



# Wireless Priority Services

- [Feature Summary and Revision History, on page 1](#)
- [Feature Description, on page 2](#)
- [How it Works, on page 7](#)
- [Configuring Wireless Priority Services, on page 7](#)

## Feature Summary and Revision History

### Summary Data

*Table 1: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 2: Revision History*

Revision Details	Release
The Wireless Priority Services feature is fully qualified in this release.	2020.03.0
First introduced. This feature is not fully qualified in this release. For more information, contact your Cisco Account representative.	2020.02.0

## Feature Description

The Wireless Priority Services (WPS) feature is supported on the SMF+PGW-C over 5GC. The SMF+PGW-C validates prioritization of WPS services for Session Creation/Modification and various handover scenarios. It also evaluates the WPS services for Paging-Policy Differentiation for Network Triggered Service Request procedures.

## Use Cases

The WPS feature implements the 3GPP recommendations for wireless priority support for the following use cases in 5GS and EPS. The use cases are defined as per *3GPP TS 23.501 (sections 5.16.3, 5.16.4, 5.16.5, 5.16.6, 5.19, and 5.21)*.

WPS supports the following use cases:

- [Multimedia Priority Services](#) , on page 2
- [Mission Critical Services](#), on page 5
- [Expanded Prioritization for VoLTE/VoNR/Emergency Calls](#), on page 6
- [DSCP Marking for N3/S5-U/S2-B over PFCP](#), on page 6

## Multimedia Priority Services

The Multimedia Priority Service (MPS) allows priority access to system resources to Service Users, creating the ability to deliver or complete sessions of a high priority nature. Service Users are government-authorized personnel, emergency management officials and/or other authorized users. MPS supports priority sessions on an "end-to-end" priority basis. MPS includes signalling priority and media priority.

MPS provides the ability to invoke, modify, maintain and release sessions with priority, and deliver the priority media packets under network congestion conditions.

All MPS-subscribed UEs get priority for QoS Flows (for example, used for IMS signalling) when established to the DN that is configured to have priority for a given Service User by setting MPS-appropriate values in the QoS profile in the UDM. Service Users are treated as On Demand MPS subscribers and not On Demand MPS subscribers, based on regional/national regulatory requirements. On Demand service is based on Service User invocation/revocation explicitly and applied to the media QoS Flows being established. Not On Demand MPS service does not require invocation and provides priority treatment for all QoS Flows only to the DN that is configured to have priority for a given Service User after attachment to the 5G network.

Priority treatment for MPS includes priority message handling for Mobility Management procedures. Priority treatment for MPS session requires appropriate ARP and 5QI setting for QoS Flows according to the operator's policy.

MPS priority mechanisms can be classified as subscription-related and invocation-related. Subscription related mechanisms are divided into - always applied and conditionally applied. Invocation-related mechanisms are divided into - for mobile originated SIP call/sessions, for mobile terminated SIP call/sessions and for Priority PDU connectivity services.

Subscription-related mechanisms that are conditionally applied include:

**UDM:** One or more ARP priority levels are assigned for prioritized or critical services. The ARP of the prioritized QoS Flows for each DN is set to an appropriate ARP priority level.

**PCF:** The "IMS Signalling Priority" information is set for the subscriber in the UDM, and the PCF modifies the ARP of the QoS Flow used for IMS signalling.

## On-Demand MPS Service

The invocation-related priority mechanisms for prioritized services are based on interaction with an Application Server and between the Application Server and the PCF over Rx/N5 interface (as described in *3GPP TS 23.228, clause 5.21* in the case of MPS using IMS).

