UPC CUPS Release Change Reference, Release 21.26

First Published: 2021-12-24

Last Modified: 2023-02-07

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 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, on page vii

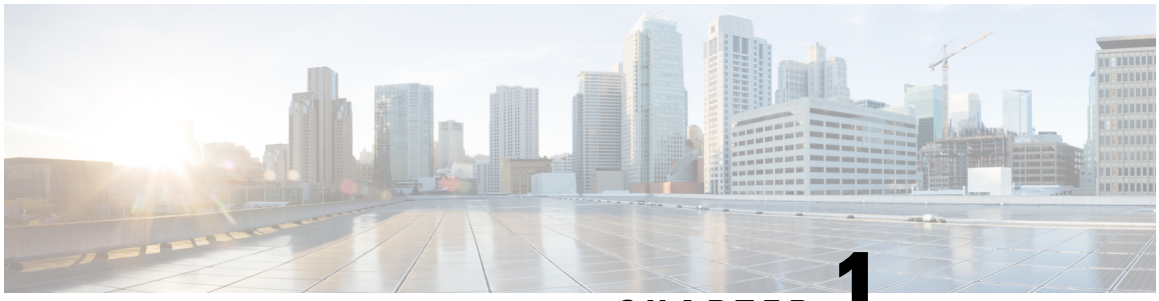
Conventions Used

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.

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

Backward Compatibility

Revision History

Revision Details	Release
First introduced.	21.26

Feature Description

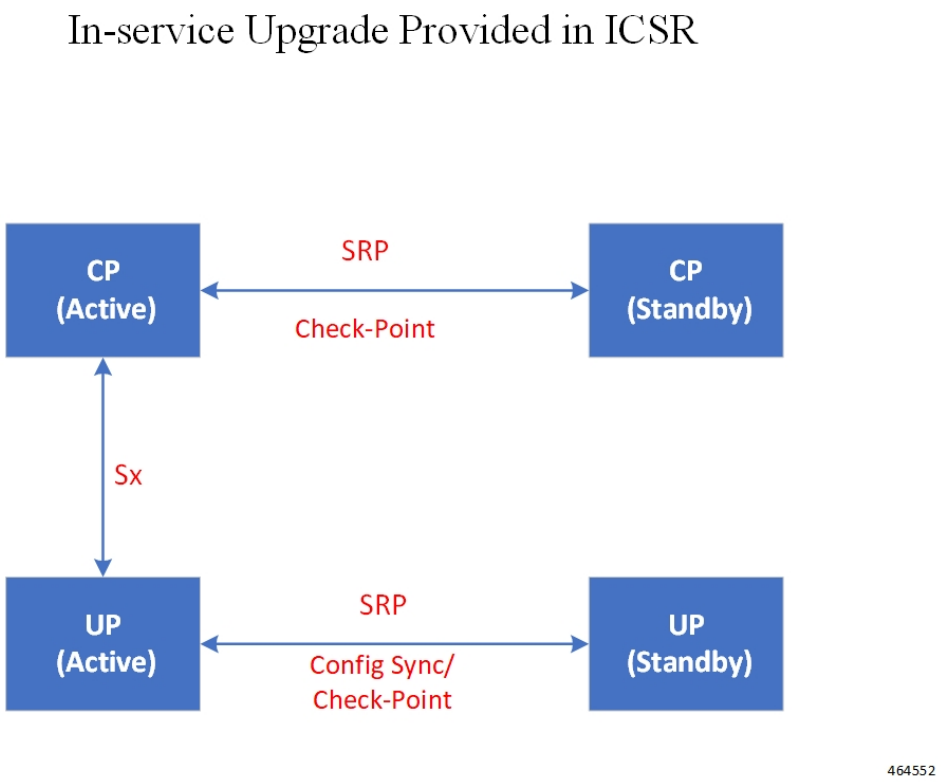
Note This is a customer-specific feature. For details, contact your Cisco Account representative.

This feature enables the customer's requirement to support online (in-service) upgrade from 21.20 to 21.26 release.

