Diameter Endpoint Configuration Mode Commands

Diameter Endpoint Configuration Mode is accessed from the Context Configuration Mode. The base Diameter protocol operation is configured in this mode.

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Important

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

app-level-retransmission

This command enables/disables setting "T" bit and retaining the same End-to-End Identifier (E2E ID) for application-level retransmissions.

Product

eHRPD

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

`[ default | no ] app-level-retransmission { retain-e2e | set-retransmission-bit }`

default

Configures this command with the default setting.

The default behavior is not to set the retransmission bit for a retried Diameter message.

retain-e2e

Sends the same End-to-End Identifier for a retried Diameter message.

set-retransmission-bit

Sets the retransmission bit for retried Diameter messages.

Usage Guidelines

Use this command to enable application-level transmission with "T" bit set.

'T' bit setting is done only for DIABASE protocol-based rerouting and not for application-based retransmissions. In order to identify such retransmissions, the server expects the T bit to be set at all levels (both DIABASE and application) of retransmission, which can be achieved with this CLI command.

In addition to using this CLI command for setting the T-bit in a retried message, it is also possible to retain the same End-to-End ID. With this feature turned on, the server can detect any duplicate/re-transmitted messages sent by Diameter clients or agents. Note that this feature is applicable to Gy and Rf messages as well.

Similar CLI command for setting T-bit is also present under Credit Control Group configuration mode, which when configured will take effect for Gy messages else endpoint configuration will be used.

Example

The following command specifies to set retransmission bit and retain e2e:

```
app-level-retransmission set-retransmission-bit retain-e2e
```

associate

This command associates/disassociates a Stream Control Transmission Protocol (SCTP) parameter template with the Diameter endpoint.

Product

ePDG

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

```
associate sctp-parameters-template template_name
no associate sctp-parameters-template
```

no

Disassociates an SCTP parameter template with the Diameter endpoint.

sctp-parameters-template *template_name*

Associates a previously created SCTP parameter template with the Diameter endpoint. *template_name* specifies the name for a pre-configured SCTP parameter template. For more information on SCTP parameter templates,

refer to the **sctp-param-template** command in the *Global Configuration Mode Commands* chapter in this guide.

Usage Guidelines

Use this command to associate a configured SCTP parameter template with the Diameter endpoint.

The SCTP parameter template allows for SCTP timer values to be configured for the interface using the Diameter endpoint configuration. For more information on SCTP parameters, refer to the *SCTP Parameter Template Configuration Mode Commands* chapter in this guide.

Important

Only one SCTP parameter template can be associated with the Diameter endpoint configuration. The SCTP parameter template should be configured prior to issuing this command.

Only the following parameters from the template will be associated with the endpoint. When no SCTP parameter template is associated with the endpoint, the following default values are used:

sctp-cookie-life *60000* (default for the parameter template as well)

sctp-max-init-retx *5* (default for the parameter template as well)

sctp-max-path-retx *10* (default in the parameter template is 5)

sctp-rto-initial *3000* (default for the parameter template as well)

sctp-rto-max *60000* (default for the parameter template as well)

sctp-rto-min *1000* (default for the parameter template as well)

sctp-sack-period *200* (default for the parameter template as well)

timeout sctp-heart-beat *30* (default for the parameter template as well)

Example

The following command associates a pre-configured SCTP parameter template called *sctp1* to the Diameter endpoint:

```
associate sctp-parameters-template sctp1
```

cea-timeout

This command configures the Capabilities-Exchange-Answer (CEA) message timeout duration for Diameter sessions.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

cea-timeout *timeout*
default cea-timeout

default

Configures this command with the default setting.

Default: 30 seconds

timeout

Specifies the timeout duration (in seconds) to make the system wait for this duration for a CEA message. *timeout* must be an integer from 1 through 120.

Usage Guidelines

Use this command to configure the CEA timer, i.e., how long to wait for the Capabilities-Exchange-Answer message.

Example

The following command sets the Diameter CEA timeout to *16* seconds:

cea-timeout 16

connection retry-timeout

This command configures the Diameter Connection Retry Timeout parameter.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-ctx-diameter)#

Syntax Description

connection retry-timeout *timeout*
default connection retry-timeout

default

Configures this command with the default setting.

Default: 30 seconds

timeout

Specifies the connection retry timeout duration in seconds. The timeout must be an integer from 1 through 3600.

Usage Guidelines Use this command to configure the Diameter Connection Retry Timeout parameter.

Example

The following command sets the Diameter Connection Retry Timer to *120* seconds:

```
connection retry-timeout 120
```

connection timeout

This command configures the Diameter Connection Timeout parameter.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

```
connection timeout timeout
default connection timeout
```

default

Configures this command with the default setting.

Default: 30 seconds

timeout

Specifies the connection timeout duration (in seconds) as an integer from 1 through 30.

Usage Guidelines Use this command to configure the Diameter Connection Timeout parameter.

Example

The following command sets the Diameter connection timeout to *16* seconds:

```
connection timeout 16
```

description

Allows you to enter descriptive text for this configuration.

Product All

Privilege

Security Administrator, Administrator

Syntax Description

description *text*
no description

no

Clears the description for this configuration.

text

Enter descriptive text as an alphanumeric string of 1 to 100 characters.

If you include spaces between words in the description, you must enclose the text within double quotation marks (" "), for example, "AAA BBBB".

Usage Guidelines

The description should provide useful information about this configuration.

destination-host-avp

This command controls encoding of the Destination-Host AVP in initial/retried requests.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-ctx-diameter)#

Syntax Description

destination-host-avp { always | initial-request [redirected-request] | retried-request [redirected-request] | session-binding [redirected-request] }
default destination-host-avp

default

Configures this command with the default setting. Default: session-binding

always

Includes the Destination-Host AVP in all types of request messages.

session-binding [redirected-request]

Includes the Destination-Host AVP when the Diameter session is bound with a host.

redirected-request: Includes the Destination-Host AVP in any redirected request message when the Diameter session is bound with a host.

initial-request

Includes the Destination-Host AVP in an initial request but not in a retried request.

redirected-request: Includes the Destination-Host AVP in any redirected request message.

retried-request

Includes the Destination-Host AVP in a retried request but not in an initial request.

redirected-request: Includes the Destination-Host AVP in any redirected request message.

Usage Guidelines

Use this command to control encoding of the Destination-Host AVP in initial/retried requests.

