



UPC CUPS Release Change Reference, Release 21.24

First Published: 2021-07-13

Last Modified: 2021-10-29

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

About this Guide	v
Conventions Used	v

CHAPTER 1

UPC CUPS Release Change Reference	1
Release 21.24.0 Feature and Behavior Changes	1
Call Summary Log	1
Revision History	1
Feature Description	2
Dedicated Bearer Establishment without PCRF	2
Revision History	2
Feature Description	2
Firewall Support in CUPS	2
Revision History	2
Feature Description	3
Lawful Intercept	3
Revision History	3
NSH Traffic Steering	3
Revision History	3
Feature Description	4
RedHat OpenStack Platform Version Update	4
Revision History	4
Feature Description	4
Redundancy Configuration Manager	4
Revision History	4
Feature Description	5
Software Management Operations	5

Revision History	5
Feature Description	5
Support for New P-GW and S-GW custom54 GTPP Dictionary	6
Revision History	6
Feature Description	6
TACACS+ Over IPSec	6
Revision History	6
Feature Description	7
User Plane Node Bring-Down Procedure	7
Revision History	7
Feature Description	7
Virtual APN in CUPS	8
Revision History	8
Feature Description	8
VRF Support for CUPS	8
Revision History	8
Feature Description	9



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 v](#)

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



CHAPTER 1

UPC CUPS Release Change Reference

- [Release 21.24.0 Feature and Behavior Changes, on page 1](#)
- [Call Summary Log, on page 1](#)
- [Dedicated Bearer Establishment without PCRF, on page 2](#)
- [Firewall Support in CUPS, on page 2](#)
- [Lawful Intercept, on page 3](#)
- [NSH Traffic Steering, on page 3](#)
- [RedHat OpenStack Platform Version Update, on page 4](#)
- [Redundancy Configuration Manager, on page 4](#)
- [Software Management Operations, on page 5](#)
- [Support for New P-GW and S-GW custom54 GTPP Dictionary, on page 6](#)
- [TACACS+ Over IPSec, on page 6](#)
- [User Plane Node Bring-Down Procedure, on page 7](#)
- [Virtual APN in CUPS, on page 8](#)
- [VRF Support for CUPS, on page 8](#)

Release 21.24.0 Feature and Behavior Changes

Call Summary Log

Revision History

Revision Details	Release
The feature is first introduced with this release in CUPS User Plane. For CUPS Control Plane, the feature was first introduced in 21.15.1. With this release, new Sx-specific information are added in S-GW and P-GW event records.	21.24

Feature Description

Call Summary Log is a mechanism using which subscriber activities like Session Creation/Deletion, Bearer Creation/Update/Deletion is reported to an external server.

For more information, refer to the *CP Call Summary Log* chapter in the *Ultra Packet Core CUPS Control Plane Administration Guide* and *UP Call Summary Log* chapter in the *Ultra Packet Core CUPS User Plane Administration Guide*.

Dedicated Bearer Establishment without PCRF

Revision History



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

Revision Details	Release
The feature is available in 21.24.1 and later releases.	21.24.1
First introduced.	Pre 21.24

Feature Description

To provide IMS services to the UE that aren't VOLTE capable, P-GW uses the deep packet inspection (DPI) functionality to create dedicated bearers without interaction with PCRF. This helps in maintaining high QoS of the voice service although the default bearer for the internet APN gets created with interaction with PCRF.

SBC IP address (IPv4 or IPv6) and protocol RTP/RTCP are configured in ruledef and a dedicated bearer is created when a subscriber traffic matches with the ruledef without interaction with PCRF to detect voice services. If no data flows, then the dedicated bearer gets removed after the configured time limit and there's no interaction with PCRF.

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

Firewall Support in CUPS

Revision History



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

Revision Details	Release
First introduced.	Pre 21.24

Feature Description

Subscriber Firewall feature on CUPS architecture allows you to configure Stateless and Stateful packet inspection and packet filtering to protect the subscribers from malicious attacks. The firewall configuration allows the system to inspect each packet of the subscriber data session. It also evaluates the security threat and applies the policies configured on uplink and downlink traffic.

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

Lawful Intercept

Revision History



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

Revision Details	Release
With this release, Lawful Intercept in CUPS supports configuration of an LI context in all the CPs with full mesh topology.	21.24
First introduced.	Pre 21.24



Note Contact your Cisco Account representative to obtain the *Ultra Packet Core CUPS Lawful Intercept Configuration Guide*

NSH Traffic Steering

Revision History



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

Revision Details	Release
NSH Traffic Steering—Sandwich Mode is available in 21.24.1 and later releases.	21.24.1
First introduced.	Pre 21.24

Feature Description

The "NSH Traffic Steering—Sandwich Mode" caters to the NSH-based Traffic Steering (TS) approach to provide the metadata needed by the service function appliance's Forwarding Engine (FE) nodes.

