Configure WPS Feature for LTE Core Networks

Contents

Introduction

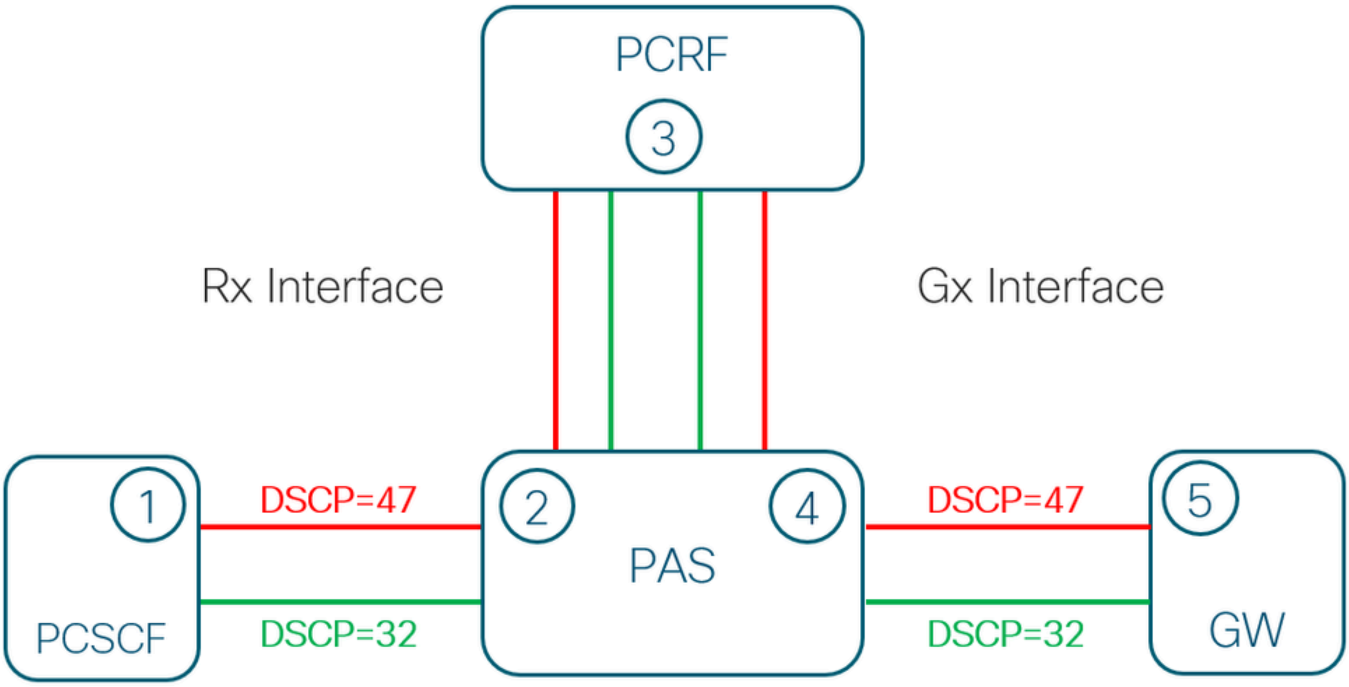
This document describes the concept, implementation, and benefits of Wireless Priority Service (WPS) in the network, using components like DRA and PCRF.

Basic Concept of WPS

WPS is one of the National Security and Emergency Preparedness (NS/EP) communications programs that provides personnel priority access and prioritized processing in all nationwide and several regional cellular networks, increasing the probability of call completion. NS/EP communication systems include landline, wireless, broadcast, cable television, radio, public safety systems, satellite communications, and the Internet.

WPS users (known as First Responders) are responsible for the command-and-control functions which are critical to the management of a response to National Security and Emergency situations. It provides personnel priority access and prioritized processing in all nationwide and several regional cellular networks, increasing the probability of call completion.

