CPS vDRA Administration Guide, Release 21.2.0

First Published: 2021-08-27

Last Modified: 2021-11-12

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface vii

About This Guide vii

Audience vii

Additional Support viii

Conventions (all documentation) viii

Communications, Services, and Additional Information ix

Important Notes x

CHAPTER 1

About CPS DRA 1

DRA Overview 1

DRA Architecture 1

DRA System Flow 2

DRA Users And Roles 2

Access CPS DRA 3

Manage Users 4

Supported Browsers 5

CHAPTER 2

Configuring CPS DRA 7

Policy Builder Overview 7

System Configuration 7

Configure System 7

Add Clusters 8

Custom Reference Data Configuration 12

Create Search Table Group 12

Create Custom Reference Data Tables 14

Diameter Configuration 17

Add Gx Application 17
Add Gy Application 18
Add Rx Application 19
Add Sd Application 20
Diameter Routing 21
CPS Service Configuration 21
View Versioned Custom Reference Data Tables 22
View Details of Versioned CRD Tables 22
Import Data of Versioned CRD Tables 22
View Graphical Illustration of CRD Tables 22
View Details of STG Element 23
View Repository Details 23
Add New Repository 24
Select Repository 25
Switch Repository 25
Publish Configuration Changes 26
Publish Changes 26
Revert Changes 26
View Notifications 27

CHAPTER 3 **Managing Custom Reference Data** 29
Custom Reference Data Overview 29
Export Custom Reference Data 29
Import Custom Reference Data 29
View Custom Reference Data Tables 30
View Multiple CRD Tables 30
Edit Multiple CRD Tables 31
Import Custom Reference Data Table 31

CHAPTER 4 **Managing DRA Operations** 33
Operations Overview 33
Monitoring DRA 33
Peer Monitoring 33
View Filtered Data 34

View Details 37
View Event Logs 39
Binding Monitoring 40
View DRA Binding Details 40
View Gx Session Details 41
View Details 42
SLF Bindings 42
View SLF Bindings Details 42
Monitoring Relay Connections 45
View Relay Connections 45
View Relay Details 46
View Relay Event Logs 47
Monitoring Installation Using Grafana 47
Viewing CPS APIs 48

CHAPTER 5 **DRA Distributor** 49
Introduction 49
Direct Routing 50
ARP and IPv6 Neighbor Discovery 51
DRA Distributor Failover 52
Active-Active 53
Connection Synchronization 53
Health Checks 53

Preface

- About This Guide, on page vii
- Audience, on page vii
- Additional Support, on page viii
- Conventions (all documentation), on page viii
- Communications, Services, and Additional Information, on page ix
- Important Notes, on page x

About This Guide

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. While any existing biased terms are being substituted, exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

This document is a part of the Cisco Policy Suite documentation set.

For information about available documentation, see the *CPS Documentation Map* for this release at Cisco.com.

Note The PATS/ATS, ANDSF, and MOG products have reached end of life and are not supported in this release. Any references to these products (specific or implied), their components or functions in this document are coincidental and are not supported. Full details on the end of life for these products are available at: https://www.cisco.com/c/en/us/products/wireless/policy-suite-mobile/eos-eol-notice-listing.html.

Audience

This guide is best used by these readers:

- Network administrators

- Network engineers
- Network operators
- System administrators

This document assumes a general understanding of network architecture, configuration, and operations.

Additional Support

For further documentation and support:

- Contact your Cisco Systems, Inc. technical representative.
- Call the Cisco Systems, Inc. technical support number.
- Write to Cisco Systems, Inc. at support@cisco.com.
- Refer to support matrix at https://www.cisco.com/c/en/us/support/index.html and to other documents related to Cisco Policy Suite.

Conventions (all documentation)

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.

Conventions	Indication
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning IMPORTANT SAFETY INSTRUCTIONS.

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Note Regulatory: Provided for additional information and to comply with regulatory and customer requirements.

Communications, Services, and Additional Information

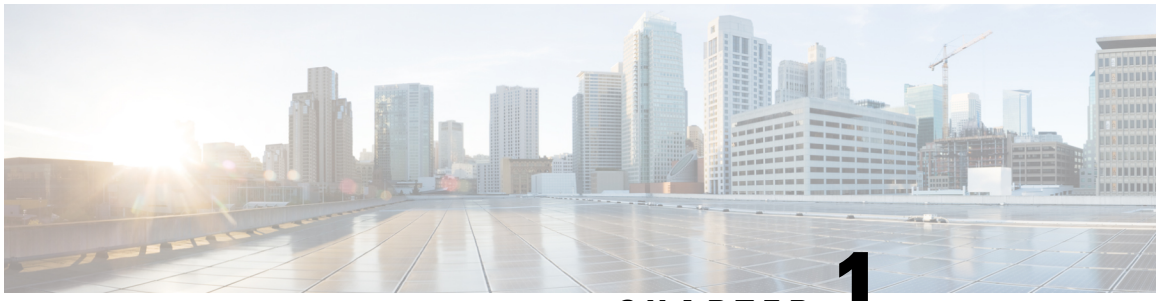
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Important Notes

Important Any feature or GUI functionality that is not documented may not be supported in this release or may be customer specific, and must not be used without consulting your Cisco Account representative.



CHAPTER 1

About CPS DRA

- DRA Overview, on page 1
- DRA Architecture, on page 1
- DRA Users And Roles, on page 2
- Access CPS DRA, on page 3
- Manage Users, on page 4
- Supported Browsers, on page 5

DRA Overview

Cisco Policy Suite DRA (Diameter Routing Agent) is a GUI platform that enables you to perform CPS vDRA related operations and launch the following applications and utilities:

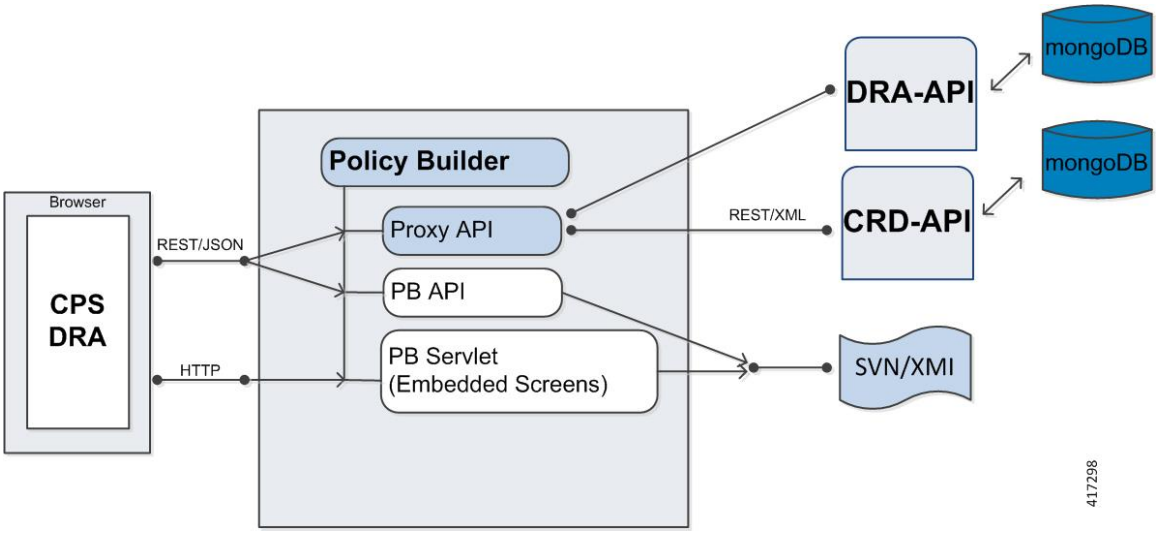
- Policy Builder - CPS Policy Builder with CPS vDRA specific options to customize and optimize CPS vDRA. For more information, see *Chapter 2 Configuring CPS DRA*.
- Custom Reference Data - Interface for service providers to create and populate data tables. For more information, see *Chapter 3 Managing Custom Reference Data*.
- Operations
  - DRA Monitoring - Interfaces to monitor the CPS vDRA related operations such as DRA Peer Monitoring, DRA Binding Monitoring, DRA SLF Bindings, and Grafana.
  - DRA API Information - Provides vPAS API and SLF API Documentation.

  For more information, see *Managing DRA Operations* chapter in this guide.

DRA Architecture

DRA GUI is compliant with CPS Central functional structure.

Figure 1: DRA Architecture



The following section describes different layers of the DRA GUI:

- PB API layer - Manages PB API requests and interfaces with other CPS APIs. The PB API layer is one unified CPS API layer.
- PB servlet layer - Manages requests and responses between DRA GUI and the embedded PB screens.
- DRA GUI client layer -DRA GUI which reuses PB2 modularity and implements CPS vDRA specific GUI.

DRA System Flow

The following section describes the DRA system flow:

1. DRA GUI initiates active/inactive peers in the PB Proxy API.
2. PB Proxy API invokes DRA API end points to retrieve CPS vDRA data.
3. DRA API returns data back to the PB Proxy API.
4. PB Proxy API returns data back to the DRA GUI.
5. DRA GUI renders the data.

DRA Users And Roles

The following types of users/roles are supported in CPS DRA:

- Admin: User with create, read, update, and delete (CRUD) access to CPS DRA.
- Read Only: Restricted to read access only.

Access CPS DRA

You can access CPS DRA on the same port as Policy Builder with */central/dra* and */central/dra/* context.

You can enter */central* or */central/* in the browser, the application server redirects you to either CPS Central or CPS DRA depending on the install type you have selected during installation.

