Ultra Cloud Core 5G User Plane Function, Release 2022.04 - Release Change Reference

First Published: 2022-10-14

Last Modified: 2022-10-21

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

CONTENTS

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.

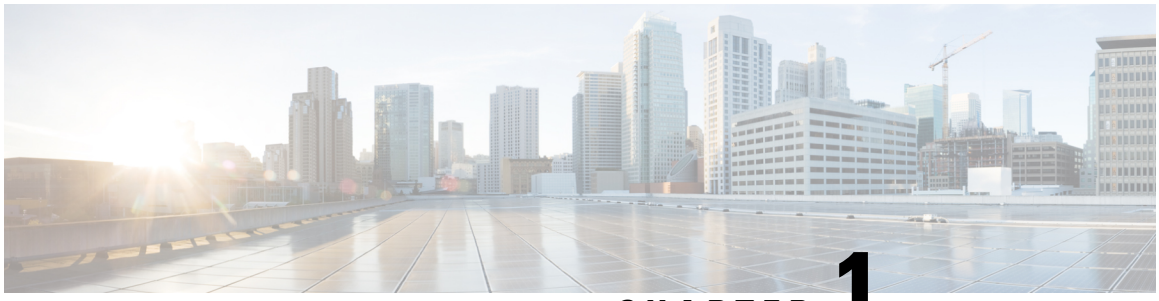
• Conventions Used, on page vii

Conventions Used

The following tables describe the conventions used throughout this documentation.

Notice Type	Description
Information Note	Provides information about important features or instructions.
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 `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
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** *variable*	This typeface represents a variable that is part of a command, for example: **show card** *slot_number* *slot_number* 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

UCC 5G UPF - Release Change Reference

Features and Behavior Change Quick Reference

Features / Behavior Changes	Release Introduced / Modified
Configurable Init Wait Timer and Mass UPF Failure Timer—CSCwb66179, on page 3	2022.04.0
Keepalived Track Interface and Virtual Routes Support in RCM—CSCwb69008, on page 4	2022.04.0
Mismatched ToS Marked Byte Count for UL and DL Packets—CSCwa22261, on page 6	2022.04.0
MPLS Support on UPF, on page 7	2022.04.0
N4/Sx over IPSec, on page 8	2022.04.0

Features / Behavior Changes	Release Introduced / Modified
NNRF Service for RCM—CSCwc49421, on page 9	2022.04.0
NRF Support, on page 10	2022.04.0
RCM Security Enhancements, on page 11	2022.04.0
RCM SNMP Traps History—CSCwa05801, on page 12	2022.04.0
Same UP Pools for SAEGW-C and SMF, on page 13	2022.04.0
Security Enhancement, on page 14	2022.04.h1
SNMP Trap for Keepalived Status Change Update Failure—CSCwc10141, on page 15	2022.04.0
SNMP Trapper Pod Modes—CSCwb66958, on page 16	2022.04.0
TCP-based High-Speed LI for UPF with IPSec, on page 17	2022.04.0
TCP Hardening between RCM and UPF, on page 18	2022.04.0
VRF Limit for Private APN and DNN , on page 19	2022.04.0

Feature Defaults Quick Reference

The following table indicates what features are enabled or disabled by default.

Feature	Default
Configurable InitWait Timer and Mass UPF Failure Timer—CSCwb66179	Disabled – Configuration Required
Keepalived Track Interface and Virtual Routes Support in RCM—CSCwb69008	Disabled – Configuration Required
Mismatched DL ToS Marked Byte Count for UL and DL Packets—CSCwa22261	Disabled – Configuration Required
MPLS Support on UPF	Disabled – Configuration Required
N4/Sx over IPSec	Enabled – Always-on
NNRF Service for RCM—CSCwc49421	Disabled – Configuration Required
NRF Support	Disabled – Configuration Required
RCM Security Enhancements	Disabled – Configuration Required
RCM SNMP Traps History—CSCwa05801	Enabled – Always-on
Same UP Pools for SAEGW-C and SMF	Disabled – Configuration Required

