RELEASE NOTES

AOS version R10.5.4
December 20, 2013

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 R10.5.4 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 11*.

A list of new or updated documents for this release appears in *Documentation Updates on page 18*.

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 R10.5.4. 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 (2nd Gen. only)	√			XB.01.02
NetVanta 1238/1238P (2nd Gen. only)	√			XB.01.02
NetVanta 1534	√			17.06.03.00
NetVanta 1534 (2nd Gen.)	√			17.08.01.00
NetVanta 1534P (2nd Gen.)	√			17.09.01.00
NetVanta 1535P	√			17.08.01.00
NetVanta 1544/1544F	√			17.06.03.00
NetVanta 1544 (2nd Gen.)	√			17.08.01.00
NetVanta 1544P (2nd Gen.)	√			17.09.01.00
NetVanta 1638	√			18.02.01.SC
NetVanta 1638P	√			18.02.01.SC
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

Platform	Standard Feature Pack	Enhanced Feature Pack	SBC Feature Pack	Minimum Boot ROM
NetVanta 3458	√	√		17.06.01.00
NetVanta 4305 (2nd Gen. only)	√	√		08.01.00
NetVanta 4430	√	√	√	17.04.01.00
NetVanta 5305	√	√		11.03.00
NetVanta 6240		√	√	A5.01.00
NetVanta 6310		√	√	A3.01.B2
NetVanta 6330		√	√	A3.01.B2
NetVanta 6355		√	√	14.06.00
Total Access 900 Series (2nd Gen. only)		√		14.04.00
Total Access 900e Series (2nd Gen. only)		√	√	14.05.00.SA

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 R10.5.4 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 R10.5.4 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.

R10.1.0 resolved a BGP implementation issue that slightly changed its behavior. Prior to R10.1.0, a static default route could be redistributed to BGP peers when the command **redistribute static** was configured. As of R10.1.0, a default static route will not be redistributed without being explicitly configured with a **network 0.0.0.0 0.0.0.0** statement.

Features and Enhancements

This section highlights the major features, commands, and behavioral changes for all Converged Access products running AOS version R10.5.0.

- Added support for advertising IPv6 routes and prefixes via OPSF version 3.
- Added support for IPv6 loopback interfaces.

This section highlights the voice specific features, commands, and behavioral changes available in products running AOS version R10.5.0.

- The SIP proxy and SIP B2BUA can now be configured to run on a non-default VRF.
- Added support for the Quad BRI S/T NIM2 module.

- Added support for two E1/PRIs along with a SIP trunk on the NetVanta 6355. One PRI connects to the PSTN and recovers timing, and the other connect to a PBX and sources timing.
- In the CLI, the output of the **show voice quality-stats**, **show media-gateway**, **show media-gateway session**, and **show media-gateway channel** commands has been enhanced for greater accuracy and readability. Corresponding changes have been made to the **Call Quality Stats**, **RTP Channel Stats**, and **RTP Session Stats** pages in the GUI.
- Added enhancements to Auto-Config, including support for Broadsoft Device Management.
- Added the ability to generate a call progress tones with call disconnect messages on network role ETSI PRI/BRI interfaces. Also added the ability to receive call progress tones on disconnect messages on user role ETSI PRI/BRI interfaces.

Fixes

This section highlights major bug fixes for all products running AOS version R10.5.4.

- It was possible for DNS queries created by an AOS IP Business Gateway to be sent using the DSP port range, which may have prevented responses from being properly received.
- It was possible for DNS queries to be sent using source port UDP 4500, which prevented responses from being properly received if **ip crypto** was enabled.
- Syslog output sent for **priority-level info** could eventually cause a memory leak on a NetVanta 1638.
- When **service password-encryption** was enabled, the auto-config password changed when the unit booted.
- In a NTP configuration, including two FQDNs that resolved to the same IP address caused the unit to lock up.
- A reboot may have occurred when multiple packet-captures were being exported in rapid succession using HTTP or HTTPS.
- Removing and then adding an NTP server in quick succession occasionally caused a reboot.
- In rare cases, a reboot may have occurred when NTP attempted to synchronize the AOS unit's clock.
- In rare cases, on a NetVanta 1544 (second generation), the Layer 3 host table and the ARP cache entries would not match, which caused added latency for traffic sent to the devices that were not properly populated in the Layer 3 host table.

