RELEASE NOTES

AOS Converged Access
AOS version R11.4.4
July 24, 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 R11.4.4 is a maintenance release that 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 15*.

A list of new or updated documents for this release appears in *Documentation Updates on page 21*.

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 R11.4.4. 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	Enhanced Feature Pack	SBC Feature Pack	Minimum Boot ROM
NetVanta 644		√		A5.01.B1
NetVanta 1335		√		15.01.00
NetVanta 3120		√		14.04.00
NetVanta 3130		√		14.04.00
NetVanta 3200/3205 (3rd Gen. only)	√	√		17.02.01.00
NetVanta 3305 (2nd Gen. only)	√	√		04.02.00
NetVanta 3430	√	√		13.03.SB
NetVanta 3430 (2nd Gen.)	√	√	√	17.05.01.00
NetVanta 3448	√	√	√	13.03.SB
NetVanta 3450	√	√		17.06.01.00
NetVanta 3458	√	√		17.06.01.00
NetVanta 4305 (2nd Gen. only)	√	√		08.01.00
NetVanta 4430	√	√	√	17.04.01.00
NetVanta 4660		√		R10.10.0
NetVanta 5305	√	√		11.03.00
NetVanta 5660		√		R11.4.0
NetVanta 6240		√	√	A5.01.00
NetVanta 6250		√	√	R10.9.0
NetVanta 6310/6330		√	√	A3.01.B2
NetVanta 6355		√	√	14.06.00
NetVanta 6360		√		R11.2.0
NetVanta 6410			√	R11.3.0

Platform	Standard Feature Pack	Enhanced Feature Pack	SBC Feature Pack	Minimum Boot ROM
Total Access 900 Series (2nd Gen. only)		√		14.04.00
Total Access 900e Series (2nd Gen. only)		√	√	14.05.00.SA
Total Access 900e Series (3rd Gen. only)		√	√	R10.9.0

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 R11.4.4 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 R11.4.4 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.
- MGCP is not supported on the NetVanta 6360.

Features and Enhancements

This section highlights the major features, commands, and behavioral changes for all Converged Access products running AOS version R11.4.0.

- Added packets matched, bytes matched, and offered rate counters for all ingress and egress QoS maps.
- Added the ability to configure the IPv4 and IPv6 firewalls to only apply to traffic destined to the unit itself on a per VRF basis. When the firewall is enabled with the **local-traffic-only** parameter, the firewall will not inspect traffic flowing through the unit.
- Added the ability to set route tags in routing protocols and route maps.
- Added IPv6 MLD listener functionality to AOS. No configuration is necessary to enable this feature.
- Added OSPF distribute lists to filter prefixes redistributed out of OSPF and to prevent routes learned by OSPF from being used in the route table or redistributed into other routing protocols.
- Added the ability to restrict the functionality available in bootcode on the NetVanta 3140, 3430 (second generation), 3448, 4660, 5660, 6250, 6360, and Total Access 900e (third generation). When enabled, the following operations are disabled: bypassing passwords, bypassing the startup configuration, erasing individual files, overwriting files, and copying files from flash memory. Use of this feature also requires a bootcode upgrade.
- Added the ability to run syslog in a named VRF instead of the default (unnamed)VRF.

This section highlights the Carrier Ethernet specific features, commands, and behavioral changes available in products running AOS version R11.4.0.

- Added the ability to automatically detect and switch between EFM bonded and non-bonded mode on the SHDSL Carrier Ethernet modules by configuring **bonding auto-detect** on the EFM group interface.

Fixes

This section highlights major bug fixes for all products running AOS version R11.4.4.

- In some cases, when issuing the **show dot11 access-point detail** command, a reboot occurred.
- Rather than immediately transitioning to stale, IPv6 ND cache entries will now stay at the reachable priority while ND cache entries are being reclaimed. This change helps prevent ND cache entries that are actively being used from getting reclaimed when they transition to the stale state.
- When using SSH and logging in as a user with a configured privilege level, the terminal length would set to 0.
- Due to changes made in R10.9.3, AOS was only able to process 3 unicast ARP requests per second.
- In rare cases, LCP going down on a link in a MLPPP bundle caused a reboot.
- Errors were displayed when the **no shutdown** command in EVC configurations was restored while booting a NetVanta 6310 or 6330.
- After configuring the privilege level of exec commands, those commands would not be set to the proper privilege level unless the configuration was saved and the unit rebooted or any **no privilege** command was issued.
- A received ARP request with a sender IP address of 0.0.0.0 (defined as an ARP Probe in RFC 5227) resulted in an ARP cache entry that would not be removed. This entry will no longer get created.
- In rare cases, a reboot occurred when performing a traceroute.
- Some sectors on flash may have been written excessively, causing premature wear and potentially preventing the unit from booting. This issue has been addressed and a refresh mechanism has been added to address any issues with premature wear.
- If VPN failover occured in a GRE over IPsec VPN configuration, the GRE tunnel may have remained down after the VPN failover occurred.
- If an LLDP neighbor was configured with multiple management address (i.e. IPv4 and IPv6), issuing the command **show lldp neighbor detail** caused the unit to lock up.
- When under 100 percent CPU load continuously for multiple days, a reboot may have occurred on the NetVanta 4660 and 5660.

This section highlights major bug fixes for all products running AOS version R11.4.3.

