



# Policy Builder Configuration

---

- [Plug-in Configuration, on page 1](#)
- [Diameter Application, on page 27](#)
- [Routing AVP Definition, on page 34](#)
- [Custom Reference Data Tables, on page 38](#)

## Plug-in Configuration

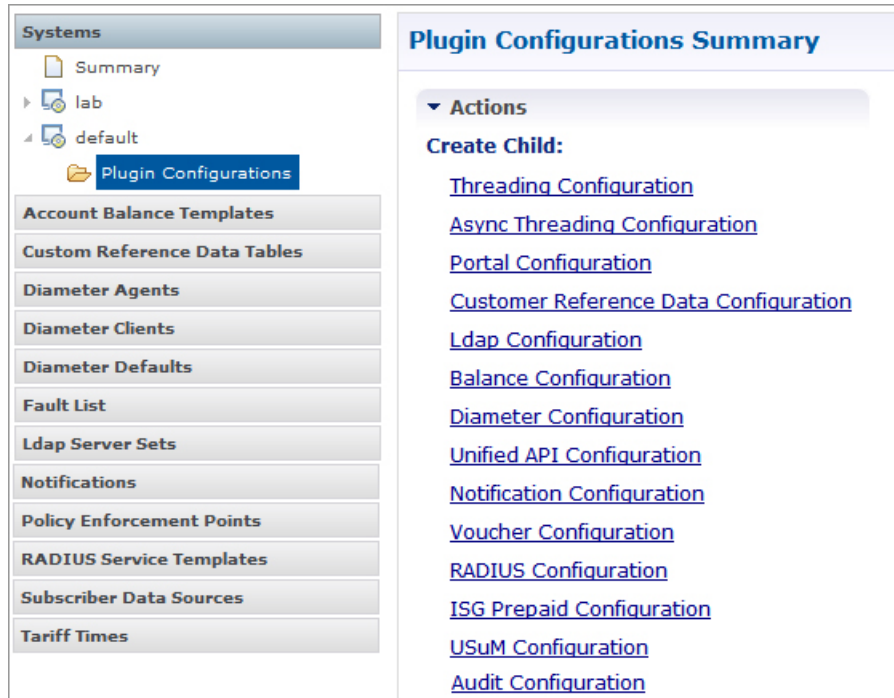
Cisco Policy Builder provides core plug-ins for customizing and optimizing your installation.

- 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



## 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: <ul style="list-style-type: none"> <li>• broadhop-bindings</li> <li>• broadhop-slf</li> <li>• broadhop-receivers</li> <li>• broadhop-qprocessor</li> </ul>
Threads	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.
<b>Action Configurations Table</b>	
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**

The screenshot shows a configuration window titled "Custom Reference Data Configuration". It contains the following fields:

- \*Primary Database IP Address:** localhost
- Secondary Database IP Address:** (empty)
- \*Database Port:** 27717
- \*Db Read Preference:** Primary (dropdown menu)
- \*Connection Per Host:** 100

215175

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.

Table 3: 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	<p>Read preference describes how sessionmgr clients route read operations to members of a replica set. You can select from the following drop-down list:</p> <ul style="list-style-type: none"> <li>• Primary: Default mode. All operations read from the current replica set primary.</li> <li>• PrimaryPreferred: In most situations, operations read from the primary but if it is unavailable, operations read from secondary members.</li> <li>• Secondary: All operations read from the secondary members of the replica set.</li> <li>• SecondaryPreferred: In most situations, operations read from secondary members but if no secondary members are available, operations read from the primary</li> </ul> <p>For more information, refer to <a href="http://docs.mongodb.org/manual/core/read-preference/">http://docs.mongodb.org/manual/core/read-preference/</a>.</p>
Connection Per Host	<p>Number of connections that are allowed per DB Host.</p> <p>Default value is 100.</p>

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.

Figure 3: DRA Configuration

**D R A Configuration**

<b>*Stale Session Timer Minutes</b>	<b>Rate Limiter</b>
<input type="text" value="1"/>	<input type="text" value="10"/>
<b>Stale Session Expiry Count</b>	<b>*Binding DB Read Preference</b>
<input type="text" value="6"/>	<input type="text" value="Nearest"/>
<b>Stale Binding Expiry Minutes</b>	<b>Stale Binding Refresh Minutes</b>
<input type="text" value="10080"/>	<input type="text" value="2880"/>

**Binding DB Retries**

**Binding Creation, Primary Alternate System**

**Binding Creation, Secondary Alternate System**

**Binding Routing, Primary Alternate System**

**Binding Routing, Secondary Alternate System**

The following parameters can be configured under DRA Configuration:

Table 4: DRA Configuration Parameters

Parameter	Description
Stale Session Timer Minutes	<p>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.</p> <p>Default: 180 minutes (recommended value)</p> <p>Minimum: 10 minutes</p> <p>Maximum: 10080 minutes</p>
Rate Limiter	<p>Indicates the number of audit RARs per second that should be sent out by CPS vDRA.</p> <p>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.</p> <p>Default: 10 (recommended value)</p> <p>Minimum: 1</p> <p>Maximum: 1000 (maximum number of RAR messages per second from vDRA to PCEF)</p>

Parameter	Description
Stale Session Expiry Count	<p>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.</p> <p>Default: 6 (recommended value)</p> <p>Minimum: 0 (Session deleted without sending RAR)</p> <p>Maximum: 10</p>
Binding DB Read Preference	<p>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.</p> <p>Default: Nearest (recommended setting)</p>
Stale Binding Expiry Minutes	<p>Duration after which the binding database records expire.</p> <p>The timer is initialized when the session is created.</p> <p>The records are deleted when the time since the last refresh exceeds Stale Binding Refresh Minutes.</p> <p>Default: 10080 minutes (168 hours or one week) (recommended value)</p> <p>Minimum: 10 minutes</p> <p>Maximum: 43200 minutes (28 days)</p> <p>For more information about binding DB audits and stale records, see <a href="#">Binding DB Audit, on page 11</a>.</p>
Stale Binding Refresh Minutes	<p>Duration for which the expiry time of the binding database records is refreshed.</p> <p>Default: 2880 minutes (48 hours or 2 days - recommended value).</p> <p>Minimum: 10 minutes</p> <p>Maximum: 10080 minutes (one week)</p> <p><b>Note</b> Stale Binding Expiry Minutes should be multiple of Stale Binding Refresh Minutes.</p> <p>Stale Binding Refresh Minutes should be greater than Stale Session Timer Minutes.</p>

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 <a href="#">DRA Inbound Endpoints, on page 17</a> .
DRA Outbound Endpoints	Refer to <a href="#">DRA Outbound Endpoints, on page 19</a> .
Relay Endpoints	Refer to <a href="#">Relay Endpoints, on page 21</a> .

## Settings

Click **Settings** check box to open the configuration pane.

