RELEASE NOTES

AOS Converged Access
AOS version R11.5.1
February 6, 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 R11.5.1 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 9*.

A list of new or updated documents for this release appears in *Documentation Updates on page 17*.

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 R11.5.1. 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 3140	√	√		R11.5.0
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

Platform	Standard Feature Pack	Enhanced Feature Pack	SBC Feature Pack	Minimum Boot ROM
NetVanta 6410			√	R11.3.0
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 R11.5.1 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 R11.5.1 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 R11.5.0.

- The **show lldp neighbor detail** and **show lldp neighbor interface** <*name*> **detail** commands now display the LLDP Inventory TLV information when present.
- Added the **ipv6 nd ra lifetime default-route** command to Layer 3 interfaces. When configured, if no IPv6 default route is present, the router lifetime value will be set to 0 for router advertisements sent out that interface.
- When **ipv6 mode host unicast** is configured on an interface, the IPv6 MTU will now be learned from received router advertisements.
- Added the ability to increase the event history size to up to 256 KB.

This section highlights the Carrier Ethernet specific features, commands, and behavioral changes available in products running AOS version R11.5.0.

- Added retransmission support per G.998.4 (G.inp) to the VDSL Carrier Ethernet module.
- Added vectoring support per G.993.5 to the VDSL Carrier Ethernet module.
- Added per-queue and per-EVC performance monitoring counters for increased visibility into packet flow behavior.

- Added support for hierarchical policers so that a two stage chain of policers can be created. Policers can now also be configured to be color aware and support coupling.
- Added the ability to automatically detect and switch between EFM bonded and non-bonded mode on the VDSL Carrier Ethernet modules by configuring **bonding auto-detect** on the EFM group interface.
- Increased the number of supported EVCs to 200.
- Added support for double-tagged Y.1731 MEPs. Previously only single-tagged MEPs were supported.
- Added support for the E-TREE MEF topology.
- Added support for E-LMI in PE mode as described in MEF 16.
- Added the ability to force the transmission of Y.1731 RDI based on the status of a configured track.
- Added the ability to filter traffic at Layer 2 based on the number of learned MAC addresses, the source MAC address, and EtherType.

This section highlights the Voice specific features, commands, and behavioral changes available in products running AOS version R11.5.0.

- Added support for SRTP and SIP over TLS on SIP-to-TDM calls on the NetVanta 6250, 6310, 6330, and Total Access 900e (third generation).

Fixes

This section highlights major bug fixes for all products running AOS version R11.5.1.

- On the NetVanta 3140, if the speed of a Gigabit Ethernet port was statically set to 100 or 1000 Mbps, and then the speed was changed to another value, a reboot may have been required before traffic could pass.
- Issuing the **test if interface switchport** <*slot/port*> or **test if interface xgigabit-switchport** <*slot/port*> commands on a track resulted in a reboot. These commands are invalid without the **line-protocol** parameter at the end (e.g. **test if interface switchport** <*slot/port*> **line-protocol**).
- 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.
- 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 has been disabled by default for the HTTPS server, SMTP client, Auto-Link client, Auto Config client, HTTPS packet capture export, and the **copy https** command. To enable SSL 3.0 support, an **allow-sslv3** parameter has been added to all of these clients and servers, with the exception of Auto-Link.

  Additionally, SSL 2.0 has been disabled in all of the previously mentioned clients. It was already disabled by default for the HTTPS server.
- Issuing the **crypto ca enroll** command resulted in the terminal length being set to 0.

This section highlights the Carrier Ethernet specific bug fixes in products running AOS version R11.5.1.

- If two EVC maps were identical except for the connected EVC, both improperly entered the **Running** state instead of both being disabled.

- If 802.3ah link OAM was enabled on an interface, issuing the **show ethernet oam discovery** or **show ethernet oam statistics** commands and pressing **<Enter>** to display additional lines resulted in CLI misalignment.

This section highlights the Voice specific bug fixes in products running AOS version R11.5.1.

- The LocalURI and RemoteURI fields in VQM PUBLISH messages were reversed for calls in the SIP-to-TDM direction.
- When using SIP TLS, during the TLS handshake process a very small amount of memory was leaked. This occurred when the device was acting as a TLS client or was acting as a TLS server and mutual authentication was enabled. If a large number of connections were created, a reboot would eventually occur.
- If a call on a voice loopback account received a reINVITE, audio was no longer looped. If no reINVITE was received, the voice loopback account would function normally.
- 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.
- When using SRTP with **ip rtp symmetric-filter** enabled, calls had one-way audio.
- 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.
- 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.
- When using SIP proxy user templates, in certain cases the Request-URI of inbound INVITEs was modified improperly.
- When using the SIP proxy, if a Remote-Party-ID header was improperly formatted, the SIP message containing the header was not proxied.
- 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.

