RELEASE NOTES

Switch Products
AOS version R11.6.0.SA
April 17, 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

AOS version R11.6.0.SA 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 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 R11.6.0.SA. 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	Minimum Boot ROM
NetVanta 1234/1234P (2nd and 3rd Gen.)	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	17.06.04.00
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 R11.6.0.SA 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 R11.6.0.SA 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 R11.6.0.SA.

- Added guest VLAN functionality, which can be used in an 802.1x environment as a default VLAN for devices that do not support 802.1x.

Fixes

This section highlights major bug fixes for all products running AOS version R11.6.0.SA.

- When running AOS R11.4.2 in some configurations with multiple VAPs, NetVanta 150s could not be controlled.
- In certain cases, NetVanta 150s could not be controlled by devices running AOS R11.4.2.
- Wi-Fi multimedia (WMM), configured with the command **qos-mode wmm**, is not supported on NetVanta 150 Access Points and the configuration commands have been removed.
- During a SNMP denial of service attack, an out of memory reboot may have occurred.
- Resolved a potential lockup when under a SSH denial of service attack with AAA configured.
- If an ECDSA or ED25519 key (both of which are unsupported) was presented to the SSH server, a **Bad string length** error was returned instead of proceeding with the remaining authentication options.
- Unsupported SSH authentication methods (e.g., null) were improperly treated as authentication failures instead of unsupported methods.
- The WEP configuration options were removed for the NetVanta 160 Access Points.
- Application of a MAC ACL to an access point did not persist through reboot.
- When connecting to a unit with SSH, if a long login banner was configured the **--MORE--** prompt was presented.
- New temporary DH key pairs were not generated for each TLS connection when using DHE ciphers with the HTTPS server, SMTP client, Auto-Link client, Auto Config client, HTTPS packet capture export, and the **copy https** command.

- Issuing the **test if interface switchport** <*slot/port*> or the **test if interface xgigabit-switchport** <*slot/port*> commands on a track resulted in a reboot. These commands are invalid without the **line-protocol** parameter at the end (e.g., **test if interface switchport** <*slot/port*> **line-protocol**).
- SnmpEngineboots was not incremented on a hard reboot.
- An AOS configuration file larger than 256 KB could not be backed up to n-Command MSP.
- To address the SSL 3.0 POODLE vulnerability, SSL 3.0 has been disabled by default for the HTTPS server, SMTP client, Auto-Link client, Auto Config client, HTTPS packet capture export, and the **copy https** command. To enable SSL 3.0 support, an **allow-sslv3** parameter has been added to all of these clients and servers, with the exception of Auto-Link.

  Additionally, SSL 2.0 has been disabled in all of the previously mentioned clients. It was already disabled by default for the HTTPS server.
- When accessing the GUI using HTTPS, cookies were sent without the **secure** attribute set.
- SNMP communities containing the @ character were not accepted on products with switchports.
- The following OpenSSL security vulnerabilities were resolved:

  SSL/TLS MITM vulnerability (CVE-2014-0224)

  Anonymous ECDH denial of service (CVE-2014-3470)

  Information leak in pretty printing functions (CVE-2014-3508)

  Crash with SRP ciphersuite in Server Hello message (CVE-2014-5139)

  Race condition in ssl_parse_serverhello_tlsext (CVE-2014-3509)

  OpenSSL TLS protocol downgrade attack (CVE-2014-3511)

  ECDHE silently downgrades to ECDH [Client] (CVE-2014-3572)

  RSA silently downgrades to EXPORT_RSA [Client] (CVE-2015-0204)

  Bignum squaring may produce incorrect results (CVE-2014-3570)
- Rebooting a NetVanta 160 after editing an associated MAC access list caused the AP to transmit SSID **Wireless11**.
- The formatting of LLDP debug was improved to make it easier to read and consistent with other AOS debugs.
- The show interface dot11ap <number> command may have shown an incorrect radio channel for a NetVanta 160.
- The GUI of a NetVanta device acting as a wireless access controller could not display the software currently running on a connected access point.
- An AOS device displayed an event message in the CLI reporting a successful NetVanta 160 software upgrade, even if the upgrade had failed.
- The command **boot config flash** <*filename*> did not function properly on many AOS platforms.
- In some cases, a host name entry in an ACL failed to resolve to the correct IP address even though the router's host table reflected the correct IP address.
- The GUI did not produce an error when VLANs are selected for a particular VAP when encapsulation 802.1q was not enabled.