This command has been introduced in release 12.0, in earlier releases, the Destination-Host AVP is not sent in session-setup/initial request (first message sent on that interface for that subscriber. The message will vary with different interfaces. For example, CCR-Initial for Gy, ACR-start for Rf, and so on). Also, Destination-Host AVP was not sent in retried requests. For example, CCR-Update failed to be responded by server. The message was retransmitted to alternate server.

In both these scenarios, it is not known which server will respond to the initial/retried message, so the Destination-Realm is encoded but not the Destination-Host. Only after a response for this message is received from one of the hosts present in that realm, the session is considered to be BOUND with that server. Any message sent after this binding will have the Destination-Host AVP encoded.

If the application has selected one of the servers using application-level commands like the **peer-select** command for credit-control or the **diameter authentication** or **accounting server** command in a AAA group, encoding of this AVP in initial/retried request is configurable.

When an application receives the Result-Code 3006 -DIAMETER_REDIRECT_INDICATION from the AAA server, the Diameter request message is forwarded to the Redirect-Host specified in the server's response. The message gets routed properly in case the Diameter host is directly connected to the AAA server. If there is a DRA between P-GW/ePDG and AAA server, the message goes into a loop as DRA always routes the packet to the AAA server which had redirected the message. To avoid the unnecessary looping, a new configurable option **redirected-request**is added to the **destination-host-avp** CLI command. This new option allows encoding the Destination-Host AVP in any type of Diameter redirected messages.

In releases prior to 19, the Destination-Host AVP was encoded in the redirected message only if the original request included Destination-Host AVP. In release 19 and beyond, encoding of Destination-Host AVP in redirected message is based on the configuration of **redirected-request** in the **destination-host-avp** command. If the CLI command is enabled, Destination-Host AVP will be included in any type of Diameter redirected messages. As per the current implementation, it is not possible to send retried messages to a different host using the same peer. This behavior is applicable for normal retry and failure-handling scenarios.

Since any redirected request is considered as retried request, if the option "**retried-request**" is used, by default Update (Interims) or Terminate (Stop) redirected-request will be encoded with Destination-Host AVP without the "**redirected-request**" option being configured. The reason to configure "**redirected-request**" as part of "**retried-request**" option is, in case of Initial-Retried request the Destination-Host AVP is not encoded if "**retried-request**" option alone is configured. To enable encoding Destination-Host AVP for Initial-Retried request, "**redirected-request**" is supported as an extension to "**retried-request**" as well.

Example

The following command specifies to include the Destination-Host AVP in initial request but not in retried request:

destination-host-avp initial-request

device-watchdog-request

This command manages the transport failure algorithm and configures the number of Device Watchdog Requests (DWRs) that will be sent before a connection is closed.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-diameter)#`

Syntax Description

device-watchdog-request max-retries *retry_count*
default device-watchdog-request max-retries

default

Configures this command with the default setting. Default: 1

retry_count

Specifies the maximum number of DWRs, and it must be an integer from 1 through 10.

Usage Guidelines

Use this command to configure the number of DWRs to be sent before closing the connection from a Diameter endpoint.

Example

The following command sets the DWRs to *3*:

device-watchdog-request max-retries 3

dpa-timeout

This command configures the Disconnect-Peer-Answer (DPA) message timeout duration for Diameter sessions.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

dpa-timeout *timeout*
default dpa-timeout

default

Configures this command with the default setting.

Default: 30 seconds

timeout

Specifies the DPA message timeout duration (in seconds) as an integer from 1 through 60.

Usage Guidelines

Use this command to set the timer for DPA message timeout during Diameter connection session. This makes the system wait for this duration for DPA message.

Example

The following command sets the Diameter DPA timeout to *16* seconds:

dpa-timeout 16

dscp

This command sets the Differential Services Code Point (DSCP) value in the IP header of the Diameter messages sent from the Diameter endpoint.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

dscp { *value* | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }
default dscp

value

Specifies to configure a unique DSCP as an integer in the range of 0 through 63.

af*xx*

Specifies the use of an assured forwarding *xx* per hop behavior (PHB).

be

Specifies the use of best effort forwarding PHB. This is the default.

cs*x*

Specifies the use of class selector *x* per PHB.

ef

Specifies the use of expedited forwarding PHB.

Usage Guidelines

Use this command to set the DSCP in the IP header of the Diameter messages sent from the Diameter endpoint. In addition to the recommended PHBs the user may configure their own DSCP as an integer in the range of 0 through 63.

Example

The following command sets the DSCP to *be*:

```
dscp be
```

dynamic-peer-discovery

This command configures the system to dynamically locate peer Diameter servers by means of DNS.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

```
dynamic-peer-discovery [ protocol { sctp | tcp } ]
{ default | no } dynamic-peer-discovery
```

default

Configures this command with the default setting.

Default: disabled

no

Removes the configuration.

protocol { sctp | tcp }

Configures peer discovery to use a specific protocol. Default: TCP

sctp: Uses Streaming Control Transmission Protocol (SCTP) for peer discovery.

tcp: Uses Transmission Control Protocol (TCP) for peer discovery.

Usage Guidelines

Use this command to configure the system to dynamically locate peer Diameter servers by means of DNS.

Configure the **dynamic-peer-realm** command to locate Diameter servers using Naming Authority Pointer (NAPTR) queries. If the peer realm command is not configured, configuring this command will still allow applications to trigger an NAPTR query on their chosen realms.

The preferred transport protocol is TCP to resolve instances were multiple NAPTR responses with the same priority are received. The one using the TCP transport protocol will be chosen. If the transport protocol is configured through the CLI, then the configured protocol is given preference.

The IP address version will be the same as that of the origin host address configured for the endpoint. For IPv4 endpoints, A-type DNS queries will be sent to resolve Fully Qualified Domain Names (FQDNs). For IPv6 endpoints, AAAA-type queries are sent.

Example

The following command configures the system to dynamically locate peer Diameter servers using SCTP:

```
dynamic-peer-discovery protocol sctp
```

dynamic-peer-failure-retry-count

This command configures the number of times the system will attempt to connect to a dynamically discovered Diameter peer.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

dynamic-peer-failure-retry-count *no_of_retries*
default dynamic-peer-failure-retry-count

default

Configures this command with the default setting.

Default: 8

no_of_retries

Specifies the number of retry attempts to connect to a dynamically discovered Diameter peer. The value must be an integer from 0 through 255.

Usage Guidelines

Use this command to configure the number of times the system attempts to connect to a dynamically discovered Diameter peer.

After the specified number of attempts if the peer is still not open, the peer is moved into blacklist and other peers are tried. The blacklisted peer will be retried after a time period of one hour.

