



User Configuration

- [Basic Configuration, on page 1](#)
- [Routing Techniques, on page 6](#)
- [Advanced Features, on page 11](#)

Basic Configuration

Before you begin using CPS vDRA, perform the following basic configurations in CPS DRA:

- Configure Systems
- Configure Diameter Application
- Configure Routing AVP Definitions

Configure Systems

In CPS DRA, navigate to the **System and Plugin Configuration**.

Configure the stack in **DRA Configuration** plugin.

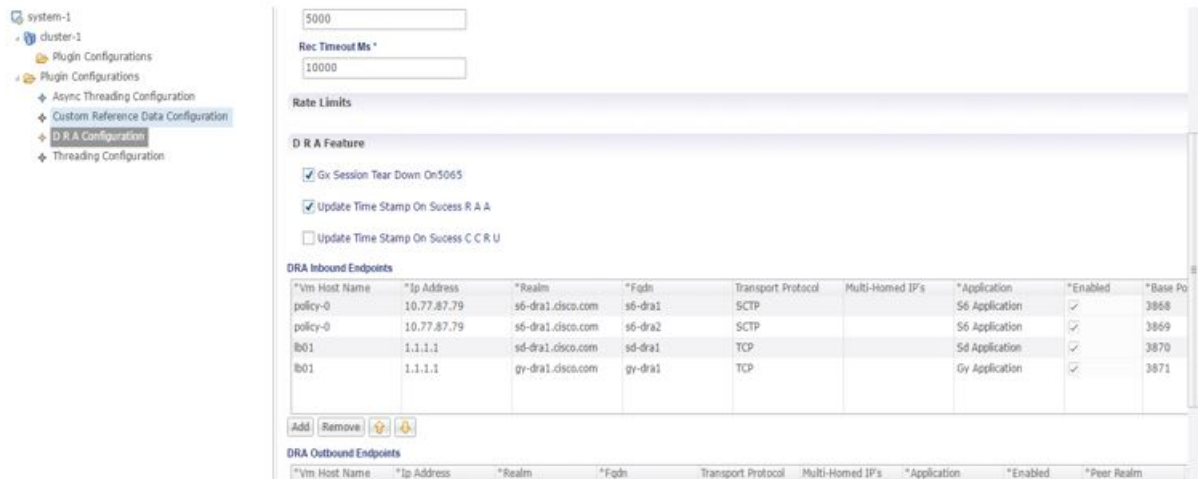
Configure the **DRA Inbound Endpoints** for incoming peer connections and **DRA Outbound Endpoints** for outgoing peer connection.

You can choose the Transport Protocol as TCP and SCTP depending on your requirement.

You can also specify the IPv4 or IPv6 address configuration for the stack connection.

The following image shows a sample configuration.

Figure 1: Sample Systems Configuration

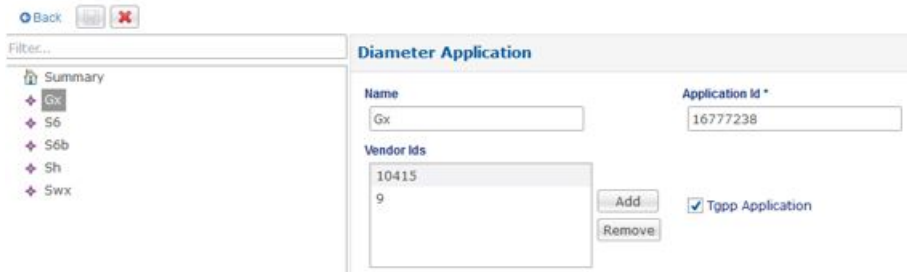


For more information, see [DRA Configuration](#).

Configure Diameter Application

Configure the Diameter applications that are required to be connected over various interfaces with CPS vDRA. The following image is a sample of a Gx application configuration:

Figure 2: Sample Diameter Application Configuration



For more information, see [Diameter Application](#).

Configure Multiple Diameter Applications for a Peer Connection

Previously, vDRA supported a single application on a peer connection. In this release, vDRA supports multiple applications on a peer connection.

To configure multiple applications for a peer connection, go to vDRA Inbound Endpoints in DRA Plugin configuration. In the Applications field, select the button as shown:

Figure 3: DRA Inbound Endpoints

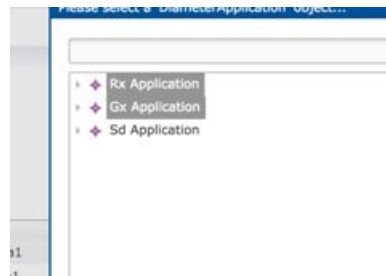
DRA Inbound Endpoints

| *Vm Host Name | *Ip Address | *Realm | *Fqdn | Transport Protocol | Multi-Homed IP's | *Application | Enabled |
|-----------------|----------------|-------------------|---------|--------------------|------------------|----------------|-------------------------------------|
| AMUKEWAR-M-P01E | 10.142.148.142 | gx-dra1.cisco.com | gx-dra1 | TCP | | | <input checked="" type="checkbox"/> |
| AMUKEWAR-M-P01E | 10.142.148.142 | rx-dra1.cisco.com | rx-dra1 | TCP | | Rx Application | <input checked="" type="checkbox"/> |
| AMUKEWAR-M-P01E | 10.142.148.142 | gx-dra2.cisco.com | gx-dra2 | TCP | | Gx Application | <input checked="" type="checkbox"/> |
| AMUKEWAR-M-P01E | 10.142.148.142 | sd-dra1.cisco.com | sd-dra1 | TCP | | Sd Application | <input checked="" type="checkbox"/> |
| AMUKEWAR-M-P01E | 10.142.148.142 | gx-dra3.cisco.com | gx-dra3 | TCP | | Gx Application | <input checked="" type="checkbox"/> |
| AMUKEWAR-M-P01E | 10.142.148.142 | rx-dra2.cisco.com | rx-dra2 | TCP | | Rx Application | <input checked="" type="checkbox"/> |

Add Remove [Icons]

Select all the applications you require.

Figure 4: Application Selection



The following example shows multiple Diameter applications for a peer connection:

Figure 5: Multiple Applications

DRA Inbound Endpoints

| *Vm Host Name | *Ip Address | *Realm | *Fqdn | Transport Protocol | Multi-Homed IP's | *Application | Enabled |
|-----------------|----------------|-------------------|---------|--------------------|------------------|--------------------------------|-------------------------------------|
| AMUKEWAR-M-P01E | 10.142.148.142 | gx-dra1.cisco.com | gx-dra1 | TCP | | Rx Application, Gx Application | <input checked="" type="checkbox"/> |
| AMUKEWAR-M-P01E | 10.142.148.142 | rx-dra1.cisco.com | rx-dra1 | TCP | | Rx Application | <input checked="" type="checkbox"/> |
| AMUKEWAR-M-P01E | 10.142.148.142 | gx-dra2.cisco.com | gx-dra2 | TCP | | Gx Application | <input checked="" type="checkbox"/> |
| AMUKEWAR-M-P01E | 10.142.148.142 | sd-dra1.cisco.com | sd-dra1 | TCP | | Sd Application | <input checked="" type="checkbox"/> |
| AMUKEWAR-M-P01E | 10.142.148.142 | gx-dra3.cisco.com | gx-dra3 | TCP | | Gx Application | <input checked="" type="checkbox"/> |

Configure Routing AVP Definitions

Configure the Routing AVP definitions to route calls on the basis of the AVPs that are present in diameter message.