This section highlights major bug fixes for all products running AOS version R11.5.0.

- Only the IANA client state was displayed in the output of the **show ipv6 dhcp interface** command. The IAPD client state was missing.
- When certain SFPs were inserted into a NetVanta 4660, 5660, 6250, or 6360, the laser temperature was incorrectly reported as 0 C.
- The output of the **show ipv6 dhcp pool** command did not list prefix information for prefix delegations.
- 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 would occur.
- When running large amounts of traffic, a reboot may have occurred if entries were added or removed from an extended access list that was referenced by a QoS map.
- 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.
- On the NetVanta 4660, 5660, 6250, and 6360, SFP DMI data did not display properly for some SFPs.
- On the NetVanta 4660, 5660, 6250, and 6360, inserting certain SFPs caused the CLI to become sluggish.
- If the control source port was changed on a TWAMP responder prior to a **no shutdown** being issued on the responder, a reboot would occur.
- Using certain software packages, compiling AdGenAosCommon.mib resulted in an error.
- The AOS TWAMP implementation did not comply with the RFC with regards to the token length of the SetupResponse message, which caused interoperability issues with other vendors. The implementation has been changed to comply with the RFC, however that change is not compatible with prior versions of AOS. To work with prior versions of AOS, the **legacy-setup-response-mode** parameter must be configured on the TWAMP probe or responder.
- 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.
- In rare cases, the unit's flash file system could not be accessed properly until the unit was rebooted.
- After issuing the **clear counters** command, the **show interface t1 0/1 performance-statistics Total-24-hour** command would not display the actual totals for the performance intervals.
- LLDP was not transmitted out PPP interfaces on the NetVanta 4305 when using the Octal T1 NIM.

This section highlights the Carrier Ethernet specific bug fixes in products running AOS version R11.5.0.

- On the NetVanta 6360, the system management EVC and system control EVC did not function properly.
- If an IPv6 neighbor solicitation flood was received, it was possible for local management traffic to be disrupted on the system management EVC and 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.

- Walking the HDSL2-SHDSL-LINE-MIB::hdsl2ShdslInventoryTable returned invalid data for some non-CPE elements on the SHDSL span.
- 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 Voice specific bug fixes in products running AOS version R11.5.0.

- 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.
- 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 would occur.
- With a high call rate and **modem-passthrough** enabled, it was possible to see SIP to ISDN call failures even though there were available B channels 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.
- When using the SIP proxy, the order of parameters inside the **uri** parameter of an Authorization header would be changed, invalidating the hashed response.
- When using the SIP proxy, in rare cases some SIP requests were routed to the wrong target.
- 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.
- If an emergency call failed and was then automatically retried, the INVITE for the retry did not contain a SDP offer, preventing early media from being sent.
- When configured, the **conferencing-uri** was used for the Request-URI, From, & 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 would improperly be used as the Layer 3 destination for new requests.
- When using MGCP, receiving caller ID information in a MDCX caused caller ID on that port to cease to function until the unit was rebooted.
- In rare cases, a reboot occurred while using the SIP proxy.
- Removing a voice trunk removed the password from all **sip-identity** statements that referenced that trunk.

Errata

The following is a list of errata that still exist in all products running AOS version R11.5.1.

- 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.
- Wi-Fi multimedia (WMM), configured with the command **qos-mode wmm**, does not function properly on NetVanta 150 Access Points.
- On the NetVanta 3120, 3130, 3448, and 3458, when traffic is flowing over one port in a channel group, if that port goes down, the port channel will bounce.

- On the NetVanta 3120, 3130, 3448, and 3458, removing and then re-adding ports to a port channel results in frames being looped between those ports.
- Routing performance on the NetVanta 3448 has decreased by roughly 27 percent compared to R11.5.0.
- Routing performance on the NetVanta 3305 has decreased by roughly 9 percent compared to R11.5.0.
- If an ECDSA or ED25519 key (both of which are unsupported) is presented to the SSH server, a **Bad string length** error will be returned instead of proceeding with the remaining authentication options.
- WEP encryption does not function properly on NetVanta 160.
- Exporting a packet capture to flash memory can result in audio loss while the file is being written to flash.
- 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.
- When viewing the Physical Interfaces page in the GUI on a unit with a T1 configured, a 503 Service Unavailable message is presented.
- In some command sets, the **exit** command is not visible even though it still functions properly.
- SNMP communities containing the @ character are not accepted on products with switchports.
- On the NetVanta 5305, VPN performance for 64 and 256 byte packets decreased moderately compared to R11.2.0.
- Rebooting a NetVanta 160 after editing an associated MAC access list causes the AP to transmit SSID **Wireless11**.
- 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.
- The **show interface dot11ap** <*number*> command may show an incorrect radio channel for a NetVanta 160.
- 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 GUI of a NetVanta device acting as a wireless access controller can not display the software currently running on a connected access point.
- An AOS device may print an event message in the CLI reporting a successful NetVanta 160 software upgrade, even if the upgrade has failed.
- The command **boot config flash** <*filename*> does not function properly on many AOS platforms.
- A 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 VLAN ID for an access point cannot be changed using the GUI.
- The **show atm pvc** counters do not increment.
- 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 R11.5.1.