The following parameters can be configured under **Settings**:



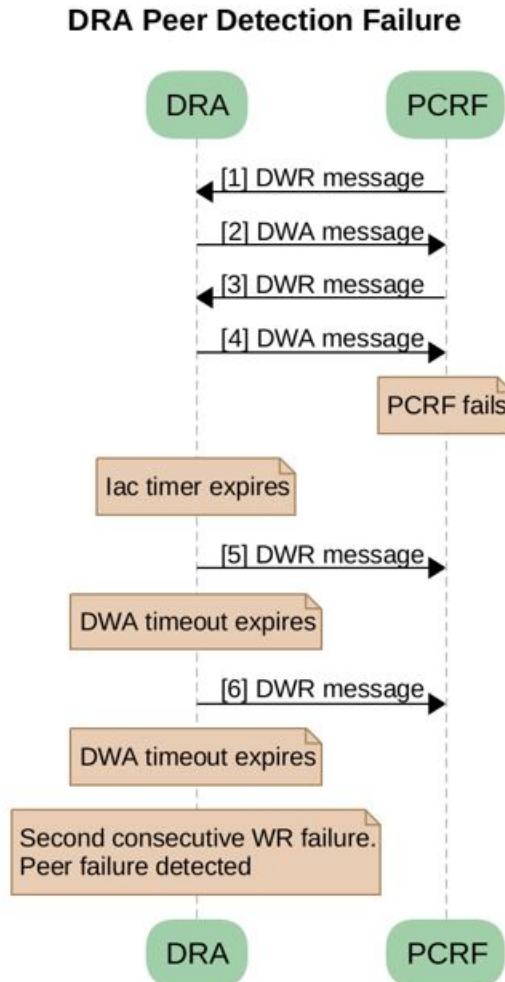
Table 5: DRA Configuration - Settings Parameters

Parameter	Description
Stop Timeout Ms	<p>Determines how long the stack waits for all resources to stop. The delay is in milliseconds.</p> <p>Default: 10000 ms (recommended value)</p> <p>Minimum: 1000 ms</p> <p>Maximum: 60000 ms (one minute)</p>
Cea Timeout Ms	<p>Determines how long it takes for CER/CEA exchanges to timeout if there is no response. The delay is in milliseconds.</p> <p>Default: 10000 ms (recommended value)</p> <p>Minimum: 1000 ms</p> <p>Maximum: 60000 ms (one minute)</p>
Iac Timeout Ms	<p>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.</p> <p>Default: 5000 ms (recommended value)</p> <p>Minimum: 1000 ms</p> <p>Maximum: 30000 ms (30 seconds)</p>
Dwa Timeout Ms	<p>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.</p> <p>The delay is in milliseconds.</p> <p>Default: 10000 ms (recommended value)</p> <p>Minimum: 1000 ms</p> <p>Maximum: 60000 ms (one minute)</p>

Parameter	Description
Dpa Timeout Ms	<p>Determines how long it takes for a DPR/DPA exchange to timeout if there is no response. The delay is in milliseconds.</p> <p>Default: 5000 ms (recommended value)</p> <p>Minimum: 1000 ms</p> <p>Maximum: 30000 ms (30 seconds)</p>
Rec Timeout Ms	<p>Determines how long it takes for the reconnection procedure to timeout. The delay is in milliseconds.</p> <p>Default: 10000 ms (recommended value)</p> <p>Minimum: 1000 ms</p> <p>Maximum: 60000 ms (one minute)</p>
Drain Timeout Ms	<p>Indicates the time that a peer connection remains open for responses to be sent to peers even if DPR is sent or received by vDRA.</p> <p>If a DPR is sent or received by vDRA, vDRA does not route requests to the disconnecting peer connection via any routing (Dest-Host, SRK, Binding, Table-Driven). However, responses and in-flight requests sent to the corresponding peers till the duration of Drain Timeout. This allows vDRA to gracefully shut down when any remote peer sends a DPR so as to minimize the diameter message loss.</p> <p>Default: 2000 ms</p> <p>Maximum: Must be less than Dpa timeout Ms</p>

The following figure illustrates the timers in peer detection:

Figure 4: vDRA 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 5: Binding DB Audit

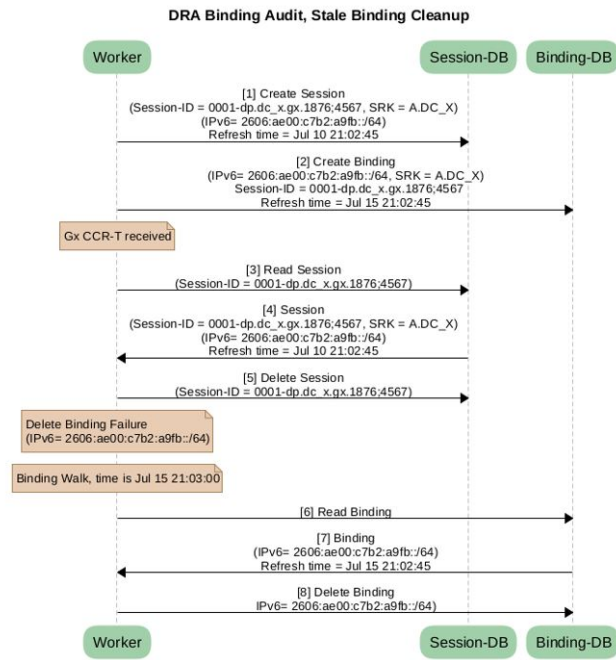
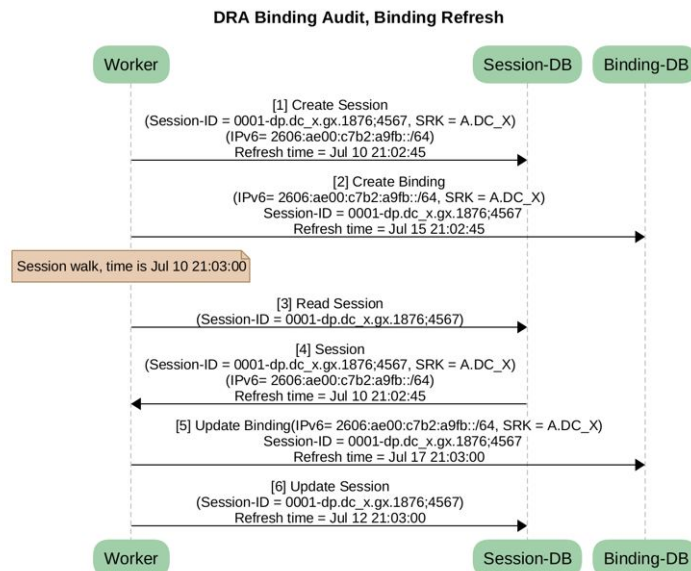


Figure 6: Binding Refresh



## 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	<p>Allowable TPS on a single instance of policy server (QNS) process running on the Policy Director.</p> <p>Minimum: 1 Maximum: 5000</p> <p><b>Note</b> Contact your Cisco representative for usecase-specific recommended values.</p>
Result-Code in Response	<p>Indicates the error code that must be used while rejecting requests, due to rate limits being reached.</p> <p>Default: 3004</p>
Error Message in Response	<p>Select the check box to drop the rate-limited messages without sending error response.</p> <p>If the check box is not selected, then the rate limited message are dropped with error response as configured.</p>
Drop Requests Without Error Response	<p>Select the check box to drop rate limited messages without sending error response.</p> <p>If the check box is unchecked, then the rate limited messages are dropped with error response as configured.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• Send Error Response</li> <li>• Drop Message</li> </ul> <p>Default: Unchecked (recommended setting)</p> <p>For more information, refer to Peer Rate Limit.</p> <p><b>Important</b> 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.</p>

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

Table 7: Rate Limiting Combinations

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	Yes	Yes

## DRA Feature

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

Figure 7: DRA Configuration - DRA Feature

### \*D R A Feature

- Gx Session Disconnect On5065
- Update Time Stamp On Sucess R A A
- Update Time Stamp On Sucess C C R U
- Enable Mediation
- Enable Doic
- Enable Proxy Bit Validation
- Enable PCRF Session Query
- Create IPv6 Bindings based on PCRF Session Query

The following parameters can be configured under **DRA Feature**:

Table 8: DRA Features

Parameter	Description
Gx Session Tear Down On5065	<p>By default, <b>Gx Session Tear Down On5065</b> flag is enabled (recommended setting).</p> <p>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.</p> <p><b>Important</b> 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.</p>
Update Time Stamp On Success RAA	<p>When this check box is selected, session timestamp will be updated on receipt of success RAA (Result-Code: 2001) from PCEF. <sup>1</sup></p> <p>Default is checked (recommended setting)</p> <p><b>Important</b> 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.</p>
Update Time Stamp On Success CCRU	<p>When this check box is selected, session timestamp will be updated on receipt of success CCR-U (Result-Code: 2001) from PCEF. <sup>2</sup></p> <p>Default is unchecked (recommended setting)</p> <p><b>Important</b> 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.</p>
Enable Proxy Bit Validation	<p>Enables P bit validation.</p> <p>vDRA validates the P bit in the Diameter request and, if set, the message maybe proxied, relayed, or redirected.</p> <p>If this option is disabled, the P bit in the request is not checked and the request is not considered proxiable.</p> <p>Default: Enabled.</p>

