Adtran Switch Engine (ASE)

4.4-47 Release Notes

Release Notes

6AMCRN4447-40A

June 2023

To the Holder of this Document

The contents of this manual are current as of the date of publication. Adtran reserves the right to change the contents without prior notice.

Trademark Information

“Adtran” and the Adtran logo are registered trademarks of Adtran, Inc. Brand names and product names included in this document are trademarks, registered trademarks, or trade names of their respective holders.

Disclaimer of Liability

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products are given “as is”, and any liability arising in connection with such hardware or software products shall be governed by Adtran’s standard terms and conditions of sale unless otherwise set forth in a separately negotiated written agreement with Adtran that specifically applies to such hardware or software products.

To the fullest extent allowed by applicable law, in no event shall Adtran be liable for errors in this document for any damages, including but not limited to special, indirect, incidental or consequential, or any losses, such as but not limited to loss of profit, revenue, business interruption, business opportunity or data, that may arise from the use of this document or the information in it.

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

901 Explorer Boulevard
P.O. Box 140000
Huntsville, AL 35814-4000
Phone: (256) 963-8000

Copyright © 2023 Adtran, Inc.
All Rights Reserved.

Table of Contents

1. Introduction 4

2. Supported Platforms 4

3. Features and Enhancements 4

4. Fixes 5

5. Errata. 7

6. Warranty and Contact Information. 9

1. Introduction

Release 4.4-47 is a major system release that adds new features and addresses customer issues that were uncovered in previous releases for the Adtran Switch Engine (ASE) switches.

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*.

Configuration guides, white papers, data sheets, and other documentation can be found on Adtran's Support Community, https://supportcommunity.adtran.com. The contents of these release notes will focus on the platforms listed in *Supported Platforms on page 4*.

2. Supported Platforms

Table 1 lists the platforms that are supported in ASE firmware release 4.4-47.

Table 1. Supported Platforms

Platform	Part Number
NetVanta 1560-08-150W	17108108PF2
NetVanta 1560-24-740W	17108124PF2
NetVanta 1560-48-740W	17108148PF2
NetVanta 1560-08-65W	17101561PF2
NetVanta 1560-24-370W	17101564PF2
NetVanta 1560-48-370W	17101568PF2
NetVanta 1560-08 (non-PoE)	17101561F1
NetVanta 1560-24 (non-PoE)	17101564F1
NetVanta 1560-48 (non-PoE)	17101568F1

3. Features and Enhancements

This section highlights major features, commands, and behavioral changes for all products running ASE version 4.4-47:

- BSW-591 Updated the SSH Dropbear version to 2020.82 to address SSH vulnerabilities discovered via Nessus scan.
- BSW-597 Updated the color scheme in ASE Web GUI.

- BSW-505 Updated PoE functionality in the NetVanta 1560-24 devices to support Broadcom-based PoE MCU as a secondary source. The NetVanta 1560-24 Broadcom-based PoE devices will not support software versions lower than 4.4-47, due to the PoE enhancements. A more specific error message was added to prevent firmware downgrades on these devices, so that the error appears as follows when attempting to download an earlier version of firmware:

```
Switch# $rade tftp://10.10.10.10/NV1560-24 v4.4-45-20220304.mfi
Downloading....
Got 14565634 bytes
This model doesn't support software version lower than 4.4-47
Invalid image, need a correct MFI image
```

- BSW-270 Added the ability to specify a 31 bit netmask in an IP Address configuration for a port.
- BSW-282/ BSW-1 Added support for RADIUS CoA VLAN assignments.
- BSW-334 Added support for the **ssh** <*tcp port*> command, which allows the TCP port on which SSH operates to be changed from the default TCP port 22 after SSH is enabled.
- BSW-341 Added support for hostnames to be specified with a numeral as the first character and to include additional special characters.
- BSW-346 Added a yes/no confirmation requirement for reloading the default configuration when using the **reload defaults** command.
- BSW-356/ BSW-592 Updated the ASE Web GUI to only display configured VLANs on the **VLAN Membership** page, rather than displaying all possible VLANs that are allowed on the system.
- BSW-422 Added System Object IDs (unique OIDs) to the system for each ASE switch. These OIDs can be retrieved via SNMP.
- BSW-645 Updated the default configuration information so that they match across all ASE platforms.
- BSW-658 Updated the system description used when identifying the device model via Link Layer Discovery Protocol (LLDP) to the following format: **System Description: [Model]**, **[Version]**, **[Date & Time]**.
- BSW-97/ BSW-290 Added enhancements to the **reload** command. The additional **in** <*time*> parameter allows a reload to be scheduled on a delay, and the additional **cancel** parameter allows a scheduled reload to be canceled.

4. Fixes

This section highlights major bug fixes in ASE release 4.4-47.

- Fixed an issue in which the PoE profile name could not display certain special characters on the **PoE** GUI configuration page.
- Fixed an issue in which NetVanta 1560-08 devices could crash when more than **256** ARP requests were received.
- Fixed an issue in which 802.1x authentication would fail for voice VLANs configured with an IP phone.
- BSW-86 Fixed an issue in which a 2.5Gb SFP was not displayed correctly in the **Port State Overview** page of the GUI.
- BSW-210 Fixed and issue in which the **access-list shutdown** command did not shutdown the interface despite the traffic matching the access control list (ACL) match criteria.
- BSW-306 Fixed an issue in which **value** was spelled incorrectly in the CLI help.

- BSW-343 Fixed an issue in which the **show auto-link** command would always report a status of CONNECTED, no matter the state of the network configuration or connection.
- BSW-344 Fixed an issue in which the **show auto-link** command would display time settings in GMT regardless of the time zone configured on the device.
- BSW-348 Fixed an issue in which an erroneous line of code would be displayed when issuing the **reload defaults** command.
- BSW-363 Fixed an issue in which the switch removed VLAN tags on voice VLANs enabled on access ports.
- BSW-365 Fixed an issue in which Link OAM MIB retrieval did not function properly when using the GUI.
- BSW-366 Fixed an issue in which the **show tech** command was not supported. Now when this command is entered, a showtech.txt file is created and placed in the switch's flash directory. This output contains various information and statistics for the switch, and is accessible via TFTP, using the **copy flash:showtech.txt tftp://**<*ip address*>**/showtech.txt** command.
- BSW-368 Fixed an issue in which selecting the **Activate Alternate Image** button from the **Software Image Selection** menu would result in an internal server error (500).
- BSW-370 Fixed an issue in which 2.5Gb SFP (P/N 1200482G1) would not function properly on an ASE device.
- BSW-406/ BSW-499 Fixed an issue in which VoIP endpoints accessing the switch via an access port and using LLDP-MED policies to use the Voice VLAN were losing communication with the switch and rebooting.
- BSW-408 Fixed an issue in which the **Reset** button for the **Add Route** configuration option was not functioning correctly in the I**P Configuration** page of the GUI (**Configuration** > **System** > **IP**).
- BSW-425 Fixed an issue in which the **Reset** button was not functioning properly for the **Aggregation Group Configuration** GUI menu.
- BSW-428 Fixed an issue in which voice VLANs enabled and active on an access port were not displayed as part of the output of the **show vlan** command.
- BSW-448 Fixed an issue in which the **include** and **exclude** output modifiers of the **show access management statistics** command were not functioning properly.
- BSW-480 Fixed an issue in which users could not access privileged mode once they exited. Added the **aaa authentication local enable** command to the switch's default configuration, which allows users to exit privileged mode and be prompted with a password at reentry.
- BSW-500 Fixed an issue in which ACE entries with the **Frame-Type IP** values entered in the GUI would not be displayed.
- BSW-518 Fixed an issue in which IP addresses could be assigned to clients via DHCP even when the port was in an unauthorized state.
- BSW-520 Fixed an issue in which some ASE devices would not send Access-Request messages after the RADIUS server was restarted.
- BSW-526 Fixed an issue in which device reauthentication would not occur when the reauthorization timer expired. When reauthentication is enabled, successfully authenticated supplicants/clients are now reauthorized after the interval specified by the **Reauthentication Period**.
- BSW-528 Fixed an issue in which clients could be placed in an authorized state, even when Access-Reject messages were sent from the RADIUS server.
- BSW-533 Fixed an issue in which continuously repeated warnings in the CLI were impeding operations. As part of the resolution, the log level has been updated from **Warning** to **Debug** for the **Warning: WARNING Error Unknown file passed** error.

- BSW-541 Fixed an issue in which RADIUS CoA disconnect messages had no effect if the Guest VLAN was enabled in the authenticator. Now, if a CoA disconnect message is sent, the client is placed in the Guest VLAN.
- BSW-553 Fixed an issue in which the voice VLAN configuration would place VoIP phones in the RADIUS VLAN on the ASE switch, even when a voice VLAN was configured.
- BSW-554 Fixed a spelling error in the output of the **show dot1x status** command.
- BSW-560 Fixed an issue in which, in some cases, the auto-link feature stopped working until the device was rebooted and displayed a status of **Error: Stopped by user**, even when auto-link was enabled.
- BSW-576 Fixed an issue in which ASE devices were sending the wrong device part number information to n-Command MSP.
- BSW-611 Fixed an issue in which mismatched speed configurations between an interface and an SFP would not force an interface to go down.
- BSW-612 Fixed an issue in which the **show running config** command for an interface would not display the configured interface duplex value in the command output.
- BSW-620 Fixed an issue in which ASE devices could crash when the **show lldp-neighbors** command was issued while an Avaya phone was connected to the device.
- BSW-652 Fixed an issue in which SNMP polling would not display any configured port descriptions.

5. Errata

The following is a list of errata that still exist in ASE release 4.4-47.

- CCM frame rates may change automatically after adding a second MEP peer to the OAM configuration. For OAM configurations with multiple peers (multi-point OAM), the hardware (VOE) does not handle the CCM messages but rather forwards those messages to the CPU. To keep the CPU from being overloaded, only one frame per second is supported.
- Spanning-tree may incorrectly prevent Link Aggregation Group (LAG) links from becoming active when **max-bundle** is set to **1**. **Workaround:** Set the **max-bundle** to a value higher than **1**.
- When configured for Link Aggregation Control Protocol (LACP) and switching back to the original active port after an active/standby port switchover, the traffic switchover takes longer than expected (exceeding three minutes).
- BSW-172 RADIUS server statistics may be reset if global RADIUS server configuration changes are made when configuring the RADIUS CoA feature.
- BSW-212 Rebooting the switch from the console interface returns the following incorrect error message: *RedBoot(tm) bootstrap and debug environment [ROMRAM] Non-certified release, version 1_5-38e0421 - built 15:33:42, Jun 1 2018*.
- BSW-230 LACP aggregation group configuration differs slightly between the GUI and the CLI. In the CLI, to change the interface in the group from static to active, you must remove the LACP group configuration from the interface, and then re-add it. For example:
  - (config)#**interface 10 GigabitEthernet 1/1**
  - (config-if)#**no aggregation group 12**
  - (config-if)#**aggregation group 12 mode active**
- BSW-240 With some SSH configurations, the ASE switch may take up to 12 seconds or longer to respond to an initial SSH packet. The SSH time to connect is influenced by the crypto settings being used at each of the SSH session.

- BSW-156 When support was added for TACACS+ authentication of Enable mode logins (in ASE 4.4-44), the default Enable mode login authentication behavior was changed. Previously, the default authentication database was set to the local database. With the addition of the TACACS+ authentication support, you must now specify the database to be used for authentication. If the local database is to be used for Enable mode login and authentication, you must enter the **aaa authentication enable local** command when accessing the switch.The entire login procedure includes the following commands:
  - **#username test privilege 0 password encrypted** <*string*>
  - **#enable secret 5 level 15** <*string*>
  - **#aaa authentication enable local**
- BSW-301 Port Storm Control configurations are not available on a per-interface basis on the NetVanta 1560-08 Series products.
- BSW-436 The **Select All** check box is not functioning properly in the **Port Configuration** menu for **Port Mirroring**. Although the feature is designed to select a single port for port mirroring, and chooses the highest port number for the destination (by default), the **Select All** check box is evoked even when specifying **Port 1** as the destination for port mirroring.
- BSW-504 LLDP information is not currently reported to n-Command MSP instances. **Workaround:** Use the device's CLI to display LLDP neighbors using the **show lldp neighbors** command.
- BSW-585 In some cases, the switch **Privilege Levels** cannot be configured in the GUI, from the **Security** > **Switch** > **Privilege Levels** menu. The **Privilege Levels** menu will open, but all the details are absent and no configuration is possible. **Workaround:** Clear the browser cache to resolve this issue.
- BSW-629 In some cases, when using 802.1x authentication with both a client PC and an IP phone, if the IP phone is rejected by the RADIUS authentication and placed in the guest VLAN, the client PC will also be placed in the guest VLAN even though it was correctly authenticated by the RADIUS server.
- BSW-630 In some cases, phones connecting to an ASE device using 802.1x authentication will be placed in a configured voice VLAN even when a RADIUS server rejects the phone's authentication request, instead of being placed in the guest VLAN.
- BSW-663 Client authentication does not function correctly when connecting an ASE device to a NPS Windows Server 2019.
- BSW-643 When using an ASE device with n-Command MSP, the device will appear in n-Command **Device Alerts** with an **Unsaved Config** warning, erroneously indicating that the ASE device is not configured. **Workaround:** Ignore the **Unsaved Config** warning.

6. Warranty and Contact Information

Warranty information can be found online by visiting www.adtran.com/warranty-terms.

To contact Adtran, choose one of the following methods:

Department	Contact Information	
Customer Care	From within the U.S.: From outside the U.S.:	(888) 4ADTRAN ((888)-423-8726) +1 (256) 963-8716
Technical Support	Support Community: Product Support:	www.supportcommunity.adtran.com www.adtran.com/support
Training	Email: Adtran University:	training@adtran.com www.adtran.com/training
Sales	For pricing and availability:	1 (800) 827-0807