How it Works

CP and UP communication in CUPS take place over Sx interface. The 1:1 redundancy is provisioned through ICSR environment with CPs and UPs sharing configuration through SRP interface. In-service upgrade is available in ICSR 1:1 environment as shown in the image below.

Figure 1: In-service Upgrade Provided in ICSR



Compatibility

The compatibility between 21.20 and 21.26 releases can be verified under the following scenarios.

Upgrade in ICSR environment:

- CP or UP with 21.20 version
- Upgrade standby CP with 21.26 version

- CP switch over
- Upgrade standby UP with 21.26 version
- UP switch over
- Upgrade both standby CP and standby UP to 21.26 version
- Configure new features

Operation	CP1	CP2	UP1	UP2
Initial state	21.20	21.20	21.20	21.20
Upgrade Standby CP (CP2)	21.20	21.26	21.20	21.20
CP Switchover	21.20	21.26	21.20	21.20
Upgrade Standby CP (CP1)	21.26	21.26	21.20	21.20
Upgrade Standby UP (UP2)	21.26	21.26	21.20	21.26
UP Switchover	21.26	21.26	21.20	21.26
Upgrade Standby UP (UP1)	21.26	21.26	21.26	21.26
Final state	21.26	21.26	21.26	21.26

Downgrade in ICSR environment:

- CP or UP with 21.26 version
- Restore 21.20 configuration on both CP and UP
- Downgrade standby CP to 21.20 version
- CP switch over
- Downgrade standby UP to 21.20 version
- UP switch over
- Downgrade both standby CP and standby UP to 21.20 version

Operation	CP1	CP2	UP1	UP2
Initial state	21.26	21.26	21.26	21.26
Downgrade Standby CP (CP2)	21.26	21.20	21.26	21.26
CP Switchover	21.26	21.20	21.26	21.26
Downgrade Standby CP (CP1)	21.20	21.20	21.26	21.26

Operation	CP1	CP2	UP1	UP2
Downgrade Standby UP (UP2)	21.20	21.20	21.26	21.20
UP Switchover	21.20	21.20	21.26	21.20
Downgrade Standby UP (UP1)	21.20	21.20	21.20	21.20
Final State	21.20	21.20	21.20	21.20

Limitations

Following are the known limitations and restrictions of this feature:

- Generic compatibility of 21.20 with 21.26 or higher, is not considered. Compatibility is validated against the customer features existing in the given configuration.
- The SNMP trap numbered 1434 (**SRPPeerUnsupportedVersion**) which is displayed in the history of the trap is ignored.
- In-service upgrade with RCM is not considered.
- In-service downgrade with RCM is not considered.
- ICSR with MultiSx is not considered.
- Configuration is not changed till upgrade is successful and stable.
- During the downgrade process, ensure to remove or disable the new configuration added to 21.26.
- This activity validates the upgrade from the customer's existing release (21.20) to the current latest N-x compliant release (21.26) along with resolving issues. Once the candidate release is identified, this test is repeated with candidate release before attempting another upgrade from the customer site.

Bias-free Terminologies

Revision History

Revision Details	Release
First introduced.	21.26

Feature Description

Our product and documentation set 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.

With this release, biased terms present in CLI commands, messages and logs are being replaced with bias-free terms. The transition to bias-free terminology used in CLI commands is backward compatible for two releases (N-2).

The following table provides the list of CLI commands that have been updated to replace the biased terms.

