Dynamic Transport Selection based on Transaction or Origin Host

Important This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.

Overview

Reliable and secure telecommunications systems are necessary for effectively managing national security incidents and emergencies. The National Security and Emergency Preparedness (NS/EP) is a set of voice, video, and data services that belong to services available from public packet-switched Service Providers and that provide priority services in support of NS/EP communications. The NS/EP communication systems

include landline, wireless, broadcast, cable television, radio, public safety systems, satellite communications, and the Internet.

Wireless Priority Services (WPS) is one of the NS/EP communications programs that provide personnel priority access and prioritized processing in all nationwide and several regional cellular networks, increasing the probability of call completion.

WPS users, also known as first responders, are responsible for the command and control functions that are critical to the management of response to national security and emergencies. The Evolved Packet Core supports WPS calls that are received from WPS users, In the Cisco Policy Suite, Diameter based interfaces such as Gx and RX that support policy and charging control function for subscribers, captures call from WPS users.

Whenever calls received from WPS users require a separate handling of control plane IP packets, DSCP marking is used. The DSCP marking helps in differentiating WPS and non-WPS users and always call from WPS user to a normal non-WPS user is treated as highest priority.

When the network carries the traffic for WPS users, all the network elements individually and collectively must adhere to the following conditions:

- **Prioritization of Control Plane Traffic**: WPS user's control plane traffic is prioritized over other subscribers between different Network Functions in the LTE Core.
- **Priority Levels**: P1, P2, and P3 are the three priority levels available for WPS users:
  - P1 and P2 users are identified in Home Subscriber System (HSS) and Gateway (GW)
  - Priority levels are used during session attach, bearer creation or during bearer modification
  - P1 and P2 WPS users are always treated as High Priority
  - When WPS -P1 user calls non-WPS user, non-WPS users and P3 WPS users are given high priority dynamically based on a call being placed
  - DSCP markings for prioritized user's control plane IP packets is marked with DSCP=47 while all other users control packets IP packets is marked with DSCP=32

Note In CPS 21.1.0 and later releases, only P1 Priority is supported.

- **Diameter Interfaces**:
  - P-GW, Policy Change Rule Function (PCRF) and Diameter Routing Agent (DRA) uses the configuration of Diameter interfaces such as Gx and Rx interfaces to support policy and charging control for subscribers.
  - P-GW and S-GW uses Non-diameter interfaces such as S5 and S1U interfaces.

Characteristics of Low and High Priority Channels for Diameter Based Interfaces

Low Priority channels indicate normal priority users and High Priority channels indicate Wireless Priority services users during Differentiated Services Code Point (DSCP) markings. The peer connections towards DRA for P-GW (Gx) is shown in the Figures.

Figure 1: High-Level Overview of Low and High Priority Channels over Gx Interface

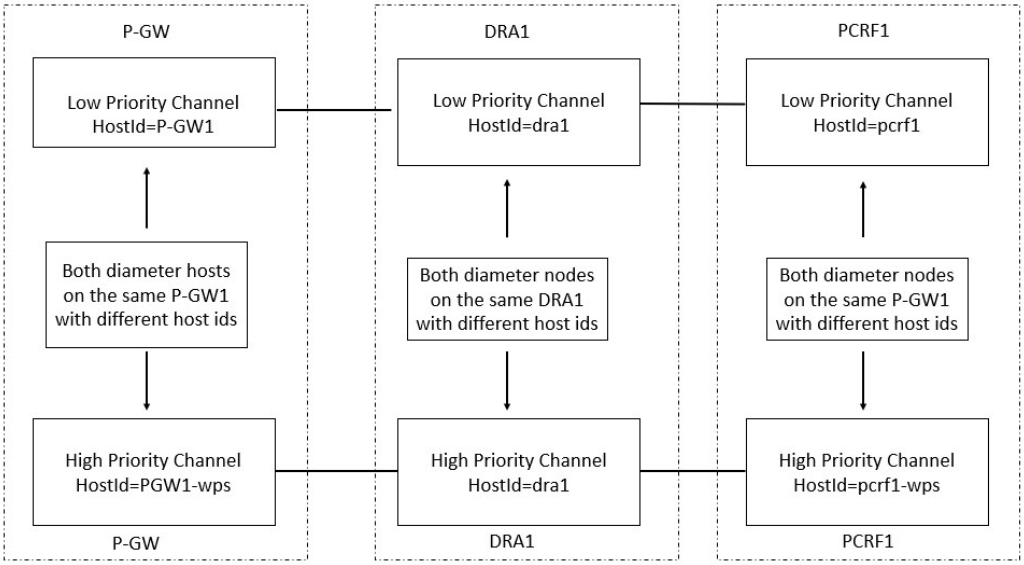


Figure 2: High-Level Overview of Low and High Priority Channels over Rx Interface

