RELEASE NOTES

Converged Access Products
AOS version R10.1.1
May 25, 2012

Trademarks

Any brand names and product names included in this manual are trademarks, registered trademarks, or trade names of their respective holders.

To the Holder of the Manual

The contents of this manual are current as of the date of publication. ADTRAN reserves the right to change the contents without prior notice.

In no event will ADTRAN be liable for any special, incidental, or consequential damages or for commercial losses even if ADTRAN has been advised thereof as a result of issue of this publication.

Toll Fraud Liability

Be advised that certain security risks are inherent in the use of any telecommunications or networking equipment, including but not limited to, toll fraud, Denial of Service (DoS) attacks, loss or theft of data, and the unauthorized or illegal use of said equipment. ADTRAN OFFERS NO WARRANTIES, EITHER

EXPRESSED OR IMPLIED, REGARDING THE PREVENTION, DETECTION, OR DETERRENCE OF TOLL FRAUD, NETWORKING ATTACKS, OR UNAUTHORIZED, ILLEGAL, OR IMPROPER USE OF ADTRAN EQUIPMENT OR SOFTWARE. THEREFORE, ADTRAN IS NOT LIABLE FOR ANY LOSSES OR DAMAGES RESULTING FROM SUCH FRAUD, ATTACK, OR IMPROPER USE, INCLUDING, BUT NOT LIMITED TO, HUMAN AND DATA PRIVACY, INTELLECTUAL PROPERTY, MATERIAL ASSETS, FINANCIAL RESOURCES, LABOR AND LEGAL COSTS. Ultimately, the responsibility for securing your telecommunication and networking equipment rests with you, and you are encouraged to review documentation regarding available security measures, their configuration and implementation, and to test such features as is necessary for your network.

ADTRAN Technical Support Community

For information on installing and configuring ADTRAN products, visit the ADTRAN Support Community, https://supportforums.adtran.com.

Pre-Sales Technical Support
(800) 615-1176
application.engineer@adtran.com

Corporate Office
901 Explorer Boulevard
P.O. Box 140000
Huntsville, AL 35814-4000
Phone: (256) 963-8000
www.adtran.com

Post-Sales Technical Support
(888) 423-8726
support@adtran.com

Contents

Introduction

AOS version R10.1.1 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 8*.

A list of new or updated documents for this release appears in *Documentation Updates on page 14*.

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 R10.1.1. 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 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 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 R10.1.1 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 R10.1.1 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* (article 2219) 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 R10.1.0.

- Added the ability to turn off the DF bit in an IP header. This is accomplished by adding the **set ip df 0** command to an applicable configured route map.
- Added the ability to perform a packet capture and export to a TFTP server or n-Command MSP.
- Added support for video SDP through the SIP proxy and the B2BUA.
- Added support for IPv6 load sharing.
- Added support for IPv4 GRE tunneling of IPv6 traffic.
- Added support for IPv6 stateful DHCP server functionality.
- Added support for IPv6 traffic shaping.
- Added support for IPv6 low latency queuing for quality of service.
- Added support for an IPv6 TFTP ALG.
- Added support for an IPv6 FTP ALG.
- Added support for IPv6 BGP.

This section highlights the voice specific features, commands, and behavioral changes available in IPBG and Gateway products running AOS version R10.1.0, unless otherwise noted.

- Added the ability to configure the caller ID time zone offset separately from system time zone offset.
- Added RTP media loopback functionality to the SIP loopback account.

- *Added the ability to route SIP and RTP for remote voice users through the Back-to-Back-User-Agent (B2BUA) based on source IP address and port rather than the information received via the SIP/SDP messaging.
- *Added support for international ringback comfort tones for blind transfer calls on the NetVanta 3430.
- Added support to handle 3xx level SIP messaging locally for SIP to SIP calls.
- Added the ability to provide local REFER handling for SIP to SIP calls.
- Added support for media anchoring.
- *Added SIP header manipulation rules, giving the user the ability to add, delete, modify, and match SIP header information.
- *Added support for IPv6 in AOS voice products.
- Added FXS voice users to the existing busy-out functionality.
- *Added support for SIP Back-to-Back-User-Agent (B2BUA) for the second generation NetVanta 3430.

