

PDSN Service Configuration Mode Commands

The PDSN Service Configuration Mode is used to create and manage PDSN service instances for the current context.

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pdsn-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.

- a11-signalling-packets, on page 3
- aaa 3gpp2-service-option, on page 3
- aaa nas-ip-address, on page 4
- access-flow traffic-validation, on page 5
- access-network, on page 6
- airlink bad-sequence-number, on page 7
- allow alt-ppp, on page 8
- always-on-indication, on page 8
- associate, on page 9
- authentication, on page 10
- bcmcs, on page 12
- bind, on page 13
- data-available-indicator, on page 15
- data-over-signaling, on page 15
- default subscriber, on page 16
- direct-lte-indicator, on page 17

- dormant-transition, on page 18
- enhanced-pcf-redirection, on page 18
- fragment, on page 19
- gre, on page 20
- inter-pdsn-handoff mobility-event-indicator, on page 22
- inter-pdsn-handover, on page 23
- ip header-compression rohc, on page 24
- ip local-port, on page 25
- ip source-violation, on page 26
- lifetime, on page 27
- max-retransmissions, on page 28
- mobile-ip foreign-agent context, on page 29
- mobile-ipv6, on page 30
- msid length, on page 31
- nai-construction, on page 32
- new-call conflict, on page 33
- pcf-monitor, on page 33
- pcf-session-id-change restart-ppp, on page 35
- pdsn type0-tft attempt-inner-match, on page 36
- peer-pcf, on page 37
- pma-capability-indicator, on page 38
- policy, on page 38
- ppp, on page 41
- qos-profile-id-mapping, on page 43
- qos update, on page 45
- radius accounting dropped-pkts, on page 46
- registration-accept, on page 47
- registration-ack-deny terminate-session-on-error, on page 47
- registration-deny, on page 48
- registration-discard, on page 50
- registration-update, on page 51
- retransmission-timeout, on page 53
- service-option, on page 54
- setup-timeout, on page 55
- simple-ip allow, on page 56
- spi, on page 57
- tft-validation wait-timeout, on page 59
- threshold a11-ppp-send-discard, on page 60
- threshold a11-rac-msg-discard, on page 61
- threshold a11-rrp-failure, on page 62
- threshold a11-rrq-msg-discard, on page 63
- threshold init-rrq-rcvd-rate, on page 64

a11-signalling-packets

Applies DSCP marking for IP header carrying outgoing A11-signalling packets.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

a11-signalling-packetsip-header-dscp *hexa_number*
[no | default] a11-signalling-packetsip-header-dscp

no

Disables the **a11-signalling-packets ip-header-dscp** option configuration.

default

Sets / Restores default value assigned for specified parameter **a11-signalling-packets ip-header-dscp**.

hexa_number

a Hexa decimal number between 0x0 and 0x3F.

Usage Guidelines

Use this command to configured value of DSCP to be set for all outgoing A11 signaling msg.

By default the CLI is disabled and DSCP is marked as 0 in ip-header.

Example

The following command configures value of DSCP to be set for all outgoing to A11 signaling message *0x3F*:

a11-signalling-packets ip-header-dscp *0x3F*

aaa 3gpp2-service-option

Specifies the value for the 3gpp2-service option.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
aaa 3gpp2-service-option number
no aaa 3gpp2-service-option
default aaa 3gpp2-service-option
```

no

Disables the aaa 3gpp2-service option configuration.

default

Sets / Restores default value assigned for specified parameter **aaa 3gpp2-service-option**.

number

Service option *number* is integer and should be between *0* to *32767*.

Usage Guidelines

Allows the configuration of a default service option value to be sent in accounting when service option values are not received from PCF. The PDSN will default the service option value to the configured value if the value is not specified by the PCF.

Example

The following command sets the service option to be *40*:

```
aaa 3gpp2-service-option 40
```

aaa nas-ip-address

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
aaa nas-ip-address IPv4 address
no aaa nas-ip-address
default aaa nas-ip-address
```

no

Disables the aaa nas-ip-address option configuration.

default

Sets / Restores default value assigned for specified parameter **aaa nas-ip-address** by default this is disabled.

ipv4 address

Specifies the IPv4 addresses to be used.

Usage Guidelines Allows the configuration.

Example

The following command configures *209.165.200.228*:

```
aaa as-ip-addres 209.165.200.228
```

access-flow traffic-validation

If **access-flow traffic-validation** is enabled for the service and the subscriber then the flows are checked against the filter rules. If the packets does not match the filter rules, and N violations occur in K seconds, the rp connection is downgraded to best-effort flow, if it is not already a best-effort flow.

Product PDSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
access-flow traffic-validation [ threshold { interval seconds | violations limit } ]
no access-flow traffic-validation
default access-flow traffic-validation [ threshold { interval | violations } ]
```

no

Disable traffic validation for the service.

default

Traffic validation configuration for the service is set to the default value.

threshold { [violations *limit*] [interval *seconds*] }

violations *limit*: Sets the parameters that determine traffic access violations. This is determined by setting the maximum number of violations within a set time period. must be an integer from *1* through *100000*.

interval *seconds* Sets the time interval, in seconds. must be an integer from *1* through *100000*.

Usage Guidelines Use this command to enable traffic validation for the current PDSN service.

Example

The following command enables traffic validation for the current PDSN service and sets the limit allowed to *100* **violations** within *5* seconds:

```
access-flow traffic-validation threshold violations 100 interval 5
```

access-network

Configures access network parameters.

Product PDSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
access-network { accounting identifier identifier_name | realm realm_name }
no access-network { accounting identifier | realm } }
```

no

Disables the **access-network**.

accounting identifier

Configures accounting for the access-network. This value must be a string from 1 to 128 characters in length.

realm *realm_name*

Configures the realm for the access-network. *realm_name* must be a string from 1 to 128 characters in length.

Usage Guidelines Use this command to configure access-network parameters for accounting and realms.

Example

The following command creates an **access-network realm** named *realm2*.

```
access-networkrealm realm2
```

airlink bad-sequence-number

Configures PDSN behavior for airlink related parameters.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

airlink bad-sequence-number { **accept** | **deny** [**use-deny-code** { **poorly-formed-request** | **unsupported-vendor-id**}]}
[**no** | **default**] **airlinkbad-sequence-number**

no

Disables the deny of bad-sequence number and accept it.

default

It is the default behavior.

accept

Accepts the A11 RRQ messages that have an Airlink Sequence number less than or equal to a previously received sequence number.

It is the default behavior.

deny

Rejects the A11 RRQ messages that have an Airlink Sequence number less than or equal to a previously received sequence number.

It uses **poorly-formed-request** option by default to deny a request.

use-deny-code { poorly-formed-request | unsupported-vendor-id }

These are optional keywords that used with **deny** sub-command to deny the A11 RRQ messages that have either an unsupported vendor Id or A11 Requests with bad/poor formation.

unsupported-vendor-id denies request on the basis of vendor Id.

poorly-formed-request will deny the A11 request on the basis of request formation or structure. It is the default deny code for **deny** sub-command.

Usage Guidelines

This command is used to configure the airlink parameters for A11 RRQs.

When configured it denies the A11 RRQ messages that have an Airlink Sequence number less than or equal to a previously received sequence number.

Example

The following command would configure the system to deny all A11 RRQ messages having unsupported vendor Id or bad structure of message, including those having airlink sequence number less than or equal to a previously received sequence number:

```
airlinkbad-sequence-number deny
```

allow alt-ppp

Allows proprietary modified versions of PPP type sessions to connect this PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
allowalt-ppp
no allow alt-ppp
default allow alt-ppp
```

no

Disables the allowed alternate PPP feature.

default

Sets the specified parameter to default.

Usage Guidelines

This command is used to deviate from standard PPP protocol and use a proprietary modified version of PPP with a pre-defined non-negotiable PPP parameters.

It is a vendor-specific licensed feature command.

Example

```
allow alt-ppp
```

always-on-indication

Enables/disables the inclusion of 3GPP2 Always On Indicators in messages to the PCF.

Product PDSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
always-on-indication
no always-on-indication
```

no

Disables the sending of 3GPP2 Always On Indication messages.

Usage Guidelines This command is available when the 3GPP2 Always-On RP Extensions feature-use license is installed.

When enabled, this command causes the PDSN service to include the Always On Indicators in the Normal Vendor Specific Extension (NVSE) part of an A11 Session Update message to the PCF. The indicator will only be sent for those subscriber sessions in which Always On functionality is enabled as determined after a successful authentication: the 3GPP2-Always-On attribute is set to a value of *1* (Active) for subscribers configured on a AAA server, or the always-on parameter is set for locally configured subscribers.

This functionality is enabled by default.

Example

Use the following command to Enables the inclusion of 3GPP2 Always On Indicators in messages to the PCF.

```
always-on-indication
```

associate

Associates a PDSN-service with a Quality of Service (QoS) policy.

Product PDSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
associate qci-qos-mapping string
no associate qci-qos-mapping
```

no

Disables the configuration to associate PDSN-serivce with qos policy.

qci-qos-mapping *string*

qci-qos-mapping configures QCI to QoS mapping for this PDSN service.

string a string of size 1 to 63.

Usage Guidelines The following is used for configuration to associate PDSN-serivce with qos policy.

Example

```
associate qci-qos-mapping sample
```

authentication

Configures authentication parameters for specific PDSN service.

Product PDSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
authentication { [ allow-noauth ] [ chap chap_priority ] [ mschap mschap_priority
 ] [ pap pap_priority  ] } | [  msid-auth  ]
default authentication
```

default

Configures authentication parameters for specific PDSN service.

allow-noauth

Default: Disabled

This option configures the system to provide subscribers with network access even though they have not been authenticated. This command issued by itself would cause the system to not attempt to authenticate subscribers.

