UPC CUPS Release Change Reference, Release 21.28

First Published: 2022-09-29

Last Modified: 2024-04-30

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 NONINFRINGEMENT 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.

CONTENTS

PREFACE

CHAPTER 1

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 3G/4G CUPS product deployed in a 3G/4G 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 RCR describes new and modified feature and behavior change information for the 21.24.x CUPS releases.

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.

Notice Type	Description
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

UPC CUPS Release Change Reference

Accurate Traffic Throttling—CSCwc62127

Revision History

Revision Details	Release
First introduced.	21.28.m18

Behavior Change

Previous Behavior: The bit rates of dummy QoS Enforcement Rules (QERs associated with rulebase PDR having valid QoS Flow Identifier (QFI)) that were incorrectly applied for policing led to incorrect throttling.

New Behavior: The bit rates of dummy QERs will be ignored for policing.

Customer Impact: The customer will observe accurate throttling of traffic

Appending Original URL to Redirect URL

Revision History

Revision Details	Release
First introduced.	21.28.m10

Feature Changes

UPF supports dynamic Advice of Charge (AoC) redirections with URL provided by Online Charging System (OCS). This redirection is performed for a particular Service ID/Rating Group combination without affecting the flows mapped to other Service ID/Rating Group combinations.

For redirection to an AoC or top-up server, the UPF appends the original HTTP URL to the redirected session. To append the original URL for redirection, the OCS indicates to the CP and UP by specifying a special "?" character to the end of the AoC redirection. The redirect URL will be appended with the original URL information using the token name configured with the **diameter redirect-url-token** command under the Credit Control Configuration mode. The AoC server redirects the user to the original location on completion of AoC.

For more information, refer to the *FUI Redirection* chapter in the *UPC CUPS User Plane Administration Guide*.

Avoid Sx Flaps during Simultaneous User Plane Registrations—CSCwd39954

Revision History

Revision Details	Release
First introduced.	21.28.4

Feature Changes

In CUPS, Sx association flaps occur on the Control Plane (CP) due to delay in processing Sx queue and messenger queue at CP Sx demux. The flaps occur during simultaneous User Plane (UP) registrations with multiple egress contexts. CUPS overcomes this scenario by establishing Sx in groups after CP reboot.

Previous Behavior: During scaled setup, the Sx flap had simultaneous UP registrations.

New Behavior: CUPS supports UP registrations at the rate of 1000 per second with a pacing of 1 ms between subsequent UP registration requests.

Customer Impact: Sx flaps require reregistration of UP.

Important You must ensure to add the **update ip-pool apn all** CLI command in the CP configuration, and run it after load or reload. The **update ip-pool apn all** command is mandatory and must be part of any CP load or reload instances. Otherwise, IP chunking to UPs may not be successful.

Behavior of Debuffered TCP Packets—CSCwh37204

Revision History

Revision Details	Release
First introduced.	21.28.m14

Behavior Change

During a CUPS collapsed (Sxab) call, the downlink TCP packets are debuffered when UE moves from idle to active state. The downlink buffered TCP packets are sent after rule matching.

Previous Behavior: If the downlink buffered TCP packet was corrupt or invalid (payload length in TCP header lesser than actual payload size), L7 analysis was done when packet was debuffered.

New Behavior: If the downlink buffered TCP packet is corrupt or invalid, L7 analysis will not be done when packet is debuffered.

Behavior of Secondary RAT Usage Reports in CDR—CSCwd20301

Revision History

Revision Details	Release
First introduced.	21.28.3

Feature Changes

In the CUPS Secondary RAT Usage records scenario where the configured number of Secondary RAT Usage records are received at CP, the CP sends the query URR to UP to get the current usage report. The CP generates the PGW-CDR on receipt of the usage report.

Previous Behavior: During load conditions, if more Secondary RAT Usage Reports are received at CP before receiving the usage report from UP, the Secondary RAT Usage records reported in PGW-CDR could be more than the configured limit.

New Behavior: During load conditions, if more Secondary RAT Usage Reports are received at CP before receiving the usage report from UP, the last Secondary RAT Usage record merges with the subsequent records received until the usage report from UP. In normal scenarios, the records reported are within the configured limit. If there is a delay in the usage report due to load conditions, the last record could be bulky.

Customer Impact: There is no impact on charging. With the new behavior, the last Secondary RAT Usage record might be bulky instead of a granular report.

Boot State Assignment Trap—CSCwe40744

Revision History

Revision Details	Release
First introduced.	21.28.m14 21.28.m7

Behavior Change

The new *UPFStateAssigned* trap displays the boot state assignment.

Previous Behavior: RCM did not support the new trap.

New Behavior: RCM supports the new *UPFStateAssigned* trap. This trap displays the assigned state for a newly booted UPF registering with RCM (pending active/standby). This trap also displays the active/standby state of a UPF on controller restart or when RCM becomes HA active, and if a fully active/standby state UPF re-registers.

The existing *UPFBootComplete* trap displays the final active/standby state.

Both these traps display the UPF IP address. On comparing the timestamp of these two traps, the user can estimate the config push time for UPF.

Customer Impact: The traps display additional information about UPF.

Configurable Init Wait Timer and Mass UPF Failure Timer—CSCwb66179

Revision History

Revision Details	Release
First introduced.	21.28.0

Feature Changes

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.

Command Changes

Use the following RCM Ops Center CLI commands to configure the Init Wait timer and Mass UPF Failure timer.

```
k8 smf profile rcm-config-ep init-wait-timeout init_wait_timeout
k8 smf profile rcm-config-ep mass-upf-failure-timeout upf_failure_timeout
```

NOTES:

- **init-wait-timeout** *init_wait_timeout*: Specify the Init Wait timer, in seconds, as an integer from 0 to 300.

  Default: 300 seconds. A value of 0 disables the Init Wait timer.

- **mass-upf-failure-timeout** *upf_failure_timeout*: Specify the Mass UPF Failure timer, in minutes, as an integer from 0 to 60.

  Default: 3 minutes. A value of less than 3 minutes disables the timer. UPFs need at least three minutes to reload. When all UPFs are simultaneously reloaded as part of the UPF-RCM workflow, a value of less than three minutes can potentially cause false positive alarms.