To access the CPS DRA Interface, use the supported URLs as described in the following table:

Table 1: Supported URLs

Install Type	Entered URLs	Redirected URLs
DRA	https:// <*ip-address*>/	https:// <*ip-address*>:7443/central/dra/
	https:// <*ip-address*>:7443/central	https:// <*ip-address*>:7443/central/dra/
	https:// <*ip-address*>:7443/central/	https:// <*ip-address*>:7443/central/dra/
	https:// <*ip-address*>:7443/central/dra	https:// <*ip-address*>:7443/central/dra/
	https:// <*ip-address*>:7443/central/dra/	https:// <*ip-address*>:7443/central/dra/
	https:// <*ip-address*>:443/central	https:// <*ip-address*>:7443/central/dra/
	https:// <*ip-address*>:443/central/	https:// <*ip-address*>:7443/central/dra/
	https:// <*ip-address*>:443/central/dra	https:// <*ip-address*>:7443/central/dra/
	https:// <*ip-address*>:443/central/dra/	https:// <*ip-address*>:7443/central/dra/
Mobile	https:// <*ip-address*>/	https:// <*ip-address*>:7443/central/
	https:// <*ip-address*>:7443/central	https:// <*ip-address*>:7443/central/
	https:// <*ip-address*>:7443/central/	https:// <*ip-address*>:7443/central/
	https:// <*ip-address*>:7443/central/dra	HTTP ERROR 404
	https:// <*ip-address*>:7443/central/dra/	HTTP ERROR 404
	https:// <*ip-address*>:443/central	https:// <*ip-address*>:443/central/
	https:// <*ip-address*>:443/central/	https:// <*ip-address*>:443/central/
	https:// <*ip-address*>:443/central/dra	HTTP ERROR 404 (As the installed system is not DRA)

The hostname is displayed in the login dialog box and system banner to differentiate between open windows while performing any operation of the CPS system. It indicates which system is being modified and prevents any errors or misconfigurations.

The hostname is displayed when the parameter `-Dhostname=lab` is configured in pb/qns.conf files. If it is not configured in the qns.conf file, it is displayed as a result of the command "hostname" on the server.

The hostname is displayed in the login panel only when the following argument is set to true:

```
-DshowSitenameLogin
```

Manage Users

Perform the following steps to add a new user:

1. Enter CONFIG mode as shown:

```
scheduler# config
Entering configuration mode terminal
scheduler(config)#
```

2. Use the **aaa authentication** command to create the user:

```
scheduler(config)# aaa authentication users user test2 gid 100 uid 9000 homedir / password
 testpassword ssh_keydir /
scheduler(config-user-test2)# commit
scheduler(config-user-test2)# exit
```

Note The **gid**, **uid**, **homedir** and **ssh_keydir** are required but not used by the application.

Add User To A Viewer Operational Group

In CONFIG mode, add the user to the “oper” group and commit the change as shown:

```
scheduler(config)# nacm groups group oper user-name test2
scheduler(config-group-oper)# commit
```

Add User To An Editor Group

In CONFIG mode, add the user to the “editor” group and commit the change as shown:

```
scheduler(config)# nacm groups group editor user-name test2
scheduler(config-group-editor)# commit
```

Add User To An Admin Group

In config mode, add the user to the “admin” group and commit the change as shown:

```
scheduler(config)# nacm groups group admin user-name test2
scheduler(config-group-admin)# commit
```

Note To provide a user with Admin CRUD access to CPS DRA Central, add the user to the “policy-admin” group.

Change A User's Password

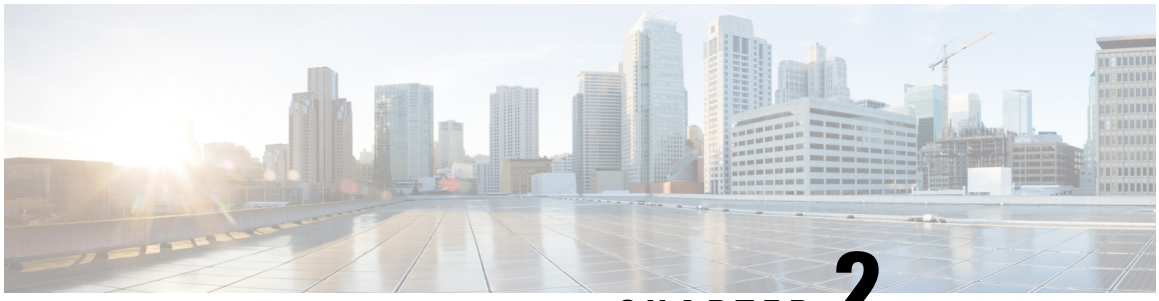
In the Management CLI, use the **aaa authentication users** user **change-password** command as shown:

```
scheduler# aaa authentication users user test2 change-password
Value for 'old-password' (<string>): ************
Value for 'new-password' (<string>): ********
Value for 'confirm-password' (<string>): ********
scheduler#
System message at 2017-03-08 21:17:18...
Commit performed by system via system using system.
```

Supported Browsers

CPS DRA supports the most recent versions of the following browsers:

- Apple Safari
- Google Chrome
- Microsoft IE
- Mozilla Firefox



CHAPTER 2

Configuring CPS DRA

- Policy Builder Overview, on page 7
- System Configuration, on page 7
- Custom Reference Data Configuration, on page 12
- Diameter Configuration, on page 17
- Diameter Routing, on page 21
- CPS Service Configuration, on page 21
- View Versioned Custom Reference Data Tables , on page 22
- View Graphical Illustration of CRD Tables, on page 22
- View Repository Details, on page 23
- Publish Configuration Changes, on page 26
- View Notifications, on page 27

Policy Builder Overview

CPS DRA allows service providers to create policies that are customized to their particular business requirements through the Policy Builder interface which is a web-based application with a graphical user interface (GUI) that enables rapid development of innovative new services.

Policy Builder page supports both configuration of the overall CPS cluster of virtual machines (VMs) as well as the configuration of services and advanced policy rules.

System Configuration

You need to define a system as it represents the customer deployment. Each system contains one or more clusters that represent a single high availability site environment. A cluster is used to define configurations related to the blades and shares the same set of policy directors.

In Policy Builder, the Environment specific data section displays a list of system configurations that enables you to perform create, read, update, and delete (CRUD) operations and to create clusters which can further overwrite and customize system configurations.

Configure System

Perform the following steps to configure a system:

Step 1 In CPS DRA, navigate to **Policy Builder**.

Step 2 Select **Systems** under **Reference Data**.

Step 3 Enter the values in each field as described in the following table:

Table 2: Configure System Parameters

Field	Description
Name	Name of the CPS system.
Description	Description of the entire system.
Session Expiration (hours)	If no messages are received in x hours, the session is removed. Default value is 8.
Session Expiration (minutes)	If no messages are received in x minutes, the session is removed. Default value is 0.
Timeout For Unknown Session	Time in minutes that CPS takes to keep a session alive after the subscriber logs off. The other network entities involved in the session close the session. Default value is 0.
Timeout For Soft Delete	Time in seconds in which a soft delete session is maintained for a CPS session after the session ends. Default value is 30.
Enable Multi Primary Key	Select this check box to allow two primary keys to be utilized by maintaining a map of each separate primary key and storing the true multi-primary key as a UUID related to the two maps. Changing this setting has a negative performance impact. Keep the Enable Multi Primary Key unchecked. Default is unchecked.

Step 4 Click **Save**.

Add Clusters

After system configuration, you can add clusters.

Step 1 To add clusters, click **Add Clusters**.

Step 2 Enter the values in each field as described in the following table:

Table 3: Cluster Parameters

Field	Description
Name	Name of the cluster.
Description	Brief description of the cluster.
DB Write Concern	Determines the write behavior of sessionMgr and for the error exceptions raised. Default option is OneInstanceSafe.
Failover SLA (ms)	Used to enter the duration (in milliseconds) to wait before starting failover database handling.
Replication Wait Time (ms)	Specifies a time limit, in milliseconds. This parameter is applicable only if you select TwoInstanceSafe in Db Write Concern. Causes write operations to return with an error after the specified limit, even if the required write concern eventually succeeds. When these write operations return, MongoDB does not undo successful data modifications performed before the write concern exceeds the replication wait time limit. The time is in milliseconds.
Trace Database Size (MB)	Determines the size in MegaBytes of the policy_trace database capped collection. Default value is 512.
Min Key Cache Time (minutes)	The minimum amount of time in minutes to keep a secondary key for a session. Default value is 2000.
Max Timer TPS	Default value is 2000.
Re-evaluation diffusion buckets	The number of batches or buckets into which CPS will divide the transactions to be processed when the rate limiting TPS function of CPS is triggered. The rate limiting feature is defined in the Max Timer TPS field. Default is 50 buckets.

Field	Description
Re-evaluation diffusion interval (ms)	Defines the delay before processing the next bucket. Enter the sum of all the delays between all the buckets. Assuming 50 re-evaluation buckets are configured (by default), the default interval of 20000 milliseconds will introduce a delay of 408 milliseconds before proceeding with the next bucket of transactions. bucket_size-1 / interval = delay between buckets 50-1 / 20000 = 408 Default is 20000 milliseconds
Broadcast Message Wait Timer (ms)	The amount of time in milliseconds for the Policy Engine to wait between sending each Broadcast Policy Message. Default value is 50.
Max Sessions Per Shard	This is the maximum number of shard per session.
Disable Secondary Key Full Scan DB	Enable or disable full scan for secondary key database lookups. By default, the secondary key database lookups is enabled. Disabling secondary key database lookups helps in reducing PCRF processing latencies.
Lookaside Key Prefixes	Added to improve Gx/Rx lookup and caching performance.
Key Prefix	To improve Gx/Rx lookup and caching performance, you can add the lookaside key prefixes. For more information, see *Cisco Policy Suite Mobile Configuration Guide*.
Admin Database	
Shard Configuration	
Primary IP Address	The IP address of the Session Manager database that holds session information for Cisco Policy Builder and Cisco Policy Server.
Secondary IP Address	The IP address of the database that provides fail over support for the primary database. This is the mirror of the database specified in the Primary IP Address field. Use this only for replication or replica pair's architecture. This field is present but deprecated to maintain downward compatibility.
Port	Port number of the database for Session data. By default, the value is 27717.

