RELEASE NOTES

AOS Converged Access
AOS version R11.10.5
October 7, 2016

Trademarks

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

To the Holder of the Manual

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

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

Toll Fraud Liability

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

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

ADTRAN Technical Support Community

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

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

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

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

Contents

Introduction

AOS version R11.10.5 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 17*.

Configuration guides, white papers, data sheets, and other documentation can be found on ADTRAN's Support Forum, https://supportforums.adtran.com. The contents of these release notes will focus on the platforms listed below.

Supported Platforms

The following platforms are supported in AOS version R11.10.5. 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/1238/1238P (2nd and 3rd Gen.)	√			XB.01.02
NetVanta 1235P	√			R10.4.0.B1
NetVanta 1335		√		15.01.00
NetVanta 1531/1531P	√			R11.1.0
NetVanta 1534	√			17.06.03.00
NetVanta 1534 (2nd Gen.)	√			17.08.01.00
NetVanta 1534P (2nd Gen.)	√			17.09.01.00
NetVanta 1535P	√			17.08.01.00
NetVanta 1544/1544F	√			17.06.04.00
NetVanta 1544 (2nd Gen.)	√			17.08.01.00
NetVanta 1544P (2nd Gen.)	√			17.09.01.00
NetVanta 1550	√			BVS1.0
NetVanta 1638/1638P	√			18.02.01.SC
NetVanta 3120		√		14.04.00
NetVanta 3130		√		14.04.00
NetVanta 3140	√	√	√	R11.5.0
NetVanta 3200/3205 (3rd Gen.)	√	√		17.02.01.00
NetVanta 3305 (2nd Gen.)	√	√		04.02.00
NetVanta 3430	√	√		13.03.SB
NetVanta 3430 (2nd Gen.)	√	√	√	17.05.01.00

Platform	Standard Feature Pack	Enhanced Feature Pack	SBC Feature Pack	Minimum Boot ROM
NetVanta 3448	√	√	√	13.03.SB
NetVanta 3450	√	√		17.06.01.00
NetVanta 3458	√	√		17.06.01.00
NetVanta 4305 (2nd Gen.)	√	√		08.01.00
NetVanta 4430	√	√	√	17.04.01.00
NetVanta 4660		√	√	R10.10.0.B5
NetVanta 5305	√	√		11.03.00
NetVanta 5660		√	√	R11.4.1.B2
NetVanta 6240		√	√	A5.01.00
NetVanta 6250		√	√	R10.9.0
NetVanta 6310/6330		√	√	A3.01.B2
NetVanta 6355		√	√	14.06.00
NetVanta 6360		√	√	R11.2.0
NetVanta 6410			√	R11.3.0
Total Access 900 Series (2nd Gen.)		√		14.04.00
Total Access 900e Series (2nd Gen.)		√	√	14.05.00.SA
Total Access 900e Series (3rd Gen.)		√	√	R10.9.0

System Notes

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

  Due to this syntax change, downgrading a unit configured in AOS version R11.10.5 to a previous AOS version, could cause service disruption because the new syntax might not be recognized by the previous version. Upgrading a unit from an older AOS version to AOS version R11.10.5 will cause no service disruption because both the old and the new syntaxes are accepted. For more information on specific commands, refer to the *AOS Command Reference Guide* available at https://supportforums.adtran.com.
- It is recommended that your browser's cache be cleared before viewing the GUI after an upgrade.
- MGCP is not supported on the NetVanta 6360.

Features and Enhancements

This section highlights the major features, commands, and behavioral changes for all Converged Access products running AOS version R11.10.2.

- The **any-activity** parameter was added to the **line-timeout** command to allow traffic from the AOS device to the client to reset the CLI session inactivity timer.

This section highlights the major features, commands, and behavioral changes for all Converged Access products running AOS version R11.10.1.

- Added FFE Flow bundling on the NetVanta 4660 and 5660 which enables FFE flows to be combined by using wildcard criteria that have no effect on the flow. This can reduce the total number of flows that must be managed while maintaining the same FFE behavior.