CLI Commands in Releases Prior to 21.26	CLI Commands in 21.26 and Later Releases
clear blacklisted-gtpu-bind-address	**clear blockedlisted-gtpu-bind-address**
clear mme-service sgw-blacklist	**clear mme-service sgw-blockedlist**
clear mme-service sgw-blacklist sgw-ip	**clear mme-service sgw-blockedlist sgw-ip**
clear mme-service sgw-blacklist mme-service-name	**clear mme-service sgw-blockedlist mme-service-name**
clear user-plane-service url-blacklisting	**clear user-plane-service url-blockedlisting**.
clear user-plane-service url-blacklisting statistics	**clear user-plane-service url-blockedlisting statistics**.
crypto blacklist file	**crypto blockedlist file**
crypto blacklist file update	**crypto blockedlist file update**
crypto whitelist	**crypto permitlist**
default url-blacklisting	**default url-blockedlisting**
default url-blacklisting action	**default url-blockedlisting action**
diameter msg-type ccrt suppress-blacklist-reporting	**diameter msg-type ccrt suppress-blockedlist-reporting**
diameter reauth-blockedlisted-content	**diameter reauth-blockedlisted-content**
flow end-condition timeout url-blacklisting	**flow end-condition timeout url-blockedlisting**
link-aggregation master group	**link-aggregation primary group**
require diameter-proxy master-slave	**require diameter-proxy primary-secondary**
sgw-blacklist	**sgw-blockedlist**
sgw-blacklist timeout	**sgw-blockedlist timeout**
sgw-blacklist timeout 8 msg-timeouts-per-min	**sgw-blockedlist timeout 8 msg-timeouts-per-min**
show active-charging url-blacklisting	**show active-charging url-blockedlisting**
show crypto blacklist	**show crypto blockedlist**
show crypto whitelist	**show crypto permitlist**
show crypto whitelist file	**show crypto permitlist file**
show mme-service sgw-blacklist	**show mme-service sgw-blockedlist**

CLI Commands in Releases Prior to 21.26	CLI Commands in 21.26 and Later Releases
show user-plane-service inline-services url-blacklisting statistics	**show user-plane-service inline-services url-blockedlisting statistics**
snmp trap suppress BlackListingDBFail	**snmp trap suppress BlockedListingDBFail**
snmp trap suppress BlacklistingDBFailClear	**snmp trap suppress BlockedlistingDBFailClear**
snmp trap suppress BlackListingDBUpgradeFail	**snmp trap suppress BlockedListingDBUpgradeFail**
snmp trap suppress BlacklistingDBUpgradeFailClear	**snmp trap suppress BlockedlistingDBUpgradeFailClear**
url-blacklisting	**url-blockedlisting**
url-blacklisting action	**url-blockedlisting action**
url-blacklisting action discard content-id	**url-blockedlisting action discard content-id**
url-blacklisting match-method	**url-blockedlisting match-method**
whitelist	**permitlist**

The help string of the following CLI commands has been updated to replace the biased terms:

- **act-mmgr-inst**
- **diameter enable-quota-retry**
- **diameter enable-quota-retry end-user-service-denied**
- **ispc link A**
- **sgsn op enable ccpu debug_log facility mmgr**
- **sgsn retry-unavailable-ggsn**
- **sgsn test mmgr**
- **show ssi ccpu debug_log facility**
- **system packet-dump di-net card 3 bond a/b**
- **uidh-insertion server-name svc bypass wl-lookup**

Design of RCM HA Switchover on Mass UP Failure

Revision History

Table 1: Revision History

Revision Details	Release
The behavior change was introduced in Release 21.26.1 and now applicable to this release.	21.25.9
First introduced.	21.26.1

Feature Changes

RCM HA switchover on mass UP failure is now supported in 5G-UPF.

Previous Behavior: RCM HA switchover occurs instantly when all UPs go down.

New Behavior: RCM HA switchover occurs after three minutes when all UPs go down.

Customer Impact: Reloading all UPs will not trigger RCM HA switchover in the usual RCM operation as the operator intentionally reloads all UPs.

Note Undetected network isolation is not likely in this case as L2 VRRP protocol will cover any such network isolation case.

DNS Readdress Server List

Revision History

Revision Details	Release
Support for DNS Readdress Server List has been added with release 21.26 as well.	21.26
First introduced.	21.25.4

Feature Description

Whenever you use an unauthorized DNS server, the request is modified to readdress the DNS IPs to use the authorized servers. **Ruledef** determines if a packet belongs to a DNS query and if the DNS query belongs to

a set of authorized DNS servers or not. If the DNS query does not belong to the authorized DNS servers, the flow action is to pick up DNS servers from the **readdress-server-list**.

