RELEASE NOTES

AOS version R10.3.3
March 4, 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

Copyright © 2013 ADTRAN, Inc.
All Rights Reserved.

Contents

Copyright © 2013 ADTRAN, Inc.

Introduction

AOS version R10.3.3 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 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 R10.3.3. 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.

Platform	Standard Feature Pack	Enhanced Feature Pack	SBC Feature Pack	Minimum Boot ROM
NetVanta 644		√		A5.01.B1
NetVanta 1234 (2nd Gen.)	√			XB.01.02
NetVanta 1238 (2nd Gen.)	√			XB.01.02
NetVanta 1534	√			17.06.03.03
NetVanta 1534 (2nd Gen.)	√			17.08.01.00
NetVanta 1534P (2nd Gen.)	√			17.09.01.00
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
NetVanta 3458	√	√		17.06.01.00

Copyright © 2013 ADTRAN, Inc.

Platform	Standard Feature Pack	Enhanced Feature Pack	SBC Feature Pack	Minimum Boot ROM
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		√	√	A2.06.B1
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 R10.3.3 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 R10.3.3 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.

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 R10.3.0.

- Added support for Telnet on a nondefault VRF.
- Added support for a TFTP client configured in a nondefault VRF.
- Added support for IPv6 management of second generation NetVanta 1230 Series switches.
- Added support for commands that allow the user to modify the queue depth for priority queues on Gigabit Ethernet interfaces. Larger queue depths provide a mechanism to handle a greater number of small-packet bursts on Gigabit Ethernet interfaces that are marked as priority traffic.
- An SNMP trap can now be sent in the event of a DNS look-up failure.
- The DNS host table will now persist across a reboot.
- Added support on the NetVanta 1638 for an SFP XIM that supports 1 Gbps and 2.5 Gbps SFP modules.

Copyright © 2013 ADTRAN, Inc.

- The DNS proxy source interface feature will allow the user to configure the source address on an outbound DNS Request. The user will be able to specify an interface from which to take the source address. The interface from which the request leaves and the interface from which the request takes its source address must be on the same VRF. Both IPv4 and IPv6 are supported.
- Added IPv6 support for NTP.

This section highlights the voice specific features, commands, and behavioral changes available in products running AOS Version R10.3.0, unless otherwise noted.

- Added support for TCP/UDP interworking for SIP.
- The unit's serial number, configured host name, and a custom text string can now be included in the SIP User-Agent header. Also, it is now possible to prevent the firmware version from being included. These can be configured both globally and at the trunk level.
- Added support for automatically configuring local emergency number dial plan entries based on the configured voice system-country.

Copyright © 2013 ADTRAN, Inc.

Fixes

This section highlights major bug fixes for all products running AOS version R10.3.3.

- Assigning a non-default VRF to a PPPoE or a PPP interface traversing a Demand interface caused the AOS device to reboot once the associated PPP interface became active.
- A large amount of broadcast or multicast traffic being terminated by a NetVanta 1638 would prevent it from initiating certain types of locally generated traffic, including ICMP and VRRP advertisements.
- 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 be reached.
- 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.
- ATM interface counters would show incorrect input/output rate statistics.
- The Cable Diagnostics troubleshooting menu in the GUI would not automatically refresh.
- A large numbers of collisions on an Ethernet interface caused the interface to stop transmitting packets.
- In certain cases, security zone policies configured in the GUI would not match the CLI configuration.
- Adding a track with a space in its name to a route caused the route to be lost on reboot.
- When the ADSL interface on the Total Access 900 with ADSL2+ was administratively shut down, the Net LED remained red.
- The NetVanta 644 would not process ARP requests for IP addresses assigned to a loopback interface.

This section highlights the voice specific bug fixes in products running AOS version R10.3.3, unless otherwise noted.

- When using a network role PRI, if the ISDN T303 timer expired, it was possible for a reboot to occur.
- It was possible for an AOS unit to get into a state where it could no longer allocate ports for RTP sessions.
- Received Allow-Events headers that improperly used semicolons as a delimiter were not properly corrected.
- 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. It was possible for this to cause a delay in the connection of two-way audio.
- SIP Bridged Line Appearance SUBSCRIBE messages from a Sylantro SIP server would not properly pass through the SIP proxy.
- When using SIP over TCP, there was a small window of time in which a SIP message could be received, but not processed by the unit.
- 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 R10.3.2.