Field	Description
End Point Configurations	
Shard Configuration	
Primary IP Address	The IP address of the Session Manager database that holds session information for Cisco Policy Builder and Cisco Policy Server.
Secondary IP Address	The IP address of the database that provides fail over support for the primary database. This is the mirror of the database specified in the Primary IP Address field. Use this only for replication or replica pair's architecture. This field is present but deprecated to maintain downward compatibility.
Port	Port number of the database for Session data. By default, the value is 27717.
Backup DB Monitor Interval In Sec	Used in thread which updates the primary balance DB (when primary balanceDB is available after fail over) with BackupBalance db records. Default value is 3 sec.
Rate Limit	Used to control the TPS (with how much TPS reconciliation should take place once primary balance db is up).
Trace Database Configurations	
Shard Configuration	
Primary IP Address	The IP address of the sessionmgr node that holds trace information which allows for debugging of specific sessions and subscribers based on unique primary keys.
Secondary IP Address	The IP address of the database that provides fail over support for the primary database. This is the mirror of the database specified in the Primary IP Address field. Use this only for replication or replica pair's architecture. This field is present but deprecated to maintain downward compatibility.
Port	Port number of the database for Session data. By default, the value is 27717.
Backup DB Monitor Interval In Sec	Used in thread which updates the primary balance DB (when primary balanceDB is available after fail over) with BackupBalance db records. Default value is 3 sec.

Field	Description
Rate Limit	Used to control the TPS (with how much TPS reconciliation should take place once primary balance db is up).
Data Center Parameter	Deprecated
Common Time Changes	Deprecated

Step 3 Click **Save**.

For field descriptions of system configuration templates, refer to *Plug-in Configuration* in *CPS vDRA Configuration Guide*.

Custom Reference Data Configuration

Custom Reference Data Schemas enables you to define custom derived data for installation, to make decisions based on that data and includes the following options:

- Search Table Groups - Enables logical grouping of multiple customer reference data tables.
- Custom Reference Data Tables - Basic tables without search functionality.

Create Search Table Group

Perform the following steps to create a search table group:

Step 1 To create a search table group, click **Search Table Group**.

Step 2 Enter the values in each field as described in the following table:

Table 4: Search Table Group Parameters

Field	Description
Name	Name of the search table group that is stored in the database. The name can contain alphanumeric characters but must start with alphabets, can be either lowercase or uppercase, but not mixed cases. Special characters are not allowed except underscore. Use underscore character "_" to separate words. Examples: logical_apn, no_spaces, logical_apn2 Non-examples: logicalAPN, 2logicalAPN Additionally, a name must have a prefix. The prefix can be any alphanumeric string that starts with an alphabet. It can be the name of project, customer, etc. The prefix is mandatory for vDRA where some CRD table are included by default in the ISO file. To avoid any duplicate names, a prefix is required. Example: fn_logical_apn where fn is a prefix
Evaluation Order	Order in which groups are evaluated. Evaluation order value is in ascending order starting with 0. **Note** Search table groups and their respective CRD tables are listed based on the evaluation order value. If the evaluation order value is the same for two or more tables, then they are listed alphabetically.
Result Columns	These are the AVPs that will be added into processing. These need to be mapped to be the same as values from underlying tables. This allows populating the same AVPs from different tables.
Name	Name of the AVP. It should start with alphanumeric characters, should be lowercase, and should not start with numbers, no special characters are allowed, use "_" to separate words. For example, logical_apn = GOOD, logicalAPN = BAD, no_spaces
Display Name	More human readable name of the AVP.
Use In Conditions	Represents the availability of the row for conditions in Policies or Use Case Templates. There is a performance cost to having these checked, so it is recommended to uncheck unless they are required.
Default Value	The default value if no results are found from a Customer Reference Data Table.

Field	Description
Table Search Initiators	This section controls whether or not the Search Table Group and all tables below will be executed.
Name	Name of the table search initiators.

Step 3 Click **Save**.

Create Custom Reference Data Tables

Perform the following steps to create custom reference data tables:

Step 1 To create custom reference data tables, click **Custom Reference Data Tables**.

Step 2 Enter the values in each field as described in the following table:

Table 5: Custom Reference Data Table Parameters

Field	Description
Name	Name of the table that is stored in the database. The name can contain alphanumeric characters but must start with alphabets, can be either lowercase or uppercase, but not mixed cases. Special characters are not allowed except underscore. Use underscore character "_" to separate words. Examples: logical_apn, no_spaces, logical_apn2 Non-examples: logicalAPN, 2logicalAPN Additionally, a name must have a prefix. The prefix can be any alphanumeric string that starts with an alphabet. It can be the name of project, customer, etc. The prefix is mandatory for vDRA where CRD tables are included by default in the ISO file. To avoid any duplicate names, a prefix is required. Example: fn_logical_apn where fn is a prefix
Display Name	Name of the table that will be displayed in Control Center.
Cache Results	Indicates if the tables should be cached in memory and should be checked for production.
Activation Condition	Custom Reference Data Trigger that needs to be true before evaluating this table. It can be used to create multiple tables with the same data depending on conditions or to improve performance if tables do not need to be evaluated based on an initial conditions.

Field	Description
Svn Crd Data	When enabled, indicates that the CRD table is an SVN CRD table and CRD data for the table is fetched from CRD CSV file present in SVN data source. When disabled, indicates that the CRD table data needs to be fetched from Mongo database.
Columns	
Name	asdf;lkj Name of the column in the database. It should be unique else an error will be thrown.
Display Name	More readable display name.
Use In Conditions	Represents the availability of the row for conditions in Policies or Use Case Templates. There is a performance cost to having these checked, so it is recommended to uncheck unless they are required.
Type	Determines the values in the control center as described below: • Text: Value can be any character. For example, example123!. • Number: Value should be a whole number. For example, 1234. • Decimal: Value can be any number. For example, 1.234. • True/False: Value can be true or false. For example, true. • Data: Value should be a date without time component. For example, May 17th 2020. • DateTime: Value should be a date and time. For example, May 17th, 2020 5:00pm.
Key	Indicates that this column is all or part of the key for the table that makes this row unique. By default, a key is required. Keys also are allowed set the Runtime Binding fields to populate this data from the current message/session. Typically, keys are bound to data from the current session (APN, RAT Type) and other values are derived from them. Keys can also be set to a value derived from another customer reference data table.
Required	Indicates whether this field will be marked required in Control Center. A key is always required.

Field	Description
Column Details	
Valid	
All	All values are allowed in control center.
List of Valid	A list of name/display name pairs that will be used to create the list. Valid values can also contain a name which will be the actual value of the column and a display value which allows Control Center to display an easier to use name.
Name	The name of the column in the database.
Display Name	Readable display name.
Validation	Validation used by Control Center
Regular Expression	The Java regular expression that will be run on the proposed new cell value to validate it.
Regular Expression Description	A message to the user indicating what the regular expression is trying to check.
Runtime	Which row match when a message is received.
None	-
Bind to Subscriber AVP	This pulls the value from an AVP on the subscriber. It will also pull values from a session AVP or a Policy Derived AVP.
Bind to Session/Policy State	This pulls the value from a Policy State Data Retriever which knows how to retrieve a single value for a session.
Bind to a result column from another table	This allows the key to be filled out from a columns value from another table. This allows 'normalizing' the table structure and not having on giant table with a lot of duplicated values.
Bind to Diameter request AVP code	This allows the key be filled out from an AVP on the diameter request.

Field	Description
Matching Operator	This allows the row to be 'matched' in other ways than having the value be 'equals'. Default value is equals. • eq: Equal • ne: Not Equal • gt: Greater than • gte: Greater than or equal • lt: Less than • lte: Less than or equal

Step 3 Click **Save**.

Diameter Configuration

CPS DRA supports the following Diameter Applications:

- Gx Application
- Gy Application
- Rx Application
- Sd Application

For more information about Diameter configuration, see the *CPS vDRA Configuration Guide*.

Add Gx Application

Perform the following steps to add Gx application:

Step 1 In CPS DRA, navigate to **Policy Builder**.

Step 2 Click **Diameter Applications**.

Step 3 To add a Gx application, click **Gx Application**.

Step 4 Enter the values in each field as described in the following table:

Table 6: Gx Application Parameters

Field	Description
Name	Name of the Gx application.
Application Id	16777238, 3GPP specified Application Identifier for Gx interface.

Field	Description
Vendor Ids	Vendor Identifiers that are required to be supported on Gx interface.
Tgpp Application	When selected it indicates this is a 3GPP defined application interface.
Application Route	
Name	Identifier of the route.
Priority	Indicates the priority of the route.
Command Code	Indicates value of command code AVP within the message.
Request Type	Indicates if the Credit Control Request type is Initial (1)/Update (2) or Terminate (3).
Destination Host	When selected it indicates the message will contain a Destination-Host.
Action Tables	Identifies the request routing table for this interface and message.

Step 5 Click **Save**.

Add Gy Application

Perform the following steps to add Gy application:

Step 1 In CPS DRA, navigate to **Policy Builder**.

Step 2 Click **Diameter Applications**.

Step 3 To add a Gy application, click **Gy Application**.

Step 4 Enter the values in each field as described in the following table:

Table 7: Gy Application Parameters

Field	Description
Name	Name of the Gy application.
Application Id	4, 3GPP specified Application Identifier for Gy interface.
Vendor Ids	Vendor Identifiers that are required to be supported on Gy interface.
Tgpp Application	When selected it indicates this is a 3GPP defined application interface.

