

Policy Builder Configuration

- Plug-in Configuration, on page 1
- Diameter Application, on page 26
- Routing AVP Definition, on page 33
- Custom Reference Data Tables, on page 37

Plug-in Configuration

Cisco Policy Builder provides core plug-ins for customizing and optimizing your installation.

- Configurations set at the system level are system-wide except as noted in the bullet items below.
- Configurations set at the cluster level apply to that cluster and the instances in it. A value set here overrides the same value set at the system level.
- Configurations set at the instance level apply to the instance only and override the same value set at the cluster or system level.

Select the **Create Child** action in a **Plug-in Configuration** node in the **Systems** tree to define them. You can change any of the variables from the default, or choose not to use a plug-in, as necessary.

When you create a system from the example, the following configuration stubs appear at the cluster and instance level:

Figure 1: Create Child Action

Systems	Plugin Configurations Summary	
Summary		
🕨 🌄 lab	▼ Actions	
🛛 😡 default	Create Child:	
🔁 Plugin Configurations	Threading Configuration	
Account Balance Templates	Async Threading Configuration	
Custom Reference Data Tables	Portal Configuration	
Diameter Agents	Customer Reference Data Configuration	
Diameter Clients	Ldap Configuration	
Diameter Defaults	Balance Configuration	
Fault List	Diameter Configuration	
Ldap Server Sets	Unified API Configuration	
Notifications	Notification Configuration	
Policy Enforcement Points		
RADIUS Service Templates	Voucher Configuration	
Subscriber Data Sources	RADIUS Configuration	
Tariff Times	ISG Prepaid Configuration	
Tariff Times	USuM Configuration	
	Audit Configuration	

Threading Configuration

A threading configuration utility is provided for advanced users.

Click **Threading Configuration** in the right pane to add the threading configuration to the system. If you are planning to run the system with higher TPS, then you need to configure Threading Configuration. For further information, contact your Cisco Technical Representative.

The Threading Plug-in controls the total number of threads in CPS vDRA that are executing at any given time.

The following parameters can be configured under Threading Configuration:

Table 1: Threading Configuration Parameters

Parameter	Description
Thread Pool Name	Name of the thread pool. Following names can be configured in CPS vDRA: • broadhop-bindings • broadhop-slf • broadhop-receivers
Threads	• broadhop-qprocessor Number of threads to set in the thread pool.

Parameter	Description
Queue Size	Size of the queue before they are rejected.
Scale By Cpu Core	Select this check box to scale the maximum number of threads by the processor cores.

Async Threading Configuration

Click Async Threading Configuration in the right pane to add the configuration in the system.

Use the default values for the Async Threading Plug-in. The Async configuration controls the number of asynchronous threads.



Note Currently, CPS vDRA does not have any asynchronous threads. However, you must add "Async Threading Configuration" and keep this table empty.

The following parameters can be configured under Async Threading Configuration.

Table 2: Async Threading Configuration

Parameter	Description
Default Processing Threads	The number of threads that are allocated to process actions based on priority.
Default Action Priority	The priority assigned to an action if it is not specified in the Action Configurations table.
Default Action Threads	The number of threads assigned to process the action if it is not specified in the Action Configurations table.
Default Action Queue Size	The number of actions that can be queued up for an action if it is not specified in the Action Configurations table.
Default Action Drop Oldest When Full	When checked, the oldest queued action is dropped from the queue when a new action is added to a full queue. Otherwise, the new action to add is ignored. This check box applies to all the threads specified. To drop a specific thread, leave this unchecked and use the Action Configurations table.
Action Configurations Ta	able
Action Name	The name of the action. This must match the implementation class name.
Action Priority	The priority of the action. Used by the default processing threads to determine which action to execute first.
Action Threads	The number of threads dedicated to processing this specific action.
Action Queue Size	The number of actions that can be queued up.

Parameter	Description
Action Drop Oldest When Full	For the specified action only: When checked, the oldest queued action is dropped from the queue when a new action is added to a full queue. Otherwise, the new action to add is ignored.

Custom Reference Data Configuration

Before you can create a custom reference data table, configure your system to use the Custom Reference Data Table plug-in configuration.

You only have to do this one time for each system, cluster, or instance. Then you can create as many tables as needed.

Click Custom Reference Data Configuration from right pane to add the configuration in the system.

Figure 2: Custom Reference Data Configuration

*Primary Database IP Address	Secondary Databa	se IP Address
localhost		
*Database Port	*Db Read Preferer	ice
27717	Primary	*
*Connection Per Host		
100	1°	

Here is an example for HA and AIO setups:

- HA example:
 - Primary Database Host/IP Address: sessionmgr01
 - Secondary Database Host/IP Address: sessionmgr02
 - Database Port: 27717
- AIO example:
 - Primary Database Host/IP Address: localhost or 127.0.0.1
 - Secondary Database Host/IP Address: NA (leave blank)
 - Database Port: 27017

The following parameters can be configured under Custom Reference Data Configuration.

Parameter	Description
Primary Database IP Address	IP address of the primary sessionmgr database.
Secondary Database IP Address	Optional, this field is the IP address of a secondary, backup, or failover sessionmgr database.
Database Port	Port number of the sessionmgr. It should be the same for both the primary and secondary databases.
Db Read Preference	Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list:
	• Primary: Default mode. All operations read from the current replica set primary.
	• PrimaryPreferred: In most situations, operations read from the primary but if it is unavailable, operations read from secondary members.
	• Secondary: All operations read from the secondary members of the replica set.
	• SecondaryPreferred: In most situations, operations read from secondary members but if no secondary members are available, operations read from the primary
	For more information, refer to http://docs.mongodb.org/manual/core/ read-preference/.
Connection Per Host	Number of connections that are allowed per DB Host.
	Default value is 100.

Table 3: Custom Reference Data Configuration

For more information on Custom Reference Data configuration, refer to the CPS Operations Guide for this release.

DRA Configuration

Click DRA Configuration from the right pane in Policy Builder to add the configuration in the system.

I

Figure 3: DRA Configuration

*Stale Session Timer Minutes	Rate Limiter
1	10
Stale Session Expiry Count	*Binding DB Read Preference
6	Nearest
Stale Binding Expiry Minutes	Stale Binding Refresh Minutes
10080 Binding DB Retries Binding Creation, Primary Alt	2880 rernate System
Binding DB Retries	
Binding DB Retries	ernate System
Binding DB Retries Binding Creation, Primary Alt Binding Creation, Secondary	ernate System Alternate System
Binding DB Retries Binding Creation, Primary Alt	ernate System Alternate System
Binding DB Retries Binding Creation, Primary Alt Binding Creation, Secondary	ernate System Alternate System

The following parameters can be configured under DRA Configuration:

Table 4: DRA Configuration Parameters

Parameter	Description
Stale Session Timer Minutes	Indicates the time after which the audit RAR should be generated (in the subsequent audit RAR process cycle that runs every minute in CPS vDRA) for sessions that are stale.
	Default: 180 minutes (recommended value)
	Minimum: 10 minutes
	Maximum: 10080 minutes
Rate Limiter	Indicates the number of audit RARs per second that should be sent out by CPS vDRA.
	For example, if there are 100 stale sessions found in the audit RAR process, but the Rate Limiter is configured as 10, then audit RARs are generated at 10 RAR/sec for the next 10 seconds.
	Default: 10 (recommended value)
	Minimum: 1
	Maximum: 1000 (maximum number of RAR messages per second from vDRA to PCEF)

Parameter	Description
Stale Session Expiry Count	Specifies the number of retries vDRA should do for a stale session if there is no response of audit RAR or if there is Result-Code in RAA (for audit RAR) other than 5002 or 2001.
	Default: 6 (recommended value)
	Minimum: 0 (Session deleted without sending RAR)
	Maximum: 10
Binding DB Read Preference	Used to select the mode when reading from Binding DB. Use "nearest" mode for better performance of traffic that needs only read operation on Binding DB.
	Default: Nearest (recommended setting)
Stale Binding Expiry Minutes	Duration after which the binding database records expire.
	The timer is initialized when the session is created.
	The records are deleted when the time since the last refresh exceeds Stale Binding Refresh Minutes.
	Default: 10080 minutes (168 hours or one week) (recommended value)
	Minimum: 10 minutes
	Maximum: 43200 minutes (28 days)
	For more information about binding DB audits and stale records, see Binding DB Audit, on page 11.
Stale Binding Refresh Minutes	Duration for which the expiry time of the binding database records is refreshed.
	Default: 2880 minutes (48 hours or 2 days - recommended value).
	Minimum: 10 minutes
	Maximum: 10080 minutes (one week)
	Note Stale Binding Expiry Minutes should be multiple of Stale Binging Refresh Minutes.
	Stale Binding Refresh Minutes should be greater than Stale Session Timer Minutes.

I

Parameter	Description
Binding Creation, Primary Alternative System	Name of vDRA system to retry Gx CCR-i
	When vDRA tries to route a Gx CCR-i request, but is unable to reach the database, the configured values of first the primary, then the secondary systems are used to route the Gx CCR-i to a different vDRA to try the database.
	The retry is stopped if that vDRA also cannot reach the database.
Binding Creation, Secondary Alternative System	Name of secondary vDRA system to retry Gx CCR-i
Binding Routing, Primary Alternative System	Name of vDRA system to retry Rx AAR
	When vDRA tries to route a Rx AAR request, but is unable to reach the database, the configured values of first the primary, then the secondary systems are used to route the Rx AAR to a different vDRA to try the database.
	The retry is stopped if that vDRA also cannot reach the database.
Binding Routing, Secondary Alternative System	Name of secondary vDRA system to retry Rx AAR
Settings	Refer to Settings.
Rate Limits	Refer to Rate Limits.
DRA Feature	Refer to DRA Feature.
DRA Inbound Endpoints	Refer to DRA Inbound Endpoints, on page 16.
DRA Outbound Endpoints	Refer to DRA Outbound Endpoints, on page 18.
Relay Endpoints	Refer to Relay Endpoints, on page 20.

Settings

Click Settings check box to open the configuration pane. An example configuration is shown below:

Settings	
*Stop Timeout Ms	
10000	
*Cea Timeout Ms	
10000	
*Iac Timeout Ms	
5000	
*Dwa Timeout Ms	
10000	
*Dpa Timeout Ms	
5000	
*Rec Timeout Ms	
10000	

The following parameters can be configured under Settings:

Table 5: DRA Configuration - Settings Parameters

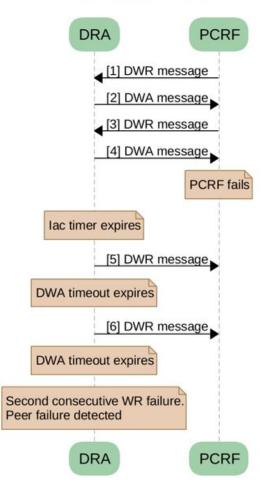
Parameter	Description
Stop Timeout Ms	Determines how long the stack waits for all resources to stop. The delay is in milliseconds.
	Default: 10000 ms (recommended value)
	Minimum: 1000 ms
	Maximum: 60000 ms (one minute)
Cea Timeout Ms	Determines how long it takes for CER/CEA exchanges to timeout if there is no response. The delay is in milliseconds.
	Default: 10000 ms (recommended value)
	Minimum: 1000 ms
	Maximum: 60000 ms (one minute)

Parameter	Description
Iac Timeout Ms	Determines how long the stack waits before initiating a DWR message exchange on a peer connection from which no Diameter messages have been received. The timeout value is in milliseconds.
	Default: 5000 ms (recommended value)
	Minimum: 1000 ms
	Maximum: 30000 ms (30 seconds)
Dwa Timeout Ms	Determines how long the stack waits for a DWA message in response to a DWR message. If no Diameter message (DWA or other message) is received on the peer connection during the first timeout period, the stack counts a failure, sends another DWR message, and restarts the Dwa timer. If no Diameter messages are received during the second timeout period, the stack counts a second failure. After two consecutive failures, the stack considers the peer connection as failed, and closes the connection.
	The delay is in milliseconds.
	Default: 10000 ms (recommended value)
	Minimum: 1000 ms
	Maximum: 60000 ms (one minute)
Dpa Timeout Ms	Determines how long it takes for a DPR/DPA exchange to timeout if there is no response. The delay is in milliseconds.
	Default: 5000 ms (recommended value)
	Minimum: 1000 ms
	Maximum: 30000 ms (30 seconds)
Rec Timeout Ms	Determines how long it takes for the reconnection procedure to timeout. The delay is in milliseconds.
	Default: 10000 ms (recommended value)
	Minimum: 1000 ms
	Maximum: 60000 ms (one minute)

The following figure illustrates the timers in peer detection:

Figure 5: vDRA Peer Detection Failure

DRA Peer Detection Failure



Binding DB Audit

The Binding DB Audit automatically deletes stale records from the binding DBs. When a Gx session record is created, binding records for the session binding keys are also created. When each binding record is created, the binding record expiry time is initialized to the sum of the session creation time and the Stale Binding Expiry Minutes (that you can configure in Policy Builder). A binding record is considered stale if it cannot be deleted when its associated session record is deleted (this occurs typically due to communication failures). The binding records are audited via a binding audit background process. If the audit process finds a binding record that is past the expiry time, the binding record is considered stale and deleted from the database. Note that the binding audit process does not perform a session DB lookup nor does it perform any Diameter signaling with the GW before deletion.

