RELEASE NOTES

AOS version R10.9.8
June 12, 2015

Trademarks

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

To the Holder of the Manual

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

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

Toll Fraud Liability

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

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

ADTRAN Technical Support Community

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

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

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

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

Contents

Introduction

AOS version R10.9.8 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 14*.

A list of new or updated documents for this release appears in *Documentation Updates on page 23*.

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 R10.9.8. To confirm the Boot ROM version of the ADTRAN unit, Telnet or console to the unit and issue the **show version** command. In the command output, the Boot ROM version will be listed as **Boot ROM version XX.XX.XX**. If you require a Boot ROM upgrade, please contact ADTRAN Technical Support (support@adtran.com or 888-423-8726) for assistance.

Platform	Standard Feature Pack	Enhanced Feature Pack	SBC Feature Pack	Minimum Boot ROM
NetVanta 644		√		A5.01.B1
NetVanta 1234/1234P (2nd Gen. only)	√			XB.01.02
NetVanta 1238/1238P (2nd Gen. only)	√			XB.01.02
NetVanta 1534	√			17.06.03.00
NetVanta 1534 (2nd Gen.)	√			17.08.01.00
NetVanta 1534P (2nd Gen.)	√			17.09.01.00
NetVanta 1535P	√			17.08.01.00
NetVanta 1544/1544F	√			17.06.03.00
NetVanta 1544 (2nd Gen.)	√			17.08.01.00
NetVanta 1544P (2nd Gen.)	√			17.09.01.00
NetVanta 1638	√			18.02.01.SC
NetVanta 1638P	√			18.02.01.SC
NetVanta 1335		√		15.01.00
NetVanta 3120		√		14.04.00
NetVanta 3130		√		14.04.00
NetVanta 3200/3205 (3rd Gen. only)	√	√		17.02.01.00
NetVanta 3305 (2nd Gen. only)	√	√		04.02.00
NetVanta 3430	√	√		13.03.SB
NetVanta 3430 (2nd Gen.)	√	√	√	17.05.01.00
NetVanta 3448	√	√	√	13.03.SB
NetVanta 3450	√	√		17.06.01.00

Platform	Standard Feature Pack	Enhanced Feature Pack	SBC Feature Pack	Minimum Boot ROM
NetVanta 3458	√	√		17.06.01.00
NetVanta 4305 (2nd Gen. only)	√	√		08.01.00
NetVanta 4430	√	√	√	17.04.01.00
NetVanta 5305	√	√		11.03.00
NetVanta 6240		√	√	A5.01.00
NetVanta 6250		√	√	R10.9.0
NetVanta 6310/6330		√	√	A3.01.B2
NetVanta 6355		√	√	14.06.00
Total Access 900 Series (2nd Gen. only)		√		14.04.00
Total Access 900e Series (2nd Gen. only)		√	√	14.05.00.SA
Total Access 900e Series (3rd Gen. only)		√	√	R10.9.0

System Notes

- Beginning with AOS version 17.09.01, the syntax of certain commands was modified from previous AOS versions by either removing or adding the **ip** keyword. In general, when the **ip** keyword appears in a command, it signifies that the command is only applicable to IPv4 functionality. As more features introduce IPv6 support, the **ipv6** keyword is added to signify the command is only applicable to IPv6 functionality. The **ip** keyword has been removed from several commands to signify that the command has both IPv4 and IPv6 functionality.

  Due to this syntax change, downgrading a unit configured in AOS version R10.9.8 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 R10.9.8 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.

Features and Enhancements

This section highlights the voice specific features, commands, and behavioral changes in products running AOS version R10.9.1.

- Added the ability to configure SIP Timers D & J, which affects how long a SIP transaction resource is reserved once the final message in a transaction is received.

This section highlights the major features, commands, and behavioral changes for all Converged Access products running AOS version R10.9.0.

- Added support for the NetVanta 6250 series.
- Added support for the third generation Total Access 900e series.
- Added support for 10 individual port channels in an ActivChassis configuration. Prior to this release, an ActivChassis configuration only supported 6 port-channels.
- Added support for IPv6 DHCP client capabilities.

- Added support for the use of named prefixes for management of IPv6 prefixes.
- Added support for the NetVanta 1131 Redundant Power Supply/Extended Power Supply (RPS/EPS) for NetVanta 1500 Series and NetVanta 1638 Series switches in ActivChassis mode.

This section highlights the voice specific features, commands, and behavioral changes available in products running AOS version R10.9.0.

- Added SIP proxy monitor to the SIP proxy rollover functionality. When the SIP proxy is in monitored rollover mode, the SIP proxy monitor will poll the primary server to detect when it is operational again and it is safe to route traffic to it. Optionally, the SIP proxy monitor can be used to monitor the active server while the proxy is not in rollover mode. This allows the proxy to detect when the server goes down without a call being placed. The SIP proxy monitor is available in stateful proxy mode only.
- Added a SIP monitor rollback timer to the SIP trunk failover functionality. The delay introduced by the rollback timer will prevent a server from being selected while the delay is in effect.

Fixes

This section highlights major bug fixes for all products running AOS version R10.9.8, unless otherwise noted.

- Some sectors on flash may have been written excessively, causing premature wear and potentially preventing the unit from booting. This issue has been addressed and a refresh mechanism has been added to address any issues with premature wear.

This section highlights the voice specific bug fixes in products running AOS version R10.9.7, unless otherwise noted.

- When using T.38, if a page transmission lasted longer than the configured value of **ip rtp session timeout** (45 seconds by default) and a reINVITE was received, the fax failed.

This section highlights major bug fixes for all products running AOS version R10.9.6.

- When AAA was configured, an SSH denial of service attack may have caused the unit to lock up.
- The NetVanta 644 failed to receive 802.1q tagged packets with an IP payload between 1497 and 1500 bytes.
- To address the SSL 3.0 POODLE vulnerability, SSL 3.0 has been disabled by default for the HTTPS server, SMTP client, Auto-Link client, Auto Config client, HTTPS packet capture export, and the **copy https** command. To enable SSL 3.0 support, an **allow-sslv3** parameter has been added to all of these clients and servers, with the exception of Auto-Link.