CUPS Support for VMware Release 7

Revision History

Revision Details	Release
First introduced.	21.28.0

Feature Description

CUPS (control plane and user plane) using VPC-SI supports VMware Release 7. CUPS uses the VMware-based deployments as an alternate deployment model to reduce cost and complexity.

For more information, refer to the *Ultra Packet Core CUPS Control Plane Administration Guide* or *Ultra Packet Core CUPS User Plane Administration Guide*.

CUPS Support on VMware ESXi 6.7

Revision History

Revision Details	Release
First introduced.	21.28.0

Feature Description

CUPS supports the VMware-based deployment model on VMware ESXi 6.7, VMXNET3 for GW-C, and PCT-PT for GW-U for Intel 6248R CPU.

For more information, see the *Ultra Packet Core CUPS Control Plane Administration Guide* or *Ultra Packet Core CUPS User Plane Administration Guide*.

Deletion of ACS Configuration—CSCwf98047

Revision History

Revision Details	Release
First introduced.	21.28.m14

Behavior Change

The deletion of ACS Configuration will be effective for existing offloaded flows on UPF.

Previous Behaviour: When ACS configuration was deleted in the config path, the offloaded flows in UPF were not onloaded.

New Behavior: After deletion of ACS configuration, the offloaded flows will be onloaded and reprogrammed in UPF.

Customer Impact: You will observe stable and defined behaviour on UPF post deletion of the ACS configuration.

DI-Net Encryption

Revision History

Revision Details	Release
First introduced.	21.28.0

Feature Description

The CUPS-DI systems uses Galois/Counter Mode (GCM) encryption algorithm for DI-Net traffic encryption. The GCM algorithm replaces Advanced Encryption Standard Cipher Block Chaining (AES CBC) algorithm for better data protection and integrity.

Note The change in encryption algorithm requires a system reload.

The new encryption algorithm is configurable via boot parameter file. The GCM algorithm supports an authenticated encryption mode. On the decrypting side, GCM uses Additional Authentication Data (AAD) to authenticate the payload.

For more information, see the *DI-Net Encryption* chapter in the *Ultra Packet Core CUPS Control Plane Administration Guide* or *Ultra Packet Core CUPS User Plane Administration Guide*.

Disabling RCM Traps—CSCwe40690

Revision History

Revision Details	Release
First introduced.	21.28.m14

Behavior Change

Previous Behavior: All RCM traps are enabled by default.

New Behavior: The following SNMP traps are disabled by default to prevent flooding of less significant traps in the **rcm show-snmp-trap history** command.

- ActiveSessmgrConnected
- ActiveSessmgrDisconnected
- CheckpointAuditEnded
- CheckpointAuditStarted
- StandbySessmgrConnected
- StandbySessmgrDisconnected

To enable these traps, use the **k8 smf profile rcm-snmp-trapper-ep snmp-trapper clear-dflt-traps** command. After issuing this command, disable the traps using the **disable-trap** command.

Customer Impact: The **rcm show-snmp-trap history** command will not be flooded with traps that are very frequent and less significant.

DNS Snooping and Tethering Detection Bypass Support

Revision History

Revision Details	Release
First introduced.	21.28.0

Feature Description

In this release, the DNS Snooping and Tethering Detection Bypass features for ECSv2 are supported as part of L3, L4, and L7 rule combination in Ruledef.

See the *L3, L4, and L7 Rule Combination in Ruledef* chapter in the *Ultra Packet Core CUPS User Plane Administration Guide* and *Ultra Packet Core CUPS User Plane Administration Guide* for more information.

EDNS Enrichment

Revision History

Revision Details	Release
First introduced.	21.28.m10

Feature Changes

CUPS supports enrichment of EDNS requests to enrich and readdress DNS requests of subscribers who are subscribed to the parental control service.

When a subscriber subscribes to a parental control service, DNS requests by the subscriber are enriched with additional information (IMSI, MSISDN, APN) and readdressed to the dedicated DNS server for appropriate analysis and treatment. This additional information is configurable through an eDNS format that specifies different fields (tag values). These fields are encoded and appended to the DNS request header.

For more information, refer to the *EDNS Enrichment* chapter in the *UPC CUPS User Plane Administration Guide*.

Enabling Standalone RCM Without Keepalived—CSCwc12468

Revision History

Revision Details	Release
First introduced. CDETS ID: CSCwc12468	21.28.0

Feature Changes

This release supports a configurable CLI to use when you run RCM without keepalived achieve MASTER status. The MASTER status is required for UPF to register.

Previous Behavior: The CLI command to enable keepalived in RCM was not required in releases prior to 21.28.x.

New Behavior: This release supports a new CLI command to use when you run RCM without keepalived to achieve MASTER status.

```
k8 smf profile rcm-config-ep ha-standalone { true | false }
```

The default setting is **false**.

Customer Impact: From release 21.28.x onwards, customers running RCM without keepalived must set the CLI command to true.

END MARKER Handling during eNB Path Switchover for Multi-Bearer PDNs—CSCwj13323

Revision History

Revision Details	Release
First introduced.	21.28.20

Behavior Change

In CUPS, SNDEM flag is set in the FAR and sent towards UP. UP sends the GTP END MARKER on the GTPU tunnel for which SNDEM flag is received.

Previous Behavior: All the bearers receive GTP END MARKER even if there is a change in F-TEID in any one of the bearers.

New Behavior: UP sends the GTP END MARKER only for the bearer on which the F-TEID is changed.

Customer Impact: END MARKER is sent to the tunnels that are being switchover to a new eNB/gNB and not to every bearer binded to the same PDN Session.

Encryption of LI Information in RCM

Revision History

Revision Details	Release
First introduced.	21.28.0

Feature Description

The RCM configuration on CUPS UP must include encrypted public and private keys to secure the LI information. When this feature is enabled, the LI information that the RCM receives is in encrypted format.

Important The users of CUPS UP running the trusted builds must enable this feature. Otherwise, recovery is not supported for LI functionality.

All UPs (both active and standby) should have the same set of public and private keys. Active UP uses public key to encrypt the LI information before sending to RCM. Standby UP uses the private key to decrypt the information received from RCM. If keys are not present in active UP running the trusted build, LI information is not sent to RCM and it impacts the LI recovery functionality. Non-trusted build, with no key configuration, continue sending LI information as plain binary.