This section highlights the voice specific bug fixes in products running AOS version R10.5.4, unless otherwise noted.

- If a SETUP message was received on an ISDN interface with a called party number type of "international", the unit would not prepend a the configured IDD prefix before attempting to route the call.
- Calls into an ISDN PRI interface were rejected if the Screening Information Element was present.
- Modifying a user through the IP business gateway's **Voice > User Accounts** GUI menu perpetually displayed the Loading message box.
- A CONNECT_ACK may not have been sent after receiving a CONNECT on an ETSI PRI configured for the user role.

- MGCP ground start calls that were disconnected from the far end resulted in a hook state mismatch between the call agent and the AOS unit. This resulted in all inbound calls failing until a call was placed from the same FXS port.
- When using the default LBO setting (**lbo long 0**) on a T1 on a 2nd Generation Total Access 900e with the v3.1 T1 framer, it was possible to for T1 errors to occur due to the pulse shape being close to out of spec.
- T.38 calls failed if it took longer than 45 seconds to send a page.
- On a SIP-to-SIP call through the B2BUA, if the destination SIP server did not respond to an INVITE, the AOS unit may have sent a 400 Bad Request response to the original INVITE instead of a 503 Service Unavailable response.
- When using MGCP, if the received caller ID name from the call agent is the O flag to indicate that it is unavailable, the unit sent the text string **Unavailable** as the caller ID name to the FXS port, instead of sending the O flag for the name.
- When the hex encoding for # (%23) was received in a SIP URI, it was not properly converted back to # before being processed by the switchboard.
- It was possible to configure the UDP port range for the DSP to overlap with the port range used by RTP Firewall Traversal, which may have caused one-way audio.

This section highlights major bug fixes for all products running AOS version R10.5.3.

- When AAA authorization was configured and the AAA server was unresponsive, if a group of commands was entered via an SSH session that must be authorized, administrative access to the AOS device was lost until the device was rebooted.
- When under heavy load, an AOS switch could stop providing PoE on some ports. A reboot would resolve this issue.
- Tunnel interface counters showed a bogus value for the last clearing of counters.
- When BGP neighbors were shut down (the default behavior), the shutdown status was not visible in a non-verbose running configuration.
- When transferring a file via HTTP with the **copy http** command, the received bytes counter created a new line in a CLI session for each received incremental value.
- In certain cases, the system uptime reported via SNMP was less than the actual system uptime.

This section highlights the voice specific bug fixes in products running AOS version R10.5.3, unless otherwise noted.

- If the T1 PRI interfaces on a NetVanta 644 were connected to the PSTN or a PBX, it was possible that the unit would reboot during startup.
- The **ip sip qos dscp** command was not present in routers without the SBC Feature Pack .
- Under a heavy call load, it was possible that successive calls could use the same memory location to store their B-channel information, causing a reboot when the latter call disconnected.
- If a request was received on a dialog in the opposite direction of the original request on that dialog, the SIP proxy may have inserted the local IP address in the host portion of the Request-URI.
- In rare cases it was possible for the DSP on the unit to cause a reboot.
- If an IP PBX used a new INVITE to hairpin a call back out a PRI trunk rather than transferring the call with a REFER, it was possible that the talk path would not connect properly.

- If a reINVITE immediately proceeded a REFER with Replaces, the resulting transfer may have failed.
- In rare cases, the NetVanta 644 would reboot if a shut / no shut was performed on the T1 interface associated with a PRI trunk.
- The GUI on the Total Access 900/900e Series listed T1 clocking options that were not valid for the product (for example: System and Through)

This section highlights major bug fixes for all products running AOS version R10.5.2.