A **readdress-server-list** is configured under the active charging server. When the flow matches a **ruledef**, the flow action can be configured to use the servers from the **readdress-server-list**.

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

Endpoint Configuration under Instance ID in RCM

Revision History

Revision Details	Release
The behavior change is introduced in 21.26 and later releases.	21.26.5
First introduced.	21.23.20

Feature Changes

Previous Behavior: Endpoints were not configured under instance-id. For example:

```
endpoint rcm-snmp-trapper
exit
endpoint rcm-chkptmgr
  replicas 2
  vip-ip 209.165.200.225
exit
endpoint rcm-keepalived
exit
endpoint rcm-configmgr
exit
endpoint rcm-bfdmgr
  vip-ip 209.165.200.225
exit
endpoint rcm-controller
  vip-ip 209.165.200.225
exit
exit
```

New Behavior: Endpoints must be defined and configured under instance-id. For example:

```
instances instance 1
cluster-id Local
slice-name 1
exit
local-instance instance 1

instance instance-id 1
  endpoint rcm-snmp-trapper
  exit
  endpoint rcm-chkptmgr
    replicas 2
    vip-ip 209.165.200.225
  exit
```

```
  endpoint rcm-keepalived
  exit
  endpoint rcm-configmgr
  exit
  endpoint rcm-bfdmgr
    vip-ip 209.165.200.225
  exit
  endpoint rcm-controller
    vip-ip 209.165.200.225
  exit
exit
```

Customer Impact: The new CLIs are required in the configuration.

GTPC Peer Record and Statistic Optimization

Revision History

Revision Details	Release
First introduced.	21.26

Feature Description

When the Gateway receives the first GTPC message from a peer, the new peer record entry is added to the Session Manager and Demux. This new peer record entry is also propagated to all Session Managers. This process occurs even if a particular GTPC peer does not have any active sessions. This causes accumulation of inactive peer records objects, which results in excess memory usage of the Session Manager and Demux, thereby causing memory overrun of affected proclets. To address this limitation, a new keyword, **peer-salvation** has been added to the existing **gtpc** CLI in the Context Configuration mode.

For more information, refer to the *GTPC Peer Record and Statistic Optimization* chapter in the *Ultra Packet Core CUPS Control Plane Administration Guide* or the *Ultra Packet Core CUPS User Plane Administration Guide*.

Ignore SSH IP Installation in UP

Revision History

Revision Details	Release
First introduced.	21.26.7

Feature Changes

Previous Behavior: In releases prior to 21.26, there was no CLI to ignore the SSH IP installation in UP.

New Behavior: In 21.26.7 and later releases, a CLI command is introduced to ignore the SSH IP installation in UP. The new CLI command, **ignore-ssh-ip**, must be configured in the RCM context in UP to discard the SSH IP message from the RCM. However, if the new CLI is not configured, then the SSH IP configuration proceeds in the usual way.

Customer Impact: Using the new CLI command, we can avoid configuring a dummy SSH IP (one unique non-routable IP for each Standby) on UP. For 4G CUPS, which do not use SSH IP, you must use the CLI command dummy SSH IP provided to UP.

Command Changes

Use the configuration given below to ignore the SSH IP installation in UP:

```
configure
   context context_name
      redundancy-configuration-module module_name
         ignore-ssh-ip
         end
```

Note By default, when this CLI is not configured, the NSO SSH IP is configured on UP as usual.

Intel Ice Lake Support for VPC-SI

Revision History

Revision Details	Release
First introduced.	21.26

Feature Description

With this release, support is added for Intel Ice Lake CPU with Intel E810 for VPC-SI platform.

Kernel Upgrade

Revision History

Revision Details	Release
First introduced.	21.26

Feature Description

With this release, the kernel is upgraded to version 5.4 for VPC-SI platform. The kernel upgrade provides enhanced security, performance, debugging and serviceability, and also allows VPC-SI to run in public cloud environments.

