

AOS

R13.2.3

Release Notes

To the Holder of this Document

This document is intended for the use of ADTRAN customers only for the purposes of the agreement under which the document is submitted, and no part of it may be used, reproduced, modified or transmitted in any form or means without the prior written permission of ADTRAN.

The contents of this document are current as of the date of publication and are subject to change without notice.

Trademark Information

“ADTRAN” and the ADTRAN logo are registered trademarks of ADTRAN, Inc. Brand names and product names included in this document are trademarks, registered trademarks, or trade names of their respective holders.

Disclaimer of Liability

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products are given “as is”, and any liability arising in connection with such hardware or software products shall be governed by ADTRAN’s standard terms and conditions of sale unless otherwise set forth in a separately negotiated written agreement with ADTRAN that specifically applies to such hardware or software products.

To the fullest extent allowed by applicable law, in no event shall ADTRAN be liable for errors in this document for any damages, including but not limited to special, indirect, incidental or consequential, or any losses, such as but not limited to loss of profit, revenue, business interruption, business opportunity or data, that may arise from the use of this document or the information in it.



©2018 ADTRAN, Inc.
All Rights Reserved.

Revision History

Rev A	January 2019	This document supports AOS R13.2.3.
-------	--------------	-------------------------------------

Table of Contents

1	Introduction	7
2	Supported Platforms	7
3	System Notes	9
4	Features and Enhancements	9
4.1	Voice Features in R13.2.1	9
4.2	General Features in R13.2.0	9
4.3	Carrier Ethernet Features in R13.2.0	10
4.4	Voice Features in R13.2.0	10
5	Fixes	10
5.1	General Bug Fixes in 13.2.3	10
5.2	General Bug Fixes in 13.2.2	10
5.3	General Bug Fixes in 13.2.1	10
5.4	General Bug Fixes in 13.2.0	11
5.5	Carrier Ethernet Specific Bug Fixes in 13.2.0	12
5.6	Voice Specific Bug Fixes in 13.2.3	12
5.7	Voice Specific Bug Fixes in 13.2.2	12
5.8	Voice Specific Bug Fixes in 13.2.1	13
5.9	Voice Specific Bug Fixes in 13.2.0	13
5.10	Switch Specific Bug Fixes in 13.2.3	14
5.11	Switch Specific Bug Fixes in 13.2.2	14
5.12	Switch Specific Bug Fixes in 13.2.1	14
5.13	Switch Specific Bug Fixes in 13.2.0	15
6	Errata	15
6.1	General Errata	15
6.2	Carrier Ethernet Specific Errata	17
6.3	Voice Specific Errata	18
6.4	Switch Specific Errata	19
7	Upgrade Instructions	20
8	Warranty and Contact Information	20
8.1	Warranty	20
8.2	Contact Information	20

List of Tables

Table 1. Supported Platforms 7

1 Introduction

AOS version R13.2.3 is a maintenance release that addresses customer issues that were uncovered in previous code releases.

This release is generally available code. Results obtained during internal testing have been evaluated and the code has been determined to be ready for general availability. Caveats discovered during testing but not addressed in this build are listed in “Errata” on page 15.

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.

2 Supported Platforms

Table 1 lists the platforms that are supported in AOS version R13.2.3. 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.

Table 1. Supported Platforms

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 3140	✓	✓	✓	R11.5.0

Table 1. Supported Platforms (Continued)

Platform	Standard Feature Pack	Enhanced Feature Pack	SBC Feature Pack	Minimum Boot ROM
NetVanta 3200/3205 (3rd Gen.)	✓	✓		17.02.01.00
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

3 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 R13.2.3 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 R13.2.3 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)

4 Features and Enhancements

4.1 Voice Features in R13.2.1

This section highlights the major Voice related features, commands, and behavioral changes for products running AOS version R13.2.1.

- SIP TLS and SRTP is now supported on calls between two SIP trunks on the NetVanta 3140, 3430 (second generation), 3448, 6250, 6310, and 6330 SBCs and the Total Access 900e (third generation) SBCs.

4.2 General Features in R13.2.0

This section highlights major features, commands, and behavioral changes for all products running AOS version R13.2.0.