Example

The following command sets the retry attempts to *10*:

```
dynamic-peer-failure-retry-count 10
```

dynamic-peer-realm

This command configures the name of the realm where peer Diameter servers can be dynamically discovered.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

`[ no ] dynamic-peer-realm` *realm_name*

no

Removes the specified dynamic peer realm name from this endpoint configuration.

realm_name

Specifies the name of the peer realm where peer Diameter server are to be dynamically discovered. *realm_name* must be an existing realm, and must be an alphanumeric string of 1 through 127 characters.

Usage Guidelines

Use this command to locate Diameter servers using Naming Authority Pointer (NAPTR) queries.

Multiple realms can be configured. Even if the **dynamic-peer-discovery** command is not enabled, the realm configuration(s) will trigger dynamic peer discovery on all diabase instances.

Example

The following command configures a peer realm, used for dynamic peer discovery, with a name of *service-provider.com*:

```
dynamic-peer-realm service-provider.com
```

dynamic-route

This command configures the expiration time for dynamic routes created after a Diameter destination host is reached.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

dynamic-route expiry-timeout *value*
default dynamic-route expiry-timeout

default

Configures this command with the default setting. Default: 86400 seconds (1 day)

value

Specifies the time (in seconds) that a dynamic route to a Diameter host will expire. The value must be an integer from 1 through 86400000.

Usage Guidelines

Use this command to set expiration times for dynamic routes that are set up after a Diameter host has been reached.

Example

The following command sets the dynamic route expiration to *43200* seconds:

```
dynamic-route expiry-timeout 43200
```

end

Exits the current configuration mode and returns to the Exec mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **end**

Usage Guidelines Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **exit**

Usage Guidelines Use this command to return to the parent configuration mode.

load-balancing-algorithm

This command configures the behavior for load balancing Diameters peers in the event of a failure of an active server.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-diameter)#`

Syntax Description **load-balancing-algorithm { highest-weight | lowest-weight-borrowing min-active-servers** *number* **}**
default load-balancing-algorithm

default

Configures this command with the default setting.

Default: **highest-weight**

highest-weight

Selects an idle server with the highest weight in failure scenarios. If multiple servers have the same high weight, load balancing is performed among those servers.

lowest-weight-borrowing min-active-servers *number*

Borrows an idle server with the lowest weight and adds it to the group of servers where load balancing is performed. *number* specifies the number of servers that must always be available as active for load balancing. *number* must be an integer from 2 through 4000.

Usage Guidelines

Use this command to configure the behavior for load balancing Diameter peers in the event of a failure of an active server.

Example

The following command configures the load balancing behavior for Diameter peers to borrowing minimally active servers (lower weight) and maintaining an active server group of *30* servers:

```
load-balancing-algorithm lowest-weight-borrowing min-active-servers 30
```

max-outstanding

This command configures the maximum number of Diameter messages that any application can send to any one peer, while awaiting responses.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

`max-outstanding` *`messages`*
`{ default | no } max-outstanding`

no

Disables the maximum outstanding messages configuration.

default

Configures this command with the default setting.

Default: 256

messages

Specifies the maximum outstanding peer transmit window size setting. The input must be an integer from 1 through 4096.

Note that, in StarOS 14.1 and later releases, though the configuration allows up to 4K Diameter messages, it is restricted to queue up to 512 Diameter messages per peer to avoid any delay in the recovery of Diameter sessions.

Usage Guidelines

Use this command to set the unanswered Diameter messages that any application may send to any one peer, while awaiting responses. An application will not send any more Diameter messages to that peer until it has disposed of at least one of those queued messages. It disposes a message by either receiving a valid response or by discarding the message due to no response.

Example

The following command sets the Diameter maximum outstanding messages setting to *1024*:

max-outstanding 1024

origin address

This command has been deprecated. See the origin host, on page 17 and origin realm, on page 19 commands.

origin host

This command sets the origin host for the Diameter endpoint.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

origin host *host_name* **address** *ipv4_address* | *ipv6_address* **[port** *port_number* **] [accept-incoming-connections] [address** *ipv4_address_secondary* | *ipv6_address_secondary* **]**
no origin host *host_name* **address** *ipv4_address* | *ipv6_address* **[port** *port_number* **]**

no

Removes the origin host configuration.

origin host *host_name*

Specifies the host name to bind the Diameter endpoint. *host_name* must be the local Diameter host name. In releases prior to 16.0, the host name must be an alphanumeric string of 1 through 64 characters.

In 16.0 and later releases, the host name must be an alphanumeric string of 1 through 255 characters.

address *ipv4_address | ipv6_address*

Specifies the IP address to bind the Diameter endpoint using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. This address must be one of the addresses of a chassis interface configured within the context in which Diameter is configured.

port *port_number*

Specifies the port number for the Diameter endpoint (on inbound connections). The port number must be an integer from 1 through 65535. Default: 3868

Important When multiple diamproxies are running in the chassis, it is highly recommended that port number is NOT specified.

Port number in the origin host should be configured only when the chassis is running in server mode, i.e. when **accept-incoming-connections** is configured.

In this case it will open a listening socket on the specified port. For configurations where chassis is operating as a client, port number should not be included. In this case, a random source port will be chosen for outgoing connections. This is applicable for both with or without multi-homing.

Important Currently if multi-homing is configured, then the specified port is used instead of randomly chosen port. This is done so that application knows which port is used by the kernel as it will have to use the same port while adding/removing IP address from the association. Nevertheless, configuring port number in origin host for client mode is not supported.

accept-incoming-connections

Accepts inbound connection requests for the specified host (enables server mode).

Important MME only: This keyword is not supported. The MME acts only in client mode; setting the S6a (HSS) endpoint to 'accept-incoming-connections' will prevent the initialization of the S6a connection to the HSS.

address *ipv4_address_secondary | ipv6_address_secondary*

Specifies the secondary bind address for the Diameter endpoint in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. This address must be one of the addresses of a chassis interface configured within the context in which Diameter is configured.

When a secondary IP address is dynamically added or removed from an SCTP association, the affected host notifies its peer of the change in configuration using the Address Configuration Change Chunk (ASCONF) chunk without terminating the SCTP connection.

Usage Guidelines

Use this command to set the bind address for the Diameter endpoint.

Diameter agent on the chassis listens to standard TCP port 3868 and also supports the acceptance of any incoming TCP connection from external server.

The command **origin host** *host-name* must be entered exactly once. Alternatively, the **origin host** *host-name* **address** *ipv4/ipv6_address* **[port** *port_number* **]** command may be entered one or more times.

