UPC CUPS Release Change Reference, Release 21.25

First Published: 2021-09-30

Last Modified: 2023-06-26

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.

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 standards documentation, or language that is used by a referenced third-party product.

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

CUPS KPIs

Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

The Ultra Packet Core CUPS KPI Reference document describes the Key Performance Indicators (KPIs) used for performance analysis on the UPC CUPS node. Guidelines and procedures are provided for calculating KPIs from an Operational and Planning perspective.

For more information, contact your Cisco Account representative.

Custom Dictionary Support

Revision History

Table 1: Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

With this release, support has been added for the following Custom dictionary in CUPS:

- dpca-custom24 (Gx): Custom-defined Diameter Policy Control Application (DPCA) dictionary.

Note This is a customer-specific feature. For more information about Diameter and GTPP dictionaries, see *AAA Interface Administration and Reference* and *GTPP Interface Administration and Reference guide*, or contact your Cisco Account representative.

Deferring SSH IP Installation

Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

After UP is up, the Day-0.5 configuration is executed on UP. When UPs register with RCM, the Controller pushes the hostID and SSH IP to UP along with the state. The SSH IP received may get configured and saved as a part of Day-0.5 configuration. To avoid that, we must defer the SSH IP installation until the Day-0.5 configuration is saved.

The Deferring SSH IP Installation functionality is CLI-controlled.

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

Design of RCM HA Switchover on Mass UP Failure

Revision History

Table 2: Revision History

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

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.

Device ID in EDNS0 Records

Revision History

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

Revision Details	Release
The feature is available in 21.25 and later releases.	21.25
First introduced.	Pre 21.24

Feature Description

The Device ID in EDNS0 offers each enterprise with a customized domain blocking through Umbrella. To enable this functionality:

- The UP must reformat a subscriber DNS request into an EDNS0 request, and
- The UP must include an Umbrella "Device ID" in the EDNS0 packet so that the Umbrella DNS resolver can use the Device ID to apply the domain filter associated/configured with the Device ID in the EDNS0 packet.

Presently, the Control Plane (CP) receives the domain filtering policy ID from PCRF/PCF. The CP passes the domain filtering policy ID to the User Plane (UP) in the Subscriber Parameters. The UP uses the domain filtering policy ID to apply domain filtering functionality to the subscriber.

For more details, see the *Device ID in EDNS0* Records chapter in the *Ultra Packet Core CUPS Conrol Plane Administration Guide* or the *Ultra Packet Core CUPS User Plane Administration Guide*.

DNS Readdress Server List

Revision History

Revision Details	Release
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*.

DSCP Marking of ESP Packets

Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

Applications such as SRP, SX, RCM, LI, and TACACS operate between nodes that are deployed across different networks. All these applications require quick turnaround while communicating with remote systems. Marking of Encapsulating Security Payload (ESP) packets with a Quality of Service (QoS) such as Differentiated Services Code Point (DSCP) helps to determine the traffic classification for these types of packets. This feature enables prioritization of IPsec packets within their IP core network, and improves scalability of interfaces such as Sx, and SRP using IPsec.

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

Event Data Records in CUPS

Revision History

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

Revision Details	Release
The feature is available in 21.25 and later releases.	21.25
First introduced.	Pre 21.24

Feature Description

ECS supports generation of Interim EDRs – EDRs that are generated for ongoing flows based on a configurable timer.

Usually, EDRs are generated for flows only when the flow terminates or when the flow reaches the configured flow idle-timeout value. These flows could have time duration that is as long as 48 hours, which makes it difficult to track subscriber activity until an EDR is generated.

Thus, with interim EDRs, ongoing flow activities are tracked by configuring an interim timeout value for a flow. On expiration of the interim timer, an EDR is generated.

For configuring an interim EDR, a new CLI keyword, **interim**, is introduced. Based on the configuration, the interim timer is applied to newly created flows. On expiration of the timer, an interim EDR is generated along with the following reason: **sn-closure-reason (23)**. The information volume available until the expiration of the timer is populated in the EDR along with its respective timestamps.

