```
ip qos-dscp qci 1 ef
```

ip source-violation

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected, or for verifying packet routing and labeling within the network.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDG Service Configuration

configure > context *context_name* **> pdg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdg-service)#
```

Syntax Description

```
ip source-violation { clear-on-valid-packet | drop-limit num period secs }
default ip source-violation { drop-limit num period secs }
no ip source-violation clear-on-valid-packet
```

clear-on-valid-packet

Configures the service to reset the drop-limit counters upon receipt of a properly addressed packet. Default: disabled

drop-limit *num*

Sets the maximum number of allowed IP source violations within the detection period before dropping a call. If *num* is not specified, the value is set to the default value.

num is an integer from 1 to 1000000. Default: 10

period *secs*

Sets the detection period (in seconds) for IP source violations as an integer from 1 through 1000000. If *secs* is not specified, the value is set to the default value. Default: 120

default ip source-violation { drop-limit *num* period *secs* }

Sets or restores the IP source violation detection defaults, as follows:

- **drop-limit**: Sets or restores the maximum number of IP source violations within the detection period before dropping the call to the default value of 10.
- **period**: Sets or restores the detection period for IP source violations to the default value of 120 seconds.

no ip source-violation clear-on-valid-packet

The drop-limit counters are not reset upon receipt of a properly addressed packet.

Usage Guidelines

Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

This function operates in the following manner: When a subscriber packet is received with a source IP address violation, the system increments the IP source violation drop-limit counter and starts the timer for the IP source violation period. Every subsequent packet received with a bad source address during the IP source violation period causes the drop-limit counter to increment. For example, if the drop-limit is set to 10, after 10 source violations, the call is dropped. The detection period timer continues to count throughout this process.

Example

The following command sets the drop limit to 15 and leaves the other values at their default values:

```
ip source-violation drop-limit 15
```

max-tunnels-per-ue

Specifies the maximum number of IKEv2/IPSec tunnels allowed per UE by the PDG/TTG. This maximum number is specified per PDG service.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDG Service Configuration

configure > context *context_name* **> pdg-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pdg-service)#`

Syntax Description

max-tunnels-per-ue *integer*
default max-tunnels-per-ue

integer

Specifies the maximum number of IKEv2/IPSec tunnels allowed per UE as an integer from 1 to 11. Default: 11

default max-tunnels-per-ue

Sets the maximum number of IKEv2/IPSec tunnels allowed per UE to its default value, which is 11.

Usage Guidelines

Use this command to set the maximum number of IKEv2/IPSec tunnels allowed per UE.

Example

Use the following command to set the maximum number of IKEv2/IPSec tunnels allowed per UE to *2*:

```
max-tunnels-per-ue 2
```

plmn id

Configures location specific mobile network identifiers used to help translate local emergency and service-related numbers. Default is disabled.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDG Service Configuration

configure > context *context_name* **> pdg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdg-service)#
```

Syntax Description

plmn id mcc *mcc_number* **mnc** *mnc_number*
no plmn id mcc *mcc_number* **mnc** *mnc_number*

mcc *mnc_number*

Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 200 through 999.

mnc *mnc_number*

Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 2-digit integer from 00 through 999.

no plmn id mcc *mcc_number* mnc *mnc_number*

Removes a previously configured PLMN identifier for the PDG service.

Usage Guidelines

The PLMN ID is included in the RAI (Routing Area Identity) field of the PDP Create Request messages sent to the GGSN. Multiple PDG services can be configured with the same PLMN identifier. Up to five PLMN IDs can be configured for each PDG service.

Example

The following command configures the PLMN identifier with an MCC of *462* and MNC of *2*:

```
plmn id mcc 462 mnc 02
```

setup-timeout

Specifies the maximum time allowed to set up a session.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDG Service Configuration

configure > context *context_name* **> pdg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdg-service)#
```

Syntax Description

setup-timeout *integer*
default setup-timeout

setup-timeout integer

Sets the session setup timeout value (in seconds) as an integer from 2 through 300. Default: 60

default setup-timeout

Sets or restores the default session setup timer value to 60 seconds.

Usage Guidelines

The PDG/TTG clears both the user session and tunnels if a call does not initiate successfully before the session setup timer expires.

Example

The following command sets the session setup timeout value to the default value of 60 seconds:

```
default setup-timeout
```