



Ultra Cloud Core 5G User Plane Function, Release 2020.02 - Configuration and Administration Guide

First Published: 2020-04-30

Last Modified: 2021-10-08

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 NON-INFRINGEMENT 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)

© 2020-2021 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

About this Guide	xv
Conventions Used	xv

CHAPTER 1

5G Architecture	1
Feature Summary and Revision History	1
Summary Data	1
Revision History	1
Overview	2
Control Plane Network Functions	2
User Plane Network Function	2
Subscriber Microservices Infrastructure Architecture	3
Control Plane Network Function Architecture	4

CHAPTER 2

5G-UPF Overview	7
Feature Summary and Revision History	7
Summary Data	7
Revision History	7
Product Description	8
Use Cases and Features	8
Configuration and Deployment Requirement for UPF	8
Anchor Point for Intra-RAT and Inter-RAT Mobility	9
External PDU Session Point of Interconnect to Data Network	9
Packet Inspection	10
User Plane Part of Policy Rule Enforcement	10
Lawful Intercept	10
Traffic Usage Reporting (Charging)	10

	QoS Handling for User Plane	11
	Downlink Packet Buffering and Data Notification Triggering	11
	Forwarding End Markers to the Source NG-RAN Node	11
	Deployment Architecture and Interfaces	11
	UPF Architecture	11
	UPF Deployment Architecture	12
	Supported Interfaces	14
	License Information	15
	Standards Compliance	15
<hr/>		
PART I	Features and Functionality	17
<hr/>		
CHAPTER 3	1:1 Redundancy	19
	Feature Summary and Revision History	19
	Summary Data	19
	Revision History	19
	Feature Description	20
	How it Works	20
	Configuring 1:1 UPF Redundancy	25
	Configuring BFD Monitoring Between Active UPF and Standby UPF	25
	Configuring BGP Status Monitoring Between Each UPF and Next-Hop Router	25
	Configuring Sx/N4 Monitoring on the Active UPF and Standby UPF	26
	Configuring VPP Monitor on Active UPF and Standby UPF	27
	Preventing User Plane Function Switchback	27
	Preventing Dual Active Error Scenarios	28
	Resetting Sx/N4 Monitor Failure	28
	Changing UPF State from Pending-Active to Active	29
	Monitoring and Troubleshooting	29
	Show Command(s) and/or Outputs	29
	show srp monitor bfd	29
	show srp monitor bgp	29
	show srp monitor sx	29
	show srp monitor vpp	30

CHAPTER 4	APN ACL Support	31
	Feature Summary and Revision History	31
	Summary Data	31
	Revision History	31
	Feature Description	32
	Rule(s)	32
	Actions	32
	Criteria	33
	Rule Order	33
	Limitations	33
	Configuring ACL	34
	Verifying ACL Configuration	34
	IP Source Violation	34
	Gating Control	35

CHAPTER 5	Bulk Statistics Support	37
	Feature Summary and Revision History	37
	Summary Data	37
	Revision History	37
	Feature Description	37

CHAPTER 6	Collection and Reporting of Usage Data over N4 Interface	41
	Feature Summary and Revision History	41
	Summary Data	41
	Revision History	41
	Feature Description	42
	How it Works	42
	Standards Compliance	43
	Configuration to Collect and Report Volume Measurement over N4 Interface	43
	Configuring Charging Action for a Required Billing Action	43
	Associating a Charging Action with a Rulebase	43

CHAPTER 7	Control Plane-Initiated N4 Association Support	45
------------------	---	-----------

- Feature Summary and Revision History 45
 - Summary Data 45
 - Revision History 45
- Feature Description 46
 - SMF initiated N4 Association Setup Procedure 46
- How it Works 46
 - Call Flows 46
 - Session Management Function Initiated N4 Association Setup Procedure 46
- Configuring the CP-Initiated N4 Association Setup Feature 46
 - CP-Initiated N4 Association Setup Feature OAM Support 47
 - Show Command Support 47

CHAPTER 8

Charging Support 49

- Feature Summary and Revision History 49
 - Summary Data 49
 - Revision History 49
- Feature Description 50
 - Offline Charging Events Reporting over N4 50
 - Online Charging Support over N4 50
- How it Works 50
 - Call Flows 50
 - PFCP Session Establishment Procedure 50
 - PFCP Session Modification Procedure 51
 - PFCP Session Reporting Procedure 52
 - PFCP Session Deletion Procedure 53
 - IEs Supported for Offline Charging Reporting 54
 - IEs Supported for Online Charging Reporting 55
 - Usage Reporting in PFCP Modification Response 56
 - Usage Reporting for Online and Offline Charging 56
 - Usage Reporting with Rating-Group and Service ID 56
 - Implementing the QAURR Flag 57
- Configuring Credit Control for Usage Reporting 57
- Configuring ACS Rulebase for Usage Reporting 57

CHAPTER 9	Deep Packet Inspection and Inline Services	61
	Feature Summary and Revision History	61
	Summary Data	61
	Revision History	61
	Feature Description	62
	How it Works	62
	DSCP Marking for Downlink and Uplink Packets	62
	Transport Level Marking IE	62
	Transport Level Marking Options IE	63
	Inner Packet Marking IE	63
	Traffic Readdressing or Redirecting	64
	Redirect Information IE	65
	Supported Inline Services	65
	Application Detection and Control	65
	Content Filtering	66
	DNS Snooping	66
	Event Data Records	68
	Feature Description	68
	How It Works	68
	Configuring Event Data Records	70
	Monitoring and Troubleshooting	71
	Flow Idle Timeout Randomization	72
	Configuring Flow Idle Timeout Randomization in ACS	73
	HTTP URL Filtering	73
	L7 Protocol	76
	DNS	76
	FTP	76
	HTTP	76
	HTTPS	78
	RTP/RTSP	78
	SIP	78
	Monitoring and Troubleshooting	79
	Tethering Detection	80

- Feature Description 80
- Configuring Tethering Support 80
- Monitoring and Troubleshooting 81
- URL Blacklisting 82
 - Feature Description 82
 - How it Works 82
 - Configuring URL Blacklisting 83
 - Monitoring and Troubleshooting 84
- Configuring the Static and Pre-Defined Rules 86
- Configuring ACS Ruledef for L7 Protocols for DPI 87
- Charging Action Configuration for L7 Protocols for DPI 89

CHAPTER 10

Dynamic and Static PCC Rules 93

- Feature Summary and Revision History 93
 - Summary Data 93
 - Revision History 94
- Feature Description 94
 - How it Works 94
 - Predefined PCC Rules Support 94
 - Provisioning of Predefined PCC Rules 94
 - Dynamic PCC Rules Support 95
 - Rate Limiting for Static and Predefined Rules 96
 - Rate Limiting for Dynamic Rules 97
 - Standards Compliance 98
 - Configuring the URR IDs 98
 - Threshold Configuration 99

CHAPTER 11

GTP-U Support 101

- Feature Summary and Revision History 101
 - Summary Data 101
 - Revision History 101
- Feature Description 102
- How it Works 103
 - Call Flows 103

	Initial Attach on E-UTRAN via MME and S-GW	103
	5G to EPS Handover with N26 Interface	104
	Error Indication Handling on UPF	105
	GTP-U Path Failure Support at UPF	105
<hr/>		
CHAPTER 12	Idle Mode Buffering and Paging	107
	Feature Summary and Revision History	107
	Summary Data	107
	Revision History	107
	Feature Description	108
	How it Works	108
	Provisioning of Buffering Action Rule in the UPF	108
	Buffering Action Rule Call Flow	108
	Downlink Data Report for First DL Packet	109
	Paging Policy Differentiation	109
	Paging Policy Indicator (PPI)	109
	Frame Format for the PDU Session User Plane Protocol	110
	QoS Flow Identifier (QFI)	110
	Paging Policy Presence	110
	Paging Policy Indicator	110
<hr/>		
CHAPTER 13	N3 Transfer of PDU Session Information	111
	Feature Summary and Revision History	111
	Summary Data	111
	Revision History	111
	Feature Description	111
	How it Works	112
	Transfer of PDU Session Information for Downlink Data Packets	112
	Transfer of PDU Session Information for Uplink Data Packets	112
	PDU Session Information Frame IEs	113
	Standards Compliance	114
	Limitations	114
<hr/>		
CHAPTER 14	N4 Interface Compliance with 3GPP Specification	115

Feature Summary and Revision History 115

- Summary Data 115
- Revision History 115

Feature Description 116

- Averaging Window 116
- Paging Policy Indicator 116
- Outer Header Creation 117
- Outer Header Removal 118

CHAPTER 15

N4 Interface Configuration 121

Feature Summary and Revision History 121

- Summary Data 121
- Revision History 121

Feature Description 122

Configuring N4 Interface 122

- Identifying an N4 Interface 122
- Modification of N4-type Parameters in an Sx Service 122
- Statistics 123
 - show control-plane-group 123
 - show sx-service all 123
 - show subscribers user-plane-only all 123
 - show user-plane-service statistics all 123
 - show subscribers user-plane-only seid number pdr all 123
 - show subscribers user-plane-only callid number pdr full all 124

CHAPTER 16

N4 Session Management, Node Level, and Reporting Procedures 125

Feature Summary and Revision History 125

- Summary Data 125
- Revision History 125

Feature Description 126

N4 Session Management, Node Level, and Reporting Procedures 126

- N4 Node-level Procedures 126
- N4 Session Management 126
- N4 Session/Node-level Reporting Procedures 126

Relationships	126
End Marker Support	127
UEs IPv4, IPv6, and IPv4v6 Support	127
How it Works	127
N4 Node-level Procedure Call Flows	127
N4 Association Setup Procedure Call Flow	127
N4 Association Update Procedure Call Flow	128
N4 Association Release Procedure Call Flow	128
N4 Heartbeat Procedure	129
N4 Session Management Procedures Call Flows	129
N4 Session Establishment Call Flow	129
N4 Session Modification Call Flow	130
N4 Session Delete Call Flow	131
N4 Session/Node Level Reporting Procedure Call Flows	131
Session Level Reporting Due to the GTP-u Error Indication Call Flow	131
Node-level Reporting Procedure due to GTP-u Path Failure Call Flow	132
UEs IPv4, IPv6, and IPv4v6 Support Call Flows	134
N4 Session Establishment and Modification Procedure for IPv6 Call Flow	134
N4 Session Establishment and Modification Procedure for IPv4v6 Call Flow	135
Configuring the N4 Session/Node Level Reporting Procedures	136
Enabling the GTP-u Echo Request Procedure	136
Verifying the N4 Session/Node Level Reporting Procedure Configuration	137
N4 Session Node Level Reporting Procedure OA and M Support	137
SNMP Traps	138

CHAPTER 17	UPF Ingress Interface	139
	Feature Summary and Revision History	139
	Summary Data	139
	Revision History	139
	Feature Description	140
	Configuring UPF Ingress Interface Type Support	140
	Verifying the UPF Ingress Interface Type Feature Configuration	140

CHAPTER 18	UPF Local Configuration	141
-------------------	--------------------------------	------------

- Feature Summary and Revision History 141
 - Summary Data 141
 - Revision History 141
- Feature Description 142
 - How it Works 142
- Configuring the Local Configuration Support for UPF 143

CHAPTER 19 **UPF Reporting of Load Control Over N4 Interface 145**

- Feature Summary and Revision History 145
 - Summary Data 145
 - Revision History 145
- Feature Description 145
 - Supported IE and Messages 146
 - Reporting Load Information to SMF 146
- Configuring the Max Sessions 147
 - Show Command Support 147

CHAPTER 20 **Session Recovery 149**

- Feature Summary and Revision History 149
 - Summary Data 149
 - Revision History 149
- Feature Description 149
- How it Works 150
- Configuring the System to Support Session Recovery 150
 - Enabling Session Recovery 150
 - Enabling Session Recovery on an Out-of-Service System 150
 - Enabling Session Recovery on an In-Service System 151
 - Disabling the Session Recovery Feature 152
 - Viewing Session Recovery Status 152
 - Viewing Recreated Session Information 153

CHAPTER 21 **Voice over New Radio 155**

- Feature Summary and Revision History 155
 - Summary Data 155

Revision History	155
Feature Description	155
How it Works	156
VoNR Call Flow for UPF	156

PART II**Troubleshooting Information 157**

CHAPTER 22**UPF Troubleshooting Information 159**

Debug Logging	159
Monitoring CLI	160
Monitoring Protocol	160
RAT Type-based Statistics	160
Subscriber Level CLI	165
VPP Statistics	165
SNMP Support	166
Troubleshooting UPF Features	167

PART III**UPF Sample Basic Configuration 169**

CHAPTER 23**Sample UPF Configuration 171**

Sample Configuration	171
----------------------	-----



About this Guide



Note Control and User Plane Separation (CUPS) represents a significant architectural change in the way StarOS-based products are deployed in the 3G, 4G, and 5G networks. This document provides information on the features and functionality specifically supported by this 5G UPF product deployed in a 5G network. It should not be assumed that features and functionality that have been previously supported in legacy or non-CUPS products are supported by this product. References to any legacy or non-CUPS products or features are for informational purposes only. Furthermore, it should not be assumed that any constructs (including, but not limited to, commands, statistics, attributes, MIB objects, alarms, logs, services) referenced in this document imply functional parity with legacy or non-CUPS products. Please contact your Cisco Account or Support representative for any questions about parity between this product and any legacy or non-CUPS products.



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. 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 preface describes the *5G User Plane Function Guide*, how it is organized and its document conventions.

This guide describes the Cisco User Plane Function (UPF) and includes infrastructure and interfaces, feature descriptions, specification compliance, session flows, configuration instructions, and CLI commands for monitoring and troubleshooting the system.

- [Conventions Used, on page xv](#)

Conventions Used

The following tables describe the conventions used throughout this documentation.

Notice Type	Description
Information Note	Provides information about important features or instructions.

Notice Type	Description
Caution	Alerts you of potential damage to a program, device, or system.
Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.

Typeface Conventions	Description
Text represented as a <code>screen display</code>	This typeface represents displays that appear on your terminal screen, for example: <code>Login:</code>
Text represented as commands	This typeface represents commands that you enter, for example: show ip access-list This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a command <i>variable</i>	This typeface represents a variable that is part of a command, for example: show card <i>slot_number</i> <i>slot_number</i> is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the File menu, then click New



CHAPTER 1

5G Architecture

- [Feature Summary and Revision History, on page 1](#)
- [Overview, on page 2](#)
- [Subscriber Microservices Infrastructure Architecture, on page 3](#)
- [Control Plane Network Function Architecture, on page 4](#)

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or FunctionalArea	<ul style="list-style-type: none">• PCF• SMF• UPF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Overview

The Ultra Cloud Core is Cisco's solution supporting 3GPP's standards for 5G new radio (NR) standalone (SA) mode. These standards define various network functions (NFs) based on the separation of control plane (CP) and user plane (UP) (e.g. CUPS) functionality for increased network performance and capabilities.

Control Plane Network Functions

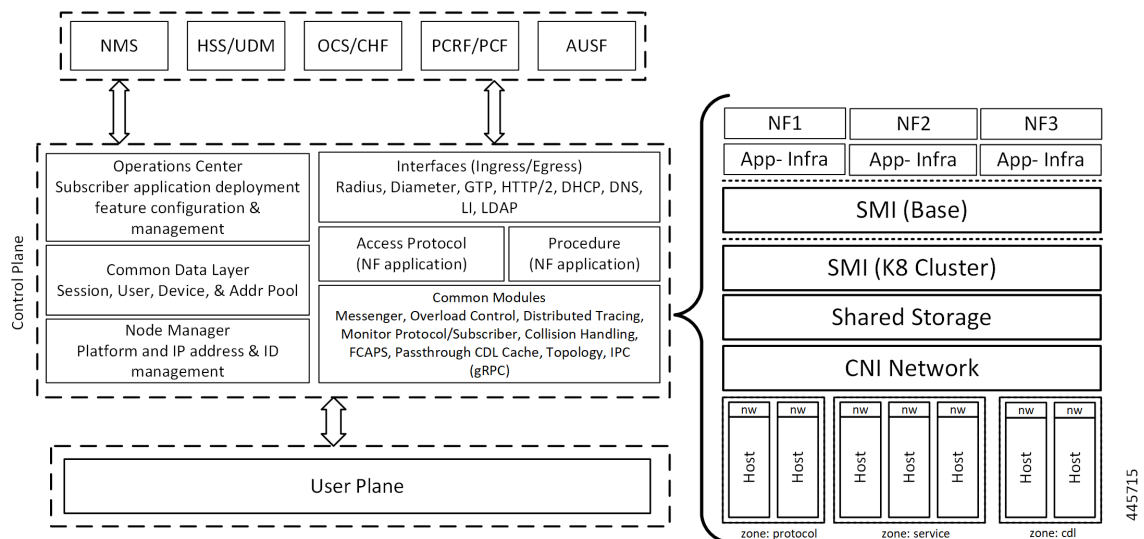
The CP-related NFs that comprise the Ultra Cloud Core are based on a common architecture designed around the following tenants:

- Cloud-scale — Fully virtualized for simplicity, speed, and flexibility
- Automation and orchestration — Optimized operations, service creation, and infrastructure
- Security — Multiple layers of security across the deployment stack from the infrastructure through the NF applications
- API exposure — Open and extensive for greater visibility, control, and service enablement
- Access agnostic — Support for heterogeneous network types (e.g. 5G, 4G, 3G, Wi-Fi, etc.)

These CP NFs are each designed as containerized applications (e.g. microservices) for deployment via the Subscriber Microservices Infrastructure (SMI).

The SMI defines the common application layers for functional aspects of the NF such as life cycle management (LCM), operations and management (OAM), and packaging.

Figure 1: Ultra Cloud Core CP Architectural Components



User Plane Network Function

The 5G UP NF within the Ultra Cloud Core is the User Plane Function. Unlike the CP-related NFs, the 5G UPF leverages the same Vector Packet Processing (VPP) technology currently in use by the user plane

component within Cisco's 4G CUPS architecture. This commonality ensures the delivery of a consistent set of capabilities between 4G and 5G such as:

- Ultra-fast packet forwarding
- Extensive integrated IP services such as Subscriber Firewall, Tethering, Deep-Packet Inspection (DPI), Internet Content Adaption Protocol (ICAP), Application Detection and Control (ADC), and header enrichment (HE)
- Integrated third-party applications for traffic and TCP optimization

For more information on UPF, refer to *Ultra Cloud Core 5G UPF Configuration and Administration Guide*.

Subscriber Microservices Infrastructure Architecture

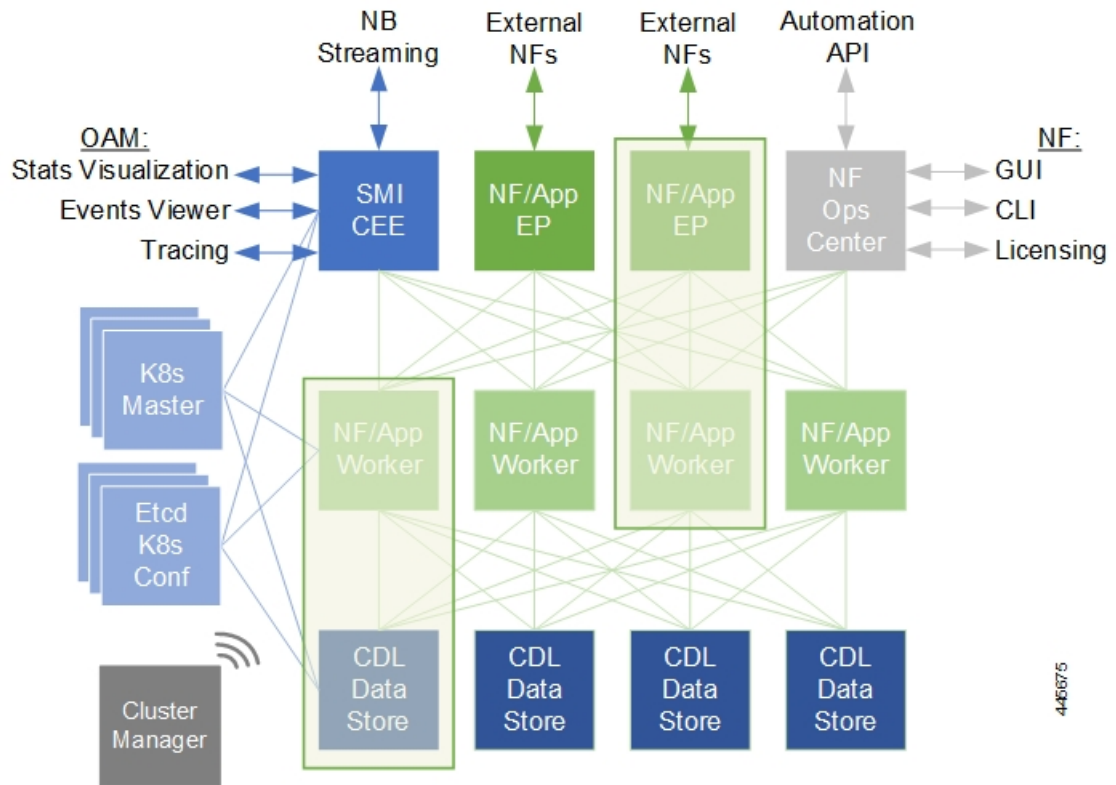
The Ultra Cloud Core Subscriber Microservices Infrastructure (SMI) is a layered stack of cloud technologies that enable the rapid deployment of, and seamless life-cycle operations for microservices-based applications.

The SMI stack consists of the following:

- SMI Cluster Manager—Creates the Kubernetes (K8s) cluster, creates the software repository, and provides ongoing LCM for the cluster including deployment, upgrades, and expansion.
- Kubernetes Management—Includes the K8s master and etcd functions, which provide LCM for the NF applications deployed in the cluster. This component also provides cluster health monitoring and resources scheduling.
- Common Execution Environment (CEE)—Provides common utilities and OAM functionalities for Cisco cloud native NFs and applications, including licensing and entitlement functions, configuration management, telemetry and alarm visualization, logging management, and troubleshooting utilities. Additionally, it provides consistent interaction and experience for all customer touch points and integration points in relation to these tools and deployed applications.
- Common Data Layer (CDL)—Provides a high performance, low latency, stateful data store, designed specifically for 5G and subscriber applications. This next generation data store offers HA in local or geo-redundant deployments.
- Service Mesh—Provides sophisticated message routing between application containers, enabling managed interconnectivity, additional security, and the ability to deploy new code and new configurations in low risk manner.
- NB Streaming—Provides Northbound Data Streaming service for billing and charging systems.
- NF/Application Worker nodes—The containers that comprise an NF application pod.
- NF/Application Endpoints (EPs)—The NF's/application's interfaces to other entities on the network.
- Application Programming Interfaces (APIs)—SMI provides various APIs for deployment, configuration, and management automation.

The following figure depicts how these components interconnect to comprise a microservice-based NF/application.

Figure 2: SMI Components



For more information on SMI components, refer to the [Ultra Cloud Core Subscriber Microservices Infrastructure documentation—Deployment Guide > Overview](#) chapter.

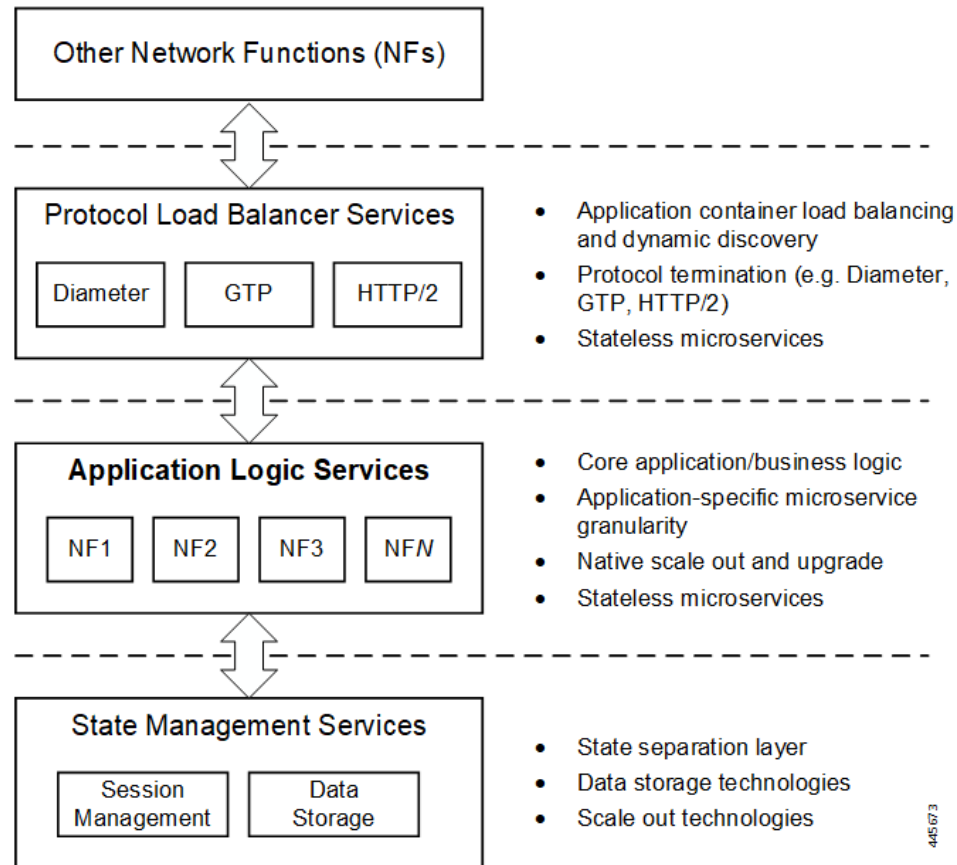
Control Plane Network Function Architecture

CP NFs are designed around a three-tiered architecture that take advantage of the stateful/stateless capabilities afforded within cloud native environments.

The architectural tiers are as follows:

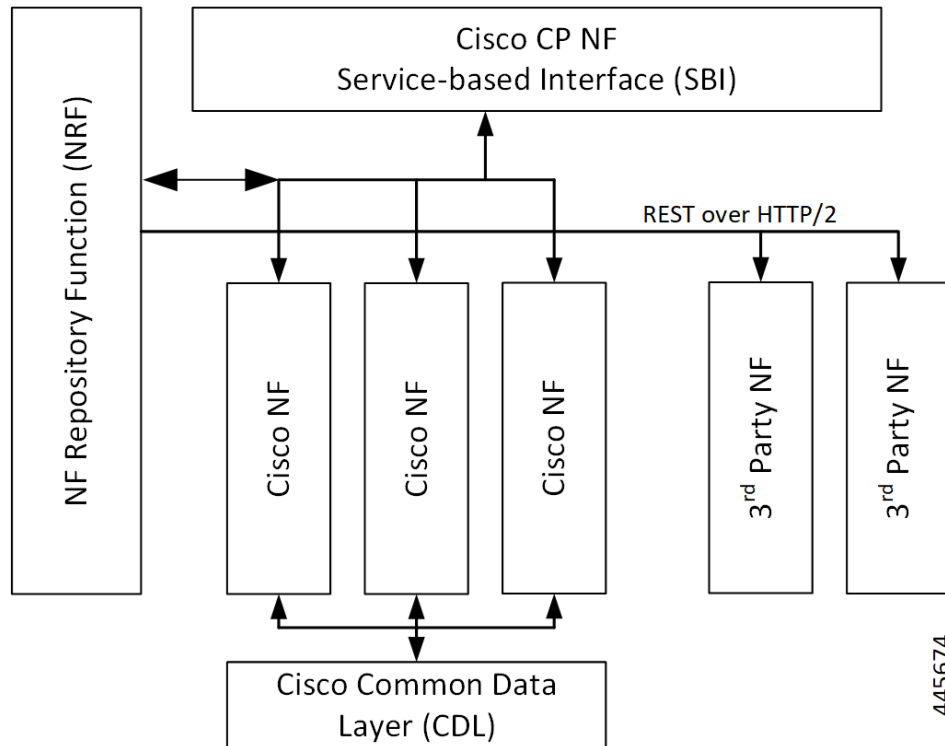
- Protocol Load Balancer Services — These are stateless microservices that are primarily responsible for dynamic discovery of application containers as well as for protocol proxy and/or termination. These include traditional 3GPP protocols and new protocols introduced with 5G.
- Applications Services — Responsible for implementing the core application/business logic, these are the stateless services that render the actual application based on the received information. This layer may contain varying degrees of microservice granularity. Application services are stateless.
- State management services — Enable stateless application services by providing a common data layer (CDL) to store/cache state information (e.g. session and subscriber data). This layer supports various data storage technologies from in-memory caches to full-fledge databases.

Figure 3: Control Plan Network Function Tiered Architecture



The three-tiered architecture on which Cisco's CP NFs are designed fully support the 5G core (5GC) Service-based Architecture (SBA) defined by 3GPP. These NFs communicate with each other and with third-party NFs over the Service-based Interface (SBI) using HTTP/2 over TCP as defined by 3GPP.

Figure 4: Cisco CP NF Service-based Architecture Support



For more information on the Cisco network functions, refer to the corresponding network function documentation.



CHAPTER 2

5G-UPF Overview

This chapter covers the following topics:

- [Feature Summary and Revision History, on page 7](#)
- [Product Description, on page 8](#)
- [Use Cases and Features, on page 8](#)
- [Deployment Architecture and Interfaces, on page 11](#)
- [License Information, on page 15](#)
- [Standards Compliance, on page 15](#)

Feature Summary and Revision History

Summary Data

Table 3: Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI
Feature Default Setting	Disabled – License Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 4: Revision History

Revision Details	Release
First introduced.	2020.02.0

Product Description

The User Plane Function (UPF) is one of the network functions (NFs) of the 5G core network (5GC). The UPF is responsible for packet routing and forwarding, packet inspection, QoS handling, and external PDU session for interconnecting Data Network (DN), in the 5G architecture.

UPF is a distinct Virtual Network Function (VNF) that offers a high-performance forwarding engine for the user traffic. Using Vector Packet Processing (VPP) technology, the UPF achieves ultra-fast packet forwarding while retaining compatibility with all the user plane functionality. For instance, Shallow Packet Inspection(SPI)/Deep Packet Inspection (DPI), traffic optimization, and inline services (NAT, Firewall, DNS snooping, and so on). UPF is currently designed to offer Integrated Deep Packet Based Inspection (DPI) Services.

A single instance of UPF provides some or all the following functionalities:

- Anchor point for Intra-RAT and Inter-RAT mobility (when applicable).
- External PDU session point of interconnect to Data Network.
- Packet routing and forwarding.
- Packet inspection. For example, Application detection that is based on the service data flow template and the optional PFDs received from the SMF in addition.
- User Plane part of policy rule enforcement. For example, Gating, Redirection, Traffic steering.
- Lawful intercept (UP collection).
- Traffic usage reporting.
- QoS handling for User Plane. For example, Uplink (UL) and Downlink (DL) rate enforcement, Reflective QoS marking in DL, and so on.
- Uplink Traffic verification (SDF to QoS Flow mapping).
- Transport level packet marking in the Uplink and Downlink.
- Downlink packet buffering and Downlink Data Notification triggering.
- Sending and forwarding of one or more "End Marker" to the source NG-RAN node.

Use Cases and Features

Configuration and Deployment Requirement for UPF

With 5G deployment, interoperability is required between Cisco UPF with non-Cisco SMF, and Cisco SMF with non-Cisco UPF. Also, decoupling of configuration-related messaging between SMF and UPF has the following benefits:

- Alignment with 3GPP standards for configuration bifurcation between User Plane and Control Plane.
- Reduced complexity for configuration management on SMF.

- Simplicity and efficiency for the configuration and change management for User Plane related configuration, as it does not require SMF to manage and distribute the configuration.
- Can be enhanced to achieve interworking between non-Cisco SMF and UPFs.

The Cisco UPF supports 3GPP-specified attributes on the N4 interface. In the current architecture, only UPF associates with the SMF.

The following features are related to this use case:

- [UPF Deployment Architecture, on page 12](#)
- [UPF Local Configuration, on page 141](#)
- [N4 Session Management, Node Level, and Reporting Procedures, on page 125](#)
- [Session Recovery, on page 149](#)
- [1:1 Redundancy, on page 19](#)
- [UPF Ingress Interface, on page 139](#)

Anchor Point for Intra-RAT and Inter-RAT Mobility

The UPF is the anchor point between the mobile infrastructure and the Data Network (DN). That is, the encapsulation and decapsulation of GPRS Tunneling Protocol for the User Plane (GTP-U). Intra-RAT mobility like Xn handover and inter-RAT mobility like 4G to 5G and 5G to 4G handover are supported for this use case.

The [GTP-U Support, on page 101](#) feature is related to this use case.

External PDU Session Point of Interconnect to Data Network

The UPF acts as an external PDU session point of interconnect to Data Network and supports N3, N4, and N6 interfaces. The PDU layer corresponds to the PDU that is transported between the UE and the PDN during a PDU session. The PDU session can be of type IPv4 or IPv6 for transporting IP packets. The GPRS tunneling protocol for the user plane (GTP-U) supports multiplexing of the traffic from different PDU sessions by tunneling user data over the N3 interface (between a 5G access node and the UPF) in the core network. The GTP encapsulates all end-user PDUs and provides encapsulation per-PDU session. This layer also transports the marking associated with the QoS flow. The 5G encapsulation layer supports multiplexing the traffic from different PDU sessions over the N9 interface (an interface between different UPFs). It provides encapsulation per PDU session and carries the marking associated with the QoS flows.

The following features are related to this use case:

- [Control Plane-Initiated N4 Association Support, on page 45](#)
- [N3 Transfer of PDU Session Information, on page 111](#)
- [N4 Session Management, Node Level, and Reporting Procedures, on page 125](#)
- [UPF Reporting of Load Control Over N4 Interface, on page 145](#)

Packet Inspection

The Cisco UPF performs L3/L4 and L7 inspection for the user traffic that is received. L3/L4 inspection involves IP-address/port matching and Deep Packet Inspection involves matching of L7 header fields.

The [Deep Packet Inspection and Inline Services, on page 61](#) feature is related to this use case.

User Plane Part of Policy Rule Enforcement

Cisco UPF provides different enforcement mechanisms based on policy received from the SMF. The UPF is the boundary between the Access and IP domains and is the ideal location to implement policy-based enforcement. The pcc-rules provided by the PCF and the pre-defined rules on the SMF are uploaded over the N4 interface and installed on the UPF on a per-DNN basis. This allows for dynamic policy changes that enable differentiated charging and QoS enforcement.

- [Dynamic and Static PCC Rules, on page 93](#)
- [Voice over New Radio, on page 155](#)

Lawful Intercept

Lawful Interception (LI) enables a LEA to perform electronic surveillance on an individual (a target) as authorized by a judicial or administrative order. To facilitate the lawful intercept process, certain legislation and regulations require service providers and Internet service providers to implement their networks to explicitly support authorized electronic surveillance. Actions taken by the service providers include: provisioning the target identity in the network to enable isolation of target communications (separating it from other users' communications), duplicating the communications for the purpose of sending the copy to the LEA, and delivering the Interception Product to the LEA.