  Flows can be wildcarded on 11 criteria that are independent for IPv4 and IPv6 and are determined on a per-interface basis. The ability for one of the criteria to be wildcarded depends on the configuration of the unit. The following criteria can be wildcarded:

  Source Address

  IP Precedence (first 3 bits of TOS byte)

  IP DSCP (first 6 bits of TOS byte)

  IP Protocol (L4)

  TCP Source Port

  TCP Destination Port

  UDP Source Port

  UDP Destination Port

  ICMP Type, Code and ID

  ESP SPI

  GRE Tunnel Key

  The wildcards that are enabled are determined automatically based on the unit's configuration. With basic routing, all wildcards will be enabled for an interface. The more enabled features and match criteria are used, the smaller the list of enabled wildcards becomes.
- Added on the NetVanta 5660, the ability to classify into queues different types of packets destined to the unit. Additionally, these queues can be policed and processed in a weighted round robin fashion to prevent any type of traffic from monopolizing the CPU.

This section highlights the major features, commands, and behavioral changes for all Converged Access products running AOS version R11.10.0.

- Added support for battery status monitoring on the Total Access 900e (third generation) Battery Enhanced model. This feature provides the user with notifications of various battery status events, such as a disconnected, low, or aged battery. It also allows the user to view information relating to the battery status at any time. The user can set the battery install date, which will be stored in non-volatile memory so that it is preserved even if the configuration is erased.
- Added RapidRoute service assurance features. Commands were added to show the current FFE peak session count and peak history. Also added is the ability to track whether the number of FFE sessions on an interface is below a configured value.
- The **bandwidth** command on a Layer 3 interface will now update the RFC 1213 MIB ifSpeed variable.

This section highlights the Carrier Ethernet specific features, commands, and behavioral changes available in products running AOS version R11.10.1.

- On the NetVanta 4660 and 5660, a SNMP trap was added that is generated whenever the T4 status becomes squelched and un-squelched as a result of crossing the **minimum-ssm-ql** threshold. Additionally, the **transmit-ql-threshold** command was added to provide a method to place an upper limit on the value of the SSM-QL sent by the device.

This section highlights the Carrier Ethernet specific features, commands, and behavioral changes available in products running AOS version R11.10.0.

- Added the ability to specify a class 1 multicast address as a target MAC address for Y.1731. An OAM frame destined for a class 1 multicast address is an OAM frame that is addressed to all peer MEPs in a MEG. There are 8 specific multicast addresses that can be used, 01:80:C2:00:00:3X where X is the level of the MEG (0-7).. Class 1 multicast addresses are now accepted as the target MAC address for continuity check messages (CCM), loop back messages (LBM), single ended synthetic loss measurement message (SLM), single ended frame-loss measurement messages (LMM), one-way delay measurement messages (1DM), and two-way delay measurement messages (DMM).

This section highlights the Voice specific features, commands, and behavioral changes available in products running AOS version R11.10.0.

- Added warm line functionality in which a number can be dialed automatically by a FXS voice user if no digits are received within the configured amount of time.
- Added the ability to monitor the registration state of a SIP voice user in tracks.
- Added the ability to configure an analog loop voltage holdover time on the Total Access 900e (third generation) Battery Enhanced model. This feature allows the unit to continue to apply loop voltage during boot. Loop voltage is applied until the holdover time expires or the unit boots and the applied configuration takes over.

Fixes

This section highlights major bug fixes for all products running AOS version R11.10.5.

- To address CVE-2016-1409, received ICMPv6 ND packets will no longer be forwarded.
- When using the **copy console flash startup-config** command, a reboot occurred if Auto-Link attempted to perform a check-in before Ctrl+D was pressed.
- When using the firewall with policy-based routing (PBR) and WAN failover, changes to the next hop specified in a route map were not applied properly after the primary connection failed unless **ip firewall fast-allow-failover** was configured.
- The licensing page in the GUI did not display the same information displayed in the CLI.
- On the NetVanta 4660, 5660, 6250, 6360, and Total Access 900e (third generation), the unit incorrectly displayed 100 percent CPU utilization after a long uptime.
- If the **shutdown** and then **no shutdown** commands were issued on a PPPoE interface, two PADT packets were transmitted instead of just one. The same issue also occurred if the **clear pppoe** <*interface*> command was issued.
- When **debug ipv6 dhcp client** was enabled, no output was displayed.