Invocation-related mechanisms for Mobile Originations (for example, via SIP/IMS) are explained below:

- PCF:
  - When an indication for a session arrives over the Rx/N5 interface and the UE does not have priority for the signaling QoS Flow, the PCF derives the ARP and 5QI parameters plus associated QoS characteristics as appropriate, as per the Service Provider policy (specified in *clause 6.1.3.11* of *3GPP TS 23.503*).
  - For MPS sessions, when establishing or modifying a QoS Flow as part of the session origination procedure, the PCF selects the ARP and 5QI parameters plus associated QoS characteristics as appropriate, to provide priority treatment to the QoS Flows.
  - When all active sessions to a particular DN are released and the UE is not configured for priority treatment to that particular PDU session, the PCF downgrades the IMS Signaling QoS Flows from appropriate settings of the ARP and 5QI parameters plus associated QoS characteristics as appropriate, to those entitled by the UE based on subscription.

Invocation-related mechanisms for Mobile Terminations (for example, via SIP/IMS) are explained below:

- PCF: When an indication for a session arrives over the Rx/N5 interface, the mechanisms as described above for Mobile Originations are applied.
- UPF: If an IP packet arrives at the UPF for a UE that is CM-IDLE, the UPF sends a "Data Notification" including the information to identify the QoS Flow for the DL data packet to the SMF (specified in *clause 4.2.3.3* of *3GPP TS 23.502*).
- SMF: If a "Data Notification" message arrives at the SMF for a QoS Flow associated with an ARP priority level value for priority use, delivery of priority indication during the Paging procedure is provided by inclusion of the ARP in the N11 interface "N1N2MessageTransfer" message (specified in *clause 4.2.3.3* of *3GPP TS 23.502*).
- AMF: If an "N1N2MessageTransfer" message arrives at the AMF containing an ARP priority level value for priority use, the AMF handles the request with priority and includes the "Paging Priority" IE in the N2 "Paging" message set to a value assigned to indicate that there is an IP packet at the UPF entitled to priority treatment (specified in *clause 4.2.3.3* of *3GPP TS 23.502*).
- SMF: For a UE that is not configured for priority treatment, upon receiving the "N7 Session Management Policy Modification" message from the PCF with an ARP priority level for priority use, the SMF sends an "N1N2MessageTransfer" to update the ARP for the Signaling QoS Flows (specified in *clause 4.3.3.2* of *3GPP TS 23.502*).
- AMF: Upon receiving the "N1N2MessageTransfer" message from the SMF with an ARP priority level for priority use, the AMF updates the ARP for the Signaling QoS Flows (specified in *clause 4.3.3.2* of *3GPP TS 23.502*).

- (R)AN: Inclusion of the "Paging Priority" in the N2 "Paging" message triggers priority handling of paging in times of congestion at the (R)AN (specified in *clause 4.2.3.3 of 3GPP TS 23.502*).

Invocation-related mechanisms for the Priority PDU connectivity services:

- PCF:
  - If the state of the Priority PDU connectivity services is modified from disabled to enabled, the QoS Flows controlled by the Priority PDU connectivity services are established/modified to have the service appropriate settings of the ARP and 5QI parameters plus associated QoS characteristics as appropriate, using the PDU Session Modification procedure (specified in *clause 4.3.3 of 3GPP TS 23.502*).
  - If the state of Priority PDU connectivity services is modified from enabled to disabled, the QoS Flows controlled by the Priority PDU connectivity services are modified from service appropriate settings of the ARP and 5QI parameters plus associated QoS characteristics as appropriate, to those entitled by the UE as per subscription, using the PDU Session Modification procedure (specified in *clause 4.3.3 of 3GPP TS 23.502*).

### Message-Priority Indication over GTP-C

An overloaded node performs message prioritization when handling incoming messages during an overloaded condition based on the relative GTP-C message priority signaled in the GTP-C header.

When message throttling is performed:

- GTP requests related to priority traffic (eMPS as described in *3GPP TS 22.153*) and emergency have the highest priority. Depending on regional/national requirements and network operator policy, these GTP requests are the last to be throttled when applying traffic reduction. The priority traffic is exempted from throttling due to GTP overload control up to the point where the requested traffic reduction cannot be achieved without throttling the priority traffic.
- For other types of sessions, message throttling considers the relative priority of the messages so that low priority messages are considered for throttling before the other messages. The relative priority of the messages is derived from the relative priority of the procedure for which the message is being sent (as specified in *clause 12.3.9.3.2*) or derived from the session parameters such as APN and ARP.