- If an IPv6 ND prefix on an interface had been generated from a named prefix, a reboot would occur if the **no ipv6** command was issued on the interface before the ND prefix generated from the named prefix was removed.
- On the NetVanta 3140, 4660, 5660, 6250, 6360 and Total Access 900e (third generation), issuing the **show ip flow top-talker hour detail** command may have resulted in a reboot.
- When running AOS R11.4.2 in certain 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.

- In very rare cases, a reboot would occur when PPP was coming up.
- When rebooting a NetVanta 6310 or 6330 running AOS R11.4.2, the connection between an EVC and the EFM group could not be restored. An error stating **%Error finding interface efm-group 1** was displayed and the EVC was non-functional due to the missing connection to the EFM group.
- During a SNMP denial of service attack, an out of memory reboot may have occurred.
- 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.
- Exporting a packet capture to flash memory resulted in audio loss while the file was being written.
- When attempting to view the Physical Interfaces page in the GUI of a NetVanta 5305 with a DS3 module installed, a 503 Service Unavailable error was presented to the user.
- In rare cases, DNS queries created by an AOS device were sent using a source port that was already in use by another local service (e.g., SIP), which prevented DNS responses from being properly received.
- On the NetVanta 6410, a cold boot resulted in a warm start SNMP trap being sent.
- In certain cases, a NULL value was reported for various statistics on NetVanta 3120, 3130, 3448, and 3458 switchports when viewed through the GUI.
- When accessing the GUI using HTTPS, cookies were sent without the **secure** attribute set.
- Rebooting a NetVanta 160 after editing an associated MAC access list caused the AP to transmit SSID **Wireless11**.
- The VLAN ID for an access point could not be changed using the GUI.

This section highlights major bug fixes for all products running AOS version 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.
- On the NetVanta 3120, 3130, 3448, and 3458, when traffic was flowing over one port in a channel group, if that port went down, the port channel would bounce.
- On the NetVanta 3120, 3130, 3448, and 3458, removing and then re-adding ports to a port channel resulted in frames being looped between those ports.
- 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.
- On the NetVanta 6310 and 6330 with an EFM module installed, the output of the **show mef evc-map** command improperly listed **MEN C-tag** and **MEN C-tag Pri** values. The NetVanta 6310 and 6330 do not support adding a C-tag.
- On the NetVanta 6310 and 6330 with an EFM module installed, two EVC maps that differed only by the matched DSCP value could not be configured, even though that is a valid configuration.
- 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.

- If a NetVanta 6310 or 6330 with a SHDSL EFM module installed received a malformed version management packet, a reboot may have occurred.
- An AOS configuration file larger than 256 KB could not be backed up to n-Command MSP.
- Crypto FFE was not available on the NetVanta 6250 in R10.10.0 and later.
- If a TFTP transfer was initiated and there was only one free policy session available in the firewall, a reboot occurred.
- When running large amounts of traffic, a reboot occurred if entries were added or removed from an extended ACL that was referenced by a QoS map.
- The NetVanta 644 failed to receive 802.1q tagged packets with an IP payload between 1497 and 1500 bytes.
- To address the SSL 3.0 POODLE vulnerability, SSL 3.0 was 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 was added to all of these clients and servers, with the exception of Auto-Link.

  Additionally, SSL 2.0 was disabled in all of the previously mentioned clients. It was already disabled by default for the HTTPS server.
- Copying a file larger than 16 MB from flash memory of an AOS device via HTTP/HTTPS (including using Auto-Link) caused the AOS device to reboot.
- On the Total Access 900e (third generation) and NetVanta 6250, the SNMP ifDescr was not unique for each of the T1 interfaces.
- If a large number of MAC addresses were learned by the unit, a slow memory leak would occur, resulting in a reboot over time.
- Clicking on the ProCare link in the GUI resulted in a reboot.
- When changing an Ethernet interface from a static IP address to PPPoE, configuring the static IP address on the PPP interface caused a reboot.
- If **no oam-pvc managed** was configured on an ATM subinterface, the PVC would still drop upon receipt of AIS or RDI.
- When viewing the Physical Interfaces page in the GUI on a unit with a T1 configured, a 503 Service Unavailable message was presented.
- If the control source port was changed on a TWAMP responder prior to **no shutdown** being issued on the responder, a reboot occurred.
- SNMP communities containing the @ character were not accepted on products with switchports.
- In rare cases, the unit would get into a state where the flash file system could not be accessed properly until the unit was rebooted.
- The formatting of LLDP debug made it very difficult to read.
- If the IPv4 or IPv6 address in a DNS PTR request matched an IP address assigned to an interface on the device, the DNS proxy responded with a malformed PTR response.
- The **show interface dot11ap** <*number*> command may have shown an incorrect radio channel for a NetVanta 160.
- The GUI of an AOS device acting as a wireless access controller could not display the software currently running on a connected access point.

- An AOS device would print an event message in the CLI reporting a successful NetVanta 160 software upgrade, even if the upgrade had failed.

This section highlights major bug fixes for all products running AOS version R11.4.1.

- On the NetVanta 4660, SFP DMI data did not display properly for some SFPs.
- On the NetVanta 4660, inserting certain SFPs caused the CLI to become sluggish.
- Using certain software packages, compiling AdGenAosCommon.mib resulted in an error.
- If the IPv4 firewall was enabled and a TCP SYN packet was sent to a local port on the router for which no service was listening, the IPv4 firewall would drop the RST-ACK.
- On the Total Access 900e (third generation) and NetVanta 6250, small runt packets without an Ethernet FCS may have caused the 10/100 Ethernet ports to become non-functional. A duplex mismatch was a possible trigger for this issue.
- LLDP was not transmitted out PPP interfaces on the NetVanta 4305 when using the Octal T1 NIM.