For information about the support of Lawful Intercept by UPF, contact your Cisco Account representative.

Traffic Usage Reporting (Charging)

The usage measurement and reporting function in UPF is controlled by the SMF. The SMF controls these functions by:

- Creating the necessary PDRs to represent the service data flow, application, bearer or session (if they are not existing already).
- Creating the URRs for each Charging Key and combination of Charging Key and Service ID. Also, creating URRs for a combination of Charging Key, Sponsor ID, and Application Service Provider ID.
Please note that, for static rules, the UPF creates the URR ID. The URR ID is created based on the online/offline and Content ID+Service ID combination that is configured on UPF.
- Associating the URRs to the relevant PDRs defined for the PFCP session, for usage reporting at SDF, Session or Application level.
- For online charging, the SMF provisions Volume and Time quota, if it receives it from the Online Charging Server (OCS).

The [Charging Support, on page 49](#) feature is related to this use case.

QoS Handling for User Plane

The 5G QoS model allow classification and differentiation of specific services, based on subscription-related and invocation-related priority mechanisms. These mechanisms provide abilities such as invoking, modifying, maintaining, and releasing QoS Flows with priority, and delivering QoS Flow packets according to the QoS characteristics under network congestion conditions.

The [Dynamic and Static PCC Rules, on page 93](#) feature is related to this use case.

Downlink Packet Buffering and Data Notification Triggering

A Buffering Action Rule (BAR) provides instructions to control the buffering behavior of the UPF. The BAR controls the buffering behavior for all Forwarding Action Rules (FARs) of the Packet Forwarding Control Protocol (PFCP) session. This control is applicable when the PFCP session is set with an Apply Action parameter, which requests packets to be buffered and associated with the respective BAR.

The [Idle Mode Buffering and Paging, on page 107](#) feature is related to this use case.

Forwarding End Markers to the Source NG-RAN Node

At the time of the handover procedure, the PDU session for the UE – which comprises of UPF node – acts as a PDU session anchor and an intermediate UPF terminating N3 reference point. The SMF sends an N4 Session Modification Request message with the new AN Tunnel Info of NG-RAN to specify the UPF to switch to the N3 paths. In addition, the SMF also specifies the UPF to send the End Marker packets on the old N3 user plane path. After the UPF receives the indication, the End Markers are constructed and sent to each N3 GTP-U tunnel toward the source NG-RAN, after sending the last PDU on the old path.

The [N4 Session Management, Node Level, and Reporting Procedures, on page 125](#) feature is related to this use case.

Deployment Architecture and Interfaces

Cisco UPF is part of the 5GC network functions portfolio (AMF/SMF/NRF/PCF/NSSF/UPF) with a common Mobile Core Platform architecture.

UPF Architecture

The User Plane Function (UPF) is a fundamental component of a 3GPP 5G core infrastructure system architecture. The UPF represents the data plane evolution of a Control and User Plane Separation (CUPS) strategy, first introduced as an extension to existing Evolved Packet Cores (EPCs) by the 3GPP in Release 14 specifications. The CUPS decouples Packet Gateway (P-GW) Control and User Plane functions, enabling the data forwarding component (PGW-U) to be decentralized. This allows packet processing and traffic aggregation to be performed closer to the network edge, increasing bandwidth efficiencies while reducing network load. The P-GW handling signaling traffic (PGW-C) remains in the core, northbound of the Mobility Management Entity (MME).

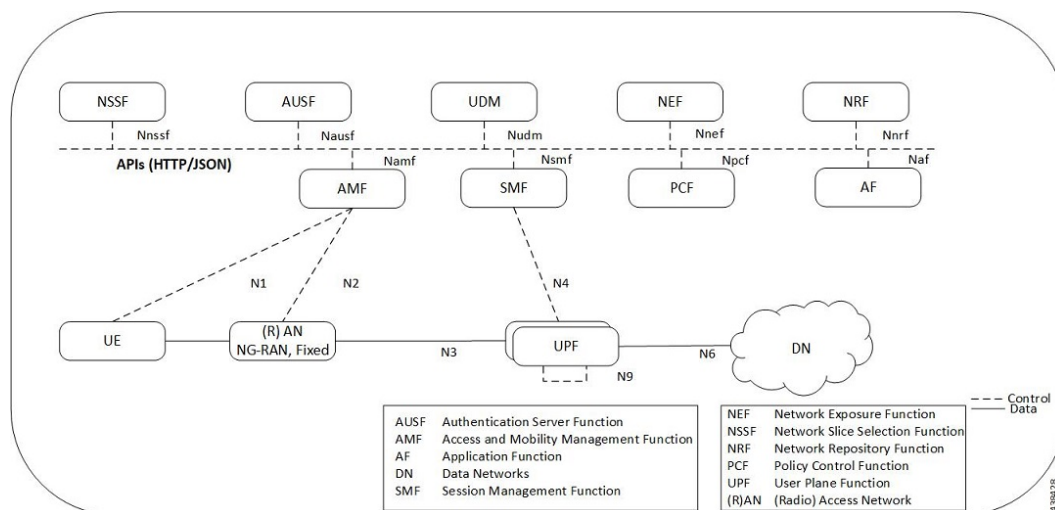
The primary goal of CUPS is to support 5G New Radio (NR) implementations enabling early IoT applications and higher data rates. Committing to a complete implementation of CUPS is a complex proposition as it only provides a subset of advantages to the operator adopting a 5G User Plane Function (5G-UPF), offering network

slicing. Deployed as a Virtual Machine (VM), the User Plane Function delivers the packet processing foundation for Service-Based Architectures (SBAs).

The UPF identifies User Plane traffic flow that is based on information received from the SMF over the N4 reference point. The N4 interface employs the Packet Forwarding Control Protocol (PFCP), which is defined in the 3GPP technical specification 29.244 for use on Sx/N4 reference points in support of CUPS. The PFCP is similar to OpenFlow but can be limited to only the functionality that is required to support mobile networks. The PFCP sessions, which are established with the UPF, define how packets are identified (Packet Detection Rule / PDR), forwarded (Forwarding Action Rules / FARs), processed (Buffering Action Rules / BARs), marked (QoS Enforcement Rules / QERs) and reported (Usage Reporting Rules / URRs).

UPF Deployment Architecture

The following diagram illustrates, at a high-level, the deployment architecture of UPF along with other NFs.



Virtualized Packet Core—Single Instance (VPC-SI)

VPC-SI consolidates the operations of physical Cisco ASR 5500 chassis running StarOS into a single Virtual Machine (VM) able to run on commercial off-the-shelf (COTS) servers. VPC-SI can be used as a stand-alone single VM within an enterprise, remote site, or customer data center. Alternatively, VPC-SI can be integrated as a part of a larger service provider orchestration solution.

VPC-SI only interacts with supported hypervisors KVM (Kernel-based Virtual Machine) and VMware ESXi. It has little or no knowledge of physical devices.

The UPF functions as user plane node in 5G-based VNF deployments. UPF is deployed as a VNFC running a single, stand-alone instance of the StarOS. Multiple UPF VNFCs can be deployed for scalability based on your deployment requirements.

Hypervisor Requirements

VPC-SI has been qualified to run under the following hypervisors:

- Kernel-based Virtual Machine (KVM) - QEMU emulator 2.0. The VPC-SI StarOS installation build includes a libvirt XML template and ssi_install.sh for VM creation under Ubuntu Server 14.04.


```
Local Params:
-----
No local param file available
```



Note For additional information about VPC-SI build components, boot parameters, configuring VPC-SI boot parameters, VM configuration, vCPU and vRAM options, VPP configuration parameters, and so on, refer the *VPC-SI System Administration Guide*.

UPF Deployment with VPC-SI

For additional information on VPC-SI, supported operating system and hypervisor packages, platform configurations, software download and installation, as well as UPF deployment, contact your Cisco Account representative.

For information on Release Package, refer the corresponding Release Notes included with the build.

UPF Deployment with SMI Cluster Manager

The Ultra Cloud Core Subscriber Microservices Infrastructure (SMI) provides a run time environment for deploying and managing Cisco's cloud native network functions (cNFs), also referred to as applications.

It is built around open source projects like Kubernetes (K8s), Docker, Helm, etcd, confd, and gRPC, and provides a common set of services used by deployed cNFs.

The SMI is a layered stack of cloud technologies that enable the rapid deployment of, and seamless life cycle operations for microservices-based applications.

The SMI stack consists of SMI Cluster Manager that creates the Kubernetes (K8s) cluster and the software repository. The SMI Cluster Manager also provides ongoing Life Cycle Management (LCM) for the cluster including deployment, upgrades, and expansion.

The SMI Cluster Manager leverages the Kernel-based Virtual Machine (KVM)—a virtualization technology—to deploy the User Plane Function (UPF) VMs.

For more information, refer the *UCC SMI Operations Guide*.

Supported Interfaces

This section describes the interfaces supported between the UPF and other network functions in 5GC.

- N3: Interface between the RAN (gNB) and the (initial) UPF; compliant with 3GPP TS 29.281 and 3GPP TS 38.415 (December-2018).
- N4: Interface between the Session Management Function (SMF) and the UPF; compliant with 3GPP TS 29.244 (December-2018).
- N6: Interface between the Data Network (DN) and the UPF; compliant with 3GPP TS 29.561 (December-2018).

License Information

The UPF require specific license(s). Contact your Cisco account representative for more information on how to obtain a license.

Standards Compliance

Cisco UPF complies with the following standards:

- Interface between the Control Plane and the User Plane Nodes: 3GPP TS 29.244 version 15.4.0. (December-2018)
- General Packet Radio System (GPRS) Tunneling Protocol User Plane (GTPv1-U): 3GPP TS 29.281 version 15.5.0 (December-2018).
- NG-RAN; PDU Session User Plane protocol: 3GPP TS 38.415 (December-2018)
- 5G System; Interworking between 5G Network and external Data Networks; Stage 3: 3GPP TS 29.561 (December-2018)



PART I

Features and Functionality

- [1:1 Redundancy, on page 19](#)
- [APN ACL Support, on page 31](#)
- [Bulk Statistics Support, on page 37](#)
- [Collection and Reporting of Usage Data over N4 Interface, on page 41](#)
- [Control Plane-Initiated N4 Association Support, on page 45](#)
- [Charging Support, on page 49](#)
- [Deep Packet Inspection and Inline Services, on page 61](#)
- [Dynamic and Static PCC Rules, on page 93](#)
- [GTP-U Support, on page 101](#)
- [Idle Mode Buffering and Paging, on page 107](#)
- [N3 Transfer of PDU Session Information, on page 111](#)
- [N4 Interface Compliance with 3GPP Specification, on page 115](#)
- [N4 Interface Configuration, on page 121](#)
- [N4 Session Management, Node Level, and Reporting Procedures, on page 125](#)
- [UPF Ingress Interface, on page 139](#)
- [UPF Local Configuration, on page 141](#)
- [UPF Reporting of Load Control Over N4 Interface, on page 145](#)
- [Session Recovery, on page 149](#)
- [Voice over New Radio, on page 155](#)



CHAPTER 3

1:1 Redundancy

- [Feature Summary and Revision History, on page 19](#)
- [Feature Description, on page 20](#)
- [How it Works, on page 20](#)
- [Configuring 1:1 UPF Redundancy, on page 25](#)
- [Monitoring and Troubleshooting, on page 29](#)

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

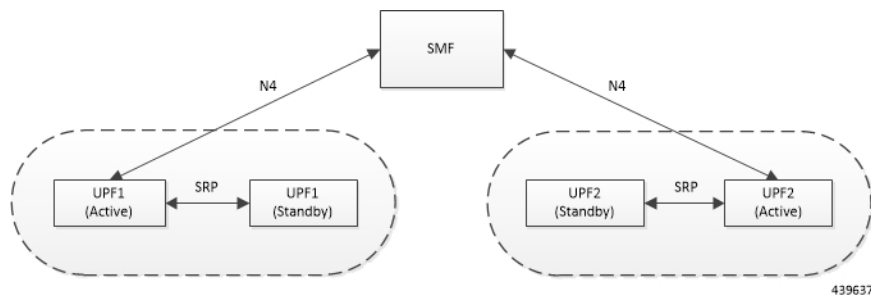
Revision Details	Release
First introduced.	2020.02.0

Feature Description

How it Works

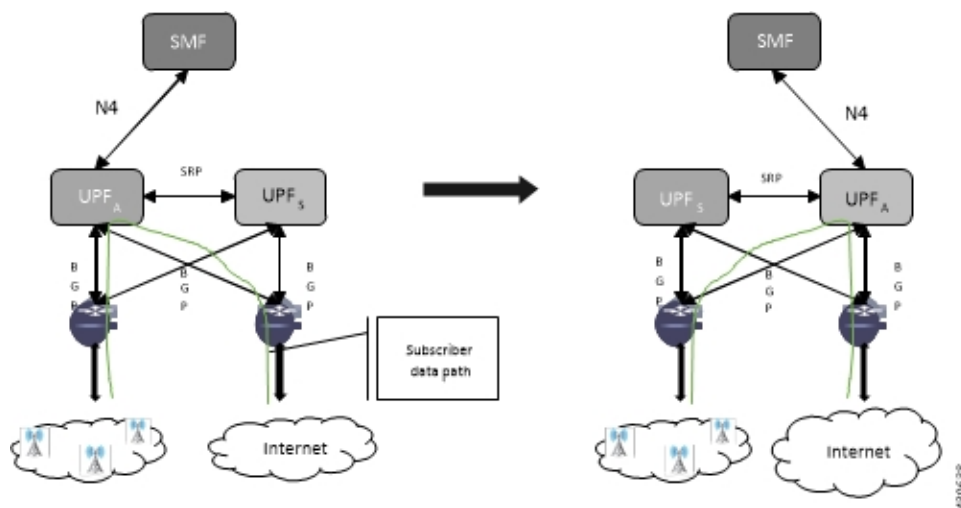
The 5G-UPF deployment leverages the ICSR framework infrastructure for checkpointing and switchover of the UPF node as shown in the following figure. The Active UPF communicates to its dedicated Standby UPF through the Service Redundancy Protocol (SRP) link that is provisioned between the UPFs.

Figure 5: UPF 1:1 Redundancy Using SRP



The Session Management Function (SMF) node does not have the Standby UPF information that is available in the UPF group configuration. Therefore, the SMF is not aware of the UPF redundancy configuration and the switchover event among the UPFs.

Figure 6: UPF 1:1 Redundancy Switchover



To make redundancy fully compliant, it addresses the following dependencies on the SRP-based ICSR in the 5G environment.

Besides the dependencies listed, the UPF implements data collection and checkpoint procedures specific to the UPF node. For example, checkpointing for IP-pool chunks. The UPF integrates these procedures into the existing ICSR checkpointing framework.

Independent Configuration of Standby UPF

After UPF is up with base configuration (for example, services, contexts, interfaces, and so on), the rest of the configuration (for example, ACS and policy-related configuration) is done through Ops-center/Redundancy and Configuration Manager (RCM) POD. This configuration is common for both SMF/UPF policies. For SRP redundancy to work, the Active and Standby UPF has same configuration, except SRP-related configuration with which SRP connections are established between Active and Standby UPF. The RCM configures Active and Standby UPF independently.

BFD Monitor Between Active UP and Standby UP

The Bidirectional Forwarding Detection (BFD) monitors the SRP link between the Active UPF and Standby UPF for a fast failure-detection and switchover. When the Standby UPF detects a BFD failure in this link, it takes over as the Active UPF.

The BFD link can be single-hop or multi-hop.

To configure the BFD monitor, between the Active UP and Standby UP, see *Configuring BFD Monitoring Between Active UPF and Standby UPF*.

Sample Configuration for Multihop BFD Monitoring

Primary UPF:

```
config
context srp
  bfd-protocol
    bfd multihop-peer 1.1.1.1 interval 50 min_rx 50 multiplier 20
  #exit
  service-redundancy-protocol
    monitor bfd context srp 1.1.1.1 chassis-to-chassis
    peer-ip-address 1.1.1.1
    bind address 1.1.0.1
  #exit
  interface srp
    ip address 1.1.0.1 2.3.4.0
  #exit
  ip route static multihop bfd bfd1 1.1.0.1 1.1.1.1
  ip route 1.1.0.1 2.3.4.0 1.1.0.1 srp
#exit
end
```

Backup UPF:

```
config
context srp
  bfd-protocol
    bfd multihop-peer 1.1.0.1 interval 50 min_rx 50 multiplier 20
  #exit
  service-redundancy-protocol
    monitor bfd context srp 1.1.0.1 chassis-to-chassis
    peer-ip-address 1.1.0.1
    bind address 1.1.0.1
  #exit
  interface srp
    ip address 1.1.0.1 255.255.255.0
  #exit
  ip route static multihop bfd bfd1 1.1.1.1 1.1.0.1
  ip route 1.1.0.1 255.255.255.0 1.1.1.1 srp
#exit
End
```

Router between Primary and Backup UPF:

```

config
  context one
    interface one
      ip address 1.1.0.1 255.255.255.0
    #exit
    interface two
      ip address 1.1.1.1 255.255.255.0
    #exit
  #exit
end

```

Sample Configuration for Single-Hop BFD Monitoring

Primary UPF:

```

config
  context srp
    bfd-protocol
    #exit
    service-redundancy-protocol
      monitor bfd context srp 1.1.0.1 chassis-to-chassis
      peer-ip-address 1.1.0.1
      bind address 1.1.2.1
    #exit
    interface srp
      ip address 1.1.0.1 255.255.255.0
      bfd interval 50 min_rx 50 multiplier 10
    #exit
    ip route static bfd srp 1.1.2.1
  #exit
end

```

Backup UPF:

```

config
  context srp
    bfd-protocol
    #exit
    service-redundancy-protocol
      monitor bfd context srp 1.1.1.1 chassis-to-chassis
      peer-ip-address 1.1.2.1
      bind address 1.1.3.1
    #exit
    interface srp
      ip address 1.1.2.1 255.255.255.0
      bfd interval 50 min_rx 50 multiplier 10
    #exit
    ip route static bfd srp 1.1.3.1
  #exit
end

```

VPP Monitor

When SRP VPP monitor is configured, the UPF chassis is SRP Active and if the VPP subsystem fails, then SRP initiates switchover to Standby UPF. Currently, VPP health monitoring is limited to heartbeat mechanism between NPUMgr task and VPP process.

To configure the VPP monitor, see *Configuring VPP Monitor on Active UPF and Standby UPF*.

Sx/N4 Association Checkpoint

Whenever an Active UPF initiates an Sx/N4 association to SMF, the Standby UPF checkpoints this data. This maintains the association information even after the UPF switchover.

The Sx/N4 heartbeat messages are sent and the Active UPF responds back even after back-to-back UPF switchovers.

Sx/N4 Monitor

It is critical to monitor the Sx/N4 interface between the UPF and SMF. The SRP monitoring is enabled on Sx/N4 interface and the existing Sx/N4 heartbeat mechanism is leveraged to detect the monitor failure. The Sx/N4 module on Active UPF, on detecting the failure, informs the SRP VPNMgr to trigger UPF switchover event so that the Standby UPF takes over.



Note Sx/N4 monitoring is available only in the UPF.

It is important to ensure that the SMF Sx/N4 heartbeat timeout is higher than the UPF Sx/N4 heartbeat timeout plus UPF ICSR switchover time. This is to ensure that the SMF does not detect the Sx/N4 path failure during a UPF switchover because of the UPF Sx/N4 monitor failure.

The Standby UPF itself has no independent connectivity to the SMF. The Active UPF Sx/N4 context is replicated to the Standby UPF so that it is ready to takeover during SRP switchover. This implies that when the Active UPF has switched over to Standby because of Sx/N4 monitor failure, the new Standby has no way of knowing if the UPF to SMF link is working. To prevent a switchback of the new Standby to Active state again due to Sx/N4 monitor failure in new Active, use the **disallow-switchover-on-peer-monitor-fail** keyword in the **monitor sx** CLI command.

After a chassis becomes Standby due to Sx/N4 monitoring failure, the Sx/N4 failure status is not reset even if Sx/N4 up checkpoint is received from the new Active UPF. This is to prevent the new Active to cause an unplanned switchback again due to Sx/N4 monitor failure when the previous cause of switchover itself was Sx/N4 monitor failure. This prevents back-to-back switchovers when SMF is down. The Sx/N4 monitor failure status must be manually reset when the operator is convinced that the network connectivity is normal. To reset, use the new **srp reset-sx-fail** CLI command (see *Resetting Sx/N4 Monitor Failure*) in the Standby chassis.

To configure the Sx/N4 monitor, see *Configuring Sx/N4 Monitoring on the Active UPF and Standby UPF*.

Sx/N4 Monitor—Pending-Active

The UPF chassis can turn into Pending-Active state for one of the following reasons:

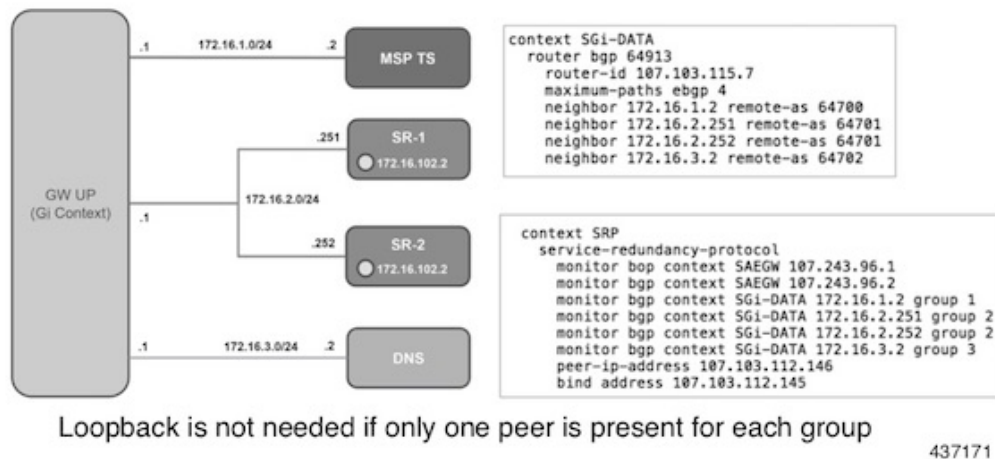
- When Sx/N4 heartbeat times out during SMF upgrade, the Sx/N4 connection is terminated. So, Sx/N4 monitoring failure triggers ICSR switchover in UPF. This switchover causes the old Standby UPF to transition to Pending-Active state. The UPF in Pending-Active state neither receives any Sx/N4 heartbeats from SMF nor any subscriber traffic. As a result, the UPF remains in Pending-Active state indefinitely and can't be utilized without a manual intervention.
- When appropriate procedure to upgrade UPF is not followed, one of the UPF may end up in Pending-Active state. Also, if SMF goes down during the UPF upgrade or if the UPF switchover takes more time than the SMF heartbeat timeout, then one of the UPF remains in Pending-Active state indefinitely.
- When Sx/N4 session times out between SMF and UPF due to network issues, and if a UPF ICSR switchover happens almost simultaneously (Double fault scenario), the UPF in Pending-Active state doesn't transition to Active state.

Whenever a UPF chassis turns Pending-Active, start a timer with a callback which forcefully transitions the UPF from Pending-Active to Active state. Before forcing the transition, check if the SRP link is up and if the SRP peer is in Standby state. If not, restart the timer. The duration of the timer is configurable using **force-pactv-to-actv-timeout** *value_seconds* CLI command (see *Changing UPF state from Pending-Active to Active* section for configuration details). When this CLI command is not configured, the UPF remains in Pending-Active state indefinitely.

BGP Monitor

Configure BGP peer monitor and peer group monitors for the next-hop routers from UPF (both Gi and Gn side). This is the existing ICSR configuration. BGP may run with BFD assist to detect fast BGP peer failure.

Figure 7: BGP Peer Groups and Routing



To configure BGP monitoring and flag BGP monitoring failure, see *Configuring BGP Status Monitoring Between Each UP and Next-Hop Router*.

UPF Session Checkpoints

The Active chassis sends a collection of UPF data as checkpoints to the peer Standby chassis in the following scenarios:

- New call setup
- For every state change in the call
- Periodically for accounting buckets

On receiving these checkpoints, the Standby chassis acts on the data and updates the necessary information either at the call, node, or instance level.

VPN IP Pool Checkpoints

During Sx/N4 Association, the IP pool allocated to each of the UPF is sent by SMF to the respective UPF. The VPNMgr receives this message in the UPF and checkpoints the same information to the Standby UPF when the SRP is configured.

The IP pool information is also sent during the SRP VPNMgr restart and during the SRP link down and up scenarios.

Validation of the presence of IP pool information in the Standby is vital before switchover. If the IP pool information is not present, then route advertisement is not possible. Therefore, traffic does not reach the UPF.

External Audit and PFD Configuration Audit Interaction

External Audit management is done in Active UPF. The Session Manager gets a start and complete notification of the Configuration Audit. The Session Manager does not start the External Audit if Configuration Audit is in progress. If the Configuration Audit start-notification arrives when the External Audit is already underway, then the Session Manager raises a flag such that the External Audit restarts when it completes. Restarting the External Audit is necessary because it does not achieve its purpose if it occurs when Configuration Audit is already underway.

Configuring 1:1 UPF Redundancy

The following sections provide information about the CLI commands available in support of the feature.

Configuring BFD Monitoring Between Active UPF and Standby UPF

Configuring BGP Status Monitoring Between Each UPF and Next-Hop Router

Use the following commands to configure Border Gateway Protocol (BGP) monitoring between each UPF and next-hop router. The command is configured in the SRP Configuration Mode.

```
configure
  context context_name
    service-redundancy-protocol
      [ no ] monitor bgp context bgp-session-context-name [
nexthop-router-ipv4-address | nexthop-router-ipv6-address ] { vrf
bgp-session-vrf-name } { group group-number }
      end
```

NOTES:

- **no**: Disables BGP status monitoring on the UPF.
- **bgp context** *bgp-session-context-name*: Specifies the context where BGP peer is configured. *bgp-session-context-name* specifies the context string.
- **nexthop-router-ipv4-address | nexthop-router-ipv6-address**: Specifies the configured BGP peer IPv4 or IPv6 address to monitor.
- **vrf** *bgp-session-vrf-name*: Specifies the BGP VPN Routing and Forwarding (VRF) instance. *bgp-session-vrf-name* specifies the VRF name.
- **group** *group-number* : Specifies the BGP peer group where the BGP peer should be included. *group-number* specifies the group number.

On implementing this keyword, the behavior is as follows:

- If any BGP peer in that group is up, the BGP peer group is up.

Omitting group configuration for a BGP monitor includes that monitor in group 0.

BGP group 0 monitors in a context from an implicit group. Each context forms a separate BGP group 0 implicit monitor group.

If any BGP peer group is down, BGP monitor is down.

- This command is disabled by default.

Alternate Algorithm to Flag BGP monitoring failure

In this release, an alternate (new) algorithm is introduced to flag BGP monitoring failure.

```
configure
  context context_name
    service-redundancy-protocol
      [ no ] monitor bgp exclusive-failover
    end
```

NOTES:

- **no**: Disables flagging of BGP monitor failure on a single BGP peer failure.
- On implementing the new **exclusive-failover** keyword, the behavior is as follows:
 - BGP peer group is Up if any BGP peer in that group is Up.
 -
 - BGP monitor is down if any BGP peer group or any non-group BGP peer is down.
- This command is disabled by default.

Configuring Sx/N4 Monitoring on the Active UPF and Standby UPF

Use the following configuration to configure Sx/N4 monitoring on the Active UPF and Standby UPF. This command is configured in the SRP Configuration Mode.

```
configure
  context context_name
    service-redundancy-protocol
      [ no ] monitor sx [ { context context_name | bind-address { ipv4_address
| ipv6_address } | { peer-address { ipv4_address | ipv6_address } } ]
    end
```

NOTES:

- **no**: Disables Sx/N4 monitoring on the Active and Standby UPF.
- **context context_name** : Specifies the context of the Sx/N4 service.
context_name must be an existing context expressed as an alphanumeric string of 1 through 79 characters.
- **bind-address { ipv4 _address | ipv6_address }**: Defines the service IP address of the Sx/N4 service, entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.



Note The IP address family of the **bind-address** and **peer-address** must be same.

- **peer-address** { *ipv4_address* | *ipv6_address* }: Defines the IP address of the Sx/N4 peer, entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
- **disallow-switchover-on-peer-monitor-fail**:
Prevents the switchback of the UPF to Active state when the working status of the UPF to SMF link is unknown.
-
- The Sx/N4 monitor state goes down when any of the monitored Sx/N4 connections are down.
- This command is disabled by default.

Configuring VPP Monitor on Active UPF and Standby UPF

```
configure
context context_name
  service-redundancy-protocol
    monitor system vpp delay-period seconds
  end
```

NOTES:

- If previously configured, use the **no monitor system vpp** CLI command to disable VPP monitoring on the Active and Standby UPF.
- **vpp delay-period** : Specifies the delay period in seconds for a switchover, after a VPP failure. *seconds* must be in the range of 0 through 300.

If the delay period is a value greater than zero (0), then the switchover is initiated after the specified delay period when VPP fails. The last VPP status notification within the delay period is the final trigger for switchover action. The default value is 0 seconds, which initiates an immediate switchover.

The need for delay is to address the scenario wherein the VPP is temporarily down and the revival is in process. This implies that a switchover may not be necessary.

- This command is disabled by default.

Preventing User Plane Function Switchback

```
configure
context context_name
  service-redundancy-protocol
    monitor sx disallow-switchover-on-peer-monitor-fail timeout seconds
  end
```

Use either of the following CLIs to allow switchback of the new Standby UPF to Active state.

```
no monitor sx disallow-switchover-on-peer-monitor-fail
```

Or

```
monitor sx disallow-switchover-on-peer-monitor-fail timeout 0
```

NOTES:

- **no**: Disables prevention of switchover.
 - **seconds]**: Prevents the switchback of the UPF to Active state when the working status of the UPF to SMF link is unknown.
- timeout seconds**: Timeout after which the switchback is allowed even if the Sx/N4 failure status is not reset in the Standby peer. The valid values range from 0 through 2073600 (24 days).



Note Assigning 0 seconds as the timeout allows unplanned switchover.

If **timeout** keyword is not specified, the Active chassis waits indefinitely for the Sx/N4 failure status to be reset in the Standby peer.

- The default configuration is to allow unplanned switchover due to Sx/N4 monitor failure in all conditions.



Note Manual planned switchover is allowed irrespective of whether this CLI is configured or not.

Preventing Dual Active Error Scenarios

Use the following CLI configuration in CP to prevent dual Active error scenarios for UPF 1:1 redundancy.

```
configure
  user-plane-group group_name
    sx-reassociation disabled
  end
```

NOTE:

- **sx-reassociation disabled**: Disables UP Sx reassociation when the association already exists with the CP.

Resetting Sx/N4 Monitor Failure

```
srp reset-sx-fail
```

Changing UPF State from Pending-Active to Active

Monitoring and Troubleshooting

Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of this feature.

show srp monitor bfd

- Type:
 - (A) - Auth. probe
 - (B) - BGP
 - (D) - Diameter
 - (F) - BFD
 - (E) - EGQC
 - (C) - Card
 - (V) - VPP
- State:
 - (I) - Initializing
 - (U) - Up
 - (D) - Down
- GroupId
- IP Addr
- Port
- Context (VRF Name)
- Last Update

show srp monitor bgp

show srp monitor sx

The output of this CLI command contains the following fields in support of Sx/N4 monitor status:

- Type:
 - (A) - Auth. probe

- (B) - BGP
- (D) - Diameter
- (F) - BFD
- (E) - EGQC
- (C) - Card
- (V) – VPP
- (S) - SX

- State:
 - (I) - Initializing
 - (U) - Up
 - (D) - Down

- GroupId
- IP Addr
- Port
- Context (VRF Name)
- Last Update

show srp monitor vpp



CHAPTER 4

APN ACL Support

This chapter covers the following topics:

- [Feature Summary and Revision History, on page 31](#)
- [Feature Description, on page 32](#)
- [IP Source Violation, on page 34](#)
- [Gating Control, on page 35](#)

Feature Summary and Revision History

Summary Data

Table 5: Summary Data

Applicable Product (s) or Functional Area	5G-UPF
Applicable Platforms	VPC-SI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	<i>UCC 5G UPF Configuration and Administration Guide</i>

Revision History

Table 6: Revision History

Revision Details	Release
First introduced.	2020.02.0

Feature Description

IP Access Lists, commonly known as Access Control Lists (ACLs), control the flow of packets into and out of the system. The configuration is per-context basis and consists of "rules" (ACL rules) or filters that control the action applicable for packets that match the filter criteria. Once configured, an ACL can be applied to an individual subscriber. Separate ACLs can be created for IPv4 and IPv6 access routes.

The following are the two main aspects of ACLs:

- Rule(s)
- Rule Order

Rule(s)

A single ACL consists of one or more ACL rules. Each rule is a filter configured to take a specific action when packets match a specific criteria.

Each rule specifies the action to take when a packet matches the specifies criteria. This section discusses the rule actions and criteria supported by the system.

Actions

ACLs specify that one of the following actions can be taken on a packet that matches the specified criteria:

- **Permit:** The packet is accepted and processed for classification and policy enforcement.
- **Deny:** The packet is rejected.
- **Redirect CSS:** The behaviour is same as Permit action.

NOTES:

- In UPF, it's recommended to use Permit option instead of Redirect CSS. Functionally, both the options are equivalent in UPF. Support for Redirect CSS option is only for backward compatibility and should be used only in such scenarios.
- Configured ACLs consisting of no rules imply a "deny any" rule. This is the default behavior for an empty ACL.
- In UPF, if ACLs aren't associated with an APN, then call is up. By default, traffic is processed for classification and policy enforcement. For non-UPF architecture, call fails as Redirect CSS is mandatory.
- If only Deny option is given in the ACL for certain traffic, then to pass the rest of the traffic, Permit option must be given explicitly.
- If only permit option is given in the ACL for certain traffic, then to pass the rest of the traffic, permit must be given explicitly for that traffic.
- Router Advertisement/Router Solicitation (RA/RS) packets are candidate for ACL. So, take caution in putting the IPv6 ACL.
- Configuration change in ACL is applied for a new call and not on the existing call.

Criteria

Each ACL consists of one or more rules specifying the criteria that packets will be compared against.

The following criteria are supported:

- **Any:** Filters all packets
- **Host:** Filters packets based on the source host IP address
- **ICMP:** Filters Internet Control Message Protocol (ICMP) packets
- **IP:** Filters Internet Protocol (IP) packets
- **Source IP Address:** Filter packets based on one or more source IP addresses
- **TCP:** Filters Transport Control Protocol (TCP) packets
- **UDP:** Filters User Datagram Protocol (UDP) packets

Each of the above criteria is described in detail in the sections that follow.