The high priority messages are given lower preference to throttle and low priority messages are given higher preference to throttle. An overloaded node also applies these message prioritization schemes when handling incoming initial messages during an overloaded condition, as part of the self-protection mechanism.

A sending GTP-C entity determines the relative message priority to signal in the message according to either procedure based or session parameters. If the message affects multiple bearers (for example, Modify Bearer Request), the relative message priority considers the highest priority ARP among all the bearers.

A GTP-C entity sets the same message priority in a Triggered message or Triggered Reply message as received in the corresponding Initial message or Triggered message respectively. For incoming GTP-C messages that do not have a message priority in the GTP-C header, the receiving GTP-C entity:

- Applies a default priority if the incoming message is an Initial message.
- Applies the message priority sent in the Initial message or Triggered message if the incoming message is a Triggered or Triggered Reply message respectively.

The nodes in the network homogeneously support this feature; otherwise an overloaded node processes initial messages received from the non-supporting nodes according to the default priority and processes initial messages received from the supporting nodes according to the message priority signaled in the GTP-C message.

### Message-Prioritization based on Session Parameters

Message prioritization is also performed based on the session parameters such as APN and ARP. The procedures and messages associated with the higher priority sessions are given lesser preference while throttling, as compared to the procedures and messages associated with the lower priority sessions. Within each group of sessions, the messages are further prioritized based on the category of the procedure for which the message is being sent.

### Message-Priority Header for PFCP

When the message throttling is performed:

- PFCP requests related to priority traffic (that is, eMPS as described in *3GPP TS 22.153*) and emergency have the highest priority. Depending on regional/national requirements and network operator policy, these PFCP requests are the last to be throttled when applying traffic reduction. Throttling exempts the priority traffic due to PFCP overload control up to the point where the requested traffic reduction cannot be achieved without throttling the priority traffic.
- For other types of sessions, the message throttling considers the relative priority of the messages so that the messages with low priority are first considered for the throttling. The relative priority of the messages is derived from the relative priority of the procedure for which the message is being sent or derived from the session parameters such as APN and ARP.

An overloaded node (UPF, SMF) may apply these message prioritization schemes when handling incoming initial messages during an overloaded condition, as part of a self-protection mechanism. Incoming messages are handled during an overloaded condition based on the relative PFCP message priority signaled in the PFCP header.

A PFCP entity determines whether to set and use the message priority in PFCP signalling, based on operator policy. A sending PFCP entity determines the relative message priority to signal in the message which are derived from the session parameters such as APN and ARP. If the message affects multiple bearers, the relative message priority is determined considering the highest priority ARP among all the bearers. A PFCP entity must set the same message priority in a Response message as received in the corresponding Request message.

For incoming PFCP messages that do not have a message priority in the PFCP header, the receiving PFCP entity:

- Applies a default priority if the incoming message is a Request message.
- Applies the message priority sent in the Request message if the incoming message is a Response message.

The SMF and UPF functions in the network homogeneously support this feature; otherwise an overloaded node will process the Request messages received from the non-supporting nodes according to the default priority and Request messages received from supporting nodes will be processed according to the message priority signalled in the PFCP message.

### Mission Critical Services

A Mission Critical Service (MCX Service) is a communication service that enables capabilities of Mission Critical Applications. The MCX service is provided to end users from Mission Critical Organizations and mission critical applications for businesses and organizations. An MCX Service is either Mission Critical

Push To Talk (MCPTT), Mission Critical Video (MCVideo), or Mission Critical Data (MCData) and represents a set of requirements between two or more MCX Service types.

MCX Services are based on the ability to invoke, modify, maintain, and release sessions with priority, and deliver the priority media packets under network congestion conditions. These services are supported in a roaming environment when roaming agreements are in place and where regulatory requirements apply.

An MCX subscription allows users to receive priority services if the network supports MCX. MCX Users require the 5GS functionality for real-time, dynamic, secure and limited interaction with the QoS and policy framework for modification of the QoS and policy framework by authorized users.