  Additionally, SSL 2.0 has been disabled in all of the previously mentioned clients. It was already disabled by default for the HTTPS server.
- On the Total Access 900e (third generation) and NetVanta 6250, the SNMP ifDescr was not unique for each of the T1 interfaces.
- When changing an Ethernet interface from a static IP address to PPPoE, configuring the static IP address on the PPP interface caused a reboot.
- When using VQM reporter, the Gap Duration (GD) reported in the BurstGapLoss values could be greater than 3,600,000, which is the maximum value allowed by RFC 6035.
- In rare cases, an AOS unit would not be able to properly access the flash file system until the unit was rebooted.

This section highlights the voice specific bug fixes in products running AOS version R10.9.6, unless otherwise noted

- When using RTP firewall traversal, if the SIP device behind the AOS unit changed RTP ports in SDP and was slow to actually start using the new ports, the NAT session for the new RTP stream may have been unexpectedly removed. The **ip rtp firewall-traversal enforce-symmetric-port** command has been added to help in this scenario.
- After the first 18x provisional response was received on a SIP trunk call through the B2BUA, if additional 18x provisional responses were received, they were not relayed to another SIP or ISDN trunk.
- When **snmp trap registration** was configured on a SIP voice trunk, a small amount of memory would leak on each successful SIP registration, eventually resulting in a reboot.
- When using SIP proxy user templates, in some cases the Request-URI of inbound INVITEs was improperly modified.
- When using the SIP proxy, if a Remote-Party-ID header was improperly formatted, the SIP message containing the header would not be proxied.
- With a high call rate and modem passthrough enabled, it was possible to see SIP to ISDN call failures even though there were available B channels on the ISDN trunks.

The section highlights major bug fixes for all products running AOS version R10.9.5.

- A route map policy that matched on an ACL with a tracked permit statement would not update properly if the ACL permit statement was invalidated by the track.
- Attempting to configure an outbound proxy on a VQM reporter resulted in an error message.
- On the Total Access 900e (third generation) and NetVanta 6250, small runt packets without an Ethernet FCS may have caused the 10/100 Ethernet ports to become non-functional. The issue may have occurred when a duplex mismatch was present.
- When **domain-proxy failover** was enabled and the AOS unit entered a failover state, the domain proxy would not respond for entries that were in the host table.
- After successfully adding or modifying a VLAN on the VLAN Interface GUI page, a 503 Service Unavailable response was generated when the page was refreshed.

This section highlights the voice specific bug fixes in products running AOS version R10.9.5, unless otherwise noted.

- When using the SIP proxy, the order of parameters inside the **uri** parameter of an Authorization header may have been changed, invalidating the hashed response.
- Under certain conditions when an FXS port was taken off-hook while in the ringing state, ring voltage would continue to be applied to the port. This led to degraded call quality and caused the FXS port to go into fault protection.
- If an emergency call failed and was automatically retried, the INVITE for the retry did not contain a SDP offer, which prevented early media from being sent.
- In rare cases, if an ISDN call with overlap dialing was abandoned very quickly, a reboot would occur.
- When configured with a user role PRI, if the local exchange sent progress indicator #2 (PI2) to indicate the presence of inband audible ringback on a SIP to PRI call, a 183 Session Progress with SDP was not sent on the SIP call leg.

- When configured, the **conferencing-uri** was used for the Request-URI, From, and To hosts instead of the Request-URI and To users.
- When two calls formed a TDM hairpin, if one or both calls were set up with sendonly or recvonly media, two-way audio would not be established when the hairpin connected.
- On the Total Access 900e (third generation) and NetVanta 6250, if an FXS port was hung up from a FXS to PRI call while a call waiting beep was being played, future calls on that PRI channel may have failed to connect properly.
- The **sip proxy sip-server rollover service-unavailable-or-timeout** command did not result in a server rollover when a 503 Service Unavailable was received in response to a REGISTER.
- On the NetVanta 644, if a 302 Moved Temporarily response was received that resulted in a TDM hairpin call, an ISDN CONNECT would not be sent on the original inbound call if inband call progress tones were provided on the outbound call resulting from the 302.
- When using T.38, outbound faxes that took longer than 60 seconds for a page to be transmitted would fail.
- When modifying an existing SIP trunk using the GUI, the transport mode of that trunk was changed from UDP to TCP, breaking communication on that trunk.
- During failover, calls were not routed to SIP proxy users from the B2BUA on the Total Access 900e (third generation) and NetVanta 6250.
- OPTIONS messages from the SIP proxy monitor did not contain a From tag.
- OPTIONS messages from the SIP proxy monitor did not use globally unique Call-IDs.
- When using the default grammar options for the From, To, and Request-URI user on the SIP proxy monitor, those three headers used invalid SIP syntax.
- In rare cases, the NetVanta 644 rebooted if a PRI interface went down and then came back up in quick succession.
- In certain call flows in which a MDCX was received, old SDP may have been reused instead of generating a new SDP answer.
- If a FQDN was configured with the **outbound-proxy primary** command on a SIP voice trunk, rollover to other servers listed in the SRV record was not attempted unless a **sip-server secondary** was also configured.
- The dynamic grouped trunk used as a fallback for local call forward handling evaluated to a score of 500 instead of the more appropriate score of 1. With **voice forward-mode local** configured, this resulted in calls forwarded via a 302 Moved Temporarily using the dynamic grouped trunk instead of a configured group trunk that did not have a cost of 0 for the matching accept template.
- When the volume of SIP to PRI calls was high, calls were sometimes routed to a completely full PRI, resulting in a SIP 486 Busy Here being sent to the server, instead of routing the call to an available PRI.
- When a CANCEL passed through the SIP proxy, if the CANCEL included a Reason header, the Reason header was lost when the message was proxied.
- In a failover scenario, spoofed SLA NOTIFY messages from the SIP proxy contained the AOS device's IP address in the Contact URI, which prevented the phones from re-subscribing to the SIP server once normal service was restored.
- On the Total Access 900e Series (third generation) and NetVanta 6250 Series, it was possible for the unit to reboot if PLC was enabled on a user or trunk configured for G.711.