- In the CLI, the **logging forwarding auxiliary-receiver-ip** <*ip address*> command was not accepted as a valid command.
- 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.

Copyright © 2013 ADTRAN, Inc.

- 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.
- NetVanta units did not respond with the correct ICMP message when a UDP traceroute was directed at the unit.
- The default SSID on a NetVanta 150 did not display properly on the virtual access point (VAP) configuration menu.
- When using SIP proxy user templates in stateful mode, ACK messages were not sent with the correct IP address in the Request-URI.
- 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 R10.3.2, unless otherwise noted.

- Received SIP messages that contained more than one SDP media description may have 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.
- An inbound call on a user role PRI may have failed if the caller ID name was received after the initial ISDN Setup message.
- A reboot may have occurred when all of the following conditions were met:
    - A received SIP message (most likely an INVITE) contained a Diversion header.
    - The user portion of URI in the Diversion header was in E.164 format.
    - The country code in the Diversion user did not match the one configured on the unit.
    - The length of the Diversion user (including the '+') was less than 16, and the combined length of the configured IDD prefix and the diversion user (excluding the '+') was greater than or equal to 16.
- With remote phones configured, if a remote phone sent a BYE without a contact header, the corresponding 200 OK response was sent to UDP 5060 instead of the layer 4 source port received in the BYE.
- In rare cases, the NetVanta 644 would reboot when trying to place a T.38 fax call.
- 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.
- The **ip sip grammar from user international** command was not changing the From header in transmitted SIP messages to the E.164 format.
- In rare cases, it was possible that the ADTRAN unit would reboot if an INVITE with a malformed Replaces header was received.

This section highlights major bug fixes for all products running AOS Version R10.3.1.

- Editing an ACL in the GUI caused a 503 Service Unavailable response.
- Failed tracks would not properly disable tracked Crypto maps.

Copyright © 2013 ADTRAN, Inc.

- After applying changes to a VLAN interface, the side menu bar in the GUI would indicate the incorrect page was being displayed.
- In certain cases, when configured for NAT, an AOS device would not modify the host portion of the contact header to the correct IP address if the user originating the call did not already exist in the proxy user database. This only occurred when using user-templates with SIP transparent proxy.
- Attempting to append a custom BGP community with a route-map would always return the error **invalid community number**.
- Sending a DNS query for an empty hostname caused an AOS device to reboot.
- ICMP probes would not function properly with DNS names as the destinations.
- An AOS device rebooted while processing a particular sequence of HTTP requests if URL filtering was enabled.
- Accessing the DHCP Lease menu in the AOS GUI would generate a **could not eval** error.
- The SIP proxy would not forward a Register message if the Contact field contained only an asterisk (*).
- QoS maps with names longer than eight characters displayed improperly in the GUI.
- In the GUI, the DHCP Server displayed a 503 Service Unavailable error between the DHCP server setting table and the DHCP leases table.
- A-type host table entries (associated to a manually configured VoIP Name Service Host) were classified as sticky when an AOS router first booted up with VNS verification enabled.
- Issuing the **clear host *** command removed permanent SRV-type DNS entries from the host table.
- The QoS menu of the GUI would display available bandwidth for a PPP interface that was in a Link Down state.

This section highlights the voice specific bug fixes in products running AOS Version R10.3.1, unless otherwise noted

- If HMR was used to remove the topmost Via header, the unit could reboot upon receipt of a reINVITE.
- Total Access 900e only: If a PRI interface was placed into the shutdown state by the user, any layer 2 interface associated with a T1 configured for data would drop.
- With a user role PRI configured, it was possible that the ADTRAN unit would reboot if the calling party name was delivered from the PSTN for an inbound call.
- DNS entries used by voice services were not being communicated properly to the VoIP Name Service. This caused those entries to not be properly refreshed before their TTL expired, which caused the first call after the TTL expired to fail.
- When using the ringback override feature, it was possible for a reboot to occur when a terminating call to a busy subscriber briefly returned inband ringing before returning inband busy.
- AOS did not properly handle two Diversion headers that were appended with a comma.
- If the MWI lamp was illuminated on a user configured for NEON MWI, the FXS port tied to that user would lock up if the FXS user went on hook while in the battery disconnect state (due to the far end hanging up first).
- Received SIP UPDATE messages were rejected with a 503 Service Unavailable response. The proper response was a 200 OK with SDP.
- When using a Total Access 900e or a NetVanta 6300 Series device as a gateway for a NetVanta UC Server, it was possible that outbound T.38 fax calls from the UC server would fail.