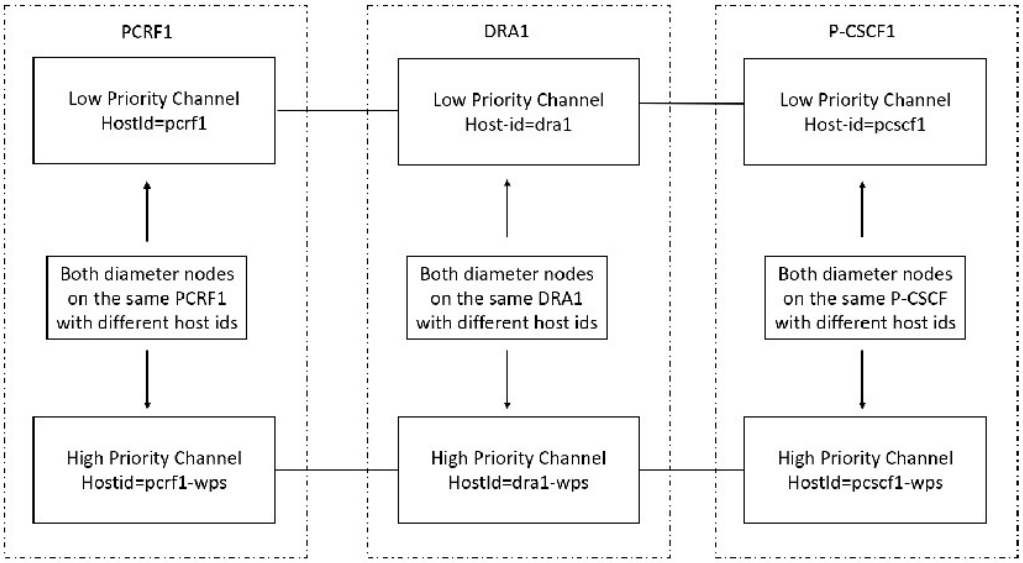


Table 1: Low and High Priority Channels based on Gx or Rx Interfaces

Priority Channel	Diameter Interfaces	IP Layer DSCP	TCP Connection over IP layer	Diameter Host FQDN
Low Priority	Gx/Rx	Equal to 32	32[1]	Not Modified For example, 0001-diamproxy. PGW-Gx', 'dra1', 'pcrf1
High Priority	Gx/Rx	Equal to 47	47	Specific to High Priority. For example, 0001-diamproxy. PGW-Gx-wps', 'dra1-wps', 'pcrf1-wps', 'pcscf1-wps'

[1] This channel is for non-WPS diameter messages but may carry WPS diameter messages in error scenarios, for example when all the WPS Peers are down.

Characteristics of Low Priority and High Priority Channels for S5 and S11 Interfaces

The S5 and S11 interfaces are GTPv2-based (which uses UDP as the transport protocol), Low and High Priority channels. Following table lists the characteristics.

Table 2: Low and High Priority Channels based on Rx Interfaces

Priority Channel	Diameter Interfaces	IP Layer DSCP	TCP Connection over IP layer	Diameter Host FQDN
Low Priority	S11 or S5	32	-	-
High Priority	S11 or S5	47	-	-

Dynamic Transport Selection based on Transaction or Origin Host on Policy Application Server

Transactions for certain Wireless Priority Service (WPS) user sessions are sent or received with different DSCP marking. You can create two sets of connections for Rx and Gx each with different DSCP marking.

Based on the Rx AAR, the Policy Application Server (PAS) chooses the right connection set for all subsequent transactions related to that session until the P-CSCF indicates a different priority. The DRA allows you to create the following policies for WPS users:

- DSCP marking for peer TCP connections: Use this function for WPS to forward WPS messages received from PAS. The WPS messages are treated as high priority in the network.
- Peer Group Message Class Mapping to configure message class for peer groups.
- Peer Group SRK Mapping.
- Peer Route for Priority Messages: Selects peers based on message priority.
- WPS Message Routing: PAS routes WPS messages over available WPS peer connections. If WPS connections are not available, then PAS routes WPS messages over available normal priority peer connection. PAS does not route non-WPS messages over WPS priority peer connection.
- Priority based destination host Re-routing: Supports rerouting of messages with destination-host based routing when WPS message is addressed to normal priority peer. This is allowed when a peer does not know the FQDN of high priority peer. This message rerouting can be enabled through option in Policy builder.
- DRA Relay Endpoint Message class mapping to configure message class for relay endpoints: Supports dedicated relay links for WPS messages with appropriate DSCP marking for the TCP connection. When forwarding WPS messages, PAS selects relay links matching the message priority.

DSCP Marking for Peer Connections

Wireless Priority Service (WPS) solution allows each of the peers connecting to PAS, establish a separate peer connection for normal and WPS messages with distinct origin FQDN. Peers uses distinct PAS endpoint for normal and WPS connection..

At the time of DSCP marking, PAS uses separate endpoints (inbound and outbound) for priority connections. Each diameter endpoint is configured with a DSCP value and all peer TCP connections to the endpoint is marked with the configured DSCP value.

Note Additional endpoints configured for WPS peer connections must use different VIPs as configuring same VIP for multiple endpoints can cause issues with load balancing by DRA distributor

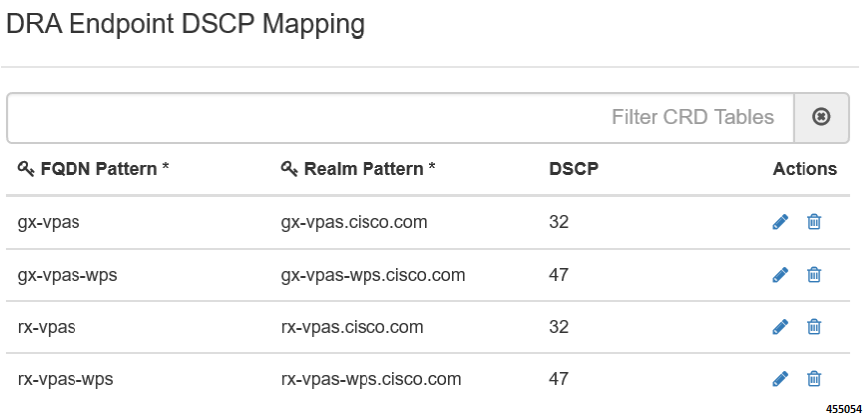
DSCP Mapping for DRA Endpoints

The DRA Endpoints DSCP Mapping allows you to configure different DSCP values for normal and WPS DRA endpoints.

If DSCP mapping is not configured for an endpoint, no action is performed. A default DSCP value is assigned to all endpoints by configuring a mapping using the wild card match as shown in the example:

```
{ FQDN Pattern= *, Realm Pattern= *, DSCP = <default value> }
```

Figure 3: DRA Endpoint DSCP Mapping



Enter or view the values the following field details:

Field	Description
FQDN Pattern	Displays an FQDN pattern of PAS endpoint.
Realm Pattern	Displays a Realm pattern of PAS endpoint.
DSCP	Displays the DSCP value for peer TCP connections to the DRA endpoint.
Actions	Allows you to perform either edit or delete actions.