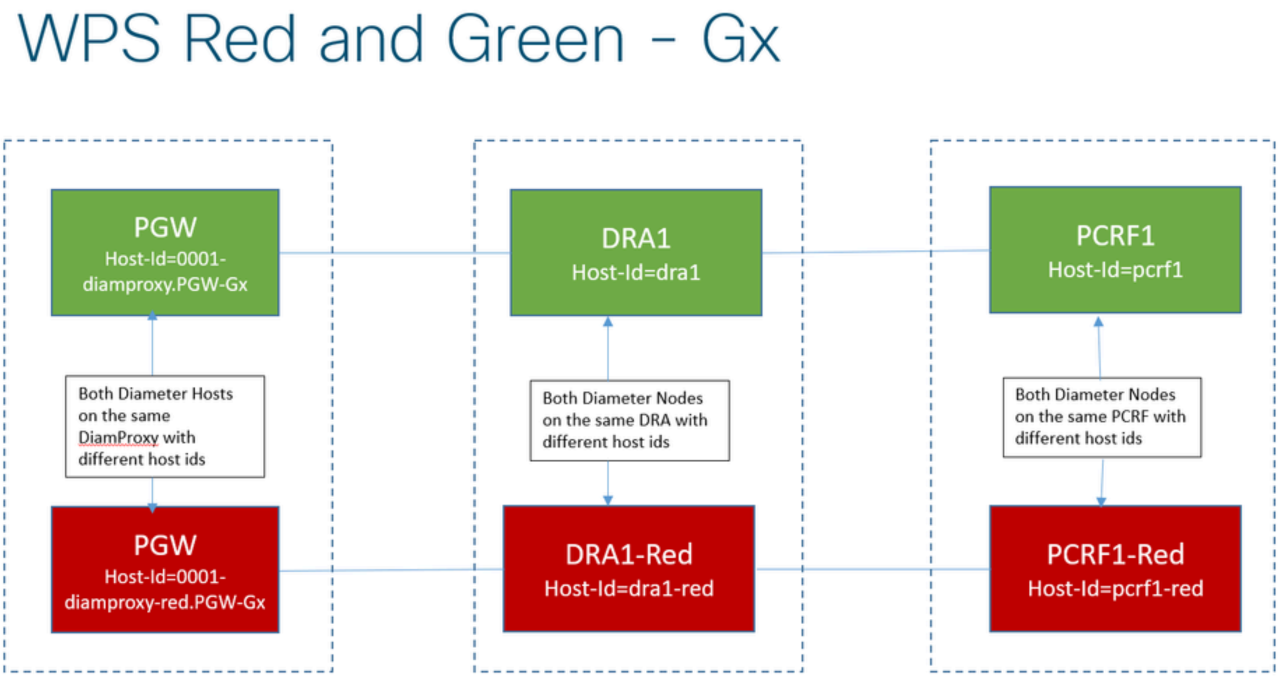
Customers network will carry the traffic for WPS users and these WPS users control plane traffic is highly prioritized over other subscribers between different Network Functions in the Long Term Evolution (LTE) Core.



Two sets of peers are maintained between PCSCF, PAS, PCRF and GW. One set is configured to mark all IP packets with DSCP=32 (GREEN Set). while the other set marks all related IP packets with DSCP=47 (RED Set)

WPS Feature Explained

- Concept: Implementation of dedicated channel (RED Channel) for the Priority message to be communicated. Separate channels are used for communication of WPS and non WPS where prioritized users control plane IP packets will be marked with Differentiated Services Code Point (DSCP) as 47 while all other users will have DSCP marked as 32.



