

RUCKUS Edge Release Notes, 2.4.0.1407

Supporting RUCKUS Edge 2.4.0.1407

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMScope DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMScope, COMMScope AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMScope HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see <https://www.commscope.com/trademarks>. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

- Document History..... 4**
- New in This Release..... 4**
 - Product Information..... 4
 - Product Support..... 4
 - New Features..... 4
- Hardware and Software Support..... 5**
 - Overview..... 5
- Known Limitations..... 5**
 - Known Limitations..... 5
- Known Issues..... 6**
 - Known Issues..... 6
- Resolved Issues..... 11**
 - Resolved Issues..... 11

Document History

Revision Number	Summary of Changes	Publication Date
A	Initial <i>Release Notes</i>	December 2025

New in This Release

The RUCKUS Edge 2.4.0.1407 release supports the following hardware and software features.

Product Information

This RUCKUS Edge 2.4.0.1407 is a patch release. This section lists each components in this release.

RUCKUS Edge Information

- RUCKUS Edge Firmware Version: 2.4.0.1407
- RUCKUS AP Firmware Version: 7.1.1.520.830 or later
- RUCKUS ICX Switch Firmware Version: 10.0.10g-cd6 or later

Product Support

This section provides information on customer service and support team details.

How Do I Get Support?

For product support information and contact details of the RUCKUS Customer Services and Support Team, go to the Support Portal <https://support.ruckuswireless.com> or <https://www.ruckuswireless.com> and select **Support**.

New Features

This section describes the new and enhanced features introduced in this release.

BUM Rate Limiting

Introduces threshold-based buffer management for L2 flooding in Bridge Domains. When fast-path buffers fall below configured limits, non-critical BUM traffic (Broadcast, Unknown-unicast, Multicast) is dropped to conserve resources.

To maintain service continuity, network-critical packets (for example, ARP, DHCP) are exempt from this rate-limiting logic, as dropping them could impact UE connectivity. Two configurable thresholds—**High** and **Critical**—govern flooding behavior:

High Threshold

- **Network-critical packets (NCP)** continue to flood.
- All other **BUM traffic** (Broadcast, Unknown-unicast, Multicast) is dropped.

Critical Threshold

- NCP behavior depends on packet source:
 - From **AP (UE side)**: Not flooded; unicasted to the uplink core sub-interface.
 - From **core port**: Dropped.
- All other BUM traffic is dropped.

This mechanism optimizes buffer utilization while preserving essential traffic flows under resource-constrained conditions.

Event Logs

When thresholds are reached, the following events are logged:

1. High Threshold exceeded
Edge <EdgeName>: Buffer high threshold limit exceeded.
2. Critical Threshold exceeded
Edge <EdgeName>: Buffer critical threshold limit exceeded.
3. Critical Threshold cleared
Edge <EdgeName>: Buffer usage has returned below the critical threshold.

Hardware and Software Support

Overview

This section provides release information about the RUCKUS Edge device.

- All configuration changes must be performed in the designated maintenance window.
- Switching the **Load Distribution** method between **Random** and **Per AP Group** in the cluster's HA settings will alter the active Edge device to which an AP connects, causing a service disruption.

Known Limitations

Known Limitations

The following table provides information on the known limitations in the current release.

TABLE 1 Feature Limitations

Feature	Limitations
Multiple Public/NAT IP address support	• NAT pool addresses must be within the same subnet as the WAN interface address for proper connectivity. - Valid: WAN: 192.0.2.1/24, NAT pool: 192.0.2.100–192.0.2.110 - Invalid: WAN: 192.0.2.1/24, NAT pool: 198.51.100.100–198.51.100.110 • In an active-backup cluster deployment, each node must be assigned a separate NAT44 public IP pool that does not overlap with the others. - Valid: Active node: 203.0.113.1–203.0.113.5, Backup node: 203.0.113.6–203.0.113.10 - Invalid: Both nodes using 203.0.113.1–203.0.113.10

TABLE 1 Feature Limitations (continued)