This section highlights major bug fixes for all products running AOS version R11.4.0.

- When using the privilege levels feature, some engineering level commands were also made accessible.
- On the NetVanta 4660, 6250, 6360, and Total Access 900e (third generation), flash to flash file copies initiated via the console port would take longer than the same copy initiated via Telnet or SSH.
- Attempting to configure the privilege level for all commands in a command set containing commands without a **no** version resulted in an error.
- The **verify-file** command provided different output when run via the console port than when run via Telnet or SSH.
- If **aaa authentication enable default enable** was configured and no enable password was configured, if you issued the **disable** command followed by the **enable** command you were prompted for the enable password even though no password was configured.
- The **tacacs-server timeout** command had no effect until the TCP session to the TACACS+ server had been established.
- On the Total Access 900e (second generation), Ethernet throughput for small packets decreased moderately compared to R11.2.0.
- If the firmware filename received by auto-config matched the currently applied firmware filename, the auto-config process would restart every 60 seconds.
- When using Auto-Link to connect to n-Command MSP, a slow memory leak occurred.
- Improved the output of the **show ipv6 interface** command to indicate how hosts will get an IPv6 address and other configuration.
- If a firmware transfer from n-Command MSP failed, the partial firmware file was not deleted from the file system.
- On the NetVanta 4660, 6250, and 6360, the laser wavelength was reported incorrectly for certain SFPs.
- On the NetVanta 4660, the hdsl2ShdslEndpointCurrStatus OID in the HDSL2-SHDSL MIB always returned noDefect(0) instead of the correct bitmap.
- The NetVanta 7100 and NetVanta 6355 platforms failed to reset QoS map statistics for applied QoS maps when the **clear counters** command was issued.
- On the NetVanta 4660, 6250, and 6360, the laser temperature was not reported correctly for certain SFPs.

- On the NetVanta 4660, 6250, and 6360, the Gigabit Ethernet Compliance Code was reported incorrectly for some SFPs.
- The parent map QoS statistics had to be cleared in order to clear the child map statistics.
- A specific QoS map entry could not be cleared without the entire map being cleared.
- When a QoS map was applied to a VLAN interface, the NetVanta 3448 and 3458 platforms failed to reset QoS map statistics after the **clear counters** command was issued.

This section highlights the Carrier Ethernet specific bug fixes in products running AOS version R11.4.4.

- The global and per-interface hardware FFE entry limits were increased to 128k. Additionally, optimizations were made to reduce the CPU utilization required to manage the FFE table.
- In rare cases and only on specific units, the NetVanta 4660, 5660, and 6360 cyclically rebooted if a SHDSL module was installed.
- In very rare cases, Gigabit Ethernet interfaces on the NetVanta 4660, 5660, and 6360 became unresponsive until the unit was rebooted.
- The **efm-group** interface type option was missing from the **cross-connect** command on PPP interfaces.

This section highlights the Carrier Ethernet specific bug fixes in products running AOS version R11.4.3.

- When under an IPv6 ping sweep attack, the CLI load protection functionality did not ensure CLI responsiveness.

This section highlights the Carrier Ethernet specific bug fixes in products running AOS version R11.4.2.

- If a queue shaper was created followed by a port shaper and then the port shaper was removed or shut down, removing or shutting down the queue shaper would not function properly.
- Entering an invalid character in a **connect men-port** or **connect uni** statement on an EVC resulted in the EVC not functioning properly.
- On the NetVanta 6360, the **system-management-evc** and **system-control-evc** commands did not function properly.
- In rare cases, a reboot occurred on the NetVanta 4660, NetVanta 5660, and NetVanta 6360.

This section highlights the Carrier Ethernet specific bug fixes in products running AOS version R11.4.1.

- If an IPv6 neighbor solicitation flood was received, it was possible for local management traffic to be disrupted on the system management EVC and the system control EVC.
- Large sub IDs were not handled properly while processing GetNext requests for the adGenAosPerformanceHistory MIB.
- Issuing SNMP GET requests on HDSL2-SHDSL-LINE-MIB::hdsl2Shdsl15MinIntervalTable and HDSL2-SHDSL-LINE-MIB::hdsl2Shdsl1DayIntervalTable did not function properly.
- When accessing the CLI via the console port, a message indicating **Bad EOC Tx Request** may have been seen when a proprietary SHDSL EOC message was received. These messages will now only be seen when **debug interface shdsl-eoc** is enabled.

- The ifMtu for the system control EVC was returned as an unsigned integer instead of a signed integer as required by RFC 2863.
- The LLDP command set was missing from EFM group subinterfaces.

This section highlights the Carrier Ethernet specific bug fixes in products running AOS version R11.4.0.