The configured DSCP values are monitored using the below KPIs:

- peer_message_total
- peer_connection_status
- relay_message_total
- relay_peer_status

If it is not configued, the default DSCP value -1 is shown.

DSCP Marking in Diameter Stack

When creating diameter stack for each endpoint (inbound/outbound), stack manager reads DSCP mapping for endpoints and assigns appropriate value to stack instances. When a peer connection is established with diameter endpoint, stack sets the corresponding DSCP value for the TCP connection. All IP packets corresponding to messages that are forwarded by PAS (outbound) are marked with the specified DSCP value. P-GW, PCRF, and P-CSCF peers handle DSCP marking for inbound messages.

When you update a DSCP mapping in Custom Reference Data, then stack manager detects the configuration change and defines the new DSCP for all new connections. DRA does not change the already set DSCP value without resetting peer connections.

Priority-based Peer Group

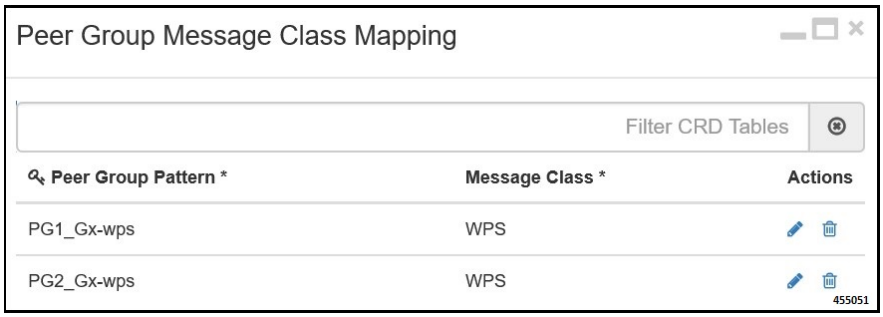
You can group all normal peers (non-WPS peers) under normal peer group and all priority WPS peers under WPS peer group. This way of grouping is useful in routing normal messages to normal peers and WPS messages to priority WPS peers.

Enter the following details in the **Peer Group Message Class Mapping** to configure priority for all peer groups.

Table 3: Priority-based Peer Group

Field	Description
Peer Group Pattern	Enter a peer group pattern name.
Message Class	Enter a Peer traffic and message class value for a peer group.

Figure 4: Assign Peer Groups to WPS Class



You can edit the values to Map peer groups to specific message class. DRA supports mapping peer groups only to message class of WPS. Configure the mapping only when a peer group is restricted to a specific message class. If the mapping is not configured for a peer group, then that peer group is designated by default to handle all message classes.

Peer Group for SRK Mapping

Map Peer groups for WPS and default peer connection to the same Session Routing Key (SRK). This enables DRA to select peer groups of default message class if WPS peer groups are down. In priority based SRK routing, DRA checks for active peers from matching WPS peer groups and fallback to peer groups of default message class if there are no active WPS peersMap Peer groups for WPS and default peer connection to the same Session Routing Key (SRK). This enables DRA to select peer groups of default message class if WPS peer groups are down. In priority based SRK routing, DRA checks for active peers from matching WPS peer groups and fallback to peer groups of default message class if there are no active WPS peers

Mapping of logically related peer groups under same SRK is useful in route selection for below two scenarios.

- For non-WPS users, when Gx session gets created in normal peer and gets updated to WPS session during Rx AAR calls, then DRA checks for message priority Attribute Value Pair (AVP) in AAR request and route the WPS message to WPS peer.

- For WPS users, if there are no active WPS peers in local/remote, then DRA routes WPS messages to normal peers as fallback option.

  The following figure illustrates a sample CRD "Peer Group SRK Mapping" configurations to support normal and WPS peer groups.

Table 4: Peer Group SRK Routing

Field	Description
Peer Group	Enter a Peer group name
Session Routing Key	Enter the Session Routing key information of Peer group.
Destination Host Routing Rule	Specify one of the following Destination Host Routing Rule: • Only • Never • Preferred • Preferred for Update Requests[2]
Destination Host Replace	Choose YES or NO to enable or disable destination host replace.

[2] When Destination-Host routing policy for PCRF Gx peer group is set to **Preferred for Update Requests**, then PAS routes the request as follows:

- PAS resets Destination-Host rule as **Preferred** and route Gx CCR-I request using Table-driven routing when destination host is set as DRA endpoints or destination host is null. If Gx CCR-I request contains destination host AVP as PCRF endpoint, then PAS routes Gx CCR-I request using destination host routing.
- PAS resets Destination-Host rule as **Preferred** and route Gx CCR-U requests using destination host routing and fallback to SRK routing only when PAS failed to find the same PCRF host mentioned in Destination-Host AVP
- PAS resets Destination-Host rule as **Never** and routes Gx CCR-T request using SRK routing

Note DRA routes second Gx CCR-T request to different PCRF host. PAS supports the new Destination-Host routing rule "Preferred for Update Requests" only for PCRF Gx peer groups. If the new Destination-Host routing rule "Preferred for Update Requests" is configured for any non-Gx peer groups, then PAS sets default Destination-Host rule as "Preferred" for route selection.

Peer Routing for Priority Message

Map WPS peer route with WPS peer groups and default peer route with default peer groups. If you want to map fallback from WPS peer to default peers, then define WPS peer route to both WPS peer groups and default peer groups. Peer route mapped to WPS peer group takes higher precedence and peer route mapped

to default peer group takes lower precedence. If WPS peer groups are inactive, this precedence is used in Table Driven Routing to select WPS peer groups and fallback to default peer groups.