Field	Description
Application Route	
Name	Identifier of the route.
Priority	Indicates the priority of the route.
Command Code	Indicates value of command code AVP within the message.
Request Type	Indicates if the Credit Control Request type is Initial (1)/Update (2) or Terminate (3).
Destination Host	When selected it indicates the message will contain a Destination-Host.
Action Tables	Identifies the request routing table for this interface and message.

Step 5 Click **Save**.

Add Rx Application

Perform the following steps to add Rx application:

Step 1 In CPS DRA, navigate to **Policy Builder**.

Step 2 Click **Diameter Applications**.

Step 3 To add a Rx application, click **Rx Application**.

Step 4 Enter the values in each field as described in the following table:

Table 8: Rx Application Parameters

Field	Description
Name	Name of the Gy application.
Application Id	16777236, 3GPP specified Application Identifier for Rx interface.
Vendor Ids	Vendor Identifiers that are required to be supported on Gy interface.
Tgpp Application	When selected it indicates this is a 3GPP defined application interface.
Application Route	
Name	Identifier of the route.
Priority	Indicates the priority of the route.

Field	Description
Command Code	Indicates value of command code AVP within the message.
Request Type	Indicates if the Credit Control Request type is Initial (1)/Update (2) or Terminate (3).
Destination Host	When selected it indicates the message will contain a Destination-Host.
Action Tables	Identifies the request routing table for this interface and message.

Step 5 Click **Save**.

Add Sd Application

Perform the following steps to add Sd application:

Step 1 In CPS DRA, navigate to **Policy Builder**.

Step 2 Click **Diameter Applications**.

Step 3 To add a Sd application, click **Sd Application**.

Step 4 Enter the values in each field as described in the following table:

Table 9: Sd Application Parameters

Field	Description
Name	Name of the Gy application.
Application Id	16777303, 3GPP specified Application Identifier for Sd interface.
Vendor Ids	Vendor Identifiers that are required to be supported on Gy interface.
Tgpp Application	When selected it indicates this is a 3GPP defined application interface.
Application Route	
Name	Identifier of the route.
Priority	Indicates the priority of the route.
Command Code	Indicates value of command code AVP within the message.
Request Type	Indicates if the Credit Control Request type is Initial (1)/Update (2) or Terminate (3).

Field	Description
Destination Host	When selected it indicates the message will contain a Destination-Host.
Action Tables	Identifies the request routing table for this interface and message.

Step 5 Click **Save**.

Diameter Routing

Diameter request message routing is done via realms and applications. A Diameter message that is forwarded by Diameter agents (proxies, redirects or relays) must include the target realm in the Destination-Realm AVP and one of the application identification AVPs (Auth-Application-Id/Acct-Application-Id/Vendor-Specific-Application-Id). The realm can be retrieved from the User-Name AVP, which is in the form of a Network Access Identifier (NAI). The realm portion of the NAI is inserted in the Destination-Realm AVP. Diameter agents have a list of locally supported realms and applications, and can have a list of externally supported realms and applications.

Routing AVP definitions links the different Application Routing tables to required CRD tables and supports the following applications:

- Gx Application
- Rx Application
- Sd Application

The following parameters can be configured under Routing AVP Definitions:

Table 10: Routing AVP Definition Parameters

Parameter	Description
Name	Name of the application.
Routing Avp Lookup	List of search table groups to perform routing AVP lookup. The AVPs from incoming messages will be looked up to match the rows of the CRD tables referenced by the search table groups listed here. For more information, see *CPS vDRA Configuration Guide*.

CPS Service Configuration

The Import/Export option enables you to perform the following operations:

- Export CPS Service Configuration into a single file.

- Import CPS Service Configuration to another environment.

For more information, see *Export and Import Service Configurations* in *CPS Operations Guide*.

View Versioned Custom Reference Data Tables

You can view the SVN CRD data of a specific versioned CRD table under the **Versioned Custom Reference Data** option. The versioned CRD tables represents a combined list of custom reference data tables present under Custom Reference Data tables and different Search Table Groups whose **Svn Crd Data** checkbox is enabled.

View Details of Versioned CRD Tables

Perform the following steps to view the CRD data of a versioned CRD table:

Step 1 Navigate to **Versioned Custom Reference Data** under **Policy Builder**.

Step 2 To view details, select a versioned CRD table listed.

The versioned CRD table details is displayed.

Import Data of Versioned CRD Tables

Perform the following steps to import CRD data of a versioned CRD table:

Step 1 Navigate to **Versioned Custom Reference Data** under **Policy Builder**.

Step 2 Click **Import** option provided against the CRD table whose data you want to import.

The **File to Import** dialog box is displayed from where you can select a CSV file containing CRD data to be imported.

Step 3 Select a file.

Step 4 After the file is loaded, select **Import**.

File imported success message is displayed.

View Graphical Illustration of CRD Tables

Experimental CRD visualization option enables users to view Search Table Group relationships graphically. The nodes displayed are Search Table Groups and the links show where column data for a search table group is pulled from another table with the "Bind to a result column from another table" setting.

You can select an STG element, view its details in the Selected Info dialog box and save the layout.

STG displays the following information:

- Layout nodes.
- Switched display of STG elements to list STG result columns instead of CRD Columns.
- Indicates columns in CRD tables under STG displaying ‘keys’ (key symbol) or ‘required’ (*).
- Indicates where columns get their values from such as subscriber AVP, other CRD column, and session data field.

View Details of STG Element

Perform the following steps to view details of the STG element:

Step 1 In CPS DRA, navigate to **Policy Builder**.

Step 2 Select **Experimental CRD visualization** under **Policy Builder**.

Step 3 To view details, select an STG element.

The following details are displayed:

Table 11: STG Element Details

Field	Description
STG Name	Name of the search table group.
STG Columns	Search table group columns.
Child Custom Reference Data Tables	Child custom reference data tables.

View Repository Details

Policy Builder displays an option that enables you can view a list of repositories as follows:

- Select **Repository** to navigate repositories list page, to view repository details and to reload configurations of the selected repository
- Select the dropdown to view the available repositories.

To switch to a new repository by selecting a repository from the dropdown list, user will have to re-login to authenticate the user with the selected repository.

The following table describes the repository details:

Table 12: Repository Details

Field	Description
Name	Name of the repository.

Field	Description
URL	URL of the branch of the version control software server that are used to check in this version of the data.
SVN Username	Username that is configured to view Policy Builder data.
Temp Directory	Temporary working local directory for the policy configurations.
Reload Repository	Select to reload the repository from the file system. **Note** Reload link is available only when the repository matches the selected (working) repository.

Add New Repository

Perform the following steps to add a new repository:

Step 1 In CPS DRA, navigate to **Policy Builder Overview**.

A **Choose Policy Builder Data Repository** dialog box is displayed.

Step 2 Click **Add Repository** link.

An **Add Repository** dialog box is displayed with the following fields/URL:

Fields	Description
Name	Name of the repository.
URL	URL of the branch of the version control software server that is used to check in this version of the data.
Local Directory	Local directory for the policy configurations. The standard path for Local Directory is /var/broadhop/pb/workspace/tmp-repository_name.

Step 3 Enter valid values.

Note If the mandatory fields are not entered, an error message is displayed.

Step 4 Click **OK**.

a. After entering values in the repository fields, the progress bar should display and hide when the response from API is returned.

b. If there is an error response from the API, it should be displayed in the error modal. On closing the error modal the add repository modal with the old values is displayed.

Select Repository

When you select Policy Builder option in the CPS DRA interface, a **Choose Policy Builder Data Repository** dialog box is displayed which enables you to select a repository.

Note The dialog box to select a repository is displayed only if you have not loaded any repository earlier. In case any error occurs while loading the available repositories, an error dialog is displayed. When you click **Close**, the DRA landing page is displayed.

Perform the following steps to select a repository:

Step 1 In CPS DRA, navigate to **Policy Builder Overview**.

A **Choose Policy Builder Data Repository** dialog box is displayed.

Step 2 Click the **Select Repository** drop-down.

Step 3 Select a repository from the drop-down list.

Step 4 Click **Done**.

The selected repository is loaded.

Note If you click **Cancel**, the application is redirected to the DRA landing page as there is no repository loaded.

Switch Repository

Perform the following steps to switch repositories:

Step 1 In CPS DRA, navigate to **Policy Builder Overview**.

Step 2 Select the **Switch Repository** icon.

A **Choose Policy Builder Data Repository** dialog box is displayed.

Note The repository which is currently loaded is displayed as selected in the repository drop-down.

Step 3 Click the **Select Repository** drop-down.

Step 4 Select a repository from the drop-down list.

Step 5 Click **Done**.

The selected repository is loaded.

Note You are notified with appropriate error messages during switching repositories in the following scenarios:

- Failure from API end.
- When SVN is down.
- When the request gets timed out.

Publish Configuration Changes

To put changes into effect and have the Cisco Policy Builder server recognize the configuration changes made in your client session, use the Publish option and save the changes to the server repository.

Publish enables you to publish or revert all the changes made in the Policy Builder.

For more information on Publishing operations, see *CPS Mobile Configuration Guide*.

Publish Changes

Perform the following steps to publish changes:

Step 1 In CPS DRA, navigate to **Policy Builder**.

Step 2 Select **Publish**.

Step 3 Enter a commit comment.

Step 4 Review the changes displayed under **Changes to commit**.

Step 5 Click the **Publish To** drop down and select the Publish Repository.

Note The Publish to drop down points to CPS server SVN configurations repository where CPS server polls for SVN changes. After receiving the notification, CPS server will check out the latest configurations from SVN.

Step 6 Select **Commit and Publish**.

Publish successful message is displayed.

Revert Changes

Perform the following steps to revert changes:

Step 1 In CPS DRA, navigate to **Policy Builder**.

Step 2 Select **Publish**.

Step 3 Review the changes displayed under **Changes to commit**.