- In rare cases, a reboot occurred when a VDSL Carrier Ethernet module was installed and the unit was under high CPU load.
- The **efm-group** interface type option was missing from the **show ip interface** command.
- The system management and system control EVCs would show an EVC Status of Running, even if all of the required attributes were not configured.
- On the NetVanta 4660, the following ifTable and ifXTable issues were present:

  ifTable:

  - ifSpeed was incorrectly reported for SHDSL interfaces when an interface was shut down. 5696000 was reported for the speed instead of 0.
  - ifSpeed was incorrectly reported for the system control EVC when the interface was shut down. 10000000 was reported for the speed instead of 0.
  - ifPhysAddress was not reported for the EFM group interface.
  - ifSpeed for EFM group subinterfaces was incorrectly reported when one or more SHDSL links that were a member of the group were down.

  ifXTable:

  - ifHighSpeed was incorrectly reported for SHDSL interfaces when an interface was down. 6 was reported instead of 0.
  - ifHighSpeed was incorrectly reported for the system control EVC when the interface was shut down. 10 was reported instead of 0.
  - ifHighSpeed for EFM group subinterfaces was incorrectly reported when one or more SHDSL links that were a member of the group were down.

This section highlights the Voice specific bug fixes in products running AOS version R11.4.4.

- If the configured value of the **max-number-calls** command on a SIP trunk was reached, any additional INVITEs would not receive a response if the Request-URI of the INVITE was an FQDN that matched the domain configured on the SIP trunk and that domain was not resolvable via DNS, or the domain resolved to an IP address that was not local to the unit.
- With **voice conferencing-mode** set to the default value of **network**, if two calls originating from a single analog phone were established across the same non-SIP trunk, a reboot occurred when a hook flash occurred. Features such as conferencing are not supported for analog users on calls that do not egress a SIP trunk.
- In rare cases, the use of the SIP proxy monitor feature resulted in a reboot.
- When assigning an FXO port to an analog trunk in the GUI, a 503 Service Unavailable response was returned.

- Only the user, host, and port were preserved from the Contact URI in the 200 OK response to the conferencing URI INVITE request and sent in the subsequent Refer-To header in the REFERs send to finalize the network conference.
- If the SIP proxy transmitted a NOTIFY to a device behind the proxy and that device never responded, some resources were not properly cleared, resulting in a SIP resource leak.
- In rare cases, when near simultaneous inbound calls were received from SIP and ISDN trunks and the call on the ISDN side backed off, a reboot occurred.

This section highlights the Voice specific bug fixes in products running AOS version R11.4.3.

- When running AOS R11.4.2, the local conferencing feature did not work.
- If a caller ID name longer than 256 characters was placed into a P-Asserted-Identity header, a reboot occurred.
- When a call was placed on hold by an analog user and then retrieved, an RTP resource may have been leaked.
- When using media anchoring, the correct DSCP value was not applied to the anchored RTP packets.
- If an INVITE was received that had a caller ID name 158 characters or longer and debug was enabled, a reboot occurred.
- In rare cases, a reboot occurred while the SIP proxy was processing a SIP message.
- Changing the default authentication credentials on a SIP voice trunk caused all configured users to re-register twice instead of only once.
- When using T.38, if a page transmission lasted longer than the configured value of **ip rtp session timeout** (45 seconds by default) and a reINVITE was received, the fax failed.
- When an FXS port was configured to use ground start and an inbound call rang but was not answered, the FXS port would not ground the tip again or send ring voltage on future calls.
- In AOS R11.4.2, dial tone detection on FXO ports failed on the NetVanta 6250, 6360, and Total Access 900e (third generation).
- If a TDM-to-SIP call was in a PreConnected state due to receiving 183 Session Progress message, audio would only flow in the SIP-to-TDM direction, which prevented interaction with some IVRs and voicemail systems.
- The **rtp media** command set on SIP trunks was not present on the NetVanta 3430, 3448, 4430, and 6410 SBCs.
- When an ISDN timeout occurred on a SIP-to-ISDN call, the unit sent a 400 Bad Request response instead of the more appropriate 408 Request Timeout response.
- If media anchoring was being used on a call that received multiple reINVITEs, the ports listed in SDP may have changed without incrementing the sess-version.
- The SIP packet capture functionality was modified so that calls are only be tracked when the packet capture is both enabled and attached to at least one interface.
- On the NetVanta 6250, 6360, and Total Access 900e (third generation) if a call negotiated to a 40 ms packetization period, which is not supported on those platforms, a reboot occurred when processing in-call DTMF.
- Calls initiated via a loopback account could not be placed if they matched a dial plan entry that ended in **$**.

- If a **conferencing-uri** was configured on a voice trunk, AOS would attempt to resolve the configured value via DNS.
- On a SIP trunk to SIP trunk call, if a SIP 488 response was received on one trunk, that response was not sent out the other trunk. Instead a 400 Bad Request response was sent out the other trunk.
- In certain call transfer scenarios where the IP PBX tried to remove itself from the RTP path and then reinsert itself, a no audio condition resulted.

This section highlights the Voice specific bug fixes in products running AOS version R11.4.2.

