

BSAP 6.6.0 Release Notes



Access Point Software Version: V6.6.0-30

BSAP Models Covered: 1800 (v1 and v2), 1840, 1920, 1925, 1930, 1935, 1940

Release Date: March 26, 2013

These Release Notes list addenda or corrections to the user documentation, new features and fixes, known issues, and other important information about this release of the Bluesocket BSAP software.

Contents

Important Notes.....	2
AP Firmware on vWLAN	2
BSAP-19XY Features Not Supported for Release 6.6.0	3
User Documentation.....	4
Wireless Regulatory Compliance	4
Version 6.6.0 BSAP Features and Improvements	5
Version 6.6.0-30 BSAP Fixes.....	6
Version 6.6.0-30 BSAP Errata.....	7

Important Notes

AP Firmware on vWLAN

As of vWLAN 2.2.x, AP firmware is not included in the vWLAN image so the latest AP firmware must be loaded in order to upgrade the APs.

BSAP Interoperability and Performance

- 802.11n wireless client interoperability is only guaranteed for Wi-Fi Alliance certified clients.
- For the highest 802.11n performance, follow these steps:
 - Use WPA2 (PSK or 802.1x) with AES when connecting 802.11n-based clients. A TKIP client will connect at a maximum transmit rate of 54 Mbps.
 - Enable 802.11n Wireless Mode, 40 MHz Channel Bandwidth (for 802.11a radio), and Packet Aggregation mode. These are configured under the 802.11 radios in the GUI in the AP template.
 - Enable 802.11n on the wireless client devices (in the hardware/firmware options).
 - For example, with the Linksys 802.11n card, use the Windows configuration interface (under Properties>Driver) and enable IBSS mode for 80211a/b/g/n/auto.
 - Ensure that all 802.11n client drivers are updated to the latest version before doing any system or performance testing.
 - It is highly recommended that WEP, WPA, and TKIP not be used, but WPA2 be used instead.
 - Running in a mixed mode environment (i.e. with legacy clients) will impact the 802.11n client's performance.
- To support multicast traffic between clients, do one of the following:
 1. On the SSID, convert multicast to unicast, and then allow the Multicast Destination IP Address (or all addresses) in the Client Role(s). This is the recommended option in an environment where only certain users should receive the multicast streams.
 2. Allow the Multicast Destination IP Address in the Unregistered Role. The drawback is that this allows it for all users, so it should only be used if all users are allowed to receive the multicast streams.

BSAP Release Notes

BSAP-19XY Features Not Supported for Release 6.6.0

BSAP-19xy APs do not support the following features for Release 6.6.0:

- Dual Mode
- Minimum Transmit Rate
- Over the Air Fairness

User Documentation

Hardware installation guides, quick start guides, and FAQs are available in the ADTRAN Support Community (<https://supportforums.adtran.com>), along with the software release notes.

Wireless Regulatory Compliance

Based on United States FCC and European DFS and ETSI regulations, ADTRAN validates the country in which the APs are being operated. This prevents the ADTRAN equipment from accidentally being used in an improper configuration.

When customers request AP licenses, they must specify the country where the AP will be deployed and operated. Note that a single vWLAN can control and manage APs in different countries and regulatory domains – and the channel and power settings are regulated by the country where the individual AP is deployed and operated.

Before the license is installed, the AP is in the root domain and not associated to any domain, so the AP's radios are disabled by default. When the licenses are uploaded, the country code is then applied to licensed BSAPs. Allowed channels and power levels are determined by the country and the platform, and once the AP is placed into a domain, the APs will scan the channels to discover neighboring APs and optimize DynamicRF™.