To prevent a binding record from becoming stale, the session audit process periodically updates the expiry time for bindings associated with sessions in the session DB. The session maintains a stale binding refresh timer that is initialized to the sum of the session creation time and Stale Binding Refresh Minutes. When the session audit process finds a session with a refresh time that has passed, it updates a new expiry time (calculated from current time plus the Stale Binding Expiry Minutes) to its associated bindings. The write is conditional

on the session-id matching the Gx session-id in the binding record. This refresh action prevents the binding audit process from incorrectly deleting active bindings from its binding database. The following figures illustrate the working of binding DB audit and refresh:

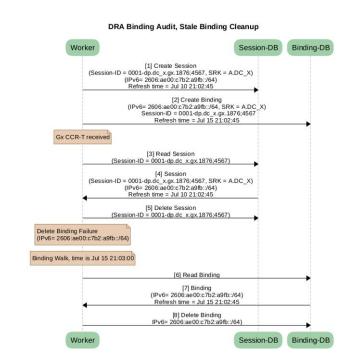
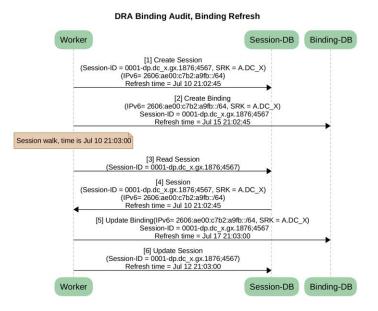


Figure 6: Binding DB Audit





Rate Limits

Rate limit per process instance on Policy Director (lb) VM can be managed using this configuration.

Default is unchecked, that is, no rate limits for Diameter traffic (recommended setting).

If enabled, the following parameters can be configured under Rate Limits:

Table 6: DRA Configuration - Rate Limits

Parameter	Description			
Rate Limit per Instance on Policy Director	Allowable TPS on a single instance of policy serve (QNS) process running on the Policy Director.			
	Minimum: 1			
	Maximum: 5000			
	Note Contact your Cisco representative for usecase-specific recommended values.			
Result-Code in Response	Indicates the error code that must be used while rejecting requests, due to rate limits being reached.			
	Default: 3004			
Error Message in Response	Select the check box to drop the rate-limited messages without sending error response.			
	If the check box is not selected, then the rate limited message are dropped with error response as configured.			
Drop Requests Without Error Response	Select the check box to drop rate limited messages without sending error response.			
	If the check box is unchecked, then the rate limited messages are dropped with error response as configured.			
	To accommodate configuration to either drop the request or send an error response, a column <i>Discard Behavior</i> can be added under Peer Rate Limit Profile. The column may have one of the two possible values:			
	Send Error Response			
	Drop Message			
	Default: Unchecked (recommended setting)			
	For more information, refer to Peer Rate Limit.			
	Important If both Rate Limit Error Code and Rate Limit Error String are provided along with Rate Limit Action as "Drop Message", the Rate Limit Action will take precedence and the other two fields will be ignored.			

Here is the list of the available combinations for rate limiting:

Rate Limiting Type	With Error Code	With Error Code and Error Message	Without Error Code (Drop	
Instance Level	Yes	Yes	Yes	
Peer Level Egress	Yes	Yes	Yes	
Peer Level Egress with Message Level	Yes	Yes	Yes	
Egress Message Level (No Peer Level RL)	Yes	Yes	Yes	
Peer Level Ingress	Yes	Yes	Yes	
Peer Level Ingress with Message Level	Yes	Yes	Yes	
Ingress Message Level (No Peer Level RL)			Yes	

Table 7: Rate Limiting Combinations

DRA Feature

Click **DRA Feature** check box to open the configuration pane.

Figure 8: DRA Configuration - DRA Feature

D R A Feature	
Gx Session Tear Down On5065	
✔ Update Time Stamp On Success R A A	
Update Time Stamp On Success C C R U	

The following parameters can be configured under DRA Feature:

Table 8: DRA Features

Parameter	Description		
Gx Session Tear Down On5065	By default, Gx Session Tear Down On5065 flag is enabled (recommended setting).		
	When the PCRF responds with a Experimental Result Code of 5065 in AAAnswer on Rx Interface, DRA deletes its internal binding and session created for the transaction.A RAR with appropriate Session-Release-Cause AVP will also be sent to the PCEF.		
	Important When using this flag, there will always be a database query to fetch Gx session id. So this means that the database transactions will linearly increase with AAR traffic on Rx Interface.		
Update Time Stamp On Success RAA	When this check box is selected, session timestamp will be updated on receipt of success RAA (Result-Code: 2001) from PCEF. $\frac{1}{2}$		
	Default is checked (recommended setting)		
	Important When using this flag, there will always be a database query to fetch Gx session id. So this means that the database transactions will linearly increase with AAR traffic on Rx Interface.		
Update Time Stamp On Success CCRU	When this check box is selected, session timestamp will be updated on receipt of success CCR-U (Result-Code: 2001) from PCEF. $\frac{2}{}$		
	Default is unchecked (recommended setting)		
	Important When using this flag, there will always be a database query to fetch Gx session id. So this means that the database transactions will linearly increase with AAR traffic on Rx Interface.		
Enable Proxy Bit Validation	Enables P bit validation.		
	vDRA validates the P bit in the Diameter request and, if set, the message maybe proxied, relayed, or redirected.		
	If this option is disabled, the P bit in the request is not checked and the request is not considered proxiable.		
	Default: Enabled.		

Parameter	Description			
Enable Mediation	Enable advanced mediation capabilities in both egress and ingress direction.			
	This feature allows you to configure vDRA to change the value of the Result-Code in Diameter Answer, use mediation to hide topology, prepend label to Destination Host AVP, etc.			
Enable Doic	Enable or disable abatement action for Diameter requests towards PCRF, HSS, AAA, and OCS servers based on reporting of overloaded conditions using the architecture described in RFC 7683 Diameter Overload Indication Conveyance (DOIC).			
	DOIC can be enabled/disabled at peer group level in Peer Group SRK Mapping table. If the destination peer is congested or overloaded, you can choose to either forward, divert, or drop messages.			
Slf Max Bulk Provisioning TPS	Rate at which subscribers are provisioned in the SLF database.			
	SLF bulk provisioning generates high number of database write operations in a short duration of time. To spread out the operations over a period of time and mitigate the performance issue, configure the TPS. The rate limit adds delay between transactions and thereby limits the number of transactions executed per second.			
	For more information about SLF bulk provisioning, see the <i>CPS vDRA Operations Guide</i> .			

- ¹ The time stamp will be updated on generation of Stale RAR. Also, if a success RAR/RAA(2001) comes after generation of Stale RAR, then the Stale RAR counter will be reset.
- ² The time stamp will be updated on generation of Stale RAR. Also, if a success CCR(U)/CAA(2001) comes after generation of Stale RAR, then the Stale RAR counter will be reset.

DRA Inbound Endpoints

The following parameters can be configured under DRA Inbound Endpoints:

Table 9: DRA Configuration - DRA Inbound Endpoints Parameters

Parameter	Description
Vm Host Name	Host Name of the VM that hosts this CPS vDRA endpoint.
Ip Address	Address on which this CPS vDRA endpoint should bind to.
Realm	Realm of the CPS vDRA endpoint.

Parameter	Description
Fqdn	Fully Qualified Domain Name of the CPS vDRA end point.
Transport Protocol	Allows you to select either 'TCP' or 'SCTP' for the selected DRA endpoint.
	Default value is TCP.
	If the DRA/relay endpoint is to be configured for SCTP, the Transport Protocol should be selected as SCTP for those endpoints.
Multi-Homed IPs	This is a comma separated list of IP addresses that CPS vDRA will use to start the diameter stack with multi-homing enabled for SCTP transport. Diameter stack with TCP transport will still use the existing 'Local Bind Ip' field to specify any specific IP address for TCP stack.
	CPS vDRA will use the 'Local Bind Ip' to bring up SCTP stack and use it along with the 'Multi Homing Hosts' to start the SCTP transport with multi-homing support.
	Note While using SCTP multi-homing functionality review the Linux network and gateway configurations for supporting multiple networks on different subnets. CPS supports Centos 6 release and reverse path filtering kernel parameter (rp_filter) values can be set for allowing packets from different subnets on Policy Director VMs. The default behavior in Centos 6 is to discard the packets in such scenarios.
	Note Both IPv4 and IPv6 are supported in vDRA endpoint configuration. For IPv6, you can enter either short or long format.
	The configuration for multi-homing is validated by netstat command on lb01:
	netstat -apn grep 3898
Application	Refers to 3GPP Application ID of the interface.
	You can select multiple applications on a peer connection.
	For example, S6a and SLg on a single IPv4/SCTP Multi-homed peer connection.
Enabled	Check to enable the endpoint.

Parameter	Description
	Refers to the port on which the CPS vDRA listens for incoming connections.

An example configuration is shown below:

Figure 9: DRA Inbound Endpoints - Example Configuration

*Vm Host Name	*Ip Address	*Realm	*Fqdn	Transport Protocol	Multi-Homed IP's	*Application	*Enabled	*Base Port	
lab	10.1.1.1	gx-dra1.cisco.com	gx-dra1	TCP		Gx Application		3868	
ab	10.1.1.1	gx-dra2.cisco.com	gx-dra2	TCP		Gx Application		3869	
ab	10.1.1.1	gx-dra3.cisco.com	gx-dra3	TCP		Gx Application	\checkmark	3870	=
ab	10.1.1.1	rx-dra1.cisco.com	rx-dra1	TCP		Rx Application		4868	
ab	10.1.1.1	rx-dra2.cisco.com	rx-dra2	TCP		Rx Application		4869	
lah	10 1 1 1	sd-dra1 cisco com	sd-dra1	TCP		Sd Application		6868	-

DRA Outbound Endpoints

The following parameters can be configured under DRA Outbound Endpoints:

Table 10: DRA Configuration - DRA Outbound Endpoints Parameters

Parameter	Description
Vm Host Name	Host Name of the VM that hosts this CPS vDRA endpoint.
Ip Address	Address on which this CPS vDRA endpoint should bind to.
Realm	Realm of the CPS vDRA endpoint.
Fqdn	Fully Qualified Domain Name of the CPS vDRA end point.
Transport Protocol	Allows you to select either 'TCP' or 'SCTP' for the selected CPS vDRA endpoint.
	Default value is TCP.
	If the DRA/relay endpoint is to be configured for SCTP, the Transport Protocol should be selected as SCTP for those endpoints.

Parameter	Description
Multi-Homed IPs	This is a comma separated list of IP addresses that CPS vDRA will use to start the diameter stack with multi-homing enabled for SCTP transport. Diameter stack with TCP transport will still use the existing 'Local Bind Ip' field to specify any specific IP address for TCP stack.
	CPS vDRA will use the 'Local Bind Ip' to bring up SCTP stack and use it along with the 'Multi Homing Hosts' to start the SCTP transport with multi-homing support.
	NoteWhile using SCTP multi-homing functionality review the Linux network and gateway configurations for supporting multiple networks on different subnets. CPS supports Centos 6 release and reverse path filtering kernel parameter (rp_filter) values can be set for allowing packets from different subnets on Policy Director VMs. The default behavior in Centos 6 is to discard the packets in such scenarios.
	Note Both IPv4 and IPv6 are supported in vDRA endpoint configuration. For IPv6, you can enter either short or long format.
	The configuration for multi-homing is validated by netstat command on lb01:
Application	Refers to 3GPP Application ID of the interface.
Enabled	Check to enable the endpoint.
Peer Realm	Diameter server realm.
Peer Host	Diameter server host. By default, the connection is initiated on the standard diameter port (3868). If a different port needs to be used than the peer name must be defined using the host:port format.