- The **t38 cng-relay-selective** command did not function properly on the NetVanta 6250, 6360, or Total Access 900e (third generation).
- In rare cases, a response received by the SIP proxy caused a reboot.
- Receiving early media SDP on a call that resulted in hairpin media and also required DTMF transcoding resulted in the call failing to connect and being torn down immediately.
- The LocalURI and RemoteURI fields in VQM PUBLISH messages were reversed for calls in the SIP to TDM direction.
- On the NetVanta 6250, 6360, and Total Access 900e (third generation), DTMF tones that were shorter than the minimum valid digit requirement were being qualified as valid digits.
- When using RTP firewall traversal, if the SIP device behind the AOS unit changed RTP ports in SDP and was slow to actually start using the new ports, the NAT session for the new RTP stream may have been unexpectedly removed. The **ip rtp firewall-traversal enforce-symmetric-port** command has been added to help in this scenario.
- The firmware image for the NetVanta 6410 did not include the .wav files for US ringback and silence that are included by default on the SBC products.
- After the first 18x provisional response was received on a SIP trunk call through the B2BUA, if additional 18x provisional responses were received, they were not relayed to another SIP or ISDN trunk.
- When **snmp trap registration** was configured on a SIP voice trunk, a small amount of memory would leak on each successful SIP registration, eventually resulting in a reboot.
- With transcoding enabled, if a SIP-to-SIP call through the B2BUA that originally did not require transcoding was reINVITEd to a CODEC that required transcoding, and was then reINVITEd again, the transcoding media anchoring session may not have been removed, resulting in two RTP streams being transmitted.
- The GUI allowed the SNMP link status traps to be enabled and disabled for FXS and FXO interfaces, but the changes could not be saved.
- When using SIP proxy user templates, in some cases the Request-URI of inbound INVITEs was improperly modified.
- When using the SIP proxy, if a Remote-Party-ID header was improperly formatted, the SIP message containing the header was not proxied.
- In R11.3.0, R11.4.0, and R11.4.1, if early media SDP was received in a 18x provisional response and the 200 OK didn't contain SDP, one-way audio occurred.
- With a high call rate and **modem-passthrough** enabled, it was possible to see SIP to ISDN call failures even though B channels were available on the ISDN trunks.
- When **voice transfer-mode local** was configured, if a REFER was received that resulted in an INVITE going back out the same trunk, headers specified in the Refer-To header of the REFER were lost.

- In rare cases when using the SIP proxy, some SIP requests were routed to the wrong target.
- When using VQM reporter, the Gap Duration (GD) reported in the BurstGapLoss values could be greater than 3,600,000, which is the maximum value allowed by RFC 6035.
- Under certain conditions when an FXS port was taken off-hook while in the ringing state, ring voltage would continue to be applied to the port leading to degraded call quality and the FXS port going into fault protection.
- Received SDP offers containing a rejected audio media stream and an image media stream were not handled properly. In this scenario, the audio media was preferred and the image media was ignored resulting in erroneous behavior.
- When generating an SNMP trap for a SIP proxy rollover, the wrong OID was used for adSipProxyRollover.
- When using MGCP, receiving caller ID information in a MDCX caused caller ID to malfunction on that port until the unit was rebooted.
- In rare cases, a reboot occurred while using the SIP proxy.
- Removing a voice trunk would remove the password from all **sip-identity** statements that referenced that trunk.
- On the NetVanta 6250 and Total Access 900e (third generation) with MGCP configured, harmless pthread messages were seen on the console during boot up. They were also seen when adding or deleting IP routes that caused the MGCP endpoints to restart.
- Within either a voice trunk or voice user with a CODEC list configured, entering **no codec-list** <*list name*> <*direction*> always removed the <*list name*>, no matter what the configured direction actually was.

This section highlights the Voice specific bug fixes in products running AOS version R11.4.1.

- When using the SIP proxy, the order of parameters inside the **uri** parameter of an Authorization header may have been changed, invalidating the hashed response.
- If an emergency call failed and was automatically retried, the INVITE for the retry did not contain a SDP offer, which prevented early media from being sent.
- When configured, the **conferencing-uri** was used for the Request-URI, From, and To hosts instead of the Request-URI and To users.
- When using TCP for a SIP trunk, if the port in the Via header differed from the port in the Contact header, the port from the Via header was improperly used as the Layer 3 destination for new requests.

This section highlights the Voice specific bug fixes in products running AOS version R11.4.0.

- In rare cases, if an ISDN call with overlap dialing was abandoned very quickly, a reboot would occur.
- Issuing the **show rtp media sessions** command repeatedly resulted in a memory leak.
- When configured with a user role PRI, if the local exchange sent progress indicator #2 (PI2) to indicate the presence of inband audible ringback on a SIP to PRI call, a 183 Session Progress with SDP was not sent on the SIP call leg.
- When two calls formed a TDM hairpin, if one or both of the calls were set up with sendonly or recvonly media, two-way audio would not be established when the hairpin connected.

- On the Total Access 900e (third generation) and NetVanta 6250, if an FXS port was hung up from a FXS to PRI call while a call waiting beep was being played, future calls on that PRI channel may have failed to connect properly.
- The **sip proxy sip-server rollover service-unavailable-or-timeout** command did not result in a server rollover when a 503 Service Unavailable was received in response to a REGISTER.
- On the NetVanta 644, if a 302 Moved Temporarily was received that resulted in a TDM hairpin call, an ISDN CONNECT would not be sent on the original inbound call if inband call progress tones were provided on the outbound call resulting from the 302.
- When using T.38, outbound faxes that took longer than 60 seconds for a page to be transmitted would fail.
- Outbound messages from some templated SIP proxy users were not routed correctly if the user was set up from an inbound request and the outbound contact user was different.
- In rare cases, the NetVanta 644 rebooted if a PRI interface went down and came back up in quick succession.
- On the Total Access 900e Series (third generation), NetVanta 6250 Series, and NetVanta 6360, it was possible for the unit to reboot if PLC was enabled on a user or trunk configured for G.711.