When the allow-noauth option is used in conjunction with commands specifying other authentication protocols and priorities to use, then if attempts to use those protocols fail, the system will treat the allow-noauth option as the lowest priority.

If no authentication is allowed, then NAI construct will be implemented in order to provide accounting records for the subscriber.

chap *chap_priority*

Default: 1

This option configures the system to attempt to use the Challenge Handshake Authentication Protocol (CHAP) to authenticate the subscriber.

A *chap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.

chap_priority must be an integer from 1 through 1000. The lower the integer, the higher the preference. CHAP is enabled by default as the highest preference.

mschap *mschap_priority*

Default: Disabled

This option configures the system to attempt to use the Microsoft Challenge Handshake Authentication Protocol (MSCHAP) to authenticate the subscriber.

A *mschap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.

mschap_priority must be an integer from 1 through 1000. The lower the integer, the higher the preference.

pap *pap_priority*

Default: 2

This option configures the system to attempt to use the Password Authentication Protocol (PAP) to authenticate the subscriber.

A *pap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.

pap_priority must be an integer from 1 through 1000. The lower the integer, the higher the preference. PAP is enabled by default as the second highest preference.

msid-auth

Default: Disabled

This option configures the system to attempt to authenticate the subscriber based on their Mobile Station Identity (MSID).

Usage Guidelines

Use to specify how the PDSN service should handle authentication and what protocols to use. The flexibility is given to configure this option to accommodate the fact that not every mobile will implement the same authentication protocols.

The chassis is shipped from the factory with the authentication options set as follows:

- allow-noauth disabled
- chap enabled with a priority of 1
- mschap disabled
- msid-auth disabled
- pap enabled with a priority of 2

Important At least one of the keywords must be used to complete the command.

Example

The following command would configure the system to allow no authentication for subscribers and would perform accounting using the default NAI-construct of *username@domain*:

```
authentication allow-noauth
```

The following command would configure the system to attempt subscriber authentication first using CHAP, then MSCHAP, and finally PAP. If the allow-noauth command was also issued, if all attempts to authenticate the subscriber using these protocols fail, then the subscriber would be allowed access:

```
authentication chap 1 mschap 2 pap 3
```

bcmcs

Sets the BCMCS (Broadcast Multicast Service) group username and password for RADIUS access.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
bcmcs { customptt | encrypted grppasswd group_passwd | flow-id value
[flow-id-type { flow-id | program-id } ] | grppasswd group_password |
grpusrnamegroup_name | ptt { destination-context dest_name |
disconnect-dscp-label dscp_label | mtu transmission_unit | rohc-profile-name
rohc_profile_name } }
default bcmcs [ custom ptt | ptt { disconnect-dscp-label | mtu |
rohc-profile-name } ]
no bcmcs { custom ptt | flow-id value [flow-id-type { flow-id | program-id }
 | grppasswd | grpusrname | ptt { destination-context | disconnect-dscp-label
 | mtu | rohc-profile-name } }
```

custom

Customise the BCMCS configuration.

flow-id *value*

Set the BCMCS flow-id. This value must be a hex string between *0x1000* and *0xFFFFFFFF*.

Making this entry opens a new mode: bcmcs-flow-id.

rohc-profile name : Configure ROHC parameters name, name should be string of size *1* to *63*.

grpusrname *group_name*

Sets the BCMCS group name for RADIUS access requests. This value must be a string from *1* to *127* characters in length.

encrypted grppasswd *group_passwd*

Set the BCMCS group password for RADIUS access requests. This value must be a string from *1* to *63* characters in length.

Password can be encrypted or clear.

ptt { destination-context *dest_name* | disconnect-dscp-label *dscp_label*| mtu *transmission_unit* | rohc-profile-name *rohc_profile_name* }

destination-context: Specify the intended destination context name. This value must be string of *1* to *79* characters in length.

disconnect-dscp-label: Configures the DSCP label to be present in the In Call Signalling packet based on which In Call Signalling and Media Flows will be disconnected. This value must be a Hexadecimal number between *0x0* and *0xFF*.

mtu *transmission_unit*: Configures maximum transmission unit, This value must be ranging from *100* to *2000*. Default is *1500*.

rohc_profile_name *rohc_profile_name*: Profile name of the ROHC compressor and decompressor. This value should be a string of *1* to *63*.

Usage Guidelines

Use this command to set the BCMCS group username and password for RADIUS access requests.

Example

```
bcmcsgrpusername group_name
bcmcsgrppasswd group_password
```

bind

Binds the PDSN service to a logical IP interface serving as the R-P interface. Specifies the maximum number of subscribers that can access this service over the interface.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

bind address *address* [**max-subscribers** *count*]
no bind address

no

Removes a previously configured binding.

address

Specifies the IP address (address) of the interface configured as the R-P interface. *address* is specified in dotted decimal notation.

max-subscribers *count*

Default: *500000*

Specifies the maximum number of subscribers that can access this service on this interface.

count can be configured to any integer value between *0* and *2500000*.



Important The maximum number of subscribers supported is dependant on the license key and the number of active PACs/PSCs installed in the system. A fully loaded system with *13* active PACs/PSCs can support *2500000* total subscribers. Refer to the license key command for additional information.

Usage Guidelines

Associate or tie the PDSN service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an R-P interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.

When configuring the **max-subscribers** option, be sure to consider the following:

- The total number of interfaces that you will configure for use as R-P interfaces
- The maximum number of subscriber sessions that all of the interfaces may handle during peak busy hours
- The average bandwidth for each of the sessions
- The type of physical port (10/100Base-Tx or 1000Base-T) to which these interfaces will be bound

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

Example

The following command would bind the logical IP interface with the address of *192.168.3.1* to the PDSN service and specifies that a maximum of *600* simultaneous subscriber sessions can be facilitated by the interface/service at any given time.

```
bind address 192.168.3.1 max-subscribers 600
```

The following command disables a binding that was previously configured:

```
no bind  address
```

data-available-indicator

Enables sending Data Available Indicator extension in R-P Registration Reply.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no | default] data-available-indicator

no

Default: Disabled

Disable the sending of the Data Available Indicator extension in R-P Registration Reply.

default

Sets / Restores default value assigned for specified parameter for **data-available-indicator**.

Usage Guidelines

Use this command to enable or disable the sending of the Data Available Indicator extension in R-P Registration Reply

Example

Use the following command to enable sending the Data Available Indicator extension in R-P Registration Reply:

```
data-available-indicator
```

Use the following command to disable sending the Data Available Indicator extension in R-P Registration Reply:

```
no data-available-indicator
```

data-over-signaling

Enables the data-over-signaling marking feature for A10 packets.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no | default] data-over signaling

default

Sets / Restores default value assigned for specified parameter for **data-over signaling**

no

Default: Enabled

Disable the data-over signaling feature for A10 packets.

Usage Guidelines

Use this command to enable or disable the data-over signaling feature for A10 packets.



Important This is a customer-specific command.

Example

no data-over-signaling

default subscriber

Specifies the name of a subscriber profile configured within the same context as the PDSN service from which to base the handling of all other subscriber sessions handled by the PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

default subscriber *profile_name*
no default subscriber

no

Enables/Disables the option **default subscriber** *profile_name*

profile_name

Specifies the name of the configured subscriber profile. *profile_name* can be between *1* and *127* alpha and/or number characters and is case sensitive.

Usage Guidelines

Each subscriber profile specifies "rules" such as permissions, PPP settings, and timeout values.

By default, the PDSN service will use the information configured for the subscriber named default within the same context. This command allows for multiple PDSN services within the same context to apply different "rules" to sessions they process. Each set of rules can be configured under a different subscriber name which is pointed to by this command.

Use the **no default subscriber** *profile_name* command to delete the configured default subscriber.

Example

To configure the PDSN service to apply the rules configured for a subscriber named *user1* to every other subscriber session it processes, enter the following command:

```
default subscriber user1
```

direct-lte-indicator

Enables sending Direct LTE Indicator VSA in Access Request.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no | default ] direct-lte-indicator
```

default

Sets / Restores default value assigned for specified parameter for **data-over signaling**

no

Default: Enabled

Disables sending Direct LTE Indicator VSA in Access Request.

Usage Guidelines

Use this command to enable or disable sending Direct LTE Indicator VSA in Access Request.



Important This is a customer-specific command.

Example

```
no direct-lte-indicator
```

dormant-transition

Configures the PDSN behavior to terminate A10 session, when the PDSN receives the A11-RRQ (Type 4) before the session for the original MN is established completely.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no | default ] dormant-transition initial-session-setup
```

no

Terminates the A10 session, when PDSN receives the A11-RRQ (Type 4) before the original session established completely.

default

Keeps the A10 session live in case of A11-RRQ (Type 4) is received before the original session is established completely.

Usage Guidelines

When the status of A10 session goes to dormant before the session for the original MN is established completely, the different MN may possibly send the A11-RRQ (Type 4) to the PDSN and PPP renegotiation may start.

This command is used to terminate the A10 session when the PDSN receives the A11-RRQ (Type 4) before the session for original MN is established completely.

Example

Following command is used to release the A10 session in case of receiving A11-RRQ (Type 4) before the original session is established completely:

```
no dormant-transition  initial-session-setup
```

enhanced-pcf-redirection

Enables or disables PDSN support for enhanced PCF redirection.

Product PDSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description **`[no] enhanced-pcf-redirection`**

no

Disables PDSN support for enhanced PCF redirection.

enhanced-pcf-redirection

Enables PDSN support for enhanced PCF redirection.

Usage Guidelines Use this command to enable or disable PDSN support for enhanced PCF redirection. By default, this feature is disabled.



Important This is a customer-specific command.

Example

The following command will disable PDSN support for enhanced PCF redirection.