Last User Location Information Tag in Custom24 CDR Dictionary

Revision History

Revision Details	Release
Support for "Last User Location Information Tag in Custom24 CDR Dictionary" feature has been added in release 21.26 as well.	21.26
First introduced. **Note** This is a customer-specific feature. For details, contact your Cisco Account representative.	21.23.14

Feature Description

Note This is a customer-specific feature. For details, contact your Cisco Account representative.

P-GW CDR does not contain the tag **lastUserLocationInformation** in last P-GW CDR when a session is cleared. **lastUserLocationInformation** generally contains latest ULI received for the subscriber.

This feature adds the **lastUserLocationInformation** field in P-GW CDR in last CDR when call is cleared for custom24 dictionary. A new command, **gtpp attribute last-uli**, is introduced to control **lastUserLocationInformation** in P-GW CDR, irrespective of whether **gtpp attribute uli** is enabled or not.

For more information about **lastUserLocationInformation** field, refer to *3GPP TS 32.298*.

Configuring Last ULI

The CDR field for lastUserLocationInformation is controlled by the **gtpp attribute last-uli** CLI command.

Use the following configuration to customize Last ULI:

```
configure
  context  context_name
    gtpp group gtpp_group_name
       [ no | default ] gtpp attribute last-uli
       end
```

NOTES:

- **last-uli**: By specifying this option the last ULI field is included in CDR.

- **gtpp**: Configures GTPP related parameters for specific context.
- **[no | default]**: Both the options disable the feature. That is, last ULI field is not added to CDR.

Verifying the Last User Location Information in Configuration

Use the **show gtpp group name default** CLI command to verify the Last User Location Information in ULI configuration:

- Last User Location Information present: Yes

Lawful Intercept in CUPS

Revision History

Revision Details	Release
Support has been added for Multiple LI Mediation Systems feature in release 21.26 as well.	21.26
With this release, support is added for Multiple LI Mediation Systems.	21.25.3
First introduced.	Pre 21.24

Feature Description

This feature supports multiple LI Mediation Systems. The Lawful Intercept in CUPS supports configuration of multiple LI servers. However existing design does not allow sending event or content information to multiple servers during same active session. This feature allows to configure two LI servers information for both event and content delivery, which makes it possible for two agencies to provision a single subscriber for interception.

For more information, refer to the *Lawful Intercept in CUPS* chapter in the *Ultra Packet Core CUPS LI Guide*

Multiple Control Plane Support on User Plane

Revision History

Note Revision history details are not provided for features introduced before release 21.24.

Revision Details	Release
With this release, the feature is enhanced to support connection of upto eight CPs with a single UP.	21.26

Revision Details	Release
With this release, the feature is enhanced to support connection of upto five CPs with a single UP.	21.25
First introduced.	Pre 21.24

Feature Description

When Multiple CPs are connected to single UP, it allows a subscriber to connect to UP using any of the available CP. One of the primary use case of Multiple Sx feature is Active-Active redundancy. Even though it does not offer redundancy, as the calls are not recovered, multiple Sx allows the UPs connected to one CP to be still accessible in case of a CP failure. If a CP fails, the calls serviced by that CP are lost. When they re-attach, the calls are routed to other available CPs which reuses the same UP pool.

For more information, refer to the *Multiple Control Plane Support on User Plane* chapter in the *Ultra Packet Core CUPS Control Plane Administration Guide* or the *Ultra Packet Core CUPS User Plane Administration Guide*.

Multiple LI and MIN-X Support

Revision History

Revision Details	Release
With this release, support has been added for multiple LI and MIN-X. **Note** This feature is not fully qualified in this release. For more information, contact your Cisco Account representative.	21.26

Feature Description

The feature enables support for configuring more than eight TCP-LI X3 connections in UP. You will now be able to allocate more than eight cores to VPP by specifying the minimum (Min) value as one for a shared TCP-LI connection on a single thread and upto the number of VPP worker threads available. Min X (all-worker) allows the session traffic on any thread to be intercepted from the same worker thread using TCP, ensuring maximum performance for the LI traffic. By allowing more than eight TCP-LI connections on the gateway, the earlier restriction of allowing only upto eight cores is removed.