The Sandwich Mode solution leverages the Cisco Nexus 9000 Series NX-OS Intelligent Traffic Director (ITD) in the Cisco USP instance.

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

RedHat OpenStack Platform Version Update

Revision History

Revision Details	Release
First introduced.	21.24

Feature Description

With this release, the RedHat OpenStack Platform version 16.1 (Train) has been validated and recommended for use with CUPS deployments.

Redundancy Configuration Manager

Revision History



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

Revision Details	Release
With this release, a new CLI command is introduced to prevent successive switchovers due to Sx monitor failure.	21.24
First introduced.	Pre 21.24

Feature Description

The Redundancy Configuration Manager (RCM) is a Cisco proprietary node/network function (NF) that provides redundancy of StarOS-based UPs. The RCM provides N:M redundancy of UPs wherein “N” is number of Active UPs and is less than 10, and “M” is number of Standby UPs in the redundancy group.

For more information, refer to the Redundancy Configuration Manager Configuration and 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-2 backward compatibility of software releases. The feature is not fully-qualified in this release.	21.24
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 previous release (N-1)/(N-2). The functionality includes support for the following:

- N-1/N-2 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 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 compatibility of software releases between CP and UP—allows seamless upgrade of the associated CP or UP from one version to another.
- N-1 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 New P-GW and S-GW custom54 GTPP Dictionary

Revision History



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

Revision Details	Release
The feature is available in 21.24.1 and later releases. This is a customer-specific feature. For more information, contact your Cisco Account representative.	21.24.1
First introduced. This is a customer-specific feature. For more information, contact your Cisco Account representative.	Pre 21.24

Feature Description

With this release, the following customer-specific dictionaries are supported in CUPS:

- P-GW custom54 GTPP Dictionary.
- S-GW custom54 GTPP Dictionary.

For more information, contact your Cisco Account representative.

TACACS+ Over IPSec

Revision History



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

Revision Details	Release
The feature is available in 21.24.1 and later releases.	21.24.1
First introduced.	Pre 21.24

Feature Description

The Terminal Access Controller Access Control Server Plus (TACACS+) is a security protocol that is used for authenticating user access permissions on StarOS. To secure the authentication data that are sent over TACACS+ client and servers, CUPS VNFs support TACACS+ over IPsec for encrypting the authentication data.

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

User Plane Node Bring-Down Procedure

Revision History



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

Revision Details	Release
The feature is available in 21.24.1 and later releases.	21.24.1
First introduced.	Pre 21.24

Feature Description

The User Plane Node Bring-Down Procedure is a Maintenance Operating Procedure (MoP) that outlines the steps to bring down a specific User Plane (UP) node for maintenance operations. The purpose of this procedure is to meet the requirement to disable specific UP node on Control Plane (CP) node while node selection takes place for new incoming sessions.

This feature provides the following functionality:

- Configuration to mark a specific UP unavailable for any new session.
- Option to delete idle subscribers.

For more information, refer to the *User Plane Node Bring-Down Procedure* chapter in the *Ultra Packet Core CUPS Control Plane Administration Guide* or the *Ultra Packet Core CUPS User Plane Administration Guide*.

Virtual APN in CUPS

Revision History



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

Revision Details	Release
In this release, support is added for the following: <ul style="list-style-type: none"> • Virtual APN selection based on preference • Virtual APN selection based on location for GGSN sessions 	21.24
First introduced.	Pre 21.24

Feature Description

Access Point Name (APN) is a logical name referring to an external packet data network and/or to a specific service that the subscriber wishes to connect to.

Virtual APNs allow differentiated services within a single APN.

The Virtual APN feature allows a carrier to use a single APN to configure differentiated services. The APN that is supplied by the MME is evaluated by the P-GW along with multiple configurable parameters. Then, the P-GW selects an APN configuration that is based on the supplied APN and those configurable parameters.

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

VRF Support for CUPS

Revision History



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

Revision Details	Release
Support is added for Delayed VRF Programming as part of VPNMgr crash outage improvement for IP pool under VRF.	21.24.1

Revision Details	Release
First introduced.	Pre 21.24

Feature Description

The VRF Support for CUPS feature enables association of IP pools with virtual routing and forwarding (VRF). These IP pools are chunked like any pools. The chunks from this pool are allocated to the User Planes (UPs) that are configured to use these pools. As in the existing deployment, VRF-associated pools in CUPS can only be of type—STATIC or PRIVATE.

The chunks from the PRIVATE VRF pool are allocated when the UP comes for registration similar to the normal private pools. The chunks from the STATIC VRF pool are allocated only when calls come up for that chunk, similar to normal static pools.

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