- If a packet capture in AOS was running indefinitely, it was possible that the unit would reboot.
- With a login banner longer than 1700 characters, an AOS device would reboot when it was accessed via SSH.
- If the configuration includes a secondary IP address, executing an SNMP walk resulted in a failure at the ipAdEntAddr OID with error OID not increasing. If the secondary IP address was removed, the walk completes successfully.
- On second generation NetVanta 1230 Series switches, LLDP MED devices were not properly added to the MAC table when Port Security was enabled.
- In rare cases, the Ethernet port on the Total Access 900 Series would falsely report an auto-negotiation event. This false detection would generate an event message, but no packets were ever dropped.
- The AOS GUI would not display a PPP interface in a state of loopback.
- A large amount of broadcast or multicast traffic being terminated by a NetVanta 1638 prevented it from initiating certain types of locally generated traffic, including ICMP and VRRP advertisements.
- A DHCP 802.1q subinterface could not be configured from the GUI, but it could be accomplished from the CLI.
- Deleting a PPP interface being used for dial backup (DBU) in a legacy DBU application while the DBU PPP interface was active, caused AOS devices to reboot.
- A large numbers of collisions on an Ethernet interface caused the interface to stop transmitting packets.
- If the firewall was enabled, the NetVanta 644 would drop fragmented packets.
- Adding a track with a space in its name to a route caused the route to be lost on reboot.

This section highlights the voice specific bug fixes in products running AOS version R10.5.2, unless otherwise noted.

- A reboot may have occured if duplicate codec entries were received in a SIP message.
- If the T1 PRI interfaces on a NetVanta 644 were connected to the PSTN or a PBX, it was possible that the unit would reboot during startup.
- The CODEC list applied to an answering TDM endpoint (including the default CODEC list if no CODEC list is applied) would take precedence over the CODEC list applied to a SIP trunk for inbound calls.
- A SIP parser error occurred when the display name ended with \\".
- HMR was unable to modify Route and Record-Route headers.
- Calls into a ring group would not connect properly.
- When using media anchoring, receiving a 183 Session Progress response after a previous 183 response on a hairpin call caused a reboot.
- Call duration in the **show voice call summary active** command output would reset after receiving a SIP reINVITE.

- It was possible for an AOS unit to get into a state where it could no longer allocate ports for RTP sessions. This state was encountered after the closure of a complex call flow.
- The **voice number-complete disable pound** command did not function properly on CAS trunks.
- Call flows with hairpinned TDM audio resulted in audio loss in both directions on the NetVanta 644.
- The SIP Server URL Field in the GUI was limited to 40 characters.
- With multiple PRIs in the same ISDN group, bringing one PRI down caused calls that should have used the other PRI to fail.

This section highlights major bug fixes for all products running AOS version R10.5.1.

- On an AOS unit acting as a DNS proxy, the unit could reboot when a client attempted to resolve a domain name and the DNS servers could not reached.
- When acting as an access controller for NetVanta 160 Access Points, an AOS device became unable to push configuration changes to the access points.
- When the ADSL interface on a Total Access 900 with ADSL2+ was administratively shut down, the Net LED would remain red.

This section highlights the voice specific bug fixes in products running AOS version R10.5.1, unless otherwise noted.

- In rare cases, a PRI interface would not recover if the T1 interface it was connected to dropped and then recovered in a short period of time.
- When using a PRI network role, if the ISDN T303 timer expired, a reboot could have occurred.
- If a unit configured with the **sip-server rollover service-unavailable-or-timeout** command received a 503 Service Unavailable response to a SIP REGISTER message, no additional registrar servers would be contacted.
- For any device that did not support Multi-VRF for SIP (i.e. NetVanta 600 Series, NetVanta 3100 Series, and NetVanta 7000 Series), SIP access-classes blocked all SIP traffic.
- When using media anchoring, if one side stopped sending RTP longer than the value set using the **ip rtp session timeout** command, then the media anchoring entry for the opposite direction would also be removed.
- If a reINVITE was received shortly or immediately after the ACK for the initial INVITE, the ADTRAN unit would respond with a 491 Request Pending. This caused a delay in the connection of two-way audio.
- The NetVanta 644 would not process ARP requests for IP addresses assigned to a loopback interface.
- SIP syntax error events will no longer be logged if they are automatically corrected by the unit.