In the **Routing AVP Definition** page, you specify the Application name and the table for table-driven routing.

In the **Diameter Application** page, configure the Application Route for table-driven routing.

The following screenshots show a sample configuration:

Figure 6: Routing Avp Definition

Routing Avp Definition

Name

Routing Avp Lookup

```
*Search Table Group
apn_mapping_table
TB_GX_NEW_SESSION_1
```

Actions

Figure 7: Diameter Application

Diameter Application

Name ***Application Id**

Vendor Ids

10415
 8164
 9

Type Application

Application Route

| Name | *Priority | *Command Code | Request Type | *Destination Hk | Action Tables |
|--------------|-----------|---------------|--------------|-------------------------------------|----------------|
| Gx Initial | 1 | 272 | 1 | <input checked="" type="checkbox"/> | Gx_Application |
| Gx Terminate | 1 | 272 | 3 | <input checked="" type="checkbox"/> | Gx_Application |
| Gx Update | 1 | 272 | 2 | <input checked="" type="checkbox"/> | Gx_Application |
| RAR | 1 | 258 | 0 | <input checked="" type="checkbox"/> | Gx_Application |

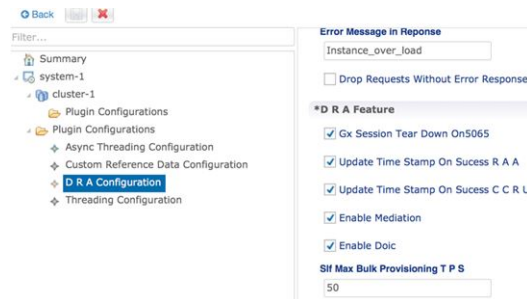
Enable Mediation

By default, mediation feature is disabled.

To enable the mediation, log in to Policy builder, select the “Enable Mediation” checkbox in **Systems > DRA Configuration > DRA Feature**.

Finally, publish the configuration changes.

Figure 8: Enable Mediation



Enable DOIC

By default, DOIC feature is disabled.

To enable the DOIC, log in to Policy Builder, select the “Enable DOIC” checkbox in **Systems > DRA Configuration > DRA Feature**.

You must also enable DOIC for the group in Peer Group SRK Mapping table as described in [Peer Group SRK Mapping](#).

Configure throttling using DOIC. For more information, see [Configure Throttling of Diameter Messages Using DOIC, on page 22](#).

Publish the configuration changes.

Configure Interfaces for SCTP Multi-homing

As a pre-requisite for SCTP multi-homing, you must first move the physical interfaces of Director VM inside the diameter-endpoint container.

To move the IPv4 interfaces, perform the following commands in vDRA Master CLI mode:

```
config diameter host dra-director-0-dra-director-52wumnq512y1
  interface ens3 ipv4 address 10.77.87.79 broadcast 10.77.87.255 prefix-length 24
diameter host dra-director-0-dra-director-52wumnq512y1 interface ens3
route default gateway 10.77.87.1
diameter host dra-director-0-dra-director-52wumnq512y1 interface ens5
  ipv4 address 10.225.115.199 broadcast 10.225.115.255 prefix-length 24
diameter host dra-director-0-dra-director-52wumnq512y1 interface ens5
  route default gateway 10.225.115.1
```

To move the IPv6 interfaces, perform the following commands in vDRA Master CLI mode:

```
config diameter host dra-director-0-dra-director-52wumnq512y1
  interface ens6 ipv6 address 2003:3051::114 prefix-length 64
diameter host dra-director-0-dra-director-52wumnq512y1 interface
ens6 route default gateway 2003:3051::1
diameter host dra-director-0-dra-director-52wumnq512y1 interface
ens7 ipv6 address 2003:3052::114 prefix-length 64
diameter host dra-director-0-dra-director-52wumnq512y1 interface
ens7 route default gateway 2003:3052::1
```

Commit the configuration.

Routing Techniques

You can define the routing of calls based on destination host, SRK, or a table.

Configure Destination Host Routing

Destination host based routing is the basic and default routing technique used by CPS vDRA.

When the incoming diameter request contains the destination-host AVP that has the direct connection with the CPS vDRA, vDRA routes the message directly to that connected host.

Before you begin

Stack must be up and running.

For more information, see [Basic Configuration, on page 1](#).

After configuring the stacks, Diameter endpoints are ready to initiate/accept Diameter connections for the defined IP address, Port, and Application-ID.

Policy DRA





For Policy DRA, you must configure the binding keys for Gx sessions.





Binding helps Policy DRA route the related Gx/Rx sessions to the same PCRF or destined PCRF.

A binding database is needed to map search keys to PCRF binding information. Each binding has a search key and binding data associated with it. The supported search keys are:

- IMSI + APN
- IPv6
- IPv4
- MSISDN + APN

Figure 9: Policy DRA Sample Configuration

| binding_key_profile | | | | | |
|----------------------|----------------------|------------------------|---------------------|---------------------|---|
| | | | | | Filter CRD Tables |
| Profile Name * (key) | IMSI APN Key Enabled | MSISDN APN Key Enabled | Framed IPv6 Enabled | Framed IPv4 Enabled | Actions |
| DefaultProfile | true | false | false | false |   |
| Rx_Profile | false | false | true | false |   |

| app_id_key_profile_mapping | | |
|----------------------------|----------------|---|
| | | Filter CRD Tables |
| Application Id * (key) | Profile Name | Actions |
| 16777238 | DefaultProfile |   |
| 16777216 | Qv_Profile |   |

If the Binding Key Profile and mapping to Application ID is not configured properly, the following errors may occur:

- Gx Calls – Session binding failure in database resulting in call failures.
- Rx Calls – Binding Retrieval failure resulting in call failures.



Note IMS DRA does not require bindings. Hence, Binding Key Profile is only valid for Policy DRA.

Configure SRK Based Routing

You can configure SRK based routing in one of the following ways:

Configure Secondary Peer Fallback



Note This configuration is valid for both Policy and IMS DRA.

In SRK based routing, you can configure routing to a set of peers. This can be used for alternate routing (secondary and tertiary routes) when the Destination Host routing fails, and for binding data to select a peer for related diameter sessions. The Session Routing Table is configured within a “Peer Group SRK Mapping” Table. If a routing with dest-host fails, CPS vDRA will try to find out secondary routes on the basis of SRK.