- If multiple RADIUS or TACACS+ servers were defined in the configuration, applying changes in the **Passwords** > **Service Authentication** section of the GUI resulted in the removal of all but one of the defined RADIUS or TACACS+ servers.
- The GUI accepted spaces in the text fields for RADIUS and TACACS+ server hosts, which allowed an invalid configuration to be applied.
- In rare cases, a reboot occurred on the NetVanta 6410.
- When reporting the SFP Tx Bias Current via the SNMP entPhySensorValue, the value was rounded to the nearest integer even though entPhySensorPrecision indicated that two decimal points of precision were being provided.
- On the NetVanta 4660, 5660, and 6360, if **speed 1000 nonegotiate** was configured on gig 0/1 and a fiber SFP was in use on that port, the ifSpeed and ifHighSpeed OIDs listed a bandwidth value of 0. The **show interface** output also displayed a bandwidth of 0.
- Brute force protection on the console port did not function properly if AAA was enabled.
- If **auto-config firmware definition-file** pointed to a binary file instead of a text file, a reboot occurred when auto-config was enabled.
- SFP information was not reported properly for SFPs that support 100Base-FX.
- On some 1 Gbps DWDM SFPs, the DWDM MSA data was interpreted as MSA data, resulting in the minimum temperature, maximum temperature, and maximum supply current being reported incorrectly.

This section highlights major bug fixes for all products running AOS version R11.10.4.

- DHCP offers destined for an interface were not processed if a static secondary IP address was applied to the interface.
- If a unicast DHCP REQUEST was received for DHCP renewal, the request was discarded if the IP address originally assigned came from a DHCP pool used to service DHCP requests relayed by another device. A similar issue was resolved for DHCP INFORM requests.
- A reboot occurred if a VRF that previously had DNS configuration applied to it was removed.
- A 503 Server Error was returned when trying to access a SHDSL interface on a NetVanta 6310 or 6330 with a SHDSL EFM NIM2 installed.
- The **default-router** parameter inside DHCP pools was not displayed when the command **show run verbose** was issued.
- TLS profile IP address validation previously resolved the Common Name (CN) in the certificate received from the peer, which was improper behavior. Now, if IP address validation is enabled, the IP address of the peer must be found in a SAN IP field or the CN if there are no SAN IP fields present.
- The RSA keys for the HTTPS server were not generated with enough entropy prior to R11.10.0. Upon upgrade to R11.10.4 and R12.1.0 and later, a new HTTPS certificate and keys will be generated to resolve this issue.
- When setting session cookies, the GUI did not set the HttpOnly flag.
- The **http source-interface** command was missing from the NetVanta 4660, 5660, and 6360.

This section highlights major bug fixes for all products running AOS version R11.10.3.

- In some cases, if the NTP server was under heavy load, the AOS unit rebooted.
- In rare cases, a reboot occurred when the **show bgp ipv4 community-list** command was issued.

- In some cases, exception reports were truncated on the NetVanta 3140, 4660, 5660, 6250, 6360, and Total Access 900e (third generation).
- If a user attempted to navigate directly to the ACL details page by pasting the full URL into their browser, a 503 Service Unavailable error message was returned.
- If a configuration change was made that updated the CPU MAC address filter (such as adding a Ethernet subinterface), IGMP traffic no longer properly reached the CPU on interfaces on which IGMP was enabled. This issue affected the NetVanta 1638, 3140, 3430, 3448, 4430, 4660, 5660, 6240, 6250, 6310, 6330, 6330, and Total Access 900e (third generation).
- It was not possible to add QoS maps to Gigabit Ethernet interfaces using the GUI.
- If the **startup-config.bak** file was not present when copying a file from an HTTP/HTTPS server to the startup configuration, the file was not successfully written to flash memory.
- On products that support the SIP proxy but not the SBC feature pack, it was not possible to enable UDP relay on ports 10000 to 13000.
- /32 routes from loopback interfaces were always advertised by RIP even when **redistribute connected** was not configured.
- The command **snmp trap link-status** was improperly enabled by default on Frame Relay subinterfaces.

This section highlights major bug fixes for all products running AOS version R11.10.2.