Errata

The following is a list of errata that still exist in all products running AOS version R11.4.4.

- When using the packet capture feature, up to double the memory specified by the **max-memory-usage** command may be used.
- On the NetVanta 6410, HTTP file transfers to the unit's flash memory can be up to 10 times slower than TFTP.
- If a track is configured to monitor the line protocol of an interface configured for 802.1q, the track will never go into a passing state even the interface is up. This issue does not affect the NetVanta 4660, 5660, or 6360. **Workaround:** Track the line protocol of the subinterface.
- When using the **show interface ppp 1 realtime** command, the input and output rates can be incorrect if **statistics rate-interval** is set to a value that is not divisible by 60.
- On the NetVanta 6310 and 6330, when a SHDSL ATM or SHDSL EFM module is installed, the **show interface shdsl x/1** command is missing.
- Copying a file larger than 16 MB from flash memory of an AOS device via HTTP/HTTPS (including using Auto-Link) will fail.
- The AOS TWAMP implementation does not comply with the RFC with regard to the token length of the SetupResponse message, which may cause interoperability issues with other vendors.
- In some command sets, the **exit** command is not visible even though it still functions properly.
- On the NetVanta 5305, VPN performance for 64 and 256 byte packets decreased moderately compared to R11.2.0.
- In certain cases, the **show interface t1 0/1 performance-statistics Total-24-hour** command will not display the actual totals for the performance intervals. The correct values are displayed in the GUI.
- Speed and duplex settings are displayed with on MEF Ethernet interfaces in **show running-config verbose** command output, even though those options are not valid and cannot be configured for that type of interface.

- In the VQM RTP Monitoring menu, the refresh button refreshes the displayed graphic, but it also duplicates information in the lower part of the menu. In addition, when the cursor hovers over a data point, multiple instances of the same data display.
- In the VQM RTP Monitoring menu, the Source IPs and Interfaces menus have invisible data points that appear and display data when the cursor hovers over them. The invisible data point information duplicates a visible data point and can usually be found hidden above the visible data point.
- On the NetVanta 3430, the setup wizard in the GUI may become unresponsive with a Please Wait message.
- The output of **show qos map interface <interface>** shows **ce-vlan-id** instead of **vlan-id** and **ce-vlan-pri** instead of **cos** on products other than the NetVanta 4660.
- On the NetVanta 6240, SNMP traps for warm start and cold start are reversed.
- On a NetVanta 4430, information for an inserted SFP does not display correctly.
- Ethernet interfaces in third generation Total Access 900e units are not visible in the Data > IP Interfaces GUI menu. These interfaces are visible and can be configured from the System > Physical Interfaces menu instead.
- Configuring a NetVanta 160's channel setting to **least-congested** may not properly adjust to the least congested channel available.
- The Total Access 900e (third generation) and NetVanta 6250 send a cold start SNMP trap on reload instead of a warm start trap.
- On the NetVanta 6250 and Total Access 900e Series (third generation), when running a large amount of traffic across a VPN tunnel with crypto FFE disabled, the unit will occasionally reboot citing a memory issue. Enabling the **ip crypto ffe** command prevents this reboot from occurring and is the desired setting when configuring VPN due to the performance increase of the FFE functionality.
- On very rare occasions, port T1 3/3 on an Octal T1 NIM can stop negotiating LCP when it is part of an MLPPP bundle. Rebooting the device will restore the interface.
- On the NetVanta 6310 or 6330, if a SHDSL circuit with a detected bad splice retrains to a different line rate, the distance of the bad splice will display incorrectly.
- On the NetVanta 6310 or 6330, if the top level ATM interface on a SHDSL ATM NIM2 module is disabled and re-enabled, the ATM circuit will no longer be able to pass traffic. The ADTRAN unit must be rebooted to correct the problem.
- When using a T1/E1 EFM NIM2 in the NetVanta 6310 or 6330, the EFM counters do not increment as traffic passes through the device.
- With the SHDSL ATM NIM2, the NetVanta 6310 and 6330 drop approximately 1 out of every 15K packets from the SHDSL to Ethernet direction.
- Removing a USB modem from the USB NIM while active could cause the AOS device to reboot. Shutting down the demand interface being used by the modem prior to removing the modem will prevent this reboot.
- The command **boot config flash** <*filename*> does not function properly on many AOS platforms.
- A host name entry in an ACL may fail to resolve to the correct IP address even though the router's host table reflects the correct IP address. Workaround: Use IP addresses instead of a host name 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 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.
- VQM may show a loopback interface in the GUI when a loopback interface is not configured.
- The VNS verification process does not remove inconsistent A-type records from the host table after the configured number of attempts.
- If the **ethernet-cfm** command is configured on a MEF Ethernet interface, the output of the following CLI commands is not formatted properly:
  1. **show ethernet cfm association**
  2. **show ethernet cfm stack**
  3. **show ethernet cfm mep local**
  4. **show ethernet cfm mep local detail**
- The **called-number** command on a demand interface does not function properly.
- When using XAUTH with a VPN client, an AOS device requests CHAP authentication from the client but does not send a CHAP challenge payload. This can cause issues with VPN clients that expect to receive this payload.
- If a USB modem is physically disconnected from a USB WWAN NIM while active NIM is active, the demand interface being used by the modem will not automatically shut down. The demand interface should be disabled before removing the modem to prevent this issue.
- On the NetVanta 6310/6330, with FFE enabled, passing traffic from the Ethernet 0/1 interface out an Ethernet NIM2 can cause the Ethernet 0/1 interface to fail. The interface is recovered with a reboot. Disabling FFE on the Ethernet 0/1 interface prevents the issue.
- An SNMP walk of the NetVanta 6355 lists the physical address for the first interface index only.
- 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 system clock may drift and lose synchronization with higher stratum devices when NTP is enabled. This issue only affects the NetVanta 3448, 3458, and 6240 products.
- 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.
- Updating PRL values on a Sprint NetVanta 3G NIM may not function properly.
- In rare cases, when an IP PBX and IP phones are both passing through NAT and the SIP proxy on an AOS device, some call flows can enter a one-way audio state. **Workaround**: Enable the **ip rtp firewall-traversal enforce-symmetric-ip** command from the Global Configuration mode.
- A large enough drift in the system clock can cause an error when the NTP server attempts to synchronize.
- On a NetVanta 1335, a switchport that is configured as a port channel cannot change the edge port mode and cannot be changed from a port channel to another configuration using the GUI.
- The **show interfaces** command output for multilink Frame Relay interfaces will display an incorrect available bandwidth value when a physical link residing in the bundle is down.