- **Any:** The rule applies to all packets.
- **Host:** The rule applies to a specific host as determined by its IP address.
- **ICMP:** The rule applies to specific Internet Control Message Protocol (ICMP) packets, Types, or Codes. ICMP type and code definitions can be found at www.iana.org (RFC 3232).
- **IP:** The rule applies to specific Internet Protocol (IP) packets or fragments.
- **Source IP Address:** The rule applies to specific packets originating from a specific source address or a group of source addresses.
- **TCP:** The rule applies to any Transport Control Protocol (TCP) traffic and could be filtered on any combination of source/destination IP addresses, a specific port number, or a group of port numbers. TCP port numbers definitions can be found at www.iana.org.
- **UDP:** The rule applies to any User Datagram Protocol (UDP) traffic and could be filtered on any combination of source/destination IP addresses, a specific port number, or a group of port numbers. UDP port numbers definitions can be found at www.iana.org.

Rule Order

A single ACL can consist of multiple rules. Each packet is compared against each of the ACL rules, in the order in which they were entered, until a match is found. Once a match is identified, all subsequent rules are ignored.

Limitations

Following are the known limitations of APN ACL feature in UPF:

- Readdress option in ACL is not supported.
- Redirect ACL for context and next-hop is not supported.
- Log option is not supported in ACLs.

- APN-level bulkstats for ACL drops (only IPv4) are supported.

Configuring ACL

To apply the ACL to individual subscriber through via APN, use the following configuration:

```

configure
  context dest_context_name [ -noconfirm ]
    { ip | ipv6 } access-list acl_list_name
      { permit | deny | redirect } acl
    end
configure
  apn apn_name
    { ip | ipv6 } access-group acl_list_name [ in | out ]
  end

```

Notes:

- The ACL to be applied must be in the destination context of the APN (which can be different from the context where the APN is configured).
- If neither the **in** nor the **out** keyword is specified, the ACL will be applied to all inbound and outbound packets.
- Four access-groups can be applied for each APN, for example:

```

ip access-group acl_list_name_1 in
ip access-group acl_list_name_2 out
ipv6 access-group acl_list_name_3 in
ipv6 access-group acl_list_name_4 out

```

Verifying ACL Configuration

Use the following CLI commands in Exec mode to check if your ACL lists were applied properly, and also for packet drops due to ACL:

- **show subscriber user-plane-only full all**
- **show subscribers user-plane-only full callid** *call_id*
- **show user-plane-service pdn-instance statistics** *name*

IP Source Violation

Source validation requires the source address of incoming packets to match the IP address of the subscriber during the session. This allows operators to configure the network to prevent problems when a user gets handed back and forth between two gateways several times during a handoff scenario.

When the UPF receives a subscriber packet with a source IP address violation, the system increments the IP source violation drop-limit counter and starts the timer for the IP source violation period. Every subsequent packet received with a bad source address during the IP source violation period causes the drop-limit counter

to increment. For example, if you set the drop limit to 10, after 10 source violations, the call is dropped. The detection period timer continues to count throughout this process.

The following must be configured in the User Planes APN configuration:

```
ip source-violation { ignore | check [ drop-limit limit ] } [
exclude-from-accounting ]
```

NOTE: For information on IP source violation CLI commands, refer to the *StarOS Command Line Interface Reference*.

Gating Control

Gating Control in the UPF enables or disables the forwarding of IP packets belonging to a service data flow or detected application's traffic to pass through to the desired endpoint. See 3GPP TS 23.203, subclause 4.3.2.

The SMF controls the gating in the UPF by creating PDRs for the service data flow(s) or application's traffic to be detected, and by associating a QER, including the Gate Status IE, to the PDRs.

The Gate Status IE indicates whether the service data flow or detected application traffic is allowed to be forwarded (the gate is open) or to be discarded (the gate is closed) in the uplink and/or in downlink directions.

The UPF identifies the UL and DL flows by the Source Interface IE in the PDI of the PDRs or the destination Interface IE in the FARs. The UPF applies UL and DL gating accordingly.

The SMF requests the UPF to discard the packets that are received for the PDR by setting the gate fields in the Gate Status IE of QERs to CLOSED.



CHAPTER 5

Bulk Statistics Support

- [Feature Summary and Revision History, on page 37](#)
- [Feature Description, on page 37](#)

Feature Summary and Revision History

Summary Data

Table 7: Summary Data

Applicable Product (s) or Functional Area	5G-UPF
Applicable Platforms	VPC-SI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	<i>UCC 5G UPF Configuration and Administration Guide</i>

Revision History

Table 8: Revision History

Revision Details	Release
First introduced.	2020.02.0

Feature Description

This chapter identifies bulk statistic schemas for the Cisco Ultra Cloud 5G User Plane Function (UPF) software release.

Bulk statistics is a collection of software features and framework that collects and exports the important performance and health-related statistics of the packet core node to an external node. These statistics provide an effective way for the operators to perform the following functions:

- Monitor the overall health and performance of the nodes.
- Help take corrective actions.
- Optimize the packet core network for better utilization.
- Reduce the overall operation expenses.

The individual statistics are configured to be collected in a group called 'schema.'

The system-supported bulk statistics allows operators to choose statistics that are of importance to them and configure the presentation format. This simplifies the post-processing of statistical data because it allows data formatting that facilitates external, backend processors to parse it.

Statistics or bulk statistics reporting is important on a Mobile Packet Core node. For a product to be deployed in the network, it has to support statistics that meets Carrier Grade requisites.

Operators use bulk statistics for the following:

- Performance KPI monitoring
- Network Fault analysis and debugging
- Network Optimization
- Traffic pattern analysis
- Node health analysis

When used along with an element management system (EMS), the data can be parsed, archived, and graphed.

In the 5G environment, the system can be configured to collect for the following network functions:

- Access and Mobility Management Function (AMF)
- Network Repository Functions (NRF)
- Network Slice Selection Functions (NSSF)
- Policy Control Function (PCF)
- Session Management Function (SMF)
- User Plane Function (UPF)

The system supports the configuration of up to four sets (primary and secondary) of receivers. Each set is configured to collect specific sets of statistics from the supported list of schemas. Statistics can be pulled manually from the system or sent at configured intervals. The bulk statistics are stored on the receivers in files.

A user can configure the format of the bulk statistic data files. Users can specify the following:

- Format of the filename
- File headers and footers to include information such as the date, system hostname, and system uptime
- IP address of the system generating the statistics (available for only for headers and footers)

- Time that the file was generated

An EMS is capable of further processing the statistics data through XML parsing, archiving, and graphing. The Bulk Statistics Server component of an EMS parses collected statistics and stores the information in its PostgreSQL database. It can also generate XML output and can send it to a Northbound NMS or an alternate bulk statistics server for further processing.

Additionally, the Bulk Statistics server can archive files to an alternate directory on the server. The directory can be on a local file system or on an NFS-mounted file system on an EMS server.

The implementation of bulk statistics in 5G is as follows:

- The NFs collect and export the statistics separately to an aggregator node in the 5G architecture.
- The receiver correlates the statistics from the NFs using the node-names or any other information that is configured as part of the bulk statistics configuration. Any EMS tool can render this data similar to how it is rendered from a standalone system.

Supported Schemas

This release supports the following schemas in the 5G architecture.

APN Schema

The APN schema provides Access Point Name (APN) statistics.

Card Schema

The Card schema provides card-level statistics.

ECS Schema

The ECS schema provides Enhanced Charging Service statistics.

GTP-U Schema

The GTP-U schema provides GPRS Tunneling Protocol- User message statistics.

P2P Schema

The P2P schema provides P2P statistics.

P-GW Schema

The P-GW schema provides user-plane service statistics.

Port Schema

The Port schema provides port-level statistics.

Rulebase

The Rulebase schema provides rule base statistics.

Sx Schema

The Sx schema provides N4 related message statistics.

System Schema

The System schema provides system-level statistics.

Userplane Schema

The Userplane schema provides User Plane statistics.



Important

For more information on bulk statistic configuration, refer to the *Bulk Statistics* chapter in the *ASR 5500 System Administration Guide*.



CHAPTER 6

Collection and Reporting of Usage Data over N4 Interface

This chapter covers the following topics:

- [Feature Summary and Revision History, on page 41](#)
- [Feature Description, on page 42](#)
- [How it Works, on page 42](#)
- [Configuration to Collect and Report Volume Measurement over N4 Interface, on page 43](#)

Feature Summary and Revision History

Summary Data

Table 9: Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 10: Revision History

Revision Details	Release
First Introduced	2020.02.0

Feature Description

With this release, the User Plane Function (UPF) supports offline charging and reporting of usage data over the N4 interface.

Here, the SMF controls the collection and reporting of usage data by creating necessary PDRs and URRs, and associates the URRs with its relevant PDRs defined for a PFCP session. It also controls data usage reporting at an IP-CAN bearer level, IP-CAN session, TDF session, SDF, or at an application level.

The URR consists of the usage measurement method, reporting triggers, threshold, and quota values.



Important

In this release, only URR creation is supported during PFCP session establishment.

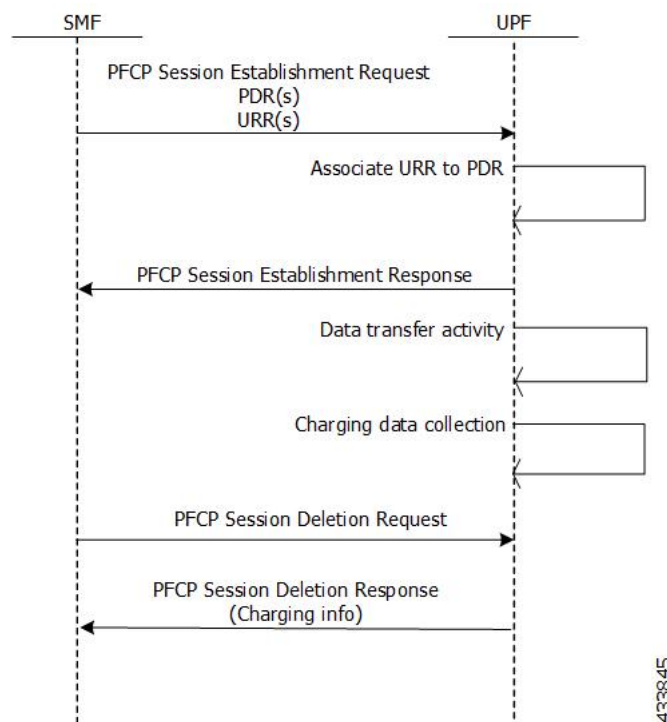
How it Works

This section describes how UPF supports offline charging of usage data.

To implement offline charging, the charging information is sent to the SMF only during PFCP session deletion.

Time and volume-based reporting is supported in the offline charging implementation. The following call flow illustrates offline charging in UPF.

Figure 8: Offline Charging in UPF



During the PFCP session deletion, UPF transfers the following charging information to the SMF:

- Timestamp of the first and last data packet
- Duration measurement – This IE specifies the time difference between URR creation and usage-reporting
- Volume measurement – This IE specifies the uplink data, downlink data and the total bytes transferred from the UPF to gNodeB.

Standards Compliance

UPF support for collection and reporting of data is compliant with the following standards:

- 3GPP TS 29.244 - LTE; Interface between the Control Plane and the User Plane of EPC Nodes
- 3GPP TS 23.501 - 5G; System Architecture for the 5G System
- 3GPP TS 23.502v - 5G; Procedures for the 5G System

Configuration to Collect and Report Volume Measurement over N4 Interface

This section describes the configuration required to collect and report volume measurement (usage data). However, to achieve this, SMF-based configurations for volume measurement needs to be configured.

The following SMF-based configuration is required to send volume measurement data in the URR by the UPF.

Configuring Charging Action for a Required Billing Action

Use the following configuration to configure charging-action for a required billing-action:

```
configure
  require active-charging
  active-charging service service_name
    charging-action charging_action_name
    billing-action interface_name
  end
```

NOTES:

- **billing-action:** Enables the specified billing type. The supported interfaces are:
 - **egcdr:** Enables the GGSN charging data record.

Associating a Charging Action with a Rulebase

Use the following configuration to associate a charging action with a rulebase:

```
configure
```

```
require active-charging
active-charging service service_name
    rulebase rulebase_name
        billing-records interface_name
        action priority priority_value ruledef ruledef_name charging-action
charging_action_name
    end
```

NOTES:

- **rulebase:** Enables the Active Charging Service Rulebase configuration.
- **billing-records:** Enables the generation of billing records. The supported interface is **egcdr**
- **action:** Decides the action to be taken on the ruledef.
- **priority:** Assigns priority to a ruledef in the rulebase. Priority must be a unique integer value ranging from 1 to 65535.
- **ruledef:** Specifies the ruledef.
- **charging-action:** Specifies the charging action.



CHAPTER 7

Control Plane-Initiated N4 Association Support

This chapter covers the following topics:

- [Feature Summary and Revision History, on page 45](#)
- [Feature Description, on page 46](#)
- [How it Works, on page 46](#)
- [Configuring the CP-Initiated N4 Association Setup Feature, on page 46](#)

Feature Summary and Revision History

Summary Data

Table 11: Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 12: Revision History

Revision Details	Release
First Introduced.	2020.02.0

Feature Description

SMF initiated N4 Association Setup Procedure

The N4 association set up procedure sets up an N4 association between the Session Management Function (SMF) and User Plane Function (UPF). It enables the SMF to use the UPF resources to establish the N4 sessions. The SMF and UPF exchange the supported functionalities on each side during this procedure.

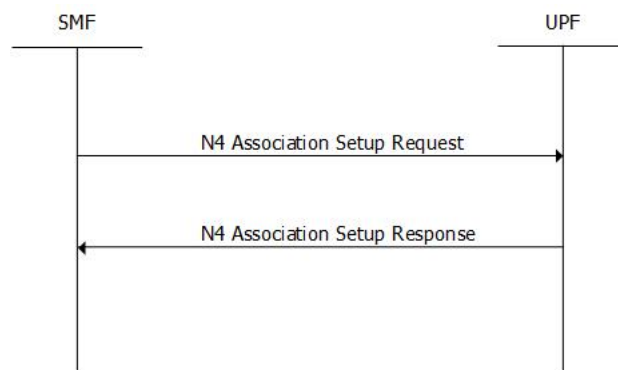
How it Works

The N4 association setup is initiated by the SMF. The setting of N4 association setup procedure is controlled through **sx-association initiated-by-cp** CLI command in the Control Plane Group Configuration mode. By default, the configuration is set to support the UPF-initiated N4 association setup procedure.

Call Flows

Session Management Function Initiated N4 Association Setup Procedure

The following call flow depicts the SMF-initiated N4 Association Setup procedure.



Step	Description
1	The SMF initiates the N4 Association Setup procedure to request the setup of an N4 association towards a UPF prior to establishing a first N4 session on this UPF.
2	After receiving an N4 Association Setup Request, the UPF sends an N4 Association Setup Response.

Configuring the CP-Initiated N4 Association Setup Feature

This section describes how to configure the CP-Initiated N4 Association Setup feature.

Configuring this feature involves using the "**sx-association initiated-by-cp**" CLI command in the Control Plane Group Configuration mode. The default configuration is UPF-initiated N4 association setup procedure.

Use the following configuration to configure the N4 association setup feature.

```
configure
  context
    control-plane-group group_name
      peer-node-id ipv4-address ip_address interface n4
      sx-association { initiated-by-cp | initiated-by-up }
    end
```

NOTES:

- **initiated-by-cp**: This keyword is used to initiate the Sx association request through control plane.
- **initiated-by-up**: This keyword is used to initiate the Sx association request through user plane.
- By default, the UPF-initiated N4 association setup procedure is configured.
- To revert to the default setting, use the **no sx-association** command.

CP-Initiated N4 Association Setup Feature OAM Support

This section describes operations, administration, and maintenance information for this feature.

Show Command Support

Use the following show command to verify the CP-initiated N4 Association Setup feature configuration.

```
show control-plane-group all
```

The following is a sample output of the show command.

```
show control-plane-group all
Control Plane Group
-----
Name           : default
Sx-Association : initiated-by-up
Name           : default
Sx-Association : initiated-by-up
Node-Id        : 1.1.2.2
Interface      : N4
```




CHAPTER 8

Charging Support

This chapter covers the following topics:

- [Feature Summary and Revision History, on page 49](#)
- [Feature Description, on page 50](#)
- [How it Works, on page 50](#)
- [Configuring Credit Control for Usage Reporting, on page 57](#)
- [Configuring ACS Rulebase for Usage Reporting, on page 57](#)

Feature Summary and Revision History

Summary Data

Table 13: Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 14: Revision History

Revision Details	Release
Usage reporting with Rating-Group and Service ID is introduced.	2020.02.5
First introduced.	2020.02.0

Feature Description

The usage measurement and reporting function in User Plane Function (UPF) is controlled by the Session Management Function (SMF). The SMF controls these functions by:

- Creating the necessary PDRs to represent the service data flow, application, bearer or session (if they are not existing already).
- Creating the URRs for each Charging Key and combination of Charging Key and Service ID. Also, creating URRs for a combination of Charging Key, Sponsor ID, and Application Service Provider Id.
- Associating the URRs to the relevant PDRs defined for the PFCP session, for usage reporting at SDF, Session or Application level.
- For online charging, the SMF provisions Volume and Time quota, if it receives it from the Online Charging Server (OCS).

Offline Charging Events Reporting over N4

The User Plane Function (UPF) supports session-based offline charging, PDU session level reporting triggers in URR (volume and time threshold), PFCP session report procedure, and usage report IE support in the PFCP modification response for the Session-AMBR change, QoS, and User Location triggers.

Online Charging Support over N4

The UPF supports flow-based online charging support, which includes URR enhancements for Volume and Time quota and Usage reporting IE in PFCP modify response. In addition, the UPF supports online charging triggers, which include a PFCP session report request support with usage reporting IE.

How it Works

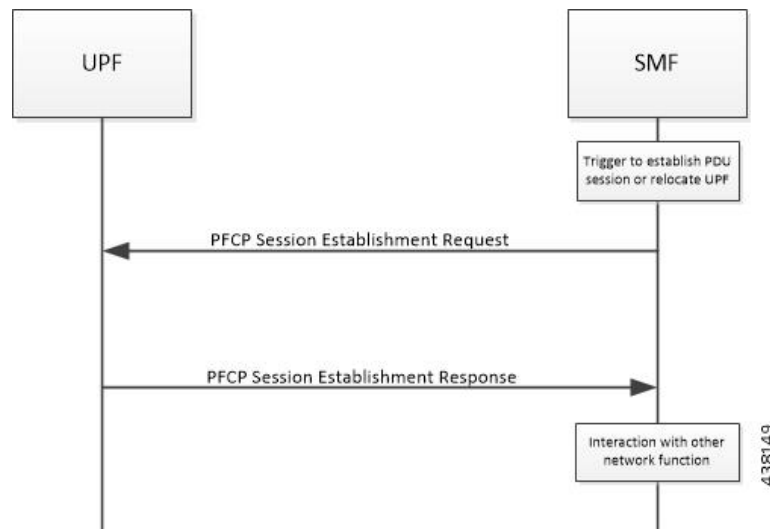
Call Flows

The following sections describe the call flows between SMF and UPF for PFCP Session Management.

PFCP Session Establishment Procedure

The PFCP Session Establishment procedure establishes a PFCP session between SMF and UPF. It also configures rules in UPF for handling incoming packets. In addition, the SMF sends Create URR IE, which comprises of triggers and thresholds that are intended for reporting.

The following call flow depicts the PFCP Session Establishment procedure.

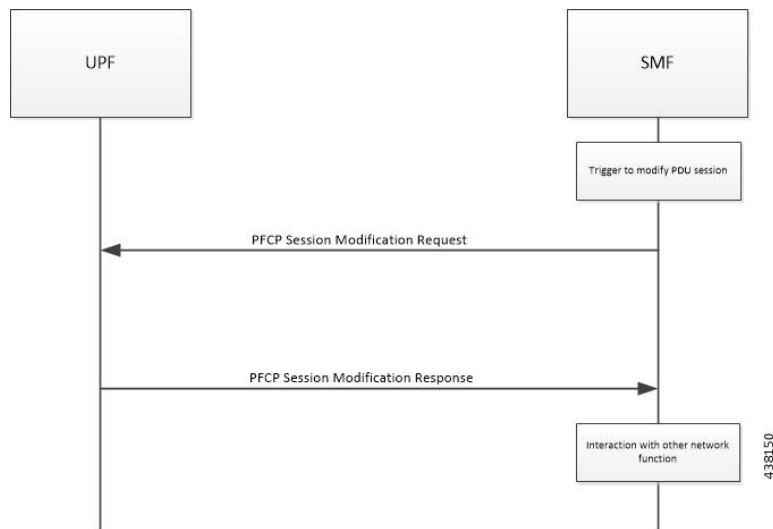


Step	Description
1	The SMF receives the trigger to establish a new PDU Session or change the UPF for an established PDU Session.
2	The SMF sends the PCF Session Establishment Request message to the UPF. This message contains the structured control information, which defines the UPF's behavior.
3	The SMF provisions URR with Create URR IE. The Create URR associates with PDRs by adding URR-ID IE in Create PDR IE. It includes various triggers and thresholds for usage reporting.
4	When the same URR is associated with multiple PDRs, URRs are linked with another URR. Therefore, if a report for an URR is sent, its linked URR is also reported.
5	The UPF responds with the PCF Session Establishment Response message to the SMF. For instance, Created PDR IE, in which UPF Flow-TEID is sent to gNB for GTP-u encapsulation for data traffic.
6	The SMF interacts with the network function, which triggered this procedure. For instance, AMF or PCF.

PCF Session Modification Procedure

The SMF uses the PCF Session Modification procedure to modify an existing PCF session on the UPF. For instance, configuring a new rule, modifying an existing rule, or deleting an existing rule, and so on. The SMF sends the Create URR IE, Update URR IE (to update the trigger or threshold) and Remove URR IE (to remove an existing URR created earlier by SMF during Session Establishment Procedure) in the same message.

The following call flow depicts the PCF Session Modification procedure.

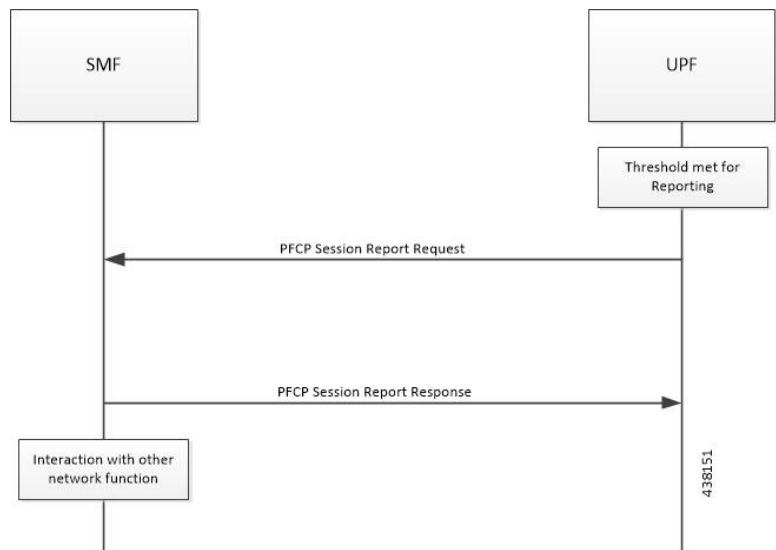


Step	Description
1	The SMF receives the trigger to modify the existing PDU Session.
2	The SMF sends an N4 session modification request message to the UPF. This message contains the structured control information, which defines the UPFs behavior.
3	The UPF identifies the PFCP session context for the Session ID to modify. It updates the parameters of this session context according to the list of parameters sent by the SMF. It then responds with a PFCP Session Modification Response message. The message contains the information, which the UPF must provide to the SMF (in response to the control information received).
4	If the SMF sends the QAURR flag set in PFCPSMReq-Flag IE or URR ID (s) with Query URR IE (e), then UPF sends the usage report IE for the corresponding URR with the PFCP Session Modification response.
5	The UPF provisions and acts based on the Create URR, Update URR or Remove URR IE sent by the SMF.
6	The SMF interacts with the network function, which triggered this procedure. For instance, AMF or PCF.

PFCP Session Reporting Procedure

The UPF uses PFCP Session Reporting procedure to report information that is related to the PFCP session to the SMF (usage report IE). Once the threshold hits the volume, time or event measurement and sets the corresponding trigger for reporting, the message is sent to the SMF by the UPF.

The following call flow depicts the PFCP Session Reporting procedure.

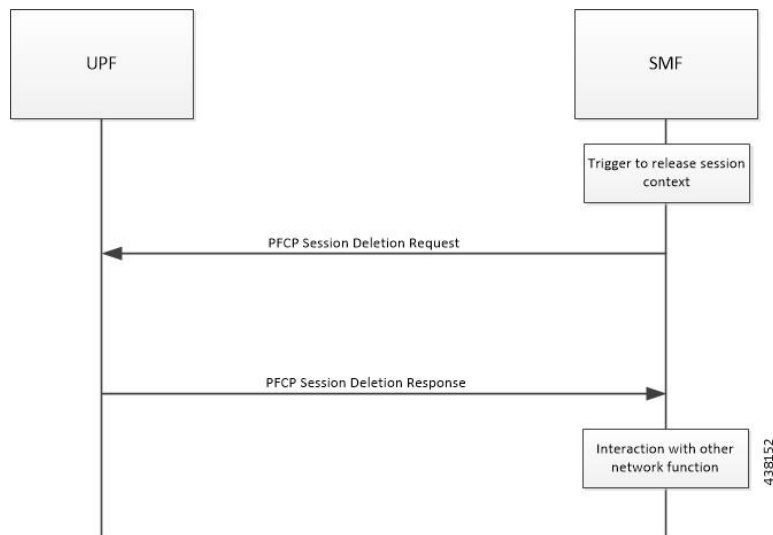


Step	Description
1	Once the provisioned threshold is met (for time, volume or event, and trigger is set for reporting), the UPF sends PFCP Session Report Request with usage report IE and usage details for volume, time, or threshold.
2	The SMF responds with PFCP Session Modification Response with success or failure message. No failure handling is needed on the UPF.
3	The SMF interacts with the network function, which triggered this procedure. For instance, AMF or PCF.

PFCP Session Deletion Procedure

The PFCP Session Deletion procedure deletes an existing PFCP session between the SMF and UPF. The SMF initiates a PFCP Session Deletion procedure toward the UPF to delete an existing PFCP session. The UPF sends the Session Deletion Response including the Usage Report for all URRs provisioned earlier.

The following call flow depicts the PFCP Session Deletion procedure.



Step	Description
1	The SMF receives the trigger to remove the PFCP session context for the PDU Session.
2	It sends the PFCP Session Delete Request message to the UPF.
3	The UPF identifies the PFCP session context for the Session ID to remove. It then removes the whole session context. In addition, the UPF responds with a PFCP Session Delete Response message that contains any information the UPF provides to the SMF. For instance, the UPF sends usage report for all the URR provisioned for this session.
4	The SMF interacts with the network function, which triggered this procedure. For instance, AMF or PCF.

IEs Supported for Offline Charging Reporting

The following trigger Information Elements (IEs) support offline charging Reporting over N4:

- **Periodic Reporting** – When this trigger is set, the UPF sends resource usage report periodically to Session Management Function (SMF). The intervals that are required for periodic reporting are sent with the measurement period IE.
- **Volume Threshold** (when the volume threshold reaches UL, DL, and Total) – This trigger is set when the volume-based measurement is required. The SMF sends the traffic volume value along with the volume threshold IE, while the UPF sends the traffic usage report when the traffic volume is reached for the specific Usage Reporting Rule (URR).
- **Time Threshold** (when the time threshold is reached) – This trigger is set when the time-based measurement is set. The SMF sends the time threshold value along with the time threshold IE, while the UPF sends resource usage report when the time threshold is reached for the specific URR.
- **Linked Usage Reporting** – The UPF sends the usage report of this specific URR when this trigger is set. In addition, the usage report is sent to any of the URRs linked to UPF when this trigger is set. The UPF sends the linked URR-Id along with the linked URR-Id IE.

- Packet Forwarding Control Protocol (PFCP) Session Deletion – A usage report generates (in a PFCP Deletion Response) for a URR due to the termination of the PFCP session. Similarly, a usage report generates (in a PFCP modification response) for a URR due to the removal of a specific URR.
- Update URR – This trigger is set when update URR request is received.

IEs Supported for Online Charging Reporting

The following IEs support online charging:

- Volume Quota – The SMF requests the UPF to stop forwarding packets or allow forwarding some limited user plane traffic (based on the operator policy in UPF) with this IE. If no Volume Threshold is provisioned – to generate a usage report – and when the measured traffic reaches the quota, this IE is used.
- Time Quota - The SMF requests the UPF to stop forwarding packets or allow forwarding some limited user plane traffic (based on operator policy in UPF) with this IE. If no Volume Threshold is provisioned – to generate a usage report – and when the measured traffic reaches the quota, this IE is used.
- Monitoring Time – This IE is used by the SMF to send the time (UTC format) at which the UPF can re-apply the volume or time threshold. Also, the SMF sends any one of the Subsequent Volume, Time, Volume Quota, Time Quota, and Quota IEs, which is re-applied at the Monitoring Timestamp.
- FAR (Forwarding Action Rule) ID for Quota Action – This IE is used by the SMF to identify the substitute FAR the UPF applies – for the traffic that is associated to the URR – when any of the Volume, Time or quota is exhausted. This FAR requires the UPF to drop the packets or redirect the traffic toward a redirect destination.
- Subsequent Volume Threshold – When volume-based measurement is used and Monitoring Time IE is available, this IE is also present. The presence of this IE indicates the existence of the traffic volume value (the network resources usage reported by the UPF to the SMF) for this specific URR and the period after the Monitoring Time.
- Subsequent Time Threshold - When time-based measurement is used and Monitoring Time IE is available, this IE is also present. The presence of this IE indicates the existence of the time usage (the network resources usage reported by the UP function to the CP function) for this specific URR and the period after the Monitoring Time.
- Linked URR ID – When the linked usage reporting is required, this IE is used. It is possible to link multiple URR-IDs with an URR. Also, linked usage reporting is also sent in the Reporting Trigger IE.
- Measurement Method – The SMF specifies the measurement method of the network usage with the presence of this IE. The measurement method is based on volume and duration.
- Measurement Period – This IE is present to modify the measurement period.
- Periodic Reporting - When this trigger is set, the UPF sends resource usage report periodically to the SMF. The intervals that are required for periodic reporting are sent with the measurement period IE. When the trigger is set to 1, a request for periodic reporting is sent.
- Volume Threshold – This trigger is set when volume-based measurement is required. The SMF sends the traffic volume value along with the volume threshold IE, while the UPF sends the traffic usage report when the traffic volume is reached for the specific Usage Reporting Rule (URR). When the trigger is set to 1, a request for reporting – when the data volume usage reaches a volume threshold – is sent.
- Time Threshold - This trigger is set when time-based measurement is set. The SMF sends the time threshold value along with the time threshold IE, while the UPF sends resource usage report when the

time threshold is reached for the specific URR. When the trigger is set to 1, a request for reporting – when the time usage reaches a time threshold - is sent.

- Start of Traffic – The UPF sends the Usage Report once the traffic starts for an application, when this trigger is set.
- Linked Usage Reporting - The UPF sends the usage report of this specific URR when this trigger is set. In addition, the usage report is sent to any of the URRs linked to UPF when this trigger is set. The UPF sends the linked URR-Id along with the linked URR-Id IE. When the trigger is set to 1, a request for linked usage reporting is sent.

Usage Reporting in PFCP Modification Response

The UPF sends session modification response after receiving session modification request based on the IEs received in the request message. The UPF includes usage report IE in the session modification response for the following scenarios:

- Query URR Handling—The URR-Id IE is included when the SMF requests immediate usage reports from the UPF in the session modification response (for the URR-Id present in this specific IE).
- Query All URRs (QAURR) Handling—The UPF sends the usage report with session modification response for all the URRs provisioned prior by the SMF for this PFCP session once it receives the QUARR flag set in PFCPSMReq-Flags IE from SMF.
- Update URR—The SMF updates the new value of the existing IE with the old value during the session modification procedure.
- Remove URR—During the session modification procedure, the SMF removes the IE, which is not received but was available earlier.

Usage Reporting for Online and Offline Charging

Usage Reporting for Online and Offline Charging is supported in the following ways:

- URR for online charging based on Rating-Group level even if the Service ID is present under Charging-Action. This behavior is seen when diameter ignore-service-id is configured under Credit Control Group.
- URR for offline charging based on a combination of Rating-Group level and Service ID, for static and predefined rules, as configured in the Charging-Action.

Both URRs are linked by the SMF. These URRs are linked such that when an online URR is reported, an offline URR is also reported.

Usage Reporting with Rating-Group and Service ID

The functionality enables usage reporting to the SMF with the Rating-Group (RG) and/or Service ID (SI) populated in the Usage Report IE within the Session Report Request.

The RG and SI are populated using proprietary PFCP IEs and are applicable for usage reporting of URRs associated only with Static and Predefined configured rules. The values are derived from the configured

charging-action associated with the ruledefs, resulting in creation of the URRs during predefined activation or traffic hit for static rules.

Any change in RG/SI properties of the charging-action is reflected only in new URRs. The existing URRs associated with such charging-actions continue to report usage with the earlier RG+SI values.

UPF does not differentiate between usage reporting for Online and Offline URRs, and reports the RG+SI/RG/SI values configured in the charging-action, resulting in creation of the URRs.

NOTE: To know how SMF handles this functionality, refer *Dynamic Configuration Change Support* section in the *SMF Charging* chapter of *UCC 5G SMF Configuration and Administration Guide*.

Implementing the QAURR Flag

The SMF sets the QAURR flag of PFCPSMReq-Flags IE to request immediate usage reports for all the URRs previously provisioned earlier. Alternatively, SMF queries report for selected URR by sending URR-ID with Query URR IE. The UPF sends the usage report IE for corresponding URR with PFCP session modification response when the SMF sends the QAURR flag set in PFCPSMReq-Flag IE or URR-Id with Query URR IE.

Configuring Credit Control for Usage Reporting

This configuration enables to accept/ignore service ID in the Service-Identifier AVP defined in the Diameter dictionaries.

```
configure
  require active charging
  active-charging service service_name
    credit-control group group_name
      diameter ignore-service-id
    end
```

- **diameter ignore-service-id** : This command can be used to disable the usage of the Service-Identifier AVP for Gy interface implementations even if any of the Diameter dictionaries support the Service-Identifier AVP, and if this AVP should not be used for Gy interactions but must be present in GCDRs/eGCDRs.

Configuring ACS Rulebase for Usage Reporting

This section describes how to create, configure, or delete an ACS rulebase. A rulebase is a collection of protocol rules to match a flow and associated actions to be taken for matching flow. The default rulebase is used when a subscriber/APN is not configured with a specific rulebase to use.