Important The keys once configured, cannot be removed.

For more information, refer to the *Lawful Intercept in CUPS* chapter in the *CUPS LI Guide*.

Enriching DNS Requests with Additional RRs

Revision History

Revision Details	Release
First introduced.	21.28.m23

Feature Changes

CUPS supports enrichment of DNS requests that contain Additional RRs.

The DNS requests are enriched by adding Option-Codes and Option-Data fields based on the configured EDNS format in the following scenarios:

- Presence of additional RRs of OPT RR type in the incoming DNS request

  If an OPT RR is present in the incoming request, it is deleted, and a new OPT RR is added as the first additional RR based on the configured EDNS format.

- Absence of additional RRs in the DNS request

  If no Additional RRs are present in the DNS request, enrichment is done by adding an OPT RR to the request.

- Presence of additional RRs other than OPT RR type in the DNS request

For more information, see the *EDNS Enrichment* chapter in the *UPC CUPS User Plane Administration Guide, Release 21.28*.

Exact Duration for SGW-CDR Fields—CSCwf12125

Revision History

Revision Details	Release
First introduced.	21.28.m14

Behavior Change

The "duration" and "changeTime" fields display the exact accumulated time in the following scenarios for S-GW CDR when:

- Zero volume CDR suppress configuration is enabled,
- Sx Session Report Request is received without data continuously, and
- Session Manager restarts

Previous Behavior: In the above scenario for SGW-CDR, the duration and changeTime fields in CDR are not accumulated.

New Behavior: In the above scenario for SGW-CDR, the duration and changeTime fields in CDR are accumulated.

Customer Impact: The changeTime and duration fields of CDR ELEMENTS display accurate information with the exact duration.

FAR Buffering Limit

Revision History

Revision Details	Release
First introduced.	21.28.m23

Feature Changes

With this release, the number of packets to be buffered per FAR on UP is configurable using the **buffering-limit far-max-packets** *far_max_packets* CLI in the ACS Configuration mode.

By default, 5 packets will be buffered per FAR. You can configure more number of FAR buffered packets to achieve QoS with fewer packet drops.

The **show user-plane-service statistics all** CLI is enhanced to display the dropped packets per FAR.

Command Changes

Use the following configuration to configure the maximum number of packets to be buffered per FAR:

```
configure
   active-charging service acs_service_name
      buffering-limit far-max-packets far_max_packets
      end
```

NOTES:

- **buffering-limit far-max-packets** *far_max_packets*—Specify the maximum number of packets to be buffered per FAR. *far_max_packets* must be an integer from 1 to 128.

  Default value: 5 packets

The packets received after maximum number of packets are already buffered and the subsequent packets are dropped. To view the number of times that packets in a specified range are dropped, use the **show user-plane-service statistics all** command.

The following is a sample output of this command:

```
[local]qvpc-si# show user-plane-service statistics all
…
  Data Statistics Related To Buffering:
    Packets Buffered:                  0    Bytes Buffered:                    0
    Packets Discarded:                 0    Bytes Discarded:                   0
    Packets Dropped per FAR (<=9)      0    Packets Dropped per FAR (10-19)    0
    Packets Dropped per FAR (20-49)    0    Packets Dropped per FAR (30-39)    0
    Packets Dropped per FAR (40-49)    0    Packets Dropped per FAR (>=50)     0
```

Generating SNMP Trap from User Plane during Warning Interval—CSCwc01756

Revision history

Revision Details	Release
First introduced.	21.28.m10

Feature Changes

In StarOS, if the password is not reset before the expiration date, you get locked out from the configured gateways. You are allowed to log on back only when the administrator resets the password manually.

Previous Behavior: When the StarOS login password is about to expire, only a warning message was displayed during login attempt. This caused disruption in the RCM workflow and the warning message was disabled for the RCM workflow.

New Behavior: A PasswordExpiryNotification SNMP trap is generated daily every 24 hours during the warning interval before password expiry.

Customer Impact: The SNMP trap gets generated every 24 hours along with the warning message.

For more information, see the *Password Expiration Notification* chapter in the *VPC-SI System Administration Guide*.

Handling Non-SYN TCP and UDP Packets for NAT Subscribers—CSCwf64696

Revision History

Revision Details	Release
First introduced.	21.28.m10

Behavior Change

To avoid generation of empty EDRs, CUPS supports the following functions:

- For TCP, the non-SYN packets for NAT subscribers will be dropped without creating a new flow.
- For UDP, the packets will be buffered while IP allocation is in progress and will be processed once IP allocation is complete.

Previous Behavior: Each non-SYN TCP packet created a flow and generated an empty EDR when the packet got dropped due to NAT or Firewall, and the flow was cleared. The UDP packets of new flows were dropped while NAT IP allocation was in progress for a subscriber.

New Behavior: For a NAT-enabled subscriber, the non-SYN TCP packet will be dropped without creating a flow. The UDP packets of new flows will not be dropped while NAT IP allocation is in progress for a subscriber. These packets will be buffered and processed once NAT IP allocation is successful.

Handling Simultaneous Gy RARs from Different DRAs with Different RGs

Revision History

Revision Details	Release
First introduced.	21.28.m1

Feature Description

CUPS supports multiple Diameter Routing Agents (DRA) to prevent the abort of pending Credit Control Request–Update (CCR-U) requests from previous Reauthorization Requests (RAR) with a different host or peer on the Gy interface.

P-GW accepts different rating-groups (RG) from different peers by configuring the **diameter pending-ccau allow-on-rar-peer-switch** CLI command in the ACS configuration mode. This command allows you to configure the DCCA client to prevent the abort of a pending CCR-U request.

For more information on the multiple DRA support in P-GW, see the *Support for Multiple DRA over Gy Interface* chapter in the *P-GW Administration Guide*.

