RELEASE NOTES

AOS version R12.3.4
December 8, 2017

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 R12.3.4 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 12*.

A list of new or updated documents for this release appears in *on page 16*.

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 R12.3.4. 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 1234/1234P/1238/1238P (2nd and 3rd Gen.)	√			XB.01.02
NetVanta 1235P	√			R10.4.0.B1
NetVanta 1335		√		15.01.00
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 1550	√			BVS1.0
NetVanta 1638/1638P	√			18.02.01.SC
NetVanta 3120 (1700600L2)		√		14.04.B1
NetVanta 3120 (1700601G2)		√		17.01.01.B2
NetVanta 3130 (1700610L2)		√		14.04.B1
NetVanta 3130 (1700611G2 & 1700612G2)		√		17.01.01.B2
NetVanta 3140	√	√	√	R11.5.0
NetVanta 3200/3205 (3rd Gen.)	√	√		17.02.01.00

Platform	Standard Feature Pack	Enhanced Feature Pack	SBC Feature Pack	Minimum Boot ROM
NetVanta 3305 (2nd Gen.)	√	√		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.)	√	√		08.01.00
NetVanta 4430	√	√	√	17.04.01.00
NetVanta 4660		√	√	R10.10.0.B5
NetVanta 5305	√	√		11.03.00
NetVanta 5660		√	√	R11.4.1.B2
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
Total Access 900 Series (2nd Gen.)		√		14.04.00
Total Access 900e Series (2nd Gen.)		√	√	14.05.00.SA
Total Access 900e Series (3rd Gen.)		√	√	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 R12.3.4 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 R12.3.4 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.
- As of R11.8.0, a valid SBC call capacity license is required for SIP B2BUA functionality on the following products:

  NetVanta 6250

  NetVanta 6360

  Total Access 900e (third generation)

Features and Enhancements

This section highlights the major features, commands, and behavioral changes for all products running AOS version R12.3.0.

- The per-interface ARP cache limit was increased to 1024 entries on the NetVanta 4660 and 5660.
- Added the ability to forward debug output via Syslog.
- Added the ability to set the target of a ping probe to the default gateway learned via DHCP on an interface.
- TLS 1.0 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 TLS 1.0 support, the **allow-tls1.0** parameter has been added to all of these clients and servers.

  Additionally, support for SSL 2.0 has been removed from AOS.

Fixes

This section highlights major bug fixes for all products running AOS version R12.3.4.

- If a value greater than 2147483647 was entered for the **dampening-interval** on a track, it was improperly stored in the configuration as 2147483647.
- On the NetVanta 4660, 5660, and 6360, LLDP messages were not received.
- In some cases, issuing the **show dot11 access-point detail** command resulted in a reboot.
- A reboot occurred when email logging was used with certain SMTP servers that supported STARTTLS.

This section highlights major bug fixes for all products running AOS version R12.3.3.

- If the **ssh key regenerate** command was issued, the CLI would hang for several seconds after the prompt was returned.
- The output of **show ssh-server mypubkey** displayed an incorrect value for the RSA public key.
- When assigning IPv6 prefixes via DHCPv6 Prefix Delegation (PD), routes were not added for the prefixes assigned via PD.
- When the IPv4 firewall was configured in local traffic only mode, a reboot occurred if a packet destined for the unit required reassembly from fragments.
- In some cases, a reboot occurred if a child QoS map was modified after its parent QoS map had been removed.
- The AOS TWAMP client sent a non-zero value for the Number of Packets field in TWAMP requests, which violated RFC 5357.
- If a DNS query for a NTP server returned both A and AAAA records, NTP did not fall back to the IP address in the A record if IPv6 wasn't configured on the unit.
- When upgrading to R12.3 and later, if **http secure-server allow-sslv2** was configured the command resulted in an error on boot and the HTTPS would remain disabled because SSLv2 is no longer supported. Now if **http secure-server allow-sslv2** is configured, the **allow-sslv2** parameter is ignored and the HTTPS server will be enabled as configured.
- The **http secure-server allow-sslv3** command did not work when running AOS R12.3.0, R12.3.1, R12.3.2, and R12.4.0.
- VRRPv3 traffic was not implicitly allowed through the IPv4 firewall.