WPS Red and Green - Gx

PGW
Host-Id=0001-diamproxy.PGW-Gx

Both Diameter Hosts on the same DiamProxy with different host ids

PGW
Host-Id=0001-diamproxy-red.PGW-Gx

DRA1
Host-Id=dra1

Both Diameter Nodes on the same DRA with different host ids

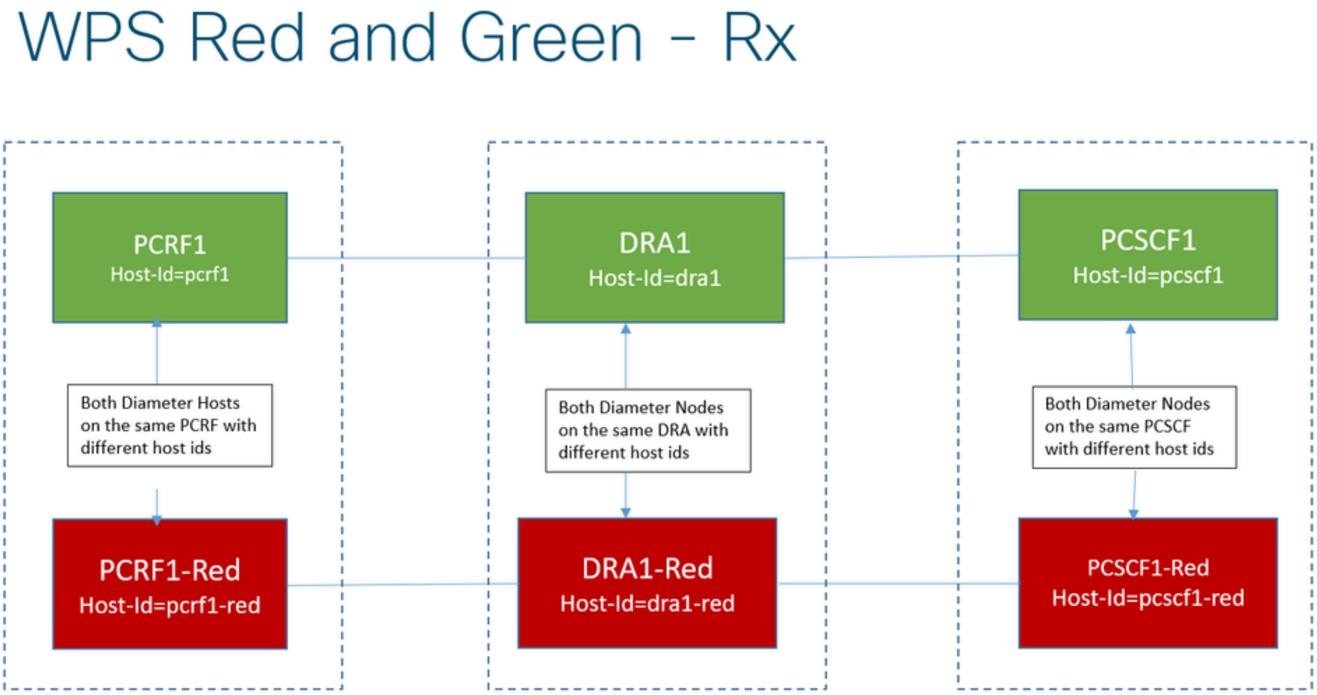
DRA1-Red
Host-Id=dra1-red

PCRF1
Host-Id=pcrf1

Both Diameter Nodes on the same PCRF with different host ids

PCRF1-Red
Host-Id=pcrf1-red

WPS_GX



WPS Red and Green - Rx

PCRF1
Host-Id=pcrf1

Both Diameter Hosts on the same PCRF with different host ids

PCRF1-Red
Host-Id=pcrf1-red

DRA1
Host-Id=dra1

Both Diameter Nodes on the same DRA with different host ids

DRA1-Red
Host-Id=dra1-red

PCSCF1
Host-Id=pcscf1

Both Diameter Nodes on the same PCSCF with different host ids

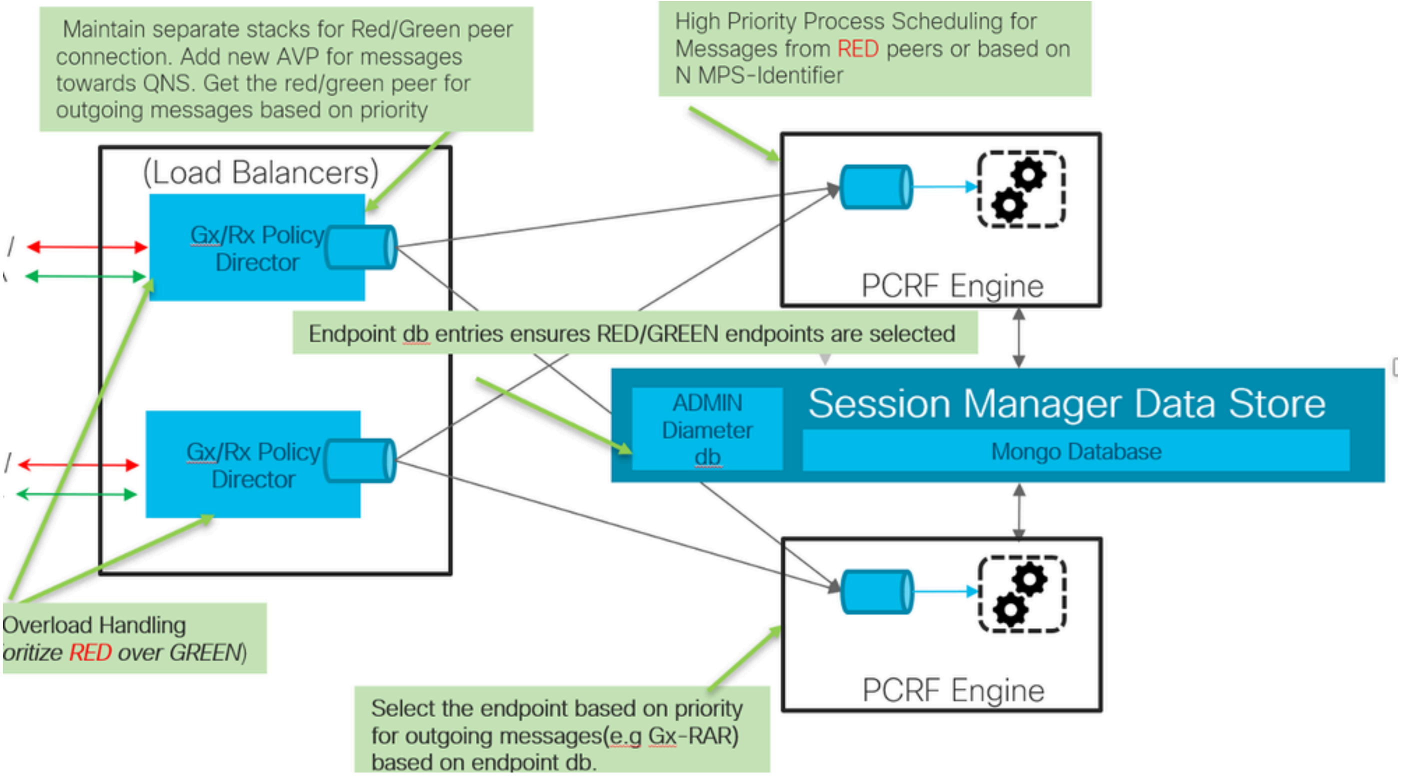
PCSCF1-Red
Host-Id=pcscf1-red

WPS_RX

- Mechanism: For the LTE Core, the indication of higher priority for a user comes over Gx or Rx. For Gx, it depends upon the channel on which the user receives the Gx messages (Origin-host based priority) or presence of Diameter Routing Message Priority (DRMP) Attribute Value Pairs (AVP). And for Rx, the Multimedia Priority Service (MPS)-Identifier and Reservation Priority AVPs only signify the Rx calls to be of WPS.

- Adaptive Policies: The implementation of WPS allows for adaptive policy configurations within the Policy and Charging Rules Function (PCRF) and Diameter Routing Agent (DRA). Through dedicated RED channels, customer-specific requirements — such as the use of specific Fully Qualified Domain Names (FQDN) or Realms — can be configured to ensure optimized traffic flow for both priority and non-priority messages.

Calls Per Second (CPS) Affected Components


Maintain separate stacks for Red/Green peer connection. Add new AVP for messages towards QNS. Get the red/green peer for outgoing messages based on priority
High Priority Process Scheduling for Messages from RED peers or based on N MPS-Identifier
(Load Balancers)
Gx/Rx Policy Director
Gx/Rx Policy Director
PCRF Engine
Endpoint db entries ensures RED/GREEN endpoints are selected
ADMIN Diameter db
Session Manager Data Store
Mongo Database
PCRF Engine
Overload Handling
oritize RED over GREEN)
Select the endpoint based on priority for outgoing messages(e.g Gx-RAR) based on endpoint db.