Parameter	Description
Enable Mediation	<p>Enable advanced mediation capabilities in both egress and ingress direction.</p> <p>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.</p>
Enable Doic	<p>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).</p> <p>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.</p>
Enable PCRF Session Query	<p>Enables or disables the PCRF session query. If you enable this, Policy DRA then supports a fallback routing for Rx AARs for VoLTE using the PCRF session query. This ensures that VoLTE calls can complete in the event that IPv6 binding is not found in the binding database.</p> <p>For an Rx AAR with an IPv6 binding query, vDRA provides the ability to route the Rx AAR based on an API query to the PCRF to determine if it has a session for the IPv6. The queries can be made in parallel to a configured set of query points on PCRFs.</p> <p>The Framed-IPv6 AVP from the Rx must be provided in the request to the PCRF. PCRF returns an SRK to be used for routing, similar to existing binding lookups.</p>



Parameter	Description
Create IPv6 Bindings based on PCRF Session Query	<p>Enables creation of IPv6 binding record in the database based on PCRF session query.</p> <p>When PCRF session query result (success) is received and if IPv6 record is not present in the database, vDRA creates an IPv6 binding record based on the response from the PCRF.</p> <p>If any CCR-I is received for the same IPv6 record, then it overwrites the IPv6 binding record. For any CCR-T, vDRA deletes the IPv6 binding record from database.</p> <p><b>Note</b> Ensure you also enable PCRF Session Query for this feature to work.</p> <p>The Stale Binding Expiry and Refresh Minutes are used to clear these binding records from the database. For more information, see <a href="#">Binding DB Audit, on page 11</a>.</p>
Slf Max Bulk Provisioning TPS	<p>Rate at which subscribers are provisioned in the SLF database.</p> <p>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.</p> <p>For more information about SLF bulk provisioning, see the <i>CPS vDRA Operations Guide</i>.</p>

<sup>1</sup> 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.

<sup>2</sup> 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**:



**Note** To handle loads of 15 K TPS or more, create multiple TCP connections with PCRF and apply the same configuration to all DRA Directors.

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.
Fqdn	Fully Qualified Domain Name of the CPS vDRA endpoint.
Transport Protocol	<p>Allows you to select either 'TCP' or 'SCTP' for the selected DRA endpoint.</p> <p>Default value is TCP.</p> <p>If the DRA/relay endpoint is to be configured for SCTP, the Transport Protocol should be selected as SCTP for those endpoints.</p>
Multi-Homed IPs	<p>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.</p> <p>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.</p> <p><b>Note</b> 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.</p> <p><b>Note</b> Both IPv4 and IPv6 are supported in vDRA endpoint configuration. For IPv6, you can enter either short or long format.</p> <p>The configuration for multi-homing is validated by netstat command on lb01:</p> <pre>netstat -apn   grep 3898</pre>



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

An example configuration is shown below:

**Figure 8: DRA Inbound Endpoints - Example Configuration**

**DRA Inbound Endpoints**

*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	<input type="checkbox"/>	3868
lab	10.1.1.1	gx-dra2.cisco.com	gx-dra2	TCP		Gx Application	<input type="checkbox"/>	3869
lab	10.1.1.1	gx-dra3.cisco.com	gx-dra3	TCP		Gx Application	<input checked="" type="checkbox"/>	3870
lab	10.1.1.1	rx-dra1.cisco.com	rx-dra1	TCP		Rx Application	<input type="checkbox"/>	4868
lab	10.1.1.1	rx-dra2.cisco.com	rx-dra2	TCP		Rx Application	<input checked="" type="checkbox"/>	4869
lab	10.1.1.1	sd-dra1.cisco.com	sd-dra1	TCP		Sd Application	<input checked="" type="checkbox"/>	6868

Add Remove  

## 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 endpoint.
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	<p>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.</p> <p>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.</p> <p><b>Note</b> 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 (<code>rp_filter</code>) 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.</p> <p><b>Note</b> Both IPv4 and IPv6 are supported in vDRA endpoint configuration. For IPv6, you can enter either short or long format.</p> <p>The configuration for multi-homing is validated by netstat command on lb01:</p> <pre>netstat -apn   grep 3898</pre>
Application	Refers to 3GPP Application ID of the interface.
Enabled	Check to enable the endpoint.
Peer Realm	Diameter server realm.
Peer Host	<p>Diameter server host.</p> <p>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.</p>

An example configuration is shown below:

**Figure 9: 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	<input checked="" type="checkbox"/>	pcrf2-gx2.cisco.com	gx-pcrf
lab	10.1.1.1	rx-dra1.cisco.com	rx-dra9	TCP		Rx Application	<input checked="" type="checkbox"/>	rx-pcrf.cisco.com	rx-pcrf:4868

Add Remove  

## 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. <b>Note</b> The 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 10: Relay Endpoints - Example Configuration**

*Vm Host Name	*Instance Id	*Ip Address	*Port	*Fqdn	*Enabled
lab	3	10.10.1.1	4868	dra3.rx	<input checked="" type="checkbox"/>

Add Remove  

## 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.

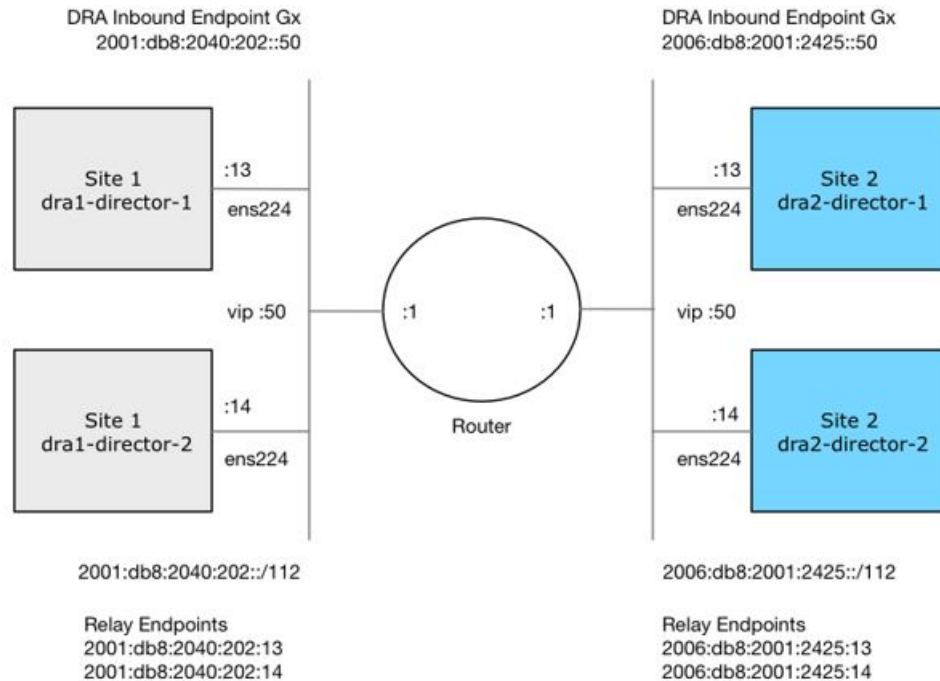
If the control and data plane use the same links, and those links are configured with VIPs, by default, the data plane uses the VIP as its source address for outgoing connections. The data plane uses the VIP as the source address only if the VIP is active on the data plane's outgoing interface.