This section highlights major bug fixes for all products running AOS version R12.3.2.

- AOS R12.3.0, R12.3.1, and R12.4.0 did not properly generate the HTTPS server TLS certificate on boot if it was not already present. As a result, if the unit was upgraded directly to one of the affected versions from a version of AOS prior to R11.7.0 and the HTTPS GUI was unavailable. This affected all AOS products except the NetVanta 1531, 1550, 1638, 3140, 4660, 5660, 6250, 6360, 6410, and Total Access 900e (third generation).
- The command **auto-link https allow tls1.0** was not properly restored on boot. Additionally, the command **autoconfig method https allow-tls1.0 allow-sslv3** was not added to the running configuration.
- In rare cases, if a flash error was detected and corrected, a reboot occurred.
- If a probe, track, or schedule had an ampersand (&) in the name, a 503 Server Error message was returned when trying to edit it from the GUI.
- On units with a DBU installed, events output to the console resulted in a small memory leak for each event.
- When using per-destination IP load sharing, it was not possible to bring up a VPN tunnel if the ingress interface for VPN traffic did not match the egress interface used to route back to that address.
- The @ character was improperly rejected in a SNMP community string if the string following the @ symbol was not a valid VLAN ID.
- On the NetVanta 1531, 1550, 3140, 4660, 5660, 6250, 6360, and Total Access 900e (third generation), the CPU utilization was inaccurate when the unit was under heavy load when running AOS R12.2.0 or later.

This section highlights major bug fixes for all products running AOS version R12.3.1.

- If an LLDP neighbor advertised an IPv6 address as its management address, a reboot occurred.
- The AOS SNTP client failed to synchronize with some NTP servers.
- If WAN failover and multiple VRFs were configured on a unit, firewall sessions were not properly cleared when the primary connection recovered from a failure.
- The **debug ntp** command returned an error when issued.
- The **Vendor-specific Data** field in the output of **show sfp-info** command did not display if the SFP returned a string padded with 0 (ASCII 0x30) instead of NULL (ASCII 0x00).
- ICMP error responses were not properly forwarded through a destination NAT.
- If a track referenced by a **tcl run** statement in the configuration was removed, the **tcl run** statement in the configuration became malformed and could not be removed. **tcl run** statements that reference a track will now be removed from the configuration when the track is removed.
- Unicast DHCP traffic that was not destined for the unit was terminated locally instead of being forwarded to the specified destination.
- When rebooting a unit with the **reload** command, PPPoE sessions were not terminated with a PADT message.
- If the **bandwidth** command was specified on an interface, the value reported via the ifHighSpeed OID did not match the value reported via the ifSpeed OID.
- When using the Network Monitor wizard in the GUI, the ACL that was created used the **hostname** parameter even if the user specified an IP address for the destination.
- The **debug ip firewall alg sip** command was available on the NetVanta 3140, 4660, and 5660 even though the SIP ALG is not present in those products.
- When redistributing an iBGP route to an eBGP neighbor, the next-hop address was not set to the device's IP address if the route was not a directly connected network.
- On a NetVanta 4660, 5660, or 6360 with a large number of Layer 3 subinterfaces and a non-default **qos cos-map**, restoration of the configuration at boot was slow.

This section highlights major bug fixes for all products running AOS version R12.3.0.

- Subinterfaces did not correctly report their speed in the ifSpeed OID unless the **bandwidth** command had been applied to that interface.
- If NTP started and the egress interface used to reach the NTP server did not have an IP address, several minutes elapsed before the clock was set once the interface was assigned an IP address.
- On units that support auto-config zero touch provisioning, the routed Ethernet ports and the VLAN 1 interface were not getting set to DHCP when no startup config was present.
- If the DSA keys used by the SSH server became corrupted, the unit rebooted when a user attempted to establish an SSH connection.
- The DHCP pool time zone offset value was not displayed properly when a negative, partial hour offset was entered.
- When using VRRPv2 or VRRPv3, the router required the primary virtual IP address configured on both units to match, which violated RFCs 3768 and 5798.
- If a unit received LLDP packets from a neighbor containing invalid MAU types, a 503 Server Error was returned when accessing the GUI.