This section highlights major bug fixes for all products running AOS version R10.5.0.

- Upgrading to firmware version R10.4.0 on the second generation NetVanta 1534P and 1544P caused the chassis fans to stall.
- In the CLI, the **logging forwarding auxiliary-receiver-ip** <*ip address*> command was not accepted as a valid command.
- On a NetVanta 1638, if an IP address was removed from a VLAN interface, devices in that VLAN were not properly added to the local route cache.
- Issuing the command **show ip route** for an IP address that was configured on a loopback interface would yield incorrect results.

- In certain cases, TCP traffic sent over or received on a GRE tunnel caused a reboot.
- When redistributing seemingly identical networks with different subnet masks (for example, 192.168.0.0/24 and 192.168.0.0/16) from BGP to OSPF, only the least specific route was properly advertised.
- Abbreviating the **show running-config | include** <*text*> command with **s run | include** <*text*> would not function.
- The administrative distance on a static route could not be changed without removing and re-adding the static route with the new administrative distance.
- The NTP server configuration could not be modified in the GUI.
- BGP would not propagate MED to eBGP neighbors when an outbound route-map was used to set the metric.
- Selecting the Clear button on the Cable Diagnostics GUI menu generated a 503 Service Unavailable response.
- Browsing to the Debug Unit menu in the GUI, could generate a 404 Not Found response.
- When creating a DHCP pool in the GUI, the NTP server field was automatically populated with the characters **::**. This caused the DHCP pool creation to fail if the characters were not manually removed prior to selecting Apply.
- The help text for the global configuration command **sntp server** incorrectly implied that it disabled the local SNTP server, although the command only modified the local SNTP client.
- The destination IP address displayed in the output of the **debug snmp** command would indicate that the ADTRAN unit was sending a reply to one of its local IP addresses.
- NetVanta units did not respond with the correct ICMP message when a UDP traceroute was directed at the unit.
- In rare cases on a NetVanta 1535P, the ActivReach connection failed to achieve link.
- The GUI Cable Diagnostics menu would not automatically refresh.
- The Ping utility in the GUI would display a more latent ping time for the first ping.
- The default SSID on a NetVanta 150 did not display properly on the virtual access point (VAP) configuration menu.
- Removing the traffic shape rate configuration from an interface resulted in two bandwidth configurations on the interface.
- Output from **show interface [ethernet** <*slot/port*> **| gigabit-ethernet** <*slot/port*>**]** command displayed incorrect information about the queuing implementation of the interface when 802.1q encapsulation was applied.
- The AOS CLI removed existing child QoS maps from a parent QoS map's configuration when attempting to remove an alternate, nonexistent child QoS map from the parent QoS map prompt.
- The **max-reserved-bandwidth** command was removed from an Ethernet interface when changing the encapsulation to 802.1q.
- HDLC keepalives could not be disabled from the CLI.
- The Analog Modem DIM would not function when attached to a second generation Dual T1 NIM.

This section highlights the voice specific bug fixes in products running AOS version R10.5.0, unless otherwise noted.