- The **show atm pvc** counters do not increment.
- The input/output rate counters for a T1 interface are exaggerated for approximately 15 seconds after clearing them.
- The GUI statistics page for the SHDSL interface does not refresh when in 4-wire mode.
- The GUI shows invalid line rate options for a SHDSL interface in 2-wire mode.
- The GUI line rate options for a SHDSL interface do not match those of the CLI.
- Configuring a port channel on a NetVanta 3448 can cause the STP topology to become unstable.
- Sierra Wireless USB305 3G modems are sometimes not recognized by the NetVanta USB WWAN NIM.
- Changing the route metric value using **ipv6 address autoconfig default metric** <*value*> command does not change the administrative distance of the default route.
- The NetVanta 5305 can drop some traffic prioritized by class-based weighted fair queuing (CBWFQ) on a MLPPP interface when a stand-alone QoS map is applied.
- A NetVanta 5305 can stop passing traffic for brief intervals when negotiating frequent VPN tunnels using Diffie Hellman Group 5.
- The output queue statistics on an Ethernet interface can fail to display output queue drops when FIFO is enabled.
- Prioritized traffic can be dropped at a significant rate on PPP interfaces when using a parent QoS map (that references a child map with priority allocation), if the shaped rate is configured for more than 75 percent of the line rate.
- If the **bandwidth remaining percent** command is used in a QoS map, the CLI does not display the correct value for Required Bandwidth in the event message generated by applying a QoS map.
- 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.
- 3G connections using a NetVanta USB WWAN NIM and a Sierra Lightning modem can fail.
- The name of a deleted IPv4 ACL cannot be used to name a new IPv6 ACL.
- The cellular interface can trigger a core dump on a NetVanta 3448 when changing states.
- Browsing to the Switchports menu from the Port Security menu on the NetVanta 1335 WiFi GUI results in a 503 Service Unavailable error.
- A Spanning Tree L2 broadcast storm lasting several hours can cause the NetVanta 1335 to reboot.
- The pass phrase for the Wireless Wizard does not persist across reboots.
- When a switchport on a NetVanta 3458 is configured for **port-security**, it does not receive BPDUs. If multiple connections between the NetVanta 3458 and another switch are made, a switching loop could occur because both ports will automatically enter a forwarding state even though the Spanning Tree protocol should cause one port to enter a blocking state.
- Using the command **debug ethernet cfm loopback request domain** <*domain name*> to filter Ethernet CFM loopback debugs may not display the debug output to the console. Removing the filter and using the **debug ethernet cfm loopback request** command will function properly.
- The output of the command **show ethernet cfm mep loca**l may display an incorrect maintenance association for a MEP ID if multiple maintenance associations are configured on the unit.

- The NetVanta 6240 should send warm_start SNMP traps when the unit is told to reboot by software. It should only send cold_start traps when the power is cycled. Instead, it is sending cold_start traps, even when reloaded by software.

The following is a list of Carrier Ethernet specific errata that exist in products running AOS version R11.4.4.

- If 802.3ah link OAM is enabled on an interface, issuing the **show ethernet oam discovery** or the **show ethernet oam statistics** command and pressing **Enter** to display additional lines results in CLI misalignment.
- Walking the HDSL2-SHDSL-LINE-MIB::hdsl2ShdslInventoryTable may return invalid data for some non-CPE elements on the SHDSL span.
- The **efm-group** interface type option is missing from the **tunnel source** command on tunnel interfaces.
- When using a SHDSL module, frame counts for broadcast and multicast traffic may not increment on the parent EFM group interface. The subinterface counters do properly increment.

The following is a list of Voice specific errata that exist in products running AOS version R11.4.4.