Step 4 Click **Revert All Changes**.

View Notifications

You can view notifications regarding various stages of all CPS products by selecting the **Alert** option provided in the toolbar.

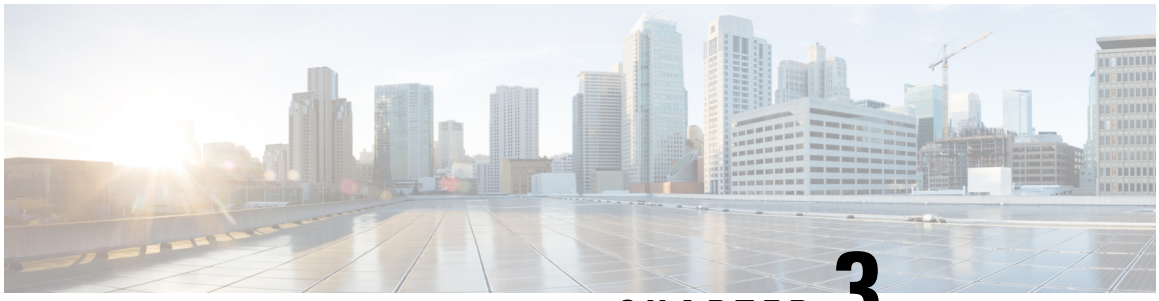
Perform the following steps to view notifications:

Step 1 Click **Alert**.

A notification message is displayed.

Step 2 Click **Accept**.

Note
- After the notification is accepted, the toolbar reverts to the default color.
- If the system upgrade deadline is approaching, the accept option is not displayed and the toolbar continues to display the alert link and notification.



CHAPTER 3

Managing Custom Reference Data

- Custom Reference Data Overview, on page 29
- Export Custom Reference Data, on page 29
- Import Custom Reference Data, on page 29
- View Custom Reference Data Tables, on page 30
- Import Custom Reference Data Table , on page 31

Custom Reference Data Overview

Custom reference data is data specific to a service provider and provides a way to create their own data tables and to populate them. It adds variations of existing use cases configured in Policy Builder.

Export Custom Reference Data

Perform the following steps to export CRD data:

Step 1 In CPS DRA, navigate to **Custom Reference Data**.

Step 2 Select **Export**.

The contents of the CRD table is generated in a csv format in a zip file.

Step 3 Click **Save File**.

Step 4 Click **OK**.

Import Custom Reference Data

Perform the following steps to import CRD tables:

Step 1 In CPS DRA, navigate to **Custom Reference Data**.

Step 2 Select **File to Import...**

The **File Upload** dialog box is displayed from where you can select a file to be imported.

Step 3 Click **Import**.

Note A warning message is displayed in the success modal for bulk import of CRD tables when the archive file to import has CRD tables with Svn Crd Data flag enabled.

View Custom Reference Data Tables

Custom Reference Data Tables section lists the custom reference data (CRD) tables in an alphabetic order along with its description.

You can select a CRD table from the displayed list and view its data. The search filter is added to support full and partial string match.

A key icon is displayed before the column name of the selected CRD tables. This provides the following information:

- Indicates whether the column in the selected CRD table is a key column or non-key column.
- Indicates the type of Runtime Binding and its value in a tooltip when you hover over it.

The following operations can be performed:

- Add a record to the table
- Edit a record of the table
- Delete a record of the table

The results are paginated for easy access and scrollbars can be used when there are more number of columns.

Note The edit, delete and add options are disabled for CRD tables with Svn Crd Data flag enabled.

View Multiple CRD Tables

Step 1 Navigate to **Custom Reference Data**.

Step 2 In the left-hand pane, select CRD tables listed under **Display Name**.

The tables are displayed on the right-hand side. You can drag and resize the tables horizontally.

Step 3 Click **Close**.

Note
- By default the **Custom Reference Data Tables** tab is expanded. Only one of the panels can be expanded at a time. For example, when the **Import/Export CRD data** tab is expanded, the **Custom Reference Data Tables** tab is closed and vice versa.
- You can use the scroll bar to view records in a large CRD table.
- You can use the **Add Row** option to enter records.
- You can use the **Close** option to close a CRD table.
- You can click **Close All** option to close multiple tables.

Edit Multiple CRD Tables

Step 1 Navigate to **Custom Reference Data**.

Step 2 In the left-hand pane, select CRD tables listed under **Display Name**.

The tables are displayed on the right-hand side.

a. To modify record values, click edit icon. A CRD record modal popup is displayed.

b. To enter record values, click **Add Row**.

c. To delete records, click delete icon.

Step 3 Click **Done**.

Step 4 Click **Close**.

Note
- You can edit only one CRD table at a time.
- The SVN CRD tables have only read only option.
- You can click **Close All** option to close multiple tables.

Import Custom Reference Data Table

Perform the following steps to import a custom reference data table:

Step 1 In CPS DRA, navigate to **Custom Reference Data**.

Step 2 Select any CRD table.

Step 3 Click the **Import** option provided against the selected CRD table.

The **File to Import** dialog box is displayed from where you can select a file to be imported.

Note The import link is disabled for CRD tables with Svn Crd Data flag enabled.

Step 4 Select a file.

Step 5 After the file is loaded, Click **Import**.

Note

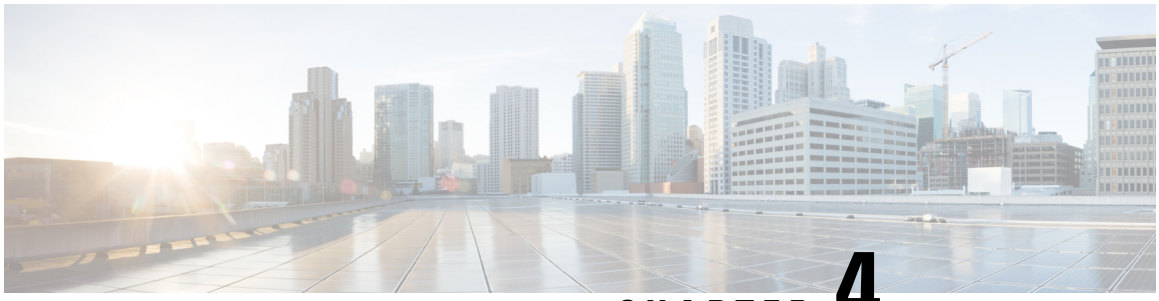
a. The selected file should be of XLS or CSV format.

b. The name of the selected file should match that of the CRD table name.

c. If you try to import data with wrong headers, "Mismatch found between imported csv headers and policy builder table columns" error message is displayed.

d. If you try to import data having duplicate records, "Duplicate rows found in the imported data for table: (table_name). Duplicate records count: (duplicate_count)? error message is displayed.

Data Imported success message is displayed.



CHAPTER 4

Managing DRA Operations

- Operations Overview, on page 33
- Monitoring DRA, on page 33
- Monitoring Installation Using Grafana, on page 47
- Viewing CPS APIs, on page 48

Operations Overview

The Operation page enables you to access various interfaces and perform operations, maintenance, and troubleshooting activities. It assists system administrators and network engineers to operate and monitor the Policy Server.

Monitoring DRA

DRA monitoring page under operations includes the following options:

- DRA Peer Monitoring
- DRA Binding Monitoring
- DRA SLF Bindings
- DRA Relay Connection
- Grafana

Peer Monitoring

DRA peer monitoring page displays the active peer endpoints (by default) for the cluster node. You can click the toggle for active/inactive peers to view the active or inactive peer endpoints.

The active and inactive peer monitoring screens have resize option for each column. You can use the scrollbar to view multiple values.

When the page is loaded, the Autorefresh checkbox is enabled by default which refreshes peers data every 30 seconds. You can stop this functionality by disabling the checkbox. After every refresh, the Data Last Refreshed field is updated with the locale time.

You can use the filter option to filter active and inactive peer endpoints. You can also view all event logs and peer details for specific active or inactive peer endpoints of the cluster node.

Pagination support is provided in active and inactive peer endpoints table data. A number of rows per page drop-down are displayed below each table which contains the different set of numbers indicating the number of rows which can be shown per page. This option enables you to perform the following tasks:

- Select the number of rows to be displayed in each page.
- Specify the page to which you want to navigate.

You can use the **Close All** option to close all the displayed popups. By default the **Close All** option is disabled. If you have many popups open, the **Close All** option gets enabled.

View Filtered Data

Step 1 In CPS DRA, navigate to **DRA Peer Monitoring**.

Step 2 Select the **Filter by** drop-down and click on any one of the following data options displayed:

- Peer Host Name
- Peer IP Address
- Admin State
- DRA Host Name
- DRA IP Address
- Application Id
- Peer Group
- Details/Event Logs
- Actions

Step 3 Enter a value in the **Filter Peer Endpoints** option.

Step 4 Click **Toggle for Active Peers** to view filtered active peer endpoints or **Toggle for Inactive Peers** to view filtered inactive peer endpoints.

Under Active Peer Endpoints:

- You can administratively disable or disconnect selected peers.
- You can multi-select peer connections and administratively disable them. You will be prompted for confirmation before executing the action.

Note In Active Peer Endpoints GUI, after admin disable of active peer, if peer's Admin State gets changed from Enabled to Disabled but still it is shown under Active Peer Endpoints, then peer has to be disconnected by using the disconnect action.

