RELEASE NOTES

BSAP 6.8.0
February 25, 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 6.8.0 is a major system release that adds new features and 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 8*.

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 6.8.0.

- 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 6.8.0-09 is the minimum version required for interoperability with vWLAN 2.4.0.12 and is not compatible with previous vWLAN versions.. In order to avoid access point downtime after the vWLAN is upgraded from 2.2.1.20 to 2.3.0.09, 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.

Features and Enhancements

This section highlights the major features, commands, and behavioral changes in BSAP 6.8.0

- **Enhanced UI and usability**
  - Refreshed, intuitive, HTML5-based administrative user interface (UI) with a bright, crisp, modern look and feel
  - Forms, fonts, font sizes, and colors are consistent throughout the product
  - Pages divided into sections with titles and page breaks
  - Admin Auth moved to Administration
  - Domain tasks appear in red
  - Navigation menus are no more than three levels deep
  - Status is linked to configuration and vice versa
  - Preferences, such as the columns chosen to display, are saved in client side cookies
  - Infinite scroll allows continuous scrolling without going page by page
  - Logs are sorted newest to oldest by default
  - Column headers always displayed
  - No need to scroll all the way to the bottom of a long list in order to scroll to the right
  - Many default values have been added, for example, the common ports used for authentication
  - Ability to simply drill down into a line without having to click a show (folder) or edit (pencil) action
- **Enhanced status**
  - Ability to see number of clients per access point and per radio
  - AP Details View
    - Ability to drill down for detailed AP information such as the clients that are associated to the radio, number of clients per radio, radio interface settings, etc.
    - Quick links to edit the AP configuration, see the AP on the floor plan, see logs regarding the AP, see alarms regarding the AP, see wireless IDS alerts from the AP, run a traffic capture on the AP, and see APs that are adjacent to the AP
  - Client Details View
    - Ability to drill down for detailed client information with quick links to logs regarding the client and to run a traffic capture to capture the client’s traffic
- **Enhanced Dashboard/Reporting**
  - Customizable dashboards with real time and historical widgets (charts and graphs)
    - Client Count Over Time
    - Client Usage Over Time

    - Current AP Firmware Versions
    - Current AP Status
    - Current Active AP Count
    - Current Active Users by Radio Mode
    - Current Client Count
    - Current Client Status
    - Top APs by Client Count Over Time
    - Top APs by Client Usage Over Time
    - Top Clients by Usage Over Time
    - Top Locations by Client Count Over Time
    - Top Locations by Usage Over Time
    - Top Roles by Client Count Over Time
    - Top Roles by Client Usage Over Time
    - Top SSIDS by Client Count Over Time
    - Top SSIDS by Client Count Over Time
  - Reports show instantly without waiting for job to run
  - Real time widgets update while you are watching and historical widgets present historical data
  - Ability to create multiple dashboards or tabs for customized perspectives
  - Ability to have more than one report on the system at any given time
  - Ability to download and email the entire dashboard (or just one widget) in PDF (containing charts and graphs) and CSV (containing data only) format
  - Ability to filter historical widgets by time and date (last 24 hours, last 7 days, last 30 days, custom)
  - Ability to customize report logo
  - The color red is no longer used in charts and graphs
- **Support for sending secure email alerts (TLS)**
- **Usernames of Active Users appear on secondary following a failover event**
- **Ability to export Logs, Alarms, and W-IDS Alerts**
- **Support for setting the minimum data rate on BSAP 1900 Series access points**
- **Additional AP Scale with multi-tenant**
  - Support for 1500 APs on vWLAN Appliance hardware and vWLAN Virtual Appliance (VMware) with minimum system requirements (500 APs were previously supported)
- **Support for new vWLAN 1U hardware appliance**

Fixes

This section highlights major bug fixes in BSAP 6.8.0.

- Samsung Galaxy S3s and S4s using Android 4.3 were not able to associate to an Open SSID when a Splash Page was configured.
- It was possible for the system to create very large AP configuration files when large port ranges were used in role policies.
- On BSAP 1900s, the 40 MHz mode could not be enabled on the 2.4 GHz radio.
- Users who moved from an open/unregistered SSID to an 802.1X SSID retained the NAC scope IP address.
- BSAPs using High Availability would not fall back to the primary even when configured to do so.
- As part of location discovery, if DHCP was blocked on the AP's native network, DHCP release messages did not reach the DHCP server to clean up leases. Locations were still discovered.
- DSCP values were not honored.
- Under certain circumstances, a BSAP 1940 would become unresponsive and not respond to a reboot command.
- Neither NAS-IP-address nor NAS-identifier were present in the RADIUS Access-Request packet sent by the AP.

Errata

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

- When using many location tags, the process to discover locations takes longer than expected and some locations may not show in the UI. To work around the issue, reboot the AP.
- "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 configuration during times when an AP reboot is acceptable."
- The APs may stop accepting connections and require the AP to be rebooted.
- The AP may reach an incongruent state causing a reboot.
- The AP may stop authenticating (802.1x) new users. A reboot of the AP clears the issue.
- The vUserMgr crashes and then reboots.
- Legacy clients which enter a power-save mode may have issues in a mixed environment supporting 802.11n on the 2.4GHz radio.
- 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.
- 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.
- AP may reboot if it is servicing clients that are in aggregation mode and the AP detects interference.
- 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.
- Dell Latitude 10-ST2e tablet devices running Windows 8 are not able to Authenticate via 802.1.x.
- 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.
- Some clients are not being redirected from a URL. They remain on the Thank You screen.
- MacBooks running Windows 7 VM cannot obtain an IP address when set to Bridge mode.
- 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.
- 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 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.

Documentation Updates

The following documents were updated or newly released for BSAP 6.8.0. These documents can be found on ADTRAN's Support Forum available at https://supportforums.adtran.com. You can select the hyperlink below to be immediately redirected to the document.

- *vWLAN Admin Guide*