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 11: 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:

```

#cloud-config
debug: True
output: {all: '| tee -a /var/log/cloud-init-output.log'}

users:
- name: cps
  sudo: ['ALL=(ALL) NOPASSWD:ALL']
  groups: docker
  ssh-authorized-keys:
    - ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDzjJjndIvUiBta4VSIbd2gJm1MWcQ8wtejgAbi
XtoFZdtMdo9G0ZDEOtXHNNDPwWujMiYakZhZWX/zON9raavU8lgD9+YcRopWUtujIC71YjtoxIjWIBBbrtqt
PlUXMUXQsi9lRQbUtslENP+tSatS3awoQupyBMMSutyBady/7Wq0UTwFsnYs5Jfs8jIQuMfVQ9uJ4mNn7wJ0
N+Iaf27rE0t3oiY5DRN6j07WhauM6lCnZ1JDlZqmTnTHQkgJ3uKmQa5x73tJ1OW89Whf+R+dfslVn/yUwK/
vf4extHTn32Dtsxkjz7kQeEDgCe/y7owimaEFcCIfeWEaj/50jegN cps@root-public-key

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\""

```

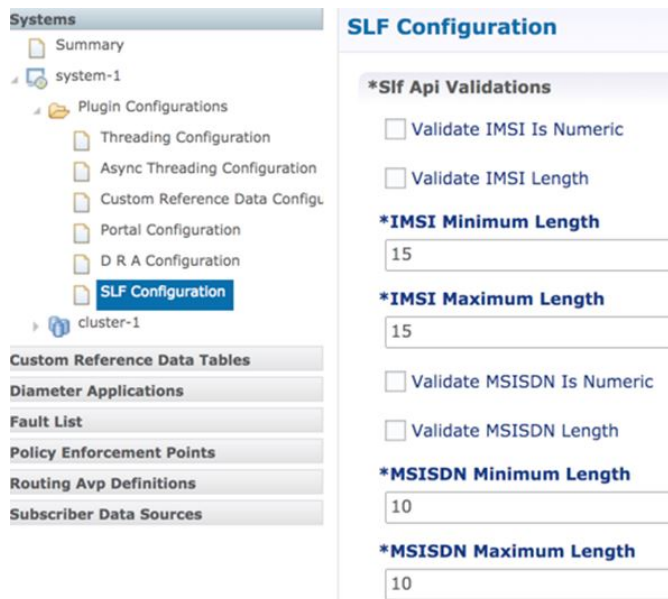
## SLF Configuration

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 12: SLF Configuration**



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

**Table 12: SLF Configuration**

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

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

## 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 13: Diameter Application - Sd Application Example

**Diameter Application**

Name: Sd Application      \*Application Id: 16777303

Vendor Ids: 10415      Add      Remove       Tgpp Application

**Application Route**

Name	*Priority	*Command Code	Cc Request Type	*Destination Host	Action Tables
Sd-TSR	0	8388637	0	<input checked="" type="checkbox"/>	New Sd Session
Sd-CCR-I	0	272	1	<input checked="" type="checkbox"/>	New Sd Session
Sd-CCR-U	0	272	2	<input checked="" type="checkbox"/>	New Sd Session
Sd-CCR-T	0	272	3	<input checked="" type="checkbox"/>	New Sd Session
RAR	0	258	0	<input checked="" type="checkbox"/>	New Sd Session

Add      Remove      ↑      ↓

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.
<b>Application Route table</b>	
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 14: Diameter Application - Gx Application Example**

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.
<b>Application Route table</b>	
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 15: Diameter Application - Rx Application Example**

**Diameter Application**

Name: Rx Application      \*Application Id: 16777236

Vendor Ids: 13019, 8164, 9      Add, Remove       Tgpp Application

Name	*Priority	*Command Code	Cc Request Type	*Destination Host	Action Tables
Rx Initial	1	265	1	<input checked="" type="checkbox"/>	New Rx Session
Rx Termination	1	275	1	<input checked="" type="checkbox"/>	New Rx Session

Add, Remove, Up, Down

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.
<b>Application Route table</b>	
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 16: Diameter Application - Sh Application Example**

**Diameter Application**

**Name**  **\*Application Id**

**Vendor Ids**

10415

Tgpp Application

**Application Route**

Name	*Priority	*Command Code	Cc Request Type	*Destination Hc	Action Tables
UDR	0	306	0	✓	Sh_Application
PUR	0	307	0	✓	Sh_Application
SNR	0	308	0	✓	Sh_Application
PNR	0	309	0	✓	Sh_Application

The following parameters are configured under Sh Application:

Table 16: Sh Application Parameters

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.
<b>Application Route table</b>	
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.

## 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 17: Diameter Application - S6a Application Example

### Diameter Application

**Name**

**\*Application Id**

**Vendor Ids**

10415

Tgpp Application

**Application Route**

Name	*Priority	*Command Code	Request Type	*Destination Host Null	Action Tables
AIR	1	318	0	<input checked="" type="checkbox"/>	S6a_Application
ULR	1	316	0	<input checked="" type="checkbox"/>	S6a_Application

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.
<b>Application Route table</b>	
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 18: Routing AVP Definition - Gx Session**

**Routing Avp Definition**

**Name**

**Routing Avp Lookup**

*Search Table Group
apn_mapping_table
TB_GX_NEW_SESSION

Add Remove ↑ ↓

215584

## Rx Session

An example configuration is shown below:

**Figure 19: Routing AVP Definition - Rx Session**

**Routing Avp Definition**

**Name**

**Routing Avp Lookup**

*Search Table Group
TB_RX_NEW_SESSION
apn_mapping_table

Add Remove ↑ ↓

215583

## Rx New Session Rules - CRD Table

An example configuration is shown below:

Figure 20: Rx New Session Rules - CRD Table

**Custom Reference Data Table** Some or all columns in this table have been published and will be read only. Newly added columns will be editable.

**\*Name:** TB\_RX\_NEW\_SESSION **Display Name:** Rx New Session Rules  Cache Results

**Activation Condition:** Rx    Best Match **\*Evaluation Order:** 0

*Name	Display Name	*Use In Condi	*Type	Key	Required
logical_apn	Logical APN	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
origin_host	Origin Host	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
peer_route	Peer Route	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
destination_host	Destination Host	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Column Details**

**Valid Values**  
The values allowed in Control Center for this column

List of Valid Values

*Name	Display Name
-------	--------------

Valid values pulled from another table's column (Key)

**Validation**  
Validation used by Control Center

**Regular Expression**

**Regular Expression Description**

**Runtime Binding**  
Which rows match when a message is received

None

Bind to Subscriber AVP code

Bind to Session/Policy State Field

**Retrieve Destination Host (Cisco)**

Bind to a result column from another table

Bind to Diameter request AVP code

**Matching Operator**  
eq

215566

## 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 21: Gx New Session Rules - CRD Table

**Custom Reference Data Table** Some or all columns in this table have been published and will be read only. Newly added columns will be editable.

**\*Name:** TB\_GX\_NEW\_SESSION **Display Name:** Gx New Session Rules  Cache Results

**Activation Condition:** Gx    Best Match **\*Evaluation Order:** 1

*Name	Display Name	*Use In Condi	*Type	Key	Required
peer_route	Peer Route	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
origin_realm	Origin Realm	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
destination_realm	Destination Realm	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
origin_host	Origin Host	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
logical_apn	Logical APN	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
imsi	IMSI	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Column Details**

**Valid Values**  
The values allowed in Control Center for this column

List of Valid Values

*Name	Display Name
-------	--------------

Valid values pulled from another table's column (Key)

**Validation**  
Validation used by Control Center

**Regular Expression**

**Regular Expression Description**

**Runtime Binding**  
Which rows match when a message is received

None

Bind to Subscriber AVP code

Bind to Session/Policy State Field

**Retrieve Origin Realm (Cisco DR)**

Bind to a result column from another table

Bind to Diameter request AVP code

**Matching Operator**  
eq

215566

## Sd New Session Rules - CRD Table

An example configuration is shown below:

Figure 22: Sd New Session Rules - CRD Table

**Custom Reference Data Table** Some or all columns in this table have been published and will be read only. Newly added columns will be editable.