- If a reINVITE was received while an FXS user was on hold, DTMF detection would be interrupted. This prevented calls from being transferred by an FXS user when used with the Music on Hold feature of Business Groups on Metaswitch.

The section highlights major bug fixes for all products running AOS version R10.9.4.

- If the **absolute-path** on a HTTP request probe contained a ?, the ? was lost when the unit was rebooted.
- In R10.9.0 and higher, if a name error response was received on an A or a AAAA DNS query, the configured domain name would be appended repeatedly, resulting in constant DNS queries.
- On some Total Access 916e (third generation), Total Access 924e (third generation), and NetVanta 6250 units, errors were seen on the copper Gigabit Ethernet interface.
- NetVanta 4660, NetVanta 6250, and Total Access 900e (third generation) units would not honor route-maps when the firewall was enabled.
- If a flood of IGMP leave messages was received on a Layer 3 interface and the interface was configured for multicast routing, the ARP cache would be filled with multicast addresses.
- If the IPv4 firewall was enabled and a message in the TCP 3-way handshake contained a PSH or RST flag, the firewall association would not reach the established state and was cleared within 20 seconds.
- In the GUI, if an EPS was not connected, an AOS switch would indicate the EPS fan status was unknown.
- The GUI of certain AOS switches would incorrectly show an EPS section, even if that switch did not support an EPS.
- If a **vap-reference** statement was configured on a dot11ap interface, that configuration would be lost when the unit was rebooted.

This section highlights the voice specific bug fixes in products running AOS version R10.9.4, unless otherwise noted.

- When using templated proxy users with the SIP proxy, received CANCEL messages from the SIP server would be interpreted as outbound messages, resulting in the offered Contact being updated improperly.
- On the Total Access 900e (third generation) and NetVanta 6250, the output caller ID levels were too high.
- If an incoming ISDN trunk call was routed to an outgoing user role ETSI ISDN trunk, the numbering plan and type of number (NPI/TON) of the incoming called and calling party numbers was not properly transferred to the outgoing numbers.
- If the second call leg of a transfer started by an FXS user received an INVITE with Replaces, the transfer would not be completed upon hanging up the phone.
- When using a user role feature group D trunk, although DNIS digits were received and recognized, they were not properly interpreted as DNIS.
- It was not possible to configure **ip rtp udp** with a range that included UDP ports 63018 and 63019.
- When entering the command **sip proxy emergency-call-routing local**, the configuration would display **sip proxy emergency-call-routing proxy** instead. Negating the command **sip proxy emergency-call-routing proxy** would restore the default parameter for the command, which is **local.**
- When using the SIP proxy in transparent mode without NAT, responses from the server would trigger unexpected rollover events.
- The **dnis-digits** command was not available on Feature Group D RBS trunks.
- When using the AOS packet capture feature, if VQM was not enabled, outbound RTP packets from the DSP were not captured reliably.

- When using the SIP proxy, 200 OK response retransmissions that were received greater than the configured value of **sip timer rollover** seconds after the initial 200 OK would fail.
- AOS would not properly handle a SIP UPDATE request when the request was received on an outbound call that had not connected.
- The 50 call NetVanta 3448 SBC would only support 40 calls.
- In stateful mode, the SIP proxy would use the configured SIP proxy server instead of the URI from the previous Contact header when proxying ACK messages.
- If a route was removed while calls were in progress, a reboot may have occurred.
- In a PSTN gateway application on the NetVanta 644, a call that was blind transferred out to the PSTN would have no audio.
- In rare cases, a DSP reboot would occur on the Total Access 900e (third generation) and the NetVanta 6250.
- If a call using a 3.1 kHz audio bearer capability was received on a PRI, the AOS unit would not wait for the calling party name to be sent in a FACILITY message after being instructed to do so in the SETUP message.
- When using media anchoring with the SBC feature pack, one-way audio may have occurred on hairpinned calls when multiple 183 Session Progress responses were received.
- When outbound requests passed through the proxy, the transport parameter would be removed if UDP was the specified transport.
- When connected via the console port to an AOS IP business gateway that had an ISDN trunk configured, benign errors would be displayed to the console in some cases.
- On a SIP-to-SIP call through the B2BUA, if received SDP specified annexb=no for a G.729 call and comfort noise (CN) was also a listed CODEC, the AOS device would specify annexb=yes in the SDP it sent.
- In some cases, transparent outbound requests through the SIP proxy would be handled as outbound proxy requests.
- When using **ringback override 180**, it was possible to have one-way or no audio after an inbound call completed due to the AOS device resending stale SDP.
- When **voice codec-priority user** was configured, calls to a ring group would result in a less preferable CODEC being selected.
- When using templated proxy users with the SIP proxy, if the device behind the proxy sent an OPTIONS message, it would be rejected with a 503 response.

This section highlights major bug fixes for all products running AOS version R10.9.3.

- If **ip proxy-arp** was enabled on an Ethernet interface and that interface was referenced with IP unnumbered on a separate interface, the AOS device may have incorrectly responded to ARP requests causing IP address conflict errors on LAN devices.
- Port channel interface counters would not update properly on NetVanta 1638 units that were not members of an ActivChassis.
- Flooding a unit with invalid IPv4 packet fragments may have caused a reboot when the firewall was enabled.
- When TACACS+ accounting was enabled, it was possible for a brute force SSH attack of long duration to cause the unit to run out of memory and possibly reboot.