WPS_Affected_Nodes

Implementation in DRA and PCRF

- Fall Back Situation: This feature ensures the implementation of fallback situation by sending the messages to Active Non-WPS peer when a WPS peer is not available locally or globally and where the message is really intended to be delivered as it is a high priority message. Here the DRA is ensuring that these messages are never lost/not processed owing to unavailability of WPS peers.
- Red/Green Query Path Capability Implementation: This feature configures separate Rest API endpoints in order to support WPS IPv6 binding queries. It selects WPS Rest API endpoints to query IPv6 binding for all WPS messages and Non-WPS Rest API endpoints to query IPv6 binding for all non-WPS messages.
- DSCP value is set as 47 for all WPS messages going to WPS Rest API endpoints and it is set with the value as 32 for non-WPS messages going to non-WPS Rest API endpoints. Partner Advanced Support (PAS) sets 'class=wps' as a query parameter for all WPS PCRF session queries.

Benefits of Establishing Red/Green Channels

Overload Protection:

WPS prioritization in the PCRF includes mechanisms that safeguard message flow, even when the network is under heavy load. This ensures that WPS communications are processed without delay, preserving the integrity of emergency responses regardless of broader network conditions.

Load Balancer Protection:

Implementing RED/GREEN channels in PCRF mitigates overloads at the Load Balancer, a critical network function. With this feature, load management becomes more efficient, indirectly protecting essential nodes like the Quality Network Service (QNS) from experiencing heavy traffic surges. Even during peak network usage, WPS messages are processed with top priority.

Fallback Mechanisms:

In the event of a WPS channel failure, the network dynamically falls back to available non-WPS paths. This ensures that essential WPS messages continue to flow without interference, while non-WPS messages remain within their designated channels, preserving the separation of critical and routine traffic.

Dedicated API Endpoints for WPS IPv6 Binding Queries:

Separate REST API endpoints for WPS queries enable more effective network management and prevent DSCP-marked WPS and non-WPS messages from interfering with each other. This structural separation of endpoints supports a smoother query process and guarantees that traffic stays within its priority classification.

Prospective Areas of Implementation

Telecommunications Networks:

In large telecom networks, WPS has proven effective in reducing latency for high-priority communications, offering faster response times and operational improvements.

Internet of Things (IoT) and Machine-to-Machine (M2M) Communications:

With the rising volume of IoT and M2M traffic, network congestion is a constant challenge. By implementing WPS, networks can manage IoT signaling traffic more efficiently, prioritizing critical data flow without compromising overall network performance.

Emergency Services:

During emergencies or peak usage periods, WPS prioritization safeguards the reliability of critical communication channels, ensuring that emergency responders receive real-time data and that their commands are relayed promptly.

Challenges and Considerations

Performance Penalties:

One drawback of WPS implementation is the performance overhead during policy evaluations. For non-WPS sessions, each query passes through a comprehensive table check, which can be resource-intensive if the table is extensive. Minimizing the tables size and ensuring efficient policy lookup are essential to mitigate this issue.

Scalability Concerns:

As the demand for IoT and high-priority communications grows, managing RED/GREEN channels will require robust scalability solutions. Network planners must be mindful of this when considering capacity expansion and long-term WPS feature adoption.

Note: Detailed concept and configuration for DRA is explained in the CPS vDRA Configuration Guide.

https://www.cisco.com/c/en/us/td/docs/wireless/quantum-policy-suite/R24-2-0/vDRA-ConfigurationGuide/cps24-2-0vdraconfigurationguide/m_dynamic-transport-selection-based-on-transaction-or-origin-host.html?bookSearch=true#Cisco_Reference.dita_29f6b345-85b3-4286-9d10-3b7af0ba5df0.

Different Types of WPS Call

1. WPS P1 call: call is considered as P1 call if Application function (AF) triggers Authorization/Authentication Request (AAR) with Reservation priority:14/15 and MPS Identifier.
2. WPS P2: call is considered as P2 call if AF triggers AAR with Reservation priority:13 and MPS Identifier.
3. WPS P3: call is considered as P3 call if AF triggers AAR with Reservation priority:11/12 and MPS Identifier. CPS will not choose RED channel for P3 call.