**Only applicable to AOS products running the SBC feature pack. Refer to Supported Platforms on page 4 for a list of products.*

Fixes

This section highlights major bug fixes for all Converged Access products running AOS version R10.1.1.

- If created in AOS 18.02 or earlier, **route-map** commands configured within a BGP neighbor would not port correctly to R10.1.0 software.
- The DNS-proxy caused the PC configuration process to lock up, which caused traffic to stop passing and the console port to stop responding.
- In R10.1.0, the processing of non-TCP broadcasts (excluding DHCP broadcasts) with the firewall enabled could cause a memory leak that eventually lead to a reboot.
- In AOS version R10.1.0, BGP authentication would not function properly when attempting to form a neighbor relationship with devices that were not using AOS version R10.1.0.
- In R10.1.0, NetVanta 3448s and NetVanta 3458s were unable to supply PoE.
- If a non-default VRF was applied to a demand interface, it caused the AOS device to reboot.
- When using an HDLC interface with integrated routing and bridging, globally disabling bridging with the command **no bridge 1 protocol ieee** caused a reboot.
- When a ping was sent from the GUI with a non-default source IP address, the source address was not modified properly.
- Frame Relay interfaces configured as interface type **dte** failed to generate LMI messages if the unit was booted with the Frame Relay interface administratively down.
- Ethernet 0/1 on a NetVanta 3450 would stop passing traffic after a speed/duplex mismatch.

This section highlights the voice specific bug fixes in IPBG and Gateway products running AOS version R10.1.1, unless otherwise noted.

- If the ADTRAN unit receives an SDP offer with the RFC 3264 sendonly attribute to place the call on hold, it will not begin sending RTP again when a sendrecv attribute is received to take the call off of hold. This issue was only present in AOS A5.03.00.
- In some cases, the nonce count was improperly parsed by the SIP stack, which caused authentication failures with some softswitch configurations when using the SIP proxy.
- A reboot occurred if the DNS Client in the ADTRAN unit received a CNAME response to a DNS request.
- When using the SIP proxy in transparent mode, if the source port of a received REGISTER was not UDP 5060, in failover the spoofed 200 OK response would be sent with a Layer 3 source address of 127.0.0.1.
- If an outbound proxy was configured on a SIP trunk, the registrar host was malformed for REGISTER messages sent during a failover condition.
- ETSI PRI only: In certain instances, a PBX configured to disallow overlap dialing rejected ISDN calls from the ADTRAN unit due to a missing information element indicating that dialing was complete.
- If the remote voice gateway changed the SSRC in an RTP stream received by the ADTRAN unit, and the sequence numbers were not contiguous, VQM and the output of the **show voice quality-stats** command would 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.
- Transferring a call to a virtual user (voicemail only) on the NetVanta UC Server ECS disconnected the call.
- In certain cases, the ISDN caller ID name was not delivered when configured for delivery in a Facility message after the Call Proceeding message instead of a Setup message.

This section highlights major bug fixes for all Converged Access products running AOS version R10.1.0.

- If the firewall was configured with policy rules to discard broadcast traffic, the broadcast traffic would nevertheless be forwarded to the local stack to be processed by any service listening.
- If an ADTRAN unit had multiple subinterfaces configured and the first subinterface was in the shutdown state, the output of the **show interface** command for all of the other subinterfaces would indicate that the line protocol was down.
- Using some authentication options, the **Reload Scheduled In** message would not appear at login if a reload was scheduled.
- In certain scenarios, REGISTER messages would not be processed properly by the SIP proxy, resulting in a **500 Server Internal Error** response.
- The CLI did not allow the user to set the DS0 speed to **56K** for an E1 NIM.
- Test patterns could not be generated consistently on E1 NIMs.