Feature	Limitations
Dual WAN	- In a Dual-WAN configuration, each WAN interface and its associated NAT pool must reside on separate subnets that do not overlap. - Valid: Active WAN: 192.0.2.1/24, Backup WAN: 198.51.100.1/24 - Invalid: Active WAN: 192.0.2.1/24, Backup WAN 192.0.2.2/24 - Both the WAN links must be configured to use the same IP mode, either STATIC or DHCP IP Settings.
Access Points	AP R370 does not support SD-LAN, PIN, and L2GRE services in RUCKUS Edge. Additionally, AP R370 does not support SD-LAN GPE in the initial GA release with AP firmware version 7.1.1. This limitation will be removed once the SD-LAN GPE support is introduced to the R370 AP in a future release.

Known Issues

Known Issues

The following table provides information on the known issues in the current release.

Issue	Description
ACX-87103	Summary: When RUCKUS Edge devices are deployed on the same subnet, IP conflicts can occur due to overlapping of NAT pool ranges. Symptom: The RUCKUS Edge device loses connectivity with RUCKUS One. Condition: This issue arises when two RUCKUS Edge devices with overlapping NAT pool ranges are deployed on the same subnet. This results from the current Edge architecture that uses shared IP allocation algorithm for both management and data traffic. Workaround: Starting release 2.4.0, validation for overlapping NAT pool ranges has been implemented across nodes within a cluster to mitigate this issue. However, this validation is limited to devices within the same cluster. To avoid conflicts, users must still ensure that NAT pool configurations are carefully managed across Edge devices belonging to different clusters. - Before the issue occurs: Verify that the NAT pool is correctly configured—each address in the NAT pool must fall within the subnet of the associated WAN interface. - If the issue has already occurred: - Remove any invalid NAT pool configurations from the RUCKUS One GUI. - Reset the Edge device: - For Virtual Edge: Deploy a new vEdge instance. - For E144: Press and hold the F/D button for more than 4 seconds to initiate a golden reset. - For E114: Press and hold the reset button for more than 4 seconds to perform a golden reset. - Repeat the onboarding process. - Apply a valid NAT pool configuration.

Issue	Description
ACX-87094	Summary: Incorrect NAT pool configuration may disrupt connectivity with RUCKUS One. Symptom: The Edge device may lose connectivity to RUCKUS One after the NAT pool configuration is applied. Condition: This occurs when the NAT pool is configured with IP addresses that fall outside the subnet of the WAN interface. Examples of WAN interface address: - Valid configuration: 192.0.2.1/24, NAT pool: 192.0.2.100–192.0.2.110 - Invalid configuration: 192.0.2.1/24, NAT pool: 198.51.100.100–198.51.100.110. Workaround: - Before the issue occurs: Verify that the NAT pool is correctly configured—each address in the NAT pool must fall within the subnet of the associated WAN interface. - If the issue has already occurred: - Remove any invalid NAT pool configurations from the RUCKUS One GUI. - Reset the Edge device: - For Virtual Edge: Deploy a new vEdge instance. - For E144: Press and hold the F/D button for more than 4 seconds to initiate a golden reset. - For E114: Press and hold the reset button for more than 4 seconds to perform a golden reset. - Repeat the onboarding process. - Apply a valid NAT pool configuration. Remove the Edge device from RUCKUS One, repeat the onboarding process, and apply a valid NAT pool configuration that aligns with the WAN interface subnet.