Abbreviations

AAA: Authorization/Authentication Answer

STR:Session Termination Request

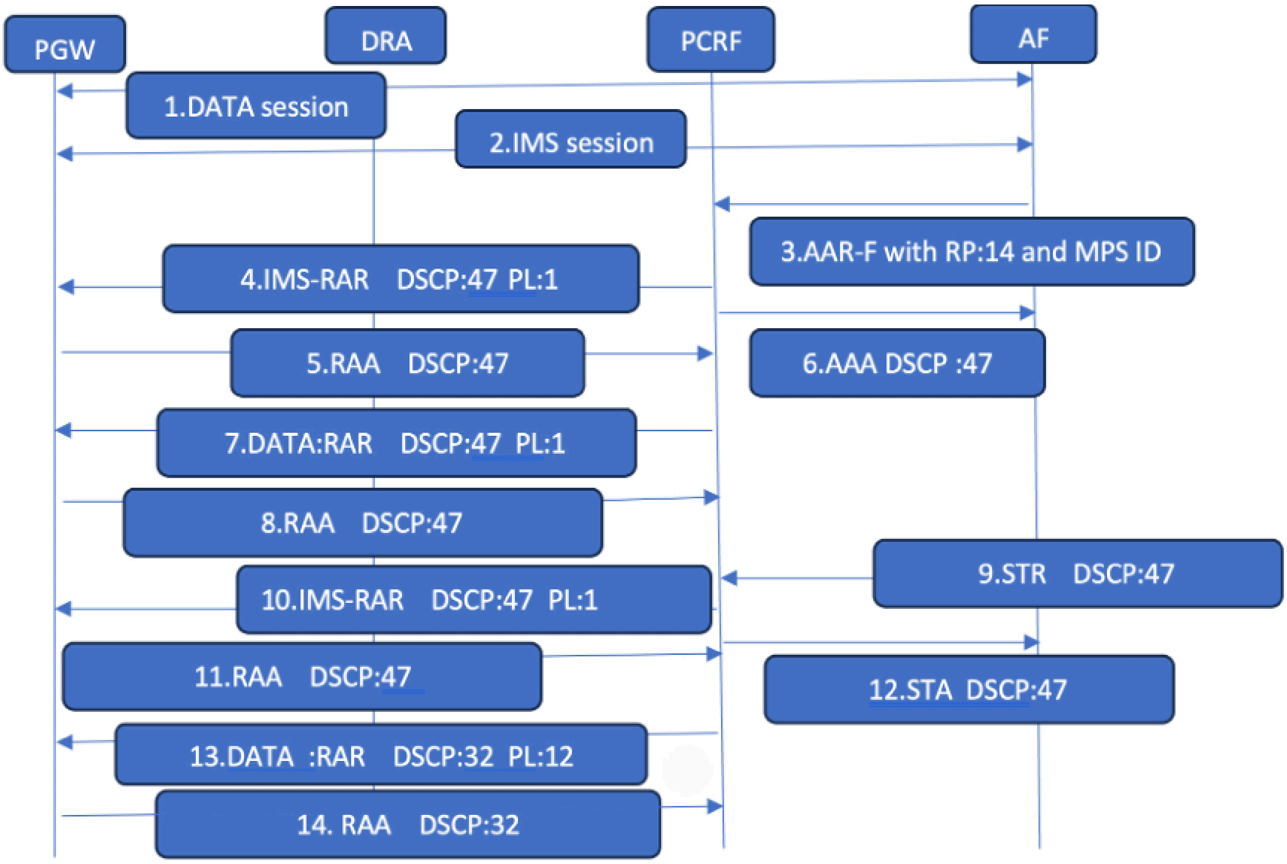
RAR: Re-Auth Request

RAA: Re-Auth Answer

Gx and Rx Call Flow

1. Initiate data and IP Multimedia Subsystem (IMS) default bearer.
2. AF triggers Authorization/Authentication Request Final (AAR-F) with Reservation priority:14/15/13 and MPS Identifier towards PCRF on Rx interface.
3. Now CPS will uplift both data and IMS bearer with Priority Level (PL):1 if Reservation priority is 14/15 in AAR-F, PL:2 if Reservation priority is 13 in AAR-F and selects RED channel.
4. Then CPS will take decision to move traffic on RED channel over Gx and Rx interface for data and IMS session.
5. AF triggers termination request to PCRF then CPS will terminate Rx session and downgrade Priority level of data session to original value.
6. All traffic starts to move on GREEN channel for data session as WPS session is terminated.