- Removing a voice user while the FXS port is offhook can result in a reboot.
- When in SIP proxy survivability, if a call is placed between a FXS port and a SIP proxy user that is using SIP over TCP, the unit will not send a BYE to the SIP proxy user when the call is disconnected by the FXS port.
- When duplicate users are registered through the SIP proxy, an outbound call from one of the duplicate users may be treated as an inbound call.
- If an AOS devices receives a reINVITE with a higher CSeq value while it is waiting for an ACK to a previous INVITE with a lower CSeq, a 500 Server Internal Error response will be sent instead of a more appropriate response, such as a 491 Request Pending. The scenario involved is described in RFC 5407 Section 3.1.4.
- Accessing the Voice > System Parameters or Voice > VoIP Settings menus in the GUI results in a 503 Service Unavailable message.
- Removing a voice trunk with active calls can result in the unit rebooting.
- Issuing the command **clear voice call active** with active MGCP calls can result in a reboot.
- The ERL tool is not functional on the NetVanta 6360.
- On the NetVanta 6360, if the onboard FXO port is configured to receive digits, a 500 ms delay is required after answering before receiving the first DTMF digit.
- Call waiting caller ID does not function properly on the NetVanta 6240.
- Receiving an initial INVITE with both audio and T.38 SDP will result in the call being placed on hold.
- The detailed voice quality statistics for a call may not accurately reflect the adjustments made by modem-passthrough.
- On the Total Access 900e Series (third generation) and NetVanta 6250 Series, if the second CODEC listed in the MGCP Local Connection Options is not one of the CODECs defined in the CODEC list assigned to the MGCP endpoint, the unit will respond with 534 Transaction Failed response resulting in a failed call.
- On the NetVanta 6250 and Total Access 900e (third generation), the **timing-source internal** command is not present. The workaround is to configure **no timing-source t1** <*slot/port*>.

- In AOS R10.4.0 and higher, **modem-passthrough** will fail to send a reINVITE to G.711 if the endpoint is configured with a CODEC list that does not contain G.711.
- The command **ip mgcp qos dscp** <*value*> will not take effect until either **ip mgcp** is disabled and then re-enabled or the AOS device is reset.
- When the SIP server monitor clears the primary SIP server from a delayed state due to a failure of the secondary SIP server, there will be a 60-second delay until a SIP registration is attempted to the primary SIP server. This delay will not occur if the SIP server monitor is clearing the secondary SIP server from a delayed state due to a failure of the primary SIP server.
- On the Total Access 900e (third generation) and NetVanta 6250, SIP must be enabled in the running configuration whenever MGCP is used for voice.
- Invalid characters are allowed in a host name for the SIP server on a voice trunk.
- On the Total Access 900e (third generation) and NetVanta 6250, if the remote voice gateway changes the SSRC in an RTP stream received by the AOS unit, and the sequence numbers are not contiguous, VQM and the output of the **show voice quality-stats** command will log lost packets for the number of packets between the last sequence number of the first stream and the first sequence number of the new stream. The output of **show voice quality-stats** <*ID*> will also not reflect that the SSRC value changed on the call.
- When G.729 Annex B is negotiated and VAD is enabled on the endpoint(s) involved in the call, the unit will generate comfort noise packets with payload type 13. This can cause issues with devices expecting comfort noise packets to have the same payload type as RTP (18). However, payload type 13 is specified in the SDP from the AOS device.
- If an ADTRAN unit is configured with single call appearance mode, forwarded calls on a PRI trunk will fail.
- When using media anchoring, receiving a 183 Session Progress after a previous 183 on hairpinned calls can result in no early media if the SDP in the second 183 differs from the first.
- Echo cancellation is not enabled on three-way calls when using the local conferencing feature.
- On NetVanta 644 and NetVanta 6240 Series units, V.21 messages will sound overly amplified when listening to the TX output of a T.38 DSP capture. This is a flaw of the capture utility and does not represent how the audio actually sounds.
- DSP captures on the NetVanta 6240 and 644 platforms consume large amounts of memory while in progress. The unit could become unstable if a DSP capture is active for an unusually long period of time.
- With the ADTRAN unit set for **voice flashhook mode transparent**, the conference originator must wait for the third-party to answer before executing the flashhook to initiate the conference.
- On the NetVanta 6240 Series, over an extended period of use, T.38 calls can cause DSP channels to cease producing a dial tone and have poor voice quality. Rebooting the unit will correct the problem.
- NetVanta 6240 only: While running 29 or more simultaneous calls using E&M Immediate, Wink, or Feature Group D, it is possible to get in a state where DTMF tone detection will not function on any outbound (DSX to SIP) call using DSP 0/1.15 or higher. While in this failed state, all calls will continue to function in either call direction on DSP 0/2, as well as all calls on DSP0/1 in the inbound direction. With a load of 28 or less calls, all calls will function reliably in both directions on both DSPs. No consistent work around has been identified at this time. A unit reboot will typically solve the problem.
- The NetVanta 6240 Series IP business gateways can reboot if 60 simultaneous calls are placed through the DSP.

- The Total Access 900e Series (second generation) cannot properly handle more than 40 simultaneous E&M RBS calls. More than 40 simultaneously active calls could result in no dial tone or no audio on the last 8 channels.
- Using the HEAD acoustics test suite, some G.168 echo cancellation test cases fail on the NetVanta 6240 and NetVanta 644. These same tests pass on Total Access 900 Series units. There is no reason to believe this would affect a customer in the field.
- On the NetVanta 6310/6330 Series, if a SIP trunk is trying to register a large number of users and the registration fails, activating **debug sip trunk-registration** will cause the Telnet and console connection to become unresponsive. A reboot clears the condition.

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 R11.4.4 or later. 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*