## Expanded Prioritization for VoLTE/VoNR/Emergency Calls

The SMF+PGW-C supports Expanded Prioritization for VoLTE/VoNR/Emergency calls. The National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority Services (NGN-PS) (formerly called NGN Government Emergency Telecommunications Service (GETS)) is a set of voice, video and data services that are based on services available from public packet-switched Service Providers. The NS/EP NGN-PS provides priority treatment for a Service User's NS/EP communications and is particularly needed when the Service Providers' networks are impaired due to congestion and/or damage from natural disasters (such as floods, earthquakes and hurricanes) and man-made disasters (such as physical, cyber or other forms of terrorist attacks).

As part of this feature, the PGW-C control message is marked with DSCP marking and also for control message belonging to the eMPS session or containing Allocation and Retention Priority (ARP) associated with the eMPS profile.

## DSCP Marking for N3/S5-U/S2-B over PFCP

### Transport Level Marking

Transport level marking is the process of marking traffic with a DSCP value based on the locally configured mapping from the QCI and optionally the ARP priority level. For EPC, the S-GW and P-GW perform transport level marking on a per EPS bearer basis. For 5GC, the S-GW and P-GW perform transport level marking on a per QoS flow basis.

The UPF performs transport level marking with a DSCP value based on the mapping from the 5QI, the Priority Level (if explicitly signaled), and optionally the ARP priority level configured at the SMF. The CP function controls transport level marking by providing the DSCP in the ToS or Traffic Class within the Transport Level Marking IE in the FAR (associated to the PDR matching the traffic to be marked).

The UP function performs transport level marking for the detected traffic and sends the marked packet to the peer entity. The CP function changes transport level marking by changing the Transport Level Marking IE in the related FAR.

## WPS Profile Support

The SMF+PGW-C supports the WPS profile defined with ARP and DSCP marking value to be set for GTP-C and PFCP Protocol IP-headers. The WPS profile sets the message priority in the GTP-C and PFCP protocols.

The SMF+PGW-C allows a maximum of 64 WPS profiles and each WPS profile will be associated under the DNN profile. See the [Configuring Wireless Priority Services, on page 7](#) section for more information.

# How it Works

## License Information

The WPS feature requires a license to be enabled on the SMF+PGW-C to support the related features - MPS, MCX, Prioritization for VoLTE/VoNR/Emergency Service. Contact your Cisco account representative for more information on how to obtain a license.

## Standards Compliance

The Wireless Priority Services feature complies with the following standards:

- 3GPP TS 22.153
- 3GPP TS 23.228
- 3GPP TS 23.282
- 3GPP TS 23.379
- 3GPP TS 23.501
- 3GPP TS 23.502
- 3GPP TS 23.503
- 3GPP TS 24.301

# Configuring Wireless Priority Services

This section describes how to configure the Wireless Priority Services feature.

## Configuring the WPS Profile

Use the following configuration to configure the WPS profile.

```
configure
  profile wps wps_profile_name
    arp arp_value
    dscp n3 n3_value
    message-priority [ gtpc pfcp ]
  end
```

### NOTES:

- **profile wps wps\_profile\_name**: Accesses the Wireless Priority Services Profile configuration. *wps\_profile\_name* must be an alphanumeric string of 1 to 63 characters.
- **arp arp\_value**: Specifies the range of ARP levels. *arp\_value* must be an integer from 1 to 15 separated either by "," or "-".

- **dscp n3 n3\_value**: Specifies the DSCP marking value for N3. *n3\_value* specifies the UP DSCP marking value within the range 0 to 0x3F.
- **message-priority { gtpc pfc }**: Specifies the message priority for GTP-C and PFCP.

### Verifying the WPS Profile Configuration

This section describes how to verify the WPS Profile configuration.

Execute the **show running-config** command to view the configuration.