- Added the ability to display thresholds for, and send SNMP traps for, the following SFP diagnostic parameters: Tx power, Rx power, Supply voltage, Bias current, and Laser temperature.
- Added the ability to query VDSL status and performance monitoring statistics via SNMP on the NetVanta 4660, 5660, and 6360.
- Added the ability to configure a hostname or FQDN as a SNMP trap target.

4.3 Carrier Ethernet Features in R13.2.0

This section highlights the major Carrier Ethernet related features, commands, and behavioral changes for products running AOS version R13.2.0.

- Added the ability to query interface, queue, dynamic counter, and MEF performance statistics via SNMP on the NetVanta 4660, 5660, and 6360. Additionally, user login and logout SNMP traps were added.

4.4 Voice Features in R13.2.0

This section highlights the major Voice related features, commands, and behavioral changes for products running AOS version R13.2.0.

- Added the ability for the SIP proxy to reuse existing client SIP connections when devices behind the SIP proxy are running SIP over TCP.

5 Fixes

5.1 General Bug Fixes in 13.2.3

This section highlights major bug fixes for all products running AOS version R13.2.3.

- Fixed an issue in which the session may have disconnected when pasting in a large block of text over Telnet or SSH.
- Fixed an issue in which the packet capture maximum memory threshold was set to 16MB when values greater than 16MB were configured.

5.2 General Bug Fixes in 13.2.2

This section highlights major bug fixes for all products running AOS version R13.2.2

- Fixed an issue in which the DNS table was flushed during every DHCP renewal instead of only if the set of DNS servers in the DHCP ACK had changed if **domain-lookup flush on-server-change** was configured.
- Fixed an issue in which a reboot may have occurred when an entry in the DNS cache used by an ACL or SNMP was refreshed due to TTL expiration. This reboot may have also occurred if the list of configured DNS servers was modified.
- Fixed an issue in which a DNS server learned via DHCP was not promoted to the primary server and would not be used if that server was originally listed as a secondary DNS server in the DHCP ACK, but upon DHCP renewal that server was now listed as the primary server in the DHCP ACK.
- Fixed an issue in which SCEP enrollment failed if the URL did not end in a '/'.
- Fixed an issue in which the CLI became sluggish when a 1442310F1 or 1442311F1 pseudowire (PWE) SFP was installed. Over time, a lockup may have occurred.

5.3 General Bug Fixes in 13.2.1

This section highlights major bug fixes for all products running AOS version R13.2.1

- Fixed an issue in which NTP mode 6 and 7 queries were processed upon receipt. NTP mode 6 and 7 queries are now rejected.

- Fixed an issue in which **auto-config mac-auth interface** defaulted to 000000000000 instead of the MAC address of the first Ethernet or Gigabit Ethernet interface on the NetVanta 3140, 6250, 6360, 6410, and Total Access 900e (third generation).
- Fixed an issue in which the value of **auto-config filename** was stored in the configuration without being surrounded by double quotes, which resulted in config restoration errors if the filename contained a space or question mark.
- Fixed an issue in which a leading space was added before the facility when syslog messages were sent. This space prevented some servers from parsing the messages.
- Fixed an issue in which an error was displayed on the console stating that the received primary address did not match the configuration if the primary and secondary IP addresses were specified in different orders between units in a VRRPv3 pair. The error message has been removed because this is a valid configuration.
- Fixed an issue in which a reboot occurred if the received IKE hash payload length exceeded the maximum of 20 bytes.
- Fixed an issue in which the **bandwidth** configuration parameter on interfaces could not be changed to a value other than zero in AOS R12.2.0 and later.