For more information, refer to the *Event Data Records in CUPS* chapter in the *Ultra Packet Core CUPS Control Plane Administration Guide* or the *Ultra Packet Core CUPS User Plane Administration Guide*.

GTPP Suppress-CDRs No Zero Volume

Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

This feature allows suppression of CDRs with zero byte data count, so that the OCG node is not overloaded with a flood of CDRs. The CDRs can be categorized as follows:

- Final-cdrs: These CDRs are generated at the end of a context.
- Internal-trigger-cdrs: These CDRs are generated due to internal triggers such as volume limit, time limit, tariff change, or user-generated interims through the CLI commands.
- External-trigger-cdrs: These CDRs are generated due to external triggers such as QoS Change, RAT change and so on. All triggers which are not considered as final-cdrs or internal-trigger-cdrs are considered as external-trigger-cdrs.

The customers can select the CDRs they want to suppress.

The CLI command mentioned below helps suppress CDRs on different CDR triggers supported in CUPS:

- **[default | no] gtpp suppress-cdrs zero-volume { external-trigger-cdr | final-cdr | internal-trigger-cdr }**

X-Header Insertion and X-Header Encryption

Revision History

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

Revision Details	Release
The feature is enhanced to support the following: • Allowing insertion of radius-calling-station-id in the X-Header format • Using "Certificate for Encryption" in the X-Header format.	21.25
First introduced	Pre 21.24

Feature Description

The X-Header Insertion and X-Header Encryption features, collectively known as Header Enrichment, enables to append headers to HTTP/WSP GET and POST request packets, and HTTP Response packets for use by end applications, such as mobile advertisement insertion (MSISDN, IMSI, IP address, user-customizable, and so on).

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

IFTASK Hyperthreading

Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

Hyperthreading uses the Parallel Computing technology to enhance the system performance on processing the packets.

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

IP Pool Management

Revision History

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

Revision Details	Release
With this release, the VPN limitation of 100 UPs per context has been removed.	21.25
First introduced.	Pre 21.24

Feature Description

With this release, the VPN limitation of 100 UPs per context has been removed.

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*.

Lawful Intercept in CUPS

Revision History

Revision Details	Release
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 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 UP Group Support

Revision History

Revision Details	Release
First Introduced	21.25

Feature Description

Remote CUPS allows progressive configuration rollout on an operator network. You can deploy and activate a pilot or canary version N+1 on a given CP or UPs pool, while the version N configuration is still active on the other CP or UP pool(s) until the operator decides to rollout this N+1 configuration to all the CP or UP pools after the monitoring period.

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

NSO-based Configuration Management

Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

The Cisco Network Service Orchestrator (NSO) based configuration management for 4G CUPS supports:

- Onboarding of Cisco Virtual Network Function (VNF) devices—CP, UP, and RCM.
- Centralized configuration management of 4G-based CPs, UPs, and RCMs for Day-N, Day-1, and Day-0.5 CUPS configuration push.

Managing customer configuration management for 4G CUPS deployments using NSO automation also exhibits reusability, standard notification management, and systematic device configuration governance.

For more information, refer to the *NSO-based Configuration Management* chapter in the *Ultra Packet Core CUPS Control Plane Administration Guide* or the *Ultra Packet Core CUPS User Plane Administration Guide*.

NSO Orchestration for 4G CUPS

Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

The Cisco Network Service Orchestrator (NSO) based VNF orchestration enables you to manage the lifecycle of newly created Virtual Network Function (VNF) devices such as CP, UP, and RCM.

The Cisco NSO Orchestration for 4G CUPS solution provides the following functions:

- Instantiation via NSO CLI, Web-Interface, or NSO RESTCONF API
- Onboarding of VNF devices such as CP, UP, and RCM upon successful instantiation
- Pushing of Day-0.5, and Day-1 CUPS configuration after successful instantiation
- Decommission of the VNF devices

For more information, refer to the *NSO Orchestration for 4G CUPS* chapter in the *Ultra Packet Core CUPS Control Plane Administration Guide* or the *Ultra Packet Core CUPS User Plane Administration Guide*.

