

PDIF Service Configuration Mode Commands

The PDIF Service Configuration Mode is used to configure the properties required for a mobile station to interface with a Packet Data Interworking Function (PDIF).

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

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

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

- aaa attribute, on page 1
- aaa authentication, on page 3
- bind, on page 4
- default, on page 5
- duplicate-session-detection, on page 6
- hss, on page 7
- ims-sh-service, on page 8
- ip source-violation, on page 9
- mobile-ip, on page 10
- setup-timeout, on page 11
- username, on page 12

aaa attribute

Sets the system attributes for AAA messages.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
aaa attribute { 3gpp2-bsid string | 3gpp2-service-option integer |
calling-station-id integer  | 3gpp2-serving-pcf ip-address }
no aaa attribute
default aaa attribute 3gpp2-service-option integer
```

no

Removes a previously configured AAA attribute.

default

Returns the specified aaa attribute to the original default system settings.

3gpp2-bsid *string*

Specifies the base-station ID and consists of the SID + NID + CELLID.

string must contain 12 hexadecimal upper-case ASCII characters.

3gpp2-service-option *integer*

Specifies the radius attribute value when sending authentication and accounting messages as an integer from 0 through 32767. Default: 4095

calling-station-id *integer*

Specifies the calling station phone number as a sequence of 1 through 15 digits.

3gpp2-serving-pcf *ip-address*

Use this command to generate attribute values without creating a new ASR 5000ASR 5500 image.

Usage Guidelines

If the RADIUS protocol is being used, accounting messages can be sent over a AAA interface to the RADIUS server.

3gpp2-serving-pcf attribute value (if configured) is sent in both RADIUS authentication and accounting messages. If the attribute value is not configured (or explicitly "not configured" using the **no** keyword), RADIUS attributes are still included with just type and length. This is because inclusion/exclusion of RADIUS attributes are still controlled through the dictionary, not via the CLI.

Example

The following command identifies the base station ID:

```
aaa attribute 3gpp2-bsid 0ab2389acb3
```

aaa authentication

Sets the aaa authentication for first and second phase authentication when multiple authentication is configured on the system.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
aaa authentication { { first-phase | second-phase } | { context-name name
 aaa-group name } }
no aaa authentication { first-phase | second-phase }
```

no aaa authentication { first-phase | second-phase }

Removes any existing authentication configuration.

first-phase context-name *name* aaa-group *name*

Specifies the context name and the aaa group name configured in the context for the first authentication phase.

Important First phase authentication is mandatory when multiple authentication is configured on the system.

- **context-name** *name*: Specifies the context where the aaa server group is defined as an alphanumeric string of 1 through 79 characters.
- **aaa-group** *name*: Specifies the name of the aaa-group to be used for authentication as an alphanumeric string of 1 through 79 characters.

second-phase context-name *name* aaa-group *name*

Specifies the context name and the aaa group name configured in the context for the second authentication phase.

- **context-name** *name*: Specifies the context where aaa server group is defined as an alphanumeric string of 1 through 79 characters.
- **aaa-group** *name*: Specifies the name of the aaa-group to be used for authentication as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Two phase-authentication happens in IKEv2 setup for setting up the IPSec session. The first authentication uses Diameter AAA EAP method and second authentication uses RADIUS AAA authentication. The same

AAA context may be used for both authentications. PDIF service allows you to specify only a single AAA group, which could normally be used for the first authentication method.

A given AAA group only supports either Diameter or RADIUS authentication. If the NAI in the first authentication is different from NAI in the second authentication each NAI can point to a different domain profile in the PDIF. Each domain profile may be configured with each AAA group, one for Diameter and the other for RADIUS.

Example

Use the following to configure first-phase authentication for an aaa group named *aaa-10* in the PDIF context:

```
first-phase context-name pdif aaa-group aaa-10
```

bind

Binds the service IP address to a crypto template and configures the number of sessions the PDIF can support.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
bind address address { crypto-template string } [ max-sessions number ]
no bind
```

no

Removes a previously configured binding.

address

Specifies the IP address of the service.

crypto-template *string*

Specifies the name of the crypto template to be bound to the service as an alphanumeric string of 0 through 127 characters.

max-sessions *number*

Specifies the maximum number of sessions to be supported by the service as an integer from 0 to 3000000. Default: 3000000

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

Usage Guidelines

Binds the IP address used as the connection point for establishing the IKEv2 sessions to the crypto template. It can also define the number of sessions the PDIF can support.

Example

The following command binds a service with the IP address *13.1.1.1* to the crypto template *T1* and sets the maximum number of sessions to *2000000*:

```
bind address 13.1.1.1 crypto-template T1 max-sessions 200000
```

default

Sets or restores the default condition for the selected parameter.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
default { { aaa attribute 3gpp2-service-option } |
duplicate-session-detection | hss { failure-handling
mac-address-validation-failure | mac-address-validation | update-profile
 } | ip source-violation { drop-limit | period } | setup-timeout |
subscriber name | username mac-address-stripping } }
```

aaa attribute 3gpp2-service-option

Configures the default value 4095.

duplicate-session-detection

Configures the default to be NAI-based.

hss { failure-handling mac-address-validation-failure | mac-address-validation | update-profile }

Configures the HSS server defaults:

failure-handling mac-address-validation-failure: By default, the MAC address is validated by IMS-Sh interface.

- **mac-address-validation**: By default, validating the MAC address is disabled.
- **update-profile**: By default, updating the PDIF profile is disabled.

ip source-violation { drop-limit | period }

Configures IP source-violation detection defaults.

- **drop-limit**: Default number of ip source violations permitted in detection period before the call is dropped is 10.
- **period**: Default detection period is 120 seconds.

setup-timeout

Default call setup time limit is 60 seconds.

subscriber *name*

Configures the default subscriber name. *name* is a string of 1-127 characters.

username mac-address-stripping

Default is to disable stripping the MAC address from the username.