This command allows the user to configure multiple endpoints with the same origin host name. That is, it allows multiple endpoints (specifically that are used under S6a, S13 and SLg) to share the same Origin Host/Origin Realm.

Important Please be noted it is not possible to associate/map origin-host across endpoints to a specific diamproxy instance or maintain a constant origin host–instance mapping. Origin hosts are a pool of host entries and will be assigned on need basis. Endpoint in itself is an independent encapsulated entity.

Example

The following command sets the origin host name to *test* and the IP address to *10.1.1.1*:

```
origin host test address 10.1.1.1
```

origin realm

This command configures the realm to use in conjunction with the origin host.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

```
[ no ] origin realm realm_name
```

no

Removes the origin realm configuration.

realm_name

Specifies the realm to bind the Diameter endpoint. The *realm_name* must be an alphanumeric string of 1 through 127 characters. The realm is the Diameter identity. The originator's realm must be present in all Diameter messages. The origin realm can typically be a company or service name.

Usage Guidelines Use this command to set the realm for the Diameter endpoint.

Diameter agent on the chassis listens to standard TCP port 3868 and also supports the acceptance of any incoming TCP connection from external server.

Example

The following command sets the origin realm to *companyx*:

```
origin realm companyx
```

osid-change

This command stores the Origin-State-Id AVP of a diameter peer node on the P-GW. This enables the P-GW to detect and clear sessions whenever there is a change in the Origin-State-Id of the diameter peer node. This command is introduced at the diameter endpoint level.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

```
[ no ] osid-change action [clear-subscribers]
```

no

Disables the command.

action

Specifies the action to be taken.

clear subscribers

Clears subscribers connected to the peer.

Usage Guidelines

Use this command to store the Origin-State-Id AVP of a diameter peer node on the P-GW. This enables the P-GW to detect and clear sessions whenever there is a change in the Origin-State-Id of the diameter peer node. This command is introduced at the diameter endpoint level.

This command is disabled by default.

Example

The following command clears subscribers whose origin state IDs have changed.

:

```
diameter endpoint PGW-Gx use-proxy
    origin host PGW-Gx address 30.30.30.1 osid-change action
clear-subscribers no watchdog-timeout response-timeout 7
```

```
    connection timeout 5
    connection retry-timeout 2
    peer PGW-Gx-server realm PGW-Gx.com address 30.30.30.2 port 5333
#exit
```

peer

This command specifies a peer address for the Diameter endpoint.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-diameter)#`

Syntax Description

peer [*] *peer_name* **[*] [realm** *realm_name* **] [destination-host-name** *host_name* **] { address** *ipv4/ipv6_address* **[[load-ratio** *load_ratio_range* **] [port** *port_number* **] [connect-on-application-access] [send-dpr-before-disconnect disconnect-cause** *disconnect_cause* **] [sctp]] + | fqdn** *fqdn* **[[port** *port_number* **] [send-dpr-before-disconnect disconnect-cause** *disconnect_cause* **] [rlf-template** *rlf_template_name* **enable-snmp-traps]] }**
no peer *peer_name* **[realm** *realm_name* **]**

no

Removes the specified peer configuration.

[*] *peer_name* [*]

Specifies the peer's name as an alphanumeric string of 1 through 63 characters that allows punctuation characters.

The Diameter server endpoint can now be a wildcarded peer name (with * as a valid wildcard character). Client peers which satisfy the wild-carded pattern are treated as valid peers and the connection will be accepted. The wildcarded token indicates that the peer name is wildcarded and any '*' in the preceding string is treated as a wildcard.

realm *realm_name*

Specifies the realm of this peer as an alphanumeric string of 1 through 127 characters. The realm name can be a company or service name.

destination-host-name *host_name*

Specifies the destination host name as an alphanumeric string of 1 through 63 characters. Note that this is an optional keyword.

If a peer is selected by Diameter base protocol to forward an application request, then the host name specified through the "**destination-host-name**" option will be used to encode the Destination-Host AVP.

This keyword "**destination-host-name**" is made optional for backward compatibility. That means, if the destination-host-name is not specified in the CLI, the peer name itself is copied to the destination-host-name for backward compatibility.

In releases prior to 17.0, the endpoint configuration allows each SCTP association to be uniquely identified by a Diameter peer name. But there was a requirement where two SCTP associations are identified with the same peer name. This kind of reused peer-name was used by HSS peers which act as Active and Standby HSS nodes. The SCTP associations in HSS behave in a manner such that one association is always SCTP active (for the active HSS) while the other SCTP association with the standby HSS would be closed and would keep flapping. To avoid this scenario and address customer's requirement, in 17.0 and later releases, this optional keyword "**destination-host-name**" has been introduced in the **peer** CLI command to allow multiple unique peers (Diameter HSS servers) to be configured with the same host name.

With this enhancement, MME will be capable of provisioning multiple Diameter SCTP associations to reach the same HSS peer name. This configuration will also ensure that all the Diameter messages are exchanged properly with the configured destination host.

Internally the peers are identified with unique peer-name. But the Origin-host AVP provided by the server (in CER/CEA/App-msgs) is validated against both peer-name and destination-host-name provided in the CLI. Even if multiple peers are responding with same Origin-Host, this can be validated and accepted based on the CLI configuration.

address *ipv4/ipv6_address*

Specifies the Diameter peer IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. This address must be the IP address of the device with which the chassis is communicating.

load-ratio *load_ratio_range*

Specifies the Load Ratio for the peer. The Load Ratio can be configured in the range of 0 through 65535.

As a default behavior, the CLI command is not enabled for a peer and the default Load Ratio is 1, which will be used in load balancing only when at least one peer has non-default Load Ratio configured.

Not specifying the **load-ratio** *load_ratio_range* keyword from peer configuration will put the peer in default Load Ratio, and when all the peers have default Load Ratio, Diameter load balancing will be round robin.

The CLI takes effect when Diameter applications starts using an endpoint for sending messages.

fqdn *fqdn*

Specifies the Diameter peer FQDN as an alphanumeric string of 1 through 127 characters.

port *port_number*

Specifies the port number for this Diameter peer. The port number must be an integer from 1 through 65535.

connect-on-application-access

Activates peer on first application access.

send-dpr-before-disconnect

Sends Disconnect-Peer-Request (DPR).

disconnect-cause

Sends Disconnect-Peer-Request to the specified peer with the specified disconnect reason. The disconnect cause must be an integer from 0 through 2, for one of the following:

- REBOOTING(0)
- BUSY(1)
- DO_NOT_WANT_TO_TALK_TO_YOU(2)

rlf-template *rlf_template_name*

Specifies the RLF template to be associated with this Diameter peer.

rlf_template_name must be an alphanumeric string of 1 through 127 characters.