Copyright © 2013 ADTRAN, Inc.

- On outbound MGCP calls against a Metaswitch, if the Metaswitch requested generation of local ringback, it was possible that there would be no audio in either direction.

This section highlights major bug fixes for all products running AOS version R10.3.0.

- With password encryption enabled, BGP authentication passwords were being encrypted a second time on reboot.
- The NetVanta 3120 would not respond to SNMP polls for VQM.
- Browsing to the Spanning Tree menu in the GUI could return a 503 Service Unavailable response.
- Generated checksums for the **show startup-config** and **show running-config** would not match when the configuration files were identical.
- Changing PoE settings using the GUI could cause a 503 Service Unavailable response.
- After upgrading to R10.1.0, the VQM reporter grammar options always showed up after booting, even if they were not configured.
- IPv6 traffic destined to 0:: was forwarded to the default gateway instead of being dropped.
- A QoS policy could not be configured on a demand interface.
- The IPv6CP protocol state could occur even when IPv6 was disabled on a PPP interface.
- When 802.1q encapsulation was disabled on an Ethernet interface, the interface could not be configured for **port-auth supplicant** mode.
- The Setup Wizard for a NetVanta 3120 became unresponsive on the System Info menu.
- Removing a PPP cross connection and then adding it back to a SHDSL interface caused the PPP interface to remain down, unless the SHDSL interface was disabled and then re-enabled.

This section highlights the voice specific bug fixes in IPBG and Gateway products running AOS version R10.3.0, unless otherwise noted.

- The default SIP authentication password for newly created voice users for the NetVanta 6355 product was random instead of the correct value of **1234**.
- In a PSTN gateway application, if an attended transfer was initiated towards the ADTRAN gateway, the transferor would send a REFER with Replaces to the gateway. The ADTRAN gateway should respond with an INVITE with Replaces back out the SIP trunk. If the transferor was the party that initiated the original call to the transferee, the INVITE was not sent. However, if the transferee initiated the original call, the INVITE was sent and the transfer executed properly.
- When using SIP over TCP, the source port displayed in the output of **debug sip stack messages** command was incorrect.

Errata

The following is a list of errata that still exist in all products running AOS version R10.3.3.

- A QoS policy applied to a subinterface will only mark inbound packets.
- On second generation NetVanta 123X switches, LLDP MED devices are not properly added to the MAC table when Port Security is enabled.
- In rare cases, the Ethernet port on the Total Access 900 series may falsely report an auto-negotiation event. This false detection will generate an event message, but no packets are dropped.

Copyright © 2013 ADTRAN, Inc.