Usage Guidelines

Configures the default settings for a given parameter.

Example

Use the following example to configure the default call setup time limit:

```
default setup-timeout
```

duplicate-session-detection

Configures the PDIF to detect duplicate call sessions using old IMSI or NAI addresses and clear old call information.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no | default ] duplicate-session-detection { imsi-based | nai-based }
```

no

Stops duplicate session detection.

default

Configures the default setting, which is NAI-based detection.

imsi-based

Configures the PDIF to detect duplicate call sessions based on the IMSI address.

nai-based

Configures the PDIF to detect duplicate call sessions based on the NAI address. This is the default setting.

Usage Guidelines

If an MS leaves the Wi-Fi coverage area and subsequently comes back online, it may initiate a new session setup procedure. After both the device authentication with HSS and the subscriber authentication with AAA server are completed, PDIF runs the internal mechanism to see whether there was any other session bound with the same IMSI. If an old session is detected, PDIF starts clearing this old session by sending a proxy-MIP Deregistration request to the HA. PDIF resumes new session setup by sending a proxy-MIP registration request. When the old session is aborted, PDIF sends Diameter STR messages and RADIUS Acct STOP messages to corresponding AAA servers.

PDIF allows duplicate session detection based on either the NAI or IMSI addresses. When detecting based on NAI, it is the first-phase (device authentication) NAI that is used.

Example

The following command configures duplicate session detection to use IMSI addressing:

```
duplicate-session-detection imsi
```

hss

Configures the Home Subscriber Server (HSS) parameters.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
hss { failure-handling { { mac-address-validation-failure | update-profile
 } action { terminate | continue } } | update-profile |
mac-address-validation }
[ no | default ] hss { failure-handling | update-profile |
mac-address-validation }
```

no

Removes a previously configured HSS profile.

default

Resets the defaults for this command.

failure-handling mac-address-validation-failure

Configures how the HSS is to handle errors.

If HSS returns a list of MAC addresses and if PDIF fails to match the subscriber MAC address against the list, the session is always terminated.

action { continue | terminate }

Configures the action to be performed depending on the failure type.

- **continue**: Ignores a mac-address-validation-failure and continue the session.
- **terminate**: Terminates the session on a mac-address-validation-failure.

mac-address-validation

If mac-address-validation is enabled, the PDIF queries the HSS for a list of MAC addresses associated with the Mobile Directory Number (MDN). Default: Disabled

update-profile

Update the HSS with the subscriber profile. Default: Disabled

Usage Guidelines

An HSS provides MAC address validation and store part of the subscriber profile. This command enables or disables validation and profile updates, and configures how the system responds to failures: terminate or continue a session.

An ims-sh-service and Diameter interface need to be configured to communicate with the HSS.

Example

The following example enables *mac-address* validation:

```
hss mac-address-validation
```

ims-sh-service

Associates the IMS-Sh-service parameters.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ims-sh-service name name
no ims-sh-service name name
```

no

Removes a previously configured IMS-Sh-service.

name

Names the IMS-Sh-service in the pdif-service context.

Usage Guidelines

This command is used to name the IMS-Sh-service.

Example

The following command names the IMS-Sh-service ims1:

```
ims-sh-service name imsi1
```

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 that the source address of the received packets matches the IP address assigned to the subscriber (either statically or dynamically) during the session.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

clear-on-valid-packet

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

drop-limit *num*

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 is an integer from 1 to 1000000. Default: 10

period *secs*

Sets the length of time (in seconds) for a source violation detection period to last.

If *secs* is not specified, the value is set to the default.

secs is an integer from 1 to1000000. Default: 120

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 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 the IP source-violation drop-limit counter and starts the timer for the IP-source violation period. Every subsequent packet received with a bad source address during the IP-source violation period causes the drop-limit counter to increment.

For example, if the drop-limit is set to 10, after 10 source violations, the call is dropped. The period timer continues to count throughout this process.

Example

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

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

mobile-ip

Sets the MIP FA context for the specific PDIF service.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
mobile-ip foreign-agent context string [ fa-service string ]
no mobile-ip
```

no

Removes previously configured parameters.

foreign-agent context *string*

Specifies the context name in which the FA is configured as an alphanumeric string of 1 through 79 characters.

fa-service *string*

Specifies the name of the FA service in the FA context as an alphanumeric string of 1 through 79 characters.

Usage Guidelines

Shows in which context the FA is located and names the FA service.

Example

This command configures MIP for the FA context named *fa1*:

```
mobile-ip foreign-agent context fa1
```

setup-timeout

Configures the maximum time allowed to set up a session.

Product

PDIF

Privilege

Security-Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
setup-timeout integer
default setup-timeout
```

setup-timeout *integer*

Specifies the session setup timer (in seconds) as an integer from 2 through 300. Default: 60

default setup-timeout

Defaults the session setup timer to 60 seconds.

Usage Guidelines

PDIF clears both user session and tunnels if a call does not initiate successfully before the timer expires.

Example

The following command sets the setup-timeout to the default 30 seconds:

```
default setup-timeout
```

username

Configures mac-address-stripping on a username coming in from a mobile station session.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
username mac-address-stripping
[ default | no ] username mac-address-stripping
```

username mac-address-stripping

Configures mac-address stripping from the Network Access Identifier (NAI).

default

Configures the default parameter which is **disabled**.

no

Returns the configuration to the default condition.

Usage Guidelines

When enabled, PDIF strips the MAC address from a mobile username NAI before sending to the RADIUS AAA server.

Example

The following example disables mac-address-stripping.

```
no username mac-address-stripping
```