The following is a sample output of the **show running-config** command.

```
show running-config profile wps wps1
profile wps wps1
arp 1,4-6,9
dscp n3 10
message-priority [ pfc gtpc ]
exit
```

## Associating WPS Profile under DNN Profile

Use the following configuration to associate the WPS profile with the configured DNN profile.

```
configure
  profile dnn intershat
    wps-profile wps_profile_name
  end
```

### NOTES:

- **wps-profile wps\_profile\_name**: Enables the Wireless Priority Services Profile configuration. This profile is configured under the existing DNN profile configuration.

### Verifying WPS Profile under DNN Profile

This section describes how to verify the WPS profile configuration under the DNN profile.

Execute the **show running-config** command to view the configuration.

The following is a sample output of the **show running-config** command.

```
show running-config profile dnn intershat
profile dnn intershat
network-element-profiles chf chf1
network-element-profiles amf amf1
network-element-profiles pcf pcf1
network-element-profiles udm udml
charging-profile chgprf1
virtual-mac b6:6d:47:47:47:47
wps-profile wps1
ssc-mode 2 allowed [ 3 ]
session type IPV4 allowed [ IPV6 IPV4V6 ]
upf apn intershat
exit
```



# WPS OAM Support

## SMF Session Gauge Counters

The "wps" label is introduced at the SMF service to account for session-level gauge counters that support WPS and non-WPS functionality.

For example:

```
smf_session_counters{always_on="disable",app_name="smf",cluster="smf",data_center="unknown",dnn="intershat",
instance_id="0",pdu_type="ipv4",rat_type="NR",service_name="smf-service",ssc_mode="ssc_mode_1",wps="non_wps"}
  10
smf_session_counters{always_on="disable",app_name="smf",cluster="smf",data_center="unknown",dnn="intershat",
instance_id="0",pdu_type="ipv4",rat_type="NR",service_name="smf-service",ssc_mode="ssc_mode_1",wps="wps"}
  20
```

## N4 Interface Metrics

The N4 interface counters related to message priority include:

- N4\_MSG\_SESSION\_DELETION\_REQUEST
- N4\_MSG\_SESSION\_ESTABLISHMENT\_REQUEST
- N4\_MSG\_SESSION\_MODIFICATION\_REQUEST

An example of the N4 interface metrics:

```
smf_proto_pfcpc_msg_total{app_name="SMF",cluster="Local",data_center="DC",instance_id="0",
message_direction="outbound",message_name="N4_MSG_SESSION_DELETION_REQUEST",msgpriority=true,
service_name="smf-protocol",status="accepted",transport_type="origin"} 4
smf_proto_pfcpc_msg_total{app_name="SMF",cluster="Local",data_center="DC",instance_id="0",
message_direction="outbound",message_name="N4_MSG_SESSION_ESTABLISHMENT_REQUEST",msgpriority=true,
service_name="smf-protocol",status="accepted",transport_type="origin"} 6
smf_proto_pfcpc_msg_total{app_name="SMF",cluster="Local",data_center="DC",instance_id="0",
message_direction="outbound",message_name="N4_MSG_SESSION_MODIFICATION_REQUEST",msgpriority=true,
service_name="smf-protocol",status="accepted",transport_type="origin"} 20
```

## GTPv2 Metrics

The GTPv2 counters related to message priority include:

- NumCreateBearerSuccess
- NumRxCreateBearerRes
- NumTxCreateSessionReq

An example of the GTPv2 metrics:

```
smf_gtpc_app_priority_events{app_name="SMF",cluster="Local",data_center="DC",
event_type="NumCreateBearerSuccess",instance_id="0",priority_msg="true",service_name="gtpc-ep"}
  2
smf_gtpc_app_priority_events{app_name="SMF",cluster="Local",data_center="DC",
event_type="NumRxCreateBearerRes",instance_id="0",priority_msg="true",service_name="gtpc-ep"}
  2
smf_gtpc_app_priority_events{app_name="SMF",cluster="Local",data_center="DC",
event_type="NumTxCreateSessionReq",instance_id="0",priority_msg="true",service_name="gtpc-ep"}
  2
```