```
no enhanced-pcf-redirection
```

fragment

Enables or disables PPP payload fragmentation.

Product PDSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description **`[ no | default ] fragment ppp-data`**

no

Disables the fragmentation of ppp data.

default

Default enables ppp data fragmentation.

Usage Guidelines

This command is to indicate to the RP module to NOT fragment PPP payloads being sent to the PCF, if the total packet size (PPP+GRE+IP) exceeds *1500* bytes.

Disabling fragmentation may cause the **sessmgr** to perform outer IP fragmentation of the outgoing packet, if the resulting packet exceeds the MED MTU.

Example

The following command enables PPP payload fragmentation.

```
fragment ppp-data
```

gre

Configures Generic Routing Encapsulation (GRE) parameters for the A10 protocol within the PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gre { checksum | checksum-verify  | ip-header-dscp value { all-control-packets
 | setup-packets-only } | protocol-type {any | byte-stream | ppp } |
reorder-timeout value | segmentation |sequence-mode { none | reorder } |
sequence-numbers | threegppp2-ext-header qos-marking }
no gre { checksum | checksum-verify | ip-header-dscp | segmentation |
sequence-numbers | threegppp2-ext-headers qos-marking }
default gre { checksum | checksum-verify | ip-header-dscp | protocol-type |
 reorder-timeout | segmentation | sequence-mode | sequence-numbers |
threegppp2-ext-headers qos-marking }
```

no

Disables the specified functionality.

default

Restores the specified parameter to its default setting.

checksum

Default: disabled

Enables the introduction of the checksum field in outgoing GRE packets.

checksum-verify

Default: disabled

Enables verification of the GRE checksum (if present) in incoming GRE packets.

ip-header-dscp *value* { all-control-packets | setup-packets-only }

Default: Disabled

Used to configure the QoS Differentiated Services Code Point (DSCP) marking for GRE packets.

- *value* : Represents the DSCP setting. It represents the first six most-significant bits of the ToS field. It can be configured to any hex value from 0x0 through 0x3F.
- **all-control-packets** : Dictates that the DSCP marking is to be provided in all GRE control packets.
- **setup-packets-only** : Dictates that the DSCP marking is to be provided only in GRE setup packets.

protocol-type { any | byte-stream | ppp }

Specifies the protocol used fro GRE encapsulation that is acceptable to

any: Specifies that the PDSN service will accept GRE packets encapsulated using any protocol.

byte-stream: Specifies that the PDSN service will accept GRE packets only encapsulated using byte stream. Using byte stream encapsulation, PPP packets are framed at different intervals and sent.

ppp: Specifies that the PDSN service will accept GRE packets only encapsulated using the Point-to-Point Protocol (PPP). Using PPP encapsulation, PPP packets are framed at regular intervals and sent.

reorder-timeout

Default: *100*

Configures max number of milliseconds to wait before processing reordered out-of-sequence GRE packets. *milliseconds* must be an integer from *0* through *5000*.

segmentation

Default: disabled

Enables GRE Segmentation for the PDSN service.

sequence-mode { none | reorder }

Default: none

Configures handling of incoming out-of-sequence GRE packets.

none: Specifies that sequence numbers in packets are ignored and all arriving packets are processed in the order they arrive.

reorder: Specifies that out of sequence packets are stored in a sequencing queue until one of the conditions is met:

- The reorder timeout occurs: All queued packets are sent for processing and the accepted sequence number is updated to the highest number in the queue.
- The queue is full (five packets): All packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number in the queue.
- An arriving packet has a sequence number such that the difference between this and the packet at the head of the queue is greater than five. All the packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number that arrived.
- A packet arrives that fills a gap in the sequenced numbers stored in the queue and creates a subset of packets whose sequence numbers are continuous with the current accepted sequence number. This subset of packets in the queue is sent for processing. The reorder timer continues to run and the accepted sequence number is updated to the highest number in the subset delivered.

sequence-numbers

Enables insertion of GRE sequence numbers in data that is about to be transmitted over the A10 interface. Data coming into the system containing sequence numbers but that is out of sequence is not re-sequenced.

threegppp2-ext-headers qos-marking

When threegppp2-ext-headers qos-marking is enabled and the PCF negotiates capability in the A11 RRQ, the PDSN will include the qos optional data attribute in the GRE 3gpp2 extension header.

The **no** keyword, enables qos-marking in the gre header based on the tos value in the header.

Usage Guidelines

The **gre protocol-type** command can be used to prevent the PDSN service from servicing PCFs that use a specific form of encapsulation.

Use the **no gre sequence-numbers** command to disable the inclusion of GRE sequence numbers in the A10 data path.

The chassis is shipped from the factory with the authentication options set as follows:

- **protocol-type any**
- sequence-numbers enabled

Example

Use this command to configure the PDSN service to exclude byte stream encapsulated GRE traffic:

```
gre protocol-type ppp
```

inter-pdsn-handoff mobility-event-indicator

Configures the PDSN to support the Mobility Event Identifier (MEI) during inter-PDSN handoffs. The presence of the Mobility Event Indicator (MEI) and Access Network Identifier (ANID) elements in a A11 handoff request represents an Inter-PDSN handoff.

Product PDSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
inter-pdsn-handoff mobility-event-indicator
no inter-pdsn-handoff mobility-event-indicator
default inter-pdsn-handoff mobility-event-indicator
```

no

Disables support for the MEI during inter-PDSN handoffs.

default

Sets / Restores default value assigned for **inter-pdsn-handoff mobility-event-indicator**. By default it is disabled.

Usage Guidelines Use this command to configure support for the MEI during inter-PDSN handoffs.

Example

Use the following command to enable support for the MEI during inter-PDSN handoffs

```
inter-pdsn-handoff  mobility-event-indicator
```

inter-pdsn-handover

Configures Inter-PDSN handoff related parameters.

Product PDSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
inter-pdsn-handover use-canid-panid
no inter-pdsn-handover use-canid-panid
default inter-pdsn-handover use-canid-panid
```

no

Disables support for the MEI during inter-PDSN handoffs parameters.

default

Sets / Restores default value assigned for **inter-pdsn-handoff mobility-event-indicator**. By default it is disabled.

Usage Guidelines

Use this command to configure Inter-PDSN handoff related parameters.

Example

Use the following command to econfigure Inter-PDSN handoff related parameters.

```
inter-pdsn-handover use-canid-panid
```

ip header-compression rohc

Enters PDSN Service ROHC Configuration Mode and allows you to configure ROHC parameters that the PDSN conveys to the PCF in the initial A11 RRP message before PPP authentication.

By default, ROHC is disabled for a PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ipheader-compression rohc
default ipheader-compression rohc
no ipheader-compression rohc
```

default

Sets all PDSN Service ROHC Configuration Mode values back to the defaults and disable ROHC for this PDSN service.

no

Disable IP header compression for this PDSN Service.

Usage Guidelines

Use this command to enter the PDSN Service ROHC Configuration Mode or disable ROHC for the current PDSN service.

Example

The following command disables ROHC for the current PDSN service and sets all of the values for commands in PDSN Service ROHC Configuration Mode back to their default settings:

```
no ip header-compression rohc
```

ip local-port

Configures the local User Datagram Protocol (UDP) port for the R-P interfaces' IP socket.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

ip local-port *number*
default ip local-port

number

Default: *699*

Specifies the UDP port number.

number can be any integer value between *1* and *65535*.

default

Designates UDP port, default value as *699*.

Usage Guidelines

Specify the UDP port that should be used for communications between the Packet Control Function (PCF) and the PDSN.



Important The UDP port setting on the PCF must match the local-port setting for the PDSN service on the system in order for the two devices to communicate.

Example

Use the following command to specify a UDP port of *3950* for the PDSN service to use to communicate with the PCF on the R-P interface:

```
iplocal-port 3950
```

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.

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.

Product

PDSN

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

no

Enables/Disables **ip source-violation clear-on-valid-packet**.

default

Configure default settings related to **ip source-violation**.

clear-on-valid-packet

Default: disabled

Configures the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet.

drop-limit *num*

Default: *10*

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

num can be any integer value from *1* to *1000000*.

period *secs*

Default: *120*

The length of time, in seconds, for a source violation detection period to last. drop-limit and reneg-limit counters are decremented each time this value is reached.

The counters are decremented in this manner: reneg-limit counter is reduced by one (1) each time the period value is reached until the counter is zero (0); drop-limit counter is halved each time the period value is reached until the counter is zero (0). If *secs* is not specified, the value is set to the default.

secs can be any integer value from *1* to *1000000*.

reneg-limit *num*

Default: *5*

Sets the number of allowed source violations within a detection period before forcing a PPP renegotiation. If *num* is not specified, the value is set to the default.

num can be any integer value from *1* to *1000000*.

Usage Guidelines

This function is intended to allow the operator to configure a network to prevent problems such as when a user gets handed back and forth between two PDIFs PDSNs a number of times during a handoff scenario.

This function operates in the following manner:

When a subscriber packet is received with a source address violation, the system increments both the IP source-violation reneg-limit and drop-limit counters 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 reneg-limit and drop-limit counters to increment.

For example, if reneg-limit is set to 5, then the system allows 5 packets with a bad source address (source violations), but on the 5th packet, it re-negotiates PPP.

If the drop-limit is set to *10*, the above process of receiving *5* source violations and renegotiating PPP occurs only once. After the second *5* source violations, the call is dropped. The period timer continues to count throughout this process.

If the configured source-violation period is exceeded at any time before the call is dropped, the reneg-limit counter is checked. If the reneg-limit counter is greater than zero (0), the reneg-limit is decremented by *1*. If the reneg-limit counter equals zero, the drop-limit is decremented by half.

Example

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

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

lifetime

Specifies the time that an A10 connection can exist before its registration is considered expired.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

lifetime *time*
no lifetime
default lifetime

no lifetime

Specifies that an A10 connection can exist for an infinite amount of time.

default lifetime

Sets / Restores default value assigned for **lifetime** as 1800.

time

Default: 1800

Specifies the time that an A10 connection can exist before its registration is considered expired.

time is measured in seconds and can be configured to any integer value between *1* and *65534*.

Usage Guidelines

Set a limit to the amount of time that a subscriber session can remain up whether or not the session is active or dormant. If the lifetime timer expires before the subscriber terminates the session, their connection will be terminated automatically.

Use the **no lifetime** command to delete a previously configured lifetime setting. If after deleting the lifetime setting you desire to return the lifetime parameter to its default setting, use the **default lifetime** command.

Example

The following command specifies a time of *3600* seconds (1 hour) for subscriber sessions on this PDSN service:

```
lifetime 3600
```

max-retransmissions

Configures the maximum number of times the PDSN service will attempt to communicate with a PCF before it marks it as unreachable.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

max-retransmissions *count*
default max-retransmissions

default

Sets / Restores default value assigned for **max-retransmissions** as *5*.

count

Specifies the maximum number of times the PDSN service will attempt to communicate with a PCF before it marks it as unreachable.

count can be configured to any integer value between *1* and *1,000,000*.

Usage Guidelines

If the value configured for the max-retransmissions is reached the call will be dropped.

The chassis is shipped from the factory with the Internet maximum number of retransmissions set to *5*.

Example

The following command configures the maximum number of retransmissions for the PDSN service to *3*:

```
max-retransmissions 3
```

mobile-ip foreign-agent context

For Mobile IP support, specifies the context in which the FA service(s) are configured.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

mobile-ip foreign-agent context *context_name* [**fa-service** *name*]
no mobile-ip foreign-agent context

no

Enables/Disables **mobile-ip foreign-agent context**

context_name

Specifies the name of the previously configured context that facilitates the FA service(s).

context_name must be between *1* and *79* alpha or numeric characters and is case sensitive.

fa-service *name*

This optional keyword allows you to link the PDSN service to a particular FA service in the specified context. *name* is the name of the FA service to link to. *name* is a string of size *1* to *63*

Usage Guidelines

FA services on the system can be configured either in the same or different contexts from those facilitating PDSN services. When they are configured in separate contexts, this command configured with a PDSN service instructs the PDSN service to route traffic to the context facilitating the FA service.

Use the **no mobile-ip foreign-agent context** to delete a previously configured destination context.

Example

The following command instructs the PDSN service to use the context named FA-destination for FA functionality:

mobile-ip foreign-agent context *fa-destination*

mobile-ipv6

Configures Mobile IPv6 parameters within specific PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

mobile-ipv6 mobile-access-gateway context *context_name* [**mag-service** *name*]

mobile-access-gateway

Configures Mobile Access Gateway (MAG) parameters within specific PDSN service.

context *context_name*

Designates name of the context in which the MAG service is configured. Must be followed by context name of MAG service.

context_name is a string of size 1 to 79.

mag-service *name*

Designates name of the MAG service in that context. Must be followed by MAG service name.

name is a string of size 1 to 63.

Usage Guidelines This command is used to configure Mobile IPv6 parameters and Mobile Access Gateway (MAG) parameters within specific PDSN service.

Example

The following command configures Mobile IPv6 parameters and Mobile Access Gateway (MAG) parameters within specific PDSN service.

mobile-ipv6 mobile-access-gateway context *pdsn1* **mag-service** *serv1*

msid length

Configures checking the length of the A11 MSID in A11 Session Specific Extn and airlink records.

Product PDSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

msid length { [**min** *min_length*] | **max** *max_length* }
default msid length

default

Specifies the default length of MSID (*10* to *15*) as per standard. By default **msid** is disabled.

min *min_length*

Specifies the minimum length for MSID.

min_length is any Integer value between *10* to *15*, but should be less than *max_length* specified with **max**. Default is *10*.

max *max_length*

Specifies the maximum length for MSID.

max_length is any Integer value between *10* to *15*, but should be more than *min_length* specified with **min**. Default is *15*.

Usage Guidelines MSID length can be configured either in the standard length or different customized length form. This command is used to specify the allowed length of MSID.

Example

The following command specifies an MSID length between *12* and *15*:

```
msid length min 12 max 15
```

nai-construction

Specifies a domain alias that will be used to represent the context which the PDSN service should use for AAA functionality.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
nai-construction domain alias
no nai-construction domain
```

domain *alias*

Alias represents the "domain" name that you would like to associate with the context in which AAA functionality is configured. alias can be between *1* and *79* alpha and/or numeric characters and is case-sensitive.

Usage Guidelines

Enabling NAI will be constructed for the subscriber in the event that their mobile station (MS) does not negotiate CHAP, PAP, or MSCHAP. If this option is selected, no further attempts will be made to authenticate the user. Instead, the constructed NAI will be used for accounting purposes.

The context specified by this command would be used to provide the communication with the RADIUS accounting server.

Use the **no nai-constructed** domain command to deleted a configured alias.



Important This command should only be used if the PDSN service is configured to allow no authentication using the authentication allow-noauth command.

Additionally, the **aaa constructed-nai** command in the Context Configuration mode can be used to configure a password for constructed NAIs.

Example

The following command configured a domain alias of aaa_context for the PDSN service to use when an NAI is constructed for a subscriber session:

```
nai-construction domain aaa_context
```

new-call conflict

Enable or disable to send A11-RUPD to current PCF, when system receives the A11-RRQ(Type1) from new PCF during the session exists.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no | default] new-call conflict terminate-session-old-pcf

no

Disable to send A11-RUPD to current PCF, when system receives the A11-RRQ(Type1) from new PCF during the session exists.

default

Enable to send A11-RUPD to current PCF, when system receives the A11-RRQ(Type1) from new PCF during the session exists.

Usage Guidelines

This configuration supports to enable or disable to send A11-RUPD to current PCF, when the system receives the A11-RRQ(Type1) from new PCF during the session exists.

If the configuration is **no new-call conflict terminate-session-old-pcf** system will not send registration update to old PCF on receiving a new call (A11-RRQ(Type1)) request for an existing active/dormant session. The default behavior is to send registration updates.

Example

The following command configured a system to send a registration update on receiving an A11-RRQ (Type 1) request for an existing active/dormant session:

```
new-call conflict terminate-session-old-pcf
```

pcf-monitor

Enables the monitoring of all the PCFs that have sessions associated with it. The PDSN stops monitoring a PCF if it is determined to be down. Once a PCF is determined to be down, the PDSN tears down all sessions that correspond to the PCF and generates AAA Accounting Stop messages. All the PCFs that are connected to the PDSN service are monitored.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
pcf-monitor[ interval seconds | max-inactivity-time seconds | num-retry num |
timeout seconds ]
 [ no | default ] pcf-monitor
```

pcf-monitor

Entering the command with no keywords enables the PCF monitoring function with all parameters set to the defaults.

no

Disables the pcf monitoring function.

default

Sets / Restores default value assigned for **pcf-monitor**.

interval *seconds*

Default: 60 seconds

Sets the amount of time to wait between ping request messages.

seconds must be an integer in the range from 1 through 3600.

max-inactivity-time *seconds*

Default: 120 seconds

The maximum amount of time (seconds) with no A10 traffic from a PCF before the ICMP-ping mechanism is triggered.

seconds must be an integer from 1 through 3600.

num-retry *num*

Default: 5

Sets the number of times that the PDSN retries to ping the PCF. When num-retry for a given PCF has been exhausted with no response, sessions that correspond to the non-responsive PCF are terminated and Accounting Stop records for each terminated session are generated.

num must be an integer in the range from 0 through 100.

timeout *seconds*

Default: 3 seconds

The amount of time to wait for a response before retrying.

seconds must be in the range from 1 through 10.

Usage Guidelines

Use this command to enable the PDSN service to monitor the PCFs that have sessions associated with the PDSN service.

Example

The following command enables PCF monitoring with parameters set to the defaults:

```
pcf-monitor
```

The following command enables PCF monitoring and sets the timeout to *10* seconds:

```
pcf-monitor timeout 10
```

The following command disables pcf-monitoring:

```
no pcf-monitor
```

pcf-session-id-change restart-ppp

Manages current session and PPP renegotiation on GRE-key change without any change in PCF/PANID/CANID. This command disables or enables the PPP renegotiation restart on receiving an RP registration request from the current PCF with GRE key (PCF session Id) change. With this command the PDSN aborts and restarts the call causing PPP renegotiation.

This is enabled by default.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no | default ] pcf-session-id-change restart-ppp
```

no

Disables the pcf-session-id-change restart-ppp function.