An example configuration is shown below:

Figure 10: DRA Outbound Endpoints - Example Configuration

*Vm Host Name	*Ip Address	*Realm	*Fqdn	Transport Protocol	Multi-Homed IP's	*Application	*Enabled	*Peer Realm	*Peer Host
lab	10.1.1.1	gx-dra1.cisco.com	gx-dra9	TCP		Gx Application		pcrf2-gx2.cisco.com	gx-pcrf
lab	10.1.1.1	rx-dra1.cisco.com	rx-dra9	ТСР		Rx Application		rx-pcrf.cisco.com	rx-pcrf:4868

Relay Endpoints

The following parameters can be configured under Relay Endpoints:

Table 11: DRA Configuration - Relay Endpoints Parameters

Parameter	Description
Vm Host Name	Host Name of the VM that hosts this Relay endpoint.
Instance Id	Instance Identifier is the ID of the current Instance.
Ip Address	Address on which this DRA endpoint should bind to.NoteThe relay endpoints must be configured on physical IPs and not on virtual IPs.
Port	Port is the listening port for this instance.
Fqdn	Fully Qualified Domain Name of the DRA end point.
Enabled	Check to enable endpoint.

An example configuration is shown below:

Figure 11: Relay Endpoints - Example Configuration

*Vm Host Name	*Instance Id	*Ip Address	*Port	*Fqdn	*Enabled
lab	3	10.10.1.1	4868	dra3.rx	

Policy Routing for Real IPs with Relay Endpoints

vDRA relay links consist of a control plane and a data plane.

The control plane uses virtual IPs and the data plane uses real IPs.

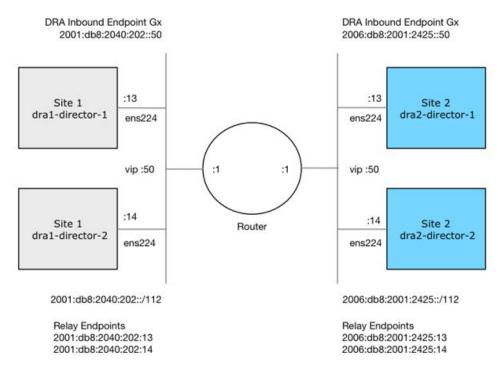
If the control and data plane use the same links, and those links are configured with VIPs, by default, the data plane uses the VIP as its source address for outgoing connections. The data plane uses the VIP as the source address only if the VIP is active on the data plane's outgoing interface.

To avoid this situation, policy routing is used to force the data plane to use the real IP address of the outgoing interface instead of the VIP.

Example of a vDRA Relay Endpoints

In the following example network, only the DRA director VMs and their relay links are displayed. In a real scenario, many more links may exist on the DRA director VMs.

Figure 12: Example of Relay Endpoints



Policy Routing

Linux policy routing includes rules and routing tables. The rules identify traffic and point to a user-defined routing table. The routing table contains customized routes.

To prevent the Relay Link's data plane from using the VIP as a source address, a rule is created to identify the real IP in the destination address and identify the desired routing table.

Configure Policy Routing

The following configuration procedure is performed on Site 1 dra1-director-1. Repeat the procedure for all other dra-directors and modify the IP addresses accordingly.

Perform the following steps on each dra-director VM to configure policy routing:

- 1. Create a custom routing table
- 2. Create an IP rule for each remote relay endpoint's real IP address
- 3. Add a route to the custom routing table that specifies the real IP source address

Set up Custom Routing Table

Set up the custom routing table as shown in the following example:

echo "200 dra.relay" | sudo tee --append /etc/iproute2/rt_tables

Define IP Rules

The following rules match the packets destined to the real IPs of interface ens224 on dra2-director1 and dra2-director2:

```
ip -6 rule add to 2006:db8:2001:2425::13 table dra.relay
ip -6 rule add to 2006:db8:2001:2425::14 table dra.relay
```

Define the Route

The following example of the route uses the router's interface as the next hop and specifies ens224's real IP address as the source address for outgoing packets.

```
ip route add 2006:db8:2001:2425::/112 via
2001:db8:2040:202::1 src 2001:db8:2040:202::13 table dra.relay
```

Validate the Routing

Use the following example commands to validate the route selection for remote relay real IP and VIP addresses.

ip -6 route show table dra.relay ip -6 route get 2006:db8:2001:2425::13 ip -6 route get 2006:db8:2001:2425::14 ip -6 route get 2006:db8:2001:2425::50

Persistent Configuration

In order for the Policy Routing configuration to survive a reboot, add the configuration commands to /etc/network/interfaces under interface ens224 as shown below:

```
auto ens224
iface ens224 inet static
address 192.169.22.13
netmask 255.255.255.0
iface ens224 inet6 static
address 2001:db8:2040:202::13
netmask 112
up ip route add 2006:db8:2001:2425::/112 via 2001:db8:2040:202::1
up ip -6 rule add to 2006:db8:2001:2425::13 table dra.relay
up ip -6 rule add to 2006:db8:2001:2425::14 table dra.relay
up ip route add 2006:db8:2001:2425::/112 via 2001:db8:2040:202::1 src 2001:
db8:2040:202::13 table dra.relay
down ip route del 2006:db8:2001:2425::/112 via 2001:db8:2040:202::1
down ip -6 rule del to 2006:db8:2001:2425::13 table dra.relay
down ip -6 rule del to 2006:db8:2001:2425::14 table dra.relay
down ip route del 2006:db8:2001:2425::/112 via 2001:db8:2040:202::1 src
2001:db8:2040:202::13 table dra.relay
```

Configure Policy Routing with Deployer/Installer

Configure the VM artifacts and the cloud config to set up policy routing using the deployer.

VM Artifacts

Add Policy Route configuration to the DRA director VM's interfaces.esxi file as shown in the following example:

```
cps@installer:/data/deployer/envs/dra-vnf/vms/dra-director
/dra-director-1$ cat interfaces.esxi
auto lo
iface lo inet loopback
```

auto ens160

```
iface ens160 inet static
address 10.81.70.191
netmask 255.255.255.0
gateway 10.81.70.1
auto ens192
iface ens192 inet static
address 192.169.21.13
netmask 255.255.255.0
auto ens224
iface ens224 inet static
address 192.169.22.13
netmask 255.255.255.0
iface ens224 inet6 static
address 2001:db8:2040:202::13
netmask 112
up ip route add 2006:db8:2001:2425::/112 via 2001:db8:2040:202::1
up ip -6 rule add to 2006:db8:2001:2425::13 table dra.relay
up ip -6 rule add to 2006:db8:2001:2425::14 table dra.relay
up ip route add 2006:db8:2001:2425::/112 via 2001:db8:2040:202::1 src
2001:db8:2040:202::13 table dra.relay
down ip route del 2006:db8:2001:2425::/112 via 2001:db8:2040:202::1
down ip -6 rule del to 2006:db8:2001:2425::13 table dra.relay
down ip -6 rule del to 2006:db8:2001:2425::14 table dra.relay
down ip route del 2006:db8:2001:2425::/112 via 2001:db8:2040:202::1 src
2001:db8:2040:202::13 table dra.relay
auto ens256
iface ens256 inet static
address 192.169.23.13
netmask 255.255.255.0
cps@installer:/data/deployer/envs/dra-vnf/vms/dra-director/dra-director-1$
```

Cloud Config

Create the dra.relay routing table on the dra-directors by adding the following bootcmd: to user_data.yml and storing the file at /data/deployer/envs/dra-vnf/vms/dra-director/user_data.yml. The sed command prevents adding a routing table every time the VM boots.

bootcmd:
 - "sed -i -e '/^200 *dra.relay/d' /etc/iproute2/rt_tables"
 - "sh -c \"echo '200 dra.relay' >> /etc/iproute2/rt_tables\""

Example of user_data.yml:

vf4extHTn32Dtsxkjz7kQeEDgCe/y7owimaEFcCIfEWEaj/50jegN cps@root-public-key

N+Iaf27rE0t3oiY5DRN6j07WhauM6lCnZ1JDlzqmTnTHQkgJ3uKmQa5x73tJ10W89Whf+R+dfslVn/yUwK/

resize rootfs: true

write files:

```
- path: /root/swarm.json
   content: |
     {
       "role": "{{ ROLE }}",
        "identifier": "{{ IDENTIFIER }}",
        "master": "{{ MASTER IP }}",
        "network": "{{ INTERNAL_NETWORK }}",
       {% if WEAVE PASSWORD is defined %}"weavePw": "{{ WEAVE PASSWORD }}",
        {% endif %}
        "zing": "{{ RUN_ZING | default(1) }}",
        "cluster id": "{{ CLUSTER ID }}",
        "system id": "{{ SYSTEM ID }}"
    }
   owner: root:root
   permissions: '0644'
  - path: /home/cps/.bash aliases
   encoding: text/plain
   content: |
     # A convenient shortcut to get to the Orchestrator CLI
     alias cli="ssh -p 2024 admin@localhost"
     alias pem="wget --quiet http://171.70.34.121/microservices/latest/cps.pem ;
     chmod 400
cps.pem ; echo 'Retrieved \"cps.pem\" key file'"
   owner: cps:cps
   permissions: '0644'
  - path: /etc/pam.d/common-password
   content: |
     # /etc/pam.d/common-password - password-related modules common to all services
    # This file is included from other service-specific PAM config files,
     # and should contain a list of modules that define the services to be
     # used to change user passwords. The default is pam unix.
     # Explanation of pam unix options:
     # The "sha512" option enables salted SHA512 passwords. Without this option,
     # the default is Unix crypt. Prior releases used the option "md5".
     # The "obscure" option replaces the old `OBSCURE CHECKS ENAB' option in
     # login.defs.
     # See the pam unix manpage for other options.
     # As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
     # To take advantage of this, it is recommended that you configure any
     # local modules either before or after the default block, and use
     # pam-auth-update to manage selection of other modules. See
     # pam-auth-update(8) for details.
     # here are the per-package modules (the "Primary" block)
    password requisite
                                                pam pwquality.so retry=3 minlen=8
    minclass=2
    password [success=2 default=ignore]
                                                pam unix.so obscure use authtok
    try_first_pass sha512 remember=5
    password sufficient
                                                pam sss.so use authtok
     # here's the fallback if no module succeeds
    password requisite
                                                pam deny.so
     # prime the stack with a positive return value if there isn't one already;
     # this avoids us returning an error just because nothing sets a success code
     # since the modules above will each just jump around
    password required
                                                pam permit.so
     # and here are more per-package modules (the "Additional" block)
     # end of pam-auth-update config
```

```
owner: root:root
  permissions: '0644'
runcmd:
  - [vmware-toolbox-cmd, timesync, enable ]
bootcmd:
  - "sed -i -e '/^200 *dra.relay/d' /etc/iproute2/rt_tables"
  - "sh -c \"echo '200 dra.relay' >> /etc/iproute2/rt_tables\""
```

SLF Configuration

You can specify whether the IMSI and MSISDN values are validated in SLF API.

By default, SLF validation is disabled.

To set up SLF validation, create SLF Configuration from the Plugin Configuration in Policy Builder.

