RELEASE NOTES

BSAP 6.7.0
August 12, 2013

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 6.7.0 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 7*.

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.

Supported Models

The following models are supported in BSAP 6.7.0.

- 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 6.7.0.17 is required for interoperability with vWLAN 2.3.0.09, but it is also backward compatible with vWLAN 2.2.1.20. 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. 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 6.7.0.

- Client density was increased on the BSAP 1900 Series. The maximum associated clients per radio on the BSAP 1900 Series is now configurable to values higher than the previous hard maximum limit of 64. The default maximum limit is now 64. The hard maximum limit of 64 associated clients per radio remains for BSAP 1800 Series.

  The value for maximum associated clients per radio should be chosen carefully based on the per-user bandwidth requirements of the applications in use on the network. For example, in greenfield deployments with exclusively 802.11n radios and three stream clients, the maximum data rate is 450 Mbps. Actual throughput, however, is typically 50 to 60 percent of the maximum data rate, approximately 270 Mbps in a clean RF environment with no interference. Since Wi-Fi is a shared medium, all clients associated to a radio are sharing the actual throughput of 270 Mbps. In this deployment example, if the applications have a per-user bandwidth requirement of 1.08 Mbps, up to 250 clients per radio can be supported. However, if the applications have a higher per-user bandwidth requirement, 10 Mbps for example, only 27 clients per radio can be supported.

  Note the examples above are based on the best case greenfield deployment of exclusively 802.11n radios and three stream clients operating at their highest data rates in a clean RF environment with no interference. Single stream 802.11n clients will have maximum data rate of 150 Mbps, dual stream 802.11n clients will have a maximum data rate of 300 Mbps, and legacy 802.11a/g clients will have a maximum data rate of 54 Mbps. Keeping in mind an actual throughput of 50 to 60 percent of these maximum data rates in a clean RF environment with no interference, if you have a mixture of client types (single stream, dual stream, or legacy) you should plan for the most prevalent client type.

  While ADTRAN has removed the hard maximum limit, and the associated clients per radio on the BSAP 1900 Series is now configurable to values higher than 64, it is important to understand that Wi-Fi is a shared medium. The more users associated to a radio, the less throughput will be available for each user because all users are sharing the pool of available bandwidth. Customers should plan accordingly for coverage AND capacity (client density), not just coverage. While areas with high user density such as libraries, cafeterias, lecture halls, conference centers, etc. may require only one access point for coverage purposes, they may require multiple access points for capacity purposes.

Fixes

This section highlights major bug fixes in BSAP 6.7.0.

- RF data was not being collected properly, leading to bad adjacencies in BSAP 19xx series units.
- After several reboots, some APs would switch partitions.
- BSAP 1920s with statically configured IP addresses and controller IP addresses would discover the secondary vWLAN in a High Availability configuration.
- BSAP 1920s would reboot when a Destination with greater than 24 characters was entered.
- APs with 8 SSIDs configured on a radio would crash.

- Clients placed in a Role with Firewall were tunneled to a BSAP 19xx which caused a crash on HA.

Errata

The following is a list of errata that still exist in BSAP 6.7.0.

- APs show their status as Updating and then reboot when the AP cannot set the channel for the 5 Ghz radio. This only affects Taiwan on channels 52-60.
- 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.
- Dynamic RF calibration fails to select proper power and channel settings.
- Unsupported client negotiations between the client an AP may cause an AP to reboot.
- Wired clients are intermittently unable to be redirected to the Captive Portal login page until after the AP is rebooted.
- After failing over to the secondary RADIUS server, the primary RADIUS server was not retried even though it is available.
- Qualcom QCA9005 Tri-Band wireless chipset has connectivity issues.
- BSAP 1930s may reboot with a lot of roaming activity.
- DHCP offers and ACKs may be dropped by the AP.
- DSCP values are not honored.
- 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.
- The TP-Link (TL-WPS510U) printer's IP address is not being added to the Active Connections table.
- 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.
- Under certain circumstances, a BSAP 1940 may become unresponsive and not respond to a reboot command.
- Under certain circumstances, a BSAP 18xx may become unresponsive and not respond to a reboot command.
- A NAS-IP-address or NAS-identifier is not present in the RADIUS Access-Request packet sent by the AP.
- 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 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.
- It is not possible to log into a BSAP 1800v1 after changing the SSH password. Workaround: Reset AP to defaults.
- APs are not setting the Tx Power sent dynamically to the value sent by the vWLAN in ContinuousRF mode.

- 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.

Documentation Updates

The following documents were updated or newly released for BSAP 6.7.0. 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 Administrator's Guide*
- *vWLAN AP Discovery*
- *Using APIs with vWLAN*
- *vWLAN Hardware Appliance Quick Start Guide*