- The AOS GUI will not display the PPP interface in a LOOPBACK state when the interface is looped.
- 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 some VPN clients that expect to receive this payload.
- When installed in a NetVanta 6310/6330 Series, the interface on a SHDSL Annex A NIM drops during RFC 2544 performance testing.
- 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 is properly advertised. This might cause problems when the more specific network needs to be routed to a different destination than the least specific network.
- In certain scenarios, the H.323 ALG may not properly translate the application layer information.
- In a legacy dial backup (DBU) application, deleting a PPP interface being used for DBU while the DBU PPP interface is active, could cause an AOS device to reboot.
- Abbreviating the **show running-config | include** <*text*> command with **s run | include** <*text*> does not function.
- The administrative distance on a static route cannot be changed without removing and re-adding the static route with the new administrative distance.
- It is not possible to modify the NTP server configuration in the GUI.
- An SNMP walk of the NetVanta 6355 lists the physical address for the first interface index only.
- When configured for **terminal length 0**, certain **show** commands do not provide complete output.
- The chassis fans in NetVanta 1500 Series switches oscillate at a higher frequency than expected during periods when the switch is not being heavily utilized.
- The last reboot on a NetVanta 1638 may indicate "System returned to ROM by Watchdog Timeout" even on a manual reboot.
- Browsing to the Debug Unit menu in the GUI, could generate a 404 Not Found response.
- 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.
- The help text for the Global Configuration mode command **sntp server** incorrectly implies that it disables the local SNTP server, whereas the command only modifies the local SNTP client.
- The IP address displayed as the destination address in the **debug snmp** command output indicates that the ADTRAN unit is sending a reply to one of its local IP addresses. This issue is purely cosmetic.
- Certain OIDs in the Bridge-MIB may not return a value on a second generation NetVanta 123X switch.
- Certain commands referencing an ACL using quotation marks and spaces cannot be saved properly.
- The Ping utility in the GUI will display a more latent ping time for the first ping.
- When creating or modifying 802.1q subinterfaces in the GUI, a 503 Service Unavailable response is generated.
- The **vap-reference** command will not replicate VLAN IDs for an AP unless 802.1q encapsulation has been manually enabled on the AP designated to receive the replicated configuration.

Copyright © 2013 ADTRAN, Inc.

- Updating PRL values on a Sprint 3G CDMA NIM might not function properly.
- Removing the **traffic-shape rate** command from an interface can result in two bandwidth configurations on the interface.
- The parent map QoS statistics must be cleared in order to clear the child map statistics.
- A specific QoS map entry cannot be cleared without the entire map being cleared.
- Output from **show interface [eth** <*slot/port*> **| gigabit-switchport** <*slot/port*>**]** command will display incorrect information about the queuing implementation of the interface when 802.1q encapsulation is applied.
- 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 command **ip rtp firewall-traversal enforce-symmetric-ip** 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.
- The T1 EFM counters do not increment as traffic passes through the device.
- Using SCEP, NetVanta routers could 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 over 1200 VNS entries on the NetVanta 3448 causes a SIP Pre-Parse error.

Copyright © 2013 ADTRAN, Inc.

- The VNS verification process does not remove inconsistent A-type records from the host table after the configured number of attempts.
- 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.
- The AOS CLI could remove 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.
- 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 **max-reserved-bandwidth** command is removed from an Ethernet interface when changing the encapsulation to 802.1q.
- 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.
- HDLC keepalives cannot be disabled from the CLI.
- NetVanta 150 might not properly handle immediate Access-Accept responses to Access-Request messages.
- In some 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 might not mirror traffic in both directions.
- Proxy user templates cannot modify SDP IP addresses correctly in some 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.

Copyright © 2013 ADTRAN, Inc.

- 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.
- 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.
- Performance issues may be experienced when using the NetVanta SHDSL ATM NIM2 on the NetVanta 6310/6330.
- In certain cases, the system uptime reported via SNMP is less than the actual system uptime.
- If the **ethernet-cfm** command is configured on a MEF Ethernet interface, the output of the following CLI commands are 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**

- 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.
- Performance throughput for 66 byte packets on the NetVanta 6355 4T1/NAT test cases has decreased approximately 40 percent. All other packet sizes, including IMIX traffic, have acceptable throughput.
- 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 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.
- 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.
- 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.

Copyright © 2013 ADTRAN, Inc.

- The NetVanta 6310 drops approximately 1 out of every 15K packets from the SHDSL to Ethernet direction with the SHDSL ATM NIM2.

The following is a list of voice specific errata that still exist in products running AOS version R10.3.3, unless otherwise noted.