Call Flow with Reservation Priority 14



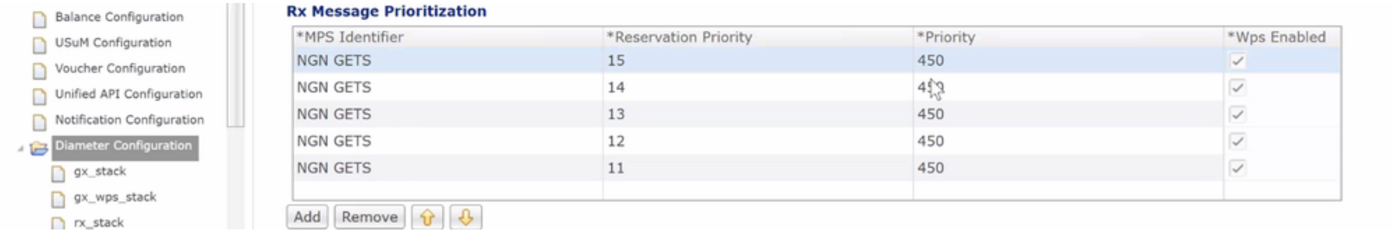
Call_Flow_With_RP_14

WPS Related Configuration in PCRF Policy Builder GUI

1.Enabling WPS based on MPS ID and Reservation Priority.

When CPS receives AAR-F from AF on Rx interface, CPS will evaluate MPS Identifier and Reservation priority AVP values matches with Next Generation Network (NGN) GETS and 15/14/13 then CPS will enable WPS from WPS enabled column.

MPS Identifier	This table will match MPS ID AVP sent from AF in AAR-F request to PCRF over Rx interface.
Reservation priority	This table will match a AVP sent from AF in AAR-F request to PCRF over Rx interface.
Priority	This is priority to be assigned to sessions before enabling WPS.
WPS enabled	Based on MPS Identifier and Reservation priority CPS will enable WPS.



Rx Message Prioritization

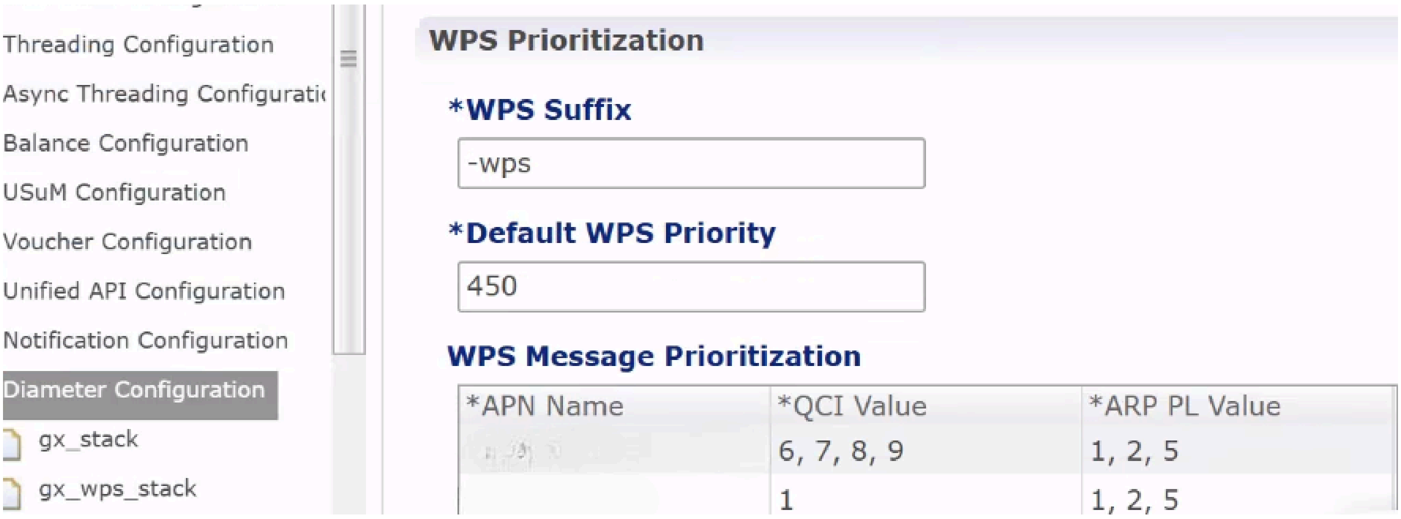
*MPS Identifier	*Reservation Priority	*Priority	*Wps Enabled
NGN GETS	15	450	✓
NGN GETS	14	450	✓
NGN GETS	13	450	✓
NGN GETS	12	450	✓
NGN GETS	11	450	✓

Enabling WPS

2.Suffix origin host with -WPS.