Rulebase configuration is the one that combines all the specified configurations together to construct the static and predefined PCC rules.

```
configure
  active-charging service service_name
    rulebase rulebase_name
      action priority action_priority { [ dynamic-only ] |
static-and-dynamic | timedef timedef_name } { group-of-ruledefs
```

```

ruledefs_group_name | ruledef ruledef_name } charging-action charging_action_name [
  monitoring-key monitoring_key ] [ description description ] }
  cca quota { holding-time holding_time content-id content_id |
retry-time retry_time [ max-retries retries ] }
  credit-control-group cc_group_name
  dynamic-rule order { always-first | first-if-tied }
  egcdr threshold { interval interval [ regardless-of-other-triggers
] | volume { downlink | total | uplink } bytes }
  route priority route_priority ruledef ruledef_name analyzer { dns |
file-transfer | ftp-control | ftp-data | h323 | http | imap | mipv6 | mms
| pop3 | pptp | radius | rtcp | rtp | rtsp | sdp | secure-http | sip [
advanced | basic-and-advanced ] | smtp | tftp | wsp-connection-less |
wsp-connection-oriented } [ description description ]
  tcp check-window-size
  tcp mss tcp_mss { add-if-not-present | limit-if-present }
  tcp packets-out-of-order { timeout timeout_duration | transmit [
after-reordering | immediately ] }
end

```

NOTES:

- **rulebase** *rulebase_name*: Specifies the name of the ACS rulebase. *rulebase_name* must be an alphanumeric string of 1 to 63 characters.
- **action priority** *action_priority* { [**dynamic-only**] | **static-and-dynamic** | **timedef** *timedef_name* } { **group-of-ruledefs** *ruledefs_group_name* | **ruledef** *ruledef_name* } **charging-action** *charging_action_name* [**monitoring-key** *monitoring_key*] [**description** *description*]}: Configures the priority order in which ruledefs are matched and the associated charging action.
 - *priority* must be an integer value in the range of 1-65535.
 - *monitoring_key* must be an integer value in the range of 100000-4000000000.
- **cca quota** { **holding-time** *holding_time* **content-id** *content_id* | **retry-time** *retry_time* [**max-retries** *retries*]}: Configures the quota for the online charging.
 - *holding_time*: must be an integer value in the range of 1-4000000000
 - *content_id*: must be an integer value in the range of 1-2147483647
 - *retry_time*: must be an integer value in the range of 0-86400
 - *retries*: must be an integer value in the range of 1-65535
- **credit-control-group** *cc_group_name*: Configures the online charging parameters used by this rulebase. *cc_group_name* must be an alphanumeric string of 1 to 63 characters.
- **dynamic-rule order**: Configures the order of dynamic rule matching vs the static rules in a rulebase.
- **egcdr threshold** { **interval** *interval* [**regardless-of-other-triggers**] | **volume** { **downlink** | **total** | **uplink** } **bytes** }: Configures the threshold for offline charging.
 - **interval**: must be an integer value in the range of 60-40000000.
 - **downlink**: must be an integer value in the range of 100000-4000000000. Default: 4000000000.
 - **uplink**: must be an integer value in the range of 100000-4000000000. Default: 4000000000.

- **total**: must be an integer value in the range of 100000-4000000000.
- **route priority** *route_priority* **ruledef** *ruledef_name* **analyzer** { **dns** | **file-transfer** | **ftp-control** | **ftp-data** | **h323** | **http** | **imap** | **mip6** | **mms** | **pop3** | **pptp** | **radius** | **rtcp** | **rtp** | **rtsp** | **sdp** | **secure-http** | **sip** [**advanced** | **basic-and-advanced**] | **sntp** | **tftp** | **wsp-connection-less** | **wsp-connection-oriented** } [**description** *description*]: This command is used only on UPF.
 - *route_priority* must be an integer value in the range of 0-65535.
 - *ruledef_name* must be an alphanumeric string of 1 to 63 characters.
- **tcp check-window-size**: This command is used only on UPF.
- **tcp mss** *tcp_mss*: This command is used only on UPF. *tcp_mss* must be an integer value in the range of 496-65535.
 - **add-if-not-present** : Specifies to add the TCP MSS if not present in the packet.
 - **limit-if-present** : Specifies to limit the TCP MSS if present in the packet.
- **tcp packets-out-of-order** { **timeout** *timeout_duration* | **transmit** [**after-reordering** | **immediately**] }:
This command is used only on UPF.
 - *timeout_duration* must be an integer value in the range of 100-30000. Default value is 5000.

Sample Configuration

```

active-charging service acs
  ruledef ip-any-rule
    ip any-match = TRUE
  #exit
  urr-list upf
    rating-group 10 ser 10 urr-id 10
    rating-group 10 urr-id 50
  #exit
  charging-action starent
    content-id 10
    service-identifier 10
    billing-action egcdr
    cca charging credit rating-group 10
  exit
  credit-control group CCG
    diameter ignore-service-id
  #exit
  rulebase starent
    billing-records egcdr
    action priority 30 ruledef ip-any-rule charging-action starent
    egcdr threshold interval 3600
    egcdr threshold volume total 200000
    egcdr threshold volume downlink 100000 uplink 100000
    dynamic-rule order first-if-tied
    credit-control-group CCG
  #exit
#exit

context ISP
  apn starent.com
  accounting-mode gtp
  gtp group my_grp accounting-context ISP

```

```
    ip context-name ISP
  #exit
  gtpv group my_grp
    gtpv egcdr service-data-flow threshold interval 1200
    gtpv egcdr service-data-flow threshold volume downlink 13000
    gtpv egcdr service-data-flow threshold volume uplink 17000
    gtpv egcdr service-data-flow threshold volume total 22222
  #exit
end
```



CHAPTER 9

Deep Packet Inspection and Inline Services

- [Feature Summary and Revision History, on page 61](#)
- [Feature Description, on page 62](#)
- [How it Works, on page 62](#)
- [Supported Inline Services, on page 65](#)
- [Configuring the Static and Pre-Defined Rules, on page 86](#)
- [Configuring ACS Ruledef for L7 Protocols for DPI, on page 87](#)
- [Charging Action Configuration for L7 Protocols for DPI, on page 89](#)

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	<i>UCC 5G UPF Configuration and Administration Guide</i>

Revision History

Revision Details	Release
New DNS attributes have been introduced in EDRs.	2021.01.0
First introduced.	2020.02.0

Feature Description

One of the key product capability of Cisco 5G-UPF is integrated Deep Packet Inspection (DPI) based services. DPI is the examination of layer 7 (L7), which contains Uniform Resource Identifier (URI) information. In some cases, layer 3 (L3) and layer 4 (L4) analyzers that identify a trigger condition are insufficient for billing purposes, so layer 7 (L7) examination is used.

DPI performs packet inspection beyond L4 inspection and is typically deployed for detection of URI information at L7 (for example, DNS, HTTP, HTTPS, RTP, and RTSP URLs).

How it Works

This section describes the following functionality of DPI:

- DSCP Marking of downlink and uplink packets.
- Traffic Readdressing or Redirecting.

DSCP Marking for Downlink and Uplink Packets

Transport-level marking is the process of marking traffic at the UPF with a Differentiated Services Code Point (DSCP) value. The transport-level marking, executed on per-QoS flow, is based on the mapping from the 5QI and optional Allocation and Retention Policy (ARP) configuration from the SMF.

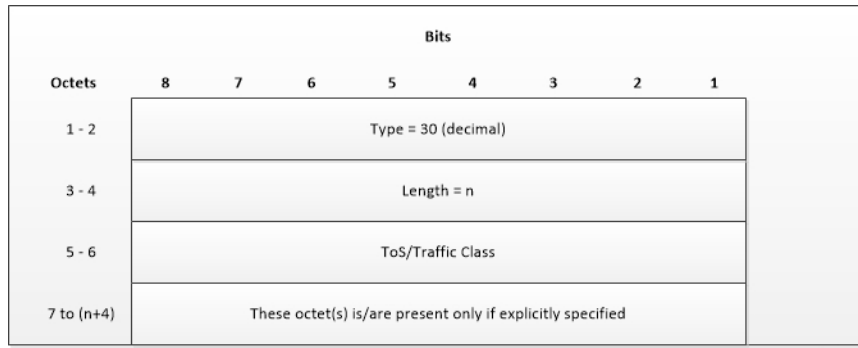
The SMF controls the transport-level marking by providing the DSCP in the ToS (IPv4) or Traffic Class (IPv6) within the "Transport Level Marking" IE in the FAR, that is associated to the PDR matching the traffic to be marked. The UPF performs the transport level marking for the detected traffic and sends the marked packet to the peer entity. The SMF can change the transport-level marking by changing the "Transport Level Marking" IE in the related FAR.

The UPF also supports the inner packet marking in which it marks the tunnel packets. As the 3GPP specification does not determine any specific IE, the UPF uses a private IE named "Inner Packet Marking".

In addition, there is also a provision to copy the DSCP of inner packet to the outer IP header. As the 3GPP specification does not determine any specific IE, the UPF uses a private IE named "Transport Level Marking Options".

Transport Level Marking IE

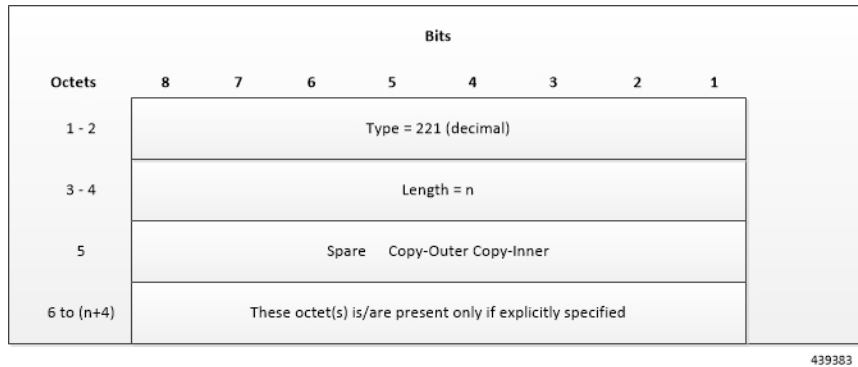
The "Transport Level Marking" IE type is encoded as shown in the following figure. It indicates the DSCP value for the downlink transport-level marking.



The encoding for Type-of-Service (ToS) or Traffic Class takes place in the form of two octets as an OctetString. The first octet contains the DSCP value in the IPv4 Type-of-Service or the IPv6 Traffic-Class field and the second octet contains the ToS/Traffic Class mask field, which is set to *0xFC*.

Transport Level Marking Options IE

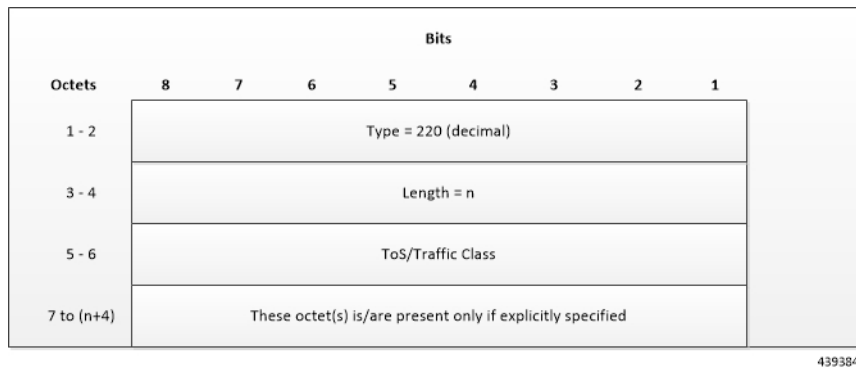
The "Transport Level Marking Options" IE type is encoded as shown in the following figure. The DSCP for downlink transport-level marking is copied from the inner packet.



The Copy-Inner and Copy-Outer flags are present in bit-0 and bit-1 of octet 5. Copy-Outer flag is not used for downlink packets because there is no outer header present in packets coming from ISP. If a Copy-Inner flag is present, then the UPF uses DSCP value from the inner packet to mark the transport-level IP header.

Inner Packet Marking IE

The "Inner Packet Marking" IE type is encoded as shown in the following figure. It indicates the DSCP value for the downlink inner packet marking.



The encoding for ToS/Traffic Class takes place in the form of two octets as an OctetString. The first octet contains the DSCP value in the IPv4 ToS or the IPv6 Traffic Class field and the second octet contains the ToS/Traffic Class mask field, which is set to *0xFC*.

NOTES:

- The original ECN bits in the IP header of User Plane packets do not change after applying transport-level marking or inner packet marking.
- If "Transport Level Marking" IE, "Inner Packet Marking" IE, or both the IEs are associated with uplink FAR, then the following rule applies for uplink packet marking:
 - If "Transport Level Marking" or "Inner Packet Marking" IE is present, its DSCP value is used.
 - If both "Transport Level Marking" and "Inner Packet Marking IE" are present, then the value from "Transport Level Marking" IE is used for uplink packet marking.

Traffic Readdressing or Redirecting

Traffic Redirection is the process of redirecting uplink application traffic to a redirect destination. For example, redirect some HTTP flows to service provisioning page. The redirect destination is provided by the PCF or it is preconfigured in the SMF or in the UPF.

The traffic redirection enforcement is applicable for the SMF or in the UPF if the traffic that the UPF supports subjects to traffic redirection. The UPF reports to the SMF whether it supports traffic redirection enforcement in the UPF through the "UP-Function Features" IE.

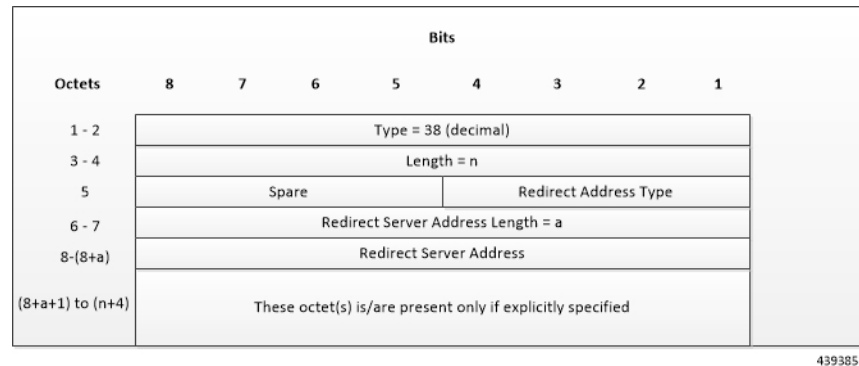
To enforce the traffic redirection in the UPF, the SMF takes the following actions:

- Creates the necessary PDRs, if it does not exist, to represent the traffic redirection.
- Creates a FAR with:
 - The "Redirect Information" IE, that includes the redirect destination, if the traffic needs redirection towards a redirect destination that is provided by the SMF. The redirect destination from the SMF prevails over a redirect destination that is preconfigured in the UPF.
 - For HTTP traffic redirection, the Redirection Address Type is set to "URL" and the SMF sets the "Destination Interface" IE in the FAR to "Access" (to forward the HTTP Response message with a status-code indicating redirect). For other types of traffic redirection, the "Destination Interface" IE in the FAR is set to "Core".

- Associates the FAR to the above PDRs of the PFCP session.

Redirect Information IE

Redirect information is encoded as follows:



"Redirect Address Type" indicates the type of the redirect address:

Redirect Address Type	Value (Decimal)
IPv4 address	0
IPv6 address	1
URL	2
SIP URI	3
Spare, for future use.	4–15

The "Redirect Server Address Length" indicates the length of the "Redirect Server Address". The "Redirect Server Address" encoding is in UTF8String format and contains the address of the redirect server (for example, HTTP redirect server, SIP server) with which the end user connects.



Important

In this release, only Redirect Address Type URL is supported for dynamic rule when FAR is associated with URR where quota expires.

Supported Inline Services

Application Detection and Control

The ADC in-line service is mainly used to detect Peer-to-Peer protocols by analyzing traffic. Other popular applications that generate the bulk of Internet traffic like Social Networking and Gaming applications can be detected.

The in-line service known as ADC is also referred as "P2P". Peer to Peer (P2P) is a term used in two slightly different contexts. At a functional level, it means protocols that interact in a peering manner, in contrast to client-server manner. There is no clear differentiation between the function of one node or another. Any node

can function as a client, a server, or both — a protocol may not clearly differentiate between the two. For example, peering exchanges may simultaneously include client and server functionality, sending and receiving information.



Note The ADC support is a licensed feature. Contact your Cisco Account or Support representative for information on how to obtain a license.

Content Filtering

Content Filtering is an in-line service available for 3GPP and 3GPP2 networks to filter HTTP requests from mobile subscribers based on the URLs in the requests. This enables operators to filter and control the content that an individual subscriber can access, so that subscribers are inadvertently not exposed to universally unacceptable content and/or content inappropriate as per the subscribers' preferences.

Content Filtering Configuration

Use the following additional configuration to enable the content filtering:

```
configure
  require user-plane content-filtering
  content-filtering category database directory path path_address
  content-filtering category database max-version version_number
end
```



Note The above configuration must be configured on the UPF, during boot time, to enable Content Filtering. Defining the above configuration post the User Plane configuration will lead to errors and inconsistencies.

Show Commands Input and/or Outputs

```
show subscribers user-plane-only callid call_id full all
```

SMF provides Content Filtering Policy ID in the Session Establishment/Modification Request. The following fields are displayed in support of this feature:

- SUBSCRIBER PARAMS
 - Content Filtering Policy ID

DNS Snooping

Charging

The charging of DNS Snooping takes place at SM-P.

Rule Definitions

Use the following CLI commands for specifying the rule definition hostnames (domain-names) and part of the host names.

```
ruledef <ruledef_name>
    ip [server-domain-name {contains|=|ends-with|starts-with} <url_string>]
    ip [server-domain-name {contains|=|ends-with|starts-with} <url_string>]
    multi-line-OR enabled
```

Use the no version of this CLI to delete the ruleline for ip server- domain-name.

```
ruledef <ruledef_name>
    no ip [server-domain-name {contains|=|ends-with|starts-with} <url_string>]
    exit
```

Use the following CLI for configurable timer of DNS entries at ECS level.

```
configure
    active-charging service service_name
        ip dns-resolved-entries timeout <value_secs>
    end
```

Whenever the ruledef containing the ip server-domain-name keyword is defined and used in rulebase, the ip-table is created per rulebase per instance.

Rule Matching

The functionality remains the same as the non-CUPS architecture.

Show CLIs

Use the following CLIs to check the table for DNS IP entries:**show user-plane-service [statistics dns-learnt-ip-addresses {summary | sessmgr instance <id> |all [verbose] }]**

Bulkstats

The following bulkstats are available in support of DNS Snooping feature:

- ecs-dns-learnt-ipv4-entries
- ecs-dns-flushed-ipv4-entries
- ecs-dns-replaced-ipv4-entries
- ecs-dns-overflown-ipv4-entries
- ecs-dns-learnt-ipv6-entries
- ecs-dns-flushed-ipv6-entries
- ecs-dns-replaced-ipv6-entries
- ecs-dns-overflown-ipv6-entries

The above bulkstats are added in the ECS schema same as in the non-CUPS architecture.



Note The SNMP Trap generation commands are not supported in CUPS DNS snooping feature.

Event Data Records

Feature Description

Event Data Records (EDR) are usage records with support to configure content information, format, and generation triggers by the system administrative user.

When a flow is terminated, the UPF generates EDRs with detail information of the terminated flow.

How It Works

EDRs are generated from User Plane on flow termination. During call setup and call modification, all call-specific attributes required for EDR generation is sent from SMF to UPF as part of the "Subscriber Params" IE within the Sx Establishment/Modification request messages.

On flow termination, the charging counters are fetched from VPP. All configured call-level attributes in the EDR format configuration along with the charging/volume counter attributes is sent to the CDRMOD proctlet. This proctlet writes these records to a file/disk, which is transferred to a configured external server.

Transaction Complete EDR

Transaction Complete EDRs are generated for HTTP EDRs when an HTTP transaction is completed. On completion, the charging counters are fetched from VPP. All configured call-level attributes in the EDR format configuration along with the charging/volume counter attributes is sent to the CDRMOD proctlet. This proctlet writes these records to a file/disk, which is transferred to a configured external server.

The following EDR attributes are supported:

- attribute sn-start-time
- attribute sn-end-time
- attribute sn-start-time format MM/DD/YYYY-HH:MM:SS:sss
- attribute sn-end-time format MM/DD/YYYY-HH:MM:SS:sss
- attribute radius-calling-station-id
- attribute radius-called-station-id
- rule-variable bearer 3gpp imsi
- rule-variable bearer 3gpp imei
- rule-variable bearer 3gpp rat-type
- rule-variable bearer 3gpp user-location-information
- rule-variable ip subscriber-ip-address
- rule-variable ip dst-address

- attribute sn-ruledef-name
- attribute sn-subscriber-port
- attribute sn-server-port
- attribute sn-app-protocol
- attribute sn-volume-amt ip bytes uplink
- attribute sn-volume-amt ip bytes downlink
- attribute sn-flow-start-time format seconds
- attribute sn-flow-end-time format seconds
- attribute sn-volume-amt ip pkts uplink
- attribute sn-volume-amt ip pkts downlink
- attribute sn-direction
- rule-variable traffic-type
- rule-variable p2p protocol
- rule-variable p2p app-identifier tls-cname
- rule-variable p2p app-identifier tls-sni
- rule-variable p2p app-identifier quic-sni
- rule-variable bearer 3gpp sgsn-address
- attribute sn-rulebase
- attribute sn-charging-action
- rule-variable flow tethered-ip-ttl
- rule-variable flow ttl
- rule-variable flow ip-control-param
- rule-variable bearer qci
- rule-variable tcp flag
- rule-variable ip server-ip-address
- attribute sn-flow-id
- attribute sn-closure-reason
- attribute sn-duration
- rule-variable ip src-address
- rule-variable ip protocol
- attribute sn-charge-volume ip bytes uplink
- attribute sn-charge-volume ip bytes downlink

The following HTTP EDR attributes are supported:

- rule-variable http url length 2000
- rule-variable http request method
- rule-variable http content type
- rule-variable http user-agent length 255
- rule-variable http reply code
- rule-variable http referer
- rule-variable http host
- rule-variable http cookie
- rule-variable http header-length
- attribute transaction-uplink-bytes
- attribute transaction-downlink-bytes

The following DNS EDR attributes are supported:

- rule-variable dns answer-ip-list
- rule-variable dns answer-name
- rule-variable dns previous-state
- rule-variable dns query-name
- rule-variable dns query-type
- rule-variable dns return-code
- rule-variable dns state
- rule-variable dns tid

Limitations

The EDR feature in UPF has the following limitations:

- EDR will be generated only for flow end condition: Idle timeout, HAGR, normal flow termination, and during the end of a session.
- Charging-Action based EDR configuration is not supported.
- Reporting EDRs are not supported.

Configuring Event Data Records

Configuring EDRs on UPF

Use the following configuration to configure EDRs on UPF:

```

active-charging service service_name
  rulebase rulebase_name
    flow end-condition { timeout | normal-end-signaling | session-end |
hagr } charging-edr charging_edr_format_name
    edr transaction-complete { http | dns } charging-edr
charging_edr_format_name
    exit
    edr-format format_name
      attribute attribute_name
    end

```

NOTES:

- **flow end-condition:** This command allows you to configure the end condition of the session flows related to a user session and triggers EDR generation.
- **timeout:** Creates an EDR with the specified EDR format whenever a flow ends due to a timeout condition.
- **normal-end-signaling:** Creates an EDR with the specified EDR format whenever flow end is signaled normally. For example, detecting FIN and ACK for a TCP flow, and create an EDR for the flow using the specified EDR format.
- **session-end:** Creates an EDR with the specified EDR format whenever a subscriber session ends. By this option session manager creates an EDR with the specified format name for every flow that has had any activity since last EDR was created for the flow on session end.
- **charging-edr** *charging_edr_format_name*: Specifies the charging EDR format.
- **hagr:** Creates an EDR with the specified EDR format whenever a flow is terminated due to Inter-chassis Session Recovery action.
- **http:** Specifies HTTP protocol related configuration.
- **dns:** Specifies DNS protocol related configuration.

Configuration to Enable EDR Module

Use the following configuration to enable EDR module.

```

configure
  context context_name
    edr-module active-charging-service
  end

```

Monitoring and Troubleshooting**show user-plane-service statistics rulebase name** *rulebase_name*

The following fields are displayed in support of this feature:

- Rulebase Name
 - EDRs
 - Charge Volume
 - Uplink Pkts

- Uplink Bytes
- Downlink Pkts
- Downlink Bytes
- Charging EDRs
 - Total Charging EDRs generated
 - EDRs generated for handoff
 - EDRs generated for timeout
 - EDRs generated for normal-end-signaling
 - EDRs generated for session end
 - EDRs generated for rule match
 - EDRs generated for hagr
 - EDRs generated for flow-end content-filtering
 - EDRs generated for flow-end url-blacklisting
 - EDRs generated for content-filtering
 - EDRs generated for url-blacklisting
 - EDRs generated for any-error packets
 - EDRs generated for firewall deny rule match
 - EDRs generated for transaction completion
 - EDRs generated for voip call end
 - EDRs generated for dcca failure handling
 - EDRs generated for TCP optimization on
 - EDRs generated for tethering signature change
 - EDRs generated for interim interval
 - Total Flow-Overflow EDRs
 - Total zero-byte EDRs suppressed

Flow Idle Timeout Randomization

Every two seconds, the Session Manager polls the time of the latest packet from Session Manager instance, or the fastpath stream to determine idle flows. Short length flows become idle quickly as they are short due to the lesser number of packets and are short lived, within 5–10 seconds. As a result, large number of idle flows must be deleted due to the timeout at the given polling cycle of two seconds. Deletion of idle flows is CPU intensive as it involves statistics reconciliation, EDR generation, and fast path stream deletion. You can accommodate more flows with this feature as the short lived flows get cleared aggressively.

Configuring Flow Idle Timeout Randomization in ACS

Use the following configuration to randomize the idle timeout flow.

```
configure
active-charging service service_name
  idle-timeout randomize-range range
    { default | no } idle-timeout randomize-range
  end
```

NOTES:

- **idle timeout:** Specifies the maximum duration that a flow can remain idle for, in seconds. Seconds must be an integer from 5 through 30. The flow will then be terminated based on the random value.
- **randomize-range:** Specifies the range of a period of time in seconds. The idle timeout applied, will be different for each flow.

For example,

```
idle-timeout randomize-range 20
```

An integer random number is generated from 0 through 20. This number is added to the configured idle timeout value to check if the flow has become idle in the two second timer processing. If the idle timeout configured is 60 seconds, the actual timeout that is applied to each flow will be random in the range between $60 + 20$ seconds causing staggered flow deletion.

- **no:** Disables the idle timeout randomization. This command is disabled by default.
- **default:** Configures the idle timeout randomization command with its default setting in seconds. Seconds must be an integer from 0 through 30. Default range is 0–30 seconds.

For example, **default idle-timeout randomize-range** is equal to **idle-timeout randomize-range 30**.

HTTP URL Filtering

The HTTP URL Filtering feature simplifies rule definitions used for URL detection.

The HTTP request packet can have a proxy (prefixed) URL and an actual URL. If a proxy URL is found in the HTTP request packet, the HTTP URL Filtering feature truncates this URL from the parsed information and only the actual URL is used for rule matching and Event Data Records (EDR) generation.

Configuring the HTTP URL Filtering Feature

This section describes how to configure the HTTP URL Filtering feature.

Configuring Group of Prefixed URLs

To configure the group of prefixed URLs, use the following CLI commands:

```
configure
active-charging service ecs_service_name
  group-of-prefixed-urls prefixed_urls_group_name
  end
```

Configuring URLs in the Group of Prefixed URLs

To configure URLs to be filtered in the group of prefixed URLs, use the following CLI commands:

```
configure
  active-charging service ecs_service_name
    group-of-prefixed-urls prefixed_urls_group_name
      prefixed-url url_1
      ...
      prefixed-url url_10
    end
```

Enabling the Group of Prefixed URLs in Rulebase

To enable the group of prefixed URLs in rulebase for processing prefixed URLs, use the following CLI commands:

```
configure
  active-charging service ecs_service_name
    rulebase rulebase_name
      url-preprocessing bypass group-of-prefixed-urls
prefixed_urls_group_name_1
      ...
      url-preprocessing bypass group-of-prefixed-urls
prefixed_urls_group_name_64
    end
```

This configuration on the control plane chassis will be pushed to the user plane with a PFD message for “group-of-prefixed-urls” and “rulebase-url-preprocessing” separately.

The group of prefixed URLs has the list of proxy URLs, which must be truncated. The rulebase contains multiple group of prefixed urls, which must be filtered. Charging ruledefs contain rules for actual URLs that must be searched after truncating URLs in the group of prefixed URLs.



Note

- Each group of prefixed URLs can have a maximum of ten prefixed URLs.
- A maximum of 64 group of prefixed URLs can be created and configured.

Show Commands

show user-plane-service group-of-prefixed-urls all | name *group_name*

This show command can be used on the user plane to verify whether the group of prefixed URLs are pushed or not. The output of this command is as follows:

- Name of the group of prefixed URLs
- Prefixed URLs
- Total number of prefixed URLs found

show user-plane-service rulebase name *rbase_name*

This show command can be used on the user plane to check whether the group of prefixed URLs is configured in rulebase or not. The output of this command is as follows:

- Name of rulebase
- Name of the groups of prefixed Urls for URL pre-processing

show user-plane-service statistics analyzer name http

The output of this command is as follows:

- Total HTTP Sessions
- Current HTTP Sessions
- Total Uplink Bytes
- Total Downlink Bytes
- Total Uplink Pkts
- Total Downlink Pkts
- Uplink Bytes Retrans
- Downlink Bytes Retrans
- Uplink Pkts Retrans
- Downlink Pkts Retrans
- Total Request Succeed
- Total Request Failed
- GET Requests
- POST Requests
- CONNECT Requests
- PUT requests
- HEAD requests
- WebSocket Flows
- Invalid packets
- Wrong FSM packets
- Unknown request method
- Pipeline overflow requests
- Corrupt request packets
- Corrupt response packets
- Unhandled request packets
- Unhandled response packets
- Partial HTTP Header Anomaly prevented
- New requests on closed connection

- Memory allocation failures
- Packets after permanent failure
- Prefixed Urls Bypassed
- FastPath Statistics
- Total FP Flows
- Uplink (Total FP Pkts)
- Downlink (Total FP Pkts)
- Uplink (Total FP Bytes)
- Downlink (Total FP Bytes)



Note Prefixed URLs Bypassed counter has been added in http analyzer stats as a performance measurement to show the number of truncated prefixed URLs.

L7 Protocol

The following L7 protocols are supported as part of DPI:

- DNS
- FTP
- HTTP
- HTTPS
- RTP/RTSP
- SIP

DNS

The UPF supports DNS protocol as part of L7 Analyzer.

FTP

The UPF supports FTP protocol as part of L7 Analyzer.

HTTP

On completion of HTTP Request/Response, the uplink/downlink data packets are offloaded to VPP in the following cases:

- Content-Length – Volume-based offloading is supported for methods like GET and POST. The HTTP flow with chunk-encoding data transfer mechanism does not get offloaded irrespective of the method defined in HTTP. If the stream is offloaded based on content-length, then the stream on the other end will also get offloaded until the former is not unloaded.

- **CONNECT Method**– The method where both uplink and downlink streams are offloaded after flow is upgraded to CONNECT.
- **WebSocket Method**– After the flow is classified as WebSocket protocol, both uplink and downlink streams are offloaded.
- The streams are onloaded back in either of the following cases:
 - FIN packet received.
 - Content-length is breached.
 - PDN update.

Header Parsing

Only the header fields defined in ruledefs, which are included in rulebase, are parsed. Or, in case of features like x-header, redirection is configured which has dependencies on some of the HTTP header fields.

HTTP Charging

- Complete packets are charged.
- Partial packets are charged on completion. Packet completing the partial packet is also charged.
- Concatenated packets are charged.
- Delay Charging is enabled – Control packets are charged against application-based rule, depending on delay charging CLI configuration.
- Response-based charging is enabled – After HTTP request's response is received, then the HTTP request is charged against response rule's CA.

X-Header Parsing and Rule-Matching

Ruledefs with x-header rule-lines are parsed and matched.

WebSocket

Involves charging of subsequent packets of the flow after HTTP GET request as per the HTTP request, if the HTTP flow is upgraded to be a websocket flow.

Response-Based TRM

Transactional Rule Matching is engaged after HTTP response packet is received.

URL-Based Redirection

For flow action redirect-url, encrypt is not supported. Currently, the following dynamic fields are supported:

- #HTTP.URI#
- #HTTP.HOST#
- #HTTP.URL#

- #ACSMGR_BEARER_CALLED_STATION_ID#
- #RULEBASE#
- #RTSP.URI#

X-Header Insertion

X-header Insertion is supported in HTTP Requests. Note that:

- Flows, for which X-header is inserted in a packet, are not offloaded.
- With X-header configuration, all TCP OOO packets irrespective of transmit order CLI, will be buffered and sent out after reordering.

Limitation

- X-Header Spoofing is not supported.
- X-Header Insertion in Response packet is not supported.
- X-Header Encryption with RSA and RC4MD5 is supported but not supported with AES.
- Monitor protocol for X-Header is not supported.
- Following X-Header fields insertion is not supported in a packet:
 - QoS
 - UIDH
 - Customer ID
 - Hash Value
 - Time of the Day
 - RADIUS String
 - Session-Id
 - Congestion Level
 - User-Profile

HTTPS

The UPF supports HTTPS protocol as part of L7 Analyzer.

RTP/RTSP

The UPF supports RTP and RTSP protocols as part of L7 Analyzer.

SIP

Session Initiation Protocol is an IETF-defined signaling protocol widely used for controlling communication sessions such as voice and video calls over Internet Protocol (IP). The protocol can be used for creating,

modifying and terminating two-party (unicast) or multiparty (multicast) sessions. Sessions may consist of one or several media streams.

The UPF supports SIP as part of L7 Analyzer.

Monitoring and Troubleshooting

This section provides information regarding the CLI command available in support of monitoring and troubleshooting the feature.

Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of this feature.

DNS

Use the following CLI command to get statistics related to DNS:

```
show user-plane-service statistics analyzer name dns
```

FTP

Use the following CLI command to get statistics related to FTP:

```
show user-plane-service statistics analyzer name ftp
```

HTTP

Use the following CLI command to get statistics related to HTTP:

```
show user-plane-service statistics analyzer name http
```

HTTPS

Use the following CLI command to get statistics related to HTTPS:

```
show user-plane-service statistics analyzer name secure-http
```

RTP

Use the following CLI command to get statistics related to RTP:

```
show user-plane-service statistics analyzer name rtp
```

RTSP

Use the following CLI commands to get statistics related to RTSP:

- **show user-plane-service statistics analyzer name rtsp**
- **show user-plane-service statistics analyzer name rtsp verbose**

SIP

Use the following CLI command to get statistics related to SIP:

```
show user-plane-service statistics analyzer name sip
```

Tethering Detection

Feature Description

Tethering refers to the use of a mobile smartphone as a USB dongle/modem to provide Internet connectivity to PC devices (laptops, PDAs, tablets, and so on) running on the smartphone's data plan. Typically, for smartphone users, most operators have in place an unlimited data plan, the usage of which is intended to be from the smartphone as a mobile device. However, some subscribers use the low cost / unlimited usage data plan to provide Internet connectivity to their laptops in places where normal Internet connection through broadband/WiFi may be costly, unavailable, or insecure.