With this option PDSN does not restart the PPP renegotiation on GRE key change from current PCF in an RP registration request, unless it indicates change in PCF/PANID/CANID.

default

Set the pcf-session-id-change function to the default state on enabled.

Usage Guidelines

GRE key (PCF session ID) is sued to identify the data packet for a session and is negotiated through the A11 signaling messages between PCF and PDSN. By default PDSN aborts and restart the PPP renegotiation on receipt of any RP registration request with change in GRE key or PCF session Id.

With use of no pcf-session-id-change restart-ppp command PDSN is configured to disable the restart of call or PPP renegotiation on receipt of any RP registration request with changed GRE key, unless it has any PCF/ANID/CANID change. PDSN silently switches the GRE key for the session, retaining the existing PPP session.

Example

The following command disables the PPP renegotiation restart action on receipt of any RP RRQ with changed GRE key from same PCF/PANID/CANID.

```
no pcf-session-id-change restart-ppp
```

pdsn type0-tft attempt-inner-match

Configures a type0 traffic flow template (tft) to a type1 traffic flow template.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no | default] pdsn type0-tft attempt-inner-match

no

Disables **pdsn type0-tft attempt-inner-match**.

default

Sets / Restores default value assigned for **pdsn type0-tft attempt-inner-match.**

Usage Guidelines

This CLI is used make PDSN match inner IP packets for an AIMS call. When enabled, the PDSN tries to match a type-0 tft to match both outer and inner packet, so that MN can use a Type-0 filter for HoA traffic which are tunneled.

This is disabled by default.

Example

The following command enables type0 tft:

```
pdsn type0-tft attempt-inner-match
```

peer-pcf

Configures settings for any PCF that has a connection with this PDSN.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

peer-pcf { *ip_address* | *ip_address/mask* } **bcmcs-framing** { **hdlc-like** | **segment-based** }

ip_address* | *ip_address/mask

ip_address must be specified using the standard IPv4 dotted decimal notation or colon notation for IPv6.

ip_address/mask must be specified using the standard IPv4 dotted decimal notation or colon notation for IPv6, followed by the mask.

bcmcs_framing { hdlc-like | segment-based }

Specifies the type of bcmcs_framing to use for this PCF connection.

- hdlc-like: applies HDLC-like framing for all BCMCS flows
- segment-based: applies segment-based framing for all BCMCS flows

Usage Guidelines

Use this command to configure the settings for any PCF that is connected to this PDSN. You can also specify bcmcs framing settings to use for the connection.

Example

The following command configures the peer-pcf for an IP address of *131.2.3.4*:

```
peer-pcf 131.2.3.4
```

pma-capability-indicator

Enables sending PMIP Capability Indicator VSA in Access Request.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
pma-capability-indicator [ 3gpp2 ]
[ no | default ] pma-capability-indicator
```

3gpp2

Use 3GPP2 defined VSA. Default is to use Custom1 VSA.

no

Enables/Disables sending PMIP Capability Indicator VSA in Access Request.

default

Sets / Restores default value assigned for PMIP Capability Indicator.

Usage Guidelines

Use this command to enable sending PMIP Capability Indicator VSA in Access Request.

Example

The following command enables sending PMIP Capability Indicator using 3GPP2 defined VSA in Access Request.

```
pma-capability-indicator 3gpp2
```

policy

Configures PDSN service policies.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

policy msid-match *msid_with_wildcards* **redirect** *address* [**weight** *weight_num*] [*address2* [**weight** *weight_num*]... *address16* [**weight** *weight_num*]] [**weight** *weight_num*]

no policy msid-match *msid_with_wildcards*

policy overload { **redirect** *address* [**weight** *weight_num*] [*address2* [**weight** *weight_num*] ... *address16* [**weight** *weight_num*]] | **reject** [**use-reject-code** { **admin-prohibited** | **insufficient-resources** }] }

no policy overload [**redirect** *address* [*address2* ... *address16*]]

default policy overload

policy pcf-zone-match *zone_number* **redirect** *address* [**weight** *weight_num*] [*address2* [**weight** *weight_num*] ... *address16* [**weight** *weight_num*]] | **restricted** [**redirect** *address* [**weight** *weight_num*] [*address2* [**weight** *weight_num*] ... *address16* [**weight** *weight_num*]]

no policy pcf-zone-match*zone_number*

[**default** | **no**] **policy rrq mei-from-current-pcf suppress-ppp-restart**

policy service-option enforce

[**default** | **no**] **policy service-option**

policy unknown-cvse enforce

[**default** | **no**] **policy unknown-cvse**

no

Enables/Disables the PDSN service policies.

default

Sets / Restores default value assigned for specified PDSN service policies.

policy msid-match *msid_with_wildcards* redirect *address* [weight *weight_num*] [*address2* [weight *weight_num*]... *address16* [weight *weight_num*]] [weight *weight_num*]

Specifies how a PDSN service should handle an incoming call that matches a list of wildcard MSIDs.

msid_with_wildcards: An MSID in which up to 16 digits have been replaced with the wildcard '$'. This defines the list of possible matches for incoming calls.

redirect: This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the PDSN service rejects new sessions with an A11 Registration Reply Code of 88H (unknown PDSN address) and provides the IP address of an alternate PDSN. This command can be issued multiple times.

address: The IP address of an alternate PDSN expressed in IP v4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

weight *weight_num*: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. *weight_num* must be an integer from 1 through 10.

policy overload { redirect *address* [weight *weight_num*] [*address2* [weight *weight_num*] ... *address16* [weight *weight_num*]] | reject [use-reject-code { admin-prohibited | insufficient-resources }] }

Specifies how a PDSN service should handle an overload condition.

redirect: This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the PDSN service rejects new sessions with an A11 Registration Reply Code of 88H (unknown PDSN address) and provides the IP address of an alternate PDSN. This command can be issued multiple times.

address: The IP address of an alternate PDSN expressed in IP v4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

weight *weight_num*: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. *weight_num* must be an integer from 1 through 10.

reject: This option will cause any overload traffic to be rejected. The PDSN will send an A11 Registration Reply Code of 82H (insufficient resources).

use-reject-codeadmin-prohibited: When this keyword is specified and traffic is rejected, the error code admin prohibited is returned instead of the error code insufficient resources. This is the default behavior.

use-reject-codeinsufficient-resources: When this keyword is specified and traffic is rejected, the error code insufficient resources is returned instead of the error code admin prohibited.

policy pcf-zone-match *zone_number* redirect *address* [weight *weight_num*] [*address2* [weight*weight_num*] ... *address16* [weight *weight_num*]] | restricted [redirect *address* [weight *weight_num*] [*address2* [weight *weight_num*] ... *address16* [weight *weight_num*]]]

Specifies how a PDSN service should handle an incoming call that matches a predefined zone number.

zone_number: An integer between 1 and 32 that defines the zone incoming calls must match for redirection.

redirect: This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the PDSN service rejects new sessions with an A11 Registration Reply Code of 88H (unknown PDSN address) and provides the IP address of an alternate PDSN. This command can be issued multiple times.

address: The IP address of an alternate PDSN expressed in IP v4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

weight *weight_num*: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. *weight_num* must be an integer from 1 through 10.

restricted: This is an optional keyword which means the zone is restricted. Restricted zone is meaningful only if enhanced PCF redirection feature is enabled, otherwise the zone follows the default behavior.

policy rrq mei-from-current-pcf suppress-ppp-restart

rrq configures policy for PPP restart after getting mei in rrq.

mei-from-current-pcf mei is received in rrq from current pcf.

suppress-ppp-restart suppresses ppp restart when mei is received in rrq from current pcf

policy service-option enforce

service-option configures R-P service-option to use for specific PDSN service. Must be followed by valid service-option number, ranging from 0 to 1000.

enforce designates enforcement of R-P service-option number.

policy unknown-cvse enforce

unknown-cvse configures PDSN service unknown cvse policy.

enforce enforces unknown cvse policy where unknown CVSEs in RRQs will cause Deny

Usage Guidelines

Policies can be implemented to dictate PDSN service behavior for various conditions such as overloading.

The system invokes the overload policy if the number of calls currently being processed exceeds the licensed limit for the maximum number of sessions supported by the system.

The system automatically invokes the overload policy when an on-line software upgrade is started.

Use the **no policy** { **overload** | **service-option** } command to delete a previously configured policy. If after deleting the policy setting you desire to return the policy parameter to its default setting, use the **default policy** command.

The chassis is shipped from the factory with the policy options set as follows:

- overload disabled
- sequence-numbers enforced enabled



Caution Incorrect configuration of the **policy msid-match** and **policy pcf-zone-match** keywords could result in sessions failing to be established. For example, if PDSN1 is configured to redirect sessions to PDSN2 while PDSN2 is configured to redirect sessions to PDSN1, a loop is created in which all sessions would fail to be connected. In addition, sessions will not be established if the PDSN to which the sessions are being redirected is unavailable.

Example

The following command configures the PDSN service to redirect traffic to two different destinations with weights of *1* and *10* respectively:

```
policy overload redirect 192.168.1.100 weight 1 192.168.1.200 weight 10
```

ppp

Sets PPP tunneling parameters for subscribers in the current PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ppp { tunnel-context context_name | tunnel-type { l2tp | none } }
[ no | default ] ppp tunnel-type
```

no

Enables/Disables the PPP tunneling parameters for subscribers in the current PDSN service.

default

Sets / Restores default value assigned for PPP tunneling parameters for subscribers in the current PDSN service.

tunnel-context *context_name*

The name of the context that has a LAC service configured to handle all tunnels from this PDSN service.

tunnel-type { l2tp |none }

l2tp: Force all subscriber sessions in this PDSN service to use L2TP tunneling.

none: Do not force L2TP tunneling. This is the default.