How it Works

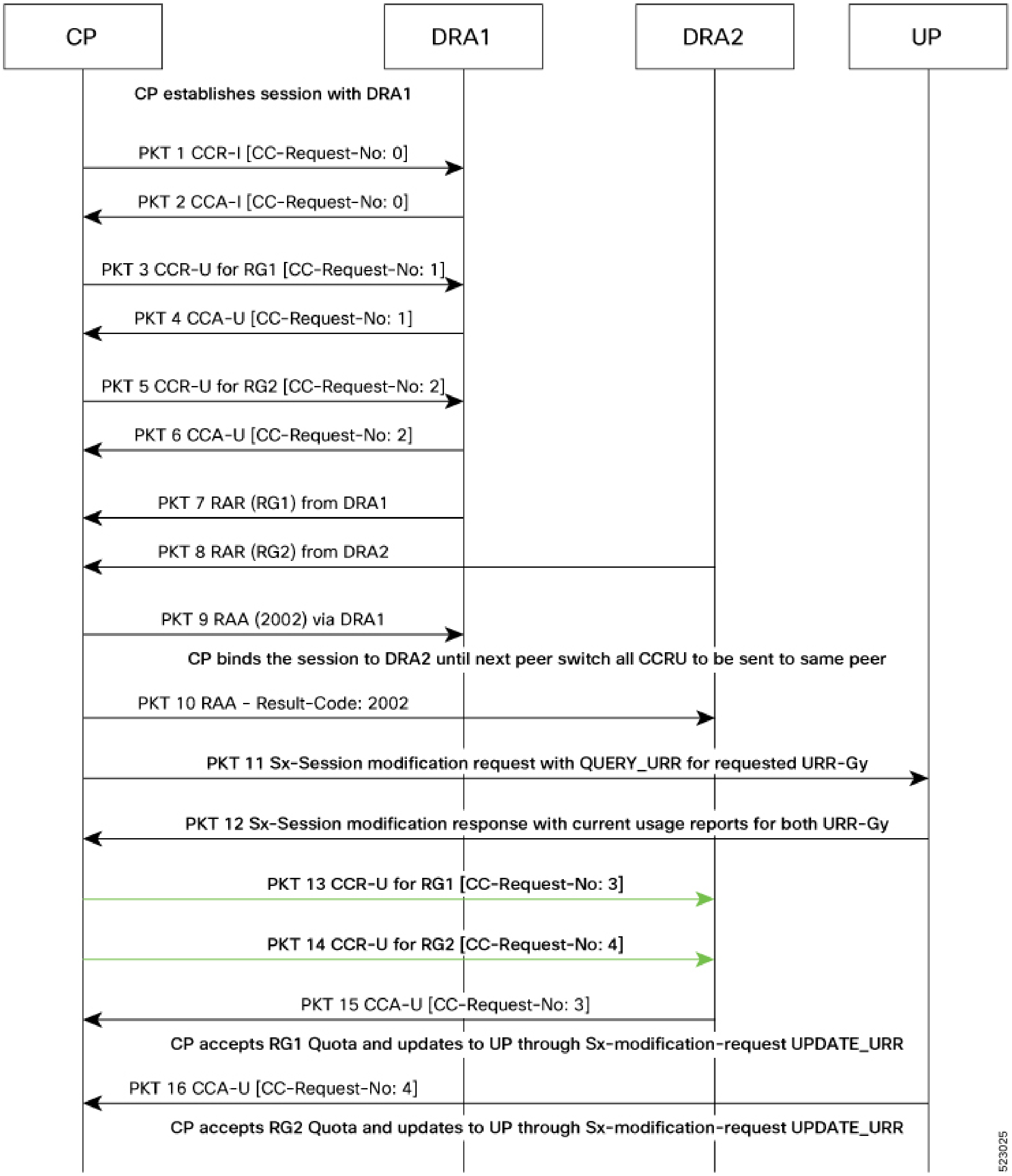
This section describes how the multiple DRA feature works in CUPS.

P-GW and CUPS handle the collision scenarios differently. In legacy P-GW, each CCR-U with FORCED REAUTHORIZATION is sent to the corresponding DRAs.

In CUPS, the user plane fetches every CCR-U that is sent along with the current usage report. During collision, if more than one specific RAR is received at the same time from different DRAs for the respective rating groups, the control plane marks the Gy-URR buckets, and sends Sx Session Modification Request to the user plane. The user plane sends back the current usage reports to the control plane for the requested Gy-URR bucket in Sx Session Modification Response. If RAR is received from different DRAs, the peer switch happens. In CUPS, each CCR-U with FORCED REAUTHORIZATION for the requested rating groups is sent to the peer DRA of the latest path switched.

The following call flow illustrates how P-GW accepts both RGs from different peers.

Figure 1: Multiple DRA Call Flow in CUPS


CP
DRA1
DRA2
UP
CP establishes session with DRA1
PKT 1 CCR-I [CC-Request-No: 0]
PKT 2 CCA-I [CC-Request-No: 0]
PKT 3 CCR-U for RG1 [CC-Request-No: 1]
PKT 4 CCA-U [CC-Request-No: 1]
PKT 5 CCR-U for RG2 [CC-Request-No: 2]
PKT 6 CCA-U [CC-Request-No: 2]
PKT 7 RAR (RG1) from DRA1
PKT 8 RAR (RG2) from DRA2
PKT 9 RAA (2002) via DRA1
CP binds the session to DRA2 until next peer switch all CCRU to be sent to same peer
PKT 10 RAA - Result-Code: 2002
PKT 11 Sx-Session modification request with QUERY_URR for requested URR-Gy
PKT 12 Sx-Session modification response with current usage reports for both URR-Gy
PKT 13 CCR-U for RG1 [CC-Request-No: 3]
PKT 14 CCR-U for RG2 [CC-Request-No: 4]
PKT 15 CCA-U [CC-Request-No: 3]
CP accepts RG1 Quota and updates to UP through Sx-modification-request UPDATE_URR
PKT 16 CCA-U [CC-Request-No: 4]
CP accepts RG2 Quota and updates to UP through Sx-modification-request UPDATE_URR
523025

Configuring the Feature

To configure the handling of multiple RAR requests involving multiple DRAs, use the following configuration:

```
configure
   context context_name
   active-charging service acs_service_name
      credit-control [ group cc_group_name ]
         diameter dictionary dictionary
            [ no ] diameter pending-ccau allow-on-rar-peer-switch
            end
```

NOTES:

- **diameter dictionary** *dictionary*: Set the diameter dictionary to handle different DRAs.