- With a large number of EVCs configured, ELMI will not send all configured EVCs in a Full Status Message.

- If a queue shaper is created followed by a port shaper and the port shaper is subsequently removed or shut down, then the queue shaper cannot be properly removed or shut down.
- An up MEP configured on a UNI in an E-TREE topology will not function properly.
- Entering an invalid character in a **connect men-port** or **connect uni** statement on an EVC results in the EVC not functioning properly. The EVC must be removed to correct the invalid **connect** statement.
- The CLI will allow configuration of multiple MEN port connections to a MAC switched EVC. This configuration is not supported.
- The **service double-tagged s-tag <id> c-tag <id>** command is listed as an option for Y.1731 MEGs, but is not actually supported.
- On the NetVanta 6360, in rare cases a reboot may be seen when a VDSL Carrier Ethernet module is installed.
- If an EVC is added while the unit is the process of sending an ELMI FULL status continued message, the data instance (DI) bit is not incremented and the EVC is not added.
- In rare cases, a reboot occurred on the NetVanta 4660, NetVanta 5660, and NetVanta 6360.
- 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 R11.5.1.

- If a TDM-to-SIP call is in a PreConnected state due to receiving 183 Session Progress message, audio will only flow in the SIP-to-TDM direction, which may prevent interaction with some IVRs and voicemail systems.
- When running AOS R11.5.0 and higher, FQDNs configured on SIP trunks, VQM reporters, **voip name-service host** entries, the SIP proxy in stateful mode, and MGCP that rely on SRV records will fail if the transport in use is not TLS.
- The **rtp dtmf-relay** and **rtp media** command sets on SIP trunks are not present on the NetVanta 3430, 3448, 4430, and 6410 SBCs.
- On a SIP to ISDN call, when an ISDN timeout occurs, the unit will send a 400 Bad Request response instead of the more appropriate 408 Request Timeout response.
- The **t38 cng-relay-selective** command does not function properly on the NetVanta 6250, 6360, or Total Access 900e (third generation).
- In rare cases, a response received by the SIP proxy may cause a reboot.
- Receiving early media SDP on a call that results in hairpin media and also requires DTMF transcoding will result in the call failing to connect and being torn down immediately.
- On the NetVanta 6250, 6360, and Total Access 900e (third generation), DTMF tones that are shorter than the minimum valid digit requirement are still being qualified as valid digits.
- Accessing the **Voice** > **System Parameters** or **Voice** > **VoIP Settings** pages in the GUI results in a 503 Service Unavailable message.
- When using RTP firewall traversal, if the SIP device behind the AOS unit changes RTP ports in SDP and is slow to actually start using the new ports, the NAT session for the new RTP stream may be unexpectedly removed.

- When using optional SRTP, if a call is answered and SRTP cannot be negotiated because there are no common cipher suites, a reboot will occur.
- The GUI allows the SNMP link status traps to be enabled and disabled for FXS and FXO interfaces, but the changes cannot be saved.
- Removing a voice trunk while calls are active may result in the unit rebooting.
- Received SDP offers containing a rejected audio media stream and an image media stream are not handled properly. In this scenario, the audio media is preferred and the image media is ignored resulting in erroneous behavior.
- When generating an SNMP trap for a SIP proxy rollover, the wrong OID is used for adSipProxyRollover.
- Issuing the command **clear voice call active** with active MGCP calls may result in a reboot.
- On the NetVanta 6250 and Total Access 900e (third generation) with MGCP configured, harmless pthread messages are seen on the console during boot up. They are also seen when adding or deleting IP routes that cause the MGCP endpoints to restart.
- 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 mandatory SRTP is configured on a voice trunk, calls will still be established if SRTP is not received in the SDP answer.
- 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.
- 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 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.

- 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 s**how 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 R11.5.1 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*
- *Configuring QoS in AOS*
- *Carrier Ethernet Services in AOS*
- *Carrier Ethernet Services QoS Guide*
- *Network Monitoring in AOS*
- *SNMP in AOS*
- *Configuring Ethernet OAM for Y.1731*
- *IPv6 in AOS*
- *SIP Signaling and Media Security in AOS*
- *DHCPv6 in AOS*