**\*Name**    Cache Results

**Activation Condition**     Best Match **\*Evaluation Order**

*Name	Display Name	*Use In Condi	*Type	Key	Required
peer_route	Peer Route	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
origin_realm	Origin Realm	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
destination_realm	Destination Realm	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
destination_host	Destination Host	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
logical_apn	Logical APN	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
msisdn	MSISDN	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Column Details**

**Valid Values**  
The values allowed in Control Center for this column

All

List of Valid Values

*Name	Display Name
-------	--------------

Valid values pulled from another table's column (Key)

**Validation**  
Validation used by Control Center

**Regular Expression**

**Regular Expression Description**

**Runtime Binding**  
Which rows match when a message is received

None

Bind to Subscriber AVP code

Bind to Session/Policy State Field

Bind to a result column from another table

Bind to Diameter request AVP code

**Matching Operator**

215587

## Logical APN List - CRD Table

An example configuration is shown below:

Figure 23: Logical APN List - CRD Table

**Custom Reference Data Table** Some or all columns in this table have been published and will be read only. Newly added columns will be editable.

**\*Name**    Cache Results

**Activation Condition**

*Name	Display Name	*Use In Condi	*Type	Key	Required
logical_apn	Logical APN	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Column Details**

**Valid Values**  
The values allowed in Control Center for this column

All

List of Valid Values

*Name	Display Name
-------	--------------

Valid values pulled from another table's column (Key)

**Validation**  
Validation used by Control Center

**Regular Expression**

**Regular Expression Description**

**Runtime Binding**  
Which rows match when a message is received

None

Bind to Subscriber AVP code

Bind to Session/Policy State Field

Bind to a result column from another table

Bind to Diameter request AVP code

**Matching Operator**

215588

## 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.

**Table 18: Regular-expression Matching and Combinations of AVPs**

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

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

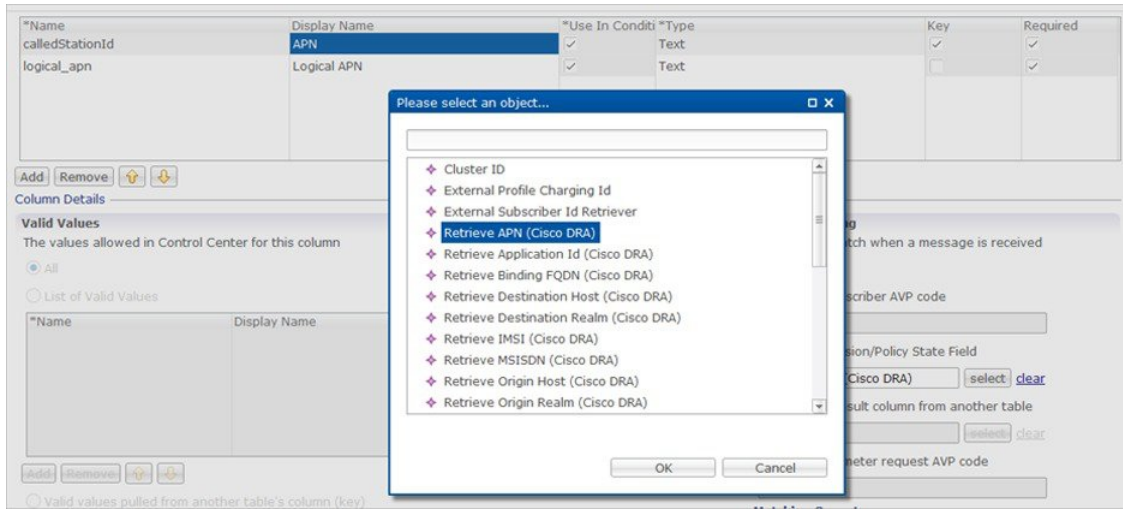
The following sample configuration shows how to retrieve the AVP and bind it to a Key Column in the CRD.

**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 24: Adding AVPs



**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 25: Peer Rate Limit - STG

**Custom Reference Data Table (Read Only)**

\*Name:       Display Name:        Cache Results

Activation Condition:          Best Match      \*Evaluation Order:

\*Columns

*Name	Display Name	*Use In Conditio	*Type	Key	Required
peer_group	Peer Group	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
peer_fqdn	Peer FQDN	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
direction	Message Direction	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
rate_limit_profile	Rate Limit Profile	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>
peer_rate_limit	Peer Rate Limit	<input checked="" type="checkbox"/>	Number	<input type="checkbox"/>	<input type="checkbox"/>
discard_behavior	Discard Behavior	<input checked="" type="checkbox"/>	Number	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Column Details

**Valid Values**  
The values allowed in Control Center for this column

All  
 List of Valid Values

*Name	Display Name

Valid values pulled from another table's column (key)

**Validation**  
Validation used by Control Center

**Regular Expression**

**Regular Expression Description**

**Runtime Binding**  
Which rows match when a message is received

None  
 Bind to Subscriber AVP code

Bind to Session/Policy State Field

Bind to a result column from another table

Bind to Diameter request AVP code

**Matching Operator**

- **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 26: Peer Group Mapping - STG**

**Custom Reference Data Table (Read Only)**

**\*Name**  **Display Name**   Cache Results

Activation Condition     Best Match **\*Evaluation Order**

**\*Columns**

*Name	Display Name	*Use In Condition	*Type	Key
realm_pattern	Realm Pattern	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>
fqdn_pattern	FQDN Pattern	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>
peer_group	Peer Group	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>
weight	Weight	<input checked="" type="checkbox"/>	Number	<input type="checkbox"/>

**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				
<input checked="" type="radio"/> All <input type="radio"/> List of Valid Values		<b>Regular Expression</b> <input type="text"/>	<input checked="" type="radio"/> None <input type="radio"/> Bind to Subscriber AVP code <input type="radio"/> Bind to Session/Policy State File				
<table border="1"> <thead> <tr> <th>*Name</th> <th>Display Name</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>		*Name	Display Name	<input type="text"/>	<input type="text"/>	<b>Regular Expression Description</b> <input type="text"/>	<input type="text"/>
*Name	Display Name						
<input type="text"/>	<input type="text"/>						

For more information, see [Peer Group Mapping](#).

## Message Retry Profile

Message retry profile has been added.



Figure 27: Message Retry Profile - STG

**Custom Reference Data Table** Some or all columns in this table have been published and will be read only. Newly added columns will be editable.

**\*Name**  **Display Name**   Cache Results

**Activation Condition**     Best Match **\*Evaluation Order**

**\*Columns**

*Name	Display Name	*Use In Condi	*Type	Key	Required
peer_group	Peer Group	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
app_id	Application Id	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
cmd_code	Command Code	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
rc_in_resp	Result Code	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
exp_rc	Experimental RC	<input checked="" type="checkbox"/>	True/False	<input type="checkbox"/>	<input type="checkbox"/>
num_retries	Number Of Retries	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>

**Column Details**

**Valid Values**

The values allowed in Control Center for this column

All

List of Valid Values

*Name	Display Name
-------	--------------

Valid values pulled from another table's column (key)

**Validation**

Validation used by Control Center

**Regular Expression**

**Regular Expression Description**

**Runtime Binding**

Which rows match when a message is received

None

Bind to Subscriber AVP code

Bind to Session/Policy State Field

Bind to a result column from another table

Bind to Diameter request AVP code

**Matching Operator**

- 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 28: Message Mediation Profile - STG**

**Custom Reference Data Table (Read Only)**

\*Name: message\_mediation\_profile    Display Name: Message Mediation Profile     Cache Results

Activation Condition:        Best Match    \*Evaluation Order: 0

*Name	Display Name	*Use In Conditio	*Type	Key	Required
app_id	Application Id	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
cmd_code	Command Code	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
msg_type	Message Type	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
avp_code	Avp Code	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
vendor_id	Avp Vendor Id	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
avp_action	Avp Action	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>