Figure 2: Active Peer Endpoints

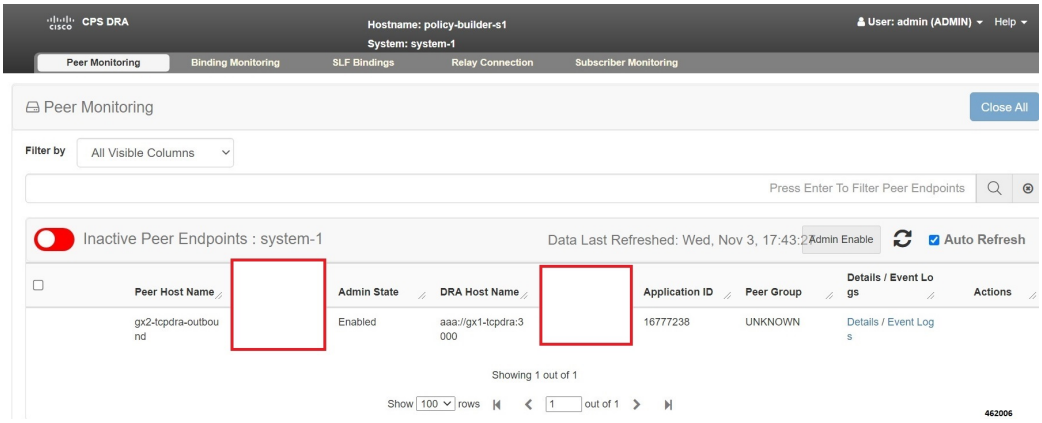
Under Inactive Peer Endpoints:

- You can enable peers which are administratively disabled. This option is enabled only for peers which are administratively disabled.
- Table always lists admin disabled peers as inactive endpoints even if there are no recent active connections from those peers.
- You can multi-select admin disabled peers and enable them. You will be prompted for confirmation before executing the action.

  Note You can administratively disable maximum 20 peer connections in a single operation using multi-selection. If more than 20 peer connections are selected, an error is prompted with an option to proceed with disabling the first 20 of selected connections.

- By default, peer connection details for inactive endpoints is retained in the system for 48 hours. If a peer is administratively disabled for more than 48 hours, then last connection details (Peer IP address, DRA endpoint, Event Logs and so on) is not displayed.

Figure 3: Inactive Peer Endpoints



The following tables describe the details displayed under Peer Endpoints section:

Table 13: Active Peer Endpoint Details

Parameter	Description
Peer Host Name	Peer host name.
Peer IP Address	Peer IP address
Admin State	Indicate the admin state of the peer. You can filter the inactive peers by admin state.
DRA Host Name	DRA host name and port.
DRA IP Address	DRA IP address
Application Id	Identifier of the Diameter application (Gx, Rx, Sy, Sh and so on).
Peer Group	Peer group of the connected peer.
Details/Event Logs	When selected provides Details and Event Logs links. To view details of a particular peer, click **Details**. To view event logs of a particular peer, click **Event Logs**.
Actions	Options are Disconnect and Disable. Disconnect: Disconnects an active peer by confirming from the user and sends the request to the API for disconnecting the active peer. Disable: Disables admin active peer by confirming from the user and sends the request to the API for disabling the active peer.

Table 14: Inactive Peer Endpoint Details

Parameter	Description
Peer Host Name	Peer host name.
Peer IP Address	Peer IP address
Admin State	Indicate the admin state of the peer. You can filter the inactive peers by admin state.
DRA Host Name	DRA host name and port.
DRA IP Address	DRA IP address
Application Id	Identifier of the Diameter application (Gx, Rx, Sy, Sh and so on).
Peer Group	Peer group of the connected peer.

Parameter	Description
Details/Event Logs	When selected provides Details and Event Logs links. To view details of a particular peer, click **Details**. To view event logs of a particular peer, click **Event Logs**.
Actions	Used to enable the peer which was disabled by admin earlier.

You can use the refresh option provided next to the toggle for active/inactive peer endpoints to refresh the table data.

You can enable the **Auto-refresh** checkbox to refresh data every 30 seconds. The **Data Last Refreshed** field displays time when data is fetched from server.

View Details

Step 1 In CPS DRA, navigate to **DRA Peer Monitoring**.

Step 2 Click **Toggle for Active Peers** to view active peer endpoints or **Toggle for Inactive Peers** to view inactive peer endpoints.

Step 3 To view details of a particular peer, click **Details**.

Figure 4: Peer Endpoint Details

Peering Information for Peer Key: gx24-tcpdra@gx24-tcpdra:3891@16777238@1

Data Last Refreshed: Fri, Jan 15, 10:36:25

Name	Value
Key	gx24-tcpdra@gx24-tcpdra:3891@16777238@1
Realm	gx24-tcpdra.cisco.com
Host	gx24-tcpdra
Application Ids	16777238
Peer Group	UNKNOWN
Peer Weight	100
Session Routing Key	
Direction	Inbound
Transport Protocol	TCP
Peer Status	UP
Last Connect Time	Fri Jan 15 03:26:29 UTC 2021
Own Host	aaa://gx24-tcpdra:3891
Own IP Addresses	
Own Port	3891
Peer Uri	aaa://gx24-tcpdra:55851
Remote IP Addresses	
Remote Port	55851
Instance Id	diameter-endpoint-s1.weave.local-1
Peer Message Class	0
Admin State	Enabled

The following details are displayed:

Table 15: Peer Endpoint Details

Parameter	Description
Application ID	Identifier of the Diameter application (Gx, Rx, Sy, Sh and so on).
Peer Group	Peer group of the connected peer.
Session Routing Key	Identifier to select peer for routing.
Realm	Realm of the connected peer.
Last Connect Time	Last connection time.
Own Host	Own host name and port of CPS vDRA.
Peer Status	Peer connection status (up/down).
Direction	Inbound/Outbound.
Key	Internal key/identifier assigned by CPS vDRA.
Host	Host name of the connected peer.

If the **Auto-refresh** checkbox is enabled, the **Data Last Refreshed** field is displayed at the top of the Details dialog box of the selected peer.

When you select **Details** modal, the **Data Last refreshed** field displays the time at which peers data was last refreshed. If the a**Auto-refresh** is performed when modal is opened, **Data Last refreshed** time in the modal is not updated and you have to re-open the modal to view the updated data.

View Event Logs

Step 1 In CPS DRA, navigate to **DRA Peer Monitoring**.

Step 2 Click **Toggle for Active Peers** to view active peer endpoints or **Toggle for Inactive Peers** to view inactive peer endpoints.

Step 3 To view event logs of a particular peer, click **Event Logs**.

The **Peer Status Logs** is displayed.

If the **Auto-refresh** checkbox is enabled, the **Data Last Refreshed** field is displayed at the top of the Event Logs dialog box of the selected peer.

When you select **Event Logs** modal, the **Data Last Refreshed** field displays the time at which modal is opened. The data is not updated when the modal is opened. You have to re-open the modal to get the updated data. Event log data is independent of auto refresh data.

Binding Monitoring

CPS vDRA stores bindings in the mongo database. 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.

You can access CPS vDRA binding information based on the following supported search keys:

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

View DRA Binding Details

Perform the following steps to view DRA binding details:

Step 1 In CPS DRA, navigate to **DRA Binding Monitoring**.

Step 2 To view CPS vDRA binding information for a supported search key, click on any one of the following options displayed in the **DRA Binding** page:

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

Step 3 Enter the required value. The search button is enabled which when clicked displays the following binding details:

Table 16: DRA Binding Details

Parameter	Description
APN	Access Point Name (Called Station ID).
Gx Session ID	Gx Session Identifier (unique) assigned by PCEF.
Session Routing Key	Identifier to select peer for routing.
Origin Host	Host name of the connected peer.

Parameter	Description
Age	Duration of session establishment. Age format is as follows: `xxxd xxh xxm xxs,` Where: • d is days • h is hours • m is minutes • s is second
Details	CPS vDRA binding details.

View Gx Session Details

Step 1 In CPS DRA, navigate to **DRA Binding Monitoring**.

Step 2 Select a supported search key and provide an input value in the search input field.

Step 3 Click **Search**.

CPS vDRA Bindings is displayed with two links for **Gx Session ID** and **Details** in each row.

Step 4 To view Gx session details, click **Gx Session ID**.

The following details are displayed in a Gx session details popup:

Table 17: Gx Session Details

Parameter	Description
Age	Duration of session establishment.
Gx Session ID	Gx Session Identifier (unique) assigned by PCEF.
IMSI	International Mobile Subscriber Identity (15 digits).
APN	Access Point Name (Called Station ID).
IPv4	IPv4 PDN address.
MSISDN	Mobile Subscriber ISDN Number (11 digits).
Origin Realm	Origin-Realm AVP from Gx CCR-I message.
Destination Realm	Destination-Realm AVP from Gx CCR-I message.
Origin Host	Origin-Host AVP from Gx CCR-I message.
Destination Host	Destination-Host AVP from Gx CCR-I message.

Parameter	Description
IPv6	IPv6 PDN address.
App Id	Identifier of the Diameter application (Gx, Rx, Sy, Sh and so on).
Session Route Key	Identifier to select peer for routing.

View Details

Step 1 In CPS DRA, navigate to **DRA Binding Monitoring**.

Step 2 Select a supported search key and provide an input value in the search input field.

Step 3 Click **Search**.

CPS vDRA Bindings is displayed with two links for **Gx Session ID** and **Details** in each row.

Step 4 To view details, click **Details**.

The following details are displayed in a details popup:

Table 18: DRA Binding Details

Parameter	Description
Age	Duration of session establishment.
Gx Session ID	Gx Session Identifier (unique) assigned by PCEF.
IMSI	International Mobile Subscriber Identity (15 digits).
APN	Access Point Name (Called Station ID).
Origin Host	Host name of the connected peer.
Session Route Key	Identifier to select peer for routing.

SLF Bindings

This section describes how to view SLF Bindings details.

View SLF Bindings Details

Perform the following steps to view SLF binding details:

In CPS DRA, navigate to **DRA SLF Monitoring**.

The **DRA SLF Monitoring** page is displayed. You can access SLF binding information based on the following supported search keys:

- Subscriber ID
- IMSI
- MSISDN

View Subscriber ID Details

Step 1 Select **Subscriber ID**.