Once the SRK of failed peer is determined by CPS vDRA, it will try to find an UP peer that is a member of:

- A peer group matching the entire SRK label. If it finds one, it will route the message to that peer.

- If it cannot find one and it is a two-label SRK, then it will try to find an UP peer in a peer group whose label2 part of its SRK matches the label2 part of the lookup SRK (where the label 1 part may be different). If it finds one, then it will route the message to that peer.

The following screenshot shows an example of SRK configuration:

Figure 10: SRK Configuration

| Peer Group * (key) | Session Routing Key | Destination Host Routing Rule * | Destination Host Replace | Destination Realm Replace | Actions |
|--------------------|---------------------|---------------------------------|--------------------------|---------------------------|---------|
| GX_DC_1 | | preferred | | | |
| SD_DC_2 | | preferred | | | |
| GX_DC_2 | | preferred | | | |
| GX_DC_3 | clusterb.dc1 | preferred | | | |
| SD_DC_3 | clusterb.dc2 | preferred | | | |
| RX_DC_2 | clusterb.dc1 | preferred | | | |

Configure Binding Retriever for Rx Calls



Note This configuration is valid for Policy only.

Rx (AAR) Message processing: Policy DRA receives the AAR request from Application Function (AF). AAR messages does not have destination host and the destination PCRF has to be found out by vDRA using the keys such as:

1. Framed Ipv6 Address
2. Framed IP address
3. IMSI APN key
4. MSISDN APN key

Binding is created by vDRA when Gx-CCRI is received at DRA. DRA creates the bindings on the basis of CRD configurations and the availability of AVPs in Gx message. If the configured keys are present in Gx message, vDRA creates and stores the binding in Binding Database. On receiving AAR request, vDRA searches for the session stored in bindings on the basis of Rx profile, and will determine the SRK of Gx-PCRF peer. DRA will then forward the Rx request to the Rx peer having the same SRK. [SRK will be configured as mentioned in following section].

Configure SLF Based Routing



Note This configuration is valid for IMS DRA only.

SLF Routing works with two major configurations and tables within CRD:

1. SLF Trigger Profile: For the incoming Diameter requests where Destination-Host is not present (or Destination-Host is present with same of DRA-Host Name) this SLF Trigger table is triggered. In this Table, there are three inputs that you need to configure:

- Application-Id: Diameter Application ID for which the SLF Query is to happen.
- Command-Code: Diameter Command Code for which the SLF query is to happen.



Note If this field is configured with a ‘*’, it indicates that SLF query is expected to happen for all the command codes for the specific application.

- Destination-Realm: Destination-Realm of the Diameter Endpoint (that is, HSS/AAA) or the Destination Realm of vDRA.

Based on the Input keys (Application-Id, Command-Code and Destination-Realm) configured, if all the entries (as mentioned above) matches with the incoming message then vDRA(SLF) picks the “SLF Lookup Type” and “SLF-Destination-Type” as configured in the SLF Trigger Table.

- SLF LookupType- Currently the SLF LookupType can be configured as IMSI or MSISDN. Based on the configured value of IMSI or, MSISDN, vDRA (SLF) further makes a query towards the SLF-DB.
- SLF Destination-Type-Based on the configured value in the ‘SLF Destination Type’, vDRA (SLF) makes a further query towards the SLF-DB.

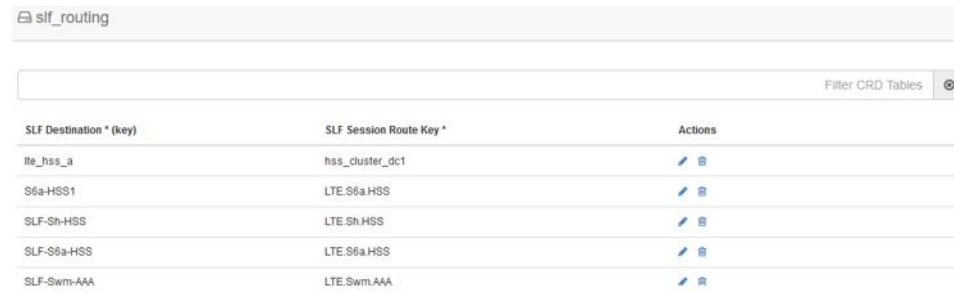
Figure 11: SLF Trigger Profile











| Application ID * (key) | Command Code * (key) | Destination Realm * (key) | Primary Lookup Type * | Secondary Lookup Type | SLF Destination Type * | Actions |
|------------------------|----------------------|------------------------------|-----------------------|-----------------------|------------------------|---------|
| 16777291 | * | slh-hss.com | | | LTE-HSS | |
| 16777217 | * | sh-hss.com | | | LTE-HSS | |
| 16777251 | * | slh-hss.com | | | LTE-HSS | |
| 16777217 | * | sh-hs.com | MSISDN | | Sh-HSS | |
| 16777251 | * | mnc286.mcc311.dranetwork.org | IMSI | | S6a-HSS | |

2. SLF Routing: After vDRA(SLF) makes the query in SLF-DB based on SLF-LookupType and SLF-Destination-Type, an SLF-Destination is obtained.

SLF Mapping table consists a mapping of ‘SLF-Destination’ which is obtained from the SLF database and a SLF-Session-Route-Key(SLF-SRK). In the SLF Mapping Table, based on the SLF-Destination an SLF-Session-Route-Key (SLF-SRK) is derived and further Peer group is derived for routing from the Peer-Group-Peer table as the next step for Routing.

Figure 12: SLF Routing



| SLF Destination * (key) | SLF Session Route Key * | Actions |
|-------------------------|-------------------------|---|
| lle_hss_a | hss_cluster_dct |   |
| S6a-HSS1 | LTE.S6a.HSS |   |
| SLF-Sh-HSS | LTE.Sh.HSS |   |
| SLF-S6a-HSS | LTE.S6a.HSS |   |
| SLF-Swm-AAA | LTE.Swm.AAA |   |

Configure Table Driven Routing

CPS vDRA has the ability to use AVPs within the Diameter messages to help determine how to route the traffic.

The AVP being evaluated is customer configurable, through the CPS DRA GUI. The addition, subtraction, or modification of the evaluation AVP is dynamic and affected real time.

Trigger Condition for Table-driven Routing:

- After Destination-Host based routing (first priority) and SRK routing (second priority) conditions are not met, vDRA goes for Table-driven routing as third priority.
- Typically, for Table-driven Routing to trigger, a Diameter message contains a Destination-Realm AVP, but no Destination-Host AVP. So, If the Dest-Host AVP is absent, empty, or equal to the DRA FQDN, then we skip Dest-Host routing altogether and proceed directly to Table-Driven routing.