Once WPS is enabled for session, CPS will suffix origin host with -WPS and enforce PL:1/2/5 based on Reservation priority.

Access Point Name (APN) name	CPS will match APN name from APN table.
Quality of Service Class Identifier (QCI)	Match QCI from QCI table.
ARP PL value	Enforce PL 1, 2, or 5 from this table; here it is 1.
WPS suffix	Apply suffix in origin host name.



WPS Prioritization

*WPS Suffix

-wps

*Default WPS Priority

450

WPS Message Prioritization

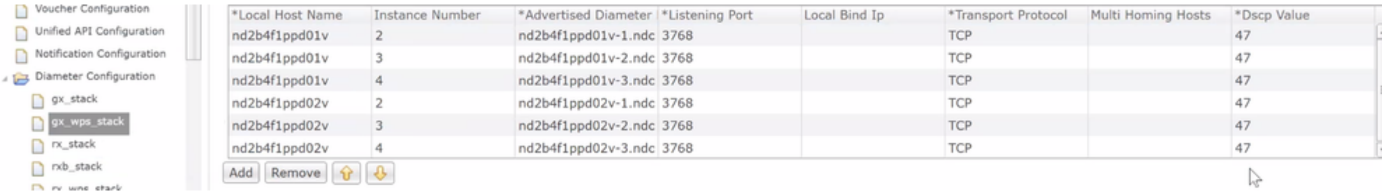
*APN Name	*QCI Value	*ARP PL Value
[redacted]	6, 7, 8, 9	1, 2, 5
	1	1, 2, 5

Suffix_WPS

3. Enabling DSCP marking to 47. This will move traffic to RED channel.

Once CPS uplifts data and IMS session with PL to 1/2. It will mark DSCP value to 47 for TCP traffic for both IMS and data sessions and now CPS will send out control plane traffic on RED channel to DRA/Packet Data Network Gateway (PGW) for both sessions.

Local hostname	Hostname of PCRF clients.
Instance number	VM instance of PCRF clients.
Listening port	Diameter PCRF port; here it is 3768.
Transport protocol	A set of rules and procedures how data is transmitted between different applications on a network; here it is TCP.
DSCP Value	A numerical identifier, ranging from 0 to 63, used within the IP header to classify and prioritize network traffic for QoS; here it is 47.



*Local Host Name	Instance Number	*Advertised Diameter	*Listening Port	Local Bind Ip	*Transport Protocol	Multi Homing Hosts	*Dscp Value
nd2b4f1ppd01v	2	nd2b4f1ppd01v-1.ndc	3768		TCP		47
nd2b4f1ppd01v	3	nd2b4f1ppd01v-2.ndc	3768		TCP		47
nd2b4f1ppd01v	4	nd2b4f1ppd01v-3.ndc	3768		TCP		47
nd2b4f1ppd02v	2	nd2b4f1ppd02v-1.ndc	3768		TCP		47
nd2b4f1ppd02v	3	nd2b4f1ppd02v-2.ndc	3768		TCP		47
nd2b4f1ppd02v	4	nd2b4f1ppd02v-3.ndc	3768		TCP		47

Enable_WPS_DSCP_47

Closure

The WPS feature within LTE Core network exemplifies how modern networks can evolve to meet the high-stakes demands of emergency services and national security. By introducing dedicated priority channels and adaptive configurations, WPS not only enhances the responsiveness of critical communications but also fortifies the networks ability to handle essential data flow under adverse conditions.

In a world where secure, timely communication can make all the difference, WPS stands as a key technology, ensuring that First Responders can depend on fast, uninterrupted connectivity when it matters most.