5.4 General Bug Fixes in 13.2.0

This section highlights major bug fixes for all products running AOS version R13.2.0

- Fixed an issue in which the RADIUS or TACACS+ connection would fail due to lack of DNS resolution if the configured server was not resolvable via the default VRF. This failure occurred because DNS queries were sent via the default VRF for a RADIUS or TACACS+ server configured in a named VRF.
- Fixed an issue in which a 503 Server Error was returned on the NetVanta 3448 and 3458 when *Apply* was clicked on an interface's page under Spanning Tree Port Information on the Data->Spanning Tree page in the GUI.
- Fixed an issue in which an error with no text was returned if **ip pim sparse-mode** was configured on an interface that did not have an IPv4 address configured.
- Fixed an issue in which a reboot infrequently occurred when AAA accounting was enabled.
- Fixed an issue in which any entered value greater than 2147483647 for the **dampening-interval** on a track was improperly stored in the configuration as 2147483647.
- Fixed an issue in which a reboot occurred if a fragment chain was sent to a local service running on the unit (e.g. SIP, GRE, etc.).
- Fixed an issue in which LLDP messages were not received on the NetVanta 4660, 5660, and 6360.
- Fixed an issue in which issuing the **show dot11 access-point detail** command sometimes resulted in a reboot.
- Fixed an issue in which the CLI would hang for several seconds after the prompt was returned when issuing the **ssh key regenerate** command.
- Fixed an issue in which a reboot occurred when email logging was used with certain SMTP servers that supported STARTTLS.
- Fixed an issue in which the output of **show ssh-server mypubkey** displayed an incorrect value for the RSA public key.

5.5 Carrier Ethernet Specific Bug Fixes in 13.2.0

This section highlights Carrier Ethernet specific bug fixes in products running AOS version R13.2.0.

- Fixed an issue in which traffic would not egress any layer 3 subinterfaces that had an outbound QoS policy applied if a non-default **ce-vlan-id tpid** was configured.

5.6 Voice Specific Bug Fixes in 13.2.3

This section highlights Voice specific bug fixes in AOS version R13.2.3.

- Fixed an issue in which received INVITEs with a tel URI in the From header were rejected.
- Fixed an issue in which AOS failed to unregister from the currently selected server when switching to a new server if validated SIP trunk failover was configured.
- Fixed an issue in which an error was returned when attempting to enable **sip tls** if a SIP access-class was applied.
- Fixed an issue in which SIP packets were sourced from 127.0.0.1 instead of the configured media-gateway address of the egress interface when the configured outbound-proxy on a SIP trunk resolved to both IPv4 and IPv6 addresses and only the IPv4 address was routable by the unit.
- Fixed an issue in which a reboot infrequently occurred if the D channel on a PRI bounced.
- Fixed an issue in which receipt of a malformed SIP message infrequently resulted in a reboot.
- Removed the unsupported **main-phone-number** configuration parameter for voice trunks.

5.7 Voice Specific Bug Fixes in 13.2.2

This section highlights Voice specific bug fixes in AOS version R13.2.2.

- Fixed an issue in which a reboot occurred if a **sip proxy failover group** was removed while **no sip proxy** was configured.
- Fixed an issue in which the SIP B2BUA failed to roll to the next configured server if **null 0** was the target of the route to the currently selected SIP server.
- Fixed an issue in which a reboot occurred in rare scenarios involving a call being placed on hold.
- Fixed an issue in which the ringback, silence, and busy signal tone files were missing from the NetVanta 3140, 4660, and 5660.
- Fixed an issue in which a currently established call would be disconnected if a new INVITE was received on a voice user that triggered call waiting and then a reINVITE for the currently established call was received while the voice user was in a call waiting state.
- Fixed an issue where HMR intercept policies were sometimes not processed on received INVITEs.
- Fixed an issue in which Call-ID variables did not work in HMR intercept policies.

5.8 Voice Specific Bug Fixes in 13.2.1

This section highlights Voice specific bug fixes in AOS version R13.2.1.