Figure 13: SLF Configuration

Systems	SLF Configuration
Summary	or comgaration
system-1 Plugin Configurations Threading Configuration Async Threading Configuration Custom Reference Data Configu Portal Configuration D R A Configuration	 *SIf Api Validations Validate IMSI Is Numeric Validate IMSI Length *IMSI Minimum Length 15
SLF Configuration	*IMSI Maximum Length
Custom Reference Data Tables	
Diameter Applications	Validate MSISDN Is Numeric
Fault List	Validate MSISDN Length
Policy Enforcement Points	
Routing Avp Definitions	*MSISDN Minimum Length
Subscriber Data Sources	10
	*MSISDN Maximum Length
	10

The following table describes the SLF API validations that you can configure:

Table 12: SLF Configuration

Field	Description
Validate IMSI is Numeric	If checked: IMSI received in the SLF API request must be numeric
	If unchecked: IMSI numeric validation is not performed on the IMSI received in the SLF API request

Field	Description
Validate IMSI Length	If checked: IMSI length is validated based on the specified IMSI Minimum Length (inclusive) and IMSI Maximum Length (inclusive) If unchecked: IMSI length validation is not performed
	on the IMSI received in the SLF API request
Validate MSISDN is Numeric	If checked: MSISDN received in the SLF API request must be numeric
	If unchecked: MSISDN numeric validation is not performed on the MSISDN received in the SLF API request
Validate MSISDN Length	If checked: MSISDN length is validated based on the specified MSISDN Minimum Length (inclusive) and MSISDN Maximum Length (inclusive)
	If unchecked: MSISDN length validation is not performed on the MSISDN received in the SLF API request

Diameter Application

Sd Application

For Sd, an Application Routing table is used to map specific diameter command codes and CC-Request-Types to a table, typically, an Sd New Session table for routing Sd TSRs to a peer route. The Sd New Session CD table will choose a peer route based on the Destination-Realm. The peer route will then point to a Peer-Group which contains multiple peer connections to a TDF and the DRA will load balance among the TDF peer connections in the Peer Group.

An example configuration is shown below:

Figure 14: Diameter Application - Sd Application Example

lame			*Application Id		
Sd Applicati	on		16777303		
endor Ids/					
10415					
		Add	✓ Tgpp Application	1	
		Remove	I gpp / ppicadio		
		Remove	I gpp / ppilodio		
		Remove			
Application F	Route	Remove			
Application F		Remove	Cc Request Type	*Destination H	Action Tables
					Action Tables New Sd Session
Name	*Priority	*Command Code	Cc Request Type	*Destination H	
Name Sd-TSR	*Priority 0	*Command Code 8388637	Cc Request Type 0	*Destination H	New Sd Session
Name Sd-TSR Sd-CCR-I	*Priority 0 0	*Command Code 8388637 272	Cc Request Type 0 1	*Destination H	New Sd Session New Sd Session

The following parameters are configured under Sd Application:

Table 13: Sd Application Parameters

Parameter	Description
Name	Name of the Sd application.
Application Id	16777303, 3GPP specified Application Identifier for Sd interface.
Vendor Ids	Vendor Identifiers that are required to be supported on Sd interface.
Tgpp Application check box	If this check box is selected, indicates this is a 3GPP defined application interface.
Application Route table	
Name	Identifier of the route.
Priority	Indicates the priority of the route.
Command Code	Indicates value of command code AVP within the message.
Cc Request Type	Indicates if the Credit Control Request type is Initial(1)/Update(2) or Terminate(3).
Destination Host Null	If this check box is selected, indicates if Destination Host will be null in messages received for this application.
Action Tables	Identifies the request routing table for this interface and message.

Gx Application

For Gx, an Application Routing table is used to map specific diameter command codes and CC-Request-Types to a table. When "Destination Host Null" is checked, it means Destination-Host AVP is null. It will then check for table driven routing.

An example configuration is shown below:

Figure 15: Diameter Application - Gx Application Example

lame		*Ap	plication Id		
Gx Application		16	777238		
/endor Ids					
8164					
9		Add	Topp Application		
The second se		Add Jgpp Application			
10415		Remove			
10415 Application Rot	ıte	Remove			
	ite *Priority	Remove *Command Code	Cc Request Type	*Destinal	ion HcAction Tables
Application Rou			Cc Request Type	*Destinat	ion HcAction Tables New Gx Session
Application Rou Name	*Priority	*Command Code			
Application Rou Name Gx Initial	*Priority 1	*Command Code 272	1		New Gx Session

C-DRA attempts to do Dest-Host routing before doing table driven routing. If the Dest-Host AVP is absent, empty, or equal to the CDRA FQDN, then we skip Dest-Host routing altogether and proceed to Table-Driven routing.

The following parameters are configured under Gx Application:

Table 14: Gx Application Parameters

Parameter	Description
Name	Name of the Gx application.
Application Id	16777238, 3GPP specified Application Identifier for Gx interface.
Vendor Ids	Vendor Identifiers that are required to be supported on Gx interface.
Tgpp Application check box	If this check box is selected, indicates this is a 3GPP defined application interface.
Application Route table	
Name	Identifier of the route.
Priority	Indicates the priority of the route.
Command Code	Indicates value of command code AVP within the message.

Parameter	Description
Cc Request Type	Indicates if the Credit Control Request type is Initial(1)/Update(2) or Terminate(3).
Destination Host Null	If this check box is selected, indicates the message will contain a Destination-Host.
Action Tables	Identifies the request routing table for this interface and message.

Rx Application

Identifies the request routing table for this interface and message.

Figure 16: Diameter Application - Rx Application Example

lame			*Application Id		
Rx Application			16777236		
endor Ids					
13019					
8164		Add	Topp Application		
9		Remove			
	*Priority	*Command Code	Cc Request Type	*Destinat	ion H(Action Tables
Name		*Command Code 265	Cc Request Type	*Destinat	
Application Route Name Rx Initial Rx Termination	*Priority				ion H(Action Tables New Rx Session New Rx Session

The following parameters are configured under Rx Application:

Table 15: Rx Application Parameters

Parameter	Description
Name	Name of the Rx application.
Application Id	16777236, 3GPP specified Application Identifier for Rx interface.
Vendor Ids	Vendor Identifiers that are required to be supported on Rx interface.
Tgpp Application check box	If this check box is selected, indicates this is a 3GPP defined application interface.
Application Route table	
Name	Identifier of the route.

Parameter	Description
Priority	Indicates the priority of the route.
Command Code	Indicates value of command code AVP within the message.
Cc Request Type	Not supported for Rx interface.
Destination Host Null	If this check box is selected, indicates if Destination Host will be null in messages received for this application.
Action Tables	Identifies the request routing table for this interface and message.

Sh Application

Sh interface is used for communication between AS and HSS for Call data query/Push subscriber profile and subscriber notification procedures.



Note

In certain scenarios, the customer might use the Sh interface between PCRF and HSS also.

An example configuration is shown below:

Figure 17: Diameter Application - Sh Application Example

lame		*	Application Id		
Sh Applicat	tion		16777217		
endor Ids/					
10415		Add	✓ Tgpp Application		
polication	Route				
Application Name	Route *Priority	*Command Code	Cc Request Type	*Destinat	ion H(Action Tables
		*Command Code 306	Cc Request Type	*Destinat	
Name	*Priority				ion HcAction Tables Sh_Application Sh_Application
Name UDR	*Priority 0	306	0		Sh_Application

The following parameters are configured under Sh Application:

Parameter	Description
Name	Name of the Sh application.
Application Id	16777217, 3GPP specified Application Identifier for Sh interface.
Vendor Ids	Vendor Identifiers that are required to be supported on Sh interface.
Tgpp Application check box	If this check box is selected, indicates this is a 3GPP defined application interface.
Application Route table	
Name	Identifier of the route.
Priority	Indicates the priority of the route.
Command Code	Indicates value of command code AVP within the message.
Cc Request Type	CC-Request-Type is not applicable for Sh interface.
Destination Host Null	If this check box is selected, indicates the message will contain a Destination-Host.
Action Tables	Identifies the request routing table for this interface and message.

Table 16: Sh Application Parameters

S6a Application

DRA supports S6a interface with the implementation of Subscriber Location Function(SLF) feature. S6a is an interface which supports the mobility management and subscriber data management procedures between MME and HSS in an LTE EPC network.

An example configuration is shown below:

Figure 18: Diameter Application - S6a Application Example

Diameter Ap	plication				
Name		*Ap	plication Id		
S6a Applicatio	n	16	777251		
Vendor Ids					
10415					
		Add	Tgpp Application		
		Remove	gpp Application		
		Itemove			
Application Ro	ute				
Name	*Priority	*Command Code	Request Type	*Destination Host Null	Action Tables
AIR	1	318	0		S6a_Application
ULR	1	316	0		S6a_Application
Add Remove	e Co Co				

The following parameters are configured under S6a Application:

Table 17: S6a Application Parameters

Parameter	Description
Name	Name of the S6a application.
Application Id	16777251, 3GPP specified Application Identifier for S6a interface.
Vendor Ids	Vendor Identifiers that are required to be supported on S6a interface.
Tgpp Application check box	If this check box is selected, indicates this is a 3GPP defined application interface.
Application Route table	
Name	Identifier of the route.
Priority	Indicates the priority of the route.
Command Code	Indicates value of command code AVP within the message.
Cc Request Type	CC-Request-Type is not applicable for S6a interface.
Destination Host Null	If this check box is selected, indicates the message will contain a Destination-Host.
Action Tables	Identifies the request routing table for this interface and message.

Routing AVP Definition

Gx Session

An example configuration is shown below:

Figure 19: Routing AVP Definition - Gx Session

lame	
New Gx Session	
Routing Avp Lookup	
*Search Table Group	
apn_mapping_table	
TB_GX_NEW_SESSION	

Rx Session

An example configuration is shown below:

Figure 20: Routing AVP Definition - Rx Session

lame	
New Rx Session	
Routing Avp Lookup	
*Search Table Group	
TB_RX_NEW_SESSION	
apn_mapping_table	

Rx New Session Rules - CRD Table

An example configuration is shown below:

Figure 21: Rx New Session Rules - CRD Table

Name		Display Name							
TB_RX_NEW_SESSION		Rx New Session Rules	Cache Res	sults					
Activation Condition			*Evaluation C	Order					
Rx	select dear	 Best Match 	0						
Columns									
"Name		Display Nam	ne		*Use In 0	Conditi "Type		Key	Required
logical_apn		Logical APN	0		4	Text		2	4
origin_host		Origin Host			1	Text		~	1
peer_route		Peer Route			4	Text			
destination_host		Destination	Host		1	Text		1	
Valid Values				alidation			Runtime Binding		
Valid Values The values allowed in Contro (e) All	ol Center for this coli	umn	Va	alidation alidation used by Control Center tegular Expression			Runtime Binding Which rows match when a message is received None. Bind to Subscriber AVP code		
Valid Values The values allowed in Contro		imn Visplay Name	va Re	alidation used by Control Center			Which rows match when a message is received None		
Valid Values The values allowed in Contro a All Dist of Valid Values			va Re	alidation used by Control Center tegular Expression			Which rows match when a message is received None		
Valid Values The values allowed in Contro All List of valid Values			va Re	alidation used by Control Center tegular Expression			Which rows match when a message is received None Bind to Subscriber AVP code		
Valid Values The values allowed in Contro All List of valid Values			va Re	alidation used by Control Center tegular Expression			Which rows match when a message is received None Bind to Subscriber AVP code Bind to Session/Policy State Field Retrieve Destion Host (Class) [select] <u>deat</u> Bind to a result column from another table		
Valid Values The values allowed in Contro All Lat of Valid Values *Name			va Re	alidation used by Control Center tegular Expression			Which rows match when a message is received None Bind to Subscriber AVP code Bind to Subscriber AVP code Bind to Session/Policy State Field Retrieve Destination Host (Ciscc) Select J dear		
Valid Values The values allowed in Contro All List of valid Values	5	isplay Name	va Re	alidation used by Control Center tegular Expression			Which rows match when a message is received None Bind to Subscriber AVP code Bind to Subscriber AVP code Retrieve Destination Host (Cisco: Select Selac Bind to a result column from another table		
List of Valid Values	5	isplay Name	va Re	alidation used by Control Center tegular Expression			Which rows match when a message is received None Bind to Subscriber AVP code Bind to Subscriber AVP code Retrieve Destination Host (Cisco: Select Selac Bind to a result column from another table		

Gx New Session Rules - CRD Table

For Gx, an Application Routing table is used to map specific diameter command codes and CC-Request-Types to a table, typically, for routing Gx CCR-Is. The Gx CCR-I should be routed based on a logical APN and the Origin-Host attribute. Regular expression matching of logical APNs and Origin-Hosts can also be configured. The implementation should be flexible to allow CRDs to be configured for routing of other attributes such as Destination-Realm and Origin-Realm.