RADIUS Server State

Revision History

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

Revision Details	Release
The feature is available in 21.25 and later releases.	21.25
First introduced.	Pre 21.24

Feature Description

This feature enables the RADIUS server to indicate the appropriate state regardless of the timing of keep-alive transmissions.

For more information, refer to the *RADIUS Server State* chapter in the *Ultra Packet Core CUPS Control Plane Administration Guide*.

RCM VM with dos2unix Utility

Revision History

Revision Details	Release
First introduced.	21.25.9

Feature Changes

Previous Behavior: The RCM “config_apply” script doesn’t work with non-Unix End of Line (EOL) file format.

New Behavior: The dos2unix utility provided with RCM VM must be used on all Windows format configuration file before applying it as input to “config_apply” script.

Customer Impact: You must convert non-Unix End of Line (EOL) file format to Unix End of Line (EOL) file format.

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-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). The functionality includes support for the following:

- N-1/N-2/N-3 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 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 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 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.

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

Support for NTP on Tagged Interface

Revision History

Revision Details	Release
First introduced.	21.25.9

Feature Changes

Previous Behavior: The Network Time Protocol (NTP) on tagged interface was not supported.

New Behavior: The NTP on tagged interface is supported.

Command Changes

Use the following configuration to enable NTP on tagged interface under NTP Configuration mode.

```
configure
  ntp
    vlan vlan_id
    end
```

NOTES:

- **vlan** *vlan_id*: The *vlan_id* is the VLAN where the local context interface is bound to. After configuration, the NTP daemon starts listening on the tagged interface.
- **no vlan**: Resets the NTP configuration to default and NTP daemon starts listening on the default untagged interface.

Support for regardless-of-other-triggers CLI Command

Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

This feature supports **regardless-of-other-triggers** option in CLI for CUPS. **regardless-of-other-triggers** option enables eG-CDR or P-GW-CDR generation at the fixed time interval irrespective of any other eG-CDR or P-GW-CDR triggers that may occur in between. Therefore, when you enable this option although other CDR triggers occur, the Time Limit CDR gets triggered dynamically at every *interval* in seconds, that is, the Time Threshold calculation is based on the sum of the last threshold time and the interval. This option supports session recovery and ICSR.

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

Support for show user-plane-service statistics charging-action CLI Command

Revision History

Table 3: Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

This command displays charging action statistics for all or specified charging actions that are configured in the Active Charging Service (ACS). A charging action represents actions to be taken when a configured rule is matched. Actions range from generating accounting records to dropping the IP packet, and so on. The charging action also determines the metering principle—Whether to count retransmitted packets, and which protocol field to use for billing (L3/L4/L7, and so on).

For more information, see *Monitoring and Troubleshooting User Plane in CUPS* chapter in the *Ultra Packet Core CUPS Control Plane Administration Guide* or the *Ultra Packet Core CUPS User Plane Administration Guide*

Support for show user-plane-service statistics group-of-ruledefs CLI Command

Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

This command displays statistics for all groups or a specified group of ruledefs configured in the active charging service. **group-of-ruledefs** is a collection of rule definitions that can be used in access policy creation.

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

Support for show user-plane-service statistics ruledef CLI Command

Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

This command displays statistics for all or specified **ruledef** that is configured in an active charging service. **ruledef** represents a set of matching conditions across multiple L3 - L7 protocol that is based on protocol fields and state information. You can use each **ruledef** across multiple rule bases within the active charging service.

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

Sxa Tunnel Retained till DSR on SAEGW

Revision History

Revision Details	Release
First introduced.	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.

TAC/RAC Profile for VAPN Selection

Revision History

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

Revision Details	Release
With this release, support is added for TAC/RAC profile configuration.	21.25
First introduced	Pre 21.24

Feature Description

With this feature, User Plane group can be selected based on Access Point Name (APN). The ability to configure Tracking Area Code (TAC) range, in rule combinations in virtual APN selection, helps in giving more flexible network design for location-based User Plane selection for edge computing and other services.

With 21.25 and later releases, support is added to configure TAC and Routing Area Code (RAC) profile in the Control Plane node. Using this feature, it is now possible to select APN based on discrete values of TAC/RAC profile instead of range.