This section highlights the voice specific bug fixes in IPBG and Gateway products running AOS version R10.1.0, unless otherwise noted.

- On an outbound INVITE, if no ANI was available, the configured trunk group identifier would not be added. The new **always** parameter was added to accomplish this.
- If a **486 Busy Here** was received while a call was in the PreConnected state, a forward disconnect would be performed at the same time the busy signal was being played out, causing the call to be disconnected before the caller heard the busy signal.
- The **clear ip rtp quality-monitoring** command was missing from the NetVanta 644.
- The **Map Conversation Statistics** menu for interfaces were not displayed on the **QoS Map** GUI menu when the map was applied to an interface.
- When running T.38 on a NetVanta 644, failure to train issues were possible for fax calls.
- In A4.08 and higher, a Record-Route header was added by the proxy in transparent mode. This caused routing issues with some devices. The previous behavior of not adding the Record-Route header in transparent mode was restored.
- Adding or removing the **isdn alert disable pi-8** command from the running configuration would incorrectly change the value associated with the **isdn ringing-signal** command.
- In rare cases, the ADTRAN unit may reboot if the SIP proxy was overloaded with voice traffic.
- Over time, a reboot would result from a memory leak that occurred when receiving REFERs when **voice transfer-mode network** was configured.
- When a secondary SIP server was configured on a SIP trunk, the unit would not fail over to the secondary server after receiving a REFER to a valid extension.
- When both **registrar threshold [absolute | percentage]** <*value*> and **registrar expire-time** <*value*> commands were present in a configuration, the **registrar expire-time** <*value*> was listed first, which led to an error when booting the unit and that portion of the configuration failed to be properly restored.
- Under certain conditions a QoS map applied to an interface would not disable itself when adequate bandwidth was not available.
- If an MGCP SignalRequest to disable VMWI was received while the dial tone was being played out that port, the FSK to disable VMWI would play while the dial tone was being played, resulting in the phone being unable to interpret the VMWI FSK.
- In some cases, it was possible that the user would see the following error message on the CLI when assigning an unnumbered address to an HDLC or PPP interface: "**%Point-to-point (non-multi-access) interfaces only**".
- The QoS wizard could not apply a QoS map to a MEF Ethernet interface.

Errata

The following is a list of errata that still exist in all Converged Access products running AOS version R10.1.1.

- The **Cable Diagnostics** troubleshooting menu in the GUI cannot be refreshed manually.
- With password encryption enabled, BGP authentication passwords are double encrypted on reboot.
- The SIP proxy will not forward a Register message if the Contact field contains only an ***** (asterisk).
- The NetVanta 3120 might not respond to SNMP polls for VQM.

- Updating PRL values on a Sprint 3G NIM might not function properly.
- Removing the **traffic-shape rate** configuration 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.
- An error message indicating conflicting tunnel MTUs is displayed even if the negotiated MTUs are the same.
- Changing PoE settings in the GUI can cause a **503 Service Unavailable** response.
- 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. The correct queuing method should be listed as FIFO unless traffic shaping is applied to the interface.
- In rare cases, when an IP PBX and IP phones are both passing through a NAT and the SIP proxy on an AOS router, some call flows can enter a one-way-audio state. Enabling the **ip rtp firewall-traversal enforce-symmetric-ip** command from the Global Configuration mode works around the issue.
- A large enough drift in the system clock can cause an error when the NTP server attempts to synchronize.
- On a NetVanta 1335, a switchport that is configured as a port channel cannot change the edge port mode and cannot be changed from a port channel to another configuration using the GUI.
- The interface 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.
- QoS maps with names longer than eight characters might not display properly in the GUI.
- The CLI context help implies the ability to apply an inbound QoS map on a Frame Relay interface. This is misleading since inbound QoS maps are only applicable to Ethernet interfaces.
- 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 **DHCP Server** GUI displays **Could not eval: 503: server error** between the DHCP server setting table and the DHCP leases table.
- 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.
- 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.
- The VNS verification process does not remove inconsistent A-type records from the host table after the configured number of attempts.
- A-type host table entries (associated to a manually configured VoIP Name Service Host) are classified as sticky when an AOS router first boots up with VNS verification enabled.
- Configuring a port channel on a NetVanta 3448 can cause the STP topology to become unstable.
- The output of the **show host** command does not display the entire FQDN.
- Issuing the **clear host *** command can remove permanent SRV-type DNS entries from the host table.
- IPv6 traffic destined to 0:: is forwarded to the default gateway instead of being dropped.
- 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 *** command does not change the administrative distance of the default route.
- QoS cannot be invoked on a demand interface.
- The NetVanta 5305 can drop some traffic prioritized by class-based weighted fair queuing (CBWFQ) on an 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.
- The **QoS** menu of the GUI displays available bandwidth for a PPP interface that is in a **Link Down** state.
- 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 150s might not properly handle immediate Access-Accept responses to Access-Request messages.

- The IPv6CP protocol state can occur even when IPv6 is disabled on a PPP interface.
- 3G connections using a NetVanta USB WWAN NIM and a Sierra Lightning modem can fail.
- The cellular interface can trigger a core dump on a NetVanta 3448 when changing states.
- 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.
- Port T1 3/3 on a NetVanta 4305 can fail intermittently when attached to an MLPPP bundle. Rebooting the device will restore the interface.
- 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 NetVanta 3120/3130 frequently fails to answer incoming calls on the DBU interface when the modem interface is configured for **dial-in** mode.
- When 802.1q encapsulation is disabled on an Ethernet interface, the interface cannot be configured for **port-auth supplicant** mode.
- The Setup Wizard for a NetVanta 3120 becomes unresponsive on the **System Info** page.
- Removing a PPP cross connection and then adding it back to a SHDSL interface causes the PPP interface to remain down, unless the SHDSL interface is disabled and then re-enabled.
- Removing and restoring cross connections multiple times can cause the PC configuration thread depth to reach 100 percent.
- Rapidly removing and adding cross connections 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** command should cause one port to enter a blocking state.
- After upgrading to R10.1.0, the VQM reporter **grammar** options always appear in the output of **show running-config** command, even if they have not been modified from the defaults.
- Using the command **debug ethernet cfm loopback request domain** <*domain name*> to filter Ethernet CFM loopback debugs may not display the debug output. Removing the filter and issuing **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 an MEPID if multiple maintenance associations are configured on the unit.

The following is a list of voice specific errata that still exist in IPBG and Gateway products running AOS version R10.1.1, unless otherwise noted.

- Under heavy ISDN call load, the unit may reboot. This issue is only present in AOS R10.1.1 and R10.2.1.

- In a PSTN gateway application, if an attended transfer is initiated towards the ADTRAN gateway the transferor will send a REFER with Replaces to the gateway. The ADTRAN gateway should be responding 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 is not sent. However, if the transferee initiates the original call, the INVITE is sent and the transfer executes properly.
- The CLI does not prevent users from configuring invalid SIP to PRI cause-code mappings.
- On the Total Access 900e platform, when 44 PRI calls (PRI to SIP direction only) and any number of analog calls (any direction) are active, the 44th PRI call will not connect approximately 80 percent of the time. Call flows of 44 PRI only calls and 44 SIP to PRI with analog calls function properly.
- The source port displayed in the output of the **debug sip stack messages** command is incorrect when using SIP over TCP.
- Stutter dial tone for message-waiting indicator in MGCP gives only three stutters instead of the ten defined in RFC 3660.
- 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.
- The **max-number-calls** command on a SIP voice trunk does not function properly when set to a value of 23.
- 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**
- 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.
- A reboot is required to change the message waiting option for an analog user to lamp only.
- In certain cases, the output of the **show sip proxy user extended** command will display dates that do not exist, such as Feb. 31.
- 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.
- When the command **p-assert-diversion** is used to add the P-Asserted-Identity header to the REFER request on a two B-channel transfer, the header might not be added.

- NetVanta 6240 only: Over an extended period of use, T.38 calls can cause DSP channels to stop producing a dial tone and have poor voice quality. Rebooting the unit corrects the problem.
- 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 unit must be rebooted to correct the problem.
- DSP captures on the NetVanta 6240 and 644 platforms consume large amounts of memory while in progress. The unit may become unstable if a DSP capture is active for an extended period of time.
- The NetVanta 6240 series IPBGs could reboot if 60 simultaneous calls are placed through the DSP.
- NetVanta 6240 only: 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.
- There are some G.168 test cases that fail to function properly on the NetVanta 6240 and 644 units. This could cause issues for customers that fully utilize G.168.
- 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.
- 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.
- NetVanta 6310/6330 series only: 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 connections to become unresponsive. A reboot corrects the condition.
- Out of Order packets can appear as a negative value in the **show voice quality-stats** command output.
- 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.
- In some scenarios, upon receipt of a reINVITE, the **sess-id** and **sess-version** in the origin field of the SDP answer could change.
- 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.
- Under certain conditions, inbound RTP streams for voice calls terminated by the ADTRAN unit cannot be exported to an external NetFlow collector.
- 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.
- The NetVanta 6310 drops approximately 1 out of every 15K packets from the SHDSL to Ethernet direction with the SHDSL ATM NIM2.
- 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.
- Outbound proxy mode for the SIP proxy does not function properly when the phones are configured to use TCP.
- PRI to ground start trunk calls do not function on the Total Access 900e when the PRI is on T1 0/3 and the ground start trunk is on FXO 0/1. The PRI will go out of service when this type of call is attempted on these ports. These calls function on the Total Access 900e if the PRI is on T1 0/4 or if the ground start trunk is on any FXO port other than 0/1.

Upgrade Instructions

Upgrading ADTRAN products to the latest version of AOS firmware is explained in detail in the configuration guide *Upgrading Firmware in AOS* (article 1630), 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 Converged Access products. These documents can be found on ADTRAN's Support Forum available at https://supportforums.adtran.com.

- AOS Command Reference Guide (60000CRG0-35E, article 2219)
- AOS Voice International Configuration Guide (6AOSCG0014-29C, article 3508)
- Configuring the AOS Voice Loopback Account (6AOSCG0020-29B, article 2363)
- Manipulating SIP Headers in AOS (6AOSCG0026-29A, article 3526)
- Configuring DHCPv6 in AOS (6AOSCG0027-29A, article 3527)
- Configuring Border Gateway Protocol in AOS for Releases 18.03.00/R10.1.0 or Later (6AOSCG0024-29B, article 3524)
- Configuring Border Gateway Protocol in AOS for Releases Prior to 18.03.00/R10.1.0 (61200860L1-29.4E, article 2915)
- Configuring IPv6 in AOS (6AOSCG0016-29D, article 3505)
- Configuring Packet Capture in AOS (AOSCG0029-29A, article 3528)
- Configuring Busy-Out Monitor in AOS (6AOSCG0030-29A, article 3529)
- Configuring Media Anchoring in AOS (6AOSCG0031-29A, article 3530)
- Session Border Controllers in AOS (6AOSCG0032-29A, article 3531)
- Configuring QoS in AOS (61200860L1-29.3H, article 1617)
- Enhanced Ethernet Quality of Service (61200821E1-29.2D, article 2338)
- Configuring Remote Phones with an AOS SIP Gateway (6AOSCG0033-29A, article 3532)