- When using an AOS switch configured for DHCP relay, if a device connected to a switchport configured for one VLAN was then moved quickly to a switchport configured for a different VLAN, DHCP relay would not always forward offers back to the correct VLAN.
- In rare cases, if auto-link was configured, but the configured auto-link target could not be contacted, the AOS device would eventually become unresponsive.
- SSH sessions to an AOS device that did not progress beyond the **authentication in progress** state could not be cleared without a reboot.
- In rare cases, AOS devices erroneously indicated they had rebooted with a core dump even though the unit did not reboot due to a software issue.
- Executing a Tcl script that issued the **show tech** command caused the AOS device to be unable to execute any more **show tech** commands until the device was rebooted.
- In rare cases, ICMP probes transmitted faster than the configured period.
- On the NetVanta 3130, the **Multi No T.413** ADSL training mode option was not present in the GUI.
- On the NetVanta 3130, the **ADSL2+ Annex M** ADSL training mode option was not present in the GUI.
- Enabling **debug icmp probe** while **debug probe** was also enabled caused a slow memory leak.

This section highlights the voice specific bug fixes in products running AOS version R10.9.3, unless otherwise noted.

- When using the Enhanced ANI Substitution feature to add a Diversion header, two Diversion headers were added.
- If an ISDN INFO message with a protocol error was received during dialing on an ISDN call using overlap dialing, the AOS device would reboot.
- When using an ISDN trunk, if the RELEASE_CMP for a previous call was received after the SETUP for a new call, but before that new call connected, the new call would fail.
- On a SBC feature pack router or an IP business gateway that was configured to play ringback from .wav files, a reboot occurred when a local transfer mode SIP trunk was playing ringback on a pending referred call and that call was forwarded.
- When using non-standard SIP ports, the SIP proxy monitor failed to send OPTIONS messages to the configured servers.
- The **show rtp media sessions** command was not present in the NetVanta 644 and Total Access 900.
- In rare cases, the NetVanta 644 would reboot if a PRI interface went down and came back up in quick succession.
- When **mwi-member** was configured on a ring group, received NOTIFY messages did not match the SIP identities/aliases configured for the ring group.
- If a call rang due to a SIP 180 response for longer than the value of **ip rtp session timeout** (45 seconds by default), there would be no talk path in the SIP to TDM direction when the call was answered.
- Local 3-way conference calls against Metaswitch would fail if one of the calls in the conference was a hairpinned between two FXS users.

This section highlights major bug fixes for all products running AOS version R10.9.2 .

- After an extended period of uptime on a NetVanta switch, LLDP-MED sometimes stopped functioning properly.

- On a NetVanta 1638 ActivChassis, if a linecard rebooted independently from the ActivChassis, hosts connected to that linecard were not able to communicate with hosts over a port channel.
- On the Total Access 900e Series (third generation) and the NetVanta 6250 Series, late collisions on an Ethernet interface configured for full duplex resulted in the interface no longer transmitting until the unit was rebooted.
- It was possible for DNS queries created by an AOS IP Business Gateway to be sent using the DSP port range, which may have prevented responses from being properly received.
- On a T1 interface, setting a description greater than 110 characters and then attempting to view the description with the **show interface t1 0/x** command caused the ADTRAN unit to reboot.
- When running debugs on a heavily loaded unit, debug output is dropped if necessary to avoid congestion. In rare cases, the unit may have rebooted when that occurred.
- It was possible for DNS queries to be sent using source port UDP 4500, which prevented responses from being properly received if **ip crypto** was enabled.
- Email notifications may have failed when TLS was required by the mail server.
- On Layer 3 switches running AOS R10.7.0 and later, IP routing could not be enabled or disabled using the GUI.

This section highlights the voice specific bug fixes in products running AOS version R10.9.2, unless otherwise noted.

- On the Total Access 900e Series (third generation) and NetVanta 6250 Series, it was possible for the unit to reboot when the **show sip proxy users** command was issued.
- SNMP trunk registration failure traps were not sent properly.
- In rare cases, RTP flows being handled by RTP firewall traversal were not NATed to the ports specified in SDP.
- If two Diversion headers were appended with a comma, AOS only preserved the second Diversion header.
- When an FXS interface was configured for a neon message waiting indication (MWI), the FXS port locked up if a fault condition was detected while the neon MWI was lit.
- In rare cases, a Total Access 900e Series (third generation) or a NetVanta 6250 Series unit running the SIP proxy may have experienced a lockup requiring the unit to be rebooted to restore functionality.
- The SIP proxy will now allow non-standard URI schemes in a Refer-To to be passed transparently.
- Hairpinned TDM calls on a NetVanta 644 may have had one-way audio or no talkpath if an ACK was received before both 200 OKs were received when both sides of the hairpin call were connected.
- In rare cases, it was possible for B-channel resources to not be released properly, preventing the channel from being used.
- In rare cases, it was possible for a DSP reboot to occur on the NetVanta 6240 Series.
- On the Total Access 900e Series (third generation) and NetVanta 6250 Series, it was possible to see erroneous messages regarding T1 state changes when performing large file transfers to or from the unit.
- If more than two Diversion headers that were appended with commas were received in a SIP message, that message would be rejected with a SIP parser error.

This section highlights major bug fixes for all products running AOS version R10.9.1.

- File transfers from an AOS device to nCommand MSP may have failed.
- Syslog output sent for **priority-level info** can eventually cause a memory leak on a NetVanta 1638.
- When polled via SNMP, a Frame Relay subinterface reports an ifSpeed of 0.
- Removing and then adding an NTP server in quick succession can cause a reboot.
- In rare cases, a reboot may have occurred when NTP attempted to synchronize the AOS unit's clock.

This section highlights the voice specific bug fixes in products running AOS version R10.9.1, unless otherwise noted.

- When using ANI/DNIS substitution, it was possible for the unit to reboot in rare cases.
- If a SIP trunk monitor or SIP proxy monitor was enabled, changing the VRF in which the SIP was running caused a reboot.
- During SIP proxy survivability, an IPv6 loopback address was inserted into the SDP of calls routed to SIP proxy users on units running R10.8.0 and later.
- When using the default LBO setting (**lbo long 0)** on a T1 on a 2nd Generation Total Access 900e with the v3.1 T1 framer, it was possible to for T1 errors to occur due to the pulse shape being close to out of spec.
- T.38 calls failed if it took longer than 45 seconds to send a page.
- On a SIP-to-SIP call through the B2BUA, if the destination SIP server did not respond to an INVITE, the AOS unit may have sent a 400 Bad Request response to the original INVITE instead of a 503 Service Unavailable response.
- When the hex encoding for # (%23) was received in a SIP URI, it was not properly converted back to # before being processed by the switchboard.
- It was possible to configure the UDP port range for the DSP to overlap with the port range used by RTP Firewall Traversal, which may have caused one-way audio.