Version 6.6.0 BSAP Features and Improvements

- There are five new APs supported under vWLAN 2.2.1, with BSAP 6.6 software:
 - BSAP-1920 – Indoor, Internal Antenna, 2x2
 - BSAP-1925 – Indoor, External Antenna, 2x2
 - BSAP-1930 – Indoor, Internal Antenna, 3-stream
 - BSAP-1935 – Indoor, External Antenna, 3-stream
 - BSAP-1940 – Outdoor, External Antenna, 3-stream
- Added a configurable reboot timeout after the control channel is lost. This allows the APs to continue to service authenticated users, if the WAN link is lost.
- Added support for SCP firmware upgrade for the new BSAP 19XX Series APs.
- When configuring an AP firmware on an external server (TFTP for 18x0 series, or SCP for 19xy series), the vWLAN no longer needs to download the firmware from the server, allowing the external server to be at a remote office/site behind a NAT device.
- When APs are upgrading for the first time, they now appear in the UI while they are upgrading.
- When the 1800 series APs detect non-802.11 interference, instead of the AP rebooting, vWLAN notifies the administrator of severe non-802.11 interference in the UI (and, optionally, sends an external Syslog, SNMP Trap, or email). The message is “[BG or A] radio: non-802.11 interference detected - change the channel and then reboot the AP.”
- Added the ability (on a per SSID basis) to optionally convert broadcast and multicast traffic to unicast traffic to optimize RF performance for applications such as multicast video that requires higher bandwidth.
- Added regulatory domain support for China on the BSAP 1800v2 and 1840 platforms.

Version 6.6.0-30 BSAP Fixes

- After 16 or more clients have been associated on a radio, extended 802.11n fields for the secondary channel were reported improperly in the beacon in the 1800v1, 1800v2, and 1840 models . This would cause newer Broadcom clients, such as the Apple Macbook, etc to disassociate from the AP and not be able to reconnect.
- 1920, 1925, 1930, 1935, and 1940 series APs may become unresponsive.
- 1800v2 and 1840 model APs would reboot due to a condition that may occur when deleting a client encryption key.
- Multicast traffic intermittently stopped on the 1800v1, 1800v2, and 1840 models.
- Ethernet performance would decrease on the 1920
- 1800v2 and 1840 radio LED stayed on even when the radio was disabled.
- When packet aggregation was enabled on the 1800v2 and 1840 models, the AP would reboot in the presence of particular client activity.
- Miscellaneous RF analysis optimizations.

Version 6.6.0-30 BSAP Errata

- During a BSAP 19xx AP firmware upgrade, if the SCP connection is lost it will not be detected again for a period of 2 hours.

Workaround: BSAP still reports accumulated byte counts. If the byte count is not increasing according to WAN link capacity, the administrator should check the server and optionally send updated server parameters.

- During a BSAP.18xx AP firmware upgrade, if the server parameters are incorrect or the AP could not reach the server, the AP will not recover.

Workaround: The only way to recover is to reboot the AP through a PoE reset or physically cycle the power on the AP. The customer must ensure the correctness and connectivity of the external TFTP server.

- APs not setting the Tx Power sent dynamically to value sent by vWLAN in ContinuousRF mode

Workaround: The user should manually set the recommended TX power by editing power and applying it to the AP.

- Under certain circumstances a BSAP-1940 may become unresponsive and not respond to a reboot command.

Workaround: Power-cycle the AP.

- Under certain circumstances a BSAP-18xx may become unresponsive and not respond to a reboot command.

Workaround: Power-cycle the AP.

- It is not possible to log into a BSAP-1800v1 after changing the SSH password.

Workaround: Reset AP to defaults.

- If a DHCP offer contains certain options **not requested** in the DHCP discover, the Location may not be added as an active Location for the AP.

Workaround: Ensure that DHCP offer options are only those requested in the DHCP discover.

- A NAS-IP-Address or NAS-Identifier is not present in the RADIUS Access-Request packet sent by the AP.

Workaround: There are no known service-impacting field issues caused by this missing value.

- Under certain circumstances, it is possible that the BSAP-1940 will reboot while performing redirection to web authentication.

Workaround: The AP will reboot automatically and begin servicing clients and performing redirection.

Copyright and Trademark Information

Copyright © 2012, 2013 ADTRAN, Inc. All rights reserved.

No part of this document may be reproduced in any form or by any means, electronic or manual, including photocopying without the written permission of ADTRAN, Inc.

The products described in this document may be protected by one or more U.S. patents, foreign patents, or pending patents.

This document is provided *as is* without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose or non-infringement. This publication could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein; these changes will be incorporated in new editions of the document. ADTRAN, Inc. may make improvements or changes in the products or the programs described in this document at any time.

Bluesocket, The Bluesocket Logo, vWLAN, Secure Mobility, BlueView, BlueProtect and BlueSecure are trademarks or registered trademarks of ADTRAN, Inc.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions

All other trademarks, trade names and company names referenced herein are used for identification purposes only and are the property of their respective companies.