An example configuration is shown below:

Figure 22: Gx New Session Rules - CRD Table

Name		Display Name									
TB_GX_NEW_SESSION		Gx New Session R	ules	Cache Results							
Activation Condition				Evaluation Order							
Gx	select dear	Best Match		1							
Columns											
Name			Display Name			*Use In	Conditi "Type		Key	Required	
peer_route			Peer Route			1	Text				
origin_realm			Origin Realm			1	Text		4	9	
destination_realm			Destination Real	n		1	Text		1	1	
origini_host			Origin Host			1	Text		Q.	U.	
logical_apn			Logical APN			1	Text		~	2	
msi			IMSI			1	Text		1	1	
dd Remove 🙀 🕹											
olumn Details				Validation				Runtime Binding			
Valid Values The values allowed in Contro	I Contractor the state			Validation Validation used t	Control Control			Which rows match when a message is received			
	Center for this col	umn									
(e) All				Regular Express	lion			None			
								Bind to Subscriber AVP code			
"Name		Display Name		Regular Express	ion Description						
								Bind to Session/Policy State Field			
								Retrieve Origin Realm (Cisco DR select dear			
								Bind to a result column from another table			
								lean lean			
								Bind to Diameter request AVP code			
								Matching Operator			

Sd New Session Rules - CRD Table

An example configuration is shown below:

Figure 23: Sd New Session Rules - CRD Table

Name		Display Name								
TB_SD_NEW_SESSION		SD_NEW_SESS	ION	Cache Results						
Activation Condition				*Evaluation Order						
select dear		Best Match		0						
Columns										
"Name			Display Name		"Use Ir	Conditi *Type	e	Key	Required	
peer_route			Peer Route		4	Text				
origin_realm			Origin Realm		1	Text		1	4	
destination_realm			Destination Rea	den	1	Text		1	1	
destination_host			Destination Hos	t.	7	Text		1	1	
logical_apn			Logical APN		9	Text		1	1	
msisdn			MSISDN		1	Text		1	1	18
kdd Remove 😚 🐣										
olumn Details										
/alid Values				Validation			Runtime Binding			
The values allowed in Control	Center for this col	lumn		Validation used by Co	ontrol Center		Which rows match when a message is rece	ved		
(e) Al			Regular Expression			None				
				Regular Expression	0					
*Name		Display Name		Regular Expression	Description					
							asieti			
							Matching Operator			

Logical APN List - CRD Table

An example configuration is shown below:

Figure 24: Logical APN List - CRD Table

Name	Display Name	-	Activation Condition					
logical_apn_list	Logical APN List	Cache Results		select dear				
Columns								
"Name		Display Name		*Use In C	onditi "Type		Key	Required
logical_apn		Logical APN		7	Text		1	1
Add Remove 😯 🕹								
Column Details								
Valid Values			Validation			Runtime Binding		
The values allowed in Control Center for this column			Validation used by Control Center			Which rows match when a message is received		
 All 			Regular Expression			(e) None		
"Name	Display Name		Regular Expression Descrip	otion				
						Matching Operator		

Dynamic AVP Retriever for Routing

DRA supports routing messages based on the following AVPs from request message:

- Destination-Host
- Destination-Realm
- Origin-Host
- Origin-Realm
- APN (from Called-Station-ID)

- IMSI (from Subscription-ID)
- MSISDN (from Subscription-ID)

Regular-expression matching and combinations of AVPs is supported. This requirement is not applicable across all messages on different interfaces. The following table shows applicability of the AVP's at a message and interface level.

Interface	Message	Origin Host	Origin Realm	Destination Host	Destination Realm	APN (Called-Station-ID)	IMSI	MSISDN
Gx	CCR-I	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	CCR-U	No	No	No	No	No	No	No
	RAR	No	No	Yes	No	No	No	No
Sd	TSR	Yes	Yes	Yes	Yes	No	No	No
	CCR-I	Yes	Yes	Yes	Yes	No	No	No
	CCR-U/T	No	No	Yes	No	No	No	No
	RAR	No	No	Yes	No	No	No	No
Rx	RAR	No	No	Yes	No	No	No	No

Table 18: Regular-expression Matching and Combinations of AVPs

Dynamic AVP Retrievers are used mostly used in Custom Reference Data where data has to be fetched from messages at runtime.

Configure Dynamic AVP Retriever

The following sample configuration shows how to retrieve the AVP and bind it to a Key Column in the CRD.

- Step 1 Select the column name from the Columns table and click select near Bind to Session/Policy State Field to open the Please select an object... dialog box.
 - **Note** You can use **Bind to Session/Policy State Field** only for those columns in the **Columns** table where **Key** column has been selected.
- **Step 2** Select the required object from the dialog box and click **OK**.

Figure 25: Adding AVPs

*Name	Display Name		*Use In C	onditi *Type		Key	Required
calledStationId	APN		7	Text		V	$\overline{\checkmark}$
logical_apn	Logical APN		1	Text			\sim
		Please select an o	bject		O X		
dd Remove 🕜 🕹 Jolum Details Zalid Values The values allowed in Control C All List of Valid Values	Center for this column	 External S Retrieve A Retrieve B 	rofile Charging Id ubscriber Id Retriev PN (Cisco DRA) pplication Id (Cisco inding FQDN (Cisco estination Host (Cis	DRA) DRA)	-	hen a message r AVP code	is received
"Name	Display Name	 ♦ Retrieve II ♦ Retrieve M ♦ Retrieve C 	estination Realm (C MSI (Cisco DRA) ISISDN (Cisco DRA) Irigin Host (Cisco DF Irigin Realm (Cisco I	A)	Cisco	olumn from anol	elect clear
			6	ок	Cancel	request AVP co	

Step 3 Repeat these steps to add additional AVPs.

Custom Reference Data Tables

Search Table Groups

Peer Rate Limit Profile

This is a Search Table Group whose key columns are Peer Group, Peer FQDN or Origin Host in the message and Message Direction.

Using this search table group, the user can configure a maximum rate for each of the configured and defined diameter peers. It also allows the user to configure a maximum rate for each server process.

The peer rate limit is shown below:

Figure 26: Peer Rate Limit - STG

peer_rate_limit_profile	Display Name Peer Rate Limit Prof	file 🗸 Ca	ache Results				
ctivation Condition		*Eval	uation Order				
select	l <u>clear</u> Best Match	0					
Columns							
Name	Display Name		*Use In C	onditic *Type		Key	Required
eer_group	Peer Group		$\overline{\checkmark}$	Text		\checkmark	
eer_fqdn	Peer FQDN		 Image: A set of the set of the	Text		Image: A start and a start	
direction	Message Direction		~	Text		~	~
rate_limit_profile	Rate Limit Profile		~	Text			
peer_rate_limit	Peer Rate Limit			Number			
discard behavior	Discard Behavior		2	Number			2
The values allowed in Control Center for t	his column	Validation used Regular Expre		er	Runtime Binding Which rows match whe	n a message is rec	eived
List of Valid Values					Bind to Subscriber	AVP code	
*Name Disp	play Name	Regular Expre	ssion Descript	ion			
					Bind to Session/Pol	icy State Field	
						select	ti <u>clear</u>
					O Bind to a result colu	umn from another t	able
						selec	l <u>clear</u>
Add Remove					Bind to Diameter re	quest AVP code	
Valid values pulled from another table	's column (kev)						
					Matching Operator		
	t <u>clear</u>				-		

- Peer Group: This is the group of peers classified together using Peer Group and Peer Group Peer values initiating the message.
- Peer FQDN: The origin host of the peer. A specific diameter peer with its Fully Qualified Domain Name can be specified in this field or use wildcards specified by * in this field for any peer or matching peers like hss*.
- Direction: Message direction (Ingress and Egress).
 - Ingress: Any diameter messages received by CPS vDRA from diameter peer. The routing decision by CPS vDRA will be taken after the ingress side rate limiting has been applied.
 - Egress: Any diameter messages forwarded/routed by CPS vDRA to diameter peer. The egress side
 rate limiting will be applied after the routing decision has been taken by CPS vDRA.
- Peer Rate Limit: This field is to specify the threshold in TPS above which the diameter messages are discarded. This can be left empty if none of the messages are to be dropped or only message level rate limit is to be applied.
- Rate Limit Profile: Profile Name applicable for this Peer Group and Peer, if specified. This profile maps to Rate Limiting at message level. This field enables the rate limit at per message/command code level. See Message Rate Limit Profile for more details.
- Rate Limit Result Code: The result code sent by CPS vDRA for response message towards diameter peer when Discard Behavior is configured as Send Error Answer. In case Discard Behavior is configured as Drop Message, this field is ignored.
- Error String: The string specified in this field is populated by CPS vDRA in AVP Error Message for response message towards diameter peer when Discard Behavior is configured as Send Error Answer. In case Discard Behavior is configured as Drop Message, this field is ignored. This is an optional field when Discard Behavior is configured as Send Error Answer.



Note If both Rate Limit Error Code and Rate Limit Error String are provided along with Rate Limit Action as "Drop Message", the Rate Limit Action takes precedence and the other two fields will be ignored.

For more information, see Peer Rate Limit Profile.

Peer Group Mapping

Figure 27: Peer Group Mapping - STG

*Name	Display Na	me				
peer_group_mapping	Peer Grou	p Mapping	Cache R	esults		
Activation Condition			*Evaluation	n Order		
	select clear Best Ma		0			
Columns						
*Name	Display Name			onditic *Type		Key
realm_pattern	Realm Pattern		V	Text		\checkmark
fqdn_pattern	FQDN Pattern		×	Text		X
peer_group	Peer Group		×	Text		
weight	Weight		~	Number		
Add) Remove) 🙀 🚯						
Valid Values		Validation			Runtime Binding	
The values allowed in Control Co	enter for this column	Validation	used by Control (Center	Which rows match	when a messag
() All		Regular E	xpression		None	
C List of Valid Values					O Bind to Subscri	ber AVP code
		Pequilar E	xpression Desc	ription	ſ	
*Name	Display Name	Kegulai L	Apression Dese			

For more information, see Peer Group Mapping.

Message Retry Profile

Message retry profile has been added.

Figure 28: Message Retry Profile - STG

*Name		Display Name	_	-				
message_retry_profile		Message Retry P	Profile	Cache Resu	lts			
Activation Condition			*6	valuation Or	der			
	select <u>clear</u>	Best Match	0	1				
Columns								
*Name			Display Name	*Use Ir	n Conditi *Type	Key	Required	
peer_group			Peer Group	1	Text	$\overline{\checkmark}$		
app_id			Application Id	\checkmark	Text	\checkmark		
cmd_code			Command Code	~	Text	$\overline{\checkmark}$		
rc_in_resp			Result Code	1	Text	$\overline{\checkmark}$	$\overline{\checkmark}$	
exp_rc			Experimental RC	~	True/False			
num retries			Number Of Retries		Text			
Valid Values	l Cashar fan thia an h	Valida		Cantas	Runtime Binding			
The values allowed in Contro	ol Center for this colu	mn Valida	ation used by Control	Center	Which rows match	h when a m	essage is receive	1
 All 		Regu	lar Expression		None			
O List of Valid Values					🔵 Bind to Subsc			
	Display Name	Regu	lar Expression Desc	ription	Ċ.			
*Name	Dispidy Hame							
*Name	bispidy Hume				O Bind to Sessio		ate Field	
*Name	bispidy Hame				O Bind to Sessic	n/Policy Sta	ate Field	
*Name	Display Name							
*Name	Dopidy Hume						select clea	
*Name	Dopidy Hunc					lt column fr	om another table	
		in (key			O Bind to a resu	lt column fr	om another table	

- Peer Group: Peer group for which the retry has to be happen.
- Application Id: Application Id of the diameter applications.
- Command Code: Command Code of the message.
- Result Code: Result code received from PCRF for timeout. The value is 7000.
- Experimental RC: Indicates whether result code is experimental or not. This is for future purpose and value in this has no effect on the message retry functionality.
- Number of Retries: Number of retries for the message.

For more information, see Message Retry Profile.

Message Mediation Profile

The message mediation profile is used to provide support for mediation of AVPs in Diameter request and answer.

- For Diameter requests, only remove is supported.
- For Diameter answers, the following actions are supported:
 - "remove" meaning remove all matching AVPs in the request.
 - "copy" meaning copy from the request if no AVPs are present in the answer.

• If the AVP is present in answer, no action is performed.

• "overwrite" meaning first remove and then copy from the request.

- Check if the AVP is present in answer, if so remove and add from request.
- If AVP is not present in answer, copy from request.