This section highlights major bug fixes for all products running AOS version R10.9.0.

- When **service password-encryption** was enabled, the auto-config password changed when the unit booted.
- In a NTP configuration, including two FQDNs that resolved to the same IP address caused the unit to lock up.
- Probe names that contain spaces were removed from track test statements on reboot.
- A NetVanta 123X Series switch would produce a 503 Service Unavailable response when the GUI Logging page was accessed.
- When using auto-link over HTTPS in AOS R10.8.0, check-ins would fail.
- When AAA authorization was configured and the AAA server was unresponsive, if a group of commands was entered via an SSH session that required authorization, administrator access to the AOS device was lost until the device was rebooted.
- In rare cases, on a NetVanta 1544 (second generation), the Layer 3 host table and the ARP cache entries would not match, which caused added latency for traffic sent to the devices that were not properly populated in the Layer 3 host table.
- A memory leak on a NetVanta 3120 eventually caused the router to reboot.

- A QoS policy applied to a subinterface would only mark inbound packets.
- It was not possible to set the default gateway option in the GUI of the NetVanta 1234 (second generation) or NetVanta 1238 (second generation).
- In ActivChassis mode, a cable diagnostics test run on a NetVanta 1638 line card would not complete properly if the cable being tested was terminated on both ends.

This section highlights the voice specific bug fixes in products running AOS version R10.9.0, unless otherwise noted.

- Calls into a network role ISDN PRI interface were rejected if the Screening Information Element was present.
- In rare cases, the NetVanta 644 would reboot when starting an RTP channel.
- A 503 Service Unavailable response may have been displayed when creating a new PRI trunk account using the GUI.
- If a SETUP message was received with the Redirecting IE set to restricted presentation, the call would fail.
- Modifying a user through the IP business gateway's **Voice** > **User Accounts** GUI menu perpetually displayed the Loading dialog box.
- If SDP without a media description was received, the call would fail.
- CONNECT_ACK may not have been sent after receiving a CONNECT on a user role ETSI PRI.
- In some cases, media anchoring would not properly connect RTP streams on hairpin calls when reINVITEs rapidly replaced existing SDP with SDP containing a new sess-id.
- MGCP ground start calls that were disconnected from the far end resulted in a hook state mismatch between the call agent and the AOS unit. This resulted in all inbound calls on that port failing until a call was placed from the same FXS port.
- Placing more than 26 simultaneous G.729 calls on a NetVanta 6310 with ETSI PRI resulted in poor audio quality.
- In rare cases, the NetVanta 644 rebooted if a **shutdown** and then a **no shutdown** was performed on the T1 interface associated with a PRI trunk.
- Enabling VQM may have caused audio to be lost when using the Remote Phone feature.
- When using MGCP, if the received caller ID name from the call agent was the O flag to indicate that it was unavailable, the unit sent the text string **Unavailable** as the caller ID name to the FXS port, instead of sending the O flag for the name.
- If a SETUP message was received that contained invalid characters in the Called Party Number, the AOS device generated a SIP INVITE with an invalid Request-URI, which resulted in a SIP parser error.

Errata

The following is a list of errata that still exist in all products running AOS version R10.9.8.

- WEP encryption does not function properly on NetVanta 160s.
- Exporting a packet capture to flash may result in audio loss while the file is being written to flash.
- When using the **show interface ppp 1 realtime** command, the input and output rates can be incorrect if **statistics rate-interval** is set to a value that is not divisible by 60.