- When sending DHCPv6 Relay-Reply messages, the AOS DHCPv6 server previously used the source port from the corresponding received Relay-Forward message as the destination port for the Relay-Reply message. The AOS DHCPv6 server now always uses UDP port 547 as the destination port for Relay-Reply messages.
- When attempting to create a voice trunk on a NetVanta 3140, 4660, or 5660 without the SBC feature pack installed, creation of the trunk failed silently instead of with an error that stated that the SBC feature pack is required to create voice trunks.
- If a GRE tunnel had an IPv6 address, but no IPv4 address, the appropriate RapidRoute wildcard entries were not disabled.
- When attempting to push a large configuration via the Push Config feature on n-Command MSP, the configuration push failed with an error stating that Chunked Transfer was not supported.
- In some cases when NTP started, an event stating **NTP Frequency format error in .ntp.drift** displayed.
- When issuing the **no privilege** <*command set name*> **all level** <*1-7*>, the first **privilege** entry in the running configuration that used the **all** keyword was removed instead of the matching entry.
- Added the **fragments** keyword to **permit ip** and **deny ip** statements in IPv4 ACLs. If this keyword is used, that ACL entry will only match non-initial fragments, allowing the user to block non-initial IPv4 fragments.

  If the **fragments** keyword is omitted from a **permit ip** or **deny ip** statement in an IPv4 ACL, both initial and non-initial IPv4 fragments will match if the Layer 3 addressing matches the ACL entry.

  If an IPv4 ACL entry specifies a protocol or Layer 4 information, that entry will not match non-initial IPv4 fragments.

  If no ACL entries match, non-initial IPv4 fragments will be implicitly permitted.
- If an interface was configured with both an IPv4 and a global unicast IPv6 address, NTP would not listen on the global unicast IPv6 address.

- Added the **fragments** keyword to **permit ipv6** and **deny ipv6** statements in IPv6 ACLs. If this keyword is used, that ACL entry will only match non-initial fragments, allowing the user to block non-initial IPv6 fragments.

  If the **fragments** keyword is omitted from a **permit ipv6** or **deny ipv6** statement in an IPv6 ACL, both initial and non-initial IPv6 fragments will match if the Layer 3 addressing matches the ACL entry.

  If an IPv6 ACL entry specifies a protocol or Layer 4 information, that entry will not match non-initial IPv6 fragments.

  If no ACL entries match, non-initial IPv6 fragments will be implicitly permitted.
- If an internal application such as the **ping** command queried a hostname (as opposed to an FQDN) and the name server had only an A or AAAA record for the hostname with the configured domain name appended (i.e. an FQDN) but not both, the command failed with a DNS related error.
- The reliability of exception report creation on the NetVanta 6410 was improved.
- When creating or editing a track on a unit running R11.10.0 or later, a 503 Server Error response was returned if the unit did not support voice.
- On products that do not support IPv6, it was not possible to remove SNMPv3 users.

This section highlights major bug fixes for all products running AOS version R11.10.1.

- In rare cases, issuing the command **show dot11 access-point detail** on an AOS access controller caused the controller to reboot.
- In some cases, if a NetVanta 3140 was under a heavy packet load, especially if a traffic shape rate was configured, the unit rebooted.
- The SysObjID value sent by the NetVanta 6360 and 6410 was incorrect.
- Clearing an NHRP entry for a spoke behind NAT using the **clear ip nhrp** <*address*> command failed.
- The **privilege interface-tunnel** command was no longer accepted in R11.9.0 and later.
- If an AS_SET with multiple ASNs from 2-byte ASN BGP speaker was received, a reboot occurred.
- Sending packets larger than the MTU when an FFE entry did not exist caused an erroneous flow entry to be created reflecting the traffic back out of the ingress interface instead of sending the appropriate ICMP message.
- Routing performance on the NetVanta 4430 decreased by 6 percent compared to R11.9.0.
- When using PPPoE or PPP over Frame Relay (PPPoFR), QoS did not function properly if the QoS policy was applied to the lowest level interface.
- If a user configured the same VLAN ID on the dot11ap subinterface that was configured on the parent dot11ap interface as the native VLAN, the configured VLAN was not shown on the subinterface in the running configuration. This issue did not affect the x/y.1 subinterface.
- On the NetVanta 3140, the GUI listed USB LTE modems as configurable WAN interfaces even though they could not be configured through the GUI.
- On R11.8.0 and later, products that did not support voice showed a Voice option in the GUI.
- In some cases, on the NetVanta 4660 and 5660, if the CPU was under 100 percent load for a long duration, a reboot occurred.
- In rare cases, if the command **no auto-link server** was issued without specifying the IP address or FQDN of the server, a reboot occurred.

- On the NetVanta 4660 and 5660, jumbo frames were dropped by Gigabit Ethernet interfaces 0/2 through 0/5 when **speed 100** was configured on those interfaces.