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

No udp-checksum Support

Revision History

Revision Details	Release
First introduced.	21.26

Feature Description

This feature supports **no udp-checksum** CLI command for CUPS under GTPU service where **udp-checksum** is disabled in the outer GTPU header for the downlink subscriber packet. When downlink packet arrives from internet, the GTPU header is added on top of the packet and is sent to the access side. The "checksum" value is zero in the outer UDP layer of this packet enabling optimization and therefore, improving the performance throughput.

For more details, see *Overview* chapter in the *Ultra Packet Core CUPS Control Plane Administration Guide* or the *Ultra Packet Core CUPS User Plane Administration Guide*.

Planned Switchover Timers on RCM

Revision History

Revision Details	Release
First introduced.	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

Planned Switchover Timers on UPF

Revision History

Revision Details	Release
First introduced.	21.26.17

Feature Changes

UPF supports the following switchover timers that can be configured through CLI:

- Timer for planned switchover completion on new Active (Standby) UPF
- Timer for receipt of Standby state from the start of pending Standby state on old Active UPF

Command Changes

Use the following configuration to configure the switchover timers on UPF:

```
configure
  context context_name
    redundancy-configuration-module rcm_name
      [ default ] planned-standby-timeout planned_timeout
      [ default ] pending-standby-timeout pending_timeout
      exit
    exit
```

NOTES:

- **planned-standby-timeout** *planned_timeout*: Specify the timeout for planned switchover completion, in seconds. *planned_timeout* must be an integer from 300 to 3600.
- **pending-standby-timeout** *pending_timeout*: Specify the timeout for pending Standby state. *planned_timeout* must be an integer from 300 to 3600.

Preventing Multiple Configuration Push Notifications

Revision History

Table 2: Revision History

Revision Details	Release
First introduced.	21.26.4

Feature Changes

Previous Behavior: On TCP reconnection between UPF and RCM Controller, the UPF sends configuration-push complete notification. If the configuration-push is notified as "false" from the UPF, RCM sends configuration-push re-notification toward NSO.

New Behavior: In 21.26.4 and later releases, you can prevent multiple configuration-push notifications toward NSO by configuring the following CLI command in RCM ops-center:

```
k8 smf profile rcm-config-ep disable-repeat-config-push { true | false }
```

By default, the CLI command is set to **false**.

Customer Impact: There is no impact if the CLI is not used. Default behavior is the same as existing behavior.

RADIUS Packet Disconnect

Revision History

Revision Details	Release
First introduced.	21.26

Feature Description

The RADIUS change of authorization provides a mechanism to change authorization dynamically after the device is authenticated. Once there is a policy change, you can send RADIUS CoA packets from the authorization server to reinitiate authentication and apply the new policy. The RADIUS CoA process allows you to change the user access immediately when needed, without the need to wait for the wired switch or access point to initiate a re-authentication process, or for the device to disconnect and re-connect again.

It is now possible to define more than one radius Change of Authorization (CoA) NAS IP address per context in a context with multiple APNs using different RADIUS servers and different NAS IP addresses.

For more details, refer to the *RADIUS Packet Disconnect* chapter in the *Ultra Packet Core CUPS Control Plane Administration Guide*.

Redesigning Configuration Manager to Support Large Common Configurations

Revision History

Revision Details	Release
First introduced	21.26

Feature Description

When the common configuration for a redundancy group exceeds 80K lines, the configuration map that is created in the RCM exceeds 1 MB, which is the defined hard limit for the combined size of all the configuration maps created out of a single repository. When the RCM supports more than one redundancy group also, you must extend this hard limit as it turns out to be a very crucial limit. This feature extends the existing hard limit to support large common configurations.

The following CLIs are added for CLI notification support in Ops-center.

[no] k8 smf profile rcm-config-ep commo-config redundancy-group *group-id* **file** *file-name*

k8 smf profile rcm-config-ep common-config update redundancy-group *group-id*

For more details, see *RCM Configuration and Administration Guide*.