- Received SIP messages that contained more than one SDP media description caused a reboot.
- When using MGCP against a Metaswitch, if the Metaswitch instructed the unit to play a call waiting tone, audio would be lost if the second incoming call was not answered.
- When using SIP proxy user templates in stateful mode, ACK messages may not have been sent with the correct IP address in the Request-URI.
- With remote phones configured, if a remote phone sent a BYE without a Contact header, the corresponding 200 OK was sent to UDP 5060 instead of the layer 4 source port received in the BYE.
- On a Total Access 900 or Total Access 900e, if a user navigated to the T1 interface GUI menu from the physical interfaces GUI menu and enabled Continuous Refresh for the T1 statistics, the T1 would begin taking clock slips if timing was being provided on that interface.
- If an IPBG was configured with Australia as the country code, there would be a five second delay in the ring cadence between the first and second ring.
- Output of the **show voice quality-stats** command may have displayed a larger average delay than the maximum value.
- The Remote section of the **show media-gateway session** command output displayed **SIP description** for all calls, including MGCP calls.
- Out of Order packets may have appeared as a negative value in the **show voice quality-stats** command output.
- If an unsupported packetization period was presented to the ADTRAN unit in an SDP answer, no indication that the presented ptime was not supported by the ADTRAN unit was sent to the remote user agent. This resulted in no talk path.

Errata

The following is a list of errata that still exist in all products running AOS version R10.5.4.

- Flooding a unit with invalid IPv4 packet fragments when the firewall is enabled can cause a reboot.
- When TACACS+ accounting is enabled, it is possible for a long duration brute force SSH attack to cause the unit to run out of memory and reboot.
- On a NetVanta switch, LLDP-MED may stop functioning properly after a long period of uptime. Rebooting the switch will resolve the issue.
- The MRRU value in output of the **show interface ppp** command always displays default MRRU of 1520, regardless of what is negotiated between the two PPP peers. This issue is purely cosmetic.
- The GetResponse after an SNMP inform can be rejected causing a retransmission of the inform message.
- Naming a hardware ACL the same name as a previously created and deleted IP ACL will result in the creation of an IP ACL with an implicit permit.
- Configuring a NetVanta 160's channel setting to **least-congested** may not properly adjust to the least congested channel available.
- In rare cases, ICMP probes may transmit faster than the configured period.
- On the NetVanta 3130, the **Multi No T.413** ADSL training mode option is not displayed in the GUI.
- On the NetVanta 3130, the **ADSL2+ Annex M** ADSL training mode option is not present in the GUI.

- On certain NetVanta routers, it is not possible to remove SNMP users.
- 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 a NetVanta 6310, if a SHDSL circuit with a detected bad splice retrains to a different line rate, the distance of the bad splice will display incorrectly.
- 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.
- The T1 EFM counters do not increment as traffic passes through the device.
- With the SHDSL ATM NIM2, the NetVanta 6310 drops approximately 1 out of every 15K packets from the SHDSL to Ethernet direction.
- Performance throughput for 66 byte packets on the NetVanta 6355 4 T1/NAT test cases has decreased approximately 40 percent. All other packet sizes, including IMIX traffic, have acceptable throughput.
- 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.
- Performance issues may be experienced when using the SHDSL ATM NIM2 on the NetVanta 6310/6330.
- In redundant Ethernet mode, if the Ethernet interface is configured with subinterfaces, the NetVanta 644 will reboot when one of the Ethernet cables is removed.
- Copying a file larger than 20 MB from flash memory of an AOS device via HTTP can cause the AOS device to reboot.
- In rare cases, SFP ports on a NetVanta 1535P could get stuck in an up/up state even when physically disconnected. Shutting down the port and re-enabling it resolves the issue.
- The GUI of a NetVanta device acting as a wireless access controller can not display the software currently running on a connected access point.
- The command **boot config flash** <*filename*> does not function properly on many AOS platforms.
- A hostname entry in an ACL may fail to resolve to the correct IP even though the router's host table reflects the correct IP address.
- In a 3G demand interface configuration, Syslog traffic can intermittently be sourced from an incorrect IP address.
- When command authorization is enabled, issuing a **show** command with the **realtime** parameter does display statistics in real time.
- The IP Top Talkers Graphs in the GUI will sometimes truncate IP addresses.
- Enabling **debug icmp probe** while **debug probe** is also enabled causes a slow memory leak.
- The **show interface adsl** command is not an available in user mode.
- Event messages indicating a firmware upgrade was attempted may appear in the AOS event log for NetVanta 160 APs that are not being upgraded.
- Having more than two entries in a Network Monitor ICMP probe test list displays **Tracked by: Nothing** in the **show probe** command output. This is only a display error; the probes still function correctly.
- In the GUI, VQM may display a loopback interface when no loopback interface is configured.
- When configured for **terminal length 0** certain **show** commands will not provide complete output.