Important Rate Limiting Function (RLF) is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

Important Peer level RLF template takes precedence over the endpoint level template.

enable-snmp-traps

Enables the Diameter RLF related SNMP Traps. Skipping this keyword will disable sending of RLF related traps.

By default, the Diameter RLF related traps (“over-threshold”, “over-limit” and “normal-state”) notifications will not be enabled.

This keyword is meaningful only with a valid RLF template. As such, the command has the following meaning:

- **rlf-template** *rlf_template_name*: Use the RLF template. Disable traps if previously configured.
- **rlf-template** *rlf_template_name* **enable-snmp-traps** : Use the RLF template and enable traps.
- Skip the whole RLF template block from the peer configuration line to detach the RLF from the peer along with the traps.

sctp

Uses Stream Control Transmission Protocol (SCTP) for this peer.

+

Indicates that more than one of the previous keywords can be entered within a single command.

Usage Guidelines

Use this command to add a peer to the Diameter endpoint.

If the Diameter server side endpoint is catering to multiple peers, there has to be an entry for each peer in the peer list for that endpoint.

In cases where the client like GGSN does not use a diameter proxy, the peer list can be as large as the number of session managers on a GGSN. This might lead to a very complex configuration at the Diameter server endpoint.

To simplify the configurations, the Diameter server endpoint accepts a wildcarded peer name (with * as a valid wildcard character).

The client peers which satisfy the wild-carded pattern are treated as valid peers and the connection will be accepted. The new token 'wildcarded*' indicates that the peer name is wildcarded and any '*' in the preceding string should be treated as a wildcard.

For example, if the peer name is prefixed and suffixed with *ggsn* (* wildcard character) and an exact match is not found for the peer name portions peers like *0001-sessmgr.ggsn-gx*, *0002-sessmgr.ggsn-gx*, will be treated as valid peers at the Diameter server endpoint.

Example

The following command adds the peer named *test* with IP address *10.1.1.1* using port *126*:

```
peer test address 10.1.1.1 port 126
```

peer-backoff-timer

This command configures the time interval after which the Diameter peer will resume sending CCR-I messages to the PCRF server.

Product

GGSN

HA

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

```
peer-backoff-timer timeout [ send-app-level-term-req ]
{ default | no } peer-backoff-timer
```

default | no

Removes the configured peer backoff timer from Diameter endpoint configuration.

Default value of peer-backoff-timer is 7 seconds.

timeout

Specifies the peer backoff timeout duration in seconds, and must be an integer from 1 through 3600.

send-app-level-term-req

Sends termination request from application irrespective of whether or not the peer-backoff-timer is running.

Usage Guidelines

Use this command to configure a peer backoff timer which will be started when the server (primary or secondary PCRF) is busy. That is, the backoff-timer is started when the result code DIAMETER_TOO_BUSY (3004) is received from the PCRF. This PCRF is then marked as unavailable for the period configured by the backoff timer.

No CCR-I messages will be sent to the server until this timer expires. This timer will be per session manager level and will be applicable only to that instance.

Example

The following command sets the peer backoff timeout to *20* seconds:

```
peer-backoff-timer 20
```

reconnect-timeout

This command configures the time interval after which the Diameter peer will be reconnected automatically when DO_NOT_WANT_TO_TALK_TO_YOU disconnect cause is received.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

```
reconnect-timeout timeout
no reconnect-timeout
```

no

Disables auto reconnect of peer after receiving the disconnect cause "DO_NOT_WANT_TO_TALK_TO_YOU".

The default configuration is **no reconnect-timeout**. The connection to peer will not be retried until it is enabled by the administrator using the **diameter enable endpoint** command in the Exec mode.

timeout

Specifies the reconnect timeout duration in seconds, and the value must be an integer from 30 through 86400.

Usage Guidelines

Use this command to configure a timer which is started at the reception of the "DO_NOT_WANT_TO_TALK_TO_YOU" disconnect cause from the Diameter peer in Disconnect-Peer-Request message. After the timer expiry, the Diameter endpoint will automatically try to reconnect to the disconnected peer.

Currently in the system, the "DO_NOT_WANT_TO_TALK_TO_YOU " in the disconnect peer request is treated as an admin disable. Hence when the system gets into this state the connection will not be retried and the connection must be enabled by the administrator using the **diameter enable endpoint** command in the Exec mode.

Example

The following command sets the reconnect timeout to *100* seconds:

```
reconnect-timeout 100
```

response-timeout

This command configures the Response Timeout parameter. Response timeout specifies the maximum allowed response time for request messages sent from Diameter applications to Diameter server. On failure of reception of response for those request message within this specified time, this will be handled as failure by the corresponding applications and appropriate failure action will be initiated.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

response-timeout *timeout*
default response-timeout

default

Configures this command with the default setting.

Default: 60 seconds

timeout

Specifies the response timeout duration in seconds, and the value must be an integer from 1 through 300.

Usage Guidelines

Use this command to configure the Response Timeout parameter.

Example

The following command sets the response timeout to *100* seconds:

```
response-timeout 100
```

rlf-template

This command configures the RLF template to be used for the Diameter endpoint for throttling and rate control.

Important RLF template cannot be deleted if it is bound to any application (peers/endpoints).

Product

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

`[ no ] rlf-template` *`rlf_template_name`* **`[ enable-snmp-traps ]`**

no

Remove the specified RLF template from global configuration.

Important Do not use "**no rlf-template** *rlf_template_name*" in endpoint configuration mode. This CLI attempts to delete the specified RLF template. This CLI is part of global configuration, and not endpoint configuration.

rlf_template_name

The name of the RLF template to be used for Diameter endpoint configuration. *rlf_template_name* must be an alphanumeric string of 1 through 127 characters.

enable-snmp-traps

Enables the Diameter RLF related SNMP Traps. Skipping this keyword will disable sending of RLF related traps.

By default, the Diameter RLF related traps (“over-threshold”, “over-limit” and “normal-state”) notifications will not be enabled.

This keyword is meaningful only with a valid RLF template. As such, the command has the following meaning:

- **rlf-template** *rlf_template_name*: Use the RLF template. Disable traps if previously configured.
- **rlf-template** *rlf_template_name* **enable-snmp-traps** : Use the RLF template and enable traps.
- **no rlf-template** *rlf_template_name*: Detach the RLF from the endpoint along with traps.

