RELEASE NOTES

Ruckus LTE AP Release Notes SC 04.01.00

Part Number: 800-72748-001
Publication Date: June 2020

Contents

About this Release

This document provides release information for Ruckus LTE AP Release SC 04.0.1.0000 including information on new features, resolved issues, and unresolved issues.

New in this Release

List of features introduced in Ruckus LTE AP Release SC 4.0.1:

- **IPv6 - IPv6 support for Ruckus SmallCell:** Ruckus SmallCell AP when switched ON from factory partition acquires either IPv4 or IPv6 address depending upon the availablity of DHCP server in customer premise. Enterprise network/Customer premises which support IPv6 acquires v6 address from the local DHCPv6 server and the AP should be switched ON in factory partition. The following are the external entities which interacts with Ruckus SmallCell AP.
  - SCR
  - SAS
  - Security Gateway (Management Cloud and EPC)
  - PTP
  - DHCP
  - NTP
  - DMS (Supports v6 only)

  Enterprise Network/Customer premises must have these additional entities for IPv6 support to be operational for CBSD functionality. These entities are required for acquiring of v6 and translation of v6 to v4 to communicate with the v4 remote entities which does not have support for v6. IPv6 support on RSC will not be operational without the below entities.
  - NAT64
  - DNS64
  - DHCP6
- **SCTP Transport Layer Path MTU discovery:** This feature discovers SCTP layer path MTU by sending probe packets using heartbeat chunk with padded bytes after S1AP and X2 associations creation. By adjusting SCTP PMTU to this new discovered value, IP layer fragmentation is avoided when SCTP pay load is having huge size.
- **Response Code 400:** As part of grant procedure, CBSD/AP selects an available frequency channel within the CBRS band i.e 3550MHZ to 3700MHZ and sends grant request for the selected frequency channel. If SAS finds interference due to the selected frequency channel, it sends response code 400 in the grant response. When response code 400 is received by the CBSD, it can select next available frequency channel and initiate new grant request. If SAS still sees interference for the new frequency channel too, it again responds with response code 400 in the grant response. This process continues for next all available frequency channels and if response code 400 is received for all channels, CBSD keep trying new grant request to all frequency channels till it gets a successful grant response. The responseCode400 feature attempts to get a grants with reduced power i.e. MaxEIRP-x(where x=1 to 3) incase SAS responds with responseCode 400 to all available frequency channels.

  The feature functionality added includes:
  - CBSD retry GrantRequest with reduced maxEIRP value i.e. MaxEIRP-x(where x=1 to 3) for the first frequency channel for which SAS responded with 400 error code.
  - Upon 3 grant request retries i.e. MaxEIRP-x(where x=1 to 3, cbsd will fall back to the existing behavior i.e cbsd continuously scans all available frequency channels with full power.
  - For CA boards, this feature is applicable to both PCC and SCC i.e either PCC/SCC or both can be get grants with reduced power
  - In case of grant is sacrificed by the SCC having grant with reduced power or full power, cbsd retry grant request for SCC and may get reduced power grant.
  - If new operation params are provided in grant response during responseCode400 algo execution, CBSD use these new operation params and exit the new algo execution.
  - CBSD raise alarm if grant request succeeds with reduced power.

This feature is applicable to all HW types.

- **TDD Config-6 :** TDD Configuration 6 is now available on Ruckus LTE APs capable of operating in CA/NON-CA mode. Max throughput *
  - Single Cell (20 MHz)
    - Downlink 64 QAM : 66.9 Mbps
    - Downlink 256 QAM: 89.2 Mbps
    - Uplink 16 QAM : 26.64 Mbps
    - Uplink 64 QAM : 39.96 Mbps
  - Dual Cell (20+20 MHz)
    - Downlink 64 QAM : 133.8 Mbps
    - Downlink 256 QAM: 178.4 Mbps

    NOTE
    Throughput values are theoretical limit of TDD config 6 in MAC. Application throughput will be little less.

- **MOCN Configuration from Cloud:** Starting from release 4.0.1, MOCN configuration at AP is supported from Cloud. Multiple PLMN IDs can be set from the Cloud – it is now possible to change, enable or disable a PLMN ID from the Cloud.
- **CMPv2 Certificate Enrollment:** AP now supports non-secure Certificate Enrollment via the Operator CMPv2 Server[1]. CMPv2 Server details can be configured at the AP from the Cloud. Based upon the configuration, AP can download the RootCA certificate and then enroll with the Operator CMPv2 Server. Once the certificate has been generated, AP uses the same in the IKEv2 message exchanges with the Operator SecGW.

  [1] Integration with Operator CMPv2 Server shall have to be carried out.
- **Crypto Configuration for Operator SecGW from Cloud:** Starting from release 4.0.1, Crypto configuration for Operator SecGW is supported from Cloud. Cloud can be used for setting Operator specific Crypto Profile at the AP for Operator/EPC SecGW. This enables easier integration with Operator/EPC SecGWs which have a Crypto Configuration which is not default at the AP.
- **Interoperability with IPv4 only Operator/EPC SecGW:** There are certain Operator/EPC SecGWs which do not like multiple IP options proposed during the IKEv2 message exchanges. Starting release 4.1, AP has the ability to support such Operator/EPC SecGWs on the basis of configuration received from the Cloud. Cloud provides a configuration option using which the AP can be configured to change its IKEv2 proposals to IPv4 only.
- **Auto-Factory Reset on Software Upgrade:** Starting from release 4.0.1, AP has support for performing factory reset as part of Software Upgrade process. After the base build on the AP performing the upgrade is 4.0.1, any new software uprades shall have the ability to perform an auto factory reset on the basis of the instructions specified in the downloaded package.
- **Crypto Configuration Enhancements:** Starting 4.1, AP supports Operator/EPC SecGWs specific configuration using features mentioned previously. AP now supports enhanced default Crypto Configuration as mentioned below:
  - IPSec Rekeying: 8 hours (previous value: 1hr)
  - KE rekeying: 24 hours (previously disabled)