Secondary RAT Usage Report in CDR Records

Revision History

Revision Details	Release
Support for "Secondary RAT Usage Report in CDR Records" feature has been added in release 21.26 as well.	21.26
First introduced.	21.23.14

Feature Description

Reporting issues pertaining to 5G **RANSecondaryRATUsageReport** occur due to lack of:

- Control in identifying whether the **RANSecondaryRATUsageReport** must be processed in CDRs or not. This allows the S-GW, P-GW, and SAEGW to either include these reports in the SGW-CDR or PGW- CDR or to simply ignore them.
- Number of available reports inside a CDR, if the control is active.
- Control in identifying whether Zero-volume reports must make it inside the CDR or not.

This results in billing loss of data. To overcome these reporting issues, you can trigger CLI controls using GTPP group configuration to:

- Allow the S-GW, P-GW, and SAEGW to either include the RANSecondary RAT Usage reports in the SGW-CDR or PGW-CDR or to simply ignore them.
- Identify the number of secondary RAT usage reports available inside the SGW-CDR or the PGW- CDR.

Note This limit must be in accordance with the system capability and ensure to consider the File-Format of the CDRs. If the configured limit exceeds, the system closes the SGW-CDR or PGW-CDR with the appropriate change-condition. For example, **max-change-condition** CDR is reused for further reports.

- Add or ignore Zero-volume reports inside the CDR.
- The CLI **gtpp limit-secondary-rat-usage** or hardcoded limit will be removed and the CLI **gtpp limit-secondary-rat-usage** is reused to control the number of records within the range 1-100.
- Provides logging when the CDR size reaches the maximum size. Through PGW-CDR counter, you can monitor the number of occurrences when the CDR exceeds its size limit.

For more details, see *Secondary RAT Usage Report in CDR Records* chapter in the *Ultra Packet Core CUPS Control Plane Administration Guide* or the *Ultra Packet Core CUPS User Plane Administration Guide*.

Software Management Operations

Revision History

Note Revision history details are not provided for features introduced before release 21.24.

Revision Details	Release
Support is extended for N-4 backward compatibility of software releases.	21.26
Support is extended for N-3 backward compatibility of software releases.	21.25
Support is extended for N-2 backward compatibility of software releases.	21.24.1
First introduced.	Pre 21.24

Feature Description

CUPS supports backward compatibility of software releases on Control Plane (CP) and User Plane (UP). The feature allows seamless upgrade/downgrade of the software from/to one previous release (N-1)/two previous releases (N-2)/three previous releases (N-3)/four previous releases (N-4). The functionality includes support for the following:

- N-1/N-2/N-3 /N-4 compatibility of software releases on two CPs in ICSR mode—allows seamless upgrade of CPs from one version to another in CP 1:1 redundancy scenario.
- N-1/N-2/N-3 /N-4 compatibility of software releases on two UPs in ICSR mode—allows seamless upgrade of UPs from one version to another in UP 1:1 redundancy scenario.
- N-1/N-2/N-3/N-4 compatibility of software releases between CP and UP—allows seamless upgrade of the associated CP or UP from one version to another.
- N-1/N-2/N-3/N-4 compatibility of software releases between CP and UP with multi-Sx—allows seamless upgrade of the associated CP or UP from one version to another in multi-Sx scenario.

Important Contact your Cisco Account representative for procedural assistance prior to upgrading or downgrading your software versions.

For more information, refer to the *Ultra Packet Core CUPS User Plane Administration Guide* > *Software Management Operations* chapter.

TAC/LAC in ULI Tag in Custom24 CDR Dictionary

Revision History

Revision Details	Release
Support for "TAC/LAC in ULI Tag in Custom24 CDR Dictionary" feature has been added in release 21.26 as well.	21.26
First introduced. **Note** This is a customer-specific feature. For details, contact your Cisco Account representative.	21.23.14

Feature Description

Note This is a customer-specific feature. For details, contact your Cisco Account representative.