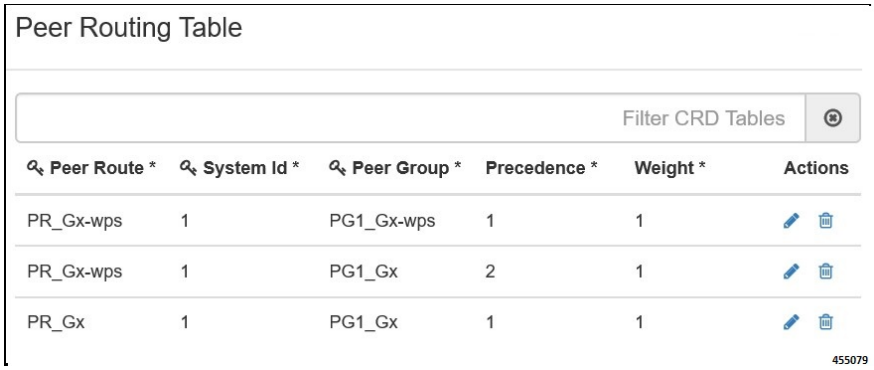
In case of default peer route, only default peer group is mapped and no fallback to WPS peer group is allowed, if default peer groups are inactive.

Enter the Peer Route List details to configure default and WPS peer groups and Peer Routing Table configurations to support default and WPS peer groups.

Table 5: Peer Routing List

Field	Description
Peer Route	Enter a Peer route list. For example, PR_Gx for normal user and PR_Gx-wps for WPS user.
Actions	Allows you to perform either edit or delete actions.

Figure 5: View Peer Route Table Details



Enter Peer Route Table details to configure default WPS peer groups.

Table 6: Peer Routing List

Field	Description
Peer Route	Enter a Peer route name for WPS peer and Non-WPS peer.
System Id	Enter System Id of the same vDRA.
Peer group	Enter a Peer group name for WPS peer and Non-WPS peer.
Precedence	Enter the priority value for selecting WPS peer groups and fallback to default peer groups, if WPS peer groups are inactive.
Weight	Enter the weightage of peer route.
Actions	Allows you to perform either edit or delete actions.

WPS Message Routing

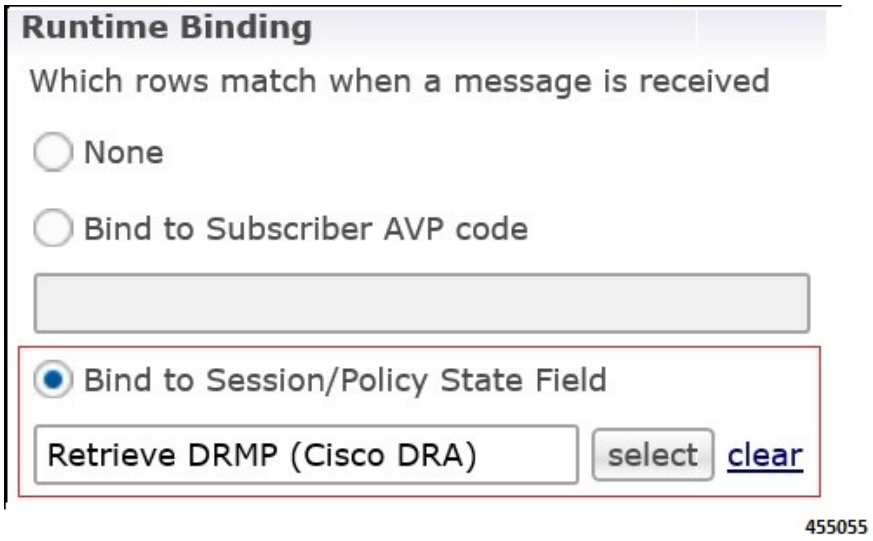
PAS routes WPS messages over available WPS peer connections. If WPS connections are not available, then PAS routes WPS messages over available normal priority peer connection. PAS does not route non-WPS messages over WPS priority peer connection.

Table Driven Routing

Table Driven Routing for WPS messages uses Origin Host or Realm. This is because WPS peers use distinct FQDN and Realm, which ensures that all messages received on WPS peer connections are routed to WPS peers.

To route WPS messages received on default peer connection, include message priorities, and configure appropriate rules matching priority in the routing table. DRA provides the option to retrieve DRMP AVP and Message Class for incoming messages and map them to Gx Routing table.

Figure 6: Runtime Binding



Use the following procedure to specify the Runtime Binding details:

1. In CPS DRA, navigate to **Policy Builder** .
2. Click,**Reference Data** and then choose **Systems**.
3. Click **Custom Reference Data Tables**.
4. In the Runtime Binding area, specify the following details.

Field	Description
None	If no rows require matching when a message is received, click the **None** radio button.

Field	Description
Bind to Subscriber AVP Code	Click the **Bind to Subscriber AVP Code** radio button to retrieve values from an AVP for the subscriber. Also, values from a session AVP or a Policy Derived AVP is displayed.
Bind Session/Policy State Field	Click the **Bind Session/Policy State Field** radio button to select the value from a Policy State Data Retriever, which retrieves a single value for a session. Choose any one of the following DRMP options to indicate after adding new Message priority AVP: • Retrieve DRMP (Cisco DRA): Displays value from DRMP message priority AVP of incoming messages. • Retrieve Message Class (Cisco DRA): Maps Message Class profile with message class type as WPS_P0. This ensures that DRA is not throttling any WPS CCR-I messages

5. In the Gx New Session Rules area, view the following details. Maps peer routes with Origin host, Origin realm and DRMP AVP for normal and WPS peer groups.

Field	Description
Logical APN	The name of the logical Access Point (APN).
Origin Host	The origin host FQDN
Peer Route	Peer route to select active peer groups.
Origin Realm	The Origin Realm.
Destination Host	Displays the destination host FQDN.
Destination Realm	Displays the destination Realm.
MSISDN	Displays the MSISDN subscriber identification attribute.
IMSI	Displays the IMSI subscriber identification attribute.
DRMP/Message Class	Displays either DRMP or custom message class AVP value.

Table Driven Workflow

Note Since **DRMP/Message Class** field is the primary key-in Gx routing table, any old exported CRD dumps should be imported to DRA before adding the new **DRMP/Message Class** field. After adding new **DRMP/Message Class** field, you must manually update these fields with default values (*) for all existing entries in Gx Routing CRD. Otherwise, DRA does not show any values for these new fields and might cause routing failure for Gx CCR-I messages.