Note For IMS-DRA only, the router will try to do the SLF routing (if all conditions are met), before moving to table-driven routing.

vDRA can parse and has the ability to route based on the following AVPs:

- 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 are also supported. The following configuration is required in Policy Builder:

1. Application Route: For more information, see [Basic Configuration, on page 1](#).

2. Routing AVP definitions: For more information, see [Basic Configuration, on page 1](#).
3. Search table group configurations: For more information, see [Search Table Groups](#).
4. CRD configuration: For more information, see [Custom Reference Data Tables](#).

Advanced Features

Configure Rate Limiting

You can use CPS vDRA to set rate limiting of traffic coming from and going towards a particular peer. You can configure this for both Ingress and Egress traffic. Rate limit is currently supported at peer level and message level.

1. Configure the Message Rate Limit Profile CRD table.

Create the rate limit profile with the rate limit profile name, application ID, command code, message type, and message rate limit. For more information, see [Search Table Groups – Message Rate Limit Profile table](#).

Figure 13: Message Rate Limit Profile

The screenshot shows a table titled "Message Rate Limit Profile" with the following columns: Rate Limit Profile Name * (key), Application Identifier * (key), Command Code * (key), Message/Request Type * (key), Message Rate Limit *, and Actions. A single row is displayed with the values: GX-CCR-I, Gx, 272, 1, 7. Below the table, there is an "Add Row" button and a pagination control showing "Show 10 rows" and "1 out of 1".

| Rate Limit Profile Name * (key) | Application Identifier * (key) | Command Code * (key) | Message/Request Type * (key) | Message Rate Limit * | Actions |
|---------------------------------|--------------------------------|----------------------|------------------------------|----------------------|---|
| GX-CCR-I | Gx | 272 | 1 | 7 | Edit Delete |

+ Add Row

Show 10 rows | 1 out of 1

2. Configure the Peer Rate Limiting CRD table.

Define the peer group, peer fqdn, message direction (ingress or egress), rate limit profile (created in step 1), peer rate limit, discard behavior (whether to silently drop or send error message). For more information, see [Search Table Groups – Peer Rate Limit Profile table](#).

If you want the discard behavior sent in the error answer, also configure the Result Code, Error String to be sent in the answer.

Figure 14: Peer Rate Limit Profile

| Peer Group * (key) | Peer FQDN * (key) | Message Direction * (key) | Rate Limit Profile | Peer Rate Limit | Discard Behavior * | Result Code | Error String | Actions |
|--------------------|-------------------|---------------------------|--------------------|-----------------|--------------------|-------------|--------------|---------|
| match=GX_DC.* | * | Ingress | GX-CCR-I | 3 | Send Error Answer | 3002 | OVERLOAD_GX | |

Configure Error Result Code Profile

CPS vDRA generates several internal errors that are not generic, for example, errors such as Timeout triggered, Peer not found, DB error, and so on.

You can configure error codes and error messages for internally generated errors in CPS vDRA.

To configure this error code, add entry in the Error Result Code Profile table as shown in the following image:

Figure 15: Error Result Code Profile

| Application Id * (key) | Error * (key) | Result Code | Exp Result Code | Vendor Id | Err Msg | Actions |
|------------------------|---------------------------|-------------|-----------------|-----------|------------------------------|---------|
| * | No Available Peer | 4004 | 5004 | 10415 | Peer not available | |
| * | No Peer Group | 4005 | | 10415 | No Peer Group Available | |
| * | No Binding Found | 3024 | | 10415 | No Binding found for request | |
| * | Message Loop Detected | 4007 | | 10415 | Loop Detected in Message | |
| * | No Binding Key For Lookup | | 4008 | 10415 | No Binding Key for Lookup | |

For a particular Application ID, if DRA generates an internal error, the error code defined in this table along with the Error Message is sent back in the answer.

If the result code is not configured and the Experimental Result Code is present, then the Experimental Result-Code is sent back in the answer along with Vendor-Id AVP. Between the Result-Code and the Experimental Result code, the Result-code is of higher priority.

Configure Peer Group Answer Timeout

You can set the different request timeout durations for different application ID and peer group. In CPS vDRA, timeout is the amount of time that vDRA waits for the answer from the destination.

To configure this feature, add an entry in the Peer Group Answer Timeout table. The timeout value is in milliseconds.

The default timeout is 1.7 seconds. You can also override the timeout for specific interface in this table as shown in the following image:

Figure 16: Peer Group Answer Timeout

| Application Id * (key) | Peer Group * (key) | Timeout Milliseconds | Actions |
|------------------------|--------------------|----------------------|---------|
| 16777238 | GX_DC_1 | 25000 | |
| 16777238 | GX_DC_2 | 22000 | |
| 16777238 | GX_DC_3 | 20000 | |
| 16777236 | RX_DC_1 | 20000 | |
| 16777303 | SD_DC_1 | 25000 | |
| 16777303 | SD_DC_2 | 25000 | |
| 16777236 | RX_DC_2 | 22000 | |

+ Add Row

Show 10 rows | 1 out of 1



















Configure Peer Load Balancing

CPS vDRA has capabilities to route messages based on weight and precedence of the peer. Perform the following steps to define the peer load balancing:

1. Configure the Peer Routes table:

- This table defines the name of the Peer Routes that are then used in the Peer Routing table.
- This table is mainly used in Table-driven routing where the peer route is derived from the application table-driven rule tables.

Figure 17: Peer Routes

| Peer Routes | |
|--------------------|---|
| Peer Route * (key) | Actions |
| GX_CONSUMER |   |
| GX_ENTERPRISE |   |
| RX_CONSUMER |   |
| RX_CONSUMER_SITE |   |
| GX_CONSUMER_C |   |
| SD_CONSUMER |   |
| SD_CONSUMER_1 |   |
| RX_ENTERPRISE |   |
| SD_CONSUMER_2 |   |

+ Add Row

Show 10 rows out of 1

- Configure the Peer Group Mapping table. This table defines the mapping of peers and realm with peer group.
 - Once the peer group is derived, CPS vDRA looks up this table to find the peers that belong to the derived peer group. Once DRA lists the peers in the peer group, it tries to match these peers with the Active Peer list, that is, peers which are currently connected to CPS vDRA.

If multiple peers are up in a peer group, CPS vDRA load balances the traffic in a round-robin manner according to peer weight.





















The peer weight range is 0-1000 and the default weight is 100. If a peer weight is 0, then that peer is skipped.

For example, if there are two peers up in a peer group with weights 100 and 200 respectively, then CPS vDRA load balances traffic between the two peers in the ratio of 33% and 67% respectively.
 - This table is applicable to SRK and Table driven routing only and is not used in Destination Host routing.