  For example: **diameter dictionary** *dcca-custom-26*

- **diameter pending-ccau allow-on-rar-peer-switch**: Allow the DCCA client to prevent the abort of pending CCAU requests.

- **no diameter pending-ccau allow-on-rar-peer-switch**: Disable the DCCA client from preventing the abort of pending CCAU requests.

Monitoring and Troubleshooting

This section provides the monitoring and troubleshooting information for the multiple DRA feature.

Show Commands and Outputs

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

show active-charging service all

Table 1: show active-charging service all

Field	Description
pending ccau:	
allow-on-rar-peer-switch	Displays "Enabled or "Disabled" to indicate the abort of pending CCA-U request if RAR is received from different host or peer on the Gy interface. If this feature is enabled, the functionality is applicable only to new Diameter sessions.

HTTP Request Methods during Redirection—CSCwi06981

Revision History

Revision Details	Release
First introduced.	21.28.m18

Behavior Change

Previous Behavior: HTTP redirection was applied only on HTTP GET and not applied on other methods such as HTTP POST.

New Behavior: HTTP redirection will now be applied on all HTTP Request methods.

Intercept Provisioning Method in UP—CSCwh28931

Revision History

Revision Details	Release
First introduced.	21.28.m14

Behavior Change

Previous Behavior: The Provisioning Method field in the output of the **show lawful-intercept active-only** and **show lawful-intercept camp-on-triggers** CLI commands was displayed in UP.

New Behavior: The user plane does not provision any intercepts as all provisioning is on the control plane. Therefore, the Provisioning Method field on UP will be restricted.

International Roaming

Revision History

Revision Details	Release
First introduced.	21.23.22 21.28.0

Feature Description

Previous Behavior: During the Initial Attach procedure, the SGW-S5U interface is configured with IPv4v6 and the PGW-S5U interface is configured with IPv4 as part of the GTPU configurations. The PGW-C does not recognize the interface details of PGW-S5U. The Sx Session Establishment Request that is initiated from CP includes the GTP-U/UDP/IPv6 Outer Header Removal (OHR) in Create PDR and a similar Outer Header Creation (OHC) in Create Far. This results in a mismatch of IE in UP and the Sx Session Establishment Request gets rejected due to which the call fails with the OUTER_HDR_REMOVAL value as PFCP_CAUSE_MANDATORY_IE_INCORRECT.

New Behavior: PGW-U supports common OHR and OHC types for IPv4 and IPv6 based on PGW-U interfaces. GTP-U/UDP/IPv6 support is added for OHR and IPv4v6 support is added for OHC.

Customer Impact: None.

For more information, see the *International Roaming* chapter in the *Ultra Packet Core CUPS Control Plane Administration Guide* or *Ultra Packet Core CUPS User Plane Administration Guide*.

Keepalived Track Interface and Virtual Routes Support in RCM—CSCwb69008

Revision History

Revision Details	Release
First introduced.	21.28.0

Feature Changes

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.

LI Keepalive Message Support

Revision History

Revision Details	Release
First introduced.	21.28.5 21.28.m6

Feature Changes

CUPS supports S8HR LI application heartbeat messages to be sent from BBIFF to LMISF at periodic intervals. This feature avoids IPsec tunnel termination or TCP socket clearance in the firewall present between BBIFF and LMISF. The keepalive message is sent on both the Xia and Xib interfaces.

This feature is configurable and the command must be executed only on CP. If executed on UP, it throws an error.

Previous Behavior: An IPsec tunnel connects the BBIFF to the firewall when in between BBIFF and LMISF. When the idle timer expires, the firewall clears the port map, resulting in termination of the IPsec tunnel or clearance of TCP sockets.

New Behavior: BBIFF sends a new unidirectional keepalive message to LMISF periodically after a configurable time interval. This avoids IPsec tunnel termination or TCP socket clearance in the firewall present between BBIFF and LMISF.

For more information, contact your Cisco Account representative.

MBR and UBR Collision Handling—CSCwh47513

Revision History

Revision Details	Release
First introduced.	21.28.m14

Behavior Change

For Pure-S calls, S-GW drops the PGW-initiated UBR during Modify Bearer Request (MBR) and Update Bearer Request (UBR) collision in the network.

Previous Behavior: If S-GW receives the PGW-initiated UBR while processing MBR for ULI change, then S-GW rejects UBR with cause "No Resource Available".

New Behavior: If S-GW receives the PGW-initiated UBR while processing MBR for ULI, MME, or eNodeB change, then S-GW drops UBR silently. P-GW then retries UBR and S-GW processes the request after MBR.

Namespace Option in RCM Script—CSCwd79932

Revision History

Revision Details	Release
First introduced.	21.28.m14 21.28.m3 21.28.3

Feature Changes

The **apply_config_v2** RCM script is modified to support the namespace option.

Previous Behavior: The script did not support the namespace option.

New Behavior: The script supports the "N" option to provide the namespace argument. By default, the value is **rcm**.

```
bash -x ./apply_config_v2.sh -g 1 -n -c UPCommon.cfg -P
/var/lib/smi/data/common_config/config4.cfg -G 4 -p connect_file -k
password -N rcm
```

NNRF Service for RCM—CSCwc49421

Revision History

Revision Details	Release
First introduced.	21.28.0

Feature Changes

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.

Optimizing GTPU Memory Usage—CSCwf21120

Revision History

Revision Details	Release
First introduced.	21.28.m14 21.28.m10

Behavior Change

Previous Behavior: For user plane service and Sx-u service, the GTPU peers were freed only after reaching one million peers.

New Behavior: For user plane service and Sx-u service, the GTPU peer entries will be removed when they become inactive. This happens after the last session associated with a GTPU peer is terminated.

Customer Impact: The user might observe differences in the output of CLI commands related to GTPU peers. Since only active peers remain in the system, the information displayed will pertain to that of active peers. This change will reduce the memory usage of GTPU manager.