Supported Hardware

Ruckus LTE AP Release SC 4.0 supports the following Access Point models:

P01-Q910-US02
P01-Q950-US02
P01-Q910-US02
P01-Q710-US02
P01-Q410-US01

NOTE

Legacy Access Points P01-Q910-US00 and P01-Q710-US00 are also supported, but without Carrier Aggregation (CA) capabilities.

Resolved Issues

Resolved Issues	Description
AZ-4365	Crash logs are not transfering in OneShot command.
AZ-4331	DMS: TransferComplete success sent when reboot triggered during download.
AZ-4204	CTT value not resetting after channel change.
AZ-4198	SEL_IND not received as per SET_STATUS_REQ(op params sent by SAS).
AZ-4310	Incorrect Alarm is raised when AP service is disabled.
AZ-4435	UL 64 QAM is not getting enabled for UEs which does not have v1180 feature support.
AZ-4150	[SC3.0] Maximum allowed dedicatedPlmnBearerResources per dedicatedPlmnUserResources per plmn should not be greater than summation of maxNumGbrDrbsPerUe and maxNumNonGbrDrbsPerUe.
AZ-3284	Increment in CTT value doesn't happen for SCC resulting in failure of channel fly.
AZ-4349	SSM_CHANNEL_SEL_FAIL_IND after spectrumInquiryResponse
AZ-4338	PCI collision alarm raised and cleared even when actually PCI collision resolution not happened.
AZ-4342	SCC not updated in NRT when x2 connection is not present.
AZ-4200	Coredump of syncmgr, lte_son, lteOam created when AP going for graceful reboot.
AZ-4594	Alt CQI table is not being sent in rrcReconfiguration during scattered profile.
AZ-4601	Hex3 crash with 60 UE scattered profile in case of RB 1
AZ-3564	LTE-AP addition falied as AP raising wrong FQDN error for Unsecured IPv4 network configuration in Factory scenario.
AZ-3715	SCC doesn't start transmission if suspension happens & revokes when MME is unreachable.
AZ-4440	Hex2 crash with multi UE.
AZ-4585	AP moving from transmitting state to IAP pending state after Reboot.
AZ-4584	Grant request never initiated to SCC even after PCC received grant and moved to operational during reduced power algorithm.
AZ-4445	CBSD is triggering MBB at each periodic SI because the current operating channel is not present in periodic SI response.
AZ-4361	[256/64QAM] eNB is doing HARQ re transmission whenever it receives ack/nack/dtx for scell, resulting degraded MCS and low dl tput.
AZ-3957	Non-CA AP (Q710-US00) not coming functional when SI response contains 10Mhz chunks. lteOamAdaptor crashed.
AZ-4358	CellTwo related records are records are needed to be removed from from Set & Get PLMNList command.
AZ-4170	AP rebooted unexpectedly with reboot cause E_STACK_ERROR_RECOVERY.
AZ-4161	Venue Stats not showing data -ELKPI.
AZ-4287	ManagedObjectInstance filed for alarm not updated when CBSD-SAS related alarm (ID-135,138,143) raised.
AZ-4386	Antenna Open Circuit is Detected - Additional Text improvement.
AZ-4395	Dot(.) from additional text of alarm removed when alarm is sent to ACS.
AZ-4429	Hex3 crash with 60 UEs.
AZ-4760	CRC Errors in uplink. Uplink transmission get succeeded mostly after 3 non-adaptive re-transmission.
AZ-4221	LTE stack not applying DSCP mark to GBR bearers except QCI-1 for egress packets.
AZ-4297	lte_tr069 crashed while recovering from ipsec proc failure.
AZ-4690	SOMC Crash Fix.
AZ-4691	LTEOAM crash Fix.
CBRSE-168	(partial): Multiple APs seeing E_SYSTEM_CRASH (sync mgr, and TR069 crashes fixed; awaiting logs data for DM and Strongswan crashes).
CBRSE-177	AP Reboots: Reason seems to be related to lteOam or lteTR029.
CBRSE-178	AP stuck in weird state with S1 up and Authorized grants but OpState false.

Resolved Issues

Resolved Issues	Description
CBRSE-188	Not able to add secondary carrier with Cradle Point, root-caused this issue and patch available for testing : Need to verify. Cradlepoint device is now available - test set up being prepared.
CBRSE-190	E_SYSTEM_CRASH in 4.0 with somc (the fix for GPS alarm coming often shall be included ; also reviewing latest logs).
CBRSE-202	(AZ-4445/AZ-4555/AZ-4585) : AP moving from transmitting state to IAP pending state after Reboot.

Known Issues

Known Issues	Description
AZ-4794	Grant suspension alarm (Alarm id - 135)not cleared even after grant authorized.
AZ-4804	AP not sending event 918 (software download success) to ACS hence not displayed on cloud.
AZ-4876	ANR not visible when NRT list already contain 32 neighbors.
AZ-4769	False alarm for certificate expired raised when iHems FQDN resolution failed.
AZ-4834/AZ-4196	SC 4.1 SOMC memory Leak.

COMMSCOPE®
RUCKUS®

350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com