- The VNS verification process does not remove inconsistent A-type records from the host table after the configured number of attempts.
- Configuring greater than 1200 VNS entries on the NetVanta 3448 causes a SIP Pre-Parse error.
- 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**
- A QoS policy applied to a subinterface can only mark inbound packets.
- Wi-Fi multimedia (WMM), configured with the command **qos-mode wmm,** does not function properly on NetVanta 150 Access Points.
- When configured with two port channels, each with more than two members, one of the port channels may not evenly distribute traffic sent over the aggregated link.
- A NetVanta 1638 may occasionally display the following message on boot: HTTP_CLIENT CONNECT_TO_HTTP_SERVER errorCode 251. This does not cause a functional problem.
- The **called-number** command on a demand interface does not function properly.
- It is possible to create a standard MAC ACL with the same name as an existing extended MAC ACL.
- The NetVanta 1638 cannot boot from a firmware image stored on a connected USB flash drive.
- 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.
- WEP encryption does not function properly on NetVanta 160s.
- Legacy switch stacking can not be configured if VLAN 2386 is created prior to enabling stacking.
- 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.
- In certain scenarios, the H.323 ALG may not properly translate the application layer information.
- 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.
- When a switchport on a NetVanta 1535P is running forced speed 100 Mbps in standard mode (not ActivReach mode), jumbo frames greater than 9000 bytes will be dropped.
- The chassis fans in some NetVanta PoE switches oscillate at a higher frequency than expected during periods when the switch is not being heavily utilized.
- The current AOS implementation of DHCP message construction may result in Windows XP machines not adopting the DNS servers defined in the DHCP Offer. A workaround using a numbered IP/hex option will allow the message to be constructed in a manner that Windows XP will accept. Microsoft also offers a hotfix to resolve this Windows issue.