During service data container recording interval, the User Location Information (ULI) received contains values such as CGI/SAI, ECGI/TAI or RAI in the UE location. The ULI tag is included in the service data container, only when the previous container's change condition value is "user location change" or any one of the values among CGI/SAI, ECGI/TAI or RAI Change.

The ULI in P-GW Charging Data Record (CDR) main level contains the same location as that of UE during establishing the P-GW CDR connection. The ULI field in custom24 Gz dictionary includes TAC/LAC always in P-GW CDR, if the TAC/LAC value was received in the previous message but not in the subsequent message. However, if TAC/LAC value is received in both the previous as well as the subsequent message then there is no change required as it is expected. This feature is applicable to all the interim and final P-GW CDRs.

When a ULI IE is received, the P-GW stores the same information in P-GW CDR. During an update in ULI IE, it gets reflected in the ULI field of P-GW CDR.

However, there are instances after receiving initial ULI with TAI+ECGI, further ULI contains ECGI only. In such a case, as part of this feature, P-GW saves the latest TAC and uses the same while writing to P-GW CDR along with ECGI.

Note As LAC is not a separate element in ULI, in case of CGI or RAI or SAI, it is expected to be received always.

How it Works

User Location Information (ULI) is an extendable IE. It is coded as depicted in following image.

Bits

Octets	8	7	6	5	4	3	2	1
1	Type=86(decimal)							
2 to 3	Length=n							
4	Spare				Instance			
5	Extended Macro eNodeB ID	Macro eNodeB ID	LAI	ECGI	TAI	RAI	SAI	CGI
a to a+6	CGI							
b to b+6	SAI							
c to c+6	RAI							
d to d+4	TAI							
e to e+6	ECGI							
f to f+4	LAI							
g to g+5	Macro eNodeB ID							
h to (n+4)	Extended Macro eNode B ID							
	These octet(s) is/are present only if explicitly specified							

For more information about CGI, SAI, RAI, TAI, ECGI and LAI identity types refer *to 3GPP TS 23.003ns*.

As part of this feature TAC+ECGI values will always be present in the ULI field in P-GW CDR. Similarly for LAC, in case of CGI/RAI/SAI, the LAC value is always included in the ULI field in P-GW CDR even if it was received earlier.

Note

- The TAC/LAC in ULI in P-GW CDR is always present for custom24 Gz dictionary.
- A new CLI is introduced for control of TAC/LAC inclusion.
- Currently, the CLI **gtpp attribute uli** controls the inclusion of ULI field in P-GW CDR.

Configuring TAC Always in ULI

This **tac-always-in-uli** CLI command allows configuration to control adding TAC/LAC always..

```
configure
  context  context_name
    gtpp group gtpp_group_name
```

```
gtpp attribute tac-always-in-uli
end
```

NOTES:

- **tac-always-in-uli**: By specifying this option, TAC always is included in the ULI field in CDR.

Verifying the Last User Location Information in Configuration

Use the show **gtpp group name default** CLI command to verify the Last User Location Information in ULI configuration:

- **TAC Always present**: Yes

UP Selection based on IP Pool Chunk Availability

Revision History

Note Revision history details are not provided for features introduced before release 21.24.

Revision Details	Release
Support of UP selection based on the availability of IP pool chunks.	21.26
With this release, the VPN limitation of 100 UPs per context has been removed.	21.25
First introduced	Pre 21.24

Feature Description

Prior to 21.26 release, the CP selects an UP based on least session usage or Round-Robin algorithm. If chunks are exhausted in a selected UP, it results in rejection of Session Establishment request by the CP until new IP pools are added for the impacted APNs. This result in wastage of IP resources in an UP, which still has some chunks with free IP addresses.

In 21.26 and later releases, this feature is enhanced to allow UP selection based on the availability of IP pool chunks. When chunks are exhausted in some UPs, and if the CP receives an attach request, the CP selects randomly any UP that has IP addresses available. Also, it ignores any other UP selection algorithm that is configured.

For more information, refer to the *IP Pool Management* chapter in the *Ultra Packet Core CUPS Control Plane Administration Guide* or the *Ultra Packet Core CUPS User Plane Administration Guide*.