- If a NetVanta 6310 or 6330 with a SHDSL EFM module installed receives a malformed version management packet, a reboot can occur.
- An AOS configuration file larger than 256 KB cannot be backed up to n-Command MSP.
- If a TFTP transfer is initiated and there is only one free policy session available in the firewall, a reboot can occur.
- Copying a file larger than 16 MB from flash memory of an AOS device via HTTP/HTTPS (including using Auto-Link) can cause the AOS device to reboot.
- The **tacacs-server timeout** command has no effect until the TCP session to the TACACS+ server has been established.
- Exception report emails do not function properly on the NetVanta 6250 and Total Access 900e (third generation).
- Regularly polling the NetVanta 1544 for bridge MIB information via SNMP will cause a memory leak and eventually cause the switch to reboot.
- When using Auto-Link to connect to n-Command MSP, a slow memory leak can occur.
- If a firmware transfer from n-Command MSP fails, the partial firmware file is not deleted from the file system.
- Rebooting a NetVanta 160 after editing an associated MAC access list causes the AP to transmit SSID **Wireless11**.
- In certain cases, the **show interface t1 0/1 performance-statistics Total-24-hour** command will not display the actual totals for the performance intervals. The correct values are displayed in the GUI.
- If a AAA authentication banner is configured, it will not display over SSH. Instead the login banner (if configured) will display.
- If an SNMPv3 group name is configured that matches the name of an existing SNMP community, the SNMPv3 group will not be added to the configuration. **Workaround:** Use a different name for the group or remove the community.
- In very rare cases, a NetVanta 1638 can get into a state where new MAC addresses cannot be added to the MAC address table. A reboot will resolve the issue.
- Speed and duplex settings are displayed with on MEF Ethernet interfaces in **show running-config verbose** command output, even though those options are not valid and cannot be configured for that type of interface.
- When running R11.1.0 boot ROM on a NetVanta 1531 and attempting to apply a backup firmware image from bootstrap, the switch will display benign errors indicating packets are being dropped due to congestion.
- A track cannot be shutdown or enabled from within the weighted list configuration mode.
- LLDP is not transmitted out PPP interfaces on the NetVanta 4305 when using the Octal T1 NIM.
- The NetVanta 7100 and NetVanta 6355 platforms fail to reset QoS map statistics for applied QoS maps when the **clear counters** command is issued.
- 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.
- The ActivChassis feature can only be disabled from the CLI.
- The authentication parameters of a configured SNMP user cannot be updated without first removing the user.
- The **debug vrrpv3 packet** command does not display debug for all VRFs.
- On the NetVanta 1335 and the NetVanta 3200, removing a NIM is sometimes not resulting in the creation of an exception report.
- In rare cases, a Layer 3 switch may be unable to push a Layer 3 host into the route cache causing latency for that particular host.
- SNMP traps for warm start and cold start are reversed on the NetVanta 6240 Series.
- SFP information for an SFP inserted into a NetVanta 4430 does not display correctly.
- If an SSH client that performs key re-exchange was being used, when a re-exchange was attempted the SSH session will become unresponsive.
- On the Total Access 900e Series (third generation), NetVanta 6250 Series, and NetVanta 4660, the output of the **show process cpu** command may incorrectly show the system load as higher than it actually is. This issue is purely cosmetic.
- 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 MRRU value in output of the **show interface ppp** command always displays default MRRU of 1520, regardless of what is negotiated between the two PPP peers. This issue is purely cosmetic.
- Naming a hardware ACL the same name as a previously created and deleted IP ACL will result in the creation of an IP ACL with an implicit permit.
- Configuring a NetVanta 160's channel setting to **least-congested** may not properly adjust to the least congested channel available.
- The Total Access 900e Series (third generation) and NetVanta 6250 Series send a cold start SNMP trap on reload instead of a warm start trap.
- The **show interface dot11ap** <*number*> command may show an incorrect radio channel for a NetVanta 160.
- When running a large amount of traffic across a VPN tunnel on the Total Access 900e Series (third generation) and the NetVanta 6250 Series with crypto FFE disabled, the unit will occasionally reboot citing a memory issue. Enabling **ip crypto ffe** prevents this reboot from occurring and is the desired setting when configuring VPN due to increased performance functionality of the FFE.
- On very rare occasions, port T1 3/3 on an Octal T1 NIM can stop negotiating LCP when it is part of an MLPPP bundle. Rebooting the device will restore the interface.
- On a NetVanta 6310, if a SHDSL circuit with a detected bad splice retrains to a different line rate, the distance of the bad splice will display incorrectly.
- If the top level ATM interface on a SHDSL ATM NIM2 module is disabled and re-enabled, the ATM circuit will no longer be able to pass traffic. The ADTRAN unit must be rebooted to correct the problem.
- The T1 EFM counters do not increment as traffic passes through the device.

- With the SHDSL ATM NIM2, the NetVanta 6310 drops approximately 1 out of every 15K packets from the SHDSL to Ethernet direction.
- 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.
- Copying a file larger than 20 MB from flash memory of an AOS device via HTTP can cause the AOS device to reboot.
- An AOS device may generate an event message in the CLI reporting a successful NetVanta 160 software upgrade, even if the upgrade failed.
- An AOS device may print an event message in the CLI reporting a successful NetVanta 160 software upgrade, even if the upgrade has failed.
- The command **boot config flash** <*filename*> does not function properly on many AOS platforms.
- A host name entry in an ACL may fail to resolve to the correct IP address even though the router's host table reflects the correct IP address. Workaround: Use IP addresses instead of a host name when creating an ACL.
- When AAA command authorization is enabled, issuing a **show** command with the **realtime** parameter does not result in viewing statistics in real time.
- The IP Top Talkers Graphs in the GUI will sometimes truncate IP addresses.
- Event messages indicating a firmware upgrade was attempted may appear in the AOS event log for NetVanta 160 APs that are not being upgraded.
- Having more than two entries in a Network Monitor ICMP probe test list will display **Tracked by: Nothing** in the **show probe** command output. This is merely a display error; the probes still function correctly.
- Accessing the GUI via HTTPS may be slow.
- VQM may show a loopback interface in the GUI when a loopback interface is not configured.
- When configured for **terminal length 0** certain **show** commands will not provide complete output.
- The VNS verification process does not remove inconsistent A-type records from the host table after the configured number of attempts.
- 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**

- Wi-Fi multimedia (WMM), configured with the command **qos-mode wmm,** does not function properly on NetVanta 150 Access Points.
- When configured with two port channels, each with more than two members, one of the port channels may not evenly distribute traffic sent over the aggregated link.
- A NetVanta 1638 may occasionally display the following message on boot: HTTP_CLIENT CONNECT_TO_HTTP_SERVER errorCode 251. This does not cause a functional problem.
- The **called-number** command on a demand interface does not function properly.