The Tethering Detection feature enables detection of subscriber data traffic originating from PC devices tethered to mobile smartphones, and also provides effective reporting to enable service providers take business decisions on how to manage such usage and to bill subscribers accordingly. Tethering Detection is supported for IPv4 (TCP) and IPv6 traffic flows.

In this release, IP-TTL based tethering is supported. This feature is configurable at the rulebase level and is applicable on all flows for all subscribers having IP-TTL configuration within the rulebase.

Configuring Tethering Support

This section describes how to configure the Tethering Support feature.

Configuring the Tethering Support feature involves the following steps:

- Rulebase Configuration for Tethering
- Ruledef Configuration for Tethering
- EDR Configuration for Tethering

Rulebase Configuration for Tethering

Use the following commands to configure the rulebase parameters for tethering.

```
configure
  active-charging service service_name
    rulebase rulebase_name
      tethering-detection ip-ttl value ttl_value
    end
```

NOTES:

- **tethering-detection:** This command allows you to enable/disable the Tethering Detection feature for the current rulebase, and specifies the database to use.
- **ip-ttl value *ttl_value*:** Specifies to perform tethering detection using IP-TTL configuration. *ttl_value* must be an integer from 1 through 255 to configure TTL values for tethered flows.

Ruledef Configuration for Tethering

Use the following commands to configure ruledef parameters for tethering.

```
configure
  active-charging service service_name
    ruledef ruledef_name
```



```

ip any-match operator_condition
tethering-detection ip-ttl flow-tethered
end

```

NOTES:

- **ip any-match** *operator_condition*: This command allows you to define rule expressions to match all IPv4/IPv6 packets.
- **ip-ttl**: Specifies to select flows that were tethered or non-tethered as per IP-TTL values.
- **flow-tethered**: Specifies to match if tethering is detected on flow.

EDR Configuration for Tethering

Use the following commands to configure EDR for tethering:

```

configure
active-charging service service_name
edr-format format_name
rule-variable flow tethered-ip-ttl priority priority_value
rule-variable flow ttl priority priority_value
end

```

NOTES:

- **edr-format** *format_name*: configures EDR formats.
- **flow**: Configures the flow related fields in an EDR.
- **tethered-ip-ttl**: IP-TTL based tethering detected on flow.
- **ttl**: Time To Live/Max hops value received in the first packet of the flow.

Monitoring and Troubleshooting

This section provides information regarding the CLI command available in support of monitoring and troubleshooting the feature.

Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of this feature.

```
show user-plane-service statistics tethering-detection
```

The following fields are displayed in support of this feature:

- Current Tethered Subscribers
- Total Tethered Subscribers
- Total flows scanned
- Total Tethered flows detected
- Total Tethered flows recovered
- Total flows bypassed for scanning

- Tethering Detection Statistics (ip-ttl)
 - Total flows scanned
 - Tethered flows detected
 - Tethered uplink packets
 - Tethered downlink packets

show user-plane-service statistics rulebase name rulebase_name

The following fields are displayed in support of this feature:

- Tethering Detection (ip-ttl)
 - Total flows scanned
 - Tethered flows detected
 - Tethered uplink packets
 - Tethered downlink packets

URL Blacklisting

Feature Description

The URL blacklisting feature regulates the subscriber's access to view or download content from websites whose URL or URI has been blacklisted. It uses a database that records a list of URLs that indicates if the detected URL is categorized to be blocked or not.

How it Works

To enable the URL blacklisting feature on UPF, URL blacklisting database should be present with a name "optblk.bin" under flash, or SFTP or under its sub-directory. This database directory path needs to be configured on user-plane, after user-plane services are brought up.

HTTP Analyzer must be enabled for URL blacklisting. The HTTP analyzer extracts URL information from the incoming HTTP request data packet. Extracted URL content is compared with the URL Blacklisting database. When the URL of incoming HTTP data packet matches with the database URL entry, that URL is treated as blacklisted URL and one of the following actions takes place on that HTTP packet:

- Termination of flow
- Packet is discarded

The URL blacklisting configurations must be configured under Rulebase configuration in Active Charging Service. Additionally, two URL blacklisting methods – Exact and Generic, are supported at Active Charging Service-level configuration.

**Important**

Blacklisting database(s) are provided by – Internet Watch Foundation (IWF) and National Center for Missing and Exploited Children (NCMEC). The UPF always receives the blacklisting database in Optimized Format.

URL Blacklisting Database Upgrade

URL database upgrade is supported in following two ways:

- Timer-based upgrade or Auto upgrade
- CLI-based upgrade or Manual upgrade

Timer-based or Auto-upgrade

After the database is loaded on the chassis for the first time, a timer, for a duration of 5 minutes, is started. This process is started to auto upgrade the database.

If at the expiry of the timer, a valid database with higher version is available at the directory path, then database upgrade procedure is initiated, and a newer version of the database is loaded on the UPF.

To upgrade a URL blacklisting database, a higher version of valid URL Blacklisting database with name “optblk_f.bin” should be present at same directory as that of current database “optblk.bin”.

After the database is upgraded successfully, the earlier “optblk.bin” file gets renamed as “optblk_0.bin” and “optblk_f.bin” file gets renamed as “optblk.bin”. Here, “optblk_0.bin” file is treated as a backup file of older database.

If an additional upgrade is performed, then “optblk_0.bin” file will be renamed as “optblk_1.bin” file and current “optblk.bin” will get renamed as “optblk_0.bin”, and so on.

See the *Loading URL Blacklisting Database on UPF* section to configure the number of backup files to be stored in the database.

CLI-based or Manual Upgrade

See the *Upgrading the URL Blacklisting Database* section to upgrade the current database to a newer version.

Configuring URL Blacklisting

Loading URL Blacklisting Database on UPF

Use the following configuration to load URL blacklisting database on UPF.

```
configure
url-blacklisting database directory path database_directory_path
url-blacklisting database max-versions max_version_value
end
```

NOTES:

- **database directory path:** Configures the database directory path.
The *database_directory_path* is a string of size 1 to 255.
- **max-versions:** Configures the maximum database upgrade versions.

The *max_version_value* is an integer from 0 to 3.

Upgrading the URL Blacklisting Database

Use this configuration to manually upgrade the URL blacklisting database.

```
upgrade url-blacklisting database
end
```

Configuration to Enable URL Blacklisting

Use the following configuration to enable URL blacklisting feature on UPF.

```
configure
  active-charging service service_name
    url-blacklisting match-method [ exact | generic ]
    rulebase rulebase_name
      url-blacklisting action [ discard | terminate-flow ]
    end
end
```

NOTES:

- **match-method [exact | generic]:** Specifies the match method used for URL blacklisting.
 - **exact:** URL Blacklisting perform an exact-match of URL.
 - **generic:** URL Blacklisting perform generic-match of URL.
- **url-blacklisting action [discard | terminate-flow]:**
 - **discard:** Discards the HTTP packet received.
 - **terminate-flow:** Terminates the flow of the HTTP packet received.

Monitoring and Troubleshooting

This section provides information regarding the CLI command available in support of monitoring and troubleshooting the feature.

Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of this feature.

```
show user-plane-service url-blacklisting database
```

The following fields are displayed in support of this feature:

- URL Blacklisting Static Rating Databases:
 - Last Upgrade Status
 - Path
 - Database Status
 - Number of URLs in DB
 - Type

- Version
- Creation Time
- Hostname
- Comment
- Last Access Time
- Last Modification Time
- Last Status Change Time

show user-plane-service url-blacklisting database url database_directory_path

The following fields are displayed in support of this feature:

- URL Blacklisting Static Rating Databases:
 - Last Upgrade Status
 - Path
 - Database Status
 - Number of URLs in DB
 - Type
 - Version
 - Creation Time
 - Hostname
 - Comment
 - Last Access Time
 - Last Modification Time
 - Last Status Change Time

show user-plane-service url-blacklisting database facility sessmgr all

The following fields are displayed in support of this feature:

- URL-Blacklisting SessMgr Instance Based Database Configuration
 - SessMgr Instance
 - BL DB Load Status
 - BL DB Version
 - Number of URLs
 - Checksum

show user-plane-service rulebase name rulebase_name

The following fields are displayed in support of this feature:

- URL-Blacklisting Action
- URL-Blacklisting Content ID

show user-plane-service inline-services info

The following fields are displayed in support of this feature:

- URL-Blacklisting: Enabled
 - URL-Blacklisting Match-method: Generic

show user-plane-service inline-services url-blacklisting statistics

The following are displayed in support of this feature:

- Cumulative URL-Blacklisting Statistics
 - Blacklisted URL hits
 - Blacklisted URL misses
 - Total rulebases matched

show user-plane-service inline-services url-blacklisting statistics rulebase name rulebase_name

The following fields are displayed in support of this feature:

- Rulebase Name
 - URL-Blacklisting Statistics
 - Blacklisted URL hits
 - Blacklisted URL misses
- Total rulebases matched

Configuring the Static and Pre-Defined Rules

This section describes how to configure the static and pre-defined rules under the charging action configuration.

```
configure
  active-charging service service_name
    charging-action charging_action_name
      flow action { discard [ downlink | uplink ] | redirect-url
redirect_url | terminate-flow }
      end
```

NOTES:

- **flow action:** Specifies the action to take on packets that match rule definitions.
 - **discard [downlink | uplink]:** Specifies to discard downlink or uplink packets.
 - **redirect-url *redirect_url*:** Specifies the URL to be redirected. For example, `http://search.com/subtarg=#HTTP.URL#`
 - **terminate-flow:** Specifies to terminate the flow.
- For redirect-url, configure HTTP analyzer under rulebase. Example:

```
route priority 70 ruledef http-port analyzer HTTP
  ruledef http-port
    tcp either-port = 80
    rule-application routing
  exit
```

Configuring ACS Ruledef for L7 Protocols for DPI

A ruledef represents a set of matching conditions across multiple L3 – L7 protocol based on protocol fields and state information. Each ruledef can be used across multiple rulebases within the active charging service.



Note In UPF, if rule-line addition or deletion inside a ruledef is done during active calls and data flows, then this configuration change is not applied for current flows. However, the configuration change applies to new calls and new flows on same calls.

The following is a sample configuration that describes how to create, configure, or delete ACS rule definitions.

```
configure
  active-charging service service_name
    ruledef ruledef_name
      dns { any-match value | query-type query_type | query-name query_name
      }
      ip any-match [ = | != ] [ TRUE | FALSE ]
      ip dst-address { operator { { ipv4_address | ipv6_address } | {
ipv4_address/mask | ipv6_address/mask } | address-group ipv6_address } | { !range |
range } host-pool host_pool_name }
      ip server-ip-address { operator { { ipv4_address | ipv6_address } | {
ipv4_address/mask | ipv6_address/mask } | address-group ipv6_address } | { !range |
range } host-pool host_pool_name }
      multi-line-or all-lines
      rule-application { charging | post-processing | routing }
      { tcp | udp } { either-port port_number }
    end
```

NOTES:

- **ruledef *ruledef_name*:** Specifies the ruledef to add, configure, or delete. *ruledef_name* must be the name of an ACS ruledef, and must be an alphanumeric string of 1 to 63 characters, and can contain punctuation

characters. Each ruledef must have a unique name. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names.

- If the named ruledef does not exist, it is created, and the CLI mode changes to the ACS Ruledef Configuration Mode wherein the ruledef can be configured.
- If the named ruledef already exists, the CLI mode changes to the ACS Ruledef Configuration Mode for that ruledef. The ACS Ruledef Configuration Mode is used to create and manage rule expressions in individual rule definitions (ruledefs).
- **ip any-match** [= | !=] [TRUE | FALSE]: This command defines the rule expressions to match IPv4/IPv6 packets. The *operator* and *condition* in the command specifies the following:
 - *operator*
 - !=: Does not equal
 - <=: Equals
 - *condition*
 - FALSE
 - TRUE
- **ip dst-address** { *operator* { { *ipv4_address* | *ipv6_address* } | { *ipv4_address/mask* | *ipv6_address/mask* } } | **address-group** *ipv6_address* } | { **!range** | **range** } **host-pool** *host_pool_name* }: This command allows defining rule expressions to match IP destination address field within IP headers.
 - *ipv4_address* | *ipv6_address*: Specifies the IP address of the destination node for outgoing traffic. *ipv4_address* | *ipv6_address* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
 - *ipv4_address/mask* | *ipv6_address/mask*: Specifies the IP address of the destination node for outgoing traffic. *ipv4_address/mask* | *ipv6_address/mask* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation with subnet mask bit. The mask bit is a numeric value which corresponds to the number of bits in the subnet mask.
 - *address-group ipv6_address*: Specifies a group of IPv6 addresses configured with wildcard input and/or specialized range input. Multiple wildcard characters can be accepted as input and only one 2 byte range input will be accepted. Both wildcard character input and 2-byte range input can be configured together within a given IPv6 address.
 - **host-pool** *host_pool_name*: Specifies the name of the host pool. *host_pool_name* must be an alphanumeric string of 1 to 63 characters.
 - The *operator* in the command specifies the following:
 - !=: Does not equal
 - <: Lesser than or equals
 - =: Equals
 - >=: Greater than or equals

- **multi-line-or all-lines**: This command allows a single ruledef to specify multiple URL expressions. When a ruledef is evaluated, if the multi-line-or all-lines command is configured, the logical OR operator is applied to all the rule expressions in the ruledef to decide if the ruledef matches or not. If the multi-line-or all-lines command is not configured, the logical AND operator is applied to all the rule expressions.
- **rule-application { charging | post-processing | routing }**: This command specifies the rule application for a rule definition.
 - **charging**: Specifies that the current ruledef is for charging purposes.
 - **post-processing**: Specifies that the current ruledef is for post-processing purposes. This enables processing of packets even if the rule matching for them has been disabled.
 - **routing**: Specifies that the current ruledef is for routing purposes. Up to 256 rule definitions can be defined for routing in an Active Charging Service. Default: Disabled.
- **dns { any-match value | query-type query_type | query-name query_name }**: This command allows you to define rule expressions to match all DNS packets, or packets based on the query type or query name.
- **ip server-ip-address ip_address_value**: This command allows you to define rule expressions to match the IP address of the destination end of the connection.
- **{ tcp | udp } { either-port port_number }**: This command allows you to define rule expressions to match either a destination or source port number in UDP/TCP headers.

Charging Action Configuration for L7 Protocols for DPI

This section describes how to configure charging action. The charging action represents actions to be taken when a configured rule is matched. Actions could range from generating an accounting record (for example, an EDR) to dropping the IP packet, and so on. The charging action will also determine the metering principle—whether to count retransmitted packets and which protocol field to use for billing (L3, L4, L7, and so on).

The charging action configuration is used to define the QoS and charging related parameters associated with ruledefs.

configure

```

active-charging service service_name
  charging-action charging_action
  allocation-retention-priority priority [ pci pci_value | pvi pvi_value

  billing-action egcdr
  cca charging credit [ rating-group coupon_id ] [ preemptively-request
]

  content-id content_id
  flow action { discard [ downlink | uplink ] | redirect-url
redirect_url | terminate-flow }
  flow limit-for-bandwidth { { direction { downlink | uplink }
peak-data-rate bps peak-burst-size bytes violate-action { discard |
lower-ip-precedence } [ committed-data-rate bps committed-burst-size bytes
[ exceed-action { discard | lower-ip-precedence } ] ] } | { id id } }

```

```

next-hop-forwarding-address ipv4_address/ipv6_address
qos-class-identifier qos_class_identifier
service-identifier service_id
tft packet-filter packet_filter_name
tft-notify-ue
tos { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 |
af33 | af41 | af42 | af43 | be | ef | lower-bits tos_value } [ downlink |
uplink ]

```

NOTES:

- **charging-action** *charging_action_name*: Specifies the name of a charging action. *charging_action_name* must be an alphanumeric string of 1 to 63 characters and can contain punctuation characters. Each charging action must have a unique name.
- If the named charging action does not exist, it is created, and the CLI mode changes to the ACS Charging Action Configuration Mode wherein the charging action can be configured.
- If the named charging action already exists, the CLI mode changes to the ACS Charging Action Configuration Mode for that charging action.
- **allocation-retention-priority** *priority* [**pci** *pci_value* | **pvi** *pvi_value*]: Configures the Allocation Retention Priority (ARP). *priority* must be an integer value in the range of 1-15.
 - **pci** *pci_value* : **Specifies the Preemption Capability Indication (PCI) value. The options are:**
 - MAY_PREEMPT - Flow can be preempted. This is the default value.
 - NOT_PREEMPT - Flow cannot be preempted
 - **pvi** *pvi_value*: Specifies the Preemption Vulnerability Indication (PVI) value. The options are:
 - NOT_PREEMPTABLE - Flow cannot be preempted. This is the default value.
 - PREEMPTABLE - Flow can be preempted
- **billing-action**: Configures the billing action for packets that match specific rule definitions.
- **cca charging credit**: Enables or disables credit control charging credit behaviour.
- **content-id**: Configures the rating group.
- **flow action**: Specifies the action to take on packets that match rule definitions.
 - **discard** [**downlink** | **uplink**]: Specifies to discard downlink or uplink packets.
 - **redirect-url** *redirect_url*: Specifies the URL to be redirected.
 - **terminate-flow**: Specifies to terminate the flow.
- **flow limit-for-bandwidth**: Configures the QoS parameters such as MBR, GBR, and so on.
 - peakdataRate(MBR): Default is 3000 bps
 - peakburstsize: Default is 3000 bytes
 - committedDataRate(GBR): Default is 144000 bps
 - committedBurstSize: Default is 3000 bytes

- **nexthop-forwarding-address** *ipv4_address/ipv6_address* ,: Configures the nexthop forwarding address.
- **qos-class-identifier** *qos_class_identifier* : Configures the QCI for a charging action. *qos_class_identifier* must be an integer value in the range of 1-9 or from 128-254 (Operator specific).
- **service-identifier** *service_id*: Configures the service identifier to use in generated billing records.*service_id* must be an integer value in the range of 1-2147483647.
- **tft packet-filter** *packet_filter_name*: Specifies the packet filter to add or remove from the current charging action. *packet_filter_name* must be the name of a packet filter, and must be an alphanumeric string of 1 to 63 characters.
- **tft-notify-ue**: Control the TFT updates towards the UE based on certain trigger conditions.
- **tos**: Configures the Type of Service (ToS) octets.



CHAPTER 10

Dynamic and Static PCC Rules

This chapter covers the following topics:

- [Feature Summary and Revision History, on page 93](#)
- [Feature Description, on page 94](#)
- [Provisioning of Predefined PCC Rules, on page 94](#)
- [Dynamic PCC Rules Support, on page 95](#)
- [Rate Limiting for Static and Predefined Rules, on page 96](#)
- [Rate Limiting for Dynamic Rules, on page 97](#)
- [Standards Compliance, on page 98](#)
- [Configuring the URR IDs, on page 98](#)
- [Threshold Configuration, on page 99](#)

Feature Summary and Revision History

Summary Data

Table 15: Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	<i>UCC 5G UPF Configuration and Administration Guide</i>

Revision History

Table 16: Revision History

Revision Details	Release
First introduced.	2020.02.0

Feature Description

Dynamic PCC rules are provisioned by the PCF to the PCEF via the HTTP interface and may be either predefined/static or dynamically generated in the PCF. Dynamic PCC rules can be installed, modified and removed at any time.

Predefined PCC rules are configured in the PCEF and can be activated or deactivated by the PCF or by the PCEF at any time. Static PCC rules within the PCEF may be grouped allowing the PCF to dynamically activate a set of static PCC rules over the HTTP reference point. Those static PCC rules to be locally activated by the PCEF are not explicitly known in the PCF, but the PCF simply knows identifiers of static PCC rules to be activated from the PCF.

How it Works

Predefined PCC Rules Support

Config URR IDs are applicable for static rules and also predefined rules. When a subscriber call comes up, it traverses the static rules in rule base. The subscriber master URR list with bucket IDs as key updates the corresponding URR buckets for the various interfaces with the charging action configuration. For dynamic rules and predefined rules, URR ID list in PDR creates the URR buckets on the User Plane.

Following are the ecosystem changes to support Cisco SMF and UPF to work independently for Charging Action (vendor agnostic way) to work:

- Configurable "Config URR IDs" at UPF
- UPF to enable the local configuration for thresholds

Provisioning of Predefined PCC Rules

Predefined PCC rule is preconfigured in the SMF (for 5GC). Predefined PCC rules can be activated or deactivated by the PCF at any time. The Predefined PCC rules may be grouped allowing the PCF to dynamically activate a set of PCC rules. The SMF may enforce an activated predefined PCC rule by the PCF in the UPF by:

- Determining the service data filters or application IDs referred by the activated predefined PCC rule(s) and the corresponding QoS and charging control information respectively.
- Creating the necessary PDR(s) to identify the service data flow(s), application(s) that the predefined PCC or ADC rule refer to, if not already existing.

- Creating the necessary QER for the QoS enforcement at service data flow or application-level accordingly.
- Creating the necessary FAR if a new FAR needs to be created as result of QoS flow binding and QoS control for forwarding the detected service data flow or application traffic, or to redirect or to apply traffic steering control if included in the predefined PCC rule.
- Creating the necessary URR(s) for each monitoring key, charging key, combination of charging key and service ID, or combination of charging key, sponsor ID and Application Service Provider ID if included in the predefined PCC rule.

And, later by:

- Associating the created URR(s) to the newly created PDR(s).
- Associating the existing FAR or the new FAR to the newly created PDR(s).

Optionally, the traffic handling policies common to many PFCP sessions (that is, predefined QER(s)/FAR(s)/URR(s)) can be configured in the UPF. The SMF activates these traffic handling policies by including the Activate Predefined Rules IE within one of the following:

- The Create PDR IE in an PFCP Session Establishment Request
- The Create PDR IE in an PFCP Session Modification Request

For traffic matching PDR(s) associated with the activated predefined rules, the UPF enforces the rules. For example, the UPF generates Usage Report(s) and sends it to the SMF, for URR, and the SMF handles the usage reports.

The URR IDs used in reports triggered by a predefined rule in UPF are also preconfigured at the SMF.

Dynamic PCC Rules Support

For dynamic PCC rules multiple flows are supported on per Packet Forwarding Control Protocol (PFCP) session:

- The 5G QoS model allows classification and differentiation of specific services based on subscription-related and invocation-related priority mechanisms. These mechanisms provide abilities such as invoking, modifying, maintaining, and releasing QoS Flows with priority, and delivering QoS Flow packets according to the QoS characteristics under network congestion conditions.
- The 5G QoS model is based on QoS Flows. The 5G QoS model supports both QoS Flows that require guaranteed flow bit rate (GBR QoS Flows) and QoS Flows that do not require guaranteed flow bit rate (Non-GBR QoS Flows).
- The QoS Flow is the finest granularity of QoS differentiation in the PDU session. A QoS Flow ID (QFI) is used to identify a QoS Flow in the 5G System. User Plane traffic with the same QFI within a PDU session receives the same traffic forwarding treatment (Example - scheduling, admission threshold).
- Within the 5GS, a QoS Flow associated with the default QoS rule is required to be established for a PDU session and remains established throughout the lifetime of the PDU session. This QoS Flow must be a Non-GBR QoS Flow.
- A QoS flow is associated with QoS requirements as specified by QoS parameters and QoS characteristics. A QoS flow can either be "GBR" or "Non-GBR" depending on its QoS profile.

- For each QoS Flow, the QoS profile includes the QoS parameters:
 - 5G QoS Identifier (5QI)
 - Allocation and Retention Priority (ARP)
- For each GBR QoS flow only, the QoS profile must also include the QoS parameters:
 - Guaranteed Flow Bit Rate (GFBR) - UL and DL
 - Maximum Flow Bit Rate (MFBR) - UL and DL
- In the case of a GBR QoS Flow only, the QoS profile may also include one or more of the QoS parameters:
 - Notification control
 - Maximum Packet Loss Rate - UL and DL

During PDR creation or modification UPF receives the QER for QoS enforcement on flows.

The QoS enforcement rule correlation ID is assigned by the CP function to correlate QERs from multiple PFCP session contexts. For instance, the enforcement of APN-AMBR in the PGW-U is achieved by setting the same QoS enforcement rule correlation ID to the QERs from different PFCP sessions associated with all the PDRs corresponding to the non-GBR bearers of all the UE's PDN connections to the same APN. The QERs that are associated to the same QoS Enforcement Rule Correlation ID in multiple PFCP sessions will be provisioned with the same QER contents in each of these PFCP sessions. The QoS enforcement rule correlation ID is only used to enforce the APN-AMBR when the UE is in EPC, it may be provided by the CP function over N4 to the UP function for a PDU session may move to EPC in a later stage.

If the UPF receives QoS Enforcement Rule Correlation ID for 5G PFCP sessions, then it will enforce it.

Rate Limiting for Static and Predefined Rules

For static and predefined rules, bandwidth limiting is achieved by the bandwidth policy configuration. Bandwidth Policy must be configured on SMF and UPF under Active Charging Service Configuration Mode.

The following is an example configuration of bandwidth policy with extended bit rate:

```

config
  active-charging service ACS
    bandwidth-policy BWP
      flow limit-for-bandwidth id 1 group-id 2
      flow limit-for-bandwidth id 2 group-id 3
      flow limit-for-bandwidth id 100 group-id 100
      group-id 2 direction uplink peak-data-rate 256000 peak-burst-size 1000 violate-action
      discard
      group-id 3 direction downlink peak-data-rate 256000 peak-burst-size 1000
      violate-action discard
      group-id 4 direction uplink peak-data-rate 300000 peak-burst-size 1200 violate-action
      lower-ip-precedence
      group-id 5 direction downlink peak-data-rate 300000 peak-burst-size 1200
      violate-action
      lower-ip-precedence committed-data-rate 256000 committed-burst-size 1000
      exceed-action
      lower-ip-precedence
  
```



```

group-id 100 direction downlink peak-data-rate-kbps 4294967295 peak-burst-size
4294967295 violate-action discard
group-id 100 direction uplink peak-data-rate-kbps 4294967295 peak-burst-size
4294967295 violate-action discard
exit
charging-action catchall
flow limit-for-bandwidth id 1
exit
rulebase cisco
bandwidth default-policy BWP
exit
end

```



Note The modification of bandwidth-policy configuration is not supported.

Rate Limiting for Dynamic Rules

As per 3GPP TS 29.244, the following IE is received from SMF for QoS enforcement in Create QER or Update QER in Session Establishment or Modification Request:

- **Maximum Bitrate:** This IE is present if an MBR enforcement action is applied to packets matching this PDR. When present, this IE indicates the uplink and/or downlink maximum bit rate to be enforced for packets matching the PDR. For 5GC, this IE may be set to the value of:
 - the Session-AMBR - for a QER that is referenced by all the PDRs of the non-GBR QoS flows of a PDU session.
 - the QoS Flow MBR - for a QER that is referenced by all the PDRs of a QoS Flow.
 - the SDF MBR - for a QER that is referenced by all the PDRs of an SDF.
- **Guaranteed Bitrate:** This IE is present if a GBR has been authorized to packets matching this PDR. When present, this IE indicates the authorized uplink and/or downlink guaranteed bit rate. This IE may be set to the value of:
 - the aggregate GBR - for a QER that is referenced by all the PDRs of a GBR bearer
 - the QoS Flow GBR - for a QER that is referenced by all the PDRs of a QoS Flow
 - the SDF GBR - for a QER that is referenced by all the PDRs of an SDF
- **QoS flow identifier (QFI):** This IE is present if the QoS flow identifier is inserted by the UPF.
- **Gate Status:** This IE indicates whether the packets are allowed to be forwarded (the gate is open) or it is discarded (the gate is closed) in the uplink and/or downlink directions.
- **QER Correlation ID:** This IE is present if the UP function is required to correlate the QERs of several PFCP sessions, for APN-AMBR enforcement of multiple UE's PDN connections to the same APN.



Note Although it is not applicable, but if UPF receives QoS Enforcement Rule Correlation ID for 5G PFCP sessions then it will enforce it.

The SMF provisions QoS enforcement in UPF by creating necessary PDRs to represent SDF, QoS Flow and session and associating respective QERs as follows:

- creating QERs for the QoS enforcement at session level, SDF level.
- creating QERs for the QoS enforcement of the aggregate of SDFs with the same GBR QFI.
- associating the session level QER to all the PDRs defined for the session.
- associating the SDF or application QER to the PDRs associated to the SDF or application.
- associating the QER of the aggregate of SDFs to the PDRs associated to SDFs or applications that share the QER.

Standards Compliance

The N4 interface between SMF and UPF is specified in 3GPP TS 23.501 and 3GPP TS 23.502.

Configuring the URR IDs

Following are the steps to achieve the configurable URR IDs:

- Configuration template outside of Charging action to allow URR-Id mapping with "Rating Group" and "Service-ID".
- If a separate RG is configured for Gy, then that RG is applied for Gy bucket. If no separate RG is configured for Gy, then the same Content-id applicable for all interfaces.
- "Service-ID" would be optional for URR-ID mapping.
- URR-ID should be unique (this need to be ensured through **show configuration error** or separate script to validate. Another option would be to check during config time itself, provided this should not lead to bigger configuration loading time). The actual URR ID value on N4 interface will have additional bits along with the config URR ID value.
- For UPF, current logic for URR-ID generation need to be updated to take value from configuration. There are no changes for URR usage/generation logic/call-flow except UPF receiving config URR-ID from configuration rather than PFD message.
- Same configuration values are required at SMF as well. Configuration mistake of SMF and UPF having different URR-ID for same mapping will be avoided once common configuration point to SMF and UPF is available/enabled.

To configure URR-IDs, perform the following steps:

```
configure
  active-charging service service_name
    urr-list list_name
      rating-group group_number { service-identifier service_number | urr-id
id_range }
    end
```

**Note**

- **urr-list** *list_name*: Configures the active charging service URR list. *list_name* must be an alphanumeric string of 1 to 63 characters.
- **rating-group** *group_number*: Specifies the rating ID used in prepaid charging. *group_number* must be an integer in the range of 0 to 2147483647.
- **service-identifier** *service_number*: Specifies the number given to the service.
- **urr-id** *id_range*: Specifies the URR identifier for rating/service group. *id_range* must be an integer in the range of 1-134217727.

Threshold Configuration

The GTPP group configuration is required for threshold calculation at UPF.

UPF uses GTPP group name available from APN configuration. Only one GTPP group should be associated under APN configuration.

The following is a sample configuration:

configure

```

context context_name
  apn apn_name
    gtp group group_name
    ip context-name name
  exit
  gtp group group_name
    gtp egcdr service-data-flow threshold interval interval
    gtp egcdr service-data-flow threshold volume downlink bytes
    gtp egcdr service-data-flow threshold volume uplink bytes
    gtp egcdr service-data-flow threshold total bytes
  end

```

If any one of the above service-data-flow thresholds is hit for offline URR, the UPF sends SX_SESSION_REPORT_REQUEST towards SMF reporting the data volume.



CHAPTER 11

GTP-U Support

This chapter covers the following topics:

- [Feature Summary and Revision History, on page 101](#)
- [Feature Description, on page 102](#)
- [How it Works, on page 103](#)

Feature Summary and Revision History

Summary Data

Table 17: Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 18: Revision History

Revision Details	Release
Optimization of UDP checksum is added in this release.	2021.02.0
First introduced	2020.02.0

Feature Description

3GPP specifies provisions for UEs capable of supporting both 5G and 4G NAS to connect to E-UTRAN and 5G core network.

To forward data (G-PDUs and End Marker packets) during an EPS to 5GS handover, the SMF:

- Provisions one PDR per E-RAB (that supports data forwarding for at least one QoS flow).
- Creates and associate one QER with each PDR, including the QFI IE set to the QFI value of one of the QoS flows mapped to the E-RAB, to request the UPF to insert a GTP-U PDU Session Container extension header including the QFI.

Data forwarding during handovers between 5GS and EPS is supported as follows (see, 3GPP TS 38.300):

- For 5G to 4G handover, the source NG-RAN node sends one or several end-markers including one QFI of those QoS flows mapped to the same E-RAB and sends the end-marker packets to the UPF over the PDU session tunnel. UPF removes the QFI and maps to an appropriate E-RAB tunnel towards SGW.
- For 4G to 5G handover, the source eNB forwards the received end markers in the EPS bearer tunnel to the SGW, which forwards them to the UPF. The UPF adds one QFI among the QoS flows mapped to that E-RAB to the end-markers and sends those end-markers to the target NG-RAN node in the per PDU session tunnel.

Error Indication and GTP-U Path Failure

The UPF notifies an Error Indication message for a GTP-U peer to the sender when a GTP-PDU is received with a TEID that does not exist. This ensures that there are no stale sessions or bearers, and maintains consistency in the network.

Error Indication and GTP-U Path Failure between SMF and UPF nodes are supported over N4 interface. For the neighbor nodes, it is supported over the S1u/S5u interfaces.

Behavior variations of local-purge or signal-peer for Error Indication and GTP-U Path Failure are considered in this implementation.

- When Error Indication is received, the UPF communicates the TEID and GTPU-peer information with the SMF to ensure deletion or modification of the GTPU-peer.
- On receiving GTP-U packet with non-existing TEID, the UPF generates and sends Error Indication with TEID and GTP-U peer entries.
- The deletion of a session or a bearer is decided based on the Path Failure detection at SMF or UPF.
- GTP-U Path Failure is detected using GTP-U echo messages between UPF nodes, and between the UPF and SMF nodes.

How it Works

Call Flows

Initial Attach on E-UTRAN via MME and S-GW

Initial attach on E-UTRAN/EPS follows the procedure defined in 3GPP TS 23.401, Section 5.3.2.1.

The following diagram shows the call flow derived from 3GPP reference for initial attach on E-UTRAN/EPS.