- On the NetVanta 4430, late collisions on a Gigabit Ethernet interface configured for full duplex may have caused the interface to cease transmitting until the unit was rebooted.

This section highlights the Carrier specific bug fixes in products running AOS version R12.3.4.

- If a non-default **ce-vlan-id tpid** was configured, traffic would not egress any layer 3 subinterfaces that had an outbound QoS policy applied.

This section highlights the Carrier specific bug fixes in products running AOS version R12.3.2.

- SyncE SSM messages were transmitted when the ESMC process was disabled.
- Removing or shutting down a MAC swap loopback resulted in a reboot.

This section highlights the Carrier specific bug fixes in products running AOS version R12.3.1.

- When switching network sync sources due to the loss of SSMs, the unit improperly went into holdover and transmitted a transient QL-EEC1 message.

This section highlights the Voice specific bug fixes in products running AOS version R12.3.4.

- If a CANCEL was received on a valid SIP dialog when using the SIP proxy, in some cases a 200 OK response was not sent.
- The SIP trunk monitor did not consider the resolved IP address and port when updating the status of server entries.
- DNS client debug was enhanced to make it clear when a DNS request was being answered from the DNS cache.
- If the SIP proxy monitor was enabled in **stateful-transparent** mode and the route to the configured SIP proxy server was removed (e.g. the egress interface went down), the SIP proxy failed to spoof 200 OK responses to REGISTER requests.
- If a **sip proxy failover group match-value** command was configured while the SIP proxy was disabled, the unit rebooted.
- If two different FQDNs were used for SIP TLS with persistent connections and the FQDNs both resolved to the same IP address, the persistent connection was continuously torn down and re-established.
- When using the SIP proxy, BYE requests destined for the network were sent to the primary configured server instead of the server with which the call was in-dialog.
- In scenarios involving an E&M wink trunk in which the unit didn't receive a valid wink, the **debug interface t1 0/x rbs** output stated **Valid Wink Received**.

This section highlights the Voice specific bug fixes in products running AOS version R12.3.3.

- When using the proxy monitor with the SIP proxy in transparent mode, if all servers failed to reply to a REGISTER the proxy did not spoof a 200 OK response, preventing the phone from entering survivability.
- On a PRI to SIP hairpin call, if the inbound SIP call immediately transitioned from ALERTING with inband audio to CONNECT, no audio was present.
- On FXO to SIP calls, if a 183 Session Progress response was received, AOS did not respond to a received 200 OK response with an ACK.
- Escaped carriage return and new line characters (i.e., \r\n) in HMR modify statements prevented the parsing of HMR variable names from working properly.

- Invalid characters were not rejected in the called party number, calling party number, and redirecting number IEs in received ISDN messages.
- If the User-Agent of a SIP device registering to AOS contained one or more space characters, static **sip location** entries that could not be removed were added to the running configuration on boot if **sip location database** was configured.
- If a server reset a persistent SIP TLS connection, the unit would attempt to reconnect immediately without any rate limiting. AOS will now retry using a backoff algorithm of 1, 2, 4, and finally 8 seconds.
- When using MGCP, if a SignalRequest for VMWI (L/vmwi) was received immediately after a SignalRequest for ring splash (L/rs), the FSK for VMWI was not delayed until after the ring splash, resulting in VMWI not being activated on the connected phone.

This section highlights the Voice specific bug fixes in products running AOS version R12.3.2.