- An ActivChassis stack cannot pass a full 10 Gbps of 64-byte frames over a single 10 Gb fiber link in a NetVanta Dual SFP+ XIM.
- It is possible to create a standard MAC ACL with the same name as an existing extended MAC ACL.
- If a line card has the same VCID as another line card, it cannot be added to the ActivChassis stack. The command **show ac detail** does not adequately point out the reason for this failure.
- If there are spanning tree topology changes in the network, spanning tree will reconverge at rates lower than rapid spanning tree (about 30 seconds).
- The NetVanta 1638 cannot boot from a firmware image stored on a connected USB flash drive.
- If an ActivChassis line card has NetVanta APs physically attached and if the line card is removed and re-added to the ActivChassis stack, the NetVanta APs will not properly indicate the AC that is controlling them. Bouncing the switchport on the line card or rebooting the ActivChassis master will resolve this issue.
- 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.
- Legacy switch stacking cannot be configured if VLAN 2386 is created prior to enabling stacking.
- If a USB modem is physically disconnected from a USB NIM while active, the demand interface being used by the modem will not automatically shut down. The demand interface should be disabled before removing the modem to prevent this issue.
- On the NetVanta 6310/6330, with FFE enabled, passing traffic from the Ethernet 0/1 interface out an Ethernet NIM2 can cause the Ethernet 0/1 interface to fail. The interface is recovered with a reboot. Disabling FFE on the Ethernet 0/1 interface prevents the issue.
- An SNMP walk of the NetVanta 6355 lists the physical address for the first interface index only.
- When a switchport on a NetVanta 1535P is running forced speed 100 Mbps in standard mode (not ActivReach mode), jumbo frames greater than 9000 bytes will be dropped.
- The chassis fans in NetVanta 1544F switches oscillate at a higher frequency than expected during periods when the switch is not being heavily utilized.
- The current AOS implementation of DHCP message construction can result in Windows XP machines not adopting the DNS servers defined within the DHCP offer. A workaround using a numbered IP/hex option will allow the message to be constructed in a manner that Windows XP will accept. Microsoft also offers a hotfix to resolve this Windows issue.
- The system clock may drift and lose synchronization with higher stratum devices when NTP is enabled. This issue only affects the NetVanta 3448, 3458, and 6240 products.
- NetVanta 1500 and 1600 Series switches may not properly prioritize traffic across port channels.
- Certain OIDs in the Bridge-MIB may not return a value on AOS switches.
- The Layer 3 switch incorrectly reports forwarded frames statistics when subjected to a traffic stream consisting of invalid IPv4 header checksum values. The frames are properly dropped by the switch, but the statistics counter erroneously reports frames being forwarded
- The **vap-reference** command will not replicate VLAN IDs for an AP unless 802.1q encapsulation has been manually enabled on the AP expecting to receive the replicated configuration.
- Updating PRL values on a Sprint NetVanta 3G NIM may not function properly.
- 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.
- In rare cases, when an IP PBX and IP phones are both passing through NAT and the SIP proxy on an AOS device, some call flows can enter a one-way audio state. **Workaround**: Enable the **ip rtp firewall-traversal enforce-symmetric-ip** command from the Global Configuration mode.
- A large enough drift in the system clock can cause an error when the NTP server attempts to synchronize.
- On a NetVanta 1335, a switchport that is configured as a port channel cannot change the edge port mode and cannot be changed from a port channel to another configuration using the GUI.
- The **show interfaces** command output for multilink Frame Relay interfaces will display an incorrect available bandwidth value when a physical link residing in the bundle is down.
- 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 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.
- Configuring a port channel on a NetVanta 3448 can cause the STP topology to become unstable.
- Sierra Wireless USB305 3G modems are sometimes not recognized by the NetVanta USB WWAN NIM.
- Changing the route metric value using **ipv6 address autoconfig default metric** <*value*> command does not change the administrative distance of the default route.
- The NetVanta 5305 can drop some traffic prioritized by class-based weighted fair queuing (CBWFQ) on a MLPPP interface when a stand-alone QoS map is applied.
- A NetVanta 5305 can stop passing traffic for brief intervals when negotiating frequent VPN tunnels using Diffie Hellman Group 5.
- The output queue statistics on an Ethernet interface can fail to display output queue drops when FIFO is enabled.
- Prioritized traffic can be dropped at a significant rate on PPP interfaces when using a parent QoS map (that references a child map with priority allocation), if the shaped rate is configured for more than 75 percent of the line rate.
- The CLI does not display the correct value for Required Bandwidth in the event message generated by applying a QoS map.
- EAP Identity Responses from a wireless client that do not contain an Identity field can result in the NetVanta 150 creating a malformed RADIUS packet.
- NetVanta 150s may not properly handle immediate Access-Accept responses to Access-Request messages.
- 3G connections using a NetVanta USB WWAN NIM and a Sierra Lightning modem can fail.
- The name of a deleted IPv4 ACL cannot be used to name a new IPv6 ACL.
- The cellular interface can trigger a core dump on a NetVanta 3448 when changing states.

- Port mirroring on a NetVanta 1544 switch may not mirror traffic in both directions.
- Browsing to the Switchports menu from the Port Security menu on the NetVanta 1335 WiFi GUI results in a 503 Service Unavailable error.
- A Spanning Tree L2 broadcast storm lasting several hours can cause the NetVanta 1335 to reboot.
- The 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.
- 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.
- Booting a second generation NetVanta 1534 or NetVanta 1535 with greater than 20 NetVanta 160 Access Points (APs) attached can cause some of the APs to pull incomplete configuration from the NetVanta switch, if they are being used as an access controller for the APs.
- Using the command **debug ethernet cfm loopback request domain** <*domain name*> to filter Ethernet CFM loopback debugs may not display the debug output to the console. Removing the filter and using the **debug ethernet cfm loopback request** command will function properly.
- The output of the command **show ethernet cfm mep loca**l may display an incorrect maintenance association for a MEP ID if multiple maintenance associations are configured on the unit.
- The NetVanta 6240 should send warm_start SNMP traps when the unit is told to reboot by software. It should only send cold_start traps when the power is cycled. Instead, it is sending cold_start traps, even when reloaded by software.

The following is a list of voice specific errata that exist in products running AOS version R10.9.8, unless otherwise noted.

- The **t38 cng-relay-selective** command does not function properly on the NetVanta 6250, 6360, or Total Access 900e (third generation).
- On the NetVanta 6250, 6360, and Total Access 900e (third generation), DTMF tones that are shorter than the minimum valid-digit requirement are still being qualified as valid digits.
- After the first 18x provisional response is received on a SIP trunk to SIP trunk call through the B2BUA, if additional 18x provisional responses are received, they will not be relayed to the other trunk.
- With transcoding enabled, if a SIP to SIP call through the B2BUA that originally didn't require transcoding is reINVITEd to a CODEC that requires transcoding, and is then reINVITEd again, the transcoding media anchoring session is not removed, resulting in two RTP streams being transmitted.
- The GUI will allow the SNMP link status traps to be enabled and disabled for FXS and FXO interfaces, but the change cannot be saved.
- When **voice transfer-mode local** is configured, if a REFER is received that results in an INVITE going back out the same trunk, headers specified in the Refer-To header of the REFER will be lost.
- Issuing the **show rtp media sessions** command repeatedly results in a memory leak.
- When generating an SNMP trap for a SIP proxy rollover, the wrong OID is used for adSipProxyRollover.
- When using TCP for a SIP trunk, if the port in the Via header differs from the port in the Contact header, the port from the Via header will improperly be used as the Layer 3 destination for new requests.