Important If the context specified by the **ppp tunnel-context** *context_name* command does not have a LAC service configured and **tunnel-type** is set to **l2tp** or the call is rejected.



Important If the PPP tunnel context has not been set or has been cleared with the **no ppp tunnel-context** command and **tunnel-type** is set to **l2tp**, the context where the current PDSN service resides is used. If that context does not have a LAC service configured the call is rejected.

Usage Guidelines

Use this command to enable or disable forced L2TP tunneling for all subscribers using this PDSN service. Also use this command to define which context defines the L2TP tunneling parameters.

Example

To set the tunnel context to the context named *context1* and enable forced L2TP tunneling, use the following commands;

```
ppp tunnel-context context1
ppp tunnel-type l2tp
```

To enable forced L2TP tunneling with IPSEC security, use the following commands;

```
ppp tunnel-type l2tp-secure
```

To disable forced tunneling, use the following command;

```
ppp tunnel-type none
```

To clear the setting for the tunnel context, use the following command;

```
no ppp tunnel-context
```

qos-profile-id-mapping

Creates the customized QoS profile identifier to QoS mapping for IMS authorization support.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
qos-profile-id-mapping profile-idid_num { [ description desc ] | [ downlink-bw
 dl_bw] | [ drop-rate drop_percentage ] | [ latency latency_duration ] | [ qos-class
 { class-A | class-B | class-C | class-D | class-E | calss-F } ] | [
uplink-bwul_bw ] } +
[ default | no ] qos-profile-id-mappingprofile-id id_num
```

default

Configures the specified QoS profile ID for QoS mapping with default values in this PDSN service.

no

Removes the configured QoS profile ID mapping in this PDSN service.

profile-id *id_num*

Specifies the profile identifier for QoS parameters to be used as the customized profile ID or modifies the QoS parameters in a profile ID (*id_num*) coming from RAN.

id_num must be an integer between 0 and 65535.

description *desc*

Specifies the user defined description for profile identifier.

desc must be an alpha and/or numeric string between 1 and 32 characters.

downlink-bw *dl_bw*

Default: 32

Specifies the downlink (towards the MN) data traffic bandwidth in kilo-bits per second for this QoS profile.

dl_bw must be an integer value between 0 and 100000.

drop-rate *drop_percentage*

Default: 0

Specifies the permitted packet drop rate in percentage for traffic flow to this QoS profile.

drop_percentage must be an integer value between 0 and 1000.

latency *latency_duration*

Default: 1000

Specifies the permitted latency duration in milli-seconds for this QoS profile.

latency_duration must be an integer value between 0 and 1000.

qos-class {class-A | class-B | class-C | class-D | class-E | class-F }

Default: Class-C

Specifies the type of QoS class associated with this QoS profile

class-A: Specifies the A type of QoS class.

class-B: Specifies the B type of QoS class.

class-C: Specifies the C type of QoS class.

class-D: Specifies the D type of QoS class.

class-E: Specifies the E type of QoS class.

class-F: Specifies the F type of QoS class.

uplink-bw *ul_bw*

Default: 32

Specifies the uplink (from the MN) data traffic bandwidth in kilo-bits per second for this QoS profile.

ul_bw must be an integer value between 0 and 100000.

+

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

Usage Guidelines

Use this command to define the values associated with the profile ID on the PDSN. This profile ID is used during the mapping to and from the authorized QoS to the QoS parameters for the A10 link. This mapping is required because the PDSN only knows the profile IDs and not the actual configured values for the profile ID in the RAN. Also this configuration allows the use of custom profile IDs for the subscribers.

If no values are defined with a QoS profile ID, the values from matching QoS profile ID from RAN will be applicable to the subscriber traffic.

Example

The following command sets the downlink bandwidth to *32* kbps, latency duration as *1000* ms, uplink bandwidth to *32* kbps, and QoS class to Class-C for the QoS profile ID *11* in a PDSN service:

```
default qos-profile-id-mapping profile-id 11
```

qos update

Sets QoS update parameters for policy mismatches or wait timeouts.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
qos-update { policy-mismatch | wait-timeout seconds action { disconnect-session
 | downgrade-to-best-effort | drop-packets } }
[ no | default ] qos-update { policy-mismatch | wait-timeout }
```

no

Enables/Disables the **qos-update** [**policy-mismatch** | **wait-timeout**].

default

Sets / Restores default value for **qos-update** [**policy-mismatch** | **wait-timeout**].

policy-mismatch

PDSN raises a TFT violation if there is a QoS policy mismatch.

wait-timeout *seconds* action { disconnect-session | downgrade-to-best-effort | drop-packets }

Sets the wait time for A11 RRQ for QoS changes. *seconds* must be an integer from 1 through 1000.

action: configures the action on the wait-timeout

- **disconnect-session**: Drops the call if the A11 RRQ has not been received for the QoS update. This includes all of the IP flows for the session.
- **downgrade-to-best-effort**: Drops packets if the A11 RRQ has not been received for the QoS update. Sends the forward traffic over best effort (flow FF or FE if available).
- **drop-packets**: Drops packets if the A11 RRQ has not been received for the QoS update.

Usage Guidelines

This command provides a PDSN service level configurable to configure an action, if the PCF ignores the QoS Update request from PDSN. It sets the amount of time to wait and the action to take, if no RRQ is received before the timeout. The action can be to drop packets for the flow, disconnect the session or to downgrade to best effort.

Example

```
qos-update policy-mismatch
```

The following command sets **wait-timeout** to *60* seconds and invokes **downgrade-to-best-effort** if the A11 RRQ has not been received for the QoS update:

```
qos-update wait-timeout 60 actiondowngrade-to-best-effort
```

radius accounting dropped-pkts

This command enables or disables RADIUS accounting related configuration for dropped packets.



Important This command is customer-specific. Contact your Cisco account representative for more information.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] radius accounting dropped-pkts
```

no

Enables the RADIUS accounting related configuration for dropped packets.

radius accounting dropped-pkts

Disables the RADIUS accounting related configuration for dropped packets. This is the default behavior.

Usage Guidelines

Use this command to enable or disable the RADIUS accounting related configuration for dropped packets.

By default, the feature is disabled.



Important The configuration will be picked up during **call-setup** and can not be changed dynamically.

Example

The following command enables the RADIUS accounting related configuration for dropped packets for the PDSN service:

```
no radius accounting dropped-pkts
```

registration-accept

Allows the PDSN to accept registration requests when a handoff disconnect is in progress. When the PDSN is tearing down a session and the MN moves over to a new PCF and initiates a new session, the PDSN by default does not accept the handoff until it tears down the old session.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no | default] registration-accept handoff session-disconnect-in-progress

no

Disable accepting of registration requests when a handoff disconnect is still in progress.

default

Default is disabled.

Sets / Restores default value assigned for **registration-accept handoff session-disconnect-in-progress**.

Usage Guidelines

Use this command to allow the PDSN service to accept registration requests when a handoff disconnect is still in progress.

Example

```
registration-accept handoffsession-disconnect-in-progress
```

registration-ack-deny terminate-session-on-error

Configures the PDSN service to terminate an A11 session when a Registration ACK received from the PCF has an error status.

Product PDSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description **[no | default] registration-ack-deny terminate-session-on-error**

no

Disable terminating A11 sessions on a Registration ACK error from the PCF.

default

Sets / Restores default value assigned to **registration-ack-deny terminate-session-on-error**.

Usage Guidelines Use this command to enable the PDSN service to terminate A11 sessions on a Registration ACK error from the PCF.

Example

Use the following command to enable this functionality in the PDSN:

```
registration-ack-deny terminate-session-on-error
```

registration-deny

Configures parameters related to registration rejection.

Product PDSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
registration-deny { handoff { closedrp-rp handoff-in-progress |
connection-setup-record-absent [ use-deny-code { poorly-formed-request |
reason-unspecified } | max-deny-reply-limit num |
mismatched-coa-source-address | new-call { connection-setup-record-absent
 | reverse-tunnel-unavailable } | session-already-active |
session-already-closed | session-already-dormant |
```

```
terminate-session-on-error | use-zero-gre-key}
[ default |no ] registration-deny { handoff { closedrp-rp handoff-in-progress
 | connection-setup-record-absent } | mismatched-coa-source-address |
new-call { connection-setup-record-absent | reverse-tunnel-unavailable } |
 session-already-active | session-already-closed | session-already-dormant
 | terminate-session-on-error | use-zero-gre-key}
```

default

Sets / Restores default value for **registration-deny**.

no

Disables the specified option.

handoff { closedrp-rp handoff-in-progress | connection-setup-record-absent [use-deny-code { poorly-formed-request | reason-unspecified }

This command configures the handoff behavior.

closedrp-rp handoff-in-progress: Configures parameters related to denying handoffs from Closed-RP to RP systems. When enabled the PDSN rejects retransmitted handoff R-P requests when a handoff is already in progress from Closed RP to RP. The deny code used is 'Reason Unspecified'. The default is disabled meaning that the PDSN simply discards such requests.

connection-setup-record-absent [**use-deny-code** { **poorly-formed-request** | **reason-unspecified** }]: When enabled the PDSN denies or discards handoff R-P sessions that do not have an Airlink Connection Setup record in the A11 Registration Request. Default is disabled. Default PDSN behavior is to accept such requests.