- The 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.
- NetVanta 1500 and NetVanta 1600 Series switches may not properly prioritize traffic across port channels.
- Certain OIDs in the Bridge-MIB may not return a value on a second generation NetVanta 123X switch.
- Certain commands referencing an ACL that uses quotations and spaces cannot be saved properly.
- The Layer 3 switch incorrectly reports forwarded frames statistics when subjected to a traffic stream consisting of invalid IPv4 header checksum values. The frames are properly dropped by the switch, but the statistics counter erroneously reports frames being forwarded
- 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 3G CDMA NIM may not function properly.
- The parent map QoS statistics must be cleared in order to clear the child map statistics.
- The NetVanta 7100 and NetVanta 6355 platforms will fail to reset statistics for applied QoS maps when the **clear counters** command is executed.
- A specific QoS map entry cannot be cleared without the entire map being cleared.
- In rare cases, when an IP PBX and IP phones are both passing through a NAT and the SIP proxy on an AOS device, some call flows can enter a one-way-audio state. Enabling the **ip rtp firewall-traversal enforce-symmetric-ip** command from the Global Configuration mode works around the issue.
- 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.
- Removing an NTP server configuration does not properly remove that server from the NTP associations table.
- When a QoS map is applied to a VLAN interface, the NetVanta 3448 and 3458 platforms fail to reset QoS map statistics after the **clear counters** command is issued. The **clear qos map** command will clear the statistics properly.
- The VLAN ID for an access point cannot be changed using the GUI.
- The **show atm pvc** counters do not increment.
- The **show bridge** <*number*> command might not show any entries.
- Using SCEP, AOS devices can fail to enroll certificates to a Red Hat Certificate Authority.
- On a NetVanta 1534, if an interface is configured as a port mirror destination (**monitor session 1 destination interface gigabit-switchport <*slot/port*>**), then port authentication will no longer be configurable on that port, even after removal of the **port mirror** command from the configuration.
- A VLAN interface for a VLAN that is not accessed by other switchports will not be advertised by GVRP.
- The NetVanta 1638 fails to count output discards when throttling down the transmission of traffic (as a result of receiving pause frames).
- 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.
- Adding an IPv6-enabled PPP interface to a bridge group does not require the user to first remove the IPv6 address from the PPP interface.
- Configuring a port channel on a NetVanta 3448 can cause the STP topology to become unstable.
- Switch platforms count input discards on the ingress interface when receiving 802.3x pause frames.
- Sierra Wireless USB305 3G modems are sometimes not recognized by the 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.
- The DNS server can take action on received DNS responses that are not associated with an open request, posing a DoS attack vulnerability.
- 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.
- The CLI does not display the correct value for Required Bandwidth in the event message generated by applying a QoS map.
- The output from **show qos map interface ppp 1** displays incorrect values for the number of packets sent.
- The NetVanta 5305 can fail to generate an event message to confirm that a QoS map has been applied.
- EAP Identity responses from a wireless client that do not contain an Identity field can result in a malformed RADIUS packet created by the NetVanta 150.
- The L3 Switch Header Error and Discard counters on the NetVanta 1544P (second generation) do not increment.
- The pass phrase for the Wireless Wizard does not persist across reboots.
- Removing and restoring cross-connects multiple times can cause the PC configuration thread depth to reach 100 percent.
- Rapidly removing and adding cross-connects using the CONSOLE port and SSH at the same time can result in a reboot.
- 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.
- NetVanta 150s might not properly handle immediate Access-Accept responses to Access-Request messages.
- In certain instances, an SFP port on a NetVanta 1544 will not function with RAD MiRiCi-E3T3 SFPs.

- 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.
- Port mirroring on a NetVanta 1544 switch may not mirror traffic in both directions.
- Proxy user templates cannot modify SDP IP addresses correctly in certain applications.
- Browsing to the Switchports menu from the Port Security menu on the NetVanta 1335 WiFi GUI results in a 503 Service Unavailable error.
- Connecting a Novatel U547 USB modem to the NetVanta USB WWAN NIM can cause the router to reboot.
- A startup configuration with greater than 2743 IPv6 prefixes on a VLAN interface causes the NetVanta 3448 to reboot.
- A Spanning Tree L2 broadcast storm lasting several hours can cause the NetVanta 1335 to reboot.
- Booting a second generation NetVanta 1534 or a NetVanta 1535 with greater than 20 NetVanta 160 Access Points (APs) attached can cause some of the APs to pull incomplete configuration from the NetVanta switch, if they are being used as the access controller for the APs.
- 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 local** may show an incorrect maintenance association for a MEPID if multiple maintenance associations are configured on the unit.
- 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.
- 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. Also, when the cursor hovers over a data point, it displays multiple instances of the same data.

The following is a list of voice specific errata that exist in products running AOS version R10.5.4, unless otherwise noted.

- When an FXS interface is configured for neon message waiting indication (MWI), the FXS port will lock up if a fault condition is experienced while the neon MWI is lit.
- SIP proxy failover may not function correctly when a SIP access class is applied to inbound SIP traffic.
- When outbound requests pass through the proxy and UDP is the specified transport, the transport-param may be removed.
- Call waiting caller ID may not function properly when received via a SIP INFO message instead of a new INVITE.
- On the NetVanta 644, hairpinned TDM calls may not have a talk path.
- In rare cases, it is possible for B-channel resources to not be released properly, preventing the channel from being used.
- In rare cases, the NetVanta 644 may reboot if a PRI interface goes down and then comes back up in quick succession.