Usage Guidelines

Use this command to configure the RLF Template to be used for the Diameter endpoint for throttling and rate control. This CLI command should be defined in the Diameter endpoint application to enable RLF module.

Important Rate Limiting Function (RLF) is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

Important This CLI command takes effect only if the RLF template is defined in the Global Configuration mode and the connection to the peer is open.

Currently in the deployment of the Diameter applications (Gx, Gy, etc.), many operators make use of "**max-outstanding** <*number*>" as a means of achieving some rate-limiting on the outgoing control traffic. With RLF in place, this is no longer required since RLF takes care of rate-limiting in all cases. If RLF is used and **max-outstanding** is also used, there might be undesirable results.

Important If RLF is being used with an "**diameter endpoint**", then set the **max-outstanding** value of the peer to be 255.

RLF provides only the framework to perform the rate limiting at the configured Transactions Per Second (TPS). The applications (like Diameter) should perform the configuration specific to each application.

For more information on this feature, refer to the *rlf-template* command in the *Global Configuration Mode Commands* chapter in this guide. For more information on RLF template configuration commands, refer to the *RLF Template Configuration Mode Commands* chapter in this guide.

Example

The following command configures an RLF template named *rlf_1* for Diameter endpoint:

```
rlf-template rlf_1
```

route-entry

This command creates an entry in the route table for Diameter peer.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

```
route-entry { [ host [ * ] host_name ] [ peer peer_id [ weight priority ] ] [
 realm [ * ] realm_name [ application credit-control peer peer_id ] [ weight
 value ] | peer peer_id [ weight value ] ] }
no route-entry { [ host [ * ] host_name ] [ peer peer_id ] [ realm [ * ]
realm_name { application credit-control peer peer_id | peer peer_id } ] }
```

no

Disables the specified route-entry table configuration.

host [*] *host_name*

Specifies the Diameter server's host name as an alphanumeric string of 1 through 63 characters. In 18.0 and later releases, the host name can additionally accept wildcard character (*). The support for wildcard entry is provided to allow routing of Diameter messages destined to any host @ any realm through the next-hop peer.

realm [*] *realm_name*

Specifies the realm name as an alphanumeric string of 1 through 127 characters. The realm may typically be a company or service name. In 18.0 and later releases, the realm name can additionally accept wildcard character (*). The support for wildcard entry is provided to allow routing of Diameter messages destined to any host @ any realm through the next-hop peer.

application credit-control

Specifies the credit control application — DCCA or RADIUS.

peer *peer_id*

Specifies the peer ID of the Diameter endpoint route as an alphanumeric string of 1 through 63 characters.

weight *priority*

Specifies the priority for a peer in the route table as an integer from 0 through 255. Default: 10

The peer with the highest weight is used. If multiple peers have the highest weight, selection is by round-robin mechanism.

Usage Guidelines

Use this command to create a route table for Diameter application.

When a Diameter client starts to establish a session with a realm/application, the system searches the route table for the best match. If an entry has no host specified, the entry is considered to match the requested value. Similarly, if an entry has no realm or application specified, the entry is considered to match any such requested value. The best match algorithm is to prefer specific matches for whatever was requested, either realm/application or host/realm/application. If there are no such matches, then system looks for route table entries that have wildcards.

Wildcard (*) based Diameter realm routing is supported in 18.0 and later releases. With this feature turned ON, the customers can avoid configuring individual Diameter peers and/or realms for all possible Diameter servers in their network.

The wild card Diameter routes can be statically configured under a Diameter endpoint configuration using the CLI "**route-entry realm * peer** *peer_name*".

These route entries are treated as default route entries to be used to send a message when there is no matching host@realm based or realm based route entry available.

The wild card Diameter route is added along with other realm based route entries in diabase. The wild card route entry will be selected to route a message only if the message's destination realm does not match with any of the other static realm based routes.

For example,

route-entry realm abc.com peer *peer1*

route-entry realm def.com peer *peer2*

route-entry realm * peer peer-default

If the message's destination realm is *abc.com* then the message will be routed to *peer1*. If the message's destination realm is *def.com* then the message will be routed to *peer2*. If the destination realm is *xyz.com* then the message will be routed to "*peer-default*".

When multiple wild card route entries are configured with same weights, then the routes are selected in a round robin fashion. When multiple wild card route entries are configured with different weights, then the route with the highest weight will be selected.

In case when there are multiple wild card routes with higher and equal weights and some routes with lower weights, then only the higher weight routes will be selected in round robin-fashion. The lower weight route can be selected only when the higher weight routes are not valid because of the peers being not in good state.

Example

The following command creates a route entry with the host name *dcca_host1* and peer ID *dcca_peer* with priority weight of *10*:

```
route-entry host dcca_host1 peer dcca_peer weight 10
```

route-failure

This command controls what action is performed for the route table after failure or recovery after failure.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

route-failure { deadtime *seconds* **| recovery-threshold percent** *percentage* **| result-code** *result_code* **| threshold** *counter* **}**

```
default route-failure { deadtime | recovery-threshold | threshold }
no route-failure result-code result_code
```

no

Disables the route-failure configuration.

default

Configures the default setting for the specified parameter.

deadtime *seconds*

Specifies the time duration (in seconds) for which the system keeps the route in FAILED status. When this time expires, the system changes the status to AVAILABLE.

seconds must be an integer from 1 through 86400. Default: 60

recovery-threshold percent *percentage*

Specifies the percentage value at which the failure counter is reset when provisionally changing the status from FAILED to AVAILABLE.

For example, if a failure counter of 16 caused the status to change to FAILED. After the configured deadtime expires, the status changes to AVAILABLE. If this keyword is configured with 75 percent, the failure counter will be reset to 12 (75 percent of 16).

percentage must be an integer from 1 through 99. Default: 90

result-code *result_code*

Configures which answer messages are to be treated as failures, in addition to requests that time out. Up to 16 different result codes can be specified.

result_code must be an integer from 0 through 4294967295.

threshold *counter*

Configures the number of errors that causes the status to become FAILED. The counter value must be an integer from 0 through 4294967295. Default: 16

The error counter begins at zero, and whenever there is a good response it decrements (but not below zero) or increments (but not above this threshold).

Usage Guidelines

Use this command to control how failure/recovery is performed for the route table. After a session is established, it is possible for the session to encounter errors or Diameter redirection messages that cause the Diameter protocol to re-use the route table to switch to a different route.

