RELEASE NOTES

BSAP 6.9.1-8
June 3, 2015

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

Contents

Introduction

BSAP 6.9.1-8 is a minor release that adds new features and addresses 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*.

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.

Supported Models

The following models are supported in BSAP 6.9.1-8.

- BSAP 1800v1 and v2
- BSAP 1840
- BSAP 1920/1925
- BSAP 1930/1935
- BSAP 1940
- BSAP 2030/2035

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 6.9.1-7 is the minimum version required for interoperability with vWLAN 2.5.1 and is not compatible with previous vWLAN versions. 6.9.1-8 is also compatible with vWLAN 2.5.1. In order to avoid access point downtime after upgrading, 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 and 20XX model APs)**.** Upgrade status can be monitored in the secure administrative GUI by navigating to **Access Points** on the **Status** tab.

System Notes

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/ac wireless client interoperability is only guaranteed for Wi-Fi Alliance certified clients. For the highest 802.11n/ac performance, follow these steps:

1. Use WPA2 (PSK or 802.1X) with advanced encryption standard (AES) when connecting 802.11n/ac-based clients. A TKIP client will connect at a maximum transmit rate of 54 Mbps. It is highly recommended that WEP and WPA not be used, but WPA2 be used instead. Running in a mixed mode environment (i.e., with legacy clients) will impact the 802.11n/ac client's performance.
2. Enable 802.11n and ac Wireless Modes, 80 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/ac 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/ac 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.

Features and Enhancements

This section highlights the major features, commands, and behavioral changes in BSAP 6.9.1-8.

- Added support for Role Based Access Control Schedules.
    - The ability to schedule when Wi-Fi access is or is not available via the role. For example, a library could prevent guests from using the internet from their parking lot when they are closed for business and allow access during normal business hours.
- Added support for Kenya country regulatory domain for BSAP 1920.
- Added support for Turkey country regulatory domain for BSAP 1930, 1935 and 1940.
- Added support for St. Vincent, St Lucia, Barbados, Dominica and Grenada country regulatory domain for BSAP 1920, 1925 and 1940.

Fixes

This section highlights major bug fixes in BSAP 6.9.1-8.

- Clients could not pass traffic intermittently on BSAP 192x APs.
- Due to a lockup, a BSAP 1920 would appear to be Down in the controller.
- For the BSAP 19xy and 203x model APs, 40Mhz mode would not enable on the 2.4GHz radio.
- BSAP 1800v1, 1800v2, and 1840 models would stop accepting client connections due to a memory management issue. The AP would have to be rebooted to clear the condition.
- The actual control channel timeout interval is longer than the configured value. It could take up to 2 minutes to detect the control channel timeout.

Errata

The following is a list of errata that still exist in BSAP 6.9.1-8.

- The AP isn't able to receive NTP servers via DHCP. **Workaround:** NTP Servers can be defined in the AP Template.
- DSCP values assigned to a role are not being observed in captured traffic post-assignment.
- Certain devices are blocked when attempting to access network resources outside their assigned schedule. The user with a blocked device (Apple specifically) is being assigned a valid and routable IP address and can appear in the UI Status page as such, but traffic the device attempts to generate, such as http or https, is still being blocked.
- A BSAP 1800/1840 may become locked up and incorrectly report: BG radio: non-802.11 interference detected - change the channel and then reboot the AP A radio: non-802.11 interference detected - change the channel and then reboot the AP. **Workaround:** Push an Apply to the AP or reboot it.
- BSAP 1800 version 1 may stop servicing clients during periods of heavy load. **Workaround:** Push an Apply to the AP or reboot it.

- BSAP 1800 version 2 uses incorrect PSM for the client resulting in missing packets and dropped connections.
- BSAP 1800 model APs may stop accepting connections and require rebooting.
- An AP may not report detected adjacent APs to vWLAN.
- Class of Service Role override on the BSAP 2030 Series 5 Ghz radio is not supported in this release. It functions on the 2.4 Ghz radio and BSAP 1900 Series APs.
- **Workaround:** If CoS is required for BSAP 2030 5 Ghz clients, configure the upstream switches for the tagging.
- The Virtual Ethernet process on an AP may shut down unexpectedly.
- Large data packets may be lost over a Layer 3 tunnel from the BSAP 1900 Series AP.
- An AP may reboot due to a noisy RF environment.
- 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 configuration 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.
- During a BSAP 19xx or 203X 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 are not setting the Tx Power sent dynamically to the value sent by vWLAN in ContinuousRF mode.
- During a BSAP 18xx AP firmware upgrade, if the server parameters are incorrect or the AP cannot reach the server, the AP will not recover. **Workaround:** 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.