**Column Details**

**Valid Values**  
The values allowed in Control Center for this column

All  
 List of Valid Values

*Name	Display Name
-------	--------------

Valid values pulled from another table's column (key)

**Validation**  
Validation used by Control Center

**Regular Expression**

**Regular Expression Description**

**Runtime Binding**  
Which rows match when a message is received

None  
 Bind to Subscriber AVP code  
 Bind to Session/Policy State Field  
 Bind to a result column from another table  
 Bind to Diameter request AVP code

**Matching Operator**

- 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 29: Peer Group Answer Timeout - STG**

**Custom Reference Data Table (Read Only)**

\*Name: peer\_group\_answer\_timeout      Display Name: Peer Group Answer Timeout       Cache Results

Activation Condition:                    Best Match      \*Evaluation Order: 0

*Name	Display Name	*Use In Condition	*Type
peer_group	Peer Group	<input checked="" type="checkbox"/>	Text
app_id	Application Id	<input checked="" type="checkbox"/>	Text
cmd_code	Command Code	<input checked="" type="checkbox"/>	Text
answer_timeout	Timeout Milliseconds	<input checked="" type="checkbox"/>	Text

Column Details

**Valid Values**  
The values allowed in Control Center for this column

All  
 List of Valid Values

*Name	Display Name

**Validation**  
Validation used by Control Center

**Regular Expression**

**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 30: Error Result Code Profile - STG

**Custom Reference Data Table (Read Only)**

\*Name:       Display Name:        Cache Results

Activation Condition:          Best Match      \*Evaluation Order:

\*Columns

*Name	Display Name	*Use In Conditio	*Type	Key	Required
app_id	Application Id	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
internal_err	Error	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
rc_in_resp	Result Code	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>
exp_rc_in_resp	Exp Result Code	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>
exp_vendor_id	Vendor Id	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>
err_msg	Err Msg	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>

Column Details

**Valid Values**  
The values allowed in Control Center for this column

All  
 List of Valid Values

*Name	Display Name

Valid values pulled from another table's column (key)

**Validation**  
Validation used by Control Center

**Regular Expression**

**Regular Expression Description**

**Runtime Binding**  
Which rows match when a message is received

None  
 Bind to Subscriber AVP code  
    
 Bind to Session/Policy State Field  
    
 Bind to a result column from another table  
    
 Bind to Diameter request AVP code

**Matching Operator**

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 31: Gx Session Routing

**Custom Reference Data Table** Some or all columns in this table have been published and will be read only. Newly added columns will be editable.

**\*Name**  **Display Name**   Cache Results

**Activation Condition**     Best Match **\*Evaluation Order**

**\*Columns**

*Name	Display Name	*Use In Conditio	*Type	Key	Required
logical_apn	Logical APN	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
origin_host	Origin Host	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
peer_route	Peer Route	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>
origin_realm	Origin Realm	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
destination_host	Destination Host	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
destination_realm	Destination Realm	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Column Details**

**Valid Values**  
The values allowed in Control Center for this column

All  
 List of Valid Values

*Name	Display Name

**Validation**  
Validation used by Control Center

**Regular Expression**

**Regular Expression Description**

**Runtime Binding**  
Which rows match when a message is received

None  
 Bind to Subscriber AVP code  
 Bind to Session/Policy State Field  
    
 Bind to a result column from another table  
    
 Bind to Diameter request AVP code

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 32: SLF Trigger Profile - STG

**Custom Reference Data Table (Read Only)**

\*Name:       Display Name:        Cache Results

Activation Condition:          Best Match      \*Evaluation Order:

*Name	Display Name	*Use In Conditio	*Type	Key	Required
application_id	Application ID	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
cmd_code	Command Code	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
dest_realm	Destination Realm	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
slf_lookup_type	SLF Lookup Type	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input checked="" type="checkbox"/>
slf_destination_type	SLF Destination Type	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Column Details

**Valid Values**  
The values allowed in Control Center for this column

All  
 List of Valid Values

*Name	Display Name
-------	--------------

Valid values pulled from another table's column (key)

**Validation**  
Validation used by Control Center

**Regular Expression**

**Regular Expression Description**

**Runtime Binding**  
Which rows match when a message is received

None  
 Bind to Subscriber AVP code  
    
 Bind to Session/Policy State Field  
    
 Bind to a result column from another table  
    
 Bind to Diameter request AVP code

**Matching Operator**

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 33: SLF Routing - STG

**Custom Reference Data Table (Read Only)**

\*Name:       Display Name:        Cache Results

Activation Condition:          Best Match      \*Evaluation Order:

*Name	Display Name	*Use In Conditio	*Type	Key	Required
slf_destination	SLF Destination	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
slf_session_route_key	SLF Session Route Key	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Column Details

**Valid Values**  
The values allowed in Control Center for this column

All  
 List of Valid Values

*Name	Display Name
-------	--------------

Valid values pulled from another table's column (key)

**Validation**  
Validation used by Control Center

**Regular Expression**

**Regular Expression Description**

**Runtime Binding**  
Which rows match when a message is received

None  
 Bind to Subscriber AVP code  
    
 Bind to Session/Policy State Field  
    
 Bind to a result column from another table  
    
 Bind to Diameter request AVP code

**Matching Operator**

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 34: S6 Table Driven Rules - STG**

**Custom Reference Data Table** Some or all columns in this table have been published and will be read only. Newly added columns will be editable.

\*Name: TB\_S6      Display Name: S6\_TB\_Rules       Cache Results

Activation Condition: [ ]       Best Match      \*Evaluation Order: 0

*Name	Display Name	*Use In Condi	*Type	Key	Required
origin_host	Origin Host	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
origin_realm	Origin Realm	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
destination_host	Destination Host	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
destination_realm	Destination Realm	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
imsi	IMSI	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
peer_route	Peer Route	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>

Column Details

**Valid Values**  
The values allowed in Control Center for this column  
 All  
 List of Valid Values  

*Name	Display Name
-------	--------------

 Valid values pulled from another table's column (key)

**Validation**  
Validation used by Control Center  
**Regular Expression**  
  
**Regular Expression Description**

**Runtime Binding**  
Which rows match when a message is received  
 None  
 Bind to Subscriber AVP code  
 Bind to Session/Policy State Field  
 Bind to a result column from another table  
 Bind to Diameter request AVP code

**Matching Operator**

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 35: APN Mapping - CRD Table

**Custom Reference Data Table** Some or all columns in this table have been published and will be read only. Newly added columns will be editable.

**\*Name**  **Display Name**   Cache Results

**Activation Condition**     Best Match **\*Evaluation Order**

**\*Columns**

*Name	Display Name	*Use In Conditio	*Type	Key	Required
called_station_id	Called Station Id	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
logical_apn	Logical APN	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>

**Column Details**

**Valid Values**  
The values allowed in Control Center for this column

All  
 List of Valid Values

*Name	Display Name

**Validation**  
Validation used by Control Center

**Regular Expression**

**Regular Expression Description**

**Runtime Binding**  
Which rows match when a message is received

None

Bind to Subscriber AVP code

Bind to Session/Policy State Field

Bind to a result column from another table

Bind to Diameter request 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 36: Peer Access Control List

**Custom Reference Data Table (Read Only)**

**\*Name** peer\_access\_control\_list **Display Name** Peer Access Control List  Cache Results

Activation Condition     Best Match **\*Evaluation Order** 0

*Name	Display Name	*Use In Conditio	*Type	Key	Required
origin_host	Origin Host	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
origin_realm	Origin Realm	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
auth_action	Authorization Action	<input checked="" type="checkbox"/>	Number	<input type="checkbox"/>	<input checked="" type="checkbox"/>
error_code	Authorization Action Deny - Result Code	<input checked="" type="checkbox"/>	Number	<input type="checkbox"/>	<input type="checkbox"/>
error_msg	Authorization Action Deny - Error Message	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>
application_id	Application Id	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input checked="" type="checkbox"/>

