



RELEASE NOTES

BSAP 6.8.0-18
May 23, 2014

Trademarks

Any brand names and product names included in this manual are trademarks, registered trademarks, or trade names of their respective holders.

To the Holder of the Manual

The contents of this manual are current as of the date of publication. ADTRAN reserves the right to change the contents without prior notice.

In no event will ADTRAN be liable for any special, incidental, or consequential damages or for commercial losses even if ADTRAN has been advised thereof as a result of issue of this publication.

Toll Fraud Liability

Be advised that certain security risks are inherent in the use of any telecommunications or networking equipment, including but not limited to, toll fraud, Denial of Service (DoS) attacks, loss or theft of data, and the unauthorized or illegal use of said equipment. ADTRAN OFFERS NO WARRANTIES, EITHER EXPRESSED OR IMPLIED, REGARDING THE PREVENTION, DETECTION, OR DETERRENCE OF TOLL FRAUD, NETWORKING ATTACKS, OR UNAUTHORIZED, ILLEGAL, OR IMPROPER USE OF ADTRAN EQUIPMENT OR SOFTWARE. THEREFORE, ADTRAN IS NOT LIABLE FOR ANY LOSSES OR DAMAGES RESULTING FROM SUCH FRAUD, ATTACK, OR IMPROPER USE, INCLUDING, BUT NOT LIMITED TO, HUMAN AND DATA PRIVACY, INTELLECTUAL PROPERTY, MATERIAL ASSETS, FINANCIAL RESOURCES, LABOR AND LEGAL COSTS.

Ultimately, the responsibility for securing your telecommunication and networking equipment rests with you, and you are encouraged to review documentation regarding available security measures, their configuration and implementation, and to test such features as is necessary for your network.

ADTRAN Technical Support Community

For information on installing and configuring ADTRAN products, visit the ADTRAN Support Community, <https://supportforums.adtran.com>.



Pre-Sales Technical Support
(800) 615-1176
application.engineer@adtran.com

Corporate Office
901 Explorer Boulevard
P.O. Box 140000
Huntsville, AL 35814-4000
Phone: (256) 963-8000
www.adtran.com

Post-Sales Technical Support
(888) 423-8726
support@adtran.com

Copyright © 2014 ADTRAN, Inc.
All Rights Reserved.

Contents

<i>Introduction</i>	4
<i>Supported Models</i>	4
<i>Wireless Regulatory Compliance</i>	4
<i>Upgrade Instructions</i>	4
<i>System Notes</i>	5
<i>Fixes</i>	6
<i>Errata</i>	6

Introduction

BSAP 6.8.0-18 is a maintenance release that addresses customer issues that were uncovered in previous code releases.

This release is generally available code. Results obtained during internal testing have been evaluated and the code has been determined to be ready for general availability. Caveats discovered during testing but not addressed in this build are listed in *Errata on page 6*.

A list of new or updated documents for this release appears in *Documentation Updates on page 8*.

Configuration guides, white papers, data sheets, and other documentation can be found on ADTRAN's Support Forum, <https://supportforums.adtran.com>. The contents of these release notes will focus on the platforms listed below.

This AP firmware should be used with vWLAN 2.4.0.12 and vPatch 2-4-0-12.

Supported Models

The following models are supported in BSAP 6.8.0-18.

- BSAP 1800v1 and v2
- BSAP 1840
- BSAP 1920/1925
- BSAP 1930/1935
- BSAP 1940

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 platform 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, it will scan the channels to discover neighboring APs and optimize DynamicRF™.

Upgrade Instructions

Bluesocket Access Point firmware version 6.8.0-18 is the minimum version required for interoperability with vWLAN 2.4.0.12 when vPatch 2-4-0-12 is applied, and is not compatible with previous vWLAN versions. In order to avoid access point downtime after the vWLAN is upgraded from to 2.4.0.12, consider upgrading Bluesocket access points in advance.

To upload locally stored AP firmware manually, follow these steps:

1. Upload new AP firmware and apply to an AP template:
 - a. Navigate to the **Configuration** tab and select **Wireless > AP Firmware**.
 - b. If you are uploading firmware for a domain, select the **Domain** tab. If you are uploading firmware for the vWLAN platform, select the **Platform** tab.
 - c. To upload the new AP firmware, select **Create AP Firmware** at the bottom of this menu.
 - d. Select the new firmware file from the location in which you stored the downloaded firmware by selecting **Browse**.
 - e. Select the domains to which to apply the new AP firmware by using the + (plus) sign. If you are uploading to the domain view, the AP firmware will automatically be available in the domain.
 - f. Choose the template(s) to which to apply the firmware change.
 - g. Select **Create AP Firmware** (or **Update AP Firmware** if editing) to apply the changes. A confirmation is displayed indicating that the AP firmware has been successfully created or updated.
2. This step should only be taken if the AP firmware is backward compatible with the older versions of vWLAN. Apply the new or updated firmware to the AP by running the following domain tasks: **Must apply configuration to APs** and **Must activate new AP firmware** (in the case of 19XX model APs). Upgrade status can be monitored in the secure administrative GUI by navigating to **Access Points** on the **Status** tab.