[**use-deny-code** { **poorly-formed-request** | **reason-unspecified** }: Sets the specified Registration Deny Code when denying a handoff because of a missing connection setup record.

max-deny-reply-limit *num*

Default: 3

Configures max number of retries of erroneous registration request message from PCF for a session before PDSN terminates the session. *num* can be from 1 to 10.

mismatched-coa-source-address

Default: disabled

Denies RP requests which have a care-of-address field that is different from the request source address.

new-call { connection-setup-record-absent [use-deny-code { poorly-formed-request | reason-unspecified } | reverse-tunnel-unavailable }

connection-setup-record-absent: Configures the PDSN to reject calls that do not have the airlink connection setup record in the RRQ.

use-deny-code { **poorly-formed-request** | **reason-unspecified** } When rejecting calls that do not have the airlink setup record, use the specified deny code.

reverse-tunnel-unavailable: Configures the PDSN to reject calls if the GRE key for a user collides with that of another user.

session-already-active

PDSN denies Registration requests for sessions that are already active with the error code "poorly formed request" .

session-already-closed

PDSN denies RP renew and dereg requests with error code 0x8E for absent R-P sessions.

session-already-dormant

PDSN denies Registration requests for sessions that are already dormant with the error code "poorly formed request" .

terminate-session-on-error

Default: Disabled.

Configures PDSN to terminate session if erroneous registration request message is received for the session.

use-zero-gre-key

Configures the PDSN to set the GRE key to zero (0) when denying a new R-P session.

Usage Guidelines

Use this command to configure parameters relating to the rejection of registration requests.

Example

To reject calls that do not have the airlink setup record in the RRQ, enter the following command:

```
registration-deny new-call connection-setup-record-absent
```

To reject calls if the GRE key collides with that of another user, enter the following command:

```
registration-deny new-call reverse-tunnel-unavailable
```

To set the GRE key to 0 (zero) when a new R-P session is denied, enter the following command:

```
registration-deny new-call use-zero-gre-key
```

registration-discard

Configures the PDSN service to discard any Registration Request message containing multiple information elements of the same type or a different GRE key for existing IMSI session.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[defualt | no] registration-discard { bad-extension | gre-key-change | handoffconnection-setup-record-absent }

default

Sets/Restores default value assigned for **registration-discard** .

no

Disables the discarding of Registration request messages containing multiple information elements or different GRE keys.

bad-extension

Default: Disabled

Configures the PDSN to discard Registration Request message containing multiple information elements of same type.

gre-key-change

Default: Disabled

Configures PDSN to discard Registration Request message containing different GRE key for existing IMSI session. Default is disable

handoff connection-setup-record-absent

Default: Disabled

When enabled, discards A11 Handoff requests that do not contain the Airlink Setup record.

Usage Guidelines

Use this command to configure the PDSN service to discard and Registration Requests that contain multiple information elements of the same type or discard Registration Requests that contain GRE keys that have different GRE keys for the existing IMSI session.

Example

To configure the PDSN service to discard of Registration Requests that have multiple information elements of the same type, enter the following command:

```
registration-discard bad-extension
```

To configure the PDSN service to discard registration Requests that contain a GRE key that is different than the existing one for the existing IMSI session, enter the following command:

```
registration-discard gre-key-change
```

registration-update

Configures registration update related parameters for the PDSN.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
registration-update { pdsn-code-nvse | wait-timeout secs }
[ default | no ] registration-update { pdsn-code-nvse | wait-timeout }
```

no

If this option is used with the **pdsn-code-nvse** keyword, then pdsn-code-nvse configuration is disabled.

If this option is used with the **wait-timeout** keyword, a separate A11 timer is not used. The PDSN waits for the ppp retransmit-timeout and then sends the A11 Update. If a value is provided, then the "ppp retransmit-timeout" is ignored and a separate A11 timeout is started immediately upon sending the LCP Term-Ack. The A11 Update is then sent when the timer expires.

A value of 0 sends the A11 Update immediately after sending the LCP Term-Ack.

default

Sets/Restores default value assigned for **registration-update** { **pdsn-code-nvse** | **wait-timeout }**

pdsn-code-nvse

Adds the PDSN code NVSE in all A11 registration update messages.

secs

The number of seconds to wait. *secs* must be an integer in the range from 0 through 16.

wait-timeout

After the Mobile Node terminates a PPP session between the PDSN and the Mobile Node, the PDSN service waits for the specified time period to receive an A11 RRQ from the PCF before it sends out a Registration-Update to clear the Session from the PCF.

Usage Guidelines

Use this command to configure registration update related

The **wait-timeout** keyword configures the PDSN to wait the specified amount of time before sending out a Registration-Update to clear the Session from the PCF.

Example

Use the following command to set the registration wait-timeout to *16* seconds:

```
registration-update wait-timeout 16
```

retransmission-timeout

Configures the maximum allowable time for the PDSN service to wait for a response from the PCF before it:

Attempts to communicate with the PCF again (if the system is configured to retry the PCF)

OR

Marks the PCF as unreachable.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
retransmission-timeout time
[default|no] retransmission-timeout
```

no

Enables/Disables the **retransmission-timeout**.

default

Sets / Restores default value assigned for **retransmission-timeout**.

time

Specifies the maximum allowable time for the PDSN service to wait for a response from the PCF before it a) attempts to communicate with the PCF again (if the system is configured to retry the PCF) or b) marks the PCF as unreachable.

time is measured in seconds and can be configured to any integer value between 1 and 1,000,000.

Usage Guidelines

Use the retransmission timeout command in conjunction with the **max-retransmissions** command in order to configure the PDSN services behavior when it does not receive a response from a particular PCF.

Use the **no retransmission-timeout** command to delete a previously configured timeout value. If after deleting the lifetime setting you desire to return the lifetime parameter to its default setting, use the **default retransmission-timeout** command.

The chassis is shipped from the factory with the retransmission timeout set to 3 seconds.

Example

The following command configures a retransmission timeout value of *5* seconds:

```
retransmission-timeout 5
```

The following command deletes a previously configured retransmission-timeout setting:

noretransmission-timeout

service-option

If the service option policy is enabled, this command specifies the service options supported by the PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

service-option *number*
no service-option *number*

no

Enables/Disables the **service-option** *number*

default

Sets / Restores default value assigned for **service-option**.

number

Default: 7, 15, 22, 23, 24, 25, 33, 59, 67

Specifies a specific Service Option (SO) number that this PDSN service is allowed to support.

number can be configured to any integer value between 1 and 1000.

Usage Guidelines

Use the service option command in conjunction with the policy service option enforce command to configure specific SO numbers that are supported. If a particular SO number is not configured, then any subscriber session received with that SO number will be rejected and an A11 Registration Reply Code of 86 (poorly formed request) will be sent.

By default, PDSN services are configured to support the following service option numbers:

- 7: PCF specific
- 15: PCF specific
- 22: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS1 forward, RS1 reverse)
- 23: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS1 forward, RS2 reverse)
- 24: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS2 forward, RS1 reverse)

- 25: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS2 forward, RS2 reverse)
- 33: 3G High Speed Packet Data
- 59: High Rate Packet Data
- 67: RP A10 connection



Important Option 67 is used for auxiliary connections for Rev-A calls. PPP encapsulation of data packets does not flow over this service option connection. ROHC can be performed without PPP for this service option.

Use the **no service-option** *number* command to delete a previously configured service option. If after deleting the service option setting you desire to return the service option parameter to its default setting, use the **default service-option command**.

Example

The following command enables a service option of *12*:

```
service-option 12
```

The following command disables the default service option *59* :

```
no service-option 59
```

setup-timeout

Specifies the maximum amount of time allowed for session setup.

Product PDSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ]setup-timeout seconds
default setup-timeout
```

default

Sets/Restores default value assigned for **setup-timeout**.

seconds

Default: 60 seconds

The maximum amount of time, in seconds, to allow for setup of a session. *seconds* must be an integer from 1 through 1000000

Usage Guidelines Use this command to set the maximum amount of time allowed for setting up a session.

Example

Use the following command to set the maximum time allowed for setting up a session to *300* seconds:

```
setup-timeout 300
```

simple-ip allow

Enables or disables Simple-IP sessions from making a connection before authorization takes place.

Product PDSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description `[ no|default ] simple-ip allow`

no

When a session attempts PPP authentication, it is assumed that it is a Simple-IP session and it is disconnected before the user is authenticated (RADIUS or local authentication). Also, if **allow-noauth** is enabled and PPP authentication is not performed, after IPCP the session is disconnected if it is discovered that it is a Simple-IP session.

default

Reset this command to allow Simple-IP sessions to connect.

Usage Guidelines Use this command to prevent Simple-IP sessions from connecting to a PDSN service.

Example

The following command configures the PDSN service so that it will reject any Simple-IP sessions:

```
no simple-ipallow
```

The following command configures the PDSN service to allow Simple-IP sessions:

```
simple-ip allow
```

spi

Configures the security parameter index (SPI) between the PDSN service and the PCF. This command also configures the redirection of call based on PCF zone.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

spi remote-address { *pcf_ip_address* | *ip_addr_mask_combo* } **spi-number** *number* { **encrypted secret** *enc_secret* | **secret** *secret* } [**description** *string*] [**hash-algorithm** { **md5** | **rfc2002-md5** }] [**replay-protection** { **nonce** | **timestamp** }] [**timestamp-tolerance** *tolerance*] [**zone** *zone_id*]
no spi remote-address *pcf_ip_address* **spi-number** *number*

remote-address { *pcf_ip_address* | *ip_addr_mask_combo* }

pcf_ip_address: Specifies the IP address of the PCF. pcf_ip_address is an IP address expressed in IP v4 dotted decimal notation.

ip_addr_mask_combo: Specifies the IP address of the PCF and specifies the IP address network mask bits. *ip_addr_mask_combo* must be specified using the form 'IP Address/Mask Bits' where the IP address must either be an IPv4 address expressed in dotted decimal notation or an IPv6 address expressed in colon notation and the mask bits are a numeric value which is the number of bits in the subnet mask.

spi-number *number*

Specifies the SPI (number) which indicates a security context between the PCF and the PDSN in accordance with IOS 4.1 and RFC 2002.

number can be configured to any integer value between 256 and 4294967295.

encrypted secret *enc_secret* | secret *secret*

Configures the shared-secret between the PDSN service and the PCF. The secret can be either encrypted or non-encrypted.

encrypted secret *enc_secret*: Specifies the encrypted shared key (enc_secret) between the PCF and the PDSN service. enc_secret must be between 1 and 254 alpha and/or numeric characters and is case sensitive.

secret *secret*: Specifies the shared key (secret) between the PCF and the PDSN services. secret must be between 1 and 127 alpha and/or numeric characters and is case sensitive.

The **encrypted** keyword is intended only for use by the chassis while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.

description *string*

This is a description for the SPI. *string* must be an alpha and or numeric string of from 1 through 31 characters.

hash-algorithm { md5 | rfc2002-md5 }

Default: md5

Specifies the hash-algorithm used between the PDSN service and the PCF.

md5: Configures the hash-algorithm to implement MD5 per RFC 1321.

rfc2002-md5: Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.

replay-protection { nonce | timestamp }

Default: timestamp

Specifies the replay-protection scheme that should be implemented by the PDSN service.

nonce: Configures replay protection to be implemented using NONCE per RFC 2002.

timestamp: Configures replay protection to be implemented using timestamps per RFC 2002.

timestamp-tolerance *tolerance*

Default: 60

Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded, then the session will be rejected. If this is set to 0, then time stamp tolerance checking is disabled at the receiving end.

tolerance is measured in seconds and can be configured to any integer value between 0 and 65535.

zone *zone_id*

Specifies the different PCF zones to configure in PDSN service. Mapping of a zone-number to a set of PDSNs can be done per PDSN service basis.

zone_id must be an integer value between 1 and 32. A maximum of 32 PCF zones can be configured for a PDSN service.

Usage Guidelines

An SPI is a security mechanism configured and shared by the PCF and the PDSN service. Please refer to IOS 4.1 and RFC 2002 for additional information.

Multiple SPIs can be configured if the PDSN service is communicating with multiple PCFs.



Important The SPI configuration on the PCF must match the SPI configuration for the PDSN service on the system in order for the two devices to communicate properly.

Use the **no** version of this command to delete a previously configured SPI.

This command used with **zone** *zone_id* redirects all calls on the basis of PCF zone to the specific PDSN on the basis of parameters configured at policy pcf-zone-match command.

Example

The following command configures the PDSN service to use an SPI of 256 when communicating with a PCF with the IP address 192.168.0.2. The key that would be shared between the PCF and the PDSN service is q397F65.

```
spi remote-address 192.168.0.2 spi-number 256 secret q397F65
```

The following command deletes the configured SPI of *400* for an PCF with an IP address of *172.100.3.200*:

```
no spi remote-address 172.100.3.200 spi-number 400
```

The following command creates the configured SPI of *400* for an PCF with an IP address of *172.100.3.200* and zone id as 11:

```
spi remote-address 172.100.3.200 spi-number 400 zone 11
```

tft-validation wait-timeout

Configures the TFT validation wait timeout value for QoS changes. The QoS update timer triggers automatic QoS updates based on dynamic policies.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

tft-validation wait-timeout *seconds*
[**default** | **no**] **tft-validation wait-timeout**

no

Removes the wait-timeout timer.

default

Sets / Restores default value assigned for **tft-validation wait-timeout**.

Usage Guidelines

Configures the TFT validation wait time value for A11 RRQ for QoS changes. *seconds* must be an integer from 1 through 65535.

Example

Use the following command to set the TFT validation wait-timeout to *5* seconds:

```
tft-validation wait-timeout 5
```

threshold a11-ppp-send-discard

Sets an alarm or alert for the PDSN service based on the number of packets that the PPP protocol processing layer internally discarded on transmit for any reason.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

threshold a11-ppp-send-discard *high_thresh* [**clear** *low_thresh*]
no threshold a11-ppp-send-discard

no

Deletes the alert or alarm.

high_thresh

Default: *0*

The high threshold number of discarded PPP send packets that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between *0* and *100000*.

clear *low_thresh*

Default:*0*

The low threshold number of discarded PPP send packets that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between *0* and *100000*.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the number of discarded PPP send packets is equal to or greater than a specified number.

Alerts or alarms are triggered for the number of discarded PPP send packets is based on the following rules:

- **Enter condition:** Actual number of discarded PPP send packets > High Threshold
- **Clear condition:** Actual number of discarded PPP send packets £ Low Threshold

Example

The following command configures a number of discarded PPP send packets threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold a11-ppp-send-discard 1000 clear 500
```

threshold a11-rac-msg-discard

Sets an alarm or alert based on the number of Discarded A11 Registration Acknowledgements for the PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

threshold a11-rac-msg-discard *high_thresh* [**clear** *low_thresh*]
no threshold a11-rac-msg-discard

no

Deletes the alert or alarm.

high_thresh

Default: 0

The high threshold number of Discarded A11 Registration Acknowledgements that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100000.

clear *low_thresh*

Default:*0*

The low threshold number of Discarded A11 Registration Acknowledgements that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between *0* and *100000*.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the number of Discarded A11 Registration Acknowledgements is equal to or greater than a specified number.

Alerts or alarms are triggered for the number of Discarded A11 Registration Acknowledgements based on the following rules:

- **Enter condition:** Actual number of Discarded A11 Registration Acknowledgements > High Threshold
- **Clear condition:** Actual number of Discarded A11 Registration Acknowledgements £ Low Threshold

Example

The following command configures a number of Discarded A11 Registration Acknowledgements threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold a11-rac-msg-discard 1000 clear 500
```

threshold a11-rrp-failure

Sets an alarm or alert based on the number of A11 Registration Response failures for the PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
threshold a11-rrp-failure high_thresh [ clear low_thresh ]
no threshold a11-rrp-failure
```

no

Deletes the alert or alarm.

high_thresh

Default: 0

The high threshold number of A11 Registration Response failures that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100000.

clear *low_thresh*

Default:0

The low threshold number of A11 Registration Response failures that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 100000.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines Use this command to set an alert or an alarm when the number of A11 Registration Response failures is equal to or greater than a specified number.

Alerts or alarms are triggered for the number of A11 Registration Response failures based on the following rules:

- **Enter condition:** Actual number of A11 Registration Response failures > High Threshold
- **Clear condition:** Actual number of A11 Registration Response failures £ Low Threshold

Example

The following command configures a number of A11 Registration Response failures threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold a11-rrp-failure 1000 clear 500
```

threshold a11-rrq-msg-discard

Sets an alarm or alert based on the number of Discarded A11 Registration Requests for the PDSN service.

Product PDSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
threshold a11-rrq-msg-discard high_thresh [ clear low_thresh ]
no threshold a11-rrq-msg-discard
```

no

Deletes the alert or alarm.

high_thresh

Default: 0

The high threshold number of Discarded A11 Registration Requests that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100000.

clear *low_thresh*

Default:0

The low threshold number of Discarded A11 Registration Requests that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 100000.



Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the number of Discarded A11 Registration Requests is equal to or greater than a specified number.

Alerts or alarms are triggered for the number of Discarded A11 Registration Requests based on the following rules:

- **Enter condition:** Actual number of Discarded A11 Registration Requests > High Threshold
- **Clear condition:** Actual number of Discarded A11 Registration Requests £ Low Threshold

Example

The following command configures a number of Discarded A11 Registration Requests threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold a11-rrq-msg-discard 1000 clear 500
```

threshold init-rrq-rcvd-rate

Sets an alarm or alert based on the average number of calls setup per second for the context.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
threshold init-rrq-rcvd-rate high_thresh [ clear low_thresh ]
no threshold init-rrq-rcvd-rate
```

no

Deletes the alert or alarm.

high_thresh

Default: 0

The high threshold average number of calls setup per second must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between *0* and *1000000*.

clear *low_thresh*

Default:0

The low threshold average number of calls setup per second that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between *0* and *1000000*.



Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the average number of calls setup per second is equal to or greater than a specified number of calls per second.

Alerts or alarms are triggered for the number of calls setup per second based on the following rules:

- **Enter condition:** Actual number of calls setup per second > High Threshold
- **Clear condition:** Actual number of calls setup per second £ Low Threshold

Example

The following command configures a number of calls setup per second threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold init-rrq-rcvd-rate 1000 clear 500
```