Planned Switchover Timers on RCM—CSCwd35392

Revision History

Revision Details	Release
First introduced.	21.28.m14 21.26.17

Feature Changes

UPF supports the following timers for planned switchover through RCM:

- Preswitchover timer that defaults to 15 seconds
- Stage 1 checkpoint flush timer from old Active UPF to Checkpointmgrs that defaults to 15 seconds
- Stage 2 Checkpoint flush timer (non critical) from old Active UPF to Checkpointmgrs that defaults to 10 seconds

Command Changes

Use the following RCM OpsCenter Configuration mode CLIs to configure the following timers:

- Preswitchover timer:

  ```
  k8 smf profile rcm-config-ep swo-timeouts pre-switchover
  preswitchover_timeout
  ```

- Stage 1 Checkpoint Flush timer:

  ```
  k8 smf profile rcm-config-ep swo-timeouts stage1-chkpt-flush
  stage1_flush_timeout
  ```

- Stage 2 Checkpoint Flush timer:

  ```
  k8 smf profile rcm-config-ep swo-timeouts stage2-chkpt-flush
  stage2_flush_timeout
  ```

NOTES:

- **k8 smf profile rcm-config-ep swo-timeouts pre-switchover** *preswitchover_timeout*: Specify the timeout for preswitchover, in seconds. *preswitchover_timeout* must be an integer from 15 to 3600.

  Default value: 15 seconds

- **k8 smf profile rcm-config-ep swo-timeouts stage1-chkpt-flush** *stage1_flush_timeout*: Specify the timeout for stage 1 checkpoint flush from old Active UPF to checkpointmgrs, in seconds. *stage1_flush_timeout* must be an integer from 15 to 3600.

  Default value: 15 seconds

- **k8 smf profile rcm-config-ep swo-timeouts stage2-chkpt-flush** *stage2_flush_timeout*: Specify the timeout for stage 2 checkpoint flush (non-critical) from old Active UPF to checkpointmgrs, in seconds. *stage2_flush_timeout* must be an integer from 15 to 3600.

  Default value: 10 seconds

Prioritizing IMEI over MAC Address

Revision History

Revision Details	Release
First introduced.	21.28.m22

Feature Changes

Previous Behavior: If IMEI was received in Create Session Request for a Wi-Fi call, the ePDG CDR encoded MAC address in the servedIMEISV field. The MAC address was given preference over IMEI and encoded in servedIMEISV. With this behavior, CDR processing was affected.

New Behavior: IMEI will be prioritized over MAC address and will be sent in the servedIMEISV field. The servedIMEIsv field in CDR is optional. If Create Session Request for a Wi-Fi call has both IMEI and MAC address, then IMEI is encoded in servedIMEIsv.

This behavior is configurable using the **gtpp prioritize-imei-over-mac-address** CLI in the GTPP Server Group Configuration mode. If the CLI is not configured, the existing behaviour will take effect.

Command Changes

Use the following configuration to prioritize IMEI over MAC address and encode IMEI in the servedIMEISV field of the CDR. If IMEI is not available, the servedIMEISV field will not be present in the CDR.

```
configure
   context context_name
      gtpp group group_name
         [ default | no ] gtpp prioritize-imei-over-mac-address
         end
```

NOTES:

- **default | no**—Specify either one of the options to prioritize MAC over IMEI and encode it in servedIMEISV field. This is the existing behavior.

  If MAC is not available, then IMEI is encoded in the servedIMEISV field.

RCM Endpoint Statistics—CSCwf06065

Revision History

Table 2: Revision History

Revision Details	Release
First introduced.	21.28.m14

Behavior Change

The RCM checkpoint manager now supports aggregate counters for endpoint statistics and Prometheus metrics.

Previous Behavior: RCM supported checkpoint statistics at the session level only.

New Behavior: RCM supports aggregate counters at the checkpoint-manager instance level under the**rcm endpointstats checkptmgr** CLI command and Prometheus metrics.

Customer Impact: The customer can view the new counters in the output of the endpoint statistics command.

RCM Helm Version Upgrade

Revision History

Revision Details	Release
First introduced.	21.28.0

Feature Changes

The RCM Helm version is upgraded from Helm2 to Helm3 for Kubernetes (K8s) pod deployment.

Previous Behavior: RCM used Helm2 and tiller for K8s pod deployment.

New Behavior: RCM uses only Helm3 for K8s pod deployment.

RCM Security Enhancements

Revision History

Revision Details	Release
First introduced.	21.28.0

Feature Changes

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.

Command Changes

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

Revision History

Revision Details	Release
First introduced.	21.28.0

Feature Changes

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.

RCM Statistics Information—CSCwe42938

Revision History

Revision Details	Release
First introduced.	2023.02.1

Behavior Change

The output of the rcm show-statistics bfdmgr command displays additional information.

Previous Behavior: The **rcm show-statistics bfdmgr** command displayed the following information:

- The minRx and minTx values in microseconds
- The locally configured multipier
- No down detect time

New Behavior: The updated **rcm show-statistics bfdmgr** command displays the following information:

- The minRx and minTx values in milliseconds
- The remotely configured multiplier when the BFD state is STATE_UP
- The down detect time in milliseconds

Customer Impact: The updated software displays the additional information. The **rcm show-statistics bfdmgr** command also displays values negotiated by both locally configured Tx/Rx and remotely configured Rx/Tx.

RCM Support for Cisco SSL—CSCwd32422

Revision History

Revision Details	Release
First introduced.	21.28.m14

Behavior Change

RCM uses Cisco SSL instead of OpenSSL.

Previous Behavior: The RCM VM and rcm-strongswan pod used the following OpenSSL version:

```
OpenSSL 1.1.1f 31 Mar 2020
```

New Behavior: The RCM VM and rcm-strongswan pod uses the following Cisco SSL version:

```
CiscoSSL 1.1.1q.7.2.440
```

Returning Correct PFCP Cause Code—CSCwh00402

Revision History

Revision Details	Release
First introduced.	21.28.m14

Behavior Change

UP now sends the PFCP error cause code PFCP_CAUSE_NO_RESOURCE_AVAILABLE in the following failure scenarios during:

- Sx Establishment Request and Sx Modification request message processing
    - Bearer stream creation failure for Sxa
    - TEP row add failure for Sxa
    - Local local_gtpu_endpt address mismatch or unavailable
    - Above failure scenarios for N4 visited call
- PFCP_IE_QGR_INFO IE processing memory failures
- NAT rulebase change or policy change cases and failure due to
    - FW-and-NAT policy initilization failure during call setup or rulebase change
    - Invalid clp destination context
    - Memory allocation failure
- Sx Establishment or Sx Modification message processing – local GTPU TEID allocation failure

Previous Behavior: UP sent the error cause PFCP_CAUSE_REQUEST_REJECTED for the above failure scenarios.

