RELEASE NOTES

BSAP 6.9.0
October 31, 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

Contents

Introduction

BSAP 6.9.0 is a major system 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 7*.

A list of new or updated documents for this release appears in *Documentation Updates on page 9*.

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 6.9.0.

- BSAP 1800v1 and v2
- BSAP 1840
- BSAP 1920/1925
- BSAP 1930/1935
- BSAP 1940
- BSAP 2030/2035
- BSAP 3495

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 6.9.0 is the minimum version required for interoperability with vWLAN 2.5.0 and is not compatible with previous vWLAN versions.. 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 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 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, 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/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 6.9.0

- Support for Mesh on BSAP 1900 series
    - Point-to-point Bridging
    - Point-to-multipoint Bridging
    - Multiple Hop Mesh
    - Ethernet Port Bridging
- Support for new 2030 Series 802.11ac 3 stream indoor APs
- Support for Minimum Transmit Rate in BSAP 1900 series

Fixes

This section highlights major bug fixes in BSAP 6.9.0.

- Resolved an issue with management of aggregation packets.
- If devices with new 802.11ac drivers that were not fully standards compliant tried to connect to a BSAP 1900 series AP, the AP would not be able to service other users.
- After multiple manual reboots, the AP would go into the down state.
- BSAP 1800v1 Series access points would generate an internal error when an unregistered client connected.
- On a large configuration push of several APs, some APs would not report locations to vWLAN which caused needless tunneling.
- If a client is in the unregistered role and attempted to perform web authentication and their authentication session was interrupted, the client to would be forced to restart the authentication process.
- Resolved an issue with the redirection process.
- Resolved a condition where an AP could reboot continually.
- On BSAP 1900 Series access points, if the DNS server obtained in the DHCP lease or statically configured via the console was unable to resolve the PTR record for the vWLAN, a certificate validation warning was presented for client web authentication even though a valid certificate was installed on the vWLAN and the vWLAN was properly configured for redirection to hostname.
- An AP would reach an incongruent state and would reboot.
- 802.11b data rates were still advertised on 1920 Series BSAPs even though the template was set for 802.11g/n only.
- 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.
- Display a warning if a default gateway was omitted from the BSAP network configuration and the RADIUS server(s) did not exist on the same broadcast domain, 802.1X (WPA/2-Enterprise) SSIDs would appear to be open SSIDs and did not enforce 802.1X authentication.

- APs displayed their status as Updating and then rebooted when the AP could not set the channel for the 5 Ghz radio.

Errata

The following is a list of errata that still exist in BSAP 6.9.0**.**

- BSAP 1800 version 1 may stop servicing clients during periods of heavy load.
- BSAP 1800 version 2 may use incorrect Power Save Mode (PSM) for some clients, resulting in missing packets and dropped connections.
- 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.
- A BSAP 1920 can appear to be down in the controller due to a kernel lockup. Sending a reboot fixes the condition.
- Apple iPad may fail to stream periodically.
- The Virtual Ethernet process on an AP may shut down unexpectedly.
- Stopping a wireless packet capture before it has run for 30 seconds could result in a fault condition. This can be avoided by allowing the capture to start and run for at least 30 seconds. If a domain task is added after a capture, this means that the AP didn't fully recover from the cancelled capture. Applying a configuration to an AP or rebooting it will recover the AP from this condition.
- BSAP 1800v1 Series access points may not upgrade until rebooted due to reduced resources available over time.
- The DSCP CoS priority Override in the User Role is not enforced.
- Large data packets may be lost over a Layer 3 tunnel from the BSAP 1900 Series AP.
- 40 MHz mode does not function on BSAP 1900 Series and BSAP 2030 Series when using the 2.4 GHz radio.
- An AP may reboot due to a noisy RF environment.
- An AP may intermittently report that the 802.11b/g radio is unavailable.
- 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, the application of any configuration requires rebooting the AP. After the reboot, the AP functions properly. **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 APs may stop accepting connections and require the AP to be rebooted.
- In certain cases where there is a lot of traffic congestion, it is possible for the AP's policer to drop all packets from a client.
- 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.
- An AP may reboot if it is servicing clients that are in aggregation mode and the AP detects interference.

- 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.