- When using MGCP, receiving caller ID information in a MDCX breaks caller ID on that port until the unit is rebooted.
- Outbound messages from certain templated SIP proxy users are not routed correctly if the user is set up from an inbound request and the outbound contact user is different.
- If the received caller ID number from a FXO interface is greater than 11 digits, the caller ID string will be corrupted.
- In rare cases, a reboot can occur during ISDN call setup/teardown.
- On an FXO to SIP call, the talk path is opened in both directions upon receipt of a 18x response with SDP. The talk path should only be opened in the SIP to FXO direction.
- 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.
- Removing a voice trunk with active calls can result in a reboot.
- The detailed voice quality statistics for a call may not accurately reflect the adjustments made by the **modem-passthrough** command.
- Using a packet capture with a size limit of 16 MB or greater may result in a reboot.
- If the trunk through which a voice user registers is deleted from the configuration, that user will still be displayed in the output of **show sip trunk-registration** command.
- On the Total Access 900e Series (third generation) and NetVanta 6250 Series, if the second CODEC listed in the MGCP Local Connection Options is not one of the CODECs defined in the CODEC list assigned to the MGCP endpoint, the unit will respond with 534 Transaction Failed response resulting in a failed call.
- On the NetVanta 6250 and Total Access 900e (third generation), the **timing-source internal** command is not present. The workaround is to configure **no timing-source t1** <*slot/port*>.
- With the conferencing mode set to network and two calls up on an FXS port, if no conferencing URI was configured, performing a hook flash will not switch between the two calls.
- In AOS R10.4.0 and higher, modem-passthrough will fail to send a reINVITE to G.711 if the endpoint is configured with a codec-list that doesn't contain G.711.
- The command **ip mgcp qos dscp** <*value*> will not take effect until either **ip mgcp** is disabled and then enabled or until the AOS device is reset.
- When both **g711alaw** and **g711ulaw** are present in a CODEC list, G.711u will be chosen by modem passthrough, even if **g711alaw** is listed higher in the CODEC list than **g711ulaw**.
- In the PRI settings, invalid switch type options are presented in the GUI drop-down list.
- 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 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 Series, SIP must be enabled in the running configuration whenever MGCP is used for voice.
- Invalid characters are allowed in a host name for the SIP server on a voice trunk.
- In the ISDN voice trunk GUI, the **Disabled:Busy on Idle** and **Disabled:Busy Immediately** Administrative Status options do not function.

- On the Total Access 900e (third generation), NetVanta 6250, and NetVanta 6360, if the remote voice gateway changes the SSRC in an RTP stream received by the AOS unit, and the sequence numbers are not contiguous, VQM and the output of the **show voice quality-stats** command will log lost packets for the number of packets between the last sequence number of the first stream and the first sequence number of the new stream. The output of **show voice quality-stats** <*ID*> will also not reflect that the SSRC value changed on the call.
- When G.729 Annex B is negotiated and VAD is enabled on the endpoint(s) involved in the call, the unit will generate comfort noise packets with payload type 13. This can cause issues with devices expecting comfort noise packets to have the same payload type as RTP (18). However, payload type 13 is specified in the SDP from the AOS device.
- If an ADTRAN unit is configured with single call appearance mode, forwarded calls on a PRI trunk will fail.
- Receiving a 183 after a 183 on hairpin calls when using media anchoring could result in no early media if the SDP in the second 183 differs from the first.
- Echo cancellation is not enabled on three-way calls when using the local conferencing feature.
- On NetVanta 6240 Series units, V.21 messages will sound overly amplified when listening to the TX output of a T.38 DSP capture. This is a flaw of the capture utility and not representative of how the audio actually sounds.
- DSP captures on the NetVanta 6240 and 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 AOS unit set for **voice flashhook mode transparent**, the conference originator must wait for the third party to answer before executing the flashhook to initiate the conference.
- On the NetVanta 6240 Series, over an extended period of use, T.38 calls can cause DSP channels to cease producing a dial tone and have poor voice quality. Rebooting the unit will correct the problem.
- NetVanta 6240 only: While running 29 or more simultaneous calls using E&M Immediate, Wink, or Feature Group D, it is possible to get in a state where DTMF tone detection will not function on any outbound (DSX to SIP) call using DSP 0/1.15 or higher. While in this failed state, all calls will continue to function in either call direction on DSP 0/2, as well as all calls on DSP0/1 in the inbound direction. With a load of 28 or less calls, all calls will function reliably in both directions on both DSPs. No consistent work around has been identified at this time. A unit reboot will typically solve the problem.
- The NetVanta 6240 Series IP Business Gateways can reboot if 60 simultaneous calls are placed through the DSP.
- The Total Access 900e Series (second generation) cannot properly handle more than 40 simultaneous E&M RBS calls. More than 40 simultaneously active calls could result in no dial tone or no audio on the last 8 channels.
- Using the HEAD acoustics test suite, some G.168 echo cancellation test cases fail on the NetVanta 6240 and NetVanta 644. These same tests pass on Total Access 900 Series units. There is no reason to believe this would affect a customer in the field.
- On the NetVanta 6310/6330 Series, if a SIP trunk is trying to register a large number of users and the registration fails, activating **debug sip trunk-registration** will cause the Telnet and console connection to become unresponsive. A reboot clears the condition.

Upgrade Instructions

Upgrading ADTRAN products to the latest version of AOS firmware is explained in detail in the configuration guide *Upgrading Firmware in AOS*, available at https://supportforums.adtran.com.

Documentation Updates

The following documents were updated or newly released for AOS version R10.9.8 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*
- *Configuring IPv6 in AOS*
- *NetVanta 1131 Redundant/Extended Power Supply Quick Start Guide*
- *NetVanta 6240/6250 Quick Start Guide*