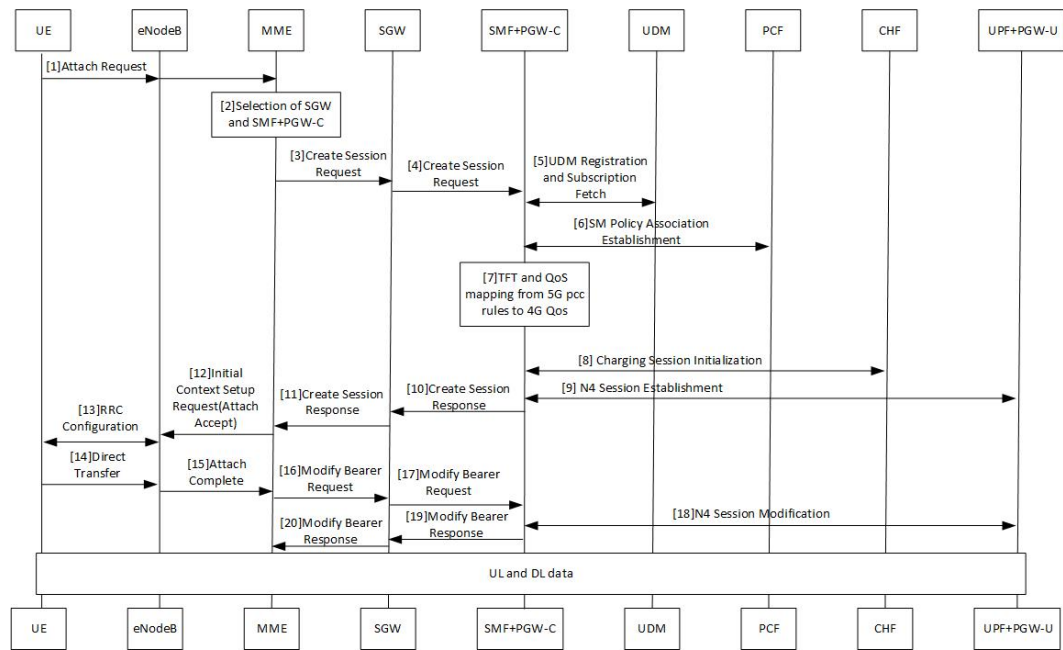


Table 19: Initial Attach on E-UTRAN via 5G Core Call Flow

Step	Description
1	At Step 9, SMF+PGW-C perform a UPF selection and perform N4 Session Establishment procedure. Since this session is a 4G session connecting to SMF+PGW-C, separate CN tunnel is created for each bearer and QFI is not sent in the QER and PDR, correlation ID might be present.
2	At Step 18, SMF+PGW-C performs N4 Session Modification to update the eNodeB TEID on the data path to the UPF.

The 3GPP specifications provide mechanisms to achieve mobility of a UE from LTE to 5G NR and vice versa. This mobility is achieved in two different architectures – with and without N26 interface between AMF and MME.

5G to EPS Handover with N26 Interface

5G to EPS handover with N26 interface is defined in 3GPP TS 23.502, Section 4.11.1.2.1. The following diagram shows the detailed call flow for N26 interface.

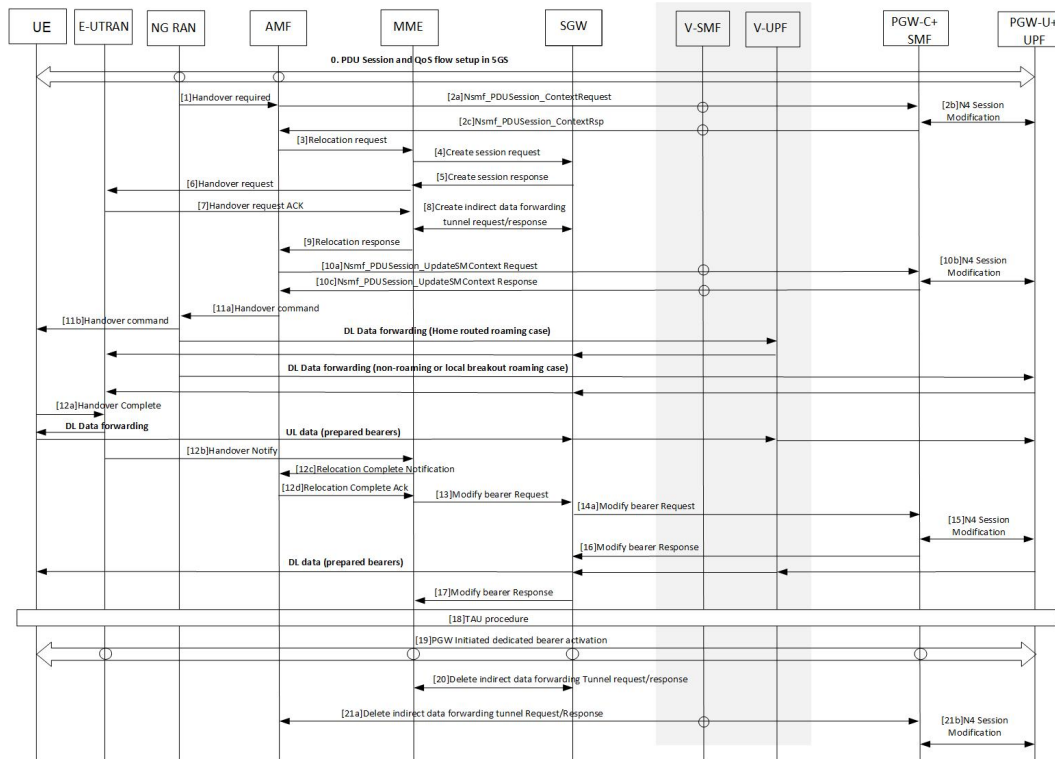


Table 20: 5G to EPS Handover with N26 Interface Call Flow

Step	Description
1	In Step 2b, the SMF+PGW-C sends the N4 Session modification to the UPF to establish the CN tunnel for each EPS bearer. The bearer mapping to the 5G QoS and PCC rules received from PCC is already present with SMF. The SMF also contains the bearer IDs obtained from the Bearer ID Allocation procedure. SMF+PGW-C creates new PDRs for the N4 session and gets TEID allocated for each bearer as required by the 4G system.
2	In Step 10b, SMF+PGW-C sends N4 Modification Request to UPF to create additional PDRs and FARs to receive the redirected DL data over the indirect tunnel from NG RAN and forward them to eNodeB. The uplink PDRs in this case has the QFI to match forwarded DL data from NG RAN and the associated QER does not have the QFI as data needs to be forwarded to eNodeB. Also, the FAR redirects the received data to eNodeB over appropriate tunnel based on the QFI.
3	At Step 11, for the QoS flows indicated in QoS Flows for Data Forwarding, NG-RAN initiates data forwarding through the UPF based on the CN Tunnel Info for Data Forwarding per PDU Session. Then the UPF maps data received from the data forwarding tunnel(s) in the 5GS to the data forwarding tunnel(s) in EPS and sends the data to the target eNodeB through the Serving GW.

Step	Description
4	In Step 15, the SMF sends N4 Modification Request to UPF to activate the DL data path to E-UTRAN. At this time, both the indirect tunnel and the direct DL path are activated towards eNodeB.
5	At Step 21, the SMF sends N4 Modification Request to the UPF to delete the indirect forwarding tunnel.

Other call flows related to EPS to 5G and 5G to EPS handover with N26 interface, or without N26 interface are defined in 3GPP 23.502, Section 4.11.1.2.1 and Section 4.11.2.

Error Indication Handling on UPF

UPF, on receiving Error Indication, initiates a PFCP Session Report Request with Error Indication Report that includes remote F-TEID containing TEID and GTP-U Peer address.

- For PGW-U, Error Indication message is sent or received over S5u.
- For SAEGW-U, Error Indication message is sent or received over S1u.
- For SGW-U, Error Indication message is sent and received over S1u and S5u.

UPF generates Error Indication with TEID and GTP-U Peer Address towards a peer when a data packet is received with TEID for which a session or bearer doesn't exist.

GTP-U Path Failure Support at UPF

GTP-U Echo Requests is initiated and sent periodically as per the configured interval on UPF. GTP-U Echo Response is sent for the GTP-U Echo Request received from SMF over GTP-U tunnel.

If Response is not received for the GTP-U Echo Request, the UPF retries Echo Requests based on configured retransmission timeout and maximum retries. When retries are exhausted, the UPF initiates PFCP node

Report Request including (Node ID, Node Report Type, User Plane Path Failure Report including Remote GTP-U Peer).

If UPF receives PFCP Node Report Response and PFCP Session Deletion Request to delete the session, it responds to the deletion request with usage reports.



CHAPTER 12

Idle Mode Buffering and Paging

This chapter covers the following topics:

- [Feature Summary and Revision History, on page 107](#)
- [Feature Description, on page 108](#)
- [Buffering Action Rule Call Flow, on page 108](#)
- [Downlink Data Report for First DL Packet, on page 109](#)
- [Paging Policy Differentiation, on page 109](#)

Feature Summary and Revision History

Summary Data

Table 21: Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 22: Revision History

Revision Details	Release
First introduced.	2020.02.0

Feature Description

A Buffering Action Rule (BAR) provides instructions to control the buffering behavior of the User Plane Function (UPF). The BAR controls the buffering behavior for all Forwarding Action Rules (FARs) of the Packet Forwarding Control Protocol (PFCP) session. This control is applicable when the PFCP session is set with an Apply Action parameter, which requests packets to be buffered and associated with the respective BAR.

How it Works

If the User Plane Function indicates the support of the feature UL or DL Buffering Control (UDBC), the SMF provides the buffering packet count IE in a BAR. The buffering count IE is created during a PFCP Session Establishment procedure or a PFCP Session Modification procedure. The SMF modifies it in a subsequent PFCP session modification request, "and" or "or" a PFCP Session Report Response message. The same BAR associates with all the FARs in a PFCP session to indicate that all service data flows in the PFCP session shares the same buffer in the UPF for the PFCP session. One BAR is created per PFCP session.

Provisioning of Buffering Action Rule in the UPF

The SMF provisions multiple buffering parameters in a BAR. It is in Create BAR or Update BAR in various PFCP messages.

Currently, UPF supports the following IE:

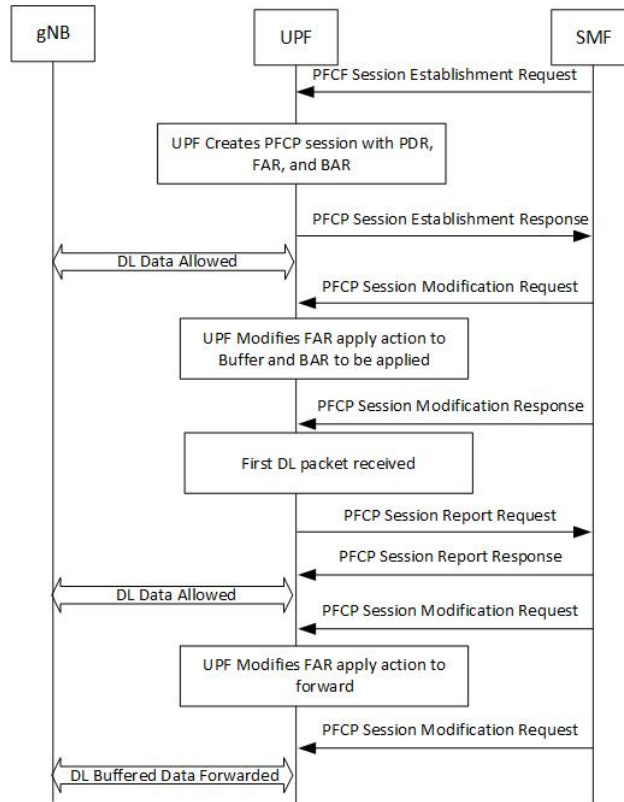
- The suggested buffering packet count IE - If the UPF indicates the support of the feature UDBC to indicate the number of packets. It includes both uplink or downlink that the SMF suggests buffering in the UPF, until it receives new instructions from the SMF. Example: when the new quota is granted.
- DL buffering suggested packet count IE – This IE is received with update BAR from SMF in Session Report Response message, if SMF wants more DL packets to be buffered on UPF.

The UPF does not apply the DL buffering duration and DL buffering suggested packet count parameters and deletes these parameters from the BAR (without explicit request from the SMF) when extended buffering of downlink data packets ends in the UPF. The UPF does not apply buffering when it receives the new instruction from the SMF. The buffered packets are either dropped or forwarded following the packet forwarding model and considering that the buffered packets are already processed earlier.

Buffering Action Rule Call Flow

This section describes the provisioning of buffering action rule in the UPF call flow.

Figure 9: Buffering Action Rule



Downlink Data Report for First DL Packet

When instructed to buffer and notify the SMF about the arrival of a DL packet, the UPF notifies the SMF, when it receives a first downlink packet for a given FAR. The UPF notifies the DL packet arrival by sending a PFCP Session Report Request including a Downlink Data Report IE identifying the PDR(s) for which downlink packets was received.

Paging Policy Differentiation

The UPF supports the Paging Policy Differentiation, for each PDR and for each packet that triggers a Downlink Data Notification, the UPF function copies the value of the DSCP in TOS (IPv4) or TC (IPv6) information received in the IP payload in Downlink Data Service Information IE.

For each PDR and for each packet that triggers a Downlink Data Notification, if the QFI of the downlink data packet is available, the QFI is also sent in Downlink Data Service Information IE.

Paging Policy Indicator (PPI)

The SMF sends the PPI value in Create QER or Update QER, if UPF needs to set Paging Policy Indicator in outgoing PDU packets.

Frame Format for the PDU Session User Plane Protocol

Downlink PDU Session Information (PDU Type 0) - This frame format is defined to allow the NG-RAN to receive some control information elements which are associated with the transfer of a packet over the interface. The following figure shows the respective DL PDU SESSION INFORMATION frame.

Figure 10: DL PDU SESSION INFORMATION (PDU Type 0) Format

Bits								Number of Octets
7	6	5	4	3	2	1	0	
PDU Type (=0)				Spare				1
PPP	RQI	QoS Flow Identifier						1
PPI		Spare						0 or 1
Padding								0-3

QoS Flow Identifier (QFI)

Description: When present, the QoS Flow Identifier (QFI) parameter indicates the QoS Flow Identifier of the QoS flow to which the transferred packet belongs.

Value Range: The value range is between 0 to 2⁶-1.

Field Length: 6 bits.

Paging Policy Presence

Description: The Paging Policy Presence (PPP) parameter indicates the presence of the Paging Policy Indicator (PPI).

Value Range: A value of 0 indicates that Paging Policy Indicator is not present and 1 indicates that Paging Policy Indicator is present.

Field Length: 1 bit.

Paging Policy Indicator

Description: When present, the Paging Policy Indicator (PPI) is used for paging policy differentiation (see details in 3GPP TS 23.501). This field applies to PDU sessions of IP type.

Value Range: the value range is between 0 to 2³-1.

Field Length: 3 bits.



CHAPTER 13

N3 Transfer of PDU Session Information

- [Feature Summary and Revision History, on page 111](#)
- [Feature Description, on page 111](#)

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Revision Details	Release
First introduced.	2020.02.0

Feature Description

The N3 transfer of PDU session information involves the inclusion of QoS Field Identifier (QFI) IE in the GTP-U extension header while performing GTP-U encapsulation toward gNodeB on the N3 interface, and removal of the GTP-U extension header while performing GTP-U decapsulation when packets are received from the gNodeB.

The QFI IE detects traffic pertaining to specific QoS sessions. It is used to send control information between the gNodeB and the UPF.

How it Works

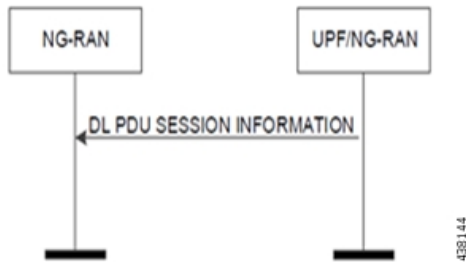
This section describes the transfer of PDU session Information procedures between the gNodeB and UPF for Uplink and Downlink packets.

Transfer of PDU Session Information for Downlink Data Packets

The Transfer of PDU Session Information for downlink data packets involves transfer of control information elements related to the PDU Session from UPF/NG-RAN to NG-RAN.

A PDU session user plane instance that makes use of this transfer procedure is associated to a single PDU Session. The procedure is invoked whenever packets for that particular PDU Session need to be transferred across the related interface instance.

The DL PDU SESSION INFORMATION frame includes a QoS Flow Identifier (QFI) field associated with the transferred packet. The NG-RAN uses the received QFI to determine the QoS flow and QoS profile which are associated with the received packet.



The following frame shows the respective DL PDU SESSION INFORMATION.

Bits								Num ber of Octet s
7	6	5	4	3	2	1	0	
PDU Type (=0)				Spare				1
PPP		RQI	QoS Flow Identifier					1
PPI			Spare					0 or 1
Padding								0-3

438145

NOTE: In current implementation, the Reflective QoS Indicator (RQI) and Paging Policy Presence (PPP) in DL PDU SESSION INFORMATION frame is not supported.

Transfer of PDU Session Information for Uplink Data Packets

The Transfer of PDU Session Information for uplink data packets involves transfer of control information elements related to the PDU Session from NG-RAN to UPF.

An UL PDU Session user plane instance that makes use of the transfer procedure is associated to a single PDU Session. This procedure is invoked whenever packets for that particular PDU Session need to be transferred across the related interface instance.

The UL PDU SESSION INFORMATION frame includes a QoS Flow Identifier (QFI) field associated with the transferred packet.



The following frame shows the respective UL PDU SESSION INFORMATION.

Bits								Num ber of Octet s
7	6	5	4	3	2	1	0	
PDU Type (=1)				Spare				1
Spare		QoS Flow Identifier						1
Padding								0-3

PDU Session Information Frame IEs

The following table describes the Information Elements present in the PDU Session Information frame.

Information Element	Description
PDU Type	<p>The PDU Type indicates the structure of the PDU session UP frame. The field takes the value of the PDU Type it identifies: "0" for PDU Type 0. The PDU type is in bit 4 to bit 7 in the first octet of the frame.</p> <p>Value range: {0= DL PDU SESSION INFORMATION, 1=UL PDU SESSION INFORMATION, 2-15=reserved for future PDU type extensions}</p> <p>Field length: 4 bits</p>
Spare	<p>The spare field is set to "0" by the sender and should not be interpreted by the receiver. This field is reserved for later versions.</p> <p>Value Range: (0-2n-1)</p> <p>Field Length: n bits</p>
QoS Flow Identifier	<p>When this IE is present, this parameter indicates the QoS Flow Identifier of the QoS flow to which the transferred packet belongs.</p> <p>Value range: {0 to 2⁶-1}</p> <p>Field length: 6 bits</p>
Padding	<p>The padding is included at the end of the frame to ensure that the PDU Session user plane protocol PDU length (including padding and the future extension) is (n*4- 2) octets, where n is a positive integer.</p> <p>Field Length: 0-3 octets.</p>

Standards Compliance

The feature complies with the following standard: 3GPP TS 38.415 V15.2.0 (NG-RAN; PDU Session User Plane Protocol).

Limitations

The following are the known limitations to this feature in this release:

- Reflective QoS Indicator (RQI) is not supported in this release.



CHAPTER 14

N4 Interface Compliance with 3GPP Specification

This chapter covers the following topics:

- [Feature Summary and Revision History, on page 115](#)
- [Feature Description, on page 116](#)

Feature Summary and Revision History

Summary Data

Table 23: Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	<ul style="list-style-type: none">• ASR 5500• VPC-SI
Feature Default Setting	Enabled - Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 24: Revision History

Revision Details	Release
Support is added for Outer Header Removal IE.	2021.04.0
In this release, PFCP library is upgraded to support the latest version of Outer Header IE.	2020.02.5

Revision Details	Release
First introduced.	2020.02.0

Feature Description

In compliance with 3GPP TS 29.244, the User Plane Function (UPF) supports the following IEs:

- Averaging Window
- Paging Policy Indicator (PPI)
- Outer Header Creation
- Outer Header Removal

Averaging Window

Averaging window IE contains the duration over which the GBR and MBR is calculated. It is sent from SMF to UPF with Create QER or Update QER parent IE, if the default pre-configured value under UPF needs to be overridden.

The following format is used for encoding and decoding of the IE:

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 157 (decimal)							
3 to 4	Length = n							
5 to 8	Averaging Window							
9 to (n+4)	These octet(s) is/are present only if explicitly specified							

NOTE: The value should be in milliseconds.

Paging Policy Indicator

The SMF sends PPI value in Create QER or Update QER, if UPF requires to set Paging Policy Indicator in outgoing packets.

In the case of Network Triggered Service Request and UPF buffering downlink data packet, the UPF includes the DSCP in TOS (IPv4) / TC (IPv6) value from the IP header of the downlink data packet. It also sends an indication of the corresponding QoS Flow in the data notification message to the SMF. When PPD applies, the SMF determines the Paging Policy Indicator (PPI) based on the DSCP received from the UPF.

In the case of Network Triggered Service Request and SMF buffering downlink data packet, when PPD applies, the SMF determines the PPI based on the DSCP in TOS (IPv4) / TC (IPv6) value from the IP header of the received downlink data packet and identifies the corresponding QoS Flow from the QFI of the received downlink data packet.

The following format is used for encoding and decoding of the IE:

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 158 (decimal)							
3 to 4	Length = n							
5	Spare					PPI value		
6 to (n+4)	These octet(s) is/are present only if explicitly specified							

NOTE: The PPI should be encoded as a 3-bit value between 0 and 7.

Outer Header Creation

Per 3GPP TS 29.244 v16.4.0, the Outer Header Creation Description field, when present, is encoded as specified in following table. It takes the form of a bitmask where each bit indicates the outer header to be created in the outgoing packet. Spare bits are ignored by the receiver.

Octet / Bit	Outer Header Created in the Outgoing Packet
5/1	GTP-U/UDP/IPv4
5/2	GTP-U/UDP/IPv6
5/3	UDP/IPv4
5/4	UDP/IPv6
5/5	IPv4
5/6	IPv6
5/7	C-TAG
5/8	S-TAG
6/1	N19 Indication
6/2	N6 Indication
6/3	TCP/IPv4
6/4	TCP/IPv6

NOTE:

- Currently, the UP/UPF doesn't support the following values of Outer Header Creation Description:
 - IPv4
 - IPv6
 - C-TAG
 - S-TAG
 - N19 Indication
 - N6 Indication

- Third and fourth bits of sixth Octet (that is, 6/3 and 6/4) are spare bits (that is, not part of 3GPP TS) used for LI over TCP.



Important If SMF/CP uses older version for Outer Header Creation, then undefined behavior (including crashes) can be seen.

Outer Header Removal

Outer Header Removal feature is used to remove GPRS Tunnelling Protocol User Plane (GTP-U) header from the uplink GTP-U packets.

The following format is used for encoding Outer Header Removal Information Element (IE):

	Bits							
Octets	8	7	6	5	4	3	2	1
1–2	Type = 95 (decimal)							
3–4	Length = n							
5	Outer Header Removal Description							
6	GTP-U Extension Header Deletion							
7 to (n+4)	These octet(s) is/are present only if explicitly specified							

Per 3GPP TS 29.244, the Outer Header Removal Description field, when present, is encoded as specified in the following table.

Table 25: Outer Header Removal Description

Outer Header to be Removed from the Incoming Packet	Value (Decimal)
GTP-U/UDP/IPv4 (See Notes 1, 2),	0
GTP-U/UDP/IPv6 (See Notes 1, 2)	1
UDP/IPv4 (See Notes 3, 6)	2
UDP/IPv6 (See Notes 3, 6)	3
IPv4 (See Note 6)	4
IPv6 (See Note 6)	5
GTP-U/UDP/IP (See Note 4)	6
VLAN S-TAG (See Note 5)	7
S-TAG and C-TAG (See Note 5)	8
For future use. Not sent. If received, it's interpreted as value "1".	9–255

NOTES:

1. The SGW-U/I-UPF stores GTP-U extension header(s). These headers are forwarded for the packets that aren't requested to be deleted by the GTP-U Extension Header Deletion field.
2. The SGW-U/I-UPF stores the GTP-U message type for a GTP-U signaling message, which must be forwarded. For example, an End Marker message.
3. This value applies to DL packets received by a PGW-U for non-IP PDN connections. These connections use SGi tunnelling based on UDP/IP encapsulation.
4. The CP function uses this value for instructing the UP function to remove the GTP-U/UDP/IP header regardless of the IP version (IPv4 or IPv6).
5. This value applies to DL packets received by a UPF over N6 for Ethernet PDU sessions.
6. This value applies to DL packets received by a UPF (PDU Session Anchor) over N6, when explicit N6 traffic routing information is provided to the SMF.

Limitations

- When outer header removal value - 6 is received for uplink PDR, the UPF maintains only IPv6 Outer Header Removal IE for uplink PDR. The UPF maintains it until an appropriate Outer Header Creation IE is received for downlink FAR.
- This feature is supported only on N4 interface.



CHAPTER 15

N4 Interface Configuration

This chapter covers the following topics:

- [Feature Summary and Revision History, on page 121](#)
- [Feature Description, on page 122](#)
- [Configuring N4 Interface, on page 122](#)

Feature Summary and Revision History

Summary Data

Table 26: Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	<i>UCC 5G UPF Configuration and Administration Guide</i>

Revision History

Table 27: Revision History

Revision Details	Release
First introduced.	2020.02.0

Feature Description

This chapter provides the configuration information to identify a peer node to be an N4 interface, and the configuration to modify N4 parameters in an Sx-Service.

Configuring N4 Interface

This section describes the following configurations:

- Identifying N4 Interface
- Adding N4-type and Modification of N4 Parameters in Sx Service

Identifying an N4 Interface

Use the following configuration to identify if a peer node is an N4 interface type.

```
configure
  control-plane-group group_name
    peer-node-id [ ipv4-address ipv4_address | ipv6-address ipv6_address ]
  interface n4
  end
```

NOTES:

- To enable the **n4 interface** CLI command, you need the **require upf** CLI command on the UPF, which depends on the UPF license.
- [**ipv4-address** *ipv4_address* | **ipv6-address** *ipv6_address*] :
 - ipv4-address** *ipv4_address*: Specifies the IPv4 address of the peer node.
 - ipv6-address** *ipv6_address*: Specifies the IPv6 address of the peer node.
- **interface n4**: Identifies the N4 interface.

Modification of N4-type Parameters in an Sx Service

Use the following configuration to modify N4-type parameters in an Sx Service.

```
configure
  context context_name
    sx-service service_name
      n4 [ max-retransmissions max_retransmission_value |
  retransmission-timeout-ms timeout_value ]
  end
```

NOTES:

- **n4**: Allows modifications to N4 parameters.

- [**max-retransmissions** *max_retransmission_value* | **retransmission-timeout-ms** *timeout_value*]:
max-retransmissions *max_retransmission_value* Configures maximum retries for Sx control packets. *max_retransmission_value* must be an integer in the range of 0 to 15. The default value is 4.
retransmission-timeout-ms: Configures the control packet retransmission timeout in Sx in milliseconds. *timeout_value* must be an integer in the range of 1000 to 20000 milliseconds. The timeout value must be configured in steps of 100; for example: 1000, 1100, 1200, and so on. The default value is 5000 milliseconds.

Statistics

This section provides information on show commands and their output available in support of this feature.

show control-plane-group

The output of this command displays the following fields for this feature:

- Interface Type – This field indicates if the peer interface is N4. It is not displayed for non-N4 interfaces.

show sx-service all

The output of this command displays the following fields for this feature:

- N4
 - N4 Retransmission Timeout
 - N4 Maximum Request Retransmission

show subscribers user-plane-only all

The output of this command displays the following fields for this feature:

- Interface
 - N4

show user-plane-service statistics all

The output of this command displays the following fields for this feature:

- N4 interface-type PDNs
 - Active
 - Setup
 - Released

show subscribers user-plane-only seid number pdr all

The output of this command displays the following fields for this feature:

show subscribers user-plane-only callid number pdr full all

- Associated-QFIs

show subscribers user-plane-only callid number pdr full all

The output of this command displays the following fields for this feature:

- QoS Flow Identifier



CHAPTER 16

N4 Session Management, Node Level, and Reporting Procedures

This chapter covers the following topics:

- [Feature Summary and Revision History, on page 125](#)
- [Feature Description, on page 126](#)
- [How it Works, on page 127](#)
- [Configuring the N4 Session/Node Level Reporting Procedures, on page 136](#)

Feature Summary and Revision History

Summary Data

Table 28: Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Revision Details	Release
First introduced.	2020.02.0

Feature Description

N4 Session Management, Node Level, and Reporting Procedures

N4 Node-level Procedures

The N4 Node-level procedures in User Plane Function (UPF) involves the following processes:

- N4 Association Set up Procedure – The procedure used for setting up an N4 association between the Session Management Function (SMF) and UPF.
- N4 Association Update Procedure – The procedure used for modifying an existing N4 association between the SMF and UPF.
- N4 Association Release Procedure – The procedure used for terminating the N4 association between the SMF and UPF.
- N4 Heartbeat Procedure – The procedure used for sending and receiving the Heartbeat request and response.
- N4 Reporting Procedure – The procedure used for reporting echo request and response for the GTP-u path failure.

N4 Session Management

N4 session management procedures are used to control the functionality of the UPF. SMF can create, update, and remove the N4 session context in the UPF, which is described in 3GPP TS 23.501, clause 5.8.2.

The following procedures are performed in N4 Session Management:

- N4 Session Establishment
- N4 Session Modification
- N4 Session Deletion

NOTE: The SMF initiates all the above procedures.

N4 Session/Node-level Reporting Procedures

Whenever the data path between UPF and gNB is down, it is detected and reported to the SMF for corrective actions. The mechanism to detect and report it to SMF is clearly defined in 3GPP specifications. The reporting happens per GTP-u Tunnel level or per GTP-u endpoint level.

Relationships

The following features support the N4 session management, node level, and reporting procedures.

End Marker Support

The UPF sends the End Marker packets to support the reordering function in the target Radio Access Network (RAN). The UPF constructs the End Marker packets that are required for the reordering function.

Constructing the End Marker Packets through UPF

At the time of the handover procedure, the PDU session for the UE – which comprises of an UPF node – acts as a PDU session anchor and an intermediate UPF terminating N3 reference point. The SMF sends an N4 Session Modification Request message with the new AN Tunnel Info of NG RAN to specify the UPF to switch to the N3 paths. In addition, the SMF also specifies the UPF to send the End Marker packets on the old N3 user plane path.

After the UPF receives the indication, the End Markers are constructed and sent to each N3 GTP-U tunnel toward the source NG RAN, after sending the last PDU on the old path.

UEs IPv4, IPv6, and IPv4v6 Support

The UPF supports UE's IPv4, IPv6, and IPv4v6 sessions.

The N4 Session Establishment and Modification procedure for IPv6 sessions is the same as for IPv4 sessions. After the session is established, the SMF sends Router Advertisement (RA) message to UE announcing the IPv6 prefix to be used for traffic. Optionally, to get the IPv6 parameter from SMF faster, the UE can also initiate IPv6 Router Solicitation (RS).

The N4 Session Establishment and Modification procedure for IPv4v6 Session are similar to the IPv4 or IPv6 sessions except for the allocation of two UE IP addresses - one for IPv4 and the other for IPv6. The SMF sends the Router Advertisement message to the UE announcing the IPv6 prefix used for traffic after the session is established. Optionally, the UE can also initiate the IPv6 Router Solicitation to receive the IPv6 parameter from the SMF quickly.

How it Works

This section describes the N4 node-level, session management, and reporting procedures and associated call flows.

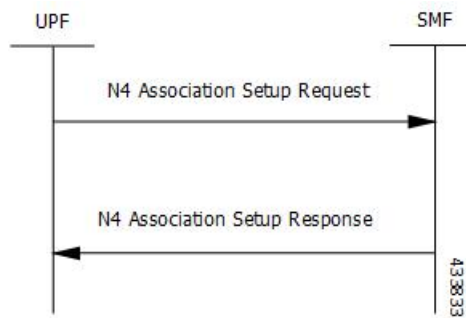
N4 Node-level Procedure Call Flows

N4 Association Setup Procedure Call Flow

The N4 Association Setup procedure creates the N4 association between the SMF and the UPF, which enables the SMF to use the UPF resources to establish N4 sessions. The N4 association setup procedure involves the following steps:

1. The UPF initiates the procedure by sending N4 Association Setup Request to the SMF.
2. The SMF sends an N4 Association Setup Response after it receives the request from the UPF.

The following call flow describes the UPF-initiated N4 Association Setup procedure:



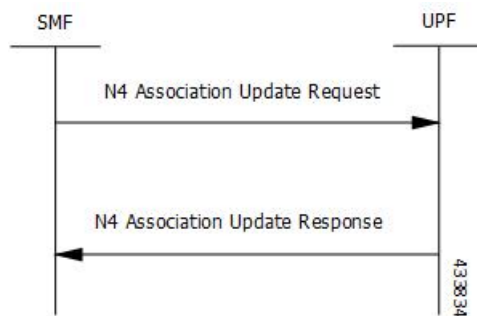
The UPF sends the following PFCP Association Setup Request:

- Node ID (UPF).
- Supported optional features in UPF. The UPF supports F-TEID allocation and release, sending of End Marker, and so on.

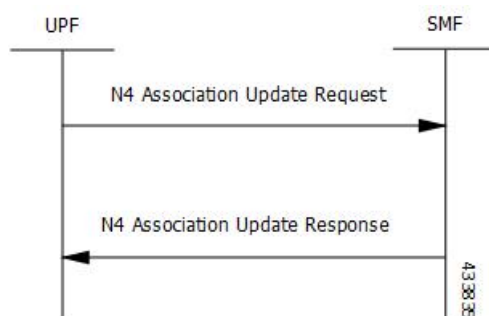
N4 Association Update Procedure Call Flow

The N4 Association Update procedure modifies an existing N4 association between the SMF and the UPF. It can be initiated either by the UPF or by the SMF to update the supported features or available UPF resources.

The following call flow depicts the SMF-initiated N4 Association Update procedure:



The following call flow depicts the UPF-initiated N4 Association Update procedure:

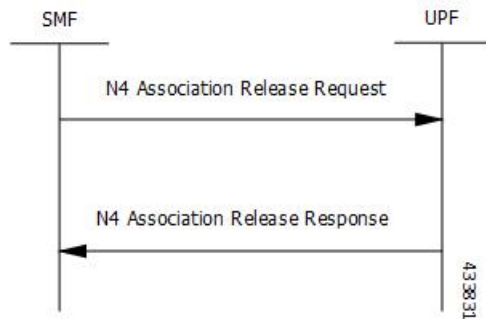


N4 Association Release Procedure Call Flow

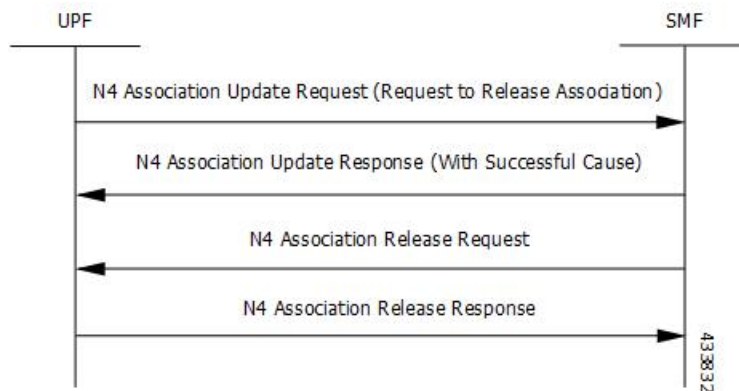
The N4 Association Release procedure terminates the N4 association between the SMF and the UPF. It can be initiated either by the SMF or by the UPF. The UPF requests the SMF to perform the release of PFCP

association by sending a PFCP Association Update Request. The SMF then initiates a PFCP Association Release Request to release the PFCP association.