Figure 18: Peer Group Mapping

Peer Group Mapping

Filter CRD Tables

| Realm Pattern * (key) | FQDN Pattern * (key) | Peer Group | Actions |
|-----------------------|----------------------|------------|---|
| gx-pcef.cisco.com | gx-pcef | GX_DC_3 |   |
| gx-pcrf.cisco.com | gx-pcrf | GX_DC_1 |   |
| rx-pcrf.cisco.com | rx-pcrf | RX_DC_2 |   |
| * | sd-pcrf | SD_DC_1 |   |
| * | gx-pcrf | GX_DC_1 |   |
| * | gx-pcrf2 | GX_DC_2 |   |
| * | gx-pcrf3 | GX_DC_1 |   |
| * | gx-pcrf4 | GX_DC_2 |   |
| * | pcrf2-gx2 | GX_DC_1 |   |
| * | rx-af | RX_DC_1 |   |

+ Add Row

Show 10 rows out of 2

3. Configure the Peer Routing table.

This table requires the following inputs:

- Peer Route – derived from the Peer Route table
- System Id – the current system ID of the CPS vDRA system
- Peer Group – derived from the Peer Group Mapping table

The outputs of this table are:

- Precedence
- Weight

Weight and Precedence are used to load balance the traffic among peers.

Figure 19: Peer Routing

| Peer Routing | | | | | |
|--------------------|-------------------|--------------------|--------------|----------|-------------------------------------|
| Peer Route * (key) | System Id * (key) | Peer Group * (key) | Precedence * | Weight * | Actions |
| SD_CONSUMER_2 | system-1 | SD_DC_1 | 1 | 1 | ✎ 🗑 |
| GX_CONSUMER | system-1 | GX_DC_1 | 1 | 1 | ✎ 🗑 |
| RX_CONSUMER | system-1 | GX_DC_1 | 1 | 1 | ✎ 🗑 |
| RX_CONSUMER | system-1 | GX_DC_2 | 1 | 1 | ✎ 🗑 |
| SD_CONSUMER | system-1 | SD_DC_2 | 1 | 1 | ✎ 🗑 |
| GX_CONSUMER_C | system-1 | GX_DC_3 | 1 | 1 | ✎ 🗑 |
| SD_CONSUMER_1 | system-1 | SD_DC_2 | 1 | 1 | ✎ 🗑 |

+ Add Row

Show 10 rows out of 1

Configure Message Retries

CPS vDRA has the capability of retrying messages to multiple connected peers, in case the destination peer is not up. Retry mechanism works completely on the basis of SRK.

To configure message retries, you need to configure the Message Retry Profile table.

Figure 20: Message Retry Profile

| Message Retry Profile | | | | | | |
|-----------------------|------------------------|----------------------|---------------------|-----------------|-------------------|-------------------------------------|
| Peer Group * (key) | Application Id * (key) | Command Code * (key) | Result Code * (key) | Experimental RC | Number Of Retries | Actions |
| GX_DC_1 | 16777238 | 272 | 3003 | false | 6 | ✎ 🗑 |
| GX_DC_1 | 16777238 | 272 | 3004 | false | 6 | ✎ 🗑 |
| GX_DC_2 | 16777238 | 272 | 3003 | false | 6 | ✎ 🗑 |
| GX_DC_2 | 16777238 | 272 | 3004 | false | 6 | ✎ 🗑 |
| match=SD_DC.* | 16777303 | 8388637 | 3004 | false | 6 | ✎ 🗑 |
| RX_DC_1 | 16777236 | 258 | 7000 | false | 6 | ✎ 🗑 |
| GX_DC_2 | 16777238 | 272 | 7000 | false | 6 | ✎ 🗑 |

+ Add Row

Show 10 rows out of 1

You can configure message retry on the basis of the following inputs:

- Peer Group
- Application Id
- Command Code

- Result-Code

The outputs of this table are:

- Number of retries
- Experimental RC

When the retry criteria matches, then:

1. First, the retry is done on any connected peer in the same peer group.
2. If no peer is found in the same peer group, the next priority is given to the peers in the peer group having the same SRK as the peer group to which the request was originally sent.
3. If the above condition also fails to find a peer, the last priority is given to the peers in the peer group that share the same second label as that of the original peer group.



Note CPS vDRA uses the Peer Group Mapping table to find the peer in the same peer group. Hence, the Peer Group Mapping table configuration is a prerequisite.

At the end, if no peer is found, retries stop. The retry also stops when the number of retries is exhausted and no response is received.

Configure Reserved IMSIs

You can now specify a reserved MCC range so that vDRA validates a parsed IMSI for SLF routing against a configured list of reserved MCC. If the IMSI matches a reserved IMSI, the value is ignored for SLF routing.

Configure the Reserved IMSI CRD table with columns for MCC Start Range and MCC End Range.

Figure 21: Reserved IMSI CRD Table

Custom Reference Data Table (Read Only)

*Name: reserved_mcc Display Name: Reserved MCC Cache Results Activation Condition:

| *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 |

Column Details

| Valid Values | Validation | Runtime Binding |
|---|---|--|
| The values allowed in Control Center for this column * All <input type="radio"/> List of Valid Values | Validation used by Control Center Regular Expression <input type="text"/> Regular Expression Description <input type="text"/> | Which rows match <input checked="" type="radio"/> None <input type="radio"/> Bind to Subscribe <input type="radio"/> Bind to Session? |

For more information, see [Reserved IMSI](#).

In DRA, configure the MCC Start Range and MCC End Range.

Figure 22: MCC Range

| Reserved MCC | | |
|--------------|---------|--|
| MCC Start | MCC End | |
| 300 | 311 | |

Any calls within Reserved IMSI range are either routed by alternate means such as table-driven routing or result with an error.

Configure Multiple Lookup in SLF Trigger Profile

Previously, in vDRA, the SLF lookup Type in the SLF trigger table had options only to support two types of lookup, that is, IMSI, MSISDN.

You can now specify Primary and Secondary Lookup Keys in the SLF Trigger Profile Table.

First, configure the columns in the CRD table as shown:

Figure 23: CRD Table Configuration

| Application ID | Command Code | Destination Realm | Primary Lookup Type | Secondary Lookup Type | |
|----------------|--------------|-----------------------------------|---------------------|-----------------------|-------|
| 16777251 | * | sf-hss.com | IMSI | | LTE→ |
| 16777291 | * | sf-hss.com | IMSI | | LTE→ |
| 16777217 | * | ims.mnc286.mcc311.3gppnetwork.org | MSISDN | IMSI | LTE→ |
| 16777251 | * | mnc286.mcc311.3gppnetwork.org | IMSI | | S6a-H |
| 16777217 | * | mnc286.mcc311.3gppnetwork.org | | | |

In the SLF Trigger Profile, you can select the Primary Lookup key from the drop down list. Similarly, you can select the Secondary Lookup key.

