Ruckus Wireless™ P300 Wireless Bridge

Release Notes for 100.1.0.9.57 (GA Refresh 3)

Part Number 800-71645-001 Rev A
Published July 2017

www.ruckuswireless.com

Copyright Notice and Proprietary Information

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader’s responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN (“MATERIAL”) IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, ZoneFlex, FlexMaster, ZoneDirector, SmartMesh, ChannelFly, SmartCell, Dynamic PSK, and Simply Better Wireless are trademarks of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

Contents

About This Document

1

This document provides release information on Ruckus Wireless P300 802.11ac Point-to-Point Outdoor Wireless Bridge base image 100.1.0.9.57, and includes new features, enhancements, known issues, caveats, workarounds, upgrade details and interoperability information.

Note: This document only covers the Ruckus Wireless P300 Bridge only. For FlexMaster release information, please refer to the FlexMaster Release Notes.

Online Training Resources

To access a variety of online Ruckus Wireless training modules, including free introductory courses to wireless networking essentials, site surveys, and Ruckus Wireless products, visit the Ruckus Wireless Training Portal at

https://training.ruckuswireless.com

Security Fixes

Note: For a list of recent security fixes, please refer to the **Security Bulletins** section of

http://www.ruckuswireless.com/security

Release 100.1.0.9.57

2

This section lists the bug fixes, resolved issues, and any known caveats or limitations in this release (P300 Release 100.1.0.9.57) which have not been previously identified in prior releases.

Please refer to previous Release Notes documents for previously documented bugs and resolved issues.

Resolved Issues

- This release adds support for passing STP (Spanning Tree Protocol) and LACP (Link Aggregation Control Protocol) packets over P300 bridge links. [FR-2127]
- Resolved an issue that could cause P300 Non-Root Bridge to be unable to establish a link to the Root Bridge if it is able to reach a local gateway through its Ethernet port. [FR-2225]
- Resolved an issue where the remote P300 fails to establish a second link if it is able to reach a local gateway through its Ethernet port when attempting to connect a second P300 pair linking two locations. [FR-2011]
- Added a warning message informing the user that the SpeedFlex tool built into the P300 UI is unable to accurately measure the maximum throughput speed due to CPU limitations, and therefore users should use SpeedFlex to verify connectivity only, or to use an external platform to run speed testing. [FR-2706]
- Resolved an issue that could result in poor throughput performance based on SpeedFlex testing when Management VLAN and Rate Limiting were enabled. [ER-4978]
- Upgraded OpenSSL and dropbear versions to apply the latest fixes to address security vulnerabilities. [FR-2220, AP-5591]

New CLI Commands

The following new commands are available to support the new/changed features above. Both (gateway detection and loop detection) should be disabled for STP and LACP scenarios.

NOTE: *Once LACP is enabled on the switch, you will be unable to manage the AP through the web interface or SSH. Therefore, if using LACP, be sure to complete all AP configuration steps prior to enabling LACP on the switch as the final step.*

Disable Gateway Detection

Disabling Mesh gateway detection can be useful in situations where the customer wants to deploy P300s with the gateway located on the NRB side. In the original mesh implementation, if a MAP detects the gateway through its Ethernet port, it will disconnect its uplink connection. Use this command to disable the mesh gateway detection mechanism on the NRB side to support this scenario.

Example

```
Usage: set meshcfg {ssid|passphrase} "<value>"
                  use meshcfg for mesh config recovery
                  {loop_detect} <enable / disable>
                  {gw_detect} <enable / disable>
             use meshcfg to manual configure mesh related parameters
                  {ssid|passphrase} can be used as mesh link
configuration recovery
                  for manual mesh provisioning, use 'set meshprov'
rkscli: set meshcfg gw_detect enable
OK


rkscli: get meshcfg
Gateway Detection Timeout: 30
No ethernet neighbor communication Status: Disabled
Loop Detection Status: Disabled
Gateway Detection Status: Enabled
OK
```

Disable Loop Detection

Disabling loop detection features can be useful in situations where the customer wants to install an additional pair of P300 bridges for redundancy. The original Ruckus mesh loop detection mechanism will prevent Spanning Tree Protocol (STP) from working properly. Although redundancy can still be achieved, some customers prefer to rely on STP to make the decisions. To support this scenario, a new AP CLI command allows customers to disable all P300 loop detection mechanisms in both the RB and NRB.

Use the following command to disable the following features for loop detection:

- Disable mesh eBeacon
- Disable loop guard in bridge
- Disable STP filter in mesh WLAN interface

Example

```
rkscli: set meshcfg loop_detect disable
OK

rkscli: get meshcfg
Gateway Detection Timeout: 30
No ethernet neighbor communication Status: Disabled
Loop Detection Status: Disabled
Gateway Detection Status: Enabled
OK
```

350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com