Known Issues

Known Issues

Issue	Description
ACX-92594	Summary: In a dual-WAN deployment, incorrect configuration of the WAN interface and NAT pool may disrupt connectivity with RUCKUS One. Symptom: The Edge device loses connectivity with RUCKUS One after applying WAN interface address and NAT pool configurations. Condition: This issue arises when WAN interfaces are configured with overlapping subnets and/or when NAT pools either overlap or do not align with the subnet of their respective WAN interfaces. • Valid Configuration: - Active WAN interface: 192.0.2.1/24 - NAT pool: 192.0.2.100–192.0.2.110 - Backup WAN interface: 198.51.100.1/24 - NAT pool: 198.51.100.100–198.51.100.110 • Invalid Configuration: - Active WAN interface: 192.0.2.1/24 - NAT pool: 192.0.2.100–192.0.2.110 - Backup WAN interface: 198.51.100.1/24 - NAT pool: 192.0.2.120–192.0.2.130 Workaround: • Before the issue occurs: Verify that the NAT pool is correctly configured—each address in the NAT pool must fall within the subnet of the associated WAN interface. • If the issue has already occurred: 1. Remove any invalid NAT pool configurations from the RUCKUS One GUI. 2. Reset the Edge device: - For Virtual Edge: Deploy a new vEdge instance. - For E144: Press and hold the F/D button for more than 4 seconds to initiate a golden reset. - For E114: Press and hold the reset button for more than 4 seconds to perform a golden reset. 3. Repeat the onboarding process. 4. Apply a valid NAT pool configuration. Remove the Edge device from RUCKUS One, repeat the onboarding process, and apply a valid NAT pool configuration that aligns with the WAN interface subnet.
ACX-66646	Summary: RUCKUS One packet prioritization issue. Symptom: Control packets from RUCKUS One are not being prioritized. Condition: During periods of traffic congestion, Edge configuration updates from RUCKUS One may fail, potentially causing the Edge device to disconnect from RUCKUS One. Workaround: None

Issue	Description
ACX-93366	Summary: Low Edge throughput for SDLAN + L2GRE with LAG. Symptom: Low throughput with L2GRE Traffic in Edge 2.4 release. Condition: Use the VPP CLI command show interface <port> to check for 'drops' and 'Rx-miss' counters, which help identify packet loss and receive issues on the interface. <pre> vpp# show interface port1 Name tag Idx State MTU (L3/IP4/IP6/MPLS) Counter Count port1 none 1 up 1500/0/0/0 rx packets 51198029 rx bytes 22905076574 tx packets 85621793 tx bytes 38042475164 drops 161 rx-miss 48130 vpp# show interface port2 Name tag Idx State MTU (L3/IP4/IP6/MPLS) Counter Count port2 none 2 up 1500/0/0/0 rx packets 89687180 rx bytes 40120521870 tx packets 53576669 tx bytes 24251393185 drops 169 rx-miss 100512 vpp# show interface port1 Name tag Idx State MTU (L3/IP4/IP6/MPLS) Counter Count port1 none 1 up 1500/0/0/0 rx packets 57410573 rx bytes 25684764445 tx packets 96012417 tx bytes 42659341105 drops 180 rx-miss 48130 vpp# show interface port2 Name tag Idx State MTU (L3/IP4/IP6/MPLS) Counter Count port2 none 2 up 1500/0/0/0 rx packets 100068933 rx bytes 44764919977 tx packets 59777787 tx bytes 27057706381 drops 188 rx-miss 100512 </pre> Workaround: Ensure the user is using the correct SFP module: Intel 10G SFP — Part# E10GSFPSR is required for proper operation.