This section highlights major bug fixes for all products running AOS version R11.10.0.

- If the running configuration was downloaded from the device using the GUI, the file name was too long to be uploaded to the unit.
- If a **startup-delay** was configured on a VRRPv3 group and it had not yet gone through another state (as would be the case on a reboot or the interface being **shutdown** then **no shutdown**), the startup delay timer was not canceled on a received secondary advertisement.
- In AOS R11.8.0 and R11.9.0, output from CLI commands in a Tcl script may have only returned partial results.
- On the NetVanta 6250, 6360, and Total Access 900e (third generation), if the CPU was under 100 percent load for a long duration of time, a reboot may have occurred.
- GRE over IPsec performance was poor on the NetVanta 3140, 4660, 5660, 6250, 6360, and Total Access 900e (third generation).
- On the NetVanta 3140, if the CPU was under 100 percent load for a long duration of time, a reboot may have occurred.
- When using NHRP and the hold time was less than or equal to 60 seconds, a resolution request was not sent during the proactive lookup time.
- If a Tcl script was added to the configuration that followed a track, was then removed, and then re-added to follow a different track, it was not added to the running configuration.
- If two SNMP communities were configured and only one community had an access class applied to it, the access class was applied to both communities.
- The power rollover SNMP trap did not contain the correct OIDs for the adGenAOSPowerRolloverOnAC and adGenAOSPwrRollOvrEvntSecSinceEpoch varbinds. AOS would send an enumeration value that ranged from 0 to 4 for the adGenAOSPowerRolloverOnAC value, rather than the TruthValue of 1 or 2 that the MIB specifies.
- If the GUI was used to disable port security and sticky MAC addresses were present, the unit locked up.
- On the NetVanta 6250 and Total Access 900e Series (third generation), when running a large amount of traffic across a VPN tunnel with crypto FFE disabled, the unit would occasionally reboot citing a memory issue.

This section highlights the Carrier Ethernet specific bug fixes in products running AOS version R11.10.5.

- 01:80:C2:00:00:2E and 01:80:C2:00:00:2F were not included in the list of Layer 2 control protocol destination MAC addresses matched by **match l2cp** on an EVC map.
- If a Y.1731 MEP was configured after the EVC monitored by that MEP was configured, E-LMI on the associated UNI port would report an EVC status of ACTIVE when the MEP was in a loss of continuity (LOC) state.
- When network sync switched from the primary to the secondary timing source, the generated SSM-QL momentarily changed to QL-EEC1.

This section highlights the Carrier Ethernet specific bug fixes in products running AOS version R11.10.4.

- The **bonding** command set was missing from EFM group interfaces on the NetVanta 5660.

This section highlights the Carrier Ethernet specific bug fixes in products running AOS version R11.10.3.

- When using Elcon SHDSL repeaters/regenerators in the circuit, in some cases the SHDSL Carrier Ethernet module did not detect the bonding mode properly when **bonding auto-detect** was configured.
- If an EFM group or Gigabit Ethernet interface was down when a Y.1731 MEP was created, the interface status TLV in the CCMs transmitted by the unit would always display as **Down**. The interface status was not properly updated when the interface came up.
- On the NetVanta 4660, 5660, and 6360, the value for **Rx Invalid CE-VLAN ID Frames** in the output of **show interface gigabit-ethernet 0/x performance-statistics** command was inaccurate.

This section highlights the Carrier Ethernet specific bug fixes in products running AOS version R11.10.2.

- If **ethernet y1731 file-save** commands were present in the running configuration and the configuration was saved, the commands were not restored upon rebooting the unit.
- On the NetVanta 6360, in rare cases a reboot occurred when a VDSL Carrier Ethernet module was installed.

This section highlights the Carrier Ethernet specific bug fixes in products running AOS version R11.10.1.

- If a MEG was configured for double-tagged service, Y.1731 traffic was not received on that MEG.
- If an EVC map was matching on multiple CE VLAN IDs and Y.1731 was being used on the EVC referenced by the EVC map, the CLI would become unresponsive for a few minutes when Y.1731 was coming up.

This section highlights the Carrier Ethernet specific bug fixes in products running AOS version R11.10.0.