Figure 24: SLF Trigger Profile

| Custom Reference Data Table (Read Only) | | | |
|---|---------------------|-------------------------------------|------------------|
| Name | Display Name | Cache Results | Evaluation Order |
| slf_trigger_profile | SLF Trigger Profile | <input checked="" type="checkbox"/> | 0 |

| Name | Display Name | *Use In Conditio | *Type |
|-----------------------|-----------------------|-------------------------------------|-------|
| application_id | Application ID | <input checked="" type="checkbox"/> | Text |
| cmd_code | Command Code | <input checked="" type="checkbox"/> | Text |
| dest_realm | Destination Realm | <input checked="" type="checkbox"/> | Text |
| primary_lookup_type | Primary Lookup Type | <input checked="" type="checkbox"/> | Text |
| secondary_lookup_type | Secondary Lookup Type | <input checked="" type="checkbox"/> | Text |
| slf_destination_type | SLF Destination Type | <input checked="" type="checkbox"/> | Text |

Modify Result Code for AVPs Using Mediation Rules

You can configure CRDs to modify the result code of AVPs and overwrite them with a specified value.

1. Define the AVPs in the Diameter Avp Dictionary as shown in the following example for ResultCode:

Figure 25: ResultCode AVP in Diameter Avp Dictionary

| Name * (key) | Avp Code | Vendor Id | Avp Type | Actions |
|--------------|----------|-----------|------------|---------|
| ResultCode | 268 | 10415 | Unsigned32 | |

+ Add Row

Show 10 rows | 1 out of 1

2. Add the condition that is used to match AVPs with a particular result code. In this example, ResultCodeIs3xxx matches the result code AVP with regular expression 3.* and checks for any 3xxx result code.

Figure 26: Add Result Code Condition in Avp Condition Profile

| Profile Name * (key) | Avp * (key) | Avp Value * | Actions |
|----------------------|-------------|-------------|---------|
| ResultCodeIs3xxx | ResultCode | match=3.* | |

+ Add Row

3. Define the action to be performed in the Avp Action Profile. In this case, ChangeResultcode is used to overwrite AVP values with the value 3002.

Figure 27: Define Action in Avp Action Profile

| Profile Name * (key) | Avp * (key) | Avp Action | Avp Value | Actions |
|----------------------|-------------|----------------------|-----------|---------|
| ChangeResultCode | ResultCode | Overwrite with value | 3002 | |

4. Add the mediation rule in the Message Mediation Profile.

In the following example, the mediation rule is considered on answer in ingress direction, when application is 16777251, command is 318, and condition profile ResultCode3xxx is met. When all criteria are satisfied, the “ChangeResultCode” action profile is applied.

Figure 28: Mediation Rule

| Application Id * (key) | Command Code * (key) | Message Type * (key) | Peer Group * (key) | Message Direction * (key) | Condition Profile * (key) | Action Profile * (key) | Actions |
|------------------------|----------------------|----------------------|--------------------|---------------------------|---------------------------|------------------------|---------|
| 16777251 | 318 | Answer | * | Ingress | ResultCode3xxx | ChangeResultCode | |

Hide Topology Using Mediation Rules

Define mediation rules to hide topology.

1. Define the AVPs in the Diameter Avp Dictionary as shown in the following example for OriginHost and OriginRealm:

Figure 29: Diameter Avp Dictionary

| Name * (key) | Avp Code | Vendor Id | Avp Type | Actions |
|--------------|----------|-----------|-------------|---|
| OriginHost | 264 | 10415 | OctetString | Edit Delete |
| OriginRealm | 296 | 10415 | OctetString | Edit Delete |

2. Define the action to be performed in the Avp Action Profile. In this case, Hiding is used to overwrite the Origin Host AVP with the value “dra” and to overwrite the Origin Realm AVP with the value “dra.cisco.com”.

Figure 30: Define Action in Avp Action Profile

| Profile Name * (key) | Avp * (key) | Avp Action | Avp Value | Actions |
|----------------------|-------------|----------------------|---------------|---|
| Hiding | OriginHost | Overwrite with value | dra | Edit Delete |
| Hiding | OriginRealm | Overwrite with value | dra.cisco.com | Edit Delete |

3. Add the mediation rule in the Message Mediation Profile.

In the following example, mediation rule is considered on request and answer in egress direction. It is applicable to all application, all commands, all peer groups and all message types (request/answer). When criteria satisfied, the “Hiding” action profile is applied.

Figure 31: Mediation Rule

| Application Id * (key) | Command Code * (key) | Message Type * (key) | Peer Group * (key) | Message Direction * (key) | Condition Profile * (key) | Action Profile * (key) | Actions |
|------------------------|----------------------|----------------------|--------------------|---------------------------|---------------------------|------------------------|---|
| - | - | - | - | Egress | - | Hiding | Edit Delete |

Configure Mediation Rule for Proxy-Unaware Endpoints

When endpoints are not proxy-aware, PCRF may send an RAR to the vDRA without Destination Host AVP because it is not proxy friendly.

In such cases, you can configure vDRA to modify the Destination-Host of the RAR based on a regex match of the Diameter Session-ID.

1. Define the AVPs in the Diameter Avp Dictionary as shown in the following example for DestinationHost and SessionId:

Figure 32: Diameter Avp Dictionary

| Name * (key) | Avp Code | Vendor Id | Avp Type | Actions |
|-----------------|----------|-----------|-------------|-----------------|
| DestinationHost | 293 | 10415 | OctetString | [edit] [delete] |
| SessionId | 263 | 0 | OctetString | [edit] [delete] |

- Define the action to be performed in the Avp Action Profile. In this case, ExtractHostFromSessionId is used to overwrite the DestinationHost AVP with the value dynamically derived from the regex string:

```
SubString("${SessionId}", "([^;]+);.*" , 1)
```

The session ID is taken from the message, then regex ([^;]+);.* is applied on the session ID and host is extracted.

For example, if the session ID is “pcef;1450914337;172.30.96.2;0”.

Regex ([^;]+);.* is applied on session ID and it will get 2 groups:

- group1= “pcef”
- group2 = “1450914337;172.30.96.2;0”

Hence, the Destination Host is set with value pcef.

Figure 33: Define Action in Avp Action Profile

| Profile Name * (key) | Avp * (key) | Avp Action | Avp Value | Actions |
|--------------------------|-----------------|----------------------|---|-----------------|
| ExtractHostFromSessionId | DestinationHost | Overwrite with value | SubString("\${SessionId}", "[^;]+);.*" , 1) | [edit] [delete] |

- Add the mediation rule in the Message Mediation Profile.

In the following example, mediation rule is considered on Gx RAR in ingress direction. When all the criteria are met, the “ExtractHostFromSessionId” action profile is applied. Action will set the DestinationHost AVP just after receiving message.