Feature	Default
Security Enhancement	Disabled – Configuration Required
SNMP Trap for Keepalived Status Change Update Failure—CSCwc10141	Disabled – Configuration Required
SNMP Trapper Pod Modes—CSCwb66958	Disabled – Configuration Required
TCP-based High-Speed LI for UPF with IPSec	Disabled – Configuration Required
TCP Hardening between RCM and UPF	Disabled – Configuration Required
VRF Limit for Private APN and DNN	Disabled – Configuration Required

Configurable Init Wait Timer and Mass UPF Failure Timer—CSCwb66179

Behavior Change Summary and Revision History

Summary Data

Table 1: Summary Data

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

Revision History

Revision Details	Release
First introduced. CDETS ID: CSCwb66179	2022.04.0

Behavior Change

RCM supports the following timers:

- **Init Wait Timer**—The Init Wait timer defers the registration of Init state UPs and registers the active UPs first. This timer starts only when RCM controller starts or when RCM moves to HA MASTER state.

  When RCM controller starts or moves to HA MASTER state, the RCM controller has no state and learns the UP state from the UPs itself. The Init state UPFs should not be assigned HostIDs that are already allocated to Active UPs.

- **Mass UPF Failure Timer**—The Mass UPF Failure timer starts when all UPs lose BFD connectivity with RCM. Depending on the network deployment, there could be network connectivity issue between RCM and UPs. If RCM cannot establish BFD connectivity to any UPF within the timeout period, then RCM HA switchover is performed.

Previous Behavior:

- The Init Wait timer starts only with the first UPF registration.
- The Init Wait Timer was not configurable and fixed to 300 seconds.
- The Mass UPF Failure timer was not configurable and fixed to 3 minutes.

New Behavior:

- The Init Wait timer starts only when the RCM controller starts or when RCM moves to HA MASTER state.
- The Init Wait timer is configurable using the **k8 smf profile rcm-config-ep init-wait-timeout** *init_wait_timeout* command.
- The Mass UPF Failure timer is configurable using the **k8 smf profile rcm-config-ep mass-upf-failure-timeout** *upf_failure_timeout* command.

Customer Impact:

- Reduced wait times for UPF registration.
- No change in behavior if the timer CLI commands are not used.
- The timer CLI commands can be used to change or disable the Init Wait timeout and Mass UPF Failure timeout.

For more information, refer to the *UCC 5G RCM Configuration and Administration Guide*.

Keepalived Track Interface and Virtual Routes Support in RCM—CSCwb69008

Behavior Change Summary and Revision History

Summary Data

Table 2: Summary Data

Applicable Product (s) or Functional Area	5G-UPF

Applicable Platforms	VPC-SI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	*UCC 5G RCM Configuration and Administration Guide*

Revision History

Revision Details	Release
First introduced. CDETS ID: CSCwb69008	2022.04.0

Behavior Change

RCM supports CLI commands to configure track interface and IPv4 virtual routes for the Keepalived pod.

When VIP gets attached to the service interface (when RCM moves to MASTER state), addition of IPv4 routes is required for non-host networking Bfdmgr.

Previous Behavior: RCM did not support CLI commands to configure track interface and IPv4 virtual routes for the Keepalived pod.

New Behavior: RCM supports Ops Center CLI commands to configure additional tracking interfaces and IPv4 virtual routes for the Keepalived pod.

Customer Impact: There is no impact if the CLI commands are not used. The CLI commands are backward compatible

Command Changes

Use the following RCM Ops Center CLI commands to configure the track interface and IPv4 virtual routes in the Keepalived pod:

```
k8 smf profile rcm-keepalived-ep vrrp-config group group_name
   ipv4-route route_serial_number
      destination host_network_ipv4 mask ipv4_mask gateway host_ipv4 device
interface_name
   track-interface track_interface
   exit
```

NOTES:

- **ipv4-route** *route_serial_number*: Configures the Keepalived IPv4 virtual routes.
- **track-interface** *track_interface*: Configures the Keepalived track interface.

For more information, refer to the *UCC 5G RCM Configuration and Administration Guide*.