Step 2 Enter a valid subscriber ID.

Step 3 Click **Search**.

The following details are displayed in a Subscriber Details popup:

Parameter	Description
Subscriber ID	Unique identifier to identify the subscriber.
Destination	Destination specified in the map.
SLF Destination Type	Type of SLF destination specified in the map.
SLF Destination	SLF Destination specified in the map.

Step 4 Click **Details**.

The following details are displayed in a Subscriber Details popup:

Parameter	Description
Subscriber ID	Unique identifier to identify the subscriber.
IMSI	International Mobile Subscriber Identity (15 digits).
MSISDN	Mobile Subscriber ISDN Number (11 digits).
Destination	Destination specified in the map.
SLF Destination Type	Type of SLF destination specified in the map.
SLF Destination	SLF Destination specified in the map.

View IMSI Details

Step 1 Select **IMSI**.

Step 2 Enter a valid IMSI.

Step 3 Click **Search**.

The following details are displayed in a Subscriber Details popup:

Parameter	Description
IMSI	International Mobile Subscriber Identity (15 digits).
Subscriber ID	Unique identifier to identify the subscriber.
Destination	Destination specified in the map.
SLF Destination Type	Type of SLF destination specified in the map.
SLF Destination	SLF Destination specified in the map.

Step 4 Click **Details**.

The following details are displayed in a Subscriber Details popup:

Parameter	Description
Subscriber ID	Unique identifier to identify the subscriber.
IMSI	International Mobile Subscriber Identity (15 digits).
MSISDN	Mobile Subscriber ISDN Number (11 digits).
Destination	Destination specified in the map.
SLF Destination Type	Type of SLF destination specified in the map.
SLF Destination	SLF Destination specified in the map.

View MSISDN Details

Step 1 Select **MSISDN**.

Step 2 Enter a valid MSISDN.

Step 3 Click **Search**.

The following details are displayed in a Subscriber Details popup:

Parameter	Description
MSISDN	Mobile Subscriber ISDN Number (11 digits).
Subscriber ID	Unique identifier to identify the subscriber.
Destination	Destination specified in the map.
SLF Destination Type	Type of SLF destination specified in the map.

Parameter	Description
SLF Destination	SLF Destination specified in the map.

Step 4 Click **Details**.

The following details are displayed in a Subscriber Details popup:

Parameter	Description
Subscriber ID	Unique identifier to identify the subscriber.
IMSI	International Mobile Subscriber Identity (15 digits).
MSISDN	Mobile Subscriber ISDN Number (11 digits).
Destination	Destination specified in the map.
SLF Destination Type	Type of SLF destination specified in the map.
SLF Destination	SLF Destination specified in the map.

Monitoring Relay Connections

You can monitor different relay connections to remote DRAs using the DRA Relay Connection option.

View Relay Connections

Perform the following steps to view relay connections:

Step 1 Navigate to **DRA Relay Connection**.

Step 2 Select the **Filter by** drop down and click on any one of the following data options displayed:

- All Visible Columns
- Remote System
- Peer
- Remote IP Address
- Local Host Name
- Status
- Direction
- Details/Event Logs
- All Data

Step 3 Enter a value in the **Filter Relay Connections** field.

Step 4 Click **Toggle for Active Relays** to view filtered active relay endpoints or **Toggle for Inactive Relays** to view filtered inactive relay endpoints.

The following table describes the details displayed under Relay Connections:

Table 19:

Parameter	Description
Remote System	Connected relay system.
Peer	Connected relay host name.
Remote IP Address	Connected relay IP address.
Local Host Name	DRA's own host name and port.
Local IP Address	DRA's own IP address.
Status	Relay connection status (up/down).
Direction	Inbound or outbound.
Details/Event Logs	Relay details/relay connection history log.

You can check the **Auto-refresh** checkbox to refresh data every 30 seconds. The **Data Last Refreshed** field displays time when data is fetched from server

View Relay Details

Perform the following steps to view relay details:

Step 1 Navigate to **DRA Relay Connection**.

Step 2 Click **Toggle for Active Relays** to view filtered active relay endpoints or **Toggle for Inactive Relays** to view filtered inactive relay endpoints.

Step 3 To view details of a particular relay connection, click **Details**.

The following details are displayed:

Table 20:

Parameter	Description
Key	Internal key or identifier assigned by DRA.
Last Connect Time	Last connection time.
Peer Status	Relay connection status (up/down).
Direction	Inbound or outbound.
Own Host	DRA's own host name and port

Parameter	Description
Own IP Address	DRA's own IP address.
Own Port	DRA's own port.
Peer Uri	Connected relay host name.
Remote I P Address	Connected relay host port.
Remote Port	Connected relay IP address.
Remote System Id	Connected relay system.

If the **Auto-refresh** checkbox is checked, the **Data Last Refreshed** field is displayed at the top of the Details dialog box of the selected peer.

When you select the **Details** modal, the **Data Last Refreshed** field displays the time at which data was last refreshed. If the **Auto-refresh** is performed when the modal is opened, **Data Last refreshed** time in the modal is not updated and you have to reopen the modal to view the updated data.

View Relay Event Logs

Perform the following steps to view relay event logs:

Step 1 Navigate to **DRA Relay Connection**.

Step 2 Click **Toggle for Active Relays** to view filtered active relay endpoints or **Toggle for Inactive Relays** to view filtered inactive relay endpoints.

Step 3 To view event logs of a particular relay connection, click **Event Logs**.

The **Event Logs for Relay Key** is displayed.

If the **Auto-refresh** checkbox is enabled, the **Data Last Refreshed** field is displayed at the top of the Event Logs dialog box of the selected peer.

When you select **Event Logs** modal, the **Data Last Refreshed** field displays the time at which modal is opened. The data is not updated when the modal is opened. You have to re-open the modal to get the updated data. Event log data is independent of auto refresh data.

Monitoring Installation Using Grafana

You can access the Grafana interface under DRA Monitoring to monitor installation. It is a third-party metrics dashboard and graph editor. Grafana provides a graphical or text-based representation of statistics and counters collected in the Prometheus database.

Note After the DRA Director (DD) failover/reboot, the TPS values in Grafana dashboards takes approx. 5 minutes to fetch and display the latest updated values. Until the values are updated, Grafana displays the old data.

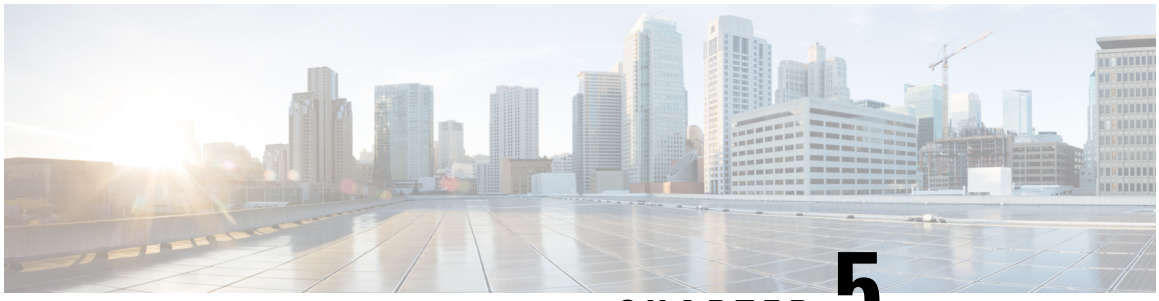
For more information about Grafana in vDRA, refer to the *Prometheus and Grafana* chapter in the *CPS vDRA Operations Guide*.

Viewing CPS APIs

API information option enables you to view API related information:

- Service Orchestration API: to manage Policy Builder data

Select the link to view the documentation and usage examples.



CHAPTER 5

DRA Distributor

Note For configurations, see *DRA Distributor Configuration* chapter in the *CPS vDRA Configuration Guide*.

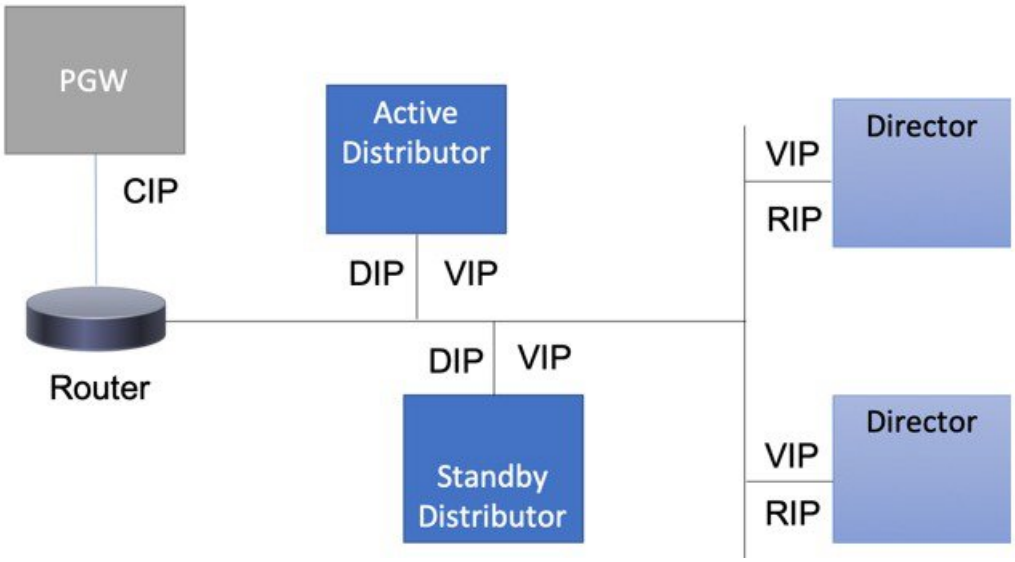
- Introduction, on page 49
- Direct Routing, on page 50
- DRA Distributor Failover, on page 52
- Health Checks, on page 53

Introduction

The DRA distributor is a load balancer that front ends the diameter connections inbound to the DRA. It then forwards the connections to a selected Director VM. For client facing traffic (for example, PGW, AF), two distributor VMs configured as an HA pair are used. In addition, two distributor VMs are used to support server facing entities (for example, PCRF).