Each Diameter client within the chassis maintains counters relating to the status of each of its connections to different hosts (when the destination is realm/application without a specific host, the host name is kept as "", i.e., blank).

Moreover, those counters are further divided according to which peer is used to reach each host. Each Diameter client maintains a status of each peer-to-host combination. Under normal good conditions the status will be AVAILABLE, while error conditions might cause the status to be FAILED.

Only combinations that are AVAILABLE will be used. If none are AVAILABLE, then system attempts the secondary peer if failover is configured and system can find an AVAILABLE combination there. If nothing is AVAILABLE, the system uses a FAILED combination.

Example

The following command configures the time duration for route failure to *90* seconds:

```
route-failure deadtime 90
```

server-mode

This command configures the Diameter endpoint to establish the system as the server side endpoint of the connection.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

```
server-mode [ demux-mode ]
```

demux-mode

Specifies that the Diameter proxy is to use the demux manager to identify the appropriate session manager. If this keyword is not enabled, the proxy will route the request directly to a session manager.

Usage Guidelines

Use this command to configure the Diameter endpoint to establish this system as the server side endpoint of the connection. When the Diameter proxy receives an incoming request, the proxy identifies the endpoint for the request. If the system is in client mode, the proxy extracts the instance ID of the session manager which serves as the session-ID of the request. If this command is enabled, the extraction of the instance ID is disabled.

Example

The following command sets the system as the server side of the Diameter endpoint and instructs the Diameter proxy to use the demux manager to identify the appropriate session manager where the request is to be routed:

```
server-mode demux-mode
```

session-id include imsi

This command associates/disassociates a Stream Control Transmission Protocol (SCTP) parameter template with the Diameter endpoint.

This command has been added under the diameter endpoint configuration mode to include IMSI in Diameter session-ID per Diameter endpoint at Gx, Gy, and Gz (Rf). Configuration changes will be applicable only to new Sessions at Gx, Gy and Rf. Configuration changes will not have any impact on existing sessions behavior at Gx, Gy, and Rf. For Gy, multiple Diameter sessions can be initiated per subscriber and the session ID format setting will bind to the subscriber. The setting will be taken to effect when the first Diameter session is established and following Gy sub sessions will keep using the session ID format used in first session.

Product

All

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

```
session-id include imsi
[no] session-id include imsi
```

no

Disables this feature, that is, IMSI is not included in the Diameter Session-ID, which is the default behavior.

include

Includes configured information in Diameter Session-ID.

imsi

Includes International Mobile Subscriber Identification (IMSI) in Diameter Session-ID.

session-id

Describes Diameter Session-ID format.

Usage Guidelines

Use this command to include IMSI in Diameter session-ID per Diameter endpoint at Gx, Gy, and Gz (Rf).

Example

The following command includes IMSI in Diameter session-ID per Diameter endpoint at Gx, Gy, and Gz (Rf):

```
session-id include imsi
```

tls

This command enables/disables the Transport Layer Security (TLS) support between a Diameter client and Diameter server node.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-diameter)#`

Syntax Description

`tls { certificate` *`certificate`* **`| password`** *`password`* **`| privatekey`** *`private_key`* **`} default tls`**

default

Disables the TLS support at Diameter endpoint.

certificate *certificate*

Specifies the certificate for TLS support. The certificate must appear encrypted, and must be an alphanumeric string of 700 through 900 characters.

password *password*

Specifies the password for TLS support. The password must be encrypted, and must be an alphanumeric string of 6 through 50 characters.

privatekey *private_key*

Specifies the private key for TLS support. The private key must be encrypted, and must be an alphanumeric string of 900 through 1500 characters.

Usage Guidelines

Use this command to configure TLS support between a Diameter client and Diameter server node. By default, TLS is disabled.

Important

Both the Diameter client and server must be configured with TLS enabled or TLS disabled; otherwise, the Diameter connection will be rejected.

Example

The following commands enable the TLS between a Diameter client and Diameter server node:

tls certificate "-----BEGIN CERTIFICATE-----

\nMIICGDCCAYECAgEBMA0GCSqGSIb3DQEBBAUAMFcxCzAJBgNVBAYTAlVTMRMwEQYD
\nVQQKEwpSVEZNLCBJbmMuMRkwFwYDVQQLExBXaWRnZXRzIERpdmlzaW9uMRgwFgYD
\nVQQDEw9UZXN0IENBMjAwMTA1MTcwHhcNMDEwNTE3MTYxMDU5WhcNMDQwMzA2MTYx
\nMDU5WjBRMQswCQYDVQQGEwJVUzETMBEGA1UEChMKUlRGTSwgSW5jLjEZMBcGA1UE
\nCxMQV2lkZ2V0cyBEaXZpc2lvbjESMBAGA1UEAxMJbG9jYWxob3N0MIGfMA0GCSqG
\nSIb3DQEBAQUAA4GNADCBiQKBgQCiWhMjNOPlPLNW4DJFBiL2fFEIkHuRor0pKw25
\nJ0ZYHW93lHQ4yxA6afQr99ayRjMY0D26pH41f0qjDgO4OXskBsaYOFzapSZtQMbT\n
+1oOLomgRxJomIFgW1RyUUkQP1n0hemtUdCLOLlO7Q\nCPqZLQIDAQABMA0GCGx
SqGSIb3DQEBBAUAA4GBAIumUwl1OoWuyN2xfoBHYAs+lRLY\nKmFLoI5+iMcWIsksm
A+b0FLRAN43wmhPnums8eXgYbDCrKLv2xWcvKDP3mps7m\nAMivwtu/eFpYz6J8
Mo1fsV4Ys08A/uPXkT23jyKo2hMu8mywkqXCXYF2e+7pEeBr\ndsbmkWK
5NgoMl8eM\n-----END CERTIFICATE-----\n"
tls privatekey BEGIN RSA PRIVATE KEY-----\nProc-Type: 4,ENCRYPTED\nDEK-Info:
DES-EDE3-CBC,5772A2A7BE34B611\n\n1yJ+xAn4MudcIfXXy7ElYngJ9EohIh8yvcy
VLmE4kVd0xeaL/Bqhvk25BjYCK5d9\nk1K8cjgnKEBjbC++0xtJxFSbUhwoKTLwn+s
BoJDcFzMKkmJXXDbSTOaNr1sVwiAR\nSnB4lhUcHguYoV5zlRJn53ft7t1mjB6Rw
GH+d1Zx6t95OqM1lnKqwekwmotVAWHj\nncu3N8qhmoPMppmzEv0fOo2/pK2
WohcJykSeN5zBrZCUxoO0NBNEZkFUcVjR+KsA\n1ZeI1mU60szqg+AoU/XtFcow
8RtG1QZKQbbXzyfbwaG+6LqkHaWYKHQEI1546yWK\nus1HJ734uUkZoyyyazG
6PiGCYV2u/aY0i3qdmyDqTvmVIvve7E4glBrtDS9h7D40\nnPShIvOatoPzIK
4Y0QSvrI3G1vTsIZT3IOZto4AWuOkLNfYS2ce7prOreF0KjhV0\n3tggw9pHd
DmTjHTilkXqheZxZ7TVu+pddZW+CuB62I8lCBGPW7os1f21e3eOD/oY\nYPCI44a
JvgP+zUORuZBWqaSJ0AAIuVW9S83Yzkz/tlSFHViOebyd8Cug4TlxK1VI\nq6hbSafh
4C8ma7YzlvqjMzqFifcIolcbx+1A6ot0UiayJTUra4d6Uc4Rbc9RIiG0\njfDWC6aii9YkAg
Rl9WqSd31yASge/HDqVXFwR48qdlYQ57rcHviqxyrwRDnfw/lX\nMf6LPiDKEco
4MKej7SR2kK2c2AgxUzpGZeAY6ePyhxbdhA0eY21nDeFd/RbwSc5s\neTiCCMr41OB
4hfBFXKDKqsM3K7klhoz6D5WsgE6u3lDoTdz76xOSTg==\n-----END RSA PRIVATE KEY-----\n"
tls password TLSpassword_3B167E