Figure 34: Mediation Rule

| Application Id * (key) | Command Code * (key) | Message Type * (key) | Peer Group * (key) | Message Direction * (key) | Condition Profile * (key) | Action Profile * (key) | Actions |
|------------------------|----------------------|----------------------|--------------------|---------------------------|---------------------------|--------------------------|-----------------|
| 16777238 | 258 | Request | * | Ingress | * | ExtractHostFromSessionId | [edit] [delete] |

Add Prefix to an AVP Using Mediation Rules

You can define a prefix for an AVP.

- First, define the AVPs in the Diameter Avp Dictionary as shown in the following example for the AVP, DestinationHost:

Figure 35: Defining DestinationHost in Diameter Avp Dictionary

| Name * (key) | Avp Code | Vendor Id | Avp Type | Actions |
|-----------------|----------|-----------|-------------|---------|
| DestinationHost | 293 | 10415 | OctetString | |
| SessionId | 263 | 0 | OctetString | |

- Define the PrependLabel profile in the Avp Action Profile that adds the prefix "core-" to the DestinationHost AVP.

Figure 36: Define PrependLabel Profile in Avp Action Profile

| Profile Name * (key) | Avp * (key) | Avp Action | Avp Value | Actions |
|----------------------|-----------------|------------|-----------|---------|
| PrependLabel | DestinationHost | Add Prefix | core- | |

- Add the mediation rule in Message Mediation Profile as shown in the following example.

In this example, the mediation rule is applied on s6 AIR request message in egress direction. When the peer group also matches hss-g, it will apply the “PrependLabel” action profile. Action will add the prefix “core-“ to destination host.

Figure 37: Mediation Rule in Message Mediation Profile

| Application Id * (key) | Command Code * (key) | Message Type * (key) | Peer Group * (key) | Message Direction * (key) | Condition Profile * (key) | Action Profile * (key) | Actions |
|------------------------|----------------------|----------------------|--------------------|---------------------------|---------------------------|------------------------|---------|
| 1677251 | 318 | Request | hss-g | Egress | x | PrependLabel | |

Configure Throttling of Diameter Messages Using DOIC

About DOIC

vDRA can throttle or divert 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).

The DOIC feature in vDRA involves the following high-level processes:

DOIC Enablement

DOIC feature is enabled/disabled in vDRA and also for the peer group.

DOIC Capability Exchange

If the DOIC feature is enabled, then for every request received, vDRA adds the OC-Supported-Features AVP to the request message to announce the DOIC support for loss of algorithm.

OCS Map

The OCS Map is the local vDRA cache, which contains the information of each reporting node with its latest overload control state information. On receipt of OC-OLR AVP from the peer, vDRA looks for the entry in OCS Map and updates the overload control state object.

Peer Overload Detection

vDRA checks the OCS entry from the OCS Map to determine whether the overload treatment is required or not.

Table Lookup

vDRA queries the Message Class Profile table to retrieve the Message classification. The message classification is used to query the DOIC Profile table to determine the Abatement Action that must be applied.

Overload Treatment

There are three types of overload treatment supported: Forward, Divert, and Drop. For more information, see [DOIC Profile](#).

Configuring DOIC in vDRA

To configure vDRA for throttling, perform the following steps:

1. Enable DOIC feature in vDRA in the Policy Builder as described in [Enable DOIC, on page 5](#).
2. Enable DOIC for the peer group using the Peer Group SRK mapping table as described in [Peer Group SRK Mapping](#).
3. Define the AVP condition in the Diameter AVP Dictionary table. For more information, see [Diameter Avp Dictionary](#).
4. Configure the Message Class Profile table to get the message classification as output. For more information, see [Message Class Profile](#).

If AVP conditions are evaluated to be true, then get Message Class. Message Class can be one of P0, P1, P2, P3, P4.
5. Use the Message class to define the abatement action in the DOIC Profile table. For more information, see [DOIC Profile](#).

Configure Throttling of Diameter Messages Using DRMP

vDRA can throttle Diameter requests based on the message priority sent in the Diameter request using the architecture described in RFC 7944 Diameter Routing Message Priority (DRMP).

To configure vDRA to use DRMP, perform the following steps as described in [Configure Throttling of Diameter Messages Using DOIC, on page 22](#). Ensure you use the DRMP AVP in the Diameter Avp Dictionary table.

With this configuration, messages with Message Class P0 are not throttled in either rate limiter or by DOIC. For the rest of the messages, the throttling is applied as configured in DOIC table or in rate limiter.

Rate limiter currently throttles message regardless of the message class/ DRMP value. However, it will not throttle the message with message class P0.

Configure vDRA for eMPS

You can configure vDRA to recognize Diameter messages as Enhanced Multimedia Priority Services (eMPS) based on Diameter Application-Id, Command-Code, and AVP values.

An eMPS request is marked as a Priority 0 (or P0 in message classification) request and is not throttled or dropped.

1. Specify the AVP in the Diameter Avp Dictionary as shown in the following example:

Figure 38: Diameter Avp Dictionary

| Diameter Avp Dictionary | | | | |
|-------------------------|----------|-----------|-------------|---|
| Name * (key) | Avp Code | Vendor Id | Avp Type | Actions |
| * | | | |   |
| Called-Station-Id | 30 | 10415 | OctetString |   |
| MPS-Identifier | 528 | 10415 | OctetString |   |



2. Specify the AVP condition in the Avp Condition Profile table.

Figure 39: Avp Condition Profile

| Avp Condition Profile | | | |
|-----------------------|-------------------|-------------|---|
| Profile Name * (key) | Avp * (key) | Avp Value * | Actions |
| * | * | |   |
| IsEmergency | Called-Station-Id | 911 |   |

3. In Message Class Profile, configure the Message/Request Type as 'None', Message Class as P0, and Ingress Peer Group as '*', so that the message is treated as eMPS irrespective of the type of message (request or response) and the peer group it is sent to.

Figure 40: Message Class Profile

| Message Class Profile | | | | | | |
|-----------------------|------------------|----------------|------------------------|---------------------|---------------|---|
| Ingress Peer Group * | Application Id * | Command Code * | Message/Request Type * | Condition Profile * | Message Class | Actions |
| * | 1677238 | 272 | None | IsEmergency | P0 |   |

[+ Add Row](#)

Show 10 rows | 1 out of 1

Configure Topology Hiding for S6a/d Diameter Application

Configure topology hiding for the S6a/d Diameter application (Diameter interface between the MME/SGSN and the HSS).

1. Configure a trusted realm profile: Define the name of a Trusted Profile and associate a realm which can be trusted with it.

Figure 41: Trusted Realm Profile

| Trusted Profile Name * | Trusted Realm * | Actions |
|------------------------|---|---|
| HSS_TRUSTED_PROFILE | imstrusted2.mnc287.mcc312.3gppnetwork.org | Edit Delete |
| MME_Trusted_Profile | mme trusted.mnc33.mcc404.3gppnetwork.org | Edit Delete |

2. Configure the Protected realm (where vDRA is to provide the topology hiding) and link it to the trusted profile.

Depending on the requests, if the destination/origin realm is trusted, vDRA skips the topology hiding. If the realm is not trusted, vDRA provides topology hiding.