- Fixed an issue in which the SDP answer generated by the unit did not contain the tag and crypto-suite from the accepted crypto attribute in the SDP offer if SRTP keys containing the MKI:length parameter were present in a SDP offer.
- Fixed an issue in which call transfers or forwards from the RTP leg that would result in hairpinned SRTP to SRTP media failed if a SIP trunk to SIP trunk call was using SRTP on one leg and RTP on the other.
- Fixed an issue in which a pair of ports was leaked from the RTP NAT port pool when using the SIP proxy without media anchoring if a call was placed on hold for longer than 60 seconds before resuming the call. Eventually calls began to fail when there were no available ports remaining.
- Fixed an issue in which a reboot occurred in rare scenarios involving a local 3-way conference.
- Fixed an issue in which A records may not have been refreshed properly and could have dropped out of the host table if the TTL of a DNS SRV record differed from the TTL of the derived A records. This discrepancy resulted in call failures.
- Fixed an issue present in R12.3.2, R12.3.3, R12.3.4, and R13.1.0 and later in which the transferor was no longer able to break dial tone if an unattended transfer was attempted from one FXS port to another FXS port on the same unit and the transfer was not completed.
- Fixed an issue in which the call was improperly rejected if a * or # was contained in the called or calling party number IEs of an ISDN setup message.
- Fixed an issue in which the SIP proxy improperly entered local survivability if a route to a secondary SIP proxy server was still available. This issue occurred if the SIP proxy monitor was enabled in **stateful-transparent** mode and the route to the primary configured SIP proxy server was removed (e.g., the egress interface went down).
- Fixed an issue in which the Via header was not populated with the ephemeral source port that was in use when using SIP TLS in client-only mode.

5.9 Voice Specific Bug Fixes in 13.2.0

This section highlights Voice specific bug fixes in AOS version R13.2.0.

- Fixed an issue in which a specially crafted SIP request was able to bypass the validation that ensures the request was from an authorized source before it was processed.
- Fixed an issue in which a 200 OK response was sometimes not sent if a CANCEL was received on a valid SIP dialog when using the SIP proxy.
- Fixed an issue in which caller ID information from the previous call was sent to the phone if the current call did not contain a SignalRequest for L/ci in the MGCP signaling.
- Fixed an issue in which one-way audio occurred after the call connected if an inbound MGCP call was initiated with a CRCX immediately followed by another MGCP request containing a SignalRequest for L/ci.
- Fixed an issue in which the SIP trunk monitor did not consider the resolved IP address and port when updating the status of server entries.
- The DNS client debug was enhanced to make it clear when a DNS request was being answered from the DNS cache.

- Fixed an issue in which the SIP proxy failed to spoof 200 OK responses to REGISTER requests 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).
- Fixed an issue in which the unit rebooted if a **sip proxy failover group match-value** command was configured while the SIP proxy was disabled.
- Fixed an issue in which a reboot occurred if an HMR intercept policy was shutdown, had changes made to it, and then was re-enabled.
- Fixed an issue in which the persistent connection was continuously torn down and re-established if two different FQDNs were used for SIP TLS with persistent connections and the FQDNs both resolved to the same IP address.
- Fixed an issue in which phones were prevented from entering survivability because the SIP proxy did not spoof a 200 OK response if all servers failed to reply to a REGISTER when using the proxy monitor with the SIP proxy in transparent mode.
- Fixed an issue in which BYE requests destined for the network were sent to the primary configured server instead of the server with which the call was in-dialog when using the SIP proxy.
- Fixed an issue in which the **debug interface t1 0/x rbs** output stated **Valid Wink Received** if a valid wink had not been received on an E&M wink trunk.
- Fixed an issue in which no audio was present on a PRI to SIP hairpin call if the inbound SIP call immediately transitioned from ALERTING with inband audio to CONNECT.
- Fixed an issue in which an inbound SIP call would be matched to the first trunk that matched the host in the P-Asserted-Identity header even if there was a better match on a different header (e.g., Via) in which the port and transport both matched. This issue occurred if **trust-domain** was configured on a SIP voice trunk and a P-Asserted-Identity header was present in an inbound INVITE.

5.10 Switch Specific Bug Fixes in 13.2.3

This section highlights Switch specific bug fixes in AOS version R13.2.3.

- Fixed an issue in which a memory leak may have occurred when using IGMP snooping on a NetVanta 1638.
- Fixed an issue in which the NetVanta 1638 switches configured for ActivChassis would occasionally reboot during upgrades.

5.11 Switch Specific Bug Fixes in 13.2.2

This section highlights Switch specific bug fixes in AOS version R13.2.2.