**Column Details**

**Valid Values**  
The values allowed in Control Center for this column

All  
 List of Valid Values

*Name	Display Name

**Validation**  
Validation used by Control Center

**Regular Expression**

**Regular Expression Description**

**Runtime Binding**  
Which rows match when a message is received

None  
 Bind to Subscriber AVP code  
 Bind to Session/Policy State Field

## Peer Routes

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

Figure 37: Peer Routes - CRD Table

**\*Name** peer\_route **Display Name** Peer Routes  Cache Results Activation Condition

*Name	Display Name	*Use In Conditio	*Type	Key	Required
peer_route	Peer Route	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Column Details**

**Valid Values**  
The values allowed in Control Center for this column

All  
 List of Valid Values

*Name	Display Name

**Validation**  
Validation used by Control Center

**Regular Expression**

**Regular Expression Description**

**Runtime Binding**  
Which rows match when a message is received

None  
 Bind to Subscriber AVP code  
 Bind to Session/Policy State Field

215568

## 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 38: Peer Group - CRD Table

**Custom Reference Data Table (Read Only)**

\*Name: peer\_group\_srk\_mapping    Display Name: Peer Group SRK Mapping    Cache Results:     Activation Condition:

\*Columns

*Name	Display Name	*Use In Conditio	*Type	Key	Required
peer_group	Peer Group	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
session_routing_key	Session Routing Key	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>
dest_host_routing_rule	Destination Host Routing Rule	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input checked="" type="checkbox"/>
dest_host_replace_rule	Destination Host Replace	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>
dest_realm_replace_rule	Destination Realm Replace	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>

Column Details

**Valid Values**  
The values allowed in Control Center for this column

All  
 List of Valid Values

*Name	Display Name

Valid values pulled from another table's column (key)

▼ Actions

Copy:

**Validation**  
Validation used by Control Center

**Regular Expression**

**Regular Expression Description**

**Runtime Binding**  
Which rows match when a message is received

None  
 Bind to Subscriber AVP code  
 Bind to Session/Policy State Field  
 Bind to a result column from another table  
 Bind to Diameter request AVP code

**Matching Operator**

- 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 39: Peer Routing - CRD Table

**Custom Reference Data Table (Read Only)**

\*Name: peer\_routing    Display Name: Peer Routing    Cache Results:     Activation Condition:

\*Columns

*Name	Display Name	*Use In Conditio	*Type	Key	Required
peer_route	Peer Route	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
system_id	System Id	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
peer_group	Peer Group	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input checked="" type="checkbox"/>
precedence	Precedence	<input checked="" type="checkbox"/>	Number	<input type="checkbox"/>	<input checked="" type="checkbox"/>
weight	Weight	<input checked="" type="checkbox"/>	Number	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Column Details

**Valid Values**  
The values allowed in Control Center for this column

All  
 List of Valid Values

*Name	Display Name

Valid values pulled from another table's column (key)

▼ Actions

Copy:

**Validation**  
Validation used by Control Center

**Regular Expression**

**Regular Expression Description**

**Runtime Binding**  
Which rows match when a message is received

None  
 Bind to Subscriber AVP code  
 Bind to Session/Policy State Field

- Peer Route: Identifier of this Peer Route.

215570

- 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.

## PCRF Session Query Peers

Use this CRD to configure the REST API parameters for Rx AAR fallback routing.

Policy DRA supports a fallback routing for Rx AARs for VoLTE using the PCRF session query.

For an Rx AAR with an IPv6 binding query, vDRA provides the ability to route the Rx AAR based on an API query to the PCRF to determine if it has a session for the IPv6. The queries can be made in parallel to a configured set of query points on PCRFs.



**Note** Ensure you have enabled PCRF Session Query in the DRA plugin configuration to use this feature.

**Figure 40: PCRF Session Query Peers CRD**

**Custom Reference Data Table** Some or all columns in this table have been published and will be read only. Newly added columns

\*Name: pcrf\_session\_query\_peers    Display Name: pcrf\_session\_query\_peers     Cache Results    Activation Condition: [select] [clear]

Svn Crd Data

*Name	Display Name	*Use In Condi*	*Type	Key
base_url	BASE_URL	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>
pcrf_group	PCRF GROUP	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>
session_query_parameter	SESSION QUERY PARAMETER	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>
user_id	USER ID	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>
password	PASSWORD	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>
timeout_ms	TIMEOUT_MS	<input checked="" type="checkbox"/>	Number	<input type="checkbox"/>

Add Remove [up] [down]

**Column Details**

Valid Values	Validation	Runtime Binding
The values allowed in Control Center for this column <input type="radio"/> All <input checked="" type="radio"/> List of Valid Values	Validation used by Control Center <b>Regular Expression</b> [text field] <b>Regular Expression Description</b> [text field]	Which rows match when a <input checked="" type="radio"/> None <input type="radio"/> Bind to Subscriber APP <input type="radio"/> Bind to Session/Policy S
*Name: framedIpv6PrefixKey    Display Name: framedIpv6PrefixKey		

This CRD contains the following fields:

- `base_url`: The HTTP URL for the PCRF REST API, supports both HTTP and HTTPS. This does not contain the Rest API endpoint name.
- `pcrf_group`: The PCRFs can be configured in logical groups by defining the common `pcrf_group`. vDRA triggers the REST API request one after another for multiple PCRFs configured with same group name. This is to support PCRF with primary and secondary API endpoints. (Optional)
- `session_query_parameter`: PCRF session query parameter. Currently, only one value is supported: `framedIpv6PrefixKey`
- `user_id`: User ID for REST API request if PCRF requires any basic authentication. (Optional)
- `password`: Password for REST API request if PCRF requires any basic authentication. (Optional)

- `timeout_ms`: REST API request timeout value. Default: 250ms. (Optional)

You can also configure a session route key for the PCRF response. When vDRA makes REST API requests to multiple PCRFs for session query using the Framed-IPv6-Prefix received in the Rx AAR message, the PCRF that has the corresponding Gx session sends a session route key in the response. vDRA then uses this key to look up the peer group and route the Rx AAR message to the correct PCRF. To configure a session route key in the response, see the Unified API Plugin Configuration in *CPS Mobile Configuration Guide*.

Additionally, diameter load balancing ensures that when a PCRF is connected to two directors and the PCEF traffic passes on one director, the traffic is then equally distributed to both directors.

vDRA can also load balance session query REST requests across multiple PCRF API endpoints. Previously, all REST queries were sent to the primary endpoint and only if the primary query fails, then the request is sent to secondary. Now, the requests are load balanced across the different PCRF endpoints within a peer group. If the session query results indicate that the PCRF does not have the corresponding Gx session for the IPv6 prefix, then vDRA does not send the query to the other PCRF configured in the same group. Similarly, for all other failures, vDRA sends the session query request to a different PCRF REST API in the same group. It is recommended that a group may contain a maximum of four PCRF REST API endpoints. If there is no group name, the PCRF API endpoint is considered as a standalone PCRF.

## IPv6 Ranges System ID Mapping

Use this CRD to specify a range of IPv6 addresses and the relay vDRA system ID.

This CRD is used to relay Rx AAR messages to other vDRA clusters based on the IPv6 range defined in the CRD.

When an Rx-AAR reaches vDRA, the AAR is checked for an IPv6 prefix. If there is an IPv6 prefix, then this CRD is checked for IPv6 ranges and to find the related primary and secondary vDRA system ID.

If the primary or secondary system is the current vDRA system-ID, then AAR message is processed locally. If the primary/secondary system ID is not the current vDRA, then current vDRA checks the relay links between current system and primary system. If the relay link is up, the the AAR is relayed to the primary system; else vDRA checks link to the secondary system.