A new Message Mediation Profile STG has been added:

Figure 29: Message Mediation Profile - STG

Name		Display Name Message Mediation Profile	Cach	e Results					
message_mediation_profile		Message Mediation Profile	_						
Activation Condition		Best Match		tion Order					
	select clear		0						
Columns									
*Name		Display Name		*Use In Cor			Key	Required	
app_id		Application Id		×	Text		v	V	
cmd_code	0	Command Code		×	Text		~	Image: A start and a start	
msg_type		Message Type		1	Text		~	 Image: A set of the set of the	
avp_code	,	Avp Code		1	Text		2	1	
vendor_id	1	Avp Vendor Id		2	Text			1	
avo action		Ave Action		V	Text				
Valid Values The values allowed in Control Cen All Ust of Valid Values	ter for this colum	in Val	idation idation used by gular Expressi			Runtime Binding Which rows match when a None Bind to Subscriber AVP		sived	
*Name	Display Nam	e Re	gular Expressi	on Descriptio	n				
						Bind to Session/Policy	State Field		
							select	clear	
						Bind to a result column	from another ta	sble	
							select	dear	
Add (Remove)						O Bind to Diameter reque		dear	
Add) (Remave) (() ()	er table's column	n (key)				Bind to Diameter reque		dear	

- Application Id: Application ID of the Diameter applications.
- · Command Code: Command code of the message.
- Message Type : Request/Answer for which the rule has to be applied.
- Avp Code : AVP code of the Diameter message.
- Vendor Id : AVP vendor ID.
- Avp Action : Provides options for copy/remove/overwrite.



Note

Application ID, Command Code, AVP Code and Vendor Id are used as key, so no duplicate rows could be defined for this combination and the same AVP action. For example, you cannot define both "remove" and "Copy from request" for the same set of Application ID, Command Code, AVP Code and Vendor Id.

Best Match check box needs to be checked if you want to use the wildcard feature.

For more information, see Message Mediation Profile in Custom Reference Data Tables chapter.

Peer Group Answer Timeout

New search table Peer Group Answer Timeout has been added.

Figure 30: Peer Group Answer Timeout - STG

Name	Display Name	Cache Results			
peer_group_answer_timeout	Peer Group Answer Timeout	Course Resolution			
Activation Condition		*Evaluation Order			
	clear Best Match	0			
Columns					
*Name		Display Name		*Use In (Conditic *Type
peer_group		Peer Group		V	Text
app_id		Application Id		\checkmark	Text
cmd_code		Command Code		\checkmark	Text
answer_timeout		Timeout Milliseconds		~	Text
Add Remove 👔 📣					
Valid Values			Validation		
The values allowed in Control Center for th	nis column		Validation used by Control Center		
() All			Regular Expression		
C List of Valid Values					
*Name	Display Name		Regular Expression Description		

- Application Id: Application Id of the diameter applications.
- Peer Group: Peer group for which the timeout is applied.
- · Command code (to enable different timeouts for different Diameter commands)
- Timeout: Timeout in milliseconds.

For more information, see Peer Group Answer Timeout.

Error Result Code Profile

Error result code profile can be used to map errors to Result-Code value and an error message string for the Error-Message AVP. It also provides support for configurable error result codes.

Figure 31: Error Result Code Profile - STG

internal_err Error rc_In_resp Result Code exp_rc_in_resp Exp Result Code exp Result Code Exp Result Code Exp Result Code Exp Result Code Finder Subscripter AvP code End to Subscripter AvP code Internet Regular Expression Description End to Session/Policy State Field Internet Regular Expression Description End to Session/Policy State Field Internet Regular Expression Description End to Session/Policy State Field Internet Regular Expression Description End to Session/Policy State Field Internet Regular Expression Description End to Session/Policy State Field Internet Regular Expression Description End to Session/Policy State Field Internet Regular Expression Description End to Session/Policy State Field Internet Regular Expression Description End to Dianeter request AVP code	*Name	Display Name							
* Columns * Name Bisplay Name * Name * Display Name * Name * Display Name * Name * Display Name * Name * Name * Display Name * Name * Name * Name * Name * Name * Display Name * Name <	error_profile	Error Result Code	e Profile	Cache Results					
'solume 'Soluma	Activation Condition			*Evaluation Order					
**Name Display Name **Use In Conditik **Type Key Required app_id Application Id Image Text Image Image internal_err Error Text Image Im		selecti clear Best Match		0					
app_id Application Id Text Image in the image	Columns								
Internal_err recip_ce_fin_resp Result Code Text Code Resp. cc_fin_resp Result Code Text Code Text Code Resp. cc_fin_resp Result Code Text Code Tex	*Name	Display Name		*Use In C	onditic *Type		Key	Required	
rc_in_resp Result Code exp_rc_in_resp Exp Result Code exp_rc_in_resp Err Msa exp response Err Msa Exp Result Code Exp Result Code Exp Result Code Exp Result Code It st of Valid Values Regular Expression Description Name Display Name Regular Expression Description It st of Valid Values It st of Valid Code It st of Valid Values It st of Valid Code It st of Valid Values It st of Valid Code It st of Valid Values It st of Valid Code It st of Valid Values It st of Valid Code It st of Valid Values It st of Valid Code It st of Valid Values It st of Valid Code It st of Valid Values It st of Valid Code It st of Valid Values It st of Valid Code It st of Valid Values It st of Valid Code It st of Valid Values It st of Valid Code It st of Valid Values It st of Valid Code It st of Valid Values It st of Valid Code It st of Valid Values It st of Valid Code	app_id	Application Id		a	Text		~	1	8
exp_rc_in_resp Exp Result Code exp_rc_in_resp Exp Result Code exp_rc_in_resp Exp Result Code exp_rc_in_resp Exp Result Code exp_rc_in_resp Fr Mso	internal_err	Error		×	Text		v	2	
exp_vendr_jd vendor Id rext rest rest rest rest rest rest rest res	rc_in_resp	Result Code		1	Text				
err mso Err Mso	exp_rc_in_resp	Exp Result Code		1	Text				
Addi Termore Image: Column Details Valid Values Validation Runtime Binding The values allowed in Control Center for this column Validation used by Control Center Which rows match when a message is received Image: All Column Details Regular Expression Image: Bind to Subsorber AVP code Image: Name Display Name Regular Expression Description Image: Bind to Subsorber AVP code Image: Name Display Name Regular Expression Description Image: Bind to Subsorber AVP code Image: Image: Display Name Image: Expression Description Image: Bind to Subsorber AVP code Image: I	exp_vendor_id	Vendor Id		a	Text				
Column Details Validation Runtime Binding Yalidation used by Control Center Which rows match when a message is received Image: All Regular Expression Image: None Image: Used of Valid Values Bind to Subscriber AVP code Image: Bind to Subscriber AVP code Image: Name Display Name Regular Expression Description Image: Bind to Subscriber AVP code Image: Regular expression Bind to Subscriber AVP code Image: Bind to Subscriber AVP code Image: Regular expression Bind to Subscriber AVP code Image: Bind to Subscriber AVP code Image: Regular expression Bind to Subscriber AVP code Image: Bind to Subscriber AVP code Image: Regular expression Bind to Subscriber AVP code Image: Bind to Code Image: Regular expression Bind to Code Image: Bind to Code Image: Regular expression Bind to Code Image: Bind to Code Image: Bind to Code Image: Bind to Code Image: Bind to Code Image: Bind to Code Image: Bind to Code Image: Bind to Code Image: Bind to Code Image: Bind to Code Image: Bind to Code Image: Bind to Code Image: Bind to Code Image: Bind to Code Image: Bind	err msg	Err Msa			Text				
Name Display Name Regular Expression Description Index to the session/Policy State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield Image: State Pield <t< th=""><th>The values allowed in Control Center</th><th>r for this column</th><th>Validatio</th><th>n used by Control Cent</th><th>er</th><th>Which rows match wh</th><th></th><th>eived</th><th></th></t<>	The values allowed in Control Center	r for this column	Validatio	n used by Control Cent	er	Which rows match wh		eived	
Att Ramow @ @@ Bind to Session/Policy State Field Image: State Field Image: Sta	 List of Valid Values 				_	 Bind to Subscriber 	AVP code		
add: Ramove: Bind to a result column from another table add: Ramove: Bind to Diameter request AVP code Valid values pulled from another table's column (key) Emotion of the pulled from another table's column (key)	*Name	Display Name	Regular	Expression Descript	ion				
Add Sind to a result column from another table Index Sind to Diameter request AVP code Valid values pulled from another table's column (key) Sind to Diameter request AVP code						O Bind to Session/Po	licy State Field		
Add: Remove: Sind to Diameter request AVP code Valid values pulled from another table's column (key) Image: Column (key)							select	clear	
Add Remove of Bind to Diameter request AVP code						Bind to a result col	umn from another t	able	
Valid values pulled from another table's column (key)							select	i clear	
Valid values pulled from another table's column (key)						O Blad to Dismaker a	anuart AUR cade		
Matching Operator						C) bind to Diameter r	equest Ave coole		

Valid values is the place where all the valid error values can be configured in STG so that they are visible in CRD drop-down.

- ApplicationId: Application ID for which the mapping of Result-Code has to be done.
- Error: Internal error list.
- ResultCode: Result Code to be sent in answer.
- ExpResultCode: Experimental result code to be sent in answer. Vendor-Id will be sent in Answer only for Experimental result-Code.
- ErrMsg: Error message AVP sent in answer.



Note

Experiment result code will be sent when Result-Code is not configured. If both Result-Code and experimental Result-Code are present, Result-Code would take precedence.

For more information, see Error Result Code Profile.

Gx Session Routing

Gx Session Routing table is required for "table driven routing". Here an example for Gx New Session Rules is provided. If table driven routing is required for Rx or Sd, user needs to create similar tables for Sd and Rx as well.

Figure 32: Gx Session Routing

A Custom Reference Data 1	Some or all columns in this	s table have bee	n published a	nd will be read only.	Newly added columns	will be editable.	
*Name gx_session_routing	Display Name Gx Session Routing	g	✓ Cache Re	esults			
Activation Condition	Best Match		*Evaluation	n Order			
	select clear		0				
*Columns							
*Name	Display Name		*Use In C	onditic *Type		Key	Required
logical_apn	Logical APN		V	Text		\checkmark	\checkmark
origin_host	Origin Host		\checkmark	Text		\checkmark	\checkmark
peer_route	Peer Route		\checkmark	Text			
origin_realm	Origin Realm		\checkmark	Text		\checkmark	 Image: A set of the set of the
destination_host	Destination Host		\checkmark	Text		\checkmark	 Image: A set of the set of the
destination realm	Destination Realm		1	Text		1	~
Add Remove 🔂 😣							
Valid Values		Validation			Runtime Binding		
The values allowed in Control Cente	r for this column	Validation use	ed by Control	Center	Which rows match	when a message is	received
 All 		Regular Exp			None	5	
 List of Valid Values 					Bind to Subscri	AVD code	
0						ber AVP code	
*Name	Display Name	Regular Exp	ression Des	cription			
					O Bind to Session	/Policy State Field	
						s	elect clear
					O Bind to a result	column from anot	ner table
						s	elect clear
					C Bind to Dismot	ar request AVD cod	-

For more information, see Gx New Session Rules.

SLF Trigger Profile

This table is used to derive SLF destination type and SLF lookup type. Keys used for this table are: Application Id, cmd_code, and dest_realm. Output of this table are slf_lookup_type and slf_destination_type.

An example configuration is given.

