RELEASE NOTES

BSAP 7.0.1
August 7, 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 7.0.1 is a major 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 7.0.1.

- 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™.

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.
   - On the SSID, do not convert multicast to unicast and 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 7.0.1.

- AP Transmit Power is now represented in dBm and mW values rather than in percentages.

Fixes

This section highlights major bug fixes in BSAP 7.0.1.

- When the AP was operational, the Status LED slowly flashed green when it should have remained solid green.
- The Mesh AP Downlink Signal Strength indicators always displayed -95, but the upstream indicators were correct.
- The BSAP 18xy platform did not include country code IE in the beacon.
- When changing from PSK to Open SSID, the device was unable connect on the first attempt.
- When reducing the power of an AP to anything less than 100 percent, the power being output was not what was expected.
- The Droid Turbo Cellular Phone could not properly transmit data on a BSAP 1800.
- A BSAP 1800/1840 would lock 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.
- The Virtual Ethernet process on an AP would shut down unexpectedly.
- The BSAP 1930 rebooted due to a certain client disassociation.

Errata

The following is a list of errata that still exist in BSAP 7.0.1.

- The supported channel width of the HT Information field in 802.11 WLAN management frames is not being set in BSAP 1800s, which leads client devices to assume that 20 MHz is the preferred channel width.
- Wireless captures cannot be taken on the A interface (5 GHz) of BSAP 1800s.
- The BSAP 1920 may reboot intermittently.
- DFS may detect radar falsely.
- The BSAP 18xy may experience a low memory condition over time.
- If Virtual Ethernet fails to connect it can result in a memory leak in the APs.
- B/G radio is being disabled intermittently when dynamic RF mode is set to **Continuous**.
- BSAP 1900s are not reporting beacon issues to vWLAN due to serve RF interference.
- The EOSP bit is not being properly set for the UAPSD power save mode.
- BSAPs support up to 1024 Schedule Rules. If the APs reboot after adding schedules, you need to reduce the number of schedules.
- BSAP 1800 version 2 was using the incorrect PSM for the client resulting in the client missing packets and dropping connection.
- BSAP 1930 Control Channel may reset often.
- When starting a wireless packet capture, take care to allow the capture to begin before taking an action on it. If the capture must be stopped, wait at least 30 seconds to let the capture fully start. If a domain task pop-up is seen after a capture, it means the AP never fully recovered after the capture. Apply configuration to or reboot the AP to recover it.
- Certain devices will present a Captive Network Assistant (CNA) even though this feature is disabled in vWLAN.
- The Sony Xperia Tablet Z running Android version 4.2.2 may fail to authenticate using 802.1x due to an issue with the device itself.

Release Specific Upgrade Instructions

Bluesocket Access Point firmware version 7.0.1 is the minimum version required for interoperability with vWLAN 2.6.1 and is not compatible with previous vWLAN versions.

To upgrade your BSAP please see the vWLAN upgrade guide located at https://supportforums.adtran.com/docs/DOC-7691.

Upon upgrading to vWLAN 2.6.1, if you have an AP that is configured in an ETSI Regulatory Domain the 5GH band will be disabled. To re-enable the radio enable the DFS feature, (if installed outdoors) or mark the AP as indoor (if installed indoors).