Issue	Description
ACX-93356	Summary: Low Edge throughput for SDLAN + L2GRE with Core-Access Separation. Symptom: Low throughput with L2GRE Traffic in Edge 2.4 release. Condition: Use the VPP CLI command show interface <port> to check for 'drops' and 'Rx-miss' counters, which help identify packet loss and receive issues on the interface. <pre> vpp# show interface port1 Name tag Idx State MTU (L3/IP4/IP6/MPLS) Counter Count port1 none 1 up 1500/0/0/0 rx packets 51198029 rx bytes 22905076574 tx packets 85621793 tx bytes 38042475164 drops 161 rx-miss 48130 vpp# show interface port2 Name tag Idx State MTU (L3/IP4/IP6/MPLS) Counter Count port2 none 2 up 1500/0/0/0 rx packets 89687180 rx bytes 40120521870 tx packets 53576669 tx bytes 24251393185 drops 169 rx-miss 100512 vpp# show interface port1 Name tag Idx State MTU (L3/IP4/IP6/MPLS) Counter Count port1 none 1 up 1500/0/0/0 rx packets 57410573 rx bytes 25684764445 tx packets 96012417 tx bytes 42659341105 drops 180 rx-miss 48130 vpp# show interface port2 Name tag Idx State MTU (L3/IP4/IP6/MPLS) Counter Count port2 none 2 up 1500/0/0/0 rx packets 100068933 rx bytes 44764919977 tx packets 59777787 tx bytes 27057706381 drops 188 rx-miss 100512 </pre> Workaround: Ensure the user is using the correct SFP module: Intel 10G SFP — Part# E10GSFPSR is required for proper operation.
ACX-93259	Summary: AP receives only two Edge IP addresses instead of four. Symptom: On RUCKUS One, all four cluster nodes have been stable and assigned IPs on the Core port. However, APs are establishing tunnels to only two of the four nodes, resulting in uneven load distribution across the Edge devices. Condition: In existing Edge clusters where the core port is configured in DHCP IP mode and the IP addresses have not been renewed for an extended period, on enabling Core and Access Port Separation feature, APs may only recognize part of the cluster and establish tunnels to a limited number of Edges. Workaround: To ensure APs receive the full list of Edge IPs and restore balanced load distribution: • Refresh the DHCP IP address • Reboot the affected Edge device (recommended) If an Edge has a DHCP-configured access port with no AP connected, perform one of the following: • Refresh the DHCP IP address for that Edge • Reboot the Edge to trigger a fresh IP assignment and AP tunnel re-establishment

Issue	Description
ACX-85997	Summary: The Edge device disconnects from the cloud when its active port interface is disconnected. Symptom: Modifying the Edge IP configuration between DHCP and static modes can lead to cloud disconnection under certain conditions: - Valid Configuration: - Port1 with static IP address and Port2 with static IP address - Port1 with DHCP IP address and Port2 with DHCP IP address - Invalid Configuration: - Port1 with DHCP IP address and Port2 with static IP address - Port1 with static IP address and Port2 DHCP IP address Condition: RUCKUS One enforces a restriction that prevents mixing static and DHCP IP types during configuration. Workaround: Ensure both ports use the same IP assignment type.

Resolved Issues

Resolved Issues

Issue	Description
ACX-104133	Added additional safeguards in FTM to prevent crashes triggered when packets were routed to the wrong worker.

Issue	Description
ACX-104861	Updated VXLAN-GPE tunnel handling to drop packets received with version-1 RKS-shim header type 0 and a zero tunnel ID.

Issue	Description
ACX-99212	Back-ported DHCP snooping and packet forwarding.

Issue	Description
ACX-101370	Addressed <code>core.linux</code> occurrences observed on nodes in the Edge cluster.

Issue	Description
ACX-93122	Resolved a problem preventing successful upgrades from 2.4.0.1232 to 2.4.0.1289.

Issue	Description
ACX-92472	Increased buffers-per-NUMA across all platforms (E144, E114, and vEdge).

Issue	Description
ACX-104650	Resolved a problem that caused the Edge connect-agent to stall at the GETSVRIP state following an upgrade, resulting in VPP reporting no status despite successful NATS connectivity.

Resolved Issues

Resolved Issues

Issue	Description
ACX-103881	Resolved a problem causing the <code>helm-delete-configdb</code> pod to stay in Pending following a system configuration reset and subsequent reconnection to RUCKUS One.

Issue	Description
ACX-100197	Resolved a problem that caused E114 devices upgrade to report an INIT Edge status and display no servers in the Edge console CLI.

Issue	Description
ACX-97121	Enhanced runtime data collection to include automatic creation of a <code>dmesg.log</code> file.

Issue	Description
ACX-96502	Resolved a defect in which E144 units onboarded to R1 and upgraded to versions 2.3 or 2.4 failed to bring up VPP after running <code>set internal-network 10.253.0.0</code> and rebooting, resulting in VPP repeatedly re-initializing.

Issue	Description
ACX-93696	Optimized StatsD operation by minimizing IP address and route-related binAPI calls to improve performance and reduce overhead.



© 2025 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>