- When using the Quad VDSL Carrier Ethernet module, vectoring error samples were not sent properly which prevented vectoring from functioning properly.
- The Y.1731 loopback unicast verbose command did not display details in the loopback test results.
- The Y.1731 performance monitoring data file names were changed to use a UTC time stamp that matches the UTC time stamp used in the data inside the files.
- If Y.1731 was in use and multiple CE VLAN IDs were present in a **match ce-vlan-id** statement on an EVC map, certain configurations resulted in the unit running out of internal resources causing either Y.1731 to fail or the unit to lock up.

This section highlights the Voice specific bug fixes in products running AOS version R11.10.5.

- Modem passthrough did not detect any fax/modem tones when inband call progress tones were provided and it took more than a few seconds to answer the call.

- When **sip proxy transparent ip-spoofing** was configured, the host portion of the Contact URI in the 200 OK response to REGISTER requests was incorrectly modified to the SIP server's IP address when the 200 OK was proxied towards the phone.
- If the SIP proxy was in use with multiple configured servers and a call was established with a secondary server, any reINVITEs on that call were improperly sent to the primary configured server.
- Outbound call matching in the SIP proxy did not function properly when **match outbound source from** was configured on a user template.
- On a call between two SIP trunks, transcoding could not be forced by CODEC lists if the received SDP offer on the inbound call and the received SDP answer on the outbound call shared a common CODEC.
- When using the SIP proxy in transparent mode, there was a very short window of time in which a proxied INVITE sent in response to an authentication challenge was not routed to the original Layer 3 destination.
- If two SIP trunks were defined that used the same FQDN but different port numbers, inbound calls did not match the correct trunk if only an A record existed for the FQDN.
- On the NetVanta 6250, 6360, and Total Access 900e (third generation), if caller ID was received on an FXO port and the continuous mark signal was less than 150 ms, caller ID was not detected properly.

This section highlights the Voice specific bug fixes in products running AOS version R11.10.4.

- If an offered media stream from SDP was rejected, memory was leaked. This resulted in a reboot over time.
- The default value for the **early-cut-through** option on ISDN voice trunks was not set properly at boot.
- If a FXS user placed a call that routed out a SIP trunk then hairpinned back from the SIP trunk and out a PRI on the same unit, and was then disconnected by the FXS user, one way audio was experienced on that DSP channel until the FXS port went offhook again. This issue only affected the NetVanta 6250, 6360, and Total Access 900e (third generation).
- If an AOS device received a reINVITE with a higher CSeq value while it was waiting for an ACK to a previous INVITE with a lower CSeq, a 500 Server Internal Error response was sent instead of a more appropriate response, such as 491 Request Pending. The scenario involved is described in RFC 5407 Section 3.1.4.
- If a dial string which contained an escaped sequence was received by the B2BUA from a registered SIP voice user or SLA, it was not unescaped at ingress. This led to double escaping at egress.
- In rare cases, a reboot occurred when using the SIP proxy.
- If an INVITE with a Replaces header was received while a call was still connecting, a reboot could occur.

This section highlights the Voice specific bug fixes in products running AOS version R11.10.3.

- If a 400, 500, or 600 level error response was received in response to a NOTIFY that was terminating the subscription, a subscription resource was leaked.
- If the SIP proxy monitor was configured in on-failure mode for use with the SIP proxy in both stateful and transparent modes, when a server failed, the SIP proxy monitor would not mark that server as down.
- When using the SIP proxy in transparent mode with the SIP proxy monitor and registration rate adaption, a 200 OK response to a REGISTER will now only be spoofed if one of the following conditions is true:
  - The REGISTER is destined to the server that handled the last successful registration.
  - All monitored servers are down.

- When the **clear sip resources** command was issued, the maximum used count for **CallLeg transcLists** was not cleared.
- If the SIP proxy monitor was used in on-failure mode with a recovery delay, the recovery delay was improperly cleared when the primary server went down instead of being cleared only after the configured delay period expired.

This section highlights the Voice specific bug fixes in products running AOS version R11.10.2.