- Removed the restriction that only allowed ADTRAN branded SFP+ modules on the NetVanta 1550 and 1638.
- Fixed an issue in which the NetVanta 1531 and 1550 did not properly reassemble fragment chains sent to the local IP stack.

5.12 Switch Specific Bug Fixes in 13.2.1

This section highlights Switch specific bug fixes in AOS version R13.2.1.

- Fixed an issue in which some 1700485F1 10GBASE-SR SFP+ modules were reported as not supported when installed in NetVanta 1550 and 1638 switches.

- Fixed an issue in which ARP responses from peer routers did not properly get added to the ARP table on the NetVanta 1638.
- Fixed an issue in which the 1200485G1 1000BASE-T SFP sometimes did not properly establish link when installed in a NetVanta 1550 switch.
- Fixed an issue in which a reboot occurred when using IGMP snooping in rare cases.
- Fixed an issue in which ARP packets sourced from and destined to the system may have been dropped when the NetVanta 1638 was used in ActivChassis configurations.

5.13 Switch Specific Bug Fixes in 13.2.0

This section highlights Switch specific bug fixes in AOS version R13.2.0.

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

6 Errata

6.1 General Errata

The following is a list of errata that still exist in all products running AOS version R13.2.3.

- Daylight savings time rules for the Canberra, Australia (GMT+10) time zone are incorrect.
- If a hostname or FQDN is configured as a SNMP trap target, DNS queries will be re-attempted on an exponential backoff if both A and AAAA DNS records do not exist for the configured hostname.
- If an interface is administratively disabled (i.e. shutdown), a linkDown SNMP trap is sent even if the interface is already in the operDown state.
- During periods of heavy CPU load, **message read failed** errors may be displayed on the console if a VDSL module is installed. These messages are benign.
- 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 if 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 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 local** 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.

6.2 Carrier Ethernet Specific Errata

The following is a list of Carrier Ethernet specific errata that exist in products running AOS version R13.2.3.

- The Invalid CE VLAN ID counter does not function on the GigabitEthernet 0/1 interface on the NetVanta 4660, 5660, and 6360 because GigabitEthernet 0/1 is not intended for use as a UNI interface on these platforms.
- The **efm-group** interface type option is missing from the **tunnel source** command on Tunnel interfaces.

6.3 Voice Specific Errata

The following is a list of Voice specific errata that exist in products running AOS version R13.2.3.

- 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.
- 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 does not contain G.711.
- The command **ip mgcp qos dscp <value>** will not take effect until either **ip mgcp** is disabled and then re-enabled or the AOS device is reset.
- When the SIP server monitor clears the primary SIP server from a delayed state due to a failure of the secondary SIP server, there will be a 60-second delay until a SIP registration is attempted to the primary SIP server. This delay will not occur if the SIP server monitor is clearing the secondary SIP server from a delayed state due to a failure of the primary SIP server.
- On the Total Access 900e (third generation) and NetVanta 6250, SIP must be enabled in the running configuration whenever MGCP is used for voice.
- 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.

6.4 Switch Specific Errata

The following is a list of Switch specific errata that exist in products running AOS version R13.2.3.

- 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.
- Creating a hardware ACL with the same name as a previously created and deleted IP ACL will result in the creation of an IP ACL with an implicit permit.
- Removing port channels from the configuration while an ActivChassis is under a heavy load could cause the ActivChassis to reboot.
- On NetVanta 1638 units 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.

7 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://support-forums.adtran.com>.

8 Warranty and Contact Information

8.1 Warranty

Warranty information can be found at:

www.adtran.com/warranty.

8.2 Contact Information

For all customer support inquiries, please contact ADTRAN Customer Care:

Contact	Support	Contact Information
Customer Care	From within the U.S. From outside the U.S. Technical Support: <ul style="list-style-type: none"> ■ Web: Training: <ul style="list-style-type: none"> ■ Email: ■ Web: 	1.888.4ADTRAN (1.888.423.8726) + 1.256.963.8716 www.adtran.com/support training@adtran.com www.adtran.com/training www.adtranuniversity.com
Sales	Pricing and Availability	1.800.827.0807