New Behavior: UP sends the error cause PFCP_CAUSE_NO_RESOURCE_AVAILABLE instead of PFCP_CAUSE_REQUEST_REJECTED for the above failure scenarios.

Route Map Configuration—CSCwf54987

Revision History

Revision Details	Release
First introduced.	21.28.6 21.28.m10

Behavior Change

CUPS supports a new CLI command to add a route-map under VPNv6 address-family.

Previous Behavior: CUPS did not support the capability to add a route-map under VPNv6 address-family.

New Behavior: CUPS supports the **route-map** option CLI command under the BGP Address-Family Configuration mode to apply a route-map.

To apply the route-map to a neighbor, use the following configuration:

```
configure
   context context_name
      router bgp as_number
         address-family vpnv6
            neighbor route-map map_name { in | out }
            end
```

NOTES:

- **address-family vpnv6**: Configure the IPv6 VPN address family configuration parameters for BGP router.
- **neighbor route-map** *map_name* **{ in | out }**: Specify the route map to apply to a neighbor. *map_name* must be the name of an existing route-map in the current context.
  - **in**: Indicates that the route map applies to incoming advertisements.
  - **out**: Indicates that the route map applies to outgoing advertisements.

Rule Match after TCP Teardown Initiation

Revision History

Revision Details	Release
First introduced.	21.28.0

Feature Changes

After TCP teardown is initiated, there is a change in rule match and charging of the received data packets.

Previous Behavior: Data packets received during or after TCP teardown initiation were matched to the previous rule that was matched for packets in that direction.

New Behavior: Data packets received during or after TCP teardown initiation will be rule matched. Depending on the rule configuration, the packets may match a different rule than that was matched for the previous packet in that direction.

Customer Impact: Difference in rule match for packets received during or after TCP teardown initiation. To be able to match the data packets correctly to the L7 rule, the TCP flag-based and packet length-based L4 rule will have to be configured to exclusively match the TCP control packets.

S8HR LI TCP Connection Timeout

Revision History

Revision Details	Release
First introduced.	21.28.7

Feature Description

CUPS LI supports the TCP connection timeout feature for an S8 Home Routing (S8HR) roaming user in the S-GW service.

For more information, contact your Cisco account representative.

Security Enhancement

Revision History

Revision Details	Release
First introduced.	21.28.1

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.

Session Checkpoint Compression Algorithms

Revision History

Revision Details	Release
First introduced.	21.28.0

Feature Changes

The RCM supports a combination of both ZLib and LZ4 compression algorithms. For M:N redundancy model, ZLib is the default algorithm that is used to compress the session checkpoint information from UPF to RCM.

In the SRP-based model, the user can choose either of the two compression algorithms for session checkpointing.

Important For data compression and decompression to work, both active and standby UPs must be configured with the same algorithm.

Command Changes

Use the **checkpoint session compression lz4** CLI command in RCM configuration mode to enable the use of LZ4 compression algorithm. You can also revert the compression algorithm to zlib using the **checkpoint session compression zlib** CLI command.

The following command sequence enables the use of LZ4 compression:

```
configure
   context context_name
      redundancy-configuration-module rcm_name
         checkpoint session compression lz4
         end
```

NOTES:

- **checkpoint session compression**: Enables compression of checkpointed session information.
- **checkpoint session compression lz4**: Compresses the checkpointed session information using algorithm - lz4.

For detailed configuration steps, see the *Configuring LZ4 Compression Algorithm* section in the *UPC CUPS User Plane Administration Guide*.

SNMP Trap for Keepalived Status Change Update Failure—CSCwc10141

Revision History

Revision Details	Release
First introduced.	21.28.0

Feature Changes

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.

SNMP Traps to Debug Sx Endpoints Misconfiguration—CSCwf04861

Revision History

Revision Details	Release
First introduced.	21.28.m14

Behavior Change

Previous Behavior: If there was any invalid monitor configuration in Sx endpoints, SNMP traps do not get triggered.

New Behavior: UPF supports the following two SNMP traps to detect misconfiguration in Sx endpoints:

- **NotAllSxMonitorsUp**—This SNMP trap is sent whenever Sx monitor is configured.

  The following conditions apply at the time of Sx monitor installation:

  1. If an Sx peer is not configured or misconfigured in the Control Group (CG), the generated trap remains as NotAllSxMonitorsUp.

  2. If an Sx peer is configured in the CG and Sx association is Down, the generated trap remains as NotAllSxMonitorsUp.

3. If an Sx peer is configured in the CG and Sx association is Up, then configured Sx monitors are checked. If any Sx monitor has the NOT STATUS_UP status, the trap generated remains as NotAllSxMonitorsUp. Otherwise, the AllSxMonitorsUp trap is generated.

4. If an Sx peer is not configured or misconfigured in the CG but the peer is subsequently configured in CG, then the preceding points 2 and 3 will apply.

- **AllSxMonitorsUp**—When an Sx monitor sends the Sx association status (up or down), the configured Sx monitors are reviewed. If an Sx monitor has the NOT STATUS_UP status, the NotAllSxMonitorsUp trap is generated. Otherwise, the AllSxMonitorsUp trap is generated.

Customer Impact: The new SNMP traps allow easy debugging.

Spoofing Detection Support

Revision History

Revision Details	Release
First introduced.	21.28.m1

Feature Changes

The X-Header Enrichment feature appends headers to HTTP or WSP GET and POST request packets, and HTTP Response packets. This feature is used by end applications for mobile advertisement insertion (MSISDN, IMSI, IP address, and so on).

This release supports spoofing detection in X-header fields using a configurable CLI. The **delete-existing** keyword option is added under the **xheader-format** command to enable spoofing detection.

For more information, see the *X-Header Insertion and Encryption* chapter in the *Ultra Packet Core CUPS Control Plane Administration Guide* and *Ultra Packet Core CUPS User Plane Administration Guide*.