Figure 42: Protected Realm Trusted Profile

| Protected Realm * | Profile Name * | Actions |
|--|---------------------|---|
| imsprotected2.mnc33.mcc404.3gppnetwork.org | HSS_TRUSTED_PROFILE | Edit Delete |

3. In the MME Alias Map, define the MME FQDN, which needs to be protected, and bind it to the Aliases that are used for topology hiding.

Figure 43: MME Alias Map

| MME FQDN * | Alias 1 * | Alias 2 | Alias 3 | Actions |
|---|---|---------------------|---------|---|
| mme1foreign.s6a.ims.mnc287.mcc312.3gppnetwork.org | foreign_mme_alias.mnc287.mcc312.3gppnetwork.org | foreign_mme_alias_2 | | Edit Delete |

4. Define all the HSS Aliases that are used for HSS topology hiding by vDRA in the HSS Aliases table. Specify whether the defined alias is shared or not by multiple protected HSSs.

Figure 44: HSS Aliases

| HSS Aliases | | |
|--|----------------|-------------------------------------|
| Filter CRD Tables | | |
| HSS Alias FQDN * | Shared Alias * | Actions |
| hss_alias_1.s6a.ims.mnc33.mcc404.3gppnetwork.org | true | ✎ ✖ |
| hss_alias_2.s6a.ims.mnc33.mcc404.3gppnetwork.org | false | ✎ ✖ |

- In the HSS Alias Map, map the protected HSS FQDN with the HSS ALIAS defined in previous HSS Aliases table. These aliases are used for the topology hiding of the protected HSSs.

Figure 45: HSS Alias Map

| HSS Alias Map | | | | |
|---|--|---------|---------|-------------------------------------|
| Filter CRD Tables | | | | |
| HSS FQDN * | Alias 1 * | Alias 2 | Alias 3 | Actions |
| hss33protected.s6a.ims.mnc33.mcc404.3gppnetwork.org | hss_alias_1.s6a.ims.mnc33.mcc404.3gppnetwork.org | | | ✎ ✖ |
| hss34protected.s6a.ims.mnc33.mcc404.3gppnetwork.org | hss_alias_1.s6a.ims.mnc33.mcc404.3gppnetwork.org | | | ✎ ✖ |

Manual Peer Disconnection using REST API

CPS vDRA provides a REST API that you can use to manually disconnect peer connections from vDRA. To disconnect a single peer connection, you need to provide the peer connection key information in the API method.

Disconnect a single peer connection

To disconnect a single peer, provide the peer-connection-key (that you can find in the peer endpoint details) in the PUT method as shown:

```
PUT localActivePeerEndpoints/disconnect/key/<peer-connection-key>
```

Responses:

```
200 OK
{
  "success": {
    "code": 0,
    "message": "Request completed successfully"
  }
}
```

Note that success means the request is accepted, and vDRA attempts to disconnect the peer connection. The success response does not indicate that the peer connection has been disconnected.

Failure response:

```
404 Not Found
{
  "error": {
    "code": 2014,
    "message": "Data for key <peer-connection-key> is not found"
  }
}
```

Policy DRA Relay Configuration

Policy DRA requires a full-mesh topology to be able to send traffic between different sites. In a multi-site DRA network, relay connections are required between every pair of relay endpoints.

Relay Endpoint Configuration

Relay endpoint is used to indicate the IP address/port combination at which vDRA listens for diameter connections. These connections are used to send/receive diameter traffic between sites.

Relay endpoints for vDRA can be configured using the Policy Builder vDRA configuration plugin.

The following fields are required for the configuration:

VM Host Name

VM Host Name is the host name of the VM. The value '*' can be used to match any host name.

Instance ID

The Instance ID field should be set to '1'. Currently, no other value is supported.

IP Address

IPv4 or IPv6 address of the interface used to listen for relay connections. Currently, only physical IP addresses are supported. VIP addresses are not supported.

Port

Port that is used to listen for relay connections. The default value is '4868'. Currently, the range of ports supported is '4868-4878'.

FQDN

FQDN is the string that is used to send the relay endpoint information to the other sites.

Enabled

Used to enable or disable the relay endpoint. It should be enabled for the relay endpoint to start listening on the configured port and IP address.

Control Plane Configuration

The control plane configuration performs the following functions:

- If the IP address is a site-local address, a global Control Plane server is created that listens to connections.
- If the IP address not a site-local address, the connections are initiated from diameter-endpoint containers to the global Control Plane server running at specified IP/port. These connections are used to send and receive global control plane information between sites.

You can configure the control plane using the orchestrator CLI. Currently, VIP addresses are supported for control plane configuration as long as the VIP is reachable. The default port is 6379.

The following example illustrates control plane configuration:

```
admin@orchestrator# show running-config control-plane
control-plane relay gx-dra1-relay-v6-1
  address [2001:421:27c1:913:250:56ff:fea6:12]
  port 6379
```



Note The IPv6 address must be encapsulated with square [] brackets.

DNS Host Configuration

The following entities must be DNS resolvable and must have DNS Host configuration entries:

- Control Plane servers from all sites
- Relay Endpoint FQDNs from all sites

The following command is an example of DNS Host configuration:

```
admin@orchestrator# show running-config network dns host
network dns host gx-dra1-relay-v6 local
address 2001:421:27c1:913:250:56ff:fea6:48
```

Virtual-IP Configuration

The following entities must have virtual-IP configuration entries:

- Control Plane Servers with VIP addresses

Relay Configuration for a 6-Site Policy DRA System

The following example describes how to configure the relay configuration for a six site Policy DRA system.

Relay Endpoints

There must be two relay endpoint entries configured in Policy Builder per site; one entry each for the two diameter-endpoint containers.

Control Plane Configuration

There must be at least two global Control Plane servers configured per site; one on each diameter-endpoint for redundancy.

The global Control Plane servers must have connections between each other. This means that every site must have control plane configuration entries for the control plane servers of every other site.

For a six site system, every site must have 12 Control Plane configuration entries (6 sites x 2 global Control Plane servers per site) configured in CLI.

DNS Host Configuration

There should be one DNS Host entry for each of the global Control Plane configuration entries. In a six site system, every site should have 12 DNS Host entries related to global Control Plane entries of all sites.

There should be one DNS Host entry for each Relay endpoints of every site. In a six site system, every site should have 12 DNS Host entries related to Relay Endpoint entries of all sites.

Virtual-IP Configuration

If any global Control Plane servers have VIP addresses, they should have Virtual-IP Configuration.

Every site should have Virtual-IP Configuration for any VIP addresses that are associated to that site.