The following lists explain the table driven workflow:

- DRA selects peer route based on the match in table row of Table-Driven routing. The matched peer route can have N number of peer groups with different or same precedence.
- DRA creates a sorted list to maintain all peer groups in higher to lower precedence order. It traverses through sorted peer group precedence list and checks whether the WPS peer group is active in local or remote site.
- If local WPS peer group is in active state, then DRA selects local WPS peer group.
- If local WPS peer group is in inactive state, then fallback to remote WPS peer group.
- Only when both local and remote WPS peer groups are in inactive state, then DRA will check for normal peer group in same peer route.
- If DRA fails to find any active normal peer in matched peer route, then DRA sends 3002 ERR response.
- In case of fallback for normal messages, since, DRA does not select peers from WPS peer group at any time, normal peer route should be mapped with only normal peer groups and WPS peer route should be mapped with WPS peer group as first precedence and if needed, then map normal peer group as second precedence.

Destination Host Routing

During Destination Host routing, DRA performs Destination host routing only when destination host AVP is present and it is not pointing to DRA endpoint FQDN. The following conditions apply:

- If destination host peer is active, then it will route the request to that destination peer.
- If destination peer is inactive, then it will fall back to SRK routing. In SRK routing, DRA can select active peer from different groups where all these groups are mapped to same SRK.

DRA gives preference to destination host priority and forwards the message to set destination host peer. P-GW and PCRF sets correct WPS destination host in request based on the message priority.

Supporting Fallback of WPS Gx RAR, Rx RAR, and Rx ASR Messages to non-WPS Peer

vDRA supports fallback of WPS Gx RAR, Rx RAR and Rx ASR messages to non-WPS peer when there is no active WPS peer available locally or globally. Through WPS Suffix keyword configuration, you can identify two connections such as WPS or non-WPS that belong to P-GW /P-CSCF. Also, through configuration, vDRA

controls suffix based destination host routing on peer group. For example, you can enable this fallback for Cisco ASR but not for affirmed P-GW.

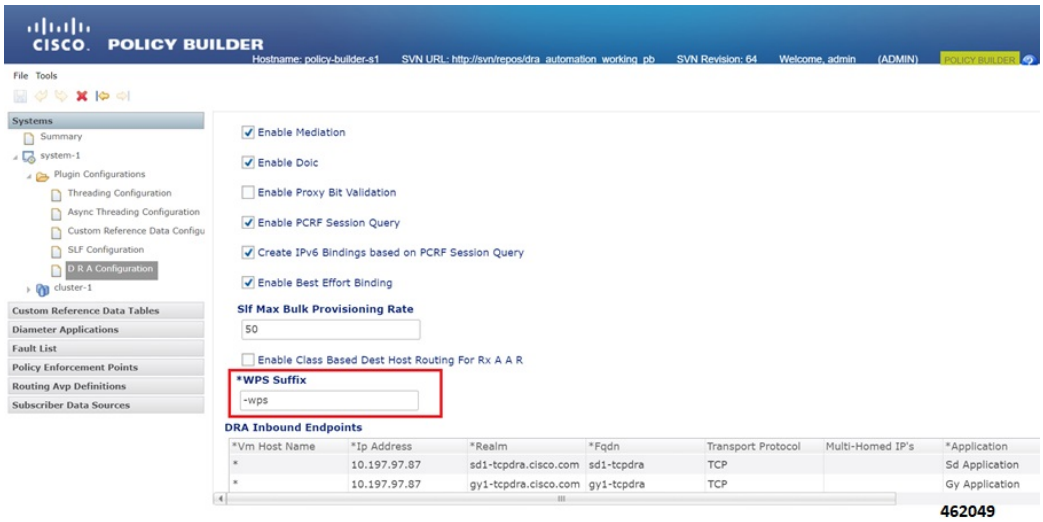
Note Suffix based destination host routing is applicable only for Gx RAR, Rx RAR and Rx ASR messages. This feature is disabled if there is no WPS suffix configured in policy builder and if there are no rows configured in “Suffix Based Dest Host Routing" CRD.

Configuring WPS Suffix in Policy Builder

Use the following procedure to configure WPS suffix keyword in the Policy builder.

1. Log in to the **Policy Builder**
2. Choose **Systems** > **Plugin Configuration** > **DRA Configuration** .
3. In the **WPS Suffix** field, enter a WPS suffix to use across all nodes. For example, you can configure a keyword “-wps” as suffix.

Figure 7: Configure WPS Suffix



Ensure to configure the same suffix keyword across P-GW and PCRF nodes. Otherwise, route failure might occur in WPS Gx/Rx RAR and Rx ASR fallback routing.

For more information about DRA features, see the *DRA Feature* section in the *CPS vDRA Configuration Guide*.

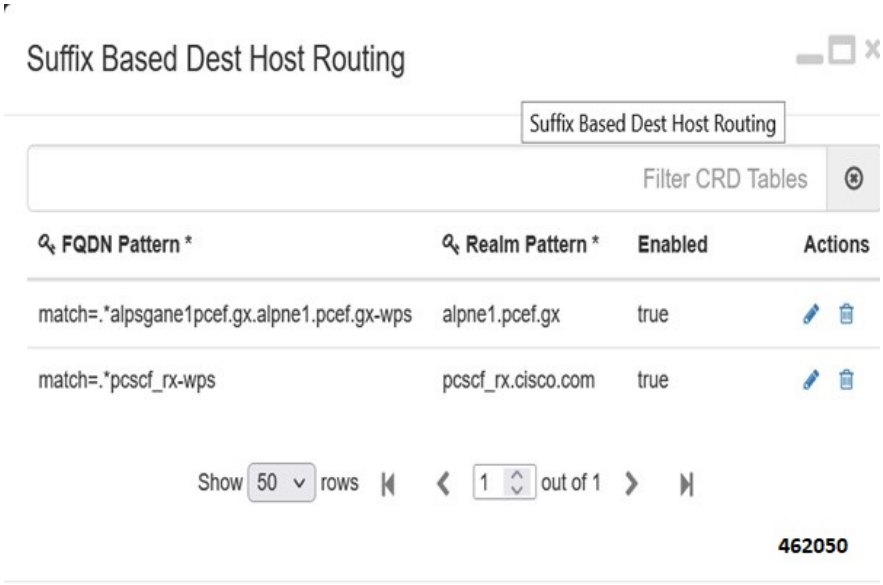
Enabling Suffix Based Dest Host Routing

vDRA supports fallback of WPS Gx RAR, Rx RAR and Rx ASR messages to non-WPS peers only for the peers configured in the **Suffix Based Dest Host Routing** CRD table. vDRA uses this CRD only when normal dest-host routing and SRK routing failed for WPS Gx RAR, Rx RAR and Rx ASR messages.