- 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 both **g711alaw** and **g711ulaw** are present in a codec-list, G.711u will be chosen by modem-passthrough, even if **g711alaw** is listed higher in the codec-list than **g711ulaw**.
- The GUI should not provide a **Disable** setting for a voice user forward disconnect.
- In the PRI settings, invalid switch type options are presented in the GUI drop-down list.
- When **mwi-member** is configured on a ring group, received NOTIFY messages will not match against SIP identities/aliases configured on the ring group.
- When using **ringback override 180**, it is possible to have one-way or no audio after an inbound call completes due to the AOS device resending stale SDP.
- If a call is ringing due to a SIP 180 response for longer than the value of **ip rtp session timeout** (45 seconds by default), there will be no talk path in the SIP to TDM direction when the call is answered.
- When **voice codec-priority user** is configured, calls to a ring group can result in a less preferable CODEC being selected.
- If SDP without a media description is received, the call will fail.
- Local three-way conference calls against a Metaswitch will fail if one of the calls in conference is a hairpin call between two FXS users.
- In the ISDN voice trunk GUI, the **Disabled:Busy on Idle** and **Disabled:Busy Immediately** Administrative Status options do not function.
- On a NetVanta 6240, it is not possible to use the GUI to configure a PRI interface.
- If an ADTRAN unit is configured with single call appearance mode, forwarded calls on a PRI trunk will fail.
- Receiving a 183 after a 183 on hairpin calls when using media anchoring could result in no early media if the SDP in the second 183 differs from the first.
- Enabling VQM can cause audio to be lost when using the Simple Remote Phone feature.
- Echo cancellation is not enabled on 3-way calls when using the local conferencing feature.
- AOS does not properly handle more than two Diversion headers that are appended with a comma.
- On 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 not representative of how the audio actually sounds.
- DSP captures on the NetVanta 6240 and NetVanta 644 platforms consume large amounts of memory while in progress. The unit could become unstable if a DSP capture is active for an extended 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.
- In either a voice trunk or voice user with a CODEC list configured, entering **no codec-list** *<list name> <direction>* command will always remove *<list name>*, no matter which direction is configured.
- For E.164 SIP to PRI calls, the called party number will not be presented to the PRI unless the **voice-international-prefix abbreviated** command is enabled.
- Connection information (c=) in a media description does not override connection information in session description.
- If the route to the primary SIP server is invalid or points to null 0, SIP server rollover does not function properly.
- The CLI does not prevent users from configuring invalid SIP to PRI cause-code mappings.
- On the Total Access 900e platform, when 44 PRI calls (PRI to SIP direction only) and any number of analog calls (any direction) are active, the 44th PRI call will not connect approximately 80 percent of the time. Call flows of 44 PRI only calls and 44 SIP to PRI with analog calls function properly.
- On a second generation Total Access 900e with two PRI configurations, there will be no audio path on the 48th and subsequent calls.
- 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.
- 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. This occurs on the NetVanta 6310/6330 Series platforms only. 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 R10.5.4 or later specifically for the AOS products. These documents can be found on ADTRAN's Support Forum available at https://supportforums.adtran.com. You can select the hyperlink below to be immediately redirected to the document.

- *AOS Command Reference Guide*

- *NetVanta 160/161 Wireless Configuration Guide*
- *NetVanta 150 Wireless Configuration Guide*
- *Configuring IPv6 in AOS*
- *Configuring Call Queuing on the NetVanta 7000 Series*
- *Session Border Controllers in AOS*
- *Configuring SMDR Reports for the NetVanta 7000 Series*
- *Configuring Transcoding in AOS*
- *Configuring Media Anchoring in AOS*
- *AOS Voice International Configuration Guide*
- *Configuring the NetVanta 7000 Series Personal Phone Manager*
- *Configuring Music On Hold on the NetVanta 7000 Series*
- *NetVanta Ethernet Port Protection Device Quick Start Guide*
- *NetVanta 1230 Series (2nd Gen) Hardware Installation Guide*
- *NetVanta 1535P ActivReach Ethernet Switch Quick Start Guide*
- *NetVanta ActivReach Media Converter Quick Start Guide*