The following call flow depicts the SMF-initiated N4 Association Release procedure:



The following call flow depicts the UPF-initiated N4 Association Release procedure:



N4 Heartbeat Procedure

The PFCP Heartbeat procedure includes the following messages:

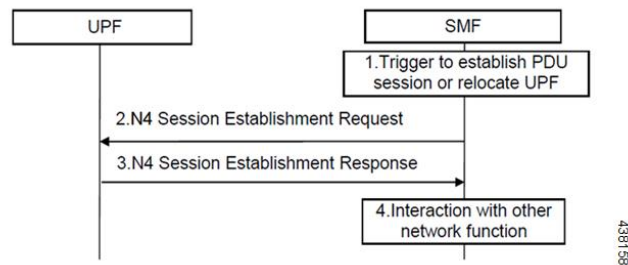
- Heartbeat Request
- Heartbeat Response

N4 Session Management Procedures Call Flows

The following section describes the N4 Session Management procedures.

N4 Session Establishment Call Flow

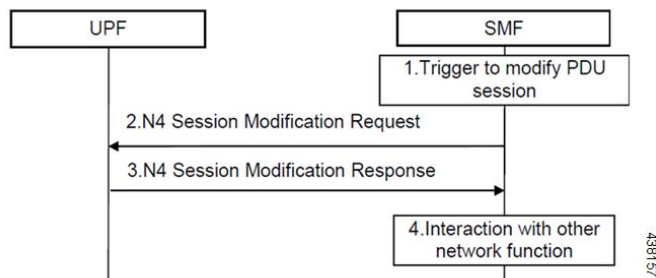
N4 Session Establishment is used to create the initial N4 session context for a PDU session at the UPF. SMF assigns a new N4 session ID and provides it to the UPF. The N4 session ID is stored by both entities and used to identify the N4 session context during their interaction. SMF also stores the relation between the N4 session ID and PDU session for a UE.



Step	Description
1	SMF receives the trigger to establish a new PDU session or change the UPF for an established PDU session.
2	SMF sends an N4 session establishment request message to the UPF that contains the structured control information which defines how the UPF needs to behave.
3	UPF responds with an N4 session establishment response message containing any information that the UPF has to provide to the SMF in response to the control information received.
4	SMF interacts with the network function which triggered this procedure. For example, AMF or PCF.

N4 Session Modification Call Flow

N4 Session Modification is used to update the N4 session context of an existing PDU session at the UPF, which is executed between SMF and UPF whenever PDU session-related parameters have to be modified.

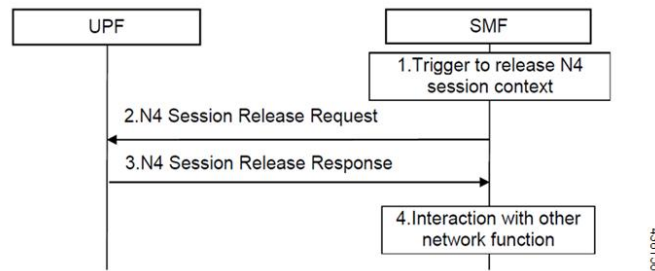


Step	Description
1	SMF receives the trigger to modify the existing PDU session.
2	SMF sends an N4 session modification request message to the UPF which contains the update for the structured control information that defines how the UPF needs to behave.
3	UPF identifies the N4 session context to be modified by the N4 session ID and updates the parameters of this N4 session context according to the list of parameters that are sent by the SMF. UPF responds with an N4 session modification response message containing any information that the UPF has to provide to the SMF in response to the control information received.

Step	Description
4	SMF interacts with the network entity which triggered this procedure. For example, AMF or PCF.

N4 Session Delete Call Flow

N4 Session Delete is used to remove the N4 session context of an existing PDU session at the UPF.

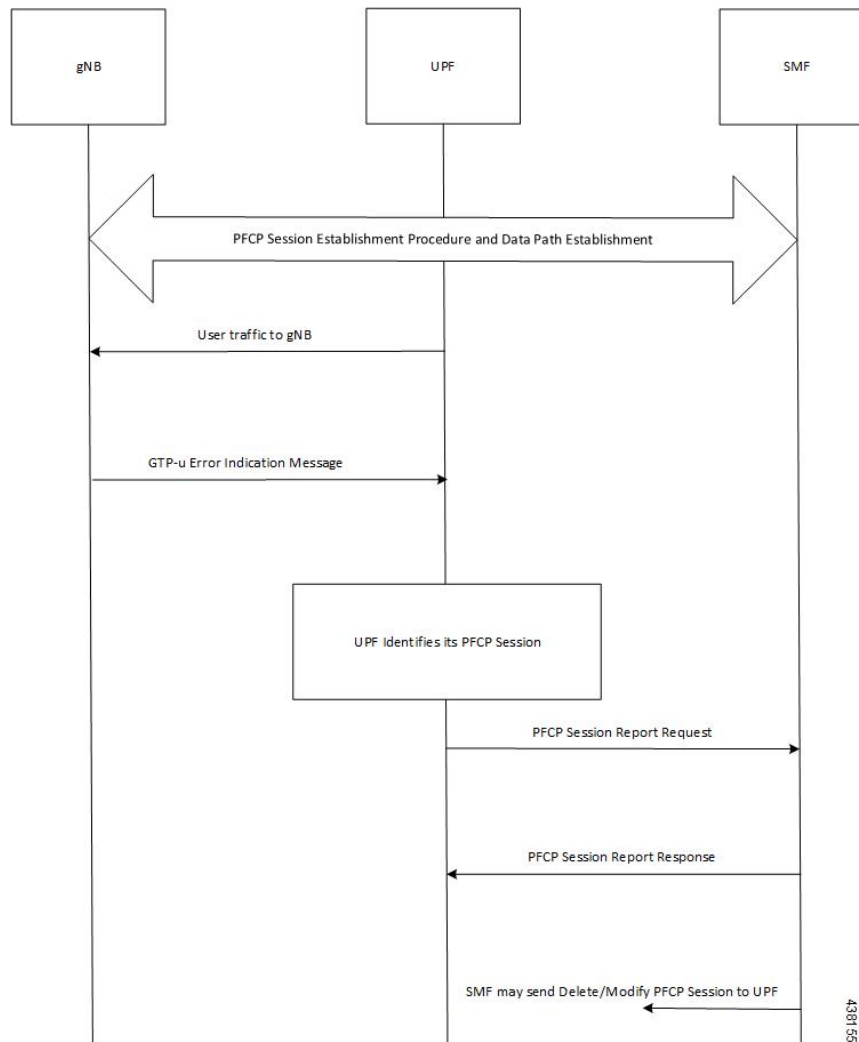


Step	Description
1	SMF receives the trigger to remove the N4 session context for the PDU session.
2	SMF sends an N4 session delete request message to the UPF.
3	UPF identifies the N4 session context to be removed by the N4 Session ID and removes the whole session context. UPF responds with an N4 session delete response message containing any information that the UPF has to provide to the SMF.
4	SMF interacts with the network entity which triggered this procedure. For example, AMF or PCF.

N4 Session/Node Level Reporting Procedure Call Flows

Session Level Reporting Due to the GTP-u Error Indication Call Flow

When the UPF receives the GTP-u Error Indication from gNB, it detects the PFCP session and sends the PFCP Session Report request to the SMF handling that session along with the Error Indication Report IE. The Error Indication IE also includes the remote F-TEID IE, which contains the GTP-u peer address and the TEID received from the GTP-u Error Indication IE.

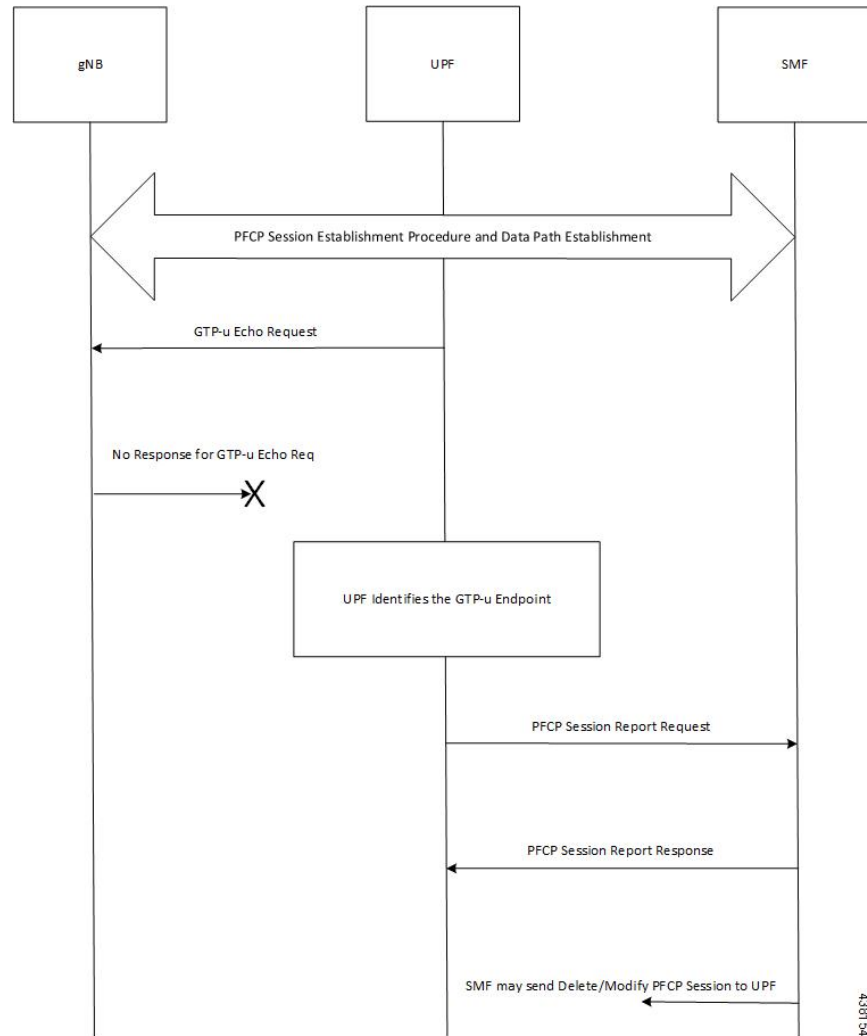


Step	Description
1	A PCFP session is established and the data traffic starts running.
2	When gNB clears up the TEID details locally for some reason, it sends the GTP-u Error Indication to UPF for unknown TEID.
3	Once the Error Indication is received, the UPF identifies the PCFP session and sends the PCFP session report request to the SMF.
4	The session report request contains the TEID and the remote IP address from where the Error Indication is received.

Node-level Reporting Procedure due to GTP-u Path Failure Call Flow

When the UPF enables GTP-u Echo procedure for GTP-u endpoints and identifies a data path failure because of no response, it sends a PCFP Node Report Request to the SMF. The Node Report Type in the PCFP Node Report Request is set to User Plane Path Failure Report when it is sent to the SMF. The Node Report procedure

includes only the peer IP address in Remote GTP-u Peer IE – the child IE of the User Plane Path Failure IE – since it is not specific to any PFCP session.

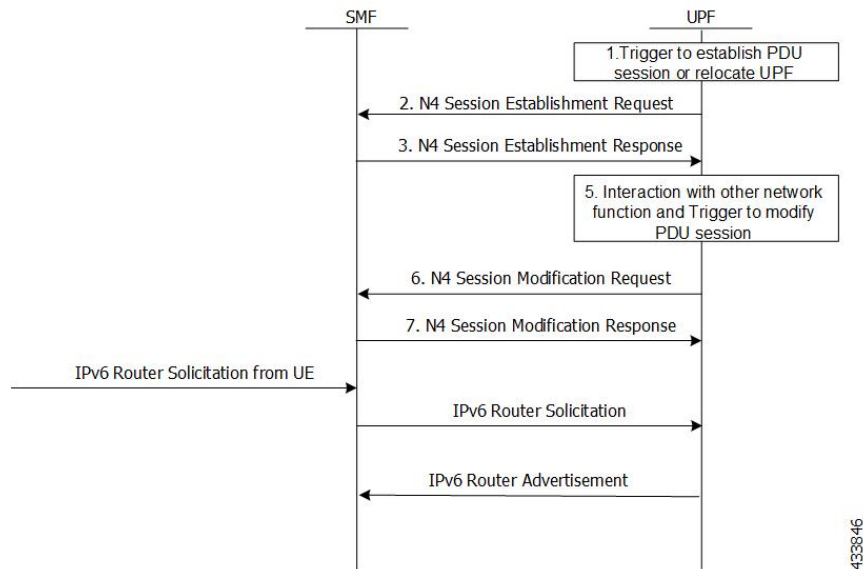


Step	Description
1	Once the PFCP session is established and GTP-u Echo procedure is configured, UPF initiates the GTP-u Echo Request for each peer with at least one GTP-u Tunnel.
2	If there is no GTP-u Echo Response received after a specified number of retries, then the UPF sends the PFCP Node Report Request to the SMF.
3	Only the peer IP address is sent in the Node Report request since it is not a GTP-u tunnel-specific failure.
4	Once the message is received, the SMF sends a Delete and Modify request for all the PFCP Sessions for that gNB to UPF.

UEs IPv4, IPv6, and IPv4v6 Support Call Flows

N4 Session Establishment and Modification Procedure for IPv6 Call Flow

The following call flow provides a high-level description of the N4 session establishment and modification procedure for IPv6.

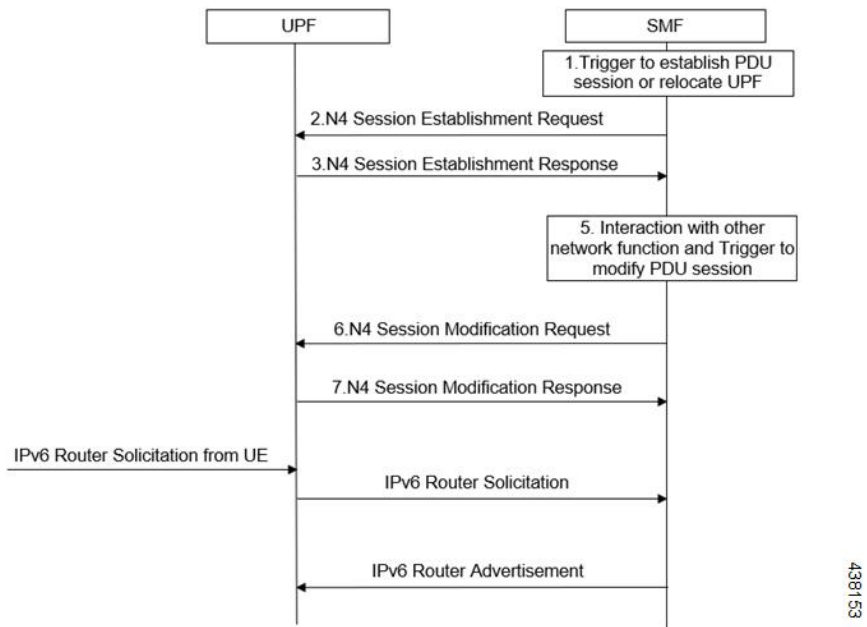


Step	Description
1	The SMF receives the trigger to establish a new PDU session or change the UPF for an established PDU session.
2	The SMF sends N4 Session Establishment Request message to the UPF, in which Create PDR IE has IPv6 UE address, and SDF filter has IPv6 filters to select the PDRs.
3	The UPF responds with an N4 Session Establishment Response message containing any information that the UPF must provide to the SMF in response to the control information received.
4	The SMF interacts with the network function and triggers to modify the PDU session.
5	The SMF sends an N4 Session Modification Request message to the UPF that contains the update for the structured control information which defines how the UPF needs to behave.
6	The UPF identifies the N4 session context to be modified by the N4 Session ID. Then, the UPF updates the parameters of this N4 session context according to the list of parameters sent by the SMF. The UPF responds with an N4 session modification response message containing any information that the UPF must provide to the SMF in response to the control information received.
7	An extra procedure is required for IPv6 sessions, which is Router Solicitation (RS) and Router Advertisement (RA). After the session is established, UE sends the RS message to network to get the link layer address. The UPF forwards this message to SMF. The SMF sends RA message with required parameters to configure the IPv6 address of UE.

Step	Description
8	The RS and RA between UPF and SMF is GTP-u encapsulated and SMF sends an extra pair of PDRs during session establishment and modification procedure, in which GTP-u Tunnel IDs are exchanged for GTP-u tunneling.
9	The additional pair of PDRs that are sent from the SMF are as follows: <ul style="list-style-type: none"> • One PDR has Source interface as Access, and Destination Interface as CP-Function, to forward IPv6 RS from UE to SMF. The SDF filter is present so that UPF can select this PDR for IPv6 RS from UE • Example: Permit in 58 from any to ff01::2 any • Another PDR has source interface as CP-Function, and Destination Interface as Access, to forward the IPv6 RA from SMF to UE. The SDF filter is present so that UPF can select this PDR for all the IPv6 RAs from SMF. • Example: Permit out 58 from any to ff01::2 any
10	After RS and RA procedure is completed, the UE sends IPv6 traffic to PDN.

N4 Session Establishment and Modification Procedure for IPv4v6 Call Flow

The following call flow provides a high-level description of the N4 session establishment and modification procedure for IPv4v6.



The IPv4v6 session establishment and modification procedure are similar to the IPv6 session establishment and modification procedure, except for the following procedures:

Step	Description
1	In the session establishment request, a PDR IE is created to include both IPv4 and IPv6 UE addresses. The SDF filter also includes the IPv4 and IPv6 filters for selecting the PDRs.
2	When the IPv6 address is assigned to the UE, an extra procedure – Router Solicitation and Router Advertisement – is required. The UE sends the Router Solicitation message to the network to receive the link layer address, once the session is established. The UPF forwards this message to the SMF and the SMF sends the Router Advertisement Message with the required parameters for configuring the IPv6 address of the UE.
3	The RS/RA between UPF and SMF is GTP-u encapsulated. In addition, the SMF sends an extra pair of PDRs during session establishment and modification procedure, in which the GTP-u tunnel IDs are exchanged for GTP-u tunneling.
4	The additional pair of PDRs that are sent from the SMF are as follows: <ul style="list-style-type: none"> • For forwarding IPv6 Router Solicitation from UE to SMF, one PDR's source interface is set to access, and its destination interface is set to CP-Function. The SDF filter is present in such a way that the UPF selects this specific PDR for the IPv6 Router Solicitation from the UE. • For instance, permit in 58 from any to ff01::2 any.
5	The UE sends the IPv6 traffic to PDN once the RS/RA procedure is complete.
6	No additional procedures are required for the IPv4 traffic for this PFCP session.

Configuring the N4 Session/Node Level Reporting Procedures

This section describes how to configure the N4 Session/Node Level Reporting procedures.

Enabling the GTP-u Echo Request Procedure

The existing CLI (Command Line Interface) in **gtpu-service** is used to enable the GTP-u Echo request procedure.

```

configure
  gtpu-service service_name
    echo-interval seconds
    echo-retransmission-timeout seconds
    max-retransmissions num
    path-failure detection-policy gtp echo
  end

```

NOTES:

- **gtpu-service *service_name***: Creates a GTP-u service enters the GTP-u Service Configuration Mode for the current context. *service_name* specifies the name of the GTP-u service.

- **echo-interval** *seconds*: Configures the rate at which GTP v1-u echo packets are sent. *seconds* specifies the number of seconds between the sending of a GTP-uv1 echo packet. It must be an integer in the range of 60–3600.
- **echo-retransmission-timeout** *seconds*: Configures the timeout for GTP-u echo message retransmissions for this service. *seconds* specifies the echo retransmission timeout, in seconds, for the GTP-u service. It must be an integer in the range of 1–20. The default value is 5.
- **max-retransmissions** *num*: Configures the maximum retry limit for GTP-u echo retransmissions. *num* specifies the number of GTP-u echo message retransmissions allowed before triggering a path failure error condition. It must be an integer in the range of 0–15.
- **path-failure detection-policy gtp echo**: Configures a path failure detection policy on GTP-u echo messages that have been retransmitted the maximum number of retry times. **gtp echo** sets the detection policy to detect a failure upon reaching the maximum number of GTP-u echo message retransmissions.

The following is a sample configuration for enabling GTP-u Echo request procedure.

```
configure
gtpu-service n3-gtpu-service
echo-interval 60
echo-retransmission-timeout 5
max-retransmissions 5
path-failure detection-policy gtp echo
end
```

Verifying the N4 Session/Node Level Reporting Procedure Configuration

This section describes how to verify the N4 Session/Node Level Reporting Procedure configuration.

N4 Session Node Level Reporting Procedure OA and M Support

Use the **show gtpu statistics** command to display the GTP-u statistics for Error Indication and GTP-u Echo Request and Response. The following is a sample output from the **show gtpu statistics** command.

```
show gtpu statistics
Path Management Messages:
Echo Request Rx:                0 Echo Response Rx:                7
Echo Request Tx:                19 Echo Response Tx:                0
SuppExtnHdr Tx:                0 SuppExtnHdr Rx:                0

Peer Stats:
Total GTPU Peers:                1
Total GTPU Peers with Stats:    1

Tunnel Management Messages:
Error Indication Tx:            0
Error Indication Rx:            0
Error Indication Rx Discarded:
```

Use the **show sx-service statistics all** command to display the Node report request and response statistics. The following is a sample output of the **show sx-service statistics all** command.

```
show sx-service statistics all
Node Report Request:
Total TX:                1 Total RX:                0
Initial TX:              1 Initial RX:                0
Retrans TX:              0 Retrans RX:                0
No Rsp received TX:     0 Discarded:                0
```

Node Report Response:

Total TX:	0	Total RX:	1
Initial TX:	0	Initial RX:	1
Accepted:	0	Accepted:	1
Denied:	0	Denied:	0
Retrans TX:	0	Discarded:	0

SNMP Traps

The following traps are available to track status and conditions GTP-u path failure.

- **EGTPUPathFailure:** This trap is generated when no response is received for GTP-U ECHO requests and data path failure is detected towards peer EPC Node.
- **EGTPUPathFailureClear:** This trap is generated when the data path towards the peer node is available.



CHAPTER 17

UPF Ingress Interface

This chapter covers the following topics:

- [Feature Summary and Revision History](#), on page 139
- [Feature Description](#), on page 140
- [Configuring UPF Ingress Interface Type Support](#), on page 140
- [Verifying the UPF Ingress Interface Type Feature Configuration](#), on page 140

Feature Summary and Revision History

Summary Data

Table 29: Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 30: Revision History

Revision Details	Release
First Introduced.	2020.02.0

Feature Description

This release supports the `upf-ingress` interface, which the UPF requires for user plane service to start. The user plane service must be associated with GTP-U service. This can be achieved using the **associate gtpu-service** CLI command in User Plane Service configuration mode.



Note To enable **upf-ingress** CLI, you need the **require upf** CLI on the UPF. However, to enable the **require upf** CLI, you need the UPF license.

Configuring UPF Ingress Interface Type Support

To associate the GTPU service with the User Plane Service, use the following configuration:

```
configure
  context context_name
    user-plane-service service_name
      [ no ] associate gtpu-service gtpu_service_name upf-ingress
    end
```

NOTES:

- **associate gtpu-service gtpu_service_name**: Associates the GTP-U service with the user plane service.
- **upf-ingress**: Configures the interface type as UPF ingress.

Verifying the UPF Ingress Interface Type Feature Configuration

Run the **show user-plane-service all** command to view the output.

```
[local]qnpc-si# show user-plane-service all

Service name           : user-plane-service
Service-Id             : 4
Context                : ingress
Status                 : STARTED
UPF Ingress GTPU Service : n3-gtpu-service
SGW Ingress GTPU Service : Not defined
SGW Egress GTPU Service : Not defined
Control Plane Tunnel GTPU Service : control_gtpu
Sx Service              : sxu
Control Plane Group     : g1
Fast-Path service       : Disabled
```

NOTES:

- Only one of the interface types **pgw-ingress** or **upf-ingress** can be configured in a single user plane service.



CHAPTER 18

UPF Local Configuration

This chapter covers the following topics:

- [Feature Summary and Revision History, on page 141](#)
- [Feature Description, on page 142](#)
- [Configuring the Local Configuration Support for UPF, on page 143](#)

Feature Summary and Revision History

Summary Data

Table 31: Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 32: Revision History

Revision Details	Release
First Introduced.	2020.02.0

Feature Description

The support for processing static and predefined rules in Control and User Plane Separation of EPC nodes (CUPS) architecture is dependent on the ruledef, rulebase, and charging action. For processing L3/L4 static and predefined rules, this information is made available at the control-plane in CUPS architecture. The control plane sends all these information to the associated user-plane using the PFD management message. The UPF cannot use the PFD management message to work with CN-SNF. With this feature, the local configuration support for the User Plane Function (UPF) is enabled, which allows the UPF to work with CN-SNF.

How it Works

The Access Control System (ACS) command line interface (CLI) is configured on the user-plane and the CLI module sends it to the ACS Controller (ACSCtrl). The ACSCtrl verifies the CLI and sends it to the Session Controller (SessCtrl). The SessCtrl stores the configuration in the SCT.

The SessCtrl maintains and stores different configuration types in a skiplist. When the length of the skiplist reaches the maximum (BULK configuration length) for a particular configuration type, the entire list is pushed in BULK from the Sessctrl to the Session Manager (SessMgr). As a result, the number of messenger event/message transactions between proclcts is greatly reduced since the configurations are sent in BULK in a single message. On the expiry of the bulk configuration timeout (2 seconds), the Bulk Configuration timer – which runs constantly at the Session Controller – pushes the different types of configurations to the SessMgrs.

- The following configuration types are supported for the Bulk Configuration push:
 - Ruledef
 - Charging Action
 - Action Priority Lines
 - Group of Ruledef Configuration
 - Rule in Group of Ruledef Configuration
 - Rulebase L3/L4/L7 Info Configuration
 - APN Configuration
 - ACS service Configuration

The configurations are pushed only through the bulk push mechanism for configurations that are either added or modified. On the other hand, when configurations are deleted, it is removed immediately without waiting for any response from the Bulk configuration push timer. The deleted configuration is removed from the SCT and other SessMgrs immediately.



Note

The Bulk configuration timeout function is invoked forcefully to push all the pending configurations to the SessMgrs before pushing the configuration delete to avoid any race conditions.

- The configuration changes applied to all the new and existing calls are listed in Table as follows

Table 33: Configuration Changes on New and Existing Call Flows

Change in Configuration	Impact on Existing Calls Current Flows	Impact on Existing Calls New Flows	Impact on New Calls
Existing ruledef contents/New rule addition	Rule match is not enforced on existing flows after configuration change. TRM is not disengaged on existing flows. This may lead to billing issues if ruledef contents were changed for ongoing flows.	The configuration changes apply on new flows. For new flows, anyways fresh rule match would happen and the ruledef changes are applied on new flows for existing calls.	The configuration changes apply on new calls. For new flows, anyways fresh rule match would happen and the ruledef changes are applied on flows for new calls.
No Ruledef	Rule in use cannot be deleted.	Rule in use cannot be deleted	Rule in use cannot be deleted
New Group of Ruledefs/Changes to existing Group of Ruledefs contents (Add or Delete Rule in Group of Ruledefs)	Rule match is not enforced on existing flows after configuration change. TRM is not disengaged on existing flows. This may lead to billing issues if Group of Ruledefs contents were changed for ongoing flows.	The configuration changes apply on new flows. For new flows, anyways fresh rule match would happen and the Group of Ruledefs changes are applied on new flows for existing calls.	The configuration changes apply on new calls. For new flows, anyways fresh rule match would happen and the Group of Ruledefs changes are applied on flows for new calls.
No Group of Ruledefs	Group of Ruledefs in use cannot be deleted	Group of Ruledefs in use cannot be deleted	Group of Ruledefs in use cannot be deleted
No Rule in GoR	Flows continue to match the ruledef defined in Group of Ruledefs unless the ruledef itself is deleted	New flows go through a fresh rule match and configuration change takes effect.	New flows go through a fresh rule match and configuration change takes effect.
Action Priority Changes/Action Priority addition	TRM is not disengaged for ongoing flows. configuration changes do not apply on existing flows	Configuration changes apply on new flows.	Configuration changes apply on new calls.
No Action Priority	No Impact on existing flows	Configuration changes apply on new flows.	Configuration changes apply on new calls.
Rulebase parameters change	Some parameter changes apply on existing calls	Some parameter changes apply on existing calls	Configuration changes apply on new calls
No Rulebase	No Rulebase is not supported	No Rulebase is not supported	No Rulebase is not supported
No APN	No APN is not supported	No APN is not supported	No APN is not supported
IP source violation	No impact on existing calls	No impact on existing calls	Configuration changes apply on new calls.

Configuring the Local Configuration Support for UPF

Use the following CLI commands to configure the User Plane Function (UPF) locally.

```
configure
  require upf
end
```




CHAPTER 19

UPF Reporting of Load Control Over N4 Interface

- [Feature Summary and Revision History, on page 145](#)
- [Feature Description, on page 145](#)
- [Configuring the Max Sessions, on page 147](#)

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	UPF
Applicable Platform(s)	VPC-SI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Revision Details	Release
First introduced.	2020.02.0

Feature Description

Load control enables the UPF to send its load information to the SMF in order to balance PFCP session load across the UPF according to their effective load. The load information reflects the operating status of the resources of the UPF. Load control allows for better balancing of the PFCP session load to prevent overload.

NOTE: Overload mitigation actions are not triggered even if the UPF reports high load.

Supported IE and Messages

To report Load Control Information (LCI) to the SMF, 3GPP specification has defined the following IEs:

- Load Control Information IE – The load control Information IE is as follows: It contains the sequence number IE and load metric IE. This IE is sent in Session Establishment Response, Session Modification Response, Session Deletion Response, and Session Report Request messages sent from UPF.
- Sequence Number IE – The Sequence Number IE contains an Unsigned32 binary integer value. The Load Control Sequence Number increases whenever the load control information changes.
- Load Metric IE – The Load Metric parameter indicates the current load level of the originating node. The computation of the Load Metric happens at the implementation basis. The node considers the various aspects, such as:
 - The used capacity of the UPF
 - The load in the node. For example, memory or CPU usage in relationship to the total memory or CPU available, and so on.

The Metric IE encoding is as follows: It indicates a percentage and takes binary coded integer values from and including 0 up to and including 100. Considers the other values as 0.

Reporting Load Information to SMF

The UPF sends its load control information to reflect the operating status of its resources at the node level. It allows the SMF to use this information to augment the UPF selection procedures. The load control information is piggybacked in PFCP request or response messages such that the exchange of load control information does not trigger extra signaling.

Considering the processing requirement of the receiver of the load control information, a larger variation in the Load Metric, example 5 or more units are reasonable value to send the new load control information.

The following criteria is used to send the Load Control Information IE:

- Whenever there is an increase or decrease in the load by 5% or more
- At 95% or above, LCI is reported for any increase
- At 5% or below, no LCI is reported
- At 100%, LCI is reported in all messages.
- System timestamp is used as Sequence Number.

NOTES:

- Currently, only session-load is considered to calculate Load Metric in the UPF.
- Multiple SessMgrs report same value of Load Metric with same sequence number.

Configuring the Max Sessions

Based on various deployment scenarios, if you do not want to load UPF to its maximum capacity in terms of the count of sessions, especially, given that in 5G a single user-session can go up to 5 Gbps. To alter the max session supported in UPF, a CLI command is available under the User Plane Service configuration. It allows the operator to configure the required number of max-sessions that are supported on UPF so that the SMF can load balance the sessions across the UPF. The following is a sample configuration:

```
configure
  context context_name
    user-plane-service user_plane_service
      load-control capacity session_value
    end
```

NOTES:

- *session_value* must be an integer in the range of 1 through the maximum value that is allowed in the platform.
- The use of this configuration is only for the LCI reporting to SMF, and not for any other purpose, such as congestion control, and so on.

The following is an example configuration:

```
configure
  context ingress
    user-plane-service ups1
      load-control capacity 2500
    end
```

Show Command Support

The output of the show command to display the User Plane Service includes the value of configured max sessions.

show user-plane-service all

```
Service name                : user-plane-service
Service-Id                  : 4
Context                      : ingress
Status                       : STARTED
UPF Ingress GTPU Service    : n3-gtpu-service
SGW Ingress GTPU Service    : Not defined
SGW Egress GTPU Service     : Not defined
Control Plane Tunnel GTPU Service : n4-gtpu-service
Sx Service                  : n4-sx
Control Plane Group         : g1
Load Control Parameters
  Capacity                   : 1000
```




CHAPTER 20

Session Recovery

- [Feature Summary and Revision History, on page 149](#)
- [Feature Description, on page 149](#)
- [How it Works, on page 150](#)
- [Configuring the System to Support Session Recovery, on page 150](#)

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI
Feature Default Setting	Disabled – License Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Revision Details	Release
First introduced.	2020.02.0

Feature Description

With robust hardware failover and redundancy protection, any hardware or software failures on the system can quickly be corrected. However, software failures can occur for numerous reasons, often without prior indication.

This chapter describes the Session Recovery feature that provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault.

**Important**

Session Recovery is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco Account representative for detailed information on specific licensing requirements.

How it Works

This section provides an overview of how this feature is implemented and the recovery process.

The Session Recovery feature provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault within the system preventing a fully connected user session from being disconnected.

Session recovery is performed by mirroring key software processes (for example, session manager and AAA manager) within the system. These mirrored processes remain in an idle state (standby-mode) wherein they perform no processing, until they may be needed in the event of a software failure (for example, a session manager task aborts).

There are some situations wherein session recovery may not operate properly. Additional software or hardware failures occur during the session recovery operation. For example, an AAA manager fails while the state information it contained was being used to populate the newly activated session manager task.

**Important**

After a session recovery operation, some statistics, such as those collected and maintained on a per manager basis (AAA Manager, Session Manager, etc.) are in general not recovered, only accounting and billing related information is checkpointed and recovered.

Configuring the System to Support Session Recovery

The following procedures allow you to configure the session recovery feature for either an operational system that is currently in-service (able to accept incoming calls) or a system that is out-of-service (not part of your production network and, therefore, not processing any live subscriber/customer data).

**Important**

The session recovery feature, even when the feature use key is present, is disabled by default on the system.

Enabling Session Recovery

As noted earlier, session recovery can be enabled on a system that is out-of-service (OOS) and does not yet have any contexts configured, or on an in-service system that is currently capable of processing calls. However, if the system is in-service, it must be restarted before the session recovery feature takes effect.