- When using the SIP proxy in transparent mode on R11.10.1 or R11.11.0, an out of memory reboot may have occurred.
- In R11.8.0 and later, ring groups did not function without a valid SBC license.
- In rare cases when using MGCP on the NetVanta 6250 and Total Access 900e (third generation), the unit failed to properly construct a CODEC string, resulting in the unit not sending RTP.
- When in survivability, the SIP proxy sent received PUBLISH requests to the B2BUA instead of responding with a 480 Temporarily Unavailable response.
- When running R11.11.0, if an outbound proxy was configured on a SIP trunk and the SIP server and/or registrar was configured as an IP address or FQDN that resolved to an A or AAAA record, 0 was used for the port in the Request-URI, From, and To URIs instead of the correct port.
- In R11.8.0 and later, voice loopback accounts using RTP media loopback did not function without a valid SBC license.
- SIP proxy user database information was not updated properly upon receipt of a REGISTER when a phone changed key registration information such as its IP address. This led to database lookup failures and calls being routed improperly.
- When using the SIP proxy in transparent mode with Layer 3 address spoofing enabled, if the phone switched its registration from the primary server to a backup server, the IP address of the primary server was spoofed instead of the backup server currently in use.
- When a media stream was rejected the port is set to 0. If the media description (m=) contained connection data (c=), it was erroneously set to 0.0.0.0 as well. This lead to the stream being incorrectly identified as being on hold.
- If a port was specified on a SIP server that was configured with an FQDN that resolved via a SRV record, the Request-URI, From URI, and To URI in REGISTER messages listed the configured port instead of the port from the SRV record.
- On R11.10.1 and R11.11.0, if VQM was enabled and the unit was under heavy SIP to SIP call load, a reboot may have occurred.
- On the NetVanta 6250, 6360, and Total Access 900e (third generation), only the lower 16 bits of the SSRC were being changed for new streams. As a result, the probability of repeating an SSRC between two streams over a short period of time was high.
- Improved the clarity of the SIP proxy debug when a device using the SIP proxy in transparent mode rolled to a new Layer 3 destination.
- After issuing the **test line** command on an FXS port on a NetVanta 6250, NetVanta 6360, or Total Access 900e (third generation), the unit no longer provided a dial tone after the line test was complete until the unit was rebooted.

- On the Total Access 900e (third generation) and NetVanta 6250, if the remote voice gateway changed the SSRC in an RTP stream received by the AOS 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. The output of **show voice quality-stats** <*ID*> also did not reflect that the SSRC value changed on the call.

This section highlights the Voice specific bug fixes in products running AOS version R11.10.1.

- In R11.9.0 and R11.10.0, calls matching a **sip proxy emergency-call-routing accept** template were not routed to the switchboard.
- On a call between two SIP trunks, transcoding could not be forced by CODEC lists if the received SDP offer on the inbound call and the received SDP answer of the outbound call shared a common CODEC.
- When using the SIP proxy in transparent mode with Layer 3 source address spoofing, in failover the media gateway IP address was used as the Layer 3 source address instead of the most recently contacted server's address.
- If the Contact URI host in a received SIP message resolved to an IP address that would be reached through a different interface than the one on which the SIP message arrived, SDP was populated with an incorrect IP address when using media anchoring. This occurred even if the address specified in the maddr parameter was reached through the interface on which the SIP message arrived.
- The **Busy Mins** and **Busy %** values in the Trunk Statistics GUI reported inaccurate values.
- SNMP OID 1.3.6.1.4.1.664.5.53.5.2.1.1.1.3 returned a value of 4 for an active call, which did not match the MIB. The MIB has been updated to match the value sent by the unit.
- When using the SIP proxy with media anchoring, VQM reported incorrect information for LocalURI, RemoteURI, and LocalCaller if a reINVITE that modified the SDP was received from the called party during a call.
- Call waiting caller ID did not function properly on the NetVanta 6240.

This section highlights the Voice specific bug fixes in products running AOS version R11.10.0.

- If an MGCP call received an MDCX that set the ConnectionMode to sendonly and then another MDCX later changed the ConnectionMode to sendrecv, the connection remained in the sendonly mode.
- When using ground start, linear hunt ring groups did not roll to the next line.
- When using SIP TLS in client/server mode, if a received Contact URI did not contain the port but did specify TLS in the transport parameter, AOS attempted to initiate a TLS connection to TCP port 5060 instead of 5061.
- When using the SIP proxy, if a reINVITE without SDP was received in the opposite direction of the original call, one-way audio occurred. This issue only affected R11.7.1 and R11.9.0.
- In some cases, if SIP proxy rollover was triggered by a 503 Service Unavailable response, a reboot occurred.
- Under certain conditions, a CANCEL destined to a SIP proxy user failed to be forwarded by the SIP proxy.
- In rare cases, a reboot occurred while processing a reINