RELEASE NOTES

Switch Products
AOS version R11.2.0
June 2, 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

AOS version R11.2.0 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 6*.

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 Platforms

The following platforms are supported in AOS version R11.2.0. To confirm the Boot ROM version of the ADTRAN unit, Telnet or console to the unit and issue the show version command. In the command output, the Boot ROM version will be listed as Boot ROM version XX.XX.XX. If you require a Boot ROM upgrade, please contact ADTRAN Technical Support (support@adtran.com or 888-423-8726) for assistance.

Platform	Standard Feature Pack	Minimum Boot ROM
NetVanta 1234/1234P (2nd Gen. only)	√	XB.01.02
NetVanta 1235P	√	R10.4.0.B1
NetVanta 1238/1238P (2nd Gen. only)	√	XB.01.02
NetVanta 1531/1531P	√	R11.1.0
NetVanta 1534	√	17.06.03.00
NetVanta 1534 (2nd Gen.)	√	17.08.01.00
NetVanta 1534P (2nd Gen.)	√	17.09.01.00
NetVanta 1535P	√	17.08.01.00
NetVanta 1544/1544F	√	17.06.03.00
NetVanta 1544 (2nd Gen.)	√	17.08.01.00
NetVanta 1544P (2nd Gen.)	√	17.09.01.00
NetVanta 1638/1638P	√	18.02.01.SC

System Notes

- Beginning with AOS version 17.09.01, the syntax of certain commands was modified from previous AOS versions by either removing or adding the ip keyword. In general, when the ip keyword appears in a command, it signifies that the command is only applicable to IPv4 functionality. As more features introduce IPv6 support, the ipv6 keyword is added to signify the command is only applicable to IPv6 functionality. The ip keyword has been removed from several commands to signify that the command has both IPv4 and IPv6 functionality.

  Due to this syntax change, downgrading a unit configured in AOS version R11.2.0 to a previous AOS version, could cause service disruption because the new syntax might not be recognized by the previous version. Upgrading a unit from an older AOS version to AOS version R11.2.0 will cause no service disruption because both the old and the new syntaxes are accepted. For more information on specific commands, refer to the *AOS Command Reference Guide* available at https://supportforums.adtran.com.
- It is recommended that your browser's cache be cleared before viewing the GUI after an upgrade.

Features and Enhancements

This section highlights the major Switch specific features, commands, and behavioral changes in products running AOS version R11.2.0.

- Added hardware ACL support for the second and third generation NetVanta 123X switches.

Fixes

This section highlights major bug fixes for all products running AOS version R11.2.0.

- If both **no enable password** and **aaa authentication enable default enable** were present in a configuration using AAA, a console user would be able to elevate to privilege level 7 by entering anything when prompted for the enable password. This issue only affected AOS versions R11.1.0 and R11.1.1.
- If a AAA authentication banner was configured, it did not display over SSH. Instead the login banner (if configured) was displayed.
- If the **absolute-path** on a HTTP request probe contained a ?, the ? was lost when the unit was rebooted.
- If an SNMPv3 group name was configured that matched the name of an existing SNMP community, the SNMPv3 group would not be added to the configuration.
- Heartbeat support was disabled in OpenSSL in order to address security concerns related to CVE-2014-0160, also known as Heartbleed. Only AOS R11.1.0 and R11.1.1 were susceptible to this issue.
- In R10.9.0 and higher, if a **name error** response was received on an A or AAAA DNS query, the configured domain name was appended repeatedly, resulting in constant DNS queries.
- Issuing certain **privilege configterminal all** commands caused the AOS device to reboot.
- It was not possible to issue the **shutdown** or **no shutdown** commands for a track from within the weighted list configuration mode.
- If the power was cycled on a unit while regenerating an SSH key, the key could become corrupted, causing the unit reboot when a user tried to connect via SSH.
- It was not possible to update the authentication parameters of a configured SNMP user without first removing the user.

- If two CLI Privilege level commands are configured with the **all** keyword, only the least specific of the two commands will take effect. For example, with the following configuration all **show ip** commands would inadvertently be set to level 7:

  privilege exec all level 7 show

  privilege exec all level 6 show ip
- When TACACS+ accounting was enabled, it was possible for a long duration brute force SSH attack to cause the unit to run out of memory and reboot.
- If a VAP reference statement was configured on a dot11ap interface, that configuration would be lost when the unit was rebooted.
- If an SSH client that performs key re-exchange was being used, when a re-exchange was attempted the SSH session would become unresponsive.
- SSH sessions to an AOS device that did not progress beyond the authentication in progress state could not be cleared without a reboot.
- Executing a Tcl script that issues the command **show tech** inhibited the ability to run future **show tech** commands until the AOS device was rebooted.
- When AAA command authorization was enabled, issuing a show command with the **realtime** parameter did not result in viewing statistics in real time.
- When configured for t**erminal length 0** certain **show** commands did not provide complete output.

This section highlights the Switch specific bug fixes in products running AOS version R11.2.0.

- When exposed to IGMP traffic with IGMP snooping enabled, the NetVanta 1531 would reboot.
- When exposed to IGMP traffic with IGMP snooping enabled, a memory leak resulted which would eventually lead to the switch running out of memory and rebooting.
- If switchports 1 through 4 on the NetVanta 1235P were configured for ActivReach, the corresponding Gigabit Ethernet port with the same number would bounce periodically.
- In the GUI, if an EPS was not connected, an AOS switch would indicate the EPS fan status was unknown.
- The GUI interface of certain AOS switches would incorrectly show an EPS section, even if that switch did not support an EPS.
- In rare cases, certain AOS switches erroneously indicated that they had rebooted with a core dump when the unit had not actually rebooted due to a software issue.

Errata

The following is a list of errata that still exist in all products running AOS version R11.2.0.

- Configuring a NetVanta 160's channel setting to **least-congested** may not properly adjust to the least congested channel available.
- The **show interface dot11ap** <*number*> command may show an incorrect radio channel for a NetVanta 160.
- Copying a file larger than 20 MB from the flash memory of an AOS device via HTTP can cause the AOS device to reboot.
- The GUI of a NetVanta device acting as a wireless access controller can not display the software currently running on a connected access point.

- An AOS device may print an event message in the CLI reporting a successful NetVanta 160 software upgrade, even if the upgrade has failed.
- The command **boot config flash** <*filename*> does not function properly on many AOS platforms.
- A hostname entry in an ACL may fail to resolve to the correct IP address even though the AOS device's host table reflects the correct IP address. Workaround: Use IP addresses instead of hostnames when creating an ACL.
- Event messages indicating a firmware upgrade was attempted may appear in the AOS event log for NetVanta 160 APs that are not being upgraded.
- Having more than two entries in a Network Monitor ICMP probe test list displays **Tracked by: Nothing** in the **show probe** command output. This is only a display error; the probes still function correctly.
- Wi-Fi multimedia (WMM), configured with the command **qos-mode wmm**, does not function properly on NetVanta 150 Access Points.
- WEP encryption does not function properly on NetVanta 160s.
- The current AOS implementation of DHCP message construction may result in Windows XP machines not adopting the DNS servers defined in the DHCP Offer. A workaround using a numbered IP/hex option will allow the message to be constructed in a manner that Windows XP will accept. Microsoft also offers a hotfix to resolve this Windows issue.
- The **vap-reference** command will not replicate VLAN IDs for an AP unless 802.1q encapsulation has been manually enabled on the AP expecting to receive the replicated configuration.
- A large enough drift in the system clock can cause an error when the NTP server attempts to synchronize.
- The GUI does not produce an error when VLANs are selected for a particular VAP when encapsulation 802.1q is not enabled.
- EAP Identity responses from a wireless client that do not contain an Identity field can result in a malformed RADIUS packet created by the NetVanta 150.
- NetVanta 150s might not properly handle immediate Access-Accept responses to Access-Request messages.
- The name of a deleted IPv4 ACL cannot be used to name a new IPv6 ACL.
- The pass phrase for the Wireless Wizard does not persist across reboots.

The following is a list of Switch specific errata that exist in products running AOS version R11.2.0.

- When running R11.1.0 bootrom on a NetVanta 1531 and attempting to apply a backup firmware image from bootstrap, the switch will print out benign errors indicating packets are being dropped due to congestion.
- The ActivChassis feature can only be disabled via the CLI.
- Creating a hardware ACL with the same name as a previously created and deleted IP ACL will result in the creation of an IP ACL with an implicit permit.
- Removing port channels from the configuration of an ActivChassis device while under a heavy load can cause the ActivChassis device to reboot.
- When configured with two port channels, each with greater than two members, one of the port channels may not evenly distribute traffic sent over the aggregated link.
- A NetVanta 1638 will occasionally print out the following message on boot **HTTP_CLIENT CONNECT_TO_HTTP_SERVER errorCode 251**. This does not cause a functional problem.

- Legacy switch stacking cannot be configured if VLAN 2386 is created prior to enabling stacking.
- An ActivChassis stack is not able to pass 10 Gb of 64 byte frames over a single 10 Gb fiber link in an SFP+ XIM.
- A standard MAC ACL can be created with the same name as an existing extended MAC ACL.
- If a line card has the same VCID as another line card, it cannot be added to the ActivChassis stack, and output from the show ac detail command does not adequately point out the reason for the failure.
- On NetVanta 1638s in ActivChassis mode, spanning tree will reconverge at non-rapid spanning tree rates (about 30 seconds) if there are spanning tree topology changes in the network.
- The NetVanta 1638 cannot boot from a firmware image stored on a connected USB drive.
- If an ActivChassis line card has NetVanta APs physically attached, and the line card is removed and re-added to the ActivChassis stack, the NetVanta APs will not properly indicate the AC controlling them. Bouncing the switchport on the line card or rebooting the ActivChassis master will resolve this issue.
- When a switchport on a NetVanta 1535P is running forced speed 100 Mbps in standard mode (not ActivReach mode), jumbo frames with size greater than 9000 bytes will be dropped.
- The chassis fans in NetVanta 1544F switches oscillate at a higher frequency than expected during a period where the switch is not being heavily utilized.
- NetVanta 1500 and NetVanta 1600 Series switches may not properly prioritize traffic across port channels.
- Certain OIDs in the Bridge-MIB may not return a value on AOS switches.
- L3 switch statistics incorrectly report forwarded frames when subjected to a traffic stream consisting of invalid IPv4 header checksum values. The frames are properly dropped by the switch, but the statistics counter erroneously reports frames being forwarded.
- A VLAN interface for a VLAN that is not accessed by other switchports will not be advertised by GVRP.
- Switch platforms count input discards on the ingress interface when receiving 802.3x pause frames.
- In certain instances, an SFP port on a NetVanta 1544 will not function with RAD MiRiCi-E3T3 SFPs.
- Port mirroring on a NetVanta 1544 switch may not mirror traffic in both directions.
- The L3 Switch Header Error and Discard counters on the NetVanta 1544P (second generation) do not increment.
- Booting a second generation NetVanta 1534 or a NetVanta 1535P that is acting as an access controller for more than 20 directly connected NetVanta 160 Access Points can cause some of the Access Points to pull incomplete configuration data from the NetVanta switch.

Upgrade Instructions

Upgrading ADTRAN products to the latest version of AOS firmware is explained in detail in the configuration guide *Upgrading Firmware in AOS*, available at https://supportforums.adtran.com.

Documentation Updates

The following documents were updated or newly released for AOS version R11.2.0 or later specifically for the AOS products. 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.

- *AOS Command Reference Guide*
- *Configuring Hardware ACLs in AOS*
- *Configuring Network Monitor in AOS*
- *Configuring Network Quality Monitoring in AOS*