Note vDRA does not use this CRD for routing of any non-WPS Gx RAR, Rx RAR and Rx ASR messages.

To configure WPS PGW/P-CSCF peers, create a new CRD **Suffix Based Dest Host Routing** as shown in the figure.

Figure 8: Create new Suffix Based dDestination Host Routing CRD



Handling Fallback

Based on WPS3B configurations, all nodes (P-GW/PCRF/PCSCF) have separate FQDN for WPS peers. This WPS FQDN is different from non-WPS FQDN and is suffixed with configured new keyword. For example, if configured suffix keyword is “-wps”, then FQDN have pgw/pgw-wps, pcscf/pcscf-wps, pcrf-gx/pcrf-gx-wps, pcrf-rx/pcrf-rx-wps.

DRA performs WPS Gx RAR, Rx RAR and Rx ASR fallback to non-WPS peer in following ways.

1. After vDRA receives Gx RAR, Rx RAR, and Rx ASR messages with destination host:
   - vDRA tries to route the message using destination host routing and then SRK routing.
   - If the WPS peer mentioned in Dest-Host AVP is inactive and fails to find active route using SRK routing, then vDRA uses “Suffix Based Dest Host“ routing.
2. vDRA gets configured suffix keyword from the Policy Builder and checks whether destination host mentioned in the Dest-Host AVP have the same suffix. The following actions happen:
   - If both are same, vDRA truncates the suffix keyword from destination host and sends the WPS message to non-WPS destination host.

Note After truncating configured suffix from destination host, vDRA first checks for local non-WPS peer and then checks for remote non-WPS peer only if there are no active local peers.

- If both are different, vDRA skips “Suffix Based Dest Host” routing and tries Table Driven routing.
- If vDRA fails to find any active route, then it sends timeout message to PCRF.

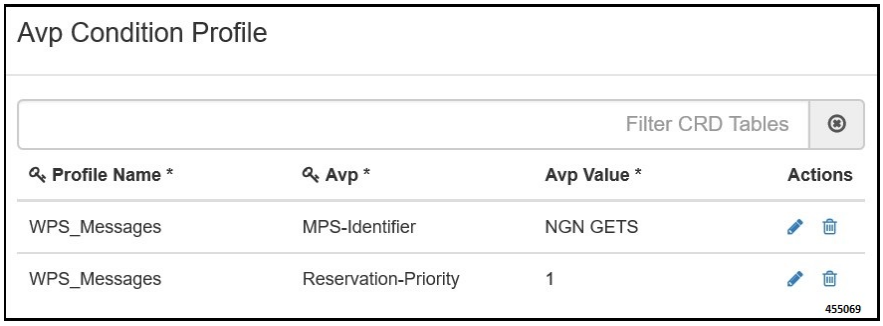
Binding-based Routing

During Binding-based routing, DRA routes Rx messages to the correct peer based on the message priority. For non-WPS users, create a Gx session in normal peers and Rx session in WPS peers. DRA routes all priority Rx messages to WPS peers. For WPS users, DRA routes all priority to both Gx and Rx on WPS peers.

To identify WPS messages, in the AVP Condition Profile area:

- Configure either MPS-Identifier AVP or Reservation Priority in Diameter AVP Dictionary and then map the AVP Condition Profile Custom Reference Data with correct values.
- Configure both MPS-Identifier AVP or Reservation Priority AVPs. Make sure that both the AVPs are mapped under the same AVP Condition Profile.

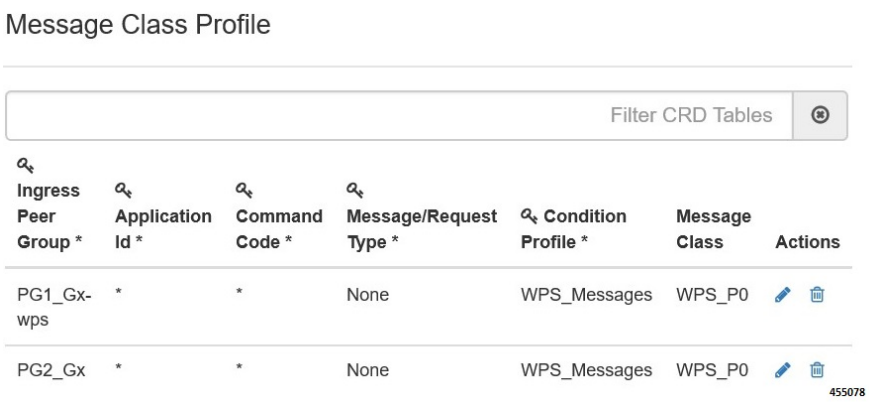
Figure 9: AVP Condition Profile mapping for both MPS-Identifier and Reservation-Priority AVPs



In the Message Class Profile area, DRA classifies new message classes for WPS.

- If Message classes profile is defined then, message classes include message class and message priority. For example, If new message class is WPS_PO, then this indicates WPS message of priority P0.
- If message class profile is not defined, then DRA classifies the message as default message class.

Figure 10: Message Class Profile



Enter the following Message Class Profile Parameters.

Table 7: Message Class Profile Parameters

Field	Description
Ingress Peer group	The name of the Ingress Peer group.
Application ID	The application identifier.
Command Code	Displays diameter message command code
Message/Request Type	Displays either a message or type of the request.
Condition Profile	Displays a condition profile for either WPS or non-WPS messages.
Message Class	Displays the message class and message priority for WPS user.
Actions	Allows you to perform either edit or delete actions.