This section highlights the Switch specific bug fixes in products running AOS version R11.6.0.SA.

- In rare cases, an ActivChassis line card VLAN became out of sync causing loss of connectivity on that network.
- VRRP did not function properly on VLAN interfaces configured for IGMP Snooping.
- When an ActivChassis master or backup reset separately from ActivChassis line cards, traffic destined for MAC addresses not currently in the MAC table of the ActivChassis were not properly broadcast out 10 gigabit uplink interfaces on the line cards.
- In rare circumstances, if a line card was disconnected from an ActivChassis, when it reconnected to the ActivChassis, it did not receive its configuration from the ActivChassis master.
- Receiving a flood of multicast traffic prevented the NetVanta 1531 from responding to management traffic, even from the console interface.
- Files with file names greater than 32 characters in length were accepted and written to flash memory on NetVanta switch products even though the files had not been read correctly.
- The ActivChassis feature could only be disabled using the CLI.

Errata

The following is a list of errata that still exist in all products running AOS version R11.6.0.SA.

- After configuring the privilege level of exec commands, those commands will not be set to the proper privilege level unless the configuration is saved and the unit rebooted or any **no privilege** command is issued.
- Copying a file larger than 16 MB from flash memory of an AOS device via HTTP/HTTPS (including using Auto-Link) will fail.
- In some command sets, the **exit** command is not visible even though it still functions properly.
- Configuring a NetVanta 160's channel setting to **least-congested** may not properly adjust to the least congested channel available.
- 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 will display **Tracked by: Nothing** in the **show probe** command output. This is merely a display error; the probes still function correctly.
- Accessing the GUI via HTTPS may be slow.
- The current AOS implementation of DHCP message construction can result in Windows XP machines not adopting the DNS servers defined within 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.
- EAP Identity Responses from a wireless client that do not contain an Identity field can result in the NetVanta 150 creating a malformed RADIUS packet.

- NetVanta 150s may 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 R11.6.0.SA.

- A switchport cannot be disabled by clearing the Enabled check box in the GUI.
- Hardware access lists cannot be used to block traffic destined for the management interface of a NetVanta 1638.
- In certain cases, NetVanta 160s using NetVanta 1238Ps as access controllers may not receive their full configuration when booted. Restarting AWCP and rebooting the NetVanta 160s resolves the issue.
- Traffic destined for devices that match static ARP entries in a Layer 3 switch will experience extra latency if a static MAC entry is not present for the same device.
- ICMP responses from a VLAN interface on the NetVanta 1531 may be periodically latent. ICMP routed or switched through the unit is not affected.
- When running R11.1.0 boot ROM 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.
- 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 while an ActivChassis is under a heavy load could cause the ActivChassis 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 when booting: **HTTP_CLIENT CONNECT_TO_HTTP_SERVER errorCode 251**. This does not cause a functional problem.
- 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 **show ac detail** command does not adequately point out the reason for this 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 added back to the ActivChassis stack, the NetVanta APs will not properly indicate the AC that controls them. Bouncing the switchport on the line card or rebooting the ActivChassis master will resolve this issue.
- Legacy switch stacking cannot be configured if VLAN 2386 is created prior to enabling stacking.
- 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 are dropped.

- The chassis fans in NetVanta 1544F switches oscillate at a higher frequency than expected during a period when the switch is not being heavily utilized.
- NetVanta 1500 and 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.
- Port mirroring on a NetVanta 1544 switch might not mirror traffic in both directions.
- The L3 Switch Header Error and Discard counters on the NetVanta 1544P (second generation) do not increment.

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 R11.6.0.SA 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*
- *Carrier Ethernet Services in AOS*
- *SNMP in AOS*
- *Configuring Ethernet OAM for Y.1731*
- *Configuring SIP Proxy in AOS*