System Notes

As of vWLAN 2.2.x, AP firmware is not included in the vWLAN image. 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:

1. Use WPA2 (PSK or 802.1x) with advanced encryption standard (AES) when connecting 802.11n-based clients. A TKIP client will connect at a maximum transmit rate of 54 Mbps. 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.
2. 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.
3. 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.
4. Ensure that all 802.11n client drivers are updated to the latest version before doing any system or performance testing.
5. To support multicast traffic between clients, do one of the following:

- 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.
- Allow the Multicast Destination IP Address in the Unregistered Role. The drawback to the Unregistered Role is it allows multicast for all users. Therefore, it should only be used if all users are allowed to receive the multicast streams.

Fixes

This section highlights major bug fixes in BSAP 6.8.0-18.

- It was possible for clients to have to reconnect to the SSID after being idle for a period of time.
- Increased APs performance in location discovery.
- In large busy deployments where the configuration was sent to the AP repeatedly and continuously, APs would stop accepting client connections.
- In a High Availability configuration, it was possible that, if failover to the node was interrupted by the master returning online, the AP would maintain a connection with both master and node vWLAN.
- Certain debug capabilities on the AP were disabled by default to maximize resources on older AP platforms.
- In the process of sending RF data to the vWLAN, a resource leak on the AP would cause the AP to reboot unexpectedly.
- Clients were not able to authenticate until the AP was rebooted.
- In deployments with many locations, location discovery on individual APs would fail to complete. A reboot of the AP was required to identify all active locations.
- The AP would stop authenticating (802.1x) new users. A reboot of the AP was required to clear the issue.

Errata

The following is a list of errata that still exist in BSAP 6.8.0-18.

- An AP may intermittently report that the 802.11bg radio is unavailable.
- An AP will not discover the vWLAN after connectivity is restored following an Internet outage.
- If devices with new 802.11ac drivers that are not fully standards compliant try to connect to a BSAP-19x0, the AP may not be able to handle other users. Please update these devices and reboot the APs.
- In some cases where there is a lot of traffic congestion, it is possible that the policer in the AP could drop all packets from a client.
- After multiple manual reboots, the AP got into a down state.
- The APs may stop accepting connections and require the AP to be rebooted.
- When packet aggregation is enabled on the radio, iOS and OS X devices can sporadically lose network connectivity.
- If an AP has eight or more wired access groups, applying any configuration requires rebooting the AP. After reboot, the AP functions normally. **Workaround:** Reduce the number of access groups, or only push configurations during times when an AP reboot is acceptable.

- Certain devices will present a Captive Network Assistant (CNA) even though this feature is disabled in vWLAN.
- The actual control channel timeout interval is longer than the configured value. It can take up to 2 minutes to detect the control channel timeout.
- The APs may stop accepting connections and require the AP to be rebooted.
- 802.11b data rates will still be advertised on the BSAP 1920 Series APs even though the template is set for 802.11g/n only.
- Clients are not able to connect to the WLAN due to a low memory condition on the AP.
- Crash caused by adding same sequence number to Block Acknowledgement Window second time in aggregation mode
- When no SSID was configured in the AP template for a radio with the Radio Mode set to AP Mode or Dual Mode, RF alerts and adjacency information were not sent from the BSAP to the vWLAN.
- BSAP 1930 APs may reboot due to certain client activity.
- If a default gateway is omitted from the BSAP network configuration and the RADIUS server(s) does not exist on the same broadcast domain, 802.1X (WPA/2-Enterprise) SSIDs come up as open SSIDs and do not enforce 802.1X authentication.
- APs show their status as Updating and then reboot when the AP cannot set the channel for the 5 Ghz radio.
- After sending an apply command, the BSAP remains in an Updating status and will not bring up its radios. A manual reboot of the AP clears the issue.
- During a BSAP 1900 Series 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.
- APs were not setting the Tx Power to the value sent by vWLAN in ContinuousRF mode.
- During a BSAP 1800 Series 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.