use-proxy

This command enables/disables Diameter proxy for the Diameter endpoint. By default this command is disabled.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

```
use-proxy [ server-mode [ demux-mode ] ]
no use-proxy
```

no

Disables Diameter proxy for the current endpoint.

This command at endpoint level will equip an application to use Diameter proxy to route all its messages to an external peer.

server-mode

Specifies that the Diameter endpoint to establish the Diameter proxy as the server side endpoint of the connection.

demux-mode

Specifies that the Diameter endpoint to establish the Diameter proxy to use the Demux manager to identify the appropriate session manager. If this keyword is not enabled, the proxy will route the request directly to a session manager.

IPCF uses BindMux to identify the appropriate session manager.

Usage Guidelines

Use this command to establish a Diameter proxy to route all its messages to an external peer. The proxy acts as an application gateway for Diameter. It gets the configuration information at process startup and decides which Diameter peer has to be contacted for each application. It establishes the peer connection upon finding no peer connection already exists.

IPCF uses Bindmux as a Demux manager to help distribute new incoming sessions across available Sessmgrs on the system.

All the incoming Diameter requests/responses land on Diamproxy. Diamproxy checks if a Sessmgr is already serving this session based on parameters like session-id and peer-id of the request/response.

If no Sessmgr is allocated to the request and the Demux mode is ON, the DiamProxy forwards the new request to Demux/Bindmux for sessmgr allocation. Demux/Bindmux has updated information about the load on all the Sessmgrs and assigns the optimal Sessmgr to the Diameter session. Once a Sessmgr is allocated for the session, a mapping of session-id to Sessmgr is added at Diamproxy. All further requests for this session will be directly routed to Sessmgr.

Each proxy task will automatically select one of the host names configured with the **origin host** command. Multiple proxy tasks will not use the same host names, so there should be at least as many host names as proxy tasks. Otherwise, some proxy tasks will not be able to perform Diameter functionality. The chassis automatically selects which proxy tasks are used by which managers (i.e., ACSMgrs, Sessmgrs), without verifying whether the proxy task is able to perform Diameter functionality.

To be able to run this command, the Diameter proxy must be enabled. In the *Global Configuration Mode Commands* chapter, see the description of the **require diameter-proxy** command.

In 17.0 and later releases, when a PCEF is connected to OCS via multiple Diameter proxies, PCEF will choose the same Diameter proxy for the subsequent messages as long as it is available. Any subsequent messages (CCR-U/CCR-T) to the same host are sent via the same peer. Once the next-hop is chosen via round-robin method, the subsequent message for the session is sent to the same next-hop (peer).

In releases prior to 18.0, when the chassis is in standby state, all the Diameter proxies are stopped. In18.0 and later releases, all the Diameter proxies will be running even when the chassis is in standby mode. Any change in ICSR grouping mask will lead to stopping and restarting of all the diamproxies on the standby chassis.

Example

The following command enables Diameter proxy for the current endpoint:

```
use-proxy
```

The following command disables Diameter proxy for the current endpoint:

```
no use-proxy
```

vsa-support

This command allows DIABASE to use vendor IDs configured in the dictionary for negotiation of the Diameter peers' capabilities regardless of the supported vendor IDs received in Capabilities-Exchange-Answer (CEA) messages.

Product

GGSN

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

```
vsa-support { all-from-dictionary | negotiated-vendor-ids }
default vsa-support
```

default

Configures this command with the default setting.

Default: **negotiated-vendor-ids**

all-from-dictionary

Allows DIABASE to use the vendor IDs from the dictionary as indicated in the Capabilities-Exchange-Request (CER) messages from Diameter peers.

negotiated-vendor-ids

Allows DIABASE to use the supported vendor IDs satisfying capability negotiation.

Usage Guidelines

Use this command to set DIABASE to use the vendor IDs from the dictionary or use the vendor IDs satisfying the capabilities negotiation.

Example

The following command enables DIABASE to use the vendor IDs specified in the dictionary:

```
vsa-support all-from-dictionary
```

watchdog-timeout

This command configures the Watchdog Timeout parameter.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax Description

watchdog-timeout *timeout*
{ default | no } watchdog-timeout

no

Disables the watchdog timeout configuration.

default

Configures this command with the default setting.

Default: 30 seconds

timeout

Specifies the timeout duration (in seconds) as an integer from 6 through 30.

Usage Guidelines

Use this command to configure the Watchdog Timeout parameter for the Diameter endpoint. If this timer expires before getting a response from the destination, other route to the same destination is tried, as long as the retry count setting has not exceeded (see the CLI command) and as long as the response timer has not expired (see the CLI command).

If the watchdog timer expires, the gateway sends the heartbeat message to Diameter endpoint. The timer is allowed to have the value up to a maximum of +2 or -2 seconds from the configured value.

Example

The following command sets the watchdog timeout setting to *15* seconds:

```
watchdog-timeout 15
```