- In rare cases when running AOS R12.3.1 on a Total Access 900/900e (second generation), calls failed due to a TDM manager connect failure.
- On the NetVanta 3140, 4660, 5660, and 6360, the value of the **voice system-country** setting was not saved.
- On the NetVanta 3140, 4660, 5660, and 6360, the automatically added always-permitted dial plan entries for emergency phone numbers were not updated when the **voice system-country** was changed from the default of United States.
- When using MGCP on a Total Access 900/900e (second generation) unit against a Genband call agent, VMWI did not function properly.
- When sending a 480 Temporarily Unavailable response to an unsupported SUBSCRIBE event type while the SIP proxy was in survivability, the unit improperly sourced the packet from 127.0.0.1.
- When using MGCP with a Genband C20 on a Total Access 900/900e (second generation) unit, some call flows resulted in no RTP being sent or received by the AOS device.
- If the SIP proxy received forked SIP CANCEL requests, only the first CANCEL was processed properly. All of the subsequent CANCELs on that Call-ID received a 500 Server Internal Error response.

This section highlights the Voice specific bug fixes in products running AOS version R12.3.1.

- When running AOS R11.10.7 and using the SIP proxy, 200 OK responses to CANCELs were not proxied properly, and SIP transaction resources were leaked.
- In certain cases the unit rebooted when running AOS R11.10.7 and using the SIP proxy.
- When running AOS R11.10.7, if a voice user was configured with a **first-name** and a **last-name** and the first name was longer than the last name, a reboot occurred in certain call scenarios.
- Certain ISDN warning messages were displayed to the console when no debug was enabled.
- The unit improperly sent a display name of a single space instead of omitting the display name if no first and last name was configured for a voice user.
- On the NetVanta 6240, Total Access 900 (2nd Generation), and Total Access 900e (2nd Generation), if a CRCX with a SignalRequest for L/dl was received, the receive audio path on the FXS port was not enabled.
- The output of the **show voice cal**l command displayed **Unknown** as the CODEC for calls that had been disconnected instead of the last used CODEC.

This section highlights the Voice specific bug fixes in products running AOS version R12.3.0.

- On a SIP-to-PRI call with late media (i.e., SDP offer in the 200 OK instead of the INVITE), if the ALERTING received on the PRI was immediately followed by a CONNECT, the call failed.
- When running R11.10.5 or R12.2.0.SA, if inband call progress tones were presented on a SIP-to-SIP or a SIP-to-ISDN call, an unexpected 180 Ringing response without SDP was sent by the unit, which prevented the inband call progress tones from being heard.
- If the first or last name configured on a voice user contained quotation marks, the Voice Users menu in the GUI would not load completely.
- In rare cases, the use of VQM resulted in a reboot.
- The busy tone, disconnect tone, and reorder tone for Australia were generated at 400 Hz instead of the correct value of 425 Hz.

This section highlights Switch specific bug fixes in AOS version R12.3.4.

- On the NetVanta 1531 and 1550, if IGMP snooping was enabled on any VLAN, IGMP reports would be forwarded back out the source interface on VLANs that did not have IGMP snooping enabled.

This section highlights Switch specific bug fixes in AOS version R12.3.2.

- The BRIDGE-MIB was not supported on the NetVanta 1550.
- When attached to a NetVanta 1534P (second generation), NetVanta 1544P (second generation), or NetVanta 1638P, BSAP 3040 units experienced random reboots.
- The **copy http** and **copy https** commands did not function on the NetVanta 1638 when using the Ethernet 0/1 interface.

This section highlights Switch specific bug fixes in AOS version R12.3.1.

- If there was a large amount of traffic that needed to be tunneled from a line card to the master in an ActivChassis, ActivChassis management traffic could be dropped resulting in a reboot. ActivChassis management traffic is now marked with an 802.1p value of 7, and any other tunneled traffic inherits the 802.1p value of the original packet.
- On the NetVanta 1531 and 1550, the unit incorrectly showed 100 percent CPU utilization after extended uptime.
- In situations where a large amount of buffering was required (e.g., a large packet with many fragments ingressing on a 1 Gbps interface and egressing on a 100 Mbps interface), the NetVanta 1531 and 1550 sometimes dropped packets.

This section highlights Switch specific bug fixes in AOS version R12.3.0.

- When using MAC Authentication Bypass, The Calling-Station-Id was improperly set to PORTAUTH instead of the client's MAC address.
- On the NetVanta 1550, the **speed 1000 nonegotiate** command did not function properly on the xgigabit-ethernet interfaces.
- If a copper SFP was inserted in ports 0/25 through 0/28 on a NetVanta 1544F, speed configurations other than **speed auto** did not persist through a reboot.