When a new connection arrives at the Distributor, it employs the Weighted Least Connections algorithm to select a Director VM for the new connection. The return traffic is sent from the Director VM directly to the originator of the connection (PGW, PCRF, and so on) bypassing the Distributor VM. This forwarding mechanism is known as Direct Routing. A pair of Distributors synchronizes the connection information to continue with the forwarding traffic if one of the Distributor VMs fails.

Figure 5: DRA Distributor



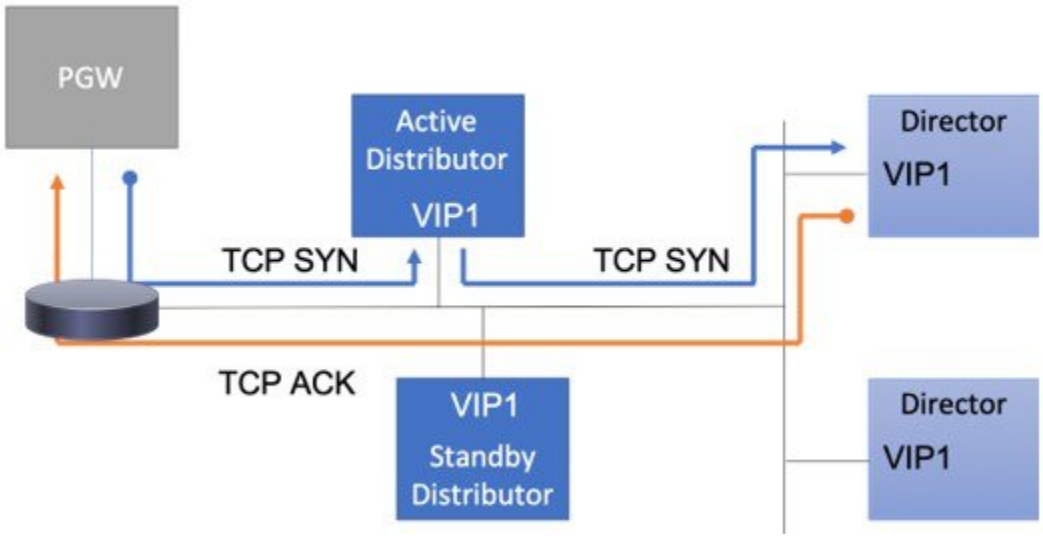
- CIP: Client IP
- DIP: Distributor IP
- VIP: Virtual IP
- RIP: Real IP

Direct Routing

The DRA Distributor VM has a Virtual IP (VIP) address and TCP port that is used by a PGW, PCRF and so on for connections that are forwarded to the DRA Director VMs. The DRA Directors have an interface with the same VIP configured as a secondary IP address. The DRA Distributor VM and DRA Director VMs must be configured on the same subnet/layer 2 network.

The DRA Distributor uses the Director VM's Real IP address (RIP) to resolve the Director's MAC address. Before forwarding packets to the Director VM, the Distributor VM replaces the source MAC address with its own, and replaces the destination MAC address with the Director VM's IP address. The source and destination IP (PGW, VIP) remain the same.

Figure 6: Direct Routing



ARP and IPv6 Neighbor Discovery

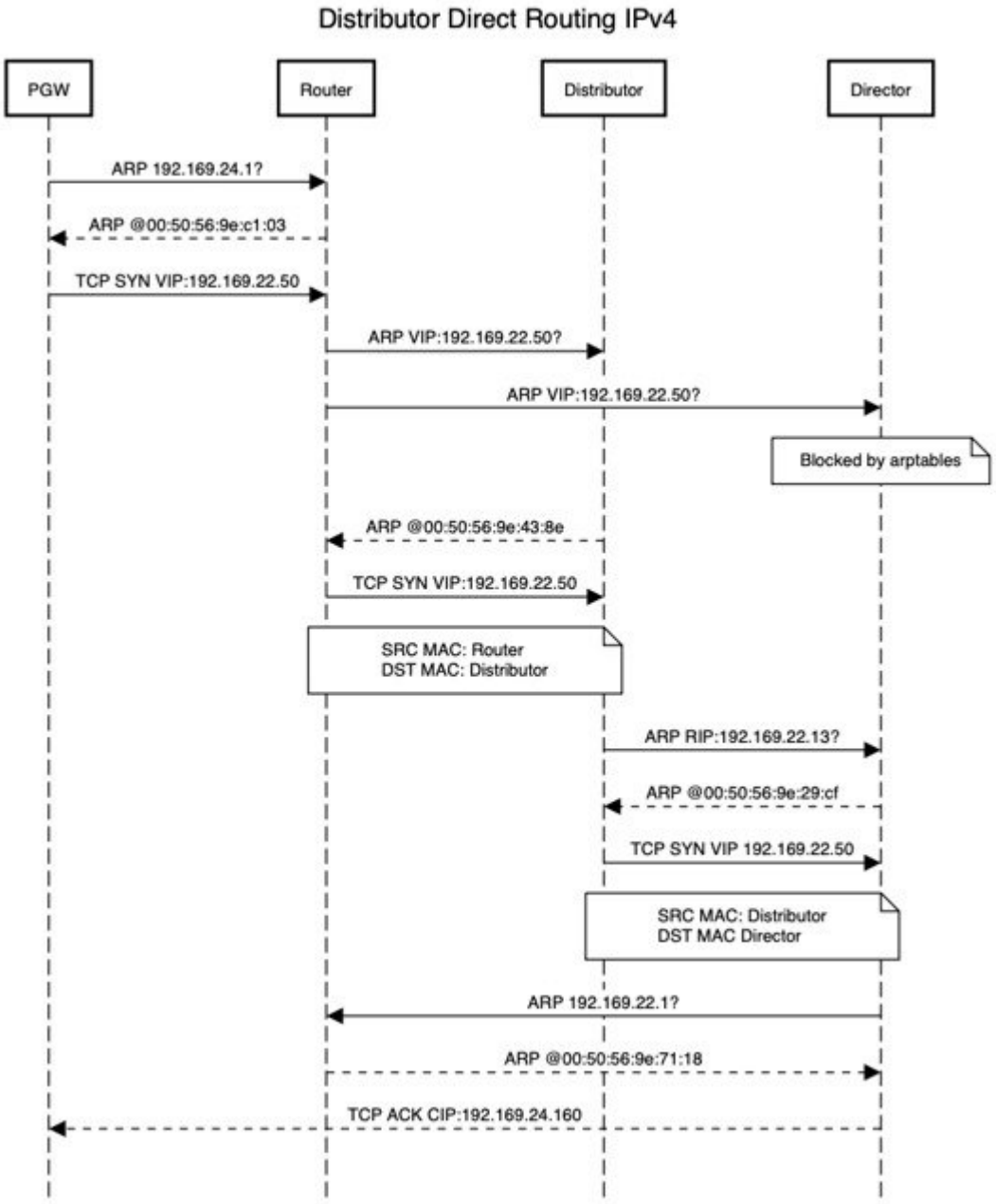
Devices responsible for forwarding PGW/PCRF and so on packets to the Active Distributor VM, such as a router, must discover the MAC address of the Distributor's interface that is configured with the VIP. Since the Distributor and Director VMs are configured with the same VIP, and the Distributor and Director VMs are on the same subnet/layer-2 network, the Director VMs must not respond to IPv4 ARP or IPv6 neighbor solicitation requests for the VIP.

In addition, the Director VMs must not send unnecessary IPv4 ARPs or IPv6 neighbor advertisements. To prevent Director VMs from advertising their MAC addresses for the VIPs, ARP tables and IPv6 tables are used to filter IPv4 ARP and IPv6 neighbor discovery respectively.

Distributor VIPs are automatically configured on the Director VMs along with the required ARP table and IPv6 table rules.

The DRA Distributor in the DRA VNF is configured using ConfD CLI on the Master VM.

Figure 7: Distributor Direct Routing



DRA Distributor Failover

If a Distributor VM fails, all VIPs on the failed VM are moved to the Standby Distributor VM. The failover is transparent to devices originating connections through the Distributor and the Director VMs.

Active-Active

VIPs can be configured as pseudo active-active by allowing VIPs to independently configure the priority of the DRA distributor VMs.

For example, a Gx VIP could configure dra-distributor-1 with priority 10 and dra-distributor-2 with priority 5 (the highest priority takes precedence). An Rx VIP could configure dra-distributor-2 with priority 10 and dra-distributor-1 with priority 5. In this scenario, the Gx VIP will start on dra-distributor-1 and the Rx VIP will start on dra-distributor-2.

Connection Synchronization

In order to support failover, connection information is periodically synchronized between a pair of Distributor VMs. Each Distributor advertises its connection information over multicast.

Health Checks

A Distributor virtual service consists of a virtual IP address/port combination and a list of real-server IP addresses used to handle connections to the VIP at the Director VMs.

A real-server IP address exists on a director VM. Health checks are performed for the diameter endpoint VIP/Port for each real-server.

Diameter Endpoint IP and Port

If a Distributor VIP's real-server fails the health check for the VIP:port (for example, 192.168.10.50:3868), the real-server is removed from the virtual service. In addition, if the Diameter Endpoint is not configured in Policy Builder, the real-server is removed from the virtual service.

Real-server Connections

In order for a Distributor virtual service to process incoming connections, it has to have at least one healthy real-server. If the virtual service does not have at least one healthy real-server, the VIP is removed from the active Distributor VM.