SRK Routing

The following workflow explains Session Routing Key (SRK) function for WPS:

- For non-WPS users, when Gx session gets created in normal peer and gets updated to WPS session during Rx AAR calls, DRA checks for message priority AVP in AAR request and route the WPS message to peers under WPS message class.
- For WPS users, if there are no active WPS peers, DRA routes WPS messages to default message class peers as fallback option.
- DRA does not route normal messages to WPS peers at any point of time.
- When DRA receives WPS messages, it checks for WPS peers in local site and then fallback to remote site.
- If DRA is not able to find any active peers of WPS message class in local/remote, then it considers default message class peers to route WPS messages.

- DRA checks for default message class peers in local and then fallback to remote site.
- When DRA accepts any peer connection, Peer Manager accepts the peer connection and it will read peer priority from the Peer Group Message Class Mapping and updates the matching message class priority in DRA peer up/down control message.
- Peer Manager publishes the control message to local/global control plane.
- Local/global control plane thread publishes the same to local/global topology manager.
- The local topology manager updates peer message class in peer endpoint state.

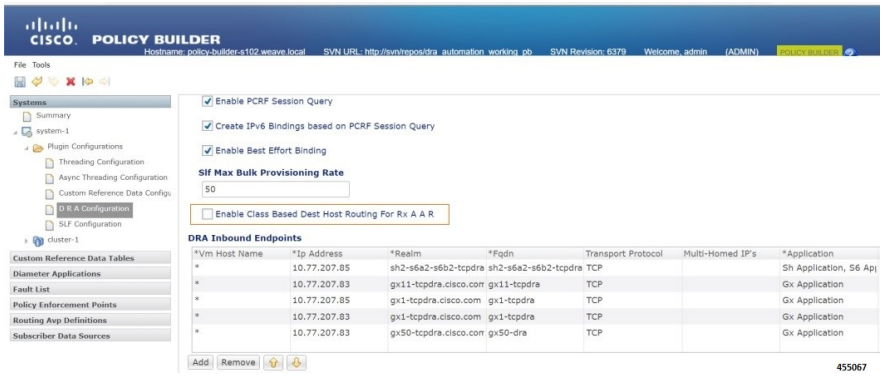
Priority-based Destination Host Rerouting

Priority-based Destination Host Rerouting feature enables DRA to identify mismatch between message class of destination host and AAR and reroutes to PCRF matching the message class. This feature is disabled by default.

In DRA, you can configure message priority AVPs in **AVP Condition Profile**, **Message Class Profile**, and map the profile to message class **WPS_P0**. The **WPS** is used as message class and **P0** indicates to message priority. For more information, refer *Binding based Routing* section.

Once you check the **Enable Class Based Dest Host Routing for Rx AAR** check box, DRA checks the message class of Rx AAR and compares with message class configured for destination peer group. If there is a mismatch in the message class and destination peer group has SRK configured, DRA performs SRK routing instead of destination host routing. SRK routing routes the message to peer matching the message class.

Figure 11: Priority-based Destination Host Rerouting Parameter



PCRF Session Query for WPS Messages

In Diameter Routing Agent (DRA), use WPS PCRF or non-WPS PCRF REST API endpoints, to send WPS PCRF session query to PCRFs, and receive Session Route Key (SRK) information for WPS Rx AAR messages.

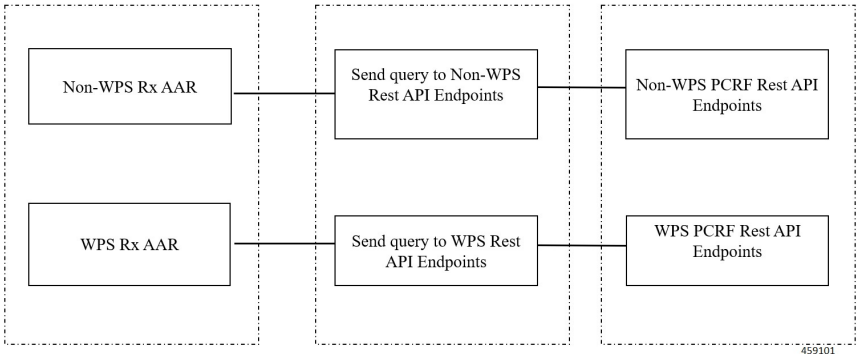
DRA allows the following functionalities:

- Separate Rest API endpoints configuration to support WPS IPv6 binding queries.
- WPS Rest API endpoints to query IPv6 binding for all WPS messages.

- PCRF session query for WPS Rx AAR messages is set with configured DSCP value as 47.
- PCRF session query for non-WPS RX AAR messages is set with configured DSCP value as 32.
- Query parameter class=wps will be added for all WPS PCRF session queries.
- Fallback to non-WPS PCRF Rest API Endpoints. This is to get session route key information for WPS Rx AAR messages when there is any issue in sending query with WPS PCRF Rest API endpoints or WPS PCRF Rest API endpoints not configured.

Architecture

The following illustration depicts WPS and non-WPS IPv6 binding queries.



Processing IPv6 Binding Query for WPS Messages

In DRA, PCRF contains new set of Rest API endpoints to serve IPv6 binding query for WPS messages. Based on message priority of Rx AAR messages, DRA selects configured Rest API endpoints as follows:

- If the incoming Rx AAR message is WPS, then DRA selects Rest API endpoints from **PCRF Session Query Peers** that are configured as message class **WPS**. All WPS Rest API endpoints are marked as **WPS** in **PCRF Peer Group Message Class Mapping** CRD.
- DRA adds **class=wps** as query parameter to the payload to indicate message class as WPS to PCRF for internal prioritization. This is applicable only for WPS PCRF session queries.
- If DRA fails to send PCRF session query using WPS PCRF Rest API endpoints or WPS PCRF Rest API endpoints are not configured, then DRA will fallback to non-WPS PCRF Rest API endpoints to send high priority WPS PCRF session query
- DRA adds **class=wps** as query parameter to the payload even at the time of fallback to non-WPS PCRF Rest API endpoints.
- If the incoming Rx AAR message is non-WPS, then DRA selects non-WPS Rest API endpoints from **PCRF Session Query Peers** to send session query.