Enabling Session Recovery on an Out-of-Service System

The following procedure is for a system that does not have any contexts configured.

To enable the session recovery feature on an out-of-service system, follow the procedure below. This procedure assumes that you begin at the Exec mode prompt.

-
- Step 1** At the Exec mode prompt, verify that the session recovery feature is enabled via the session and feature use licenses on the system by running the **show license info** command.
- If the current status of the Session Recovery feature is Disabled, you cannot enable this feature until a license key is installed in the system.
- Step 2** Use the following configuration example to enable session recovery.
- ```
configure
 require session recovery
end
```
- Note** After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the System Administration Guide for your deployment.
- Step 3** Save your configuration as described in *Verifying and Saving Your Configuration*.
- The system, when started, enables session recovery, creates all mirrored "standby-mode" tasks, and performs packet processing card reservations and other operations automatically.
- Step 4** After the system has been configured and placed in-service, you should verify the preparedness of the system to support this feature as described in *Viewing Session Recovery Status* section.
- 

## Enabling Session Recovery on an In-Service System

When enabling session recovery on a system that already has a saved configuration, the session recovery commands are automatically placed before any service configuration commands in the configuration file.

To enable the session recovery feature on an in-service system, follow the procedure below. This procedure assumes that you begin at the Exec mode prompt.

- 
- Step 1** At the Exec mode prompt, verify that the session recovery feature is enabled via the session and feature use licenses on the system by running the **show license info** command:
- If the current status of the Session Recovery feature is Disabled, You cannot enable this feature until a license key is installed in the system.
- Step 2** Use the following configuration example to enable session recovery.
- ```
configure
  require session recovery
end
```
- This feature does not take effect until after the system has been restarted.
- Step 3** Save your configuration as described in *Verifying and Saving Your Configuration*.
- Step 4** Perform a system restart by entering the **reload** command:
- The following prompt appears:

Are you sure? [Yes|No]:

Confirm your desire to perform a system restart by entering **yes**.

The system, when restarted, enables session recovery and creates all mirrored "standby-mode" tasks, performs packet processing card reservations, and other operations automatically.

Step 5 After the system has been restarted, you should verify the preparedness of the system to support this feature as described in *Viewing Session Recovery Status* section.

More advanced users may opt to simply insert the **require session recovery** command syntax into an existing configuration file using a text editor or other means, and then applying the configuration file manually. Exercise caution when doing this to ensure that this command is placed among the first few lines of any existing configuration file; it must appear before the creation of any non-local context.

Disabling the Session Recovery Feature

To disable the session recovery feature on a system, enter the **no require session recovery** command from the Global Configuration mode prompt.



Important If this command is issued on an in-service system, then the system must be restarted by issuing the **reload** command.

Viewing Session Recovery Status

To determine if the system is capable of performing session recovery, when enabled, enter the **show session recovery status verbose** command from the Exec mode prompt.

The output of this command should be similar to the examples shown below.

```
[local]host_name# show session recovery status
Session Recovery Status:
  Overall Status           : SESSMGR Not Ready For Recovery
  Last Status Update      : 1 second ago
```

```
[local]host_name# show session recovery status
Session Recovery Status:
  Overall Status           : Ready For Recovery
  Last Status Update      : 8 seconds ago
```

```
[local]host_name# show session recovery status verbose
Session Recovery Status:
  Overall Status           : Ready For Recovery
  Last Status Update      : 2 seconds ago
```

```

cpu state      ----sessmgr----      ----aaamgr----      demux
active  standby  active  standby  active  status
-----
1/0 Active  7      1      7      1      7      Good
[local]host_name#
```


Viewing Recreated Session Information

To view session state information and any session recreation status, enter the following command:

```
show subscriber debug-info callid id
```

The following example shows the output of this command both before and after a session recovery operation has been performed. The "Redundancy Status" fields in this example have been bold-faced for clarity.

```
username: user1                callid: 01callb1                msid: 0000100003
Card/Cpu: 4/2
Sessmgr Instance: 7
Primary callline:
Redundancy Status: Original Session
  Checkpoints      Attempts      Success      Last-Attempt      Last-Success
  Full:            69           68           29800ms           29800ms
  Micro:           206          206          20100ms           20100ms
Current state: SMGR_STATE_CONNECTED
FSM Event trace:
  State              Event
  SMGR_STATE_OPEN    SMGR_EVT_NEWCALL
  SMGR_STATE_NEWCALL_ARRIVED SMGR_EVT_ANSWER_CALL
  SMGR_STATE_NEWCALL_ANSWERED SMGR_EVT_LINE_CONNECTED
  SMGR_STATE_LINE_CONNECTED SMGR_EVT_LINK_CONTROL_UP
  SMGR_STATE_LINE_CONNECTED SMGR_EVT_AUTH_REQ
  SMGR_STATE_LINE_CONNECTED SMGR_EVT_IPADDR_ALLOC_SUCCESS
  SMGR_STATE_LINE_CONNECTED SMGR_EVT_AUTH_SUCCESS
  SMGR_STATE_LINE_CONNECTED SMGR_EVT_UPDATE_SESS_CONFIG
  SMGR_STATE_LINE_CONNECTED SMGR_EVT_LOWER_LAYER_UP
Data Reorder statistics
Total timer expiry: 0          Total flush (tmr expiry): 0
Total no buffers: 0          Total flush (no buffers): 0
Total flush (queue full): 0  Total flush (out of range): 0
Total flush (svc change): 0  Total out-of-seq pkt drop: 0
Total out-of-seq arrived: 0
IPv4 Reassembly Statistics:
  Success: 0          In Progress: 0
  Failure (timeout): 0  Failure (no buffers): 0
  Failure (other reasons): 0
Redirected Session Entries:      Allowed:
2000      Current: 0
          Added: 0          Deleted:
          0
          Revoked for use by different subscriber: 0
Peer callline:
Redundancy Status: Recreated Session
  Checkpoints      Attempts      Success      Last-Attempt      Last-Success
  Full:            0            0            0ms               0ms
  Micro:           0            0            0ms               0ms
Current state: SMGR_STATE_CONNECTED
FSM Event trace:
  State              Event
  SMGR_STATE_LINE_CONNECTED SMGR_EVT_LOWER_LAYER_UP
  SMGR_STATE_CONNECTED SMGR_EVT_AUTH_REQ
  SMGR_STATE_CONNECTED SMGR_EVT_AUTH_SUCCESS
  SMGR_STATE_CONNECTED SMGR_EVT_REQ_SUB_SESSION
  SMGR_STATE_CONNECTED SMGR_EVT_RSP_SUB_SESSION
  SMGR_STATE_CONNECTED SMGR_EVT_ADD_SUB_SESSION
  SMGR_STATE_CONNECTED SMGR_EVT_AUTH_REQ
  SMGR_STATE_CONNECTED SMGR_EVT_AUTH_SUCCESS
  SMGR_STATE_CONNECTED SMGR_EVT_AUTH_REQ
  SMGR_STATE_CONNECTED SMGR_EVT_AUTH_SUCCESS
  SMGR_STATE_CONNECTED SMGR_EVT_AUTH_REQ
```

```

SMGR_STATE_CONNECTED          SMGR_EVT_AUTH_SUCCESS
SMGR_STATE_CONNECTED          SMGR_EVT_AUTH_REQ
SMGR_STATE_CONNECTED          SMGR_EVT_AUTH_SUCCESS
SMGR_STATE_CONNECTED          SMGR_EVT_AUTH_REQ
SMGR_STATE_CONNECTED          SMGR_EVT_AUTH_SUCCESS
Data Reorder statistics
  Total timer expiry:          0          Total flush (tmr expiry): 0
  Total no buffers:            0          Total flush (no buffers): 0
  Total flush (queue full):    0          Total flush (out of range):0
  Total flush (svc change):    0          Total out-of-seq pkt drop: 0
  Total out-of-seq arrived:    0
IPv4 Reassembly Statistics:
  Success:                     0          In Progress:                0
  Failure (timeout):           0          Failure (no buffers):       0
  Failure (other reasons):     0
Redirected Session Entries:
  Allowed:                      2000       Current:                     0
  Added:                        0          Deleted:                     0
  Revoked for use by different subscriber: 0

```



CHAPTER 21

Voice over New Radio

This chapter covers the following topics:

- [Feature Summary and Revision History, on page 155](#)
- [Feature Description, on page 155](#)

Feature Summary and Revision History

Summary Data

Table 34: Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 35: Revision History

Revision Details	Release
First Introduced.	2020.02.0

Feature Description

The UPF supports Voice over New Radio (VoNR) with the existing Session Establishment and Modification procedures. In these procedures, the SMF creates the PDR for 5QI=5 Non-GBR flow for IMS signaling and

PDR for 5QI=1 GBR flow for voice traffic. The UPF does not require any special handling to support mobile-originated or mobile-terminated call flows.

How it Works

The following are the steps in the call flow in which the PDRs are created with 5QI value 5 for IMS signaling and 5QI value 1 or Voice Traffic.

VoNR Call Flow for UPF

This section describes the steps for VoNR session and respective PDR Creation on UPF.

Figure 11: VoNR Call Flow

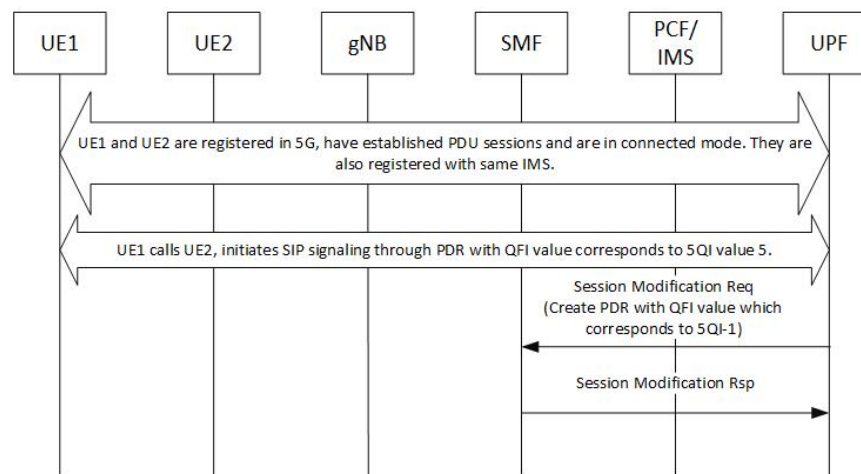


Table 36: VoNR Call Flow

Step	Description
1	UE1 and UE2 are registered on 5G network. They establish the IMS PDU session and both are registered with same IMS. Both UEs are in connected mode.
2	For IMS signaling, a non-GBR QoS PDRs (UL and DL) is created by SMF which has the QFI value that corresponds to 5QI value 5.
3	Similarly, for Conversational Voice traffic, the PDRs for GBR QoS flow is created with the QFI value that corresponds to 5QI value 1.
4	The QFI to 5QI mapping is maintained by SMF, hence the QFI does not have the values same as 5QI.
5	The above steps are valid for both Mobile Originated (MO) or Mobile Terminate (MT) call flows.
6	Refer to 3GPP TS 23.501, Section 5.7.4 for other types of 5QI mappings for GBR or Non-GBR flows.



PART II

Troubleshooting Information

- [UPF Troubleshooting Information, on page 159](#)



CHAPTER 22

UPF Troubleshooting Information

This chapter covers the following topics related to monitoring and troubleshooting the UPF features:

- [Debug Logging](#) , on page 159
- [Monitoring CLI](#), on page 160
- [Monitoring Protocol](#), on page 160
- [RAT Type-based Statistics](#), on page 160
- [Subscriber Level CLI](#), on page 165
- [VPP Statistics](#), on page 165
- [SNMP Support](#), on page 166
- [Troubleshooting UPF Features](#), on page 167

Debug Logging



Important

The debug logging CLIs must be enabled with the help of System Administrator. Enabling debug logging CLIs can be resource intensive.

Use the following debug CLIs as required:

- **logg filter active facility sx level debug**
- **logg filter active facility user-data level debug**
- **logg filter active facility sessmgr level debug**
- **logg filter active facility uplane level debug**
- **logg filter active facility egtpc level debug**
- **logg filter active facility gtpu level debug**
- **logg filter active facility egtpu level debug**
- **logg filter active facility gtpumgr level debug**
- **logg filter active facility sxdemux level debug**
- **logg filter active facility user-l3tunnel level debug**

- `logg filter active facility aaamgr level debug`
- `logg filter active facility vpp level debug`
- `logg filter active facility dpath level debug`
- `logg active pdu-verbosity 5`

Monitoring CLI

Subscriber Level Message

Use the `mon sub callid` CLI command for subscriber level message.

Resource Tracking

Use the `show task resources facility sessmgr all` CLI command to track the CPU/Memory for PROCLET.

Service Status

Use the `show service all` CLI command to check the service status.

Sx Peer Status

Use the `show sx peers` CLI command to check the Sx peer status.

Monitoring Protocol

When using the `monitor protocol` command, enable option 49 for PFCP, and option 26 for GTP-U.

RAT Type-based Statistics

The RAT Type-based Statistics feature equip users to view data statistics segregated by RAT Type in UPF.

RAT Type-based data statistics in UPF maintains separate buckets. These buckets are created at Session Manager instance level. Bucket is assigned to a subscriber at the time of call-setup, based on RAT Type IE received in “Subscriber-Parameters”. If the IE is not received, “Unknown” RAT Type bucket is assigned to that subscriber. During the session, if UPF receives a new RAT Type for a subscriber, the bucket is changed accordingly.



Important

Data statistics are not checkpointed and lost during Session Recovery/ICSR. Only “Current-Subscriber” statistics are recalculated after recovery (during the time of call-audit).

Show Command and Output

The following CLI command displays node-level RAT statistics for UPF: `show user-plane-service statistics rat { 5g-nr | all | eutran | unknown | wlan }`

NOTES:

- **5g-nr:** Displays the data statistics for 5G NR subscribers.
- **all:** Displays the data statistics for all RAT Type subscribers.
- **eutran:** Displays the data statistics for EUTRAN subscribers.
- **unknown:** Displays the data statistics for subscribers of unknown RAT type.
- **wlan:** Displays the data statistics for WLAN subscribers.

Statistics

The following table provides description of each field.

Table 37: show user-plane-service statistics rat all

Field	Description
Current Subscribers	
5G NR	Specifies the total number of current 5G NR subscribers.
EUTRAN	Specifies the total number of current EUTRAN subscribers.
WLAN	Specifies the total number of current WLAN subscribers.
Unknown	Specifies the total number of current subscribers of unknown RAT type.
Data Statistics	
5G NR	Specifies the data statistics for 5G NR subscribers.
Uplink	Specifies data statistics for 5G NR subscribers in uplink direction.
Total Pkts	Specifies the total number of uplink packets for 5G NR subscribers.
Total Bytes	Specifies the total number of uplink bytes for 5G NR subscribers.
Total Dropped Pkts	Specifies the total number of uplink packets dropped for 5G NR subscribers.
Total Dropped Bytes	Specifies the total number of uplink bytes dropped for 5G NR subscribers.
Downlink	Specifies data statistics for 5G NR subscribers in downlink direction.
Total Pkts	Specifies the total number of downlink packets for 5G NR subscribers.
Total Bytes	Specifies the total number of downlink bytes for 5G NR subscribers.
Total Dropped Pkts	Specifies the total number of downlink packets dropped for 5G NR subscribers.
Total Dropped Bytes	Specifies the total number of downlink bytes dropped for 5G NR subscribers.
EUTRAN	Specifies the data statistics for EUTRAN subscribers.
Uplink	Specifies data statistics for EUTRAN subscribers in uplink direction.

Field	Description
Total Pkts	Specifies the total number of uplink packets for EUTRAN subscribers.
Total Bytes	Specifies the total number of uplink bytes for EUTRAN subscribers.
Total Dropped Pkts	Specifies the total number of uplink packets dropped for EUTRAN subscribers.
Total Dropped Bytes	Specifies the total number of uplink bytes dropped for EUTRAN subscribers.
Downlink	Specifies data statistics for EUTRAN subscribers in downlink direction.
Total Pkts	Specifies the total number of downlink packets for EUTRAN subscribers.
Total Bytes	Specifies the total number of downlink bytes for EUTRAN subscribers.
Total Dropped Pkts	Specifies the total number of downlink packets dropped for EUTRAN subscribers.
Total Dropped Bytes	Specifies the total number of downlink bytes dropped for EUTRAN subscribers.
WLAN	Specifies the data statistics for WLAN subscribers.
Uplink	Specifies data statistics for WLAN subscribers in uplink direction.
Total Pkts	Specifies the total number of uplink packets for WLAN subscribers.
Total Bytes	Specifies the total number of uplink bytes for WLAN subscribers.
Total Dropped Pkts	Specifies the total number of uplink packets dropped for WLAN subscribers.
Total Dropped Bytes	Specifies the total number of uplink bytes dropped for WLAN subscribers.
Downlink	Specifies data statistics for WLAN subscribers in downlink direction.
Total Pkts	Specifies the total number of downlink packets for WLAN subscribers.
Total Bytes	Specifies the total number of downlink bytes for WLAN subscribers.
Total Dropped Pkts	Specifies the total number of downlink packets dropped for WLAN subscribers.
Total Dropped Bytes	Specifies the total number of downlink bytes dropped for WLAN subscribers.
Unknown	Specifies the data statistics for subscribers of unknown RAT type.
Uplink	Specifies data statistics for unknown RAT type subscribers in uplink direction.
Total Pkts	Specifies the total number of uplink packets for unknown RAT type subscribers.
Total Bytes	Specifies the total number of uplink bytes for unknown RAT type subscribers.

Field	Description
Total Dropped Pkts	Specifies the total number of uplink packets dropped for unknown RAT type subscribers.
Total Dropped Bytes	Specifies the total number of uplink bytes dropped for unknown RAT type subscribers.
Downlink	Specifies data statistics for unknown RAT type subscribers in downlink direction.
Total Pkts	Specifies the total number of downlink packets for unknown RAT type subscribers.
Total Bytes	Specifies the total number of downlink bytes for unknown RAT type subscribers.
Total Dropped Pkts	Specifies the total number of downlink packets dropped for unknown RAT type subscribers.
Total Dropped Bytes	Specifies the total number of downlink bytes dropped for unknown RAT type subscribers.

Bulk Statistics

The following bulk statistics are included in the User Plane Service schema to track RAT Type-based data statistics events.

Table 38: *show bulkstats variables user-plane-service*

Variable Name	Data Type	Key	Counter Type
vpname	String	1	Info
vpnid	Int32	1	Info
servname	String	1	Info
servid	Int32	1	Info
curr-pdn-rat-eutran	Int64	0	Gauge
curr-pdn-rat-5g-nr	Int64	0	Gauge
curr-pdn-rat-wlan	Int64	0	Gauge
curr-pdn-rat-unknown	Int64	0	Gauge
uplink-total-pkts-pdn-rat-eutran	Int64	0	Counter
uplink-total-bytes-pdn-rat-eutran	Int64	0	Counter
uplink-total-pkts-dropped-pdn-rat-eutran	Int64	0	Counter
uplink-total-bytes-dropped-pdn-rat-eutran	Int64	0	Counter
downlink-total-pkts-pdn-rat-eutran	Int64	0	Counter

Variable Name	Data Type	Key	Counter Type
downlink-total-bytes-pdn-rat-eutran	Int64	0	Counter
downlink-total-pkts-dropped-pdn-rat-eutran	Int64	0	Counter
downlink-total-bytes-dropped-pdn-rat-eutran	Int64	0	Counter
uplink-total-pkts-pdn-rat-5g-nr	Int64	0	Counter
uplink-total-bytes-pdn-rat-5g-nr	Int64	0	Counter
uplink-total-pkts-dropped-pdn-rat-5g-nr	Int64	0	Counter
uplink-total-bytes-dropped-pdn-rat-5g-nr	Int64	0	Counter
downlink-total-pkts-pdn-rat-5g-nr	Int64	0	Counter
downlink-total-bytes-pdn-rat-5g-nr	Int64	0	Counter
downlink-total-pkts-dropped-pdn-rat-5g-nr	Int64	0	Counter
downlink-total-bytes-dropped-pdn-rat-5g-nr	Int64	0	Counter
uplink-total-pkts-pdn-rat-wlan	Int64	0	Counter
uplink-total-bytes-pdn-rat-wlan	Int64	0	Counter
uplink-total-pkts-dropped-pdn-rat-wlan	Int64	0	Counter
uplink-total-bytes-dropped-pdn-rat-wlan	Int64	0	Counter
downlink-total-pkts-pdn-rat-wlan	Int64	0	Counter
downlink-total-bytes-pdn-rat-wlan	Int64	0	Counter
downlink-total-pkts-dropped-pdn-rat-wlan	Int64	0	Counter
downlink-total-bytes-dropped-pdn-rat-wlan	Int64	0	Counter
uplink-total-pkts-pdn-rat-unknown	Int64	0	Counter
uplink-total-bytes-pdn-rat-unknown	Int64	0	Counter
uplink-total-pkts-dropped-pdn-rat-unknown	Int64	0	Counter
uplink-total-bytes-dropped-pdn-rat-unknown	Int64	0	Counter
downlink-total-pkts-pdn-rat-unknown	Int64	0	Counter
downlink-total-bytes-pdn-rat-unknown	Int64	0	Counter
downlink-total-pkts-dropped-pdn-rat-unknown	Int64	0	Counter
downlink-total-bytes-dropped-pdn-rat-unknown	Int64	0	Counter

Subscriber Level CLI

Use the following subscriber level CLIs as required:

- **show subscribers user-plane-only full all**
- **show subscribers user-plane-only { seid *seid_value* | callid *callid_value* } pdr all**
- **show subscribers user-plane-only { seid *seid_value* | callid *callid_value* } far all**
- **show subscribers user-plane-only { seid *seid_value* | callid *callid_value* } qer all**
- **show subscribers user-plane-only { seid *seid_value* | callid *callid_value* } urr all**
- **show subscribers user-plane-only { seid *seid_value* | callid *callid_value* } bar all**
- **show subscribers user-plane-only { seid *seid_value* | callid *callid_value* } pdr full all**
- **show subscribers user-plane-only { seid *seid_value* | callid *callid_value* } urr full all**
- **show subscribers user-plane-only { seid *seid_value* | callid *callid_value* } far full all**
- **show subscribers user-plane-only { seid *seid_value* | callid *callid_value* } qer full all**
- **show subscribers user-plane-only { seid *seid_value* | callid *callid_value* } bar full all**
- **show subscribers user-plane-only { seid *seid_value* | callid *callid_value* } pdr id *id_value***
- **show subscribers user-plane-only { seid *seid_value* | callid *callid_value* } flows full**
- **show subscribers user-plane-only { seid *seid_value* | callid *callid_value* } bli full all**

VPP Statistics

To determine if the flows are offloaded to VPP, check for Fastpath statistics in the output of the following CLI commands:

- **show user-plane-service statistics all**
- **show user-plane-service statistics analyzer name ip [verbose]**
- **show user-plane-service statistics analyzer name ipv6 [verbose]**
- **show user-plane-service statistics analyzer name tcp [verbose]**
- **show user-plane-service statistics analyzer name udp [verbose]**
- **show user-plane-service statistics analyzer name http [verbose]**
- **show user-plane-service statistics analyzer name rtp [verbose]**
- **show subscribers user-plane-only full callid *call_id***

SNMP Support

The system uses the Simple Network Management Protocol (SNMP) to send traps or events to the EMS server or an alarm server on the network. You must configure SNMP settings to communicate with those devices.

The *SNMP MIB Reference* describes the MIBs and SNMP traps supported by UPF and StarOS.

The following SNMP traps are available in support of their respective feature/functionality:

N4 Session/Node Level Reporting Procedure

The following traps are available to track status and conditions GTP-U path failure:

- **EGTUPPathFailure:** This trap is generated when no response is received for GTP-U ECHO requests and data path failure is detected towards peer EPC Node.
- **EGTUPPathFailureClear:** This trap is generated when the data path towards the peer node is available.

UP Session Recovery

The following traps are available after session recovery in the User Plane node:

- **ManagerFailure:** This trap is generated when there is failure in the Software manager.
- **TaskFailed:** This trap is generated when a noncritical task has failed and the appropriate recovery steps begin.
- **TaskRestart:** This trap is generated when a noncritical task has restarted after an earlier failure.
- **SessMgrRecoveryComplete:** This trap is generated when Session Manager recovery completes. This is typically caused by the failure of Session Manager task and successful completion of recovery.
- **ManagerRestart:** This trap is generated when the identified manager task has been restarted.

Sx Association

The following traps are available to track the status of an Sx Association:

- **SxPeerAssociated:** This trap is triggered when an Sx association is detected.
- **SxPeerAssociationRelease:** This trap is triggered when an Sx association release is detected.

URL Blacklisting

The following SNMP trap are available in support of URL Blacklisting feature:

- **BLDBError:** Specifies the blacklisting OPTBLDB file error displayed with an error code.
- **BLDBErrorClear:** Specifies the blacklisting OPTBLDB file error removed.
- **BLDBUpgradeError:** Specifies the blacklisting OPTBLDB file error displayed with an error code.
- **BLDBUpgradeErrorClear:** Specifies the Blacklisting OPTBLDB file error removed.

Enabling SNMP Traps

Use the following configuration to enable an SNMP trap.

```
configure
  snmp trap enable trap_name
end
```

For supplemental information about SNMP Support, see *Management Settings* chapter in the *ASR 5500 System Administration Guide*.

Troubleshooting UPF Features

N4 or Datapath

The following CLI commands are available for troubleshooting N4 or datapath related issues:

- **show gtpu statistics**
- **show user-plane-service { all | bandwidth-policy | charging-action | edr-format | group-of-ruledefs | gtp-group | name | pdn-instance | rulebase | ruledef | statistics | xheader-format }**

NOTES:

- **all**: Displays all User Plane services.
- **bandwidth-policy**: Displays information for bandwidth-policy in User Plane service.
- **charging-action**: Displays information for Charging actions in User Plane service.
- **edr-format**: Displays information for EDR format in user Plane service.
- **group-of-ruledefs**: Displays information on Group of Ruledefs configured in User Plane service.
- **gtp-group**: Displays information for bandwidth policy in User Plane service.
- **name**: Displays information for specific User Plane service name.
- **pdn-instance**: Displays information for PDN instance.
- **rulebase**: Displays information for rulebase in User Plane service.
- **ruledef**: Displays information for ruledef in User Plane service.
- **statistics**: Displays node-level statistics for User Plane.

Additionally, you can also use: **show user-plane-service statistics { all | analyzer | charging-action | fapi | rulebase | tethering-detection }**

- **xheader-format**: Displays information for X-Header format in User Plane service.
- **show user-plane-service content-filtering category policy-id (all | id id_value)**
 - **content-filtering**: Displays content filtering information.
 - **category**: Displays content filtering category information.
 - **policy-id**: Displays content filtering category Policy-ID and its definition.
 - **all**: Displays definitions of all content filtering category policies.

- **id *id_value***: Displays content filtering category definition of a particular Policy-ID. *id_value* is an integer ranging from 1 through 4,294,967,295.

- **show sx-service { all | name | statistics }**

NOTES:

- **all**: Displays all Sx Services.
- **name**: Displays information for specific Sx Service name.
- **statistics**: Displays the total of collected information for specific protocol since last restart or clear command.

Content Filtering

Use the following CLI command for troubleshooting CF related issues: **show user-plane-service inline-services { content-filtering | info | url-blacklisting }**

NOTES:

- **content-filtering**: Displays content filtering information.
- **info**: Displays information of inline services.
- **url-blacklisting**: Displays URL Blacklisting parameters in User Plane service.

URL Blacklisting

Use the following CLI command for troubleshooting URL Blacklisting related issues: **show user-plane-service url-blacklisting database { all | debug-only | facility | url }**

NOTES:

- **all**: Displays all URL Blacklisting database configurations.
- **debug-only**: Displays the URL Blacklisting static database debug information.
- **facility**: Displays URL Blacklisting database configuration per facility.
- **url**: Displays particular database information for URL Blacklisting.



PART **III**

UPF Sample Basic Configuration

- [Sample UPF Configuration, on page 171](#)



CHAPTER 23

Sample UPF Configuration

- [Sample Configuration, on page 171](#)

Sample Configuration

The following is only a sample configuration file provided solely for your reference. You must create and modify your own configuration file according to the specific needs of your deployment.

```
----- snip -----
  active-charging service acs
  bandwidth-policy BWP
    flow limit-for-bandwidth id 1 group-id 2
    flow limit-for-bandwidth id 2 group-id 3
    flow limit-for-bandwidth id 100 group-id 100
  group-id 2 direction uplink peak-data-rate 256000 peak-burst-size 1000 violate-action
  discard
  group-id 2 direction downlink peak-data-rate 200000 peak-burst-size 1000 violate-action
  discard
  group-id 3 direction downlink peak-data-rate 256000 peak-burst-size 1000 violate-action
  discard
  group-id 4 direction uplink peak-data-rate 300000 peak-burst-size 1200 violate-action
  lower-ip-precedence
  group-id 100 direction downlink peak-data-rate-kbps 4294967295 peak-burst-size
  4294967295 violate-action discard

  ruledef L3_SERVER
    ip server-ip-address = 2.2.2.2/32
    tcp either-port = 80
  #exit
  ruledef L4_PORT
    tcp either-port = 80
    udp either-port = 80
    multi-line-or all-lines
  #exit
  ruledef L7_HTTP
    http host contains 2.2.2.2
    multi-line-or all-lines
  #exit
  ruledef http-pkts
    http any-match = TRUE
  #exit
  ruledef http-port
    tcp either-port = 80
    rule-application routing
  #exit
```

```

ruledef ip-any-rule
  ip any-match = TRUE
#exit
urr-list urrs
  rating-group 10 urr-id 5
#exit
charging-action starent
  content-id 10
  billing-action egcdr
#exit
rulebase default
#exit
credit-control group default
  pending-traffic-treatment noquota buffer
  pending-traffic-treatment quota-exhausted pass
  usage-reporting quotas-to-report based-on-grant

rulebase starent
  billing-records egcdr
  dynamic-rule order first-if-tied
  action priority 5 ruledef http-pkts charging-action standard
  action priority 10 ruledef L7_HTTP charging-action starent
  action priority 20 ruledef L4_PORT charging-action starent
  action priority 100 ruledef L3_SERVER charging-action starent
  action priority 10000 ruledef ip-any-rule charging-action starent
  route priority 1 ruledef http-port analyzer http
  egcdr threshold interval 1000
  bandwidth default-policy BWP
#exit
traffic-optimization-policy default
#exit
#exit
context ingress
  interface N3_interface
    ip address 1.1.2.1 1.1.2.2
    ipv6 address abc0:0:0:cb::1/64 secondary
  #exit
  interface N3_interface_LOGICAL loopback
    ip address 1.1.2.1 1.1.2.2
  #exit
  interface N3_interface_LOGICAL2 loopback
    ip address 1.1.2.1 1.1.2.2
  #exit
  interface N4U_interface
    ip address 1.1.2.1 1.1.2.2
    ipv6 address abc0:0:0:cd::1/64 secondary
    ipv6 address abc0:0:0:ca::1/64 secondary
  #exit
  interface N4U_interface_LOGICAL loopback
    ip address 1.1.2.1 1.1.2.2
  #exit
  interface N4_interface
    ip address 1.1.2.1 1.1.2.2
    ipv6 address abc0:0:0:cc::1/64 secondary
  #exit
  interface N4_interface_LOGICAL loopback
    ip address 1.1.2.1 1.1.2.2
  #exit
  subscriber default
  exit
  aaa group default
  #exit
  gtpv group default
  #exit

```

```

gtpu-service N3-GNB1
  bind ipv4-address 1.1.1.1
exit
gtpu-service N3-GNB2
  bind ipv4-address 1.1.2.1
exit
gtpu-service control_gtpu
  bind ipv4-address 1.1.2.1
exit
sx-service N4
  instance-type userplane
  bind ipv4-address 1.1.2.1
  sx-protocol heartbeat interval 3600
  sx-protocol heartbeat max-retransmissions 1
  sx-protocol association reattempt-timeout 30
exit
user-plane-service user-plane-service
  associate gtpu-service N3-GNB1 upf-ingress
  associate gtpu-service control_gtpu cp-tunnel
  associate sx-service N4
  associate fast-path service
  associate control-plane-group default
  load-control capacity 900
exit
user-plane-service user-plane-service1
exit
ip route 1.1.2.1 1.1.2.2 1.1.2.3 N4_interface
ip route 1.1.2.1 1.1.2.2 1.1.2.3 N4_interface
ip route 1.1.2.1 1.1.2.2 1.1.2.3 N3_interface
ip route 1.1.2.1 1.1.2.2 1.1.2.3 N3_interface
ip route 1.1.2.1 1.1.2.2 1.1.2.3 N4_interface
ip route 1.1.2.1 1.1.2.2 1.1.2.3 N3_interface
ip route 1.1.2.1 1.1.2.2 1.1.2.3 N4_interface
ip route 1.1.2.1 1.1.2.2 1.1.2.3 N3_interface
#exit
context egress
  interface N6_interface
    ip address 1.1.2.1 1.1.2.2
    ipv6 address abc0:0:0:cf::1/64 secondary
  #exit
  subscriber default
  exit
  apn starent.com
    pdp-type ipv4 ipv6
    selection-mode subscribed sent-by-ms chosen-by-sgsn
    gtp group default accounting-context egress
    ip context-name egress
    active-charging rulebase starent
  exit
  aaa group default
  #exit
  gtp group default
    gtp attribute local-record-sequence-number
    gtp dictionary custom24
    gtp egcdr service-data-flow threshold interval 60
    gtp egcdr service-data-flow threshold volume downlink 13000
    gtp egcdr service-data-flow threshold volume uplink 17000
    gtp egcdr service-data-flow threshold volume total 22222
  #exit
  ipv6 route 2:2:2:2::/64 next-hop abc0::ab:1c:2ff:def9:1ab interface N6_interface
  ip route 1.1.2.1 1.1.2.2 1.1.2.3 N6_interface
  ip route 1.1.2.1 1.1.2.2 1.1.2.3 N6_interface
  ipv6 route 2:2:2:2::/64 next-hop abc0::ab:1c:2ff:def9:1ab interface N6_interface
  ip route 1.1.2.1 1.1.2.2 1.1.2.3 N6_interface

```

```
#exit
control-plane-group default
  sx-association initiated-by-cp
  peer-node-id ipv4-address 1.1.1.1 interface n4
#exit
user-plane-group default
#exit
port ethernet 1/11
  no shutdown
  vlan 203
    no shutdown
    bind interface N4U_interface ingress
  #exit
  vlan 204
    no shutdown
    bind interface N4_interface ingress
  #exit
  vlan 205
    no shutdown
    bind interface N3_interface ingress
  #exit
  vlan 206
    no shutdown
  #exit
  vlan 207
    no shutdown
    bind interface N6_interface egress
  #exit
#exit
end
```