- On non-SBC feature pack routers, the **ip sip qos dscp** command was not available.
- When using a Voice Interface Module (VIM) in conjunction with the second generation NetVanta Dual T1 NIM in a NetVanta 6355, the second T1 in an MLPPP bundle will have TDM group errors.
- It is possible to configure the UDP port range for the DSP to overlap with the firewall traversal port range used by RTP Firewall Traversal. This could cause one-way audio.
- The command **voice number-complete disable pound** does not function properly on CAS trunks.
- When the hex encoding of # (%23) is received in a SIP URI, it is not properly converted back to # before being processed by the switchboard.
- Enabling VQM can cause audio to be lost when using the Simple Remote Phone feature.
- AOS does not properly handle more than two Diversion headers that are appended with a comma.
- NetVanta 6240 only: While running 29 or greater 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 that uses DSP 0/1.15 or higher. While in this failed state, all calls in either call direction on DSP 0/2 and all calls in the inbound direction on DSP0/1 will continue to function. 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 fix the problem.
- For SIP to PRI calls on which the called party number is in E.164 format, the called party number will not be presented to the PRI unless **voice international-prefix abbreviated** is configured
- 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 will send the text string **Unavailable** as the caller ID name to the FXS port , instead of sending the O flag for the name.
- Connection information (c=) in a media description does not override connection information in session description.
- If an ADTRAN unit is configured with single call appearance mode, forwarded calls on a PRI trunk will fail.
- SIP traffic will not route to a SIP server on a remote network unless a static default route exists.
- The GUI on the Total Access 900/900e series lists T1 clocking options that are not valid for the product (i.e., System and Through)
- On either a voice trunk or a voice user with a CODEC list configured, entering the command **no codec-list** <*list name*> <*direction*> always removes the <*list name*>, regardless of the configured direction.
- Echo cancellation will not be enabled on three-way calls when using the local conferencing feature.
- If an IPBG is configured with Australia as the country code, there will be a five second delay in the ring cadence between the first and second ring.
- 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.

Copyright © 2013 ADTRAN, Inc.

- 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 will 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.
- Output of the **show voice quality-stats** command may display a larger average delay than the maximum value.
- The Total Access 900e Series 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.
- When using media anchoring, calls that are placed between SIP and FXS voice users on the same unit will have one-way audio if the call is placed through a SIP trunk.
- The **Remote** section of the **show media-gateway session** output displays SIP description for all calls, including MGCP calls.
- During G.711 A-law SIP to ETSI PRI calls, low voice quality scores are experienced on the outbound audio stream towards the SIP network. This issue is not seen on the ETSI PRI endpoints or with G.711 u-law and G.729 CODECs. A person listening to the audio on the SIP side will hear audio just below G.729 quality.
- The output of the command **show ethernet cfm mep local** may display an incorrect maintenance association for a MEPID if multiple maintenance associations are configured on the unit.
- 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.
- 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.
- The NetVanta 6240 Series IPBGs could reboot if 60 simultaneous calls are placed through the DSP.
- 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.
- NetVanta 6240 only: Call Waiting Caller ID does not display on analog lines configured for MGCP.
- 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 the configuration includes a secondary IP address, executing an SNMP walk results in a failure at the ipAdEntAddr OID with error OID not increasing. If the secondary IP address is removed, the walk completes successfully.
- 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.
- Out of Order packets can appear as a negative value in the **show voice quality-stats** command output.
- If an unsupported packetization period is presented to the ADTRAN unit in an SDP answer, no indication that the presented ptime is not supported by the ADTRAN unit will be sent to the remote user agent. This will result in no talk path.
- With multiple PRIs in the same ISDN group, bringing one PRI down will cause calls that should use the other PRI to fail. A workaround is to use two ISDN groups that only contain one PRI each.

Copyright © 2013 ADTRAN, Inc.

- 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.

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 R10.1.0 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*
- *AOS Voice International Configuration Guide*
- *Configuring the AOS Voice Loopback Account*
- *Manipulating SIP Headers and Messages in AOS*
- *Configuring DHCPv6 in AOS*
- *Configuring Border Gateway Protocol in AOS for Releases 18.03.00/R10.1.0 or Later*
- *Configuring Border Gateway Protocol in AOS for Releases Prior to 18.03.00/R10.1.0*
- *Configuring IPv6 in AOS*
- *Configuring Packet Capture in AOS*
- *Configuring Busy-Out Monitor in AOS*
- *Configuring Media Anchoring in AOS*
- *Session Border Controllers in AOS*
- *Configuring QoS in AOS*
- *Configuring Enhanced Ethernet Quality of Service*
- *Configuring Remote Phones with an AOS SIP Gateway*

Copyright © 2013 ADTRAN, Inc.