Note DRA does not use high priority WPS PCRF Rest API endpoints to send any PCRF session query for non-WPS messages.

Configuring IPv6 Binding Query Messages

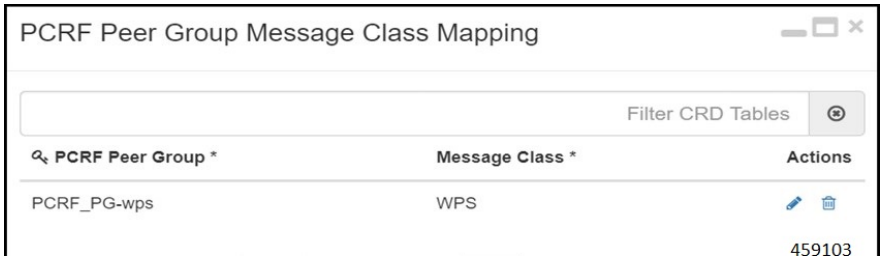
Use the following steps to configure IPV6 binding query messages:

1. Configure separate Rest API Endpoints for WPS IPv6 binding queries:

   In the **PCRF Session Query Peers** CRD, create a separate PCRF group for all WPS-related Rest API endpoints. For more information about configuring the REST API parameters for Rx AAR fallback routing, see the section *PCRF Session Query Peers* in the *Policy Builder Configuration* chapter.

2. Configure message class as WPS for WPS PCRF peer groups. Create a new CRD **PCRF Peer Group Message Class Mapping** as shown in the Figure. Only PCRF peer groups created in CRD are**PCRF Session Query Peers** configured in this new CRD.

   Figure 12: PCRF Peer Group Message Class Mapping Configuration



3. Configure DSCP value for PCRF REST API Endpoints. Use linux command iptables/ip6tables to configure DSCP value as 47 for WPS PCRF Rest API endpoints and DSCP value as 32 for non-WPS PCRF Rest API endpoints.

```
For example:
If non-WPS PCRF Rest API endpoint is http://10.197.99.271:9000/dra/api/bindings and WPS
 PCRF Rest API endpoint is
http://10.197.99.271:9001/dra/api/bindings, then DSCP value can be set as:
iptables -t mangle -A PREROUTING -d 10.197.99.271 -p tcp --dport 9000 -j TOS --set-tos
128
iptables -t mangle -A PREROUTING -d 10.197.99.271 -p tcp --dport 9001 -j TOS --set-tos
188
```

Note Left shift DSCP value by 2 to get TOS value.

(47 << 2) = 188

(32 << 2) = 128

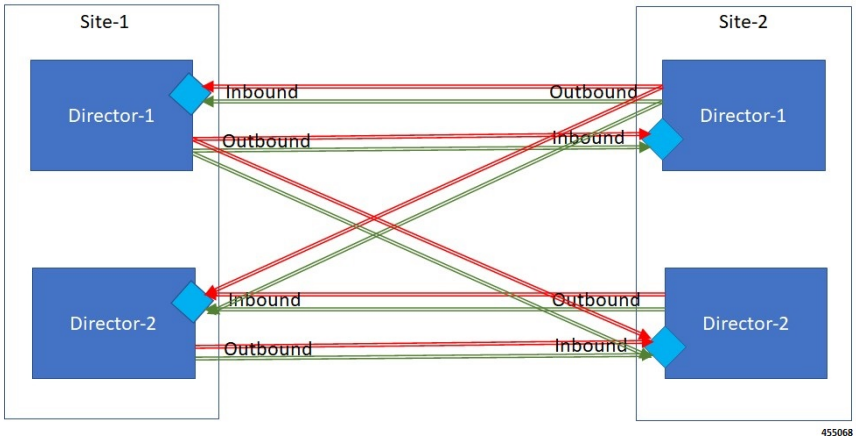
Priority based Relay Routing

Policy Application Server supports Priority-based relay routing for WPS messages through the following mechanism:

- Relay Endpoints for Priority Messages
- Advertising Relay Link Priority in Control Plane

- Relay Link Selection based on Priority

Figure 13: : Priority-based Relay Routing Flow



Relay Endpoints for Priority Messages

As part of the WPS feature, Dimameter Routing Agent (DRA) has two relay connections to relay peers. One relay link for WPS relay messages and another one for normal relay messages.

To route WPS relay messages to WPS relay link, DRA updates relay logic as follows

- Configures two relay endpoints in the Policy Builder. One for WPS relay messages and another one for normal relay messages. Normal and WPS relay endpoints are configured with unique FQDN.
- Configures relay endpoints message class in **DRA Relay Endpoint Message Class Mapping** for WPS.

Advertising Relay Link Priority in Control Plane

The remote relay system identifies the relay priority and routes WPS messages through WPS relay link.

Note Changes to control plane message is backward compatible. Hence, systems that do not support message class priority can ignore this Advertising Relay link priority function.

Selecting Relay Link based on Priority

The following procedural steps describes how DRA selects the relay link based on priority:

1. Creates queue for remote relay endpoints using remote SystemId and remote relay message class. This is mainly to differentiate between WPS relay and default relay queue. DRA maintains two outbound and inbound connections with relay system:

- WPS relay connection to forward WPS messages
- Default relay connection to forward default messages

During routing whenever remote peers are selected to route messages, remote relay endpoint is selected based on the message class of the selected destination host peer or incoming request.

2. DRA compares the message class of message and destination host peer with message class of relay system to select the WPS relay endpoint, to forward only WPS messages, and selects default relay endpoint to forward default messages.
3. When DRA receives control plane messages for remote relay system, it stores the relay systemId in topology Manager along with relay message class.
4. DRA routes WPS relay messages over normal relay endpoint link only when WPS endpoint is down.