Command Changes

The **delete-existing** option is added to the **insert** command in the X-Header Format Configuration mode.

The **delete-existing** option enables spoofing detection in X-header fields. The X-header field configured with this keyword will be removed from the HTTP header if it already exists, and only the gateway inserted field will remain. By default, anti-spoofing is disabled. and if required, should be enabled at a field level.

To configure an X-header format, use the following configuration:

```
configure
  active-charging service ecs_service_name
    xheader-format xheader_format_name
      insert xheader_field_name string-constant xheader_field_value | variable
{ bearer { 3gpp { apn | charging-characteristics | charging-id | imei |
imsi | qos | rat-type | s-mcc-mnc | sgsn-address } | acr | customer-id |
 ggsn-address | mdn | msisdn-no-cc | radius-string |
radius-calling-station-id | session-id | sn-rulebase |
subscriber-ip-address | username } [ encrypt ] [ delete-existing ] | http
 { host | url } }
      end
```

Sxa Tunnel Retained till DSR on SAEGW—CSCwe80030

Revision History

Revision Details	Release
First introduced.	21.28.m14 21.28.6 21.28.m10 21.25.17

Feature Changes

During X2/S1 handover with S-GW relocation, support is added to retain the Sxa tunnel endpoints of source SGW-U. This tunnel retention enables uplink data to flow over SGW-U until the path switches. The new CLI command **sxa-tunnel-del-at-dsr-on-sgw-change** helps SAEGW/PGW-C to retain the Sxa tunnel of source SGW-U until a Delete Session Request (DSR) is sent from MME.

Previous Behavior: During X2/S1-based handover with S-GW relocation, the SAEGW/PGW-C sent Sx Session Modification Request to SAEGW/PGW-U to remove traffic endpoints of source S-GW (Sxa). Due to this, Sxa traffic endpoints were deleted.

New Behavior: During X2/S1-based handover with S-GW relocation, when you configure the **sxa-tunnel-del-at-dsr-on-sgw-change** CLI, it helps the SAEGW/PGW-U to retain Sxa traffic endpoints of source S-GW until DSR is received.

Customer Impact: Data passed over source SGW-U during X2/S1 based handover will have GTP-U error indication.

Command Changes

To enable or disable Sxa tunnel deletion, use the following configuration:

```
configure
  context context_name
    saegw-service service_name
      [ no ] sxa-tunnel-del-at-dsr-on-sgw-change
      end
```

NOTES:

- **sxa-tunnel-del-at-dsr-on-sgw-change**: Enable Sxa tunnel deletion at DSR during X2/S1-based handover with S-GW relocation.

- **no sxa-tunnel-del-at-dsr-on-sgw-change**: Disable Sxa tunnel deletion at DSR during X2/S1-based handover with S-GW relocation.
- By default, the configuration is disabled.
- The configuration is applied to all current and new sessions.

TCP Hardening between RCM and UPF—CSCwc25287

Revision History

Table 3: Revision History

Revision Details	Release
First introduced.	21.28.m14

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*.

TEID Collision Handling during MOCN

Revision History

Revision Details	Release
First introduced.	21.28.m7

Feature Description

Tunnel Endpoint Identifier (TEID) collisions support the Multiple Operator Core Network (MOCN) scenario on CUPS. During TEID collision, P-GW or GGSN allocates a TEID to a home subscriber. In case of a stale session, in an S-GW or SGSN, the same TEID that is allocated by P-GW or GGSN, is allocated to a roaming subscriber.

To eliminate this scenario, CUPS supports TEID Collision with User Location Information (ULI) change to reject a request by configuring P-GW and GGSN when TEID collision occurs. This feature allows comparison only with Mobile Country Code (MCC) instead of comparison with MCC and Mobile Network Code (MNC). This feature supports the MOCN scenario on GGSN, P-GW, and SAEGW.

For more information, refer to the *TEID Collision Handling during MOCN* chapter in the *Ultra Packet Core CUPS Control Plane Administration Guide*.

Updated TCP Heartbeat Timestamps—CSCwe60240

Revision History

Revision Details	Release
First introduced.	21.28.m14

Behavior Change

The output of the **rcm show-statistics checkpointmgr-endpointstats** RCM Ops Center CLI command related to the TCP heartbeat feature is updated in this release.

Previous Behavior: If TCP heartbeat was disabled, the "Lasthbrcvd" and "Lasthbsend" fields printed junk values of the last sent and last received timestamps.

New Behavior: The "Lasthbsend" field is printed only when TCP heartbeat is enabled on RCM.

Customer Impact: When the TCP heartbeat feature is enabled, the output of the **rcm show-statistics checkpointmgr-endpointstats** CLI command is updated with the correct timestamp.

URR Volume Quota Calculation—CSCwd61752

Revision History

Revision Details	Release
First introduced.	21.28.m7 21.26.h5

Behavior Change

Previous Behavior: UPF recalculated the URR volume quota values as per the usage after UP recovery.

New Behavior: The volume quota values provided by OCS must be the same after UP recovery.

Warning Message for Traffic Data Checking Options on CP—CSCwe61210

Revision History

Revision Details	Release
First introduced.	21.28.m10

Feature Changes

Previous Behavior: The **show subscribers [tx-data | rx-data | idle-time]** and **clear subscribers [tx-data | rx-data | idle-time]** CLI commands were executed on both user plane and control plane.

New Behavior: The **show subscribers [tx-data | rx-data | idle-time]** and **clear subscribers [tx-data | rx-data | idle-time]** commands are specific to user plane. If these commands are executed on control plane, they will not be processed and CP displays a warning message.

The following is a sample warning message that displays when you configure the **show subscribers rx-data** or **clear subscribers rx-data** command:

Warning: rx-data option not relevant on CUPS-CP platform. Please use this option on the UP side

UCS C220 M6 Server Support for VPC-DI CP

Revision History

Table 4: Revision History

Revision Details	Release
First introduced.	21.28.mh14

Feature Description

The VPC-DI Control Plane supports Cisco UCS C220 M6 server on the RHOSP.

For more information about the Hardware and Software configurations, refer the *VPC-DI System Administration Guide*.