Figure 33: SLF Trigger Profile - STG

Name		Display Name							
slf_trigger_profile		SLF Trigger Profile		Cache Resu	lts				
Activation Condition		h		*Evaluation O	rder				
		Best Match		0					
Columns				-					
*Name		Display Name		*1	Use In Co	nditic *Type		Key	Required
application_id		Application ID				Text		2	a
cmd_code		Command Code			/	Text		1	~
dest_realm		Destination Realm				Text		1	4
slf_lookup_type		SLF Lookup Type		, i	2	Text			2
slf_destination_type		SLF Destination Type			7	Text			
	er for this colu	mn	Validat	tion ion used by Contro	ol Center		Runtime Binding Which rows match when a n	nessage is receive	ed
	er for this colu	mn	Validat		ol Center]			ed
The values allowed in Control Center	er for this colu Display Nar		Validat Regula	ion used by Contro]	Which rows match when a n		ed
The values allowed in Control Center All Ust of Valid Values			Validat Regula	ion used by Contro ar Expression]	Which rows match when a n	ode	ed
The values allowed in Control Center All Ust of Valid Values			Validat Regula	ion used by Contro ar Expression]	Which rows match when a m None Bind to Subscriber AVP c	ode	
The values allowed in Control Center All Ust of Valid Values.			Validat Regula	ion used by Contro ar Expression			Which rows match when a m None Bind to Subscriber AVP c	ode ate Pield (select) c	lear
The values allowed in Control Center All Ust of Valid Values			Validat Regula	ion used by Contro ar Expression]	Which rows match when a m None Blind to Subscriber AVP o Blind to Session/Policy St	ode ate Pield (select) c	icar a
The values allowed in Control Center All Ust of Valid Values Name			Validat Regula	ion used by Contro ar Expression]	Which rows match when a m None Blind to Subscriber AVP o Blind to Session/Policy St	ode ate Pield (selecti) c rom another tabl	icar a
All Ust of Valid Values Nome	Display Nar	ne	Validat Regula	ion used by Contro ar Expression		1	Which rows match when a m None Bind to Subscriber AVP o Bind to Session/Policy St Bind to a result column t	ode ate Pield (selecti) c rom another tabl	icar a
The values allowed in Control Center All Ust of Valid Values *Name	Display Nar	ne	Validat Regula	ion used by Contro ar Expression]	Which rows match when a m None Bind to Subscriber AVP o Bind to Session/Policy St Bind to a result column t	ode ate Pield (selecti) c rom another tabl	icar a

For more information, see SLF Trigger Profile.

SLF Routing

This table is used to derive SLF session route key from SLF Destination. An example configuration is given.

Figure 34: SLF Routing - STG

Name		Display Name						
slf_routing		SLF Routing	Cac	he Results				
ctivation Condition	select dear	Best Match	*Evalu	ation Order				
Columns								
*Name		Display Name		*Use In Cor	nditic *Type		Key	Required
slf_destination		SLF Destination		2	Text		V	1
slf_session_route_key		SLF Session Route Key		<u>v</u>	Text			7
The values allowed in Control C All List of Valid Values	enter for this col	umn	Validation used b Regular Expres			Runtime Binding Which rows match when a m None Bind to Subscriber AVP o		L.
*Name	Display Na	me	Regular Expres	sion Description				
]	Bind to Session/Policy St	ate Field	
							select de	3.0
						Bind to a result column f	rom another table	
							select de	ar
Add Barrows & D						O Bind to Diameter request	AVP code	
Add Ramova 🙀 🕹						Bind to Diameter request	AVP code	
Add Remove 🔐 💀	ther table's colur					Bind to Diameter request Matching Operator	AVP code	

For more information, see SLF Routing.

S6/Sh Table Driven Rules

This table is used for the table driven routing of S6/Sh messages. Fields origin_host, origin_realm, dest_realm, dest_host, msisdn, imsi are used as keys to derive the peer_route.

An example configuration is given.

Figure 35: S6 Table Driven Rules - STG

*Name		Display Name						
TB_S6		S6_TB_Rules		Cache Results				
Activation Condition				*Evaluation Order				
	select clear	Best Match		0				
Columns								
*Name			Display Name		*Use In C	Conditi *Type	Key	Required
origin_host			Origin Host			Text	$\overline{\checkmark}$	V
origin_realm			Origin Realm		$\overline{\checkmark}$	Text	1	$\overline{\checkmark}$
destination_host			Destination Ho	ost	V	Text	1	V
destination_realm			Destination Re	alm	$\overline{\checkmark}$	Text		
imsi			IMSI		V	Text	1	~
neer route			Reer Route			Text		
Valid Values	enter for this col	umn	Validation Validation us	ed by Control Center	Runtime Bin Which rows	ding match when a me	ssage is rece	ived
Column Details	enter for this col	umn					ssage is rece	ived
Valid Values The values allowed in Control Ce	enter for this col	umn	Validation us		Which rows			ived
Valid Values The values allowed in Control Ce All		umn Display Name	Validation us Regular Exp		Which rows	match when a me		ived
Valid Values The values allowed in Control Ce all List of Valid Values			Validation us Regular Exp	pression	Which rows None Bind to S	match when a me		ived
Valid Values The values allowed in Control Ce all List of Valid Values			Validation us Regular Exp	pression	Which rows None Bind to S	match when a me	e Field	ived
Valid Values The values allowed in Control Ce			Validation us Regular Exp	pression	Which rows None Bind to S Bind to S 	match when a me	e Field	dear
Valid Values The values allowed in Control Ce			Validation us Regular Exp	pression	Which rows None Bind to S Bind to S 	match when a men iubscriber AVP code	e Field select n another ta	dear
Valid Values The values allowed in Control Ce all List of Valid Values			Validation us Regular Exp	pression	Which rows None Bind to 5	match when a men iubscriber AVP code	e Field select) n another ta	<u>dear</u> ble
Valid Values The values allowed in Control Ce All Dat of Valid Values Name		Visplay Name	Validation us Regular Exp	pression	Which rows None Bind to 5	match when a mes	e Field select) n another ta	<u>dear</u> ble

For more information, see S6/Sh Table Driven Rules.

Custom Reference Data Tables

APN Mapping

This table provides information related to APN Mapping. The read-only APN Mapping are shown below:

Figure 36: APN Mapping - CRD Table

Name	Display Name		_				
apn_mapping	APN Mapping		Cache Res	ults			
ctivation Condition		*	Evaluation	Order			
	select clear Best Match	[0				
Columns							
Name	Display Name		*Use In C	onditic *Type		Key	Required
called_station_id	Called Station Id		\checkmark	Text		 Image: A set of the set of the	~
logical_apn	Logical APN		\checkmark	Text			
dd Remove 😯 👃							
alid Values		Validation			Runtime Binding		
The values allowed in Control	Center for this column	Validation used	by Control C	enter	Which rows match whe	en a message is r	eceived
 All 		Regular Expre	ssion		None		
List of Valid Values					Bind to Subscriber	AVP code	
*Name	Display Name	Regular Expre	ssion Desci	iption			
					Bind to Session/Po		_
							ect <u>clear</u>
					 Bind to a result col 		
						sel	ect <u>clear</u>
						equest AVP code	

- Called-Station-Id: This is the AVP from which APN is derived. This also is the key column for this table. It is bound to the session or Policy State field as shown in the snapshot.
- Logical_APN: This is the mapped logical name that is used for referencing and processing the message within the system.

Note

For sample data configuration, refer the CPS Control Center Interface Guide for Full Privilege Administrators for this release.

Peer Access Control List

You can use the Peer Access Control List to specify the list of peers (by realm, FQDN, and applications) that can establish peer connections to vDRA so that unknown peers are not permitted to create Diameter peer connections.

Figure 37: Peer Access Control List

Name	Display Name						
peer_access_control_list	Peer Access Control List		Cache R				
Activation Condition			*Evaluation	Order			
	anletta citar		0				
Columns							
*Name	Display Name		*Use In C	onditic *Type		Key	Required
origin_host	Origin Host		¥.	Text		1	1
origin_realm	Origin Realm		1	Text		1	1
auth_action	Authorization Action		V	Number			1
error_code	Authorization Action Deny - Res	sult Code	1	Number			
error_msg	Authorization Action Deny - Erro	or Message	2	Text			
annlication id	Annlication Id		1	Text			1
Add Memore We we							
Column Details							
Valid Values	Val	lidation			Runtime Binding		
The values allowed in Control Cent	er for this column Val	lidation use	d by Control	Center	Which rows match	when a message is	s received
 All 	Re	gular Expr	ession		(None		
C List of Valid Values					O Bind to Subscri	ber AVP code	
*Name	Display Name Re	gular Expr	ession Des	cription			
					O Bind to Session	/Policy State Field	
					<u></u>		sleet) clear

Peer Routes

This tables provides the information related to Peer Routes available in the system. The read-only peer routes are shown below:

Figure 38: Peer Routes - CRD Table

*Name	Display Name		Activation Co	ondition			
peer_route	Peer Routes	Cashe Results			selected dear		
Columns							
*Name	Display Name		*Use In Co	nditi *Type		Key	Required
peer_route	Peer Route		2	Text		~	[✓]
Add Remove 6 6	8						
Valid Values		Validation			Runtime Binding		
The values allowed in	Control Center for this column	Validation use	d by Control C	Center	Which rows match wh	nen a message is	received
() All		Regular Expr	ession		None		
*Name	Display Name	Regular Expr	ession Descri	ption			
					O Bind to Session/P		
						-00	lette clear

Peer Group SRK Mapping

This table provides the information related to Peer Groups in the system. The read-only peer groups are shown below:

Figure 39: Peer Group - CRD Table

Name	Display Name		Activation Con	dition			
peer_group_srk_mapping	Peer Group SRK Mapping	Cache Results			select dear		
Columns							
*Name	Display Name		*Use In (Conditic *Type		Key	Require
peer_group	Peer Group		1	Text		1	×
session_routing_key	Session Routing	Key	1	Text			
lest_host_routing_rule	Destination Host	Routing Rule	1	Text			1
dest_host_replace_rule	Destination Host	Replace	1	Text			
dest_realm_replace_rule	Destination Real	m Replace	V	Text			
Ndd Remove with the							
/alid Values		Validation			Runtime Binding		
	Center for this column		by Control Cente	r		n a message is receive	ed
The values allowed in Control	Center for this column	Validation used	by Control Cente	r	Which rows match whe	n a message is receive	ed
The values allowed in Control All 	Center for this column			r	Which rows match whe		ed
The values allowed in Control	Center for this column	Validation used	ession		Which rows match whe		ed
The values allowed in Control All List of Valid Values 	Center for this column Display Name	Validation used			Which rows match whe		ed
The values allowed in Control		Validation used	ession		Which rows match whe	IVP code	ed
The values allowed in Control		Validation used	ession		Which rows match whe	WP code	
The values allowed in Control All List of Valid Values		Validation used	ession		Which rows match whe None Bind to Subscriber J Bind to Session/Poll	LVP code cy State Field	dear
The values allowed in Control		Validation used	ession		Which rows match whe	WP code cy State Field selecte c	dear e
The values allowed in Control		Validation used	ession		Which rows match whe None Bind to Subscriber J Bind to Session/Poll	LVP code cy State Field	dear e
The values allowed in Control All Ust of Valid Values Name		Validation used	ession		Which rows match whe None Bind to Subscriber J Bind to Session/Poll	vvP code cy State Field mn from another table select) c	dear e
The values allowed in Control All List of Valid Values *Name Add. Remove () ()	Display Name	Validation used	ession		Which rows match whe	vvP code cy State Field mn from another table select) c	dear e
The values allowed in Control	Display Name	Validation used	ession		Which rows match whe	vvP code cy State Field mn from another table select) c	dear e

- Peer Group: Name of the peer group.
- Session Routing Key: Routing token for this Peer Group.
- Destination Host Routing Rule: Defines Routing behavior of this group.

Peer Routing

This table provides the information related to peer routing in the system. The read-only peer routings are shown below:

Figure 40: Peer Routing - CRD Table

*Name	Display Name	Cada Sends	Activation (Condition			
peer_routing	Peer Routing	Gadhe Results			selected clear		
Columns							
*Name	Display Name		*Use In C	onditi *Type		Key	Required
peer_route	Peer Route		1	Text			1
system_id	System Id		~	Text		$\overline{\mathbf{v}}$	1
peer_group	Peer Group		~	Text		1	1
precedence	Precedence		2	Number			1
weight	Weight		V	Number			9
Column Details							
Valid Values	ntrol Center for this column	Validation Validation use	d hu Control	Cashar	Runtime Binding Which rows match whe		an entire of
	nuroi center for this column			Center		en a message is	received
					None		
		Regular Expre					
		Regular Expre					
	Display Name	Regular Expre		iption	O Bind to Subscriber		
	Display Name			iption	Bind to Subscriber Bind to Session/Pol		

• Peer Route: Identifier of this Peer Route.

- System ID: System Identifier for this VM.
- Peer Group: Identifier of the Peer group on this peer Route.
- Precedence: of the peer group on this Peer Route.
- Weight: Weight of the peer group on this Peer Route.