Errata

The following is a list of errata that still exist in all products running AOS version R12.3.4.

- If **ip pim sparse-mode** is configured on an interface that does not have an IPv4 address configured, an error with no text is returned.
- In rare cases, a reboot will occur when AAA accounting is enabled.
- Router advertisements for delegated prefixes assigned to a interface do not use the valid lifetime specified in the received IA_PD Prefix option. **Workaround:** Configure **ipv6 nd prefix named-prefix <prefix name> <prefix sub-bits>** for each delegated prefix assigned to the interface.
- Making any changes in the GUI for an Ethernet interface configured for DHCP causes the DHCP client to perform a DHCP release/renew on that interface when the changes are applied.
- A few legacy cellular interface commands were incorrectly removed when USB LTE support was added. The removed commands include:

  snmp trap cellular

  snmp trap link-status

  snmp trap threshold-ecio

  snmp trap threshold-rssi
- When using the Novatel USB 551L modem with a NetVanta 3140, a small number of lost frames will occur with packets smaller than 512 bytes. The loss occurs in the modem and not the NetVanta 3140.
- Assigning the IP address 192.168.190.1 to a NetVanta 160 AP from an AOS controller prevents the AP from pulling a full configuration from the controller.
- 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.
- 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.
- 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 can freeze 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.
- The Total Access 900e (third generation) and NetVanta 6250 send a cold start SNMP trap on reload instead of a warm start trap.
- 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.
- 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.
- 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.
- VQM may show a loopback interface in the GUI when a loopback interface is not configured.
- 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.
- 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.
- A NetVanta 5305 can stop passing traffic for brief intervals when negotiating frequent VPN tunnels using Diffie Hellman Group 5.
- 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.
- 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.
- 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 R12.3.4.

- The **efm-group** interface type option is missing from the **tunnel source** command on tunnel interfaces.

The following is a list of Voice specific errata that exist in products running AOS version R12.3.4.

- If a voice trunk is removed while calls are active, a reboot may occur.
- Enabling the SIP stack on a device allocates numerous resources. If this resource allocation fails, the device will reboot. Multiple sockets must be available and local SIP ports, typically UDP and TCP 5060, must be available as well, otherwise the resource allocation will fail and the device will reboot.
- TLS negotiation will fail when using ECDSA ciphers for SIP TLS.
- When using the SIP proxy with media anchoring, VQM reports incorrect information for LocalURI, RemoteURI, and LocalCaller if a reINVITE that modifies the SDP is received from the called party during a call.
- Issuing the command **clear voice call active** with active MGCP calls may result in a reboot.
- If **sip tls** is configured while **sip** is disabled, **no sip tls** must be issued before **sip** can be enabled, otherwise the following error will be displayed: %Error: Failed to modify SIP Access-class with new VRF.
- If a CA profile is removed while SIP TLS calls using that profile are active, BYE messages will not be sent for any of the active calls.
- 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.
- Receiving an initial INVITE with both audio and T.38 SDP will result in the call being placed on hold.
- 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 doesn't 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.

- 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 fewer 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.
- 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.

The following is a list of Switch specific errata that exist in products running AOS version R12.3.4.

- On a NetVanta 1544F, a switchport interface with a connected SFP interconnect cable cannot be shut down properly.
- The idle process on a NetVanta 1638, visible with the command **show processes cpu**, is named **procnto-600-,** rather than **Idle**, like other AOS platforms.
- Certain NetVanta PoE switches require the command **power inline 2-point** be configured on applicable switchports in order to power Polycom VVX phones with three attached color expansion modules.
- In an ActivChassis configuration utilizing port channels that are distributed among individual line cards, if more than 1 Gbps is sent across the port channel the ActivChassis will sometimes discard some traffic.
- 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.
- 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.
- 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.
- Certain OIDs in the Bridge-MIB may not return a value on AOS switches.
- Port mirroring on a NetVanta 123x (second and third generation) 1534, and 1544 cannot send transmit mirrored frames without a VLAN tag.

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.