**Figure 41: IPv6 Ranges System ID Mapping CRD**

**Custom Reference Data Table** Some or all columns in this table have been published and will be read only. Newly added columns will be editable.

**\*Name** `ipv6_range_sys_id_map` **Display Name** IPv6 Ranges System ID Mapping  Cache Results **Activation Condition**

Svn Crd Data

**\*Columns**

*Name	Display Name	*Use In Conditic	*Type	Key	Required
ipv6_start_range	IPv6 Start Range	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ipv6_end_range	IPv6 End Range	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
primary_system_id	Primary System Id	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input checked="" type="checkbox"/>
secondary_system_id	Secondary System ID	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>

**Table 19: IPv6 Ranges System ID Mapping Fields**

Fields	Description
IPv6 Start Range	Starting IP of IPv6 range in long format.
IPv6 End Range	Ending IP of IPv6 range in long format.

Fields	Description
Primary system ID	Mandatory field. Indicates the System ID of vDRA in a vDRA cluster to which the request can be relayed.
Secondary system ID	Secondary vDRA to which the request can be relayed if the primary is not present.



**Note** The ranges are expected to be mutually exclusive and unique. Verify the values when provisioning the same.

## Binding Key Profile

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

**Figure 42: Binding Key Profile - CRD Table**

**Custom Reference Data Table (Read Only)**

\*Name: binding\_key\_profile    Display Name: Binding Key Profile     Cache Results    Activation Condition:

*Name	Display Name	*Use In Conditio	*Type	Key	Required
profile_name	Profile Name	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
imsi_apn	IMSI APN Key Enabled	<input checked="" type="checkbox"/>	True/False	<input type="checkbox"/>	<input type="checkbox"/>
msisdn_apn	MSISDN APN Key Enabled	<input checked="" type="checkbox"/>	True/False	<input type="checkbox"/>	<input type="checkbox"/>
framed_ipv6_prefix	Framed IPv6 Enabled	<input checked="" type="checkbox"/>	True/False	<input type="checkbox"/>	<input type="checkbox"/>
framed_ipv4	Framed IPv4 Enabled	<input checked="" type="checkbox"/>	True/False	<input type="checkbox"/>	<input type="checkbox"/>

**Column Details**

**Valid Values**  
The values allowed in Control Center for this column

All  
 List of Valid Values

*Name	Display Name

Valid values pulled from another table's column (key)

**Validation**  
Validation used by Control Center

**Regular Expression**

**Regular Expression Description**

**Runtime Binding**  
Which rows match when a message is received

None  
 Bind to Subscriber AVP code  
 Bind to Session/Policy State Field  
 Bind to a result column from another table  
 Bind to Diameter request AVP code

**Matching Operator**

**Actions**  
Copy:

- 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.

## AppId 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 43: AppId Key Profile Mapping- CRD Table**

**Custom Reference Data Table (Read Only)**

**\*Name**  **Display Name**   Cache Results **Activation Condition**

**\*Columns**

*Name	Display Name	*Use In Conditio	*Type	Key	Required
application_id	Application Id	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
profile_name	Profile Name	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>

**Column Details**

**Valid Values**  
The values allowed in Control Center for this column

All  
 List of Valid Values

*Name	Display Name

Valid values pulled from another table's column (key)

**Actions**  
Copy:

**Validation**  
Validation used by Control Center

**Regular Expression**

**Regular Expression Description**

**Runtime Binding**  
Which rows match when a message is received

None  
 Bind to Subscriber AVP code  
 Bind to Session/Policy State Field  
    
 Bind to a result column from another table  
    
 Bind to Diameter request AVP code

**Matching Operator**

## Message Rate Limit Profile

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

Figure 44: Message Rate Limit Profile - CRD Table

**Custom Reference Data Table (Read Only)**

\*Name:     Display Name:      Cache Results    Activation Condition:

**\*Columns**

*Name	Display Name	*Use In Conditio	*Type	Key	Required
profile_name	Rate Limit Profile Name	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
app_id	Application Identifier	<input checked="" type="checkbox"/>	Number	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
command_code	Command Code	<input checked="" type="checkbox"/>	Number	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
mesg_type	Message/Request Type	<input checked="" type="checkbox"/>	Number	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
rate_limit	Message Rate Limit	<input checked="" type="checkbox"/>	Number	<input type="checkbox"/>	<input checked="" type="checkbox"/>

**Column Details**

**Valid Values**  
The values allowed in Control Center for this column

All  
 List of Valid Values

*Name	Display Name
-------	--------------

Valid values pulled from another table's column (key)

**Validation**  
Validation used by Control Center

**Regular Expression**

**Regular Expression Description**

**Runtime Binding**  
Which rows match when a message is received

None  
 Bind to Subscriber AVP code  
 Bind to Session/Policy State Field  
 Bind to a result column from another table  
 Bind to Diameter request AVP code

- 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 45: Reserved IMSI**

*Name	Display Name	*Use In Condit*	*Type
mcc_start	MCC Start	<input checked="" type="checkbox"/>	Number
mcc_end	MCC End	<input checked="" type="checkbox"/>	Number

## 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 46: Trusted Realm Profile**

*Name	Display Name	*Use In Condit*	*Type	Key	Required
profile_name	Trusted Profile Name	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
trusted_realm	Trusted Realm	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

## 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 47: Protected Realm Trusted Profile Mapping

*Name	Display Name	*Use In Condit*	*Type	Key	Required
protected_realm	Protected Realm	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
profile_name	Trusted Profile Name	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input checked="" type="checkbox"/>

## 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 48: MME Alias Map

*Name	Display Name	*Use In Condit*	*Type	Key	Required
mme_host	MME FQDN	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input checked="" type="checkbox"/>
alias1	Alias 1	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input checked="" type="checkbox"/>
alias2	Alias 2	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>
alias3	Alias 3	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>

## 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 49: HSS Aliases

**Custom Reference Data Table (Read Only)**

\*Name:     Display Name:      Cache Results    Activation Condition:

Show Crd Data

*Name	Display Name	*Use In Condit	*Type	Key	Required
hss_alias	HSS Alias FQDN	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
is_shared_alias	Shared Alias	<input checked="" type="checkbox"/>	True/False	<input type="checkbox"/>	<input checked="" type="checkbox"/>

## 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 50: HSS Alias Map

**Custom Reference Data Table (Read Only)**

\*Name:     Display Name:      Cache Results    Activation Condition:

Show Crd Data

*Name	Display Name	*Use In Condit	*Type	Key	Required
hss_host	HSS FQDN	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
alias1	Alias1	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input checked="" type="checkbox"/>
alias2	Alias2	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>
alias3	Alias3	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input type="checkbox"/>

## 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 51: Binding Key Profile Creation Map - CRD Table

**Custom Reference Data Table (Read Only)**

**\*Name**  
bind\_key\_profile\_creation\_map

**Display Name**  
Binding Key Profile Creation Map

Cache Results

Activation Condition  
  clear  Svn Crd Data  Best Match

**\*Evaluation Order**  
0

**\*Columns**

*Name	Display Name	*Use In Conditio	*Type	Key	Required
appl_id	Application Identifier	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
called_station_id	Called Station Id	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
profile_name	Binding Key Profile	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input checked="" type="checkbox"/>

- 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 52: Binding Key Profile Read Map - CRD Table

**Custom Reference Data Table (Read Only)**

**\*Name**  
bind\_key\_profile\_read\_map

**Display Name**  
Binding Key Profile Read Map

Cache Results

Activation Condition  
  clear  Svn Crd Data  Best Match

**\*Evaluation Order**  
0

**\*Columns**

*Name	Display Name	*Use In Conditio	*Type	Key	Required
appl_id	Application Identifier	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
origin_host	Origin Host	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
origin_realm	Origin Realm	<input checked="" type="checkbox"/>	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
binding_profile	Binding Key Profile	<input checked="" type="checkbox"/>	Text	<input type="checkbox"/>	<input checked="" type="checkbox"/>

- 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.