Binding Key Profile

This table provides the information related to binding key profile in the system. The read-only keys are shown below:

Figure 41: Binding Key Profile - CRD Table

Name	Display Name		Activation Cond	ition			
binding_key_profile	Binding Key Profile	Cache Results			selecti dear		
Columns							
*Name	Display Nam	8	*Use In O	onditic *Type		Key	Require
profile_name	Profile Name		· ·	Text		1	V.
imsi_apn	IMSI APN Ke	y Enabled	12 C	True/False			
msisdn_apn	MSISON APA	Key Enabled	1	True/False			
framed_ipv6_prefix	Framed IPv6	Enabled	2	True/False			
framed_ipv4	Framed IPv4	Enabled	2	True/False			
All List of Valid Values		Regular Expr			None Bind to Subscriber AVP	code	
*Name	Display Name	Begular Expr	ession Descriptio				I.
	anapital manna				Bind to Session/Policy 5	State Cald	
				_	Control to Sesarchy Policy :		
						select clear	
					Bind to a result column	from another table	
						select clear	
Add Remove		1.0			O Bind to Diameter reque	st AVP code	
	m another table's column (key)						1
C vana vance punce ing					Matching Operator		
	selects dear						
Actions							
10000119							

- Profile Name: This is the name given to the Bind profile that is associated with keys that are either enabled and/or disabled.
- MSI APN Key Enabled: Enabling this field would mean that bindings will be stored in IMSI APN collections in bindings database.
- MSISDN APN Key Enabled: Enabling this field would mean that bindings will be stored in MSISDN APN collections in bindings database.
- Framed IPv6 Enabled: Enabling this would mean binding data would be stored in "ipv6bindings" collection.
- Framed IPv4 Enabled: Enabling this would mean binding data getting stored in "ipv4bindings" collection.

Refer to Binding Key Profile for configuration in Control Center.

Appld Key Profile Mapping

This table stores the mapping between Application Identifiers and Bind Key Profile Names. The Application Identifiers are pre-provisioned for two Application Identifiers as Gx and Rx. Similarly, the BindingKeyProfile is also tied to the Profile Name column of the "BindingKeyType_Profile" table:

Figure 42: Appld Key Profile Mapping- CRD Table

Name	Display Name		Activation Cont	lition			
app_id_key_profile_mapping	App Id Key Profile Mapping	Cache Results			select clear		
Columns							
*Name	Display Name		*Use In C	onditic *Type		Key	Required
application_id	Application Id		V	Text		Image: A start and a start	2
profile_name	Profile Name		~	Text			
Add) Remove 🖗 🕹							
/alid Values		Validation			Runtime Binding		
The values allowed in Control Ce	nter for this column		d by Control Center	5	Which rows match when a	message is received	
 All 		Regular Expr	ession	_	None		
C List of Valid Values					Bind to Subscriber AVI	P code	
*Name	Display Name	Regular Expr	ession Descriptio	'n			
					Bind to Session/Policy	State Field	_
						select des	IC.
					Bind to a result column		
						select des	
					Bind to Diameter requ		
Add Remove 😯					U Bind to Diameter requ	est AVP code	
Valid values pulled from anot	her table's column (key)						
	select dear				Matching Operator		
					100		
- Actions							
Copy:							

Message Rate Limit Profile

This table gives a provision to configure Message Rate Limits at a profile level.

*Name	Display Name		ation Condition			
message_rate_limit_profile	Message Rate Limit Profile	Cache Results		select clear		
*Columns						
*Name	Display Name	*Use In	Conditic *Type		Key	Required
profile_name	Rate Limit Profile Name		Text			\checkmark
app_id	Application Identifier		Number		~	\checkmark
command_code	Command Code		Number			V
mesg_type	Message/Request Type		Number		V	V
rate_limit	Message Rate Limit		Number			V
Column Details Valid Values The values allowed in Control Cer		Validation Validation used by Control	Center	Runtime Binding Which rows match w	hen a message is r	eceived
Valid Values The values allowed in Control Cer All	nter for this column		Center	Which rows match w	-	eceived
Valid Values The values allowed in Control Cer	nter for this column	Validation used by Control		Which rows match w	-	eceived
Valid Values The values allowed in Control Cer All List of Valid Values	nter for this column	Validation used by Control Regular Expression		Which rows match w	er AVP code	eceived
Valid Values The values allowed in Control Cer All List of Valid Values	nter for this column	Validation used by Control Regular Expression		Which rows match w None Bind to Subscribe	er AVP code Policy State Field	eceived
Valid Values The values allowed in Control Cer All List of Valid Values	nter for this column	Validation used by Control Regular Expression		Which rows match w None Bind to Subscribe	er AVP code Policy State Field	ect <u>clear</u>
Valid Values The values allowed in Control Cer All List of Valid Values	nter for this column	Validation used by Control Regular Expression		Which rows match w None Bind to Subscribe Bind to Session/F	Prolicy State Field	ect clear

- Profile Name: Unique Identifier for a profile.
- Application ID: Application Identifier for this row. 3GPP App Ids only are allowed here.
- Command Code: Command Code of the message that is applicable on the said interface specified by Application Id above.
- Message Type: Initial/Update/Terminate or None for messages that do not have them. The message
 request type should be same as specified for the command code in Policy Builder under Diameter
 Application.
- Rate Limit: This field is to specify the threshold in TPS above which the diameter messages are discarded. This value should be more than the Peer Rate Limit in order for message level rate limit to be applied.
- Profile Name: Unique Identifier for a profile.

Refer to Message Rate Limit Profile for configuration in Control Center.

Reserved IMSI

You can configure the Reserved IMSI CRD table to validate a parsed IMSI for SLF routing against a configured list of reserved MCC ranges.

The CRD has two main columns : MCC Start range and MCC End Range. The MCC consists of the first three digits of an IMSI.

If the IMSI matches a reserved IMSI, the value is ignored for SLF routing.

You can provide support up to ten distinct (non-overlapping) MCC ranges as Reserved IMSIs.

The DRA/SLF ignores AVPs that contain such IMSIs, and continues searching other AVPs in the Diameter request, for a valid address to be used for address resolution.

The following image shows a sample Reserved IMSI configuration:

Figure 44: Reserved IMSI

*Name	Display Name	Caste Results	Activitie	in Condition	
reserved_mcc	Reserved MCC	Cathe Results			interest char
*Columns					
*Name	Display Name		*Use In Cor	nditic *Type	
mcc_start	MCC Start		2	Number	
mcc_end	MCC End		0	Number	
(add) (America) (iii) (Column Details					
Valid Values		Validation			Runtime Binding
The values allowed in	Control Center for this column	Validation used by	Control Cer	nter	Which rows match
(8.44)		Regular Express	lon		· None
C Dat of Valid Values					O Bind to Subscrit
*Name	Display Name	Regular Express	ion Descrip	otion	
					O Bird to Similary

Trusted Realm Profile

Trusted Realm Profile is used for topology hiding. The CRD includes the following columns:

- Trusted Profile Name: Profile Name having a trusted realm mapped to it.
- Trusted Realm: Realm for which Topology Hiding is not required.

Figure 45: Trusted Realm Profile

Name	Display Name				
trusted_realm_profile	Trusted Realm Profile	Cache Rea			
Activation Condition	annut clear	[2] Best Hatz			
Evaluation Order					
0					
Columns					
*Name	Display Name	*Use In C	Conditic *Type	Key	Required
	Trusted Profile Name	2	Text	3	4
profile_name	Trusten Fruthe Henrie			100	
profile_name trusted_realm	Trusted Realm	~	Text	~	

Protected Realm Trusted Profile Mapping

Protected Realm Trusted Profile Mapping is used for topology hiding. The CRD includes the following columns:

- Protected Realm: Realm that is protected (topology hiding is required).
- Profile Name: Profile having realms that are trusted for this protected realm and that do not require topology hiding.

Figure 46: Protected Realm Trusted Profile Mapping

Name	Display Name				
protected_realm_trusted_profile	Protected Realm Trusted Profile #				
ctivation Condition	The Ort Date	2 Inst Parch			
Evaluation Order					
0					
Columna					
0 Columns	Display Name	*Use In Care	DOX *Type	Key	Required
0 Columna Name	Display Name Protected Realm	120000	DDX *Type Text	Key	2
0					Required

MME Alias Map

MME Alias Map is used for topology hiding. The CRD includes the following columns:

- MME FQDN: FQDN of MME that requires topology hiding.
- Alias1: Mandatory. An alias identity used for the protected host that belongs to an MME in the network.
- Alias 2: Optional. Alternate Alias that can be used for Topology Hiding for the given MME FQDN.
- Alias 3: Optional. Alternate Alias that can be used for Topology Hiding for the given MME FQDN.

Figure 47: MME Alias Map

Name	Display Name		Activati	ion Condition			
mme_allas_map	MME Allas Map	Cadre Results	1		mainith Cent		
The Crd Deca							
Columns							
			Alter In the	inditic *Type		Key	Required
*Name	Display Name		-Use in Co	motor - type		No.4	
	MME FQON		-Use In Co	Text		3	1
*Name mme_host allas1	12.22 - 24.22		4				
mme_host	MME FQON			Text			1

Add deres - -

HSS Aliases

HSS Aliases is used for topology hiding. The CRD includes the following columns:

- HSS Alias FQDN: Alias FQDN used to replace a protected HSS FQDN.
- Shared Alias: Boolean variable used to indicate whether the Alias FQDN is shared across multiple HSS servers or not.

Figure 48: HSS Aliases

hss_aliases HSS Aliases	Cache Results		Malanti, Cost		
Svn Ord Data					
Columns					
*Name Display Name		Use In Condition	(*Type	Key	Required
hss_alias HSS Alias FQDN	6	1	Text	2	4
is_shared_alias Shared Alias		21	True/False		2

Add Harmon Q .

HSS Alias Map

HSS Alias Map is used for topology hiding. The CRD includes the following columns:

- HSS FQDN: FQDN of HSS peer.
- Alias1: Required field which is derived from HSS Alias CRD.
- Alias2: Optional. Alias for the HSS FQDN.
- Alias3: Optional. Alias for the HSS FQDN.

Figure 49: HSS Alias Map

Name	Display Name		Activities	Condition			
hss_alias_map	HSS Allas Map	Ceche Results			simh) cear		
Svn Crd Deta							
Columns							
*Name	Display Name		*Use In Cond	lick *Type	Ki		Required
hss_host	HS\$ FQDN		<i>2</i>	Text	-	č.	8
allast	Allas1		9	Text			2
alias1							
alias2	Alias2		9	Text			

Binding Key Profile Creation Map

This table provides the information related to binding key type profile creation map in the system. The read-only keys are shown below:

Figure 50: Binding Key Profile Creation Map - CRD Table

*Name	Display Name	_			
bind_key_profile_creation_map	Binding Key Profile Creation Map	Cache Res	sults		
Activation Condition	adb) clear Svn Crd Data	🖌 Best Matc	h		
*Evaluation Order					
a contraction of the state					
0					
0					
0 Columns	Display Name	*Use In C	Conditic *Type	Кеу	Required
0 Columns	Display Name Application Identifier	*Use In C	Conditic *Type Text	Key 🗸	Required
0 *Columns *Name				1000	Alexander and a second
0 *Columns *Name appl_id	Application Identifier		Text		

- Application Identifier: Application ID of the message.
- Called Station Id: Called-Station-Id AVP value from the Diameter message.
- Binding Key Profile: Profile name from binding key profile.

Refer to Binding Key Profile Creation Map for configuration in CPS Central.

Binding Key Profile Read Map

This table provides the information related to binding key type profile read map in the system. The read-only keys are shown below:

Figure 51: Binding Key Profile Read Map - CRD Table

*Name	Display Name				
bind_key_profile_read_map	Binding Key Profile Read Map	Cache Re	suits		
Activation Condition	electi clear	🛃 Best Mato	h		
*Evaluation Order					
0					
0					
0	Display Name	*Use In C	Conditic *Type	Кеу	Required
0 *Columns *Name	Display Name Application Identifier	*Use In C	Conditic *Type Text	Key	Required
0 Columns *Name appl_id					
0 *Columns	Application Identifier	v	Text		

Add Remove 😚 😽

- Application ID: Application ID from the message.
- Origin Host: Origin host from the message.
- Origin Realm: Origin realm from the message.
- Binding Key Profile: Profile name from binding key profile.

Refer to Binding Key Profile Read Map for configuration in CPS Central.