Mismatched ToS Marked Byte Count for UL and DL Packets—CSCwa22261

Behavior Change Summary and Revision History

Summary Data

Table 3: Summary Data

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

Revision History

Table 4: Revision History

Revision Details	Release
Provided updated output for **show subscribers user-plane-only full all** and **show user-plane-service statistics qos-group sessmgr all** CLI commands.	2022.04.0
First introduced	2021.02.0

Behavior Change

Previous Behaviour: Both ToS marked Packets counter and Byte counter were available in IPv6 Traffic with DSCP Marking.

New Behaviour: Now, only the ToS marked Packets counter is available in IPv6 Traffic with DSCP Marking.

For more information, refer to the UCC 5G UPF Configuration and Administration Guide > DSCP Markings For Collapse Calls chapter.

MPLS Support on UPF

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	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	*UCC 5G UPF Configuration and Administration Guide*

Revision History

Table 6: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

This feature enables MPLS support on UPF. VPC-SI uses VPP as the dataplane forwarder. VPP encapsulates and decapsulates subscriber traffic with MPLS labels.

UPF supports the following functionalities for MPLS support:

- Uses the VPP MPLS stack to send the MPLS labeled packet
- Uses the VPP MPLS stack to process the incoming labeled MPLS packet
- MPLS on UPF uses only MP-BGP as the label distribution protocol
- VPPCTL CLI commands to display FTN and ILM tables that are in VPP for debugging and comparing values with boxer configuration

For more information, refer to the UCC 5G UPF Configuration and Administration Guide > MPLS Support on UPF chapter.

N4/Sx over IPSec

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	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	*UCC 5G UPF Configuration and Administration Guide*

Revision History

Table 8: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

In Cisco Cloud Native 5G, the IPSec functionality is available in Tunnel mode both on Session Management Function (SMF) and User Plane Function (UPF). The IPSec crypto-maps are associated under the appropriate interface on respective nodes. The IPSec tunnel is created between each SMF or UPF pair explicitly. This feature supports the IPv4 and IPv6 tunneling mode. There is no change on the N4/Sx service configuration.

The IPSec tunnel mode encapsulates the entire IP packet to provide a virtual secure hop between two gateways. In the VPN form of functionality, the entire IP packets are encapsulated inside another and delivered to the destination. It encapsulates the full IP header and payload.

For more information, refer to the UPF Configuration and Administration Guide > N4/Sx over IPSec chapter.

NNRF Service for RCM—CSCwc49421

Feature Summary and Revision History

Summary Data

Table 9: Summary Data

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

Revision History

Table 10: Revision History

Revision Details	Release
First introduced. CDETS ID: CSCwc49421	2022.04.0

Behavior Change

The RCM host configuration includes a new service type "NNRF". In the string-based approach, RCM acts as a configurator and pushes the configuration of all services including the NNRF service.

In the Yang-based approach, NSO acts as a configurator and allows configuration of only the service names in RCM. NSO pushes the whole configuration including the NNRF service.

Important The script support does exist currently for NNRF service type. So, you must manually configure this service type.

Previous Behavior: The NNRF service type was not supported.

New Behavior: The RCM host configuration includes the NNRF service type.

Customer Impact: You can use the NNRF commands in RCM.

For more information, refer to the *UCC 5G RCM Configuration and Administration Guide*.

NRF Support

Feature Summary and Revision History

Summary Data

Table 11: Summary Data

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

Revision History

Table 12: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

In the 5G service-based architecture, the Network Repository Function (NRF) maintains an updated repository of all 5G Network Functions (NFs) available in the operator's network. NRF also contains the details of the services provided by the 5G NFs, and allows the 5G NFs to instantiate, scale, and terminate without or minimal manual intervention. NRF interacts with all NFs in the 5G core network.

UPF supports only the NRF Management service that enables NF instances in the serving PLMN to register, update, or deregister their profiles in the NRF.

For more information, refer to the UCC 5G UPF Configuration and Administration Guide > NRF Support chapter.

RCM Security Enhancements

Behavior Change Summary and Revision History

Summary Data

Table 13: Summary Data

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

Revision History

Revision Details	Release
First introduced.	21.28

Feature Description

As part of security enhancement, RCM supports the following functionality:

- Partition Usage in RCM VM—In RCM VM, the */tmp* and */var/tmp* directories are mounted as separate partitions to prevent privilege escalation attacks.
- RCM provides flexibility to configure the host-networking mode for SNMP trapper pod. The **k8 smf profile rcm-snmp-trapper-ep snmp-trapper host-networking { false | true }** CLI command configures the SNMP trapper pod in host networking mode and non-host networking mode.
- RCM supports the conversion of host networking pods to non-host networking mode for restricting pod access to host network namespace. The CLI commands **k8 smf profile rcm-bfd-ep host-networking { true | false }** and **k8 smf profile rcm-bfd-ep node-port-enabled { true | false }** can be configured to run BFDmgr in non-host networking mode.
- RCM supports the tracking interface and IPv4 virtual-routes configuration for the Keepalived pod. The IPv4 virtual-routes configuration installs routes when RCM moves to MASTER state.

For more information, refer to the *UCC 5G RCM Configuration and Administration Guide*.

RCM Ops Center Configuration

Use the following RCM Ops Center CLI commands to configure the following functionality:

- To configure the SNMP trapper pod in host networking mode and non-host networking mode:

  k8 smf profile rcm-snmp-trapper-ep snmp-trapper host-networking { false | true }

- To configure host networking mode and non-host networking mod in BFDmgr:

  k8 smf profile rcm-bfd-ep host-networking { true | false }

  Default value: **true**

- To configure node port:

  k8 smf profile rcm-bfd-ep node-port-enabled { true | false }

  Default value: **false**

  The node port must be set to **true** when host networking is set to **false**.

- To configure tracking interfaces in Keepalived pod:

  k8 smf profile rcm-keepalived-ep vrrp-config group *vrrp_group_name*
  track-interface *interface_name*
  exit

- To configure IPv4 virtual routes in Keepalived pod:

  k8 smf profile rcm-keepalived-ep vrrp-config group *vrrp_group_name*
  ipv4-route *route_serial_number*
  destination *host_network_ipv4* **mask** *ipv4_mask* **gateway** *host_ipv4* **device** *interface-name*
  exit
  exit

RCM SNMP Traps History—CSCwa05801

Behavior Change Summary and Revision History

Summary Data

Table 14: 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	*UCC 5G RCM Configuration and Administration Guide*

Revision History

Revision Details	Release
First introduced. CDETS ID: CSCwa05801	2022.04.0

Behavior Change

The **rcm show-snmp-trap history** CLI command displays the history of SNMP event traps.

Previous Behavior: RCM did not support any command to display the SNMP trap history.

New Behavior: RCM supports the **rcm show-snmp-trap history** CLI command to display the SNMP trap history. This command displays details for the latest 5000 SNMP traps.

Customer Impact: This command eases debugging with the detailed history of SNMP traps.

For more information, refer to the *UCC 5G RCM Configuration and Administration Guide*.

Same UP Pools for SAEGW-C and SMF

Feature Summary and Revision History

Summary Data

Table 15: Summary Data

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

Revision History

Table 16: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

The same pool of UPs can be used by SAEGW-C and SMF. The user plane can act as UP and UPF at the same time. It can serve SAEGW over the Sx interface and SMF over the N4 interface. The same subscriber IP pool on SAEGW and SMF is supported only with different VRFs.

This functionality is qualified for the user plane acting as UP and UPF to simultaneously support CUPS and SAEGW Sx interfaces (Sxa, Sxb, and Sxab) for 2G, 3G, 4G RAT, and SMF N4 interface for 5G call.

Note The combined UP and UPF call is not qualified in this release.

For more information, refer to the UCC 5G UPF Configuration and Administration Guide > 5G-UPF Overview chapter.

Security Enhancement

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
First introduced.	2022.04.h1

Feature Description

During upgrade or downgrade, it is recommended to use the compatible configuration files to avoid lockout. The configuration files saved from a new trusted build will not work on older builds (trusted or regular) and new regular builds.

Customer Impact: Possible impact during upgrade or downgrade activities.

SNMP Trap for Keepalived Status Change Update Failure—CSCwc10141

Behavior Change Summary and Revision History

Summary Data

Table 17: Summary Data

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

Revision History

Revision Details	Release
First introduced. CDETS ID: CSCwc10141	2022.04.0

Behavior Change

Previous Behavior: The SNMP trap for status change update failure was not supported by the keepalived pod.

New Behavior: The keepalived pod generates and raises the **RCMControllerStateUpdateFailure** SNMP trap when RCM status change request through HTTP POST from RCM keepalived to RCM controller fails.

Customer Impact: The new SNMP trap eases diagnosis of issues in the keepalived pod.

For more information, refer to the *UCC 5G RCM Configuration and Administration Guide*.

SNMP Trapper Pod Modes—CSCwb66958

Behavior Change Summary and Revision History

Summary Data

Table 18: Summary Data

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

Revision History

Table 19: Revision History

Revision Details	Release
First introduced. CDETS ID: CSCwb66958	2022.04.0

Behavior Change

Previous Behavior: The SNMP trapper pod worked only in host networking mode.

New Behavior: The SNMP trapper pod can be configured in host networking mode and non-host networking mode using the **k8 smf profile rcm-snmp-trapper-ep snmp-trapper host-networking [false | true]** command.

Customer Impact: You can use the command to configure non-host networking mode for the SNMP trapper pod.

For more information, refer to the *UCC 5G RCM Configuration and Administration Guide*.

TCP-based High-Speed LI for UPF with IPSec

Feature Summary and Revision History

Summary Data

Table 20: Summary Data

Applicable Product (s) or Functional Area	5G-UPF
Applicable Platforms	VPC-SI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	None

Revision History

Table 21: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Description

User Plane or UPF platform supports TCP-based High Speed LI to support High Speed UE (HSUE). To support HSUE LI with IPSec, it is recommended to use multiple TCP connections where each VPP thread has single TCP connections with IPSec bound to that thread. For example, if a VPP maintains 16 threads, to achieve LI, there must be 16 TCP connections inline with 16 IPSec connections.

Note For more information, contact your Cisco Account representative.

TCP Hardening between RCM and UPF

Feature Summary and Revision History

Summary Data

Table 22: Summary Data

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

Revision History

Table 23: Revision History

Revision Details	Release
First introduced.	2022.04.0

Feature Changes

TCP hardening between RCM and UPF is supported with this release. As part of RCM checkpoint manager hardening, UPF supports the heartbeat mechanism between UP sessmgr and RCM checkpoint manager. This feature provides CLI support to enable or disable TCP hardening between RCM and UPF.

Previous Behavior: TCP hardening was not supported and not configurable.

New Behavior: Use the following CLI commands to configure the heartbeat mechanism:

- To enable or disable sending the heartbeat from UP sessmgr to RCM checkpointmgr, use the following command in the Context > Redundancy-Configuration-Module mode. This command is disabled by default.

  up-sm-heartbeat { disable | enable }

  To verify the configuration, use the **show config context** *context_name* command.

- To enable or disable heartbeat from RCM to active or standby UPF, use the following command in RCM Ops-center. This command is disabled by default.

  k8 smf profile rcm-config-ep enable-up-heartbeat { false | true }

Customer Impact: The heartbeat mechanism addresses the intermittent issues of TCP connectivity with UP sessmgr and RCM checkpoint managers.

For more information, refer to the *UCC 5G RCM Configuration and Administration Guide*.

VRF Limit for Private APN and DNN

Feature Summary and Revision History

Summary Data

Table 24: 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	*UCC 5G UPF Configuration and Administration Guide*

Revision History

Table 25: Revision History

Revision Details	Release
UPF supports up to 129 VRFs for private APN/DNN.	2022.04.0
Support is added for the following functionality: • Overlapping IP Pools • Removal of mandatory VRF ordering between SMF and UPF.	2021.01.0
First introduced.	2020.02.0

Feature Description

The Virtual Routing and Forwarding (VRF) feaure allows multiple instances of a routing table to coexist within the same router at the same time. In UPF, VRF enables association of IP address pools with VRF.

In this release, UPF supports up to 129 VRFs for private APN/DNN.

For more information, refer to the UCC 5G UPF Configuration and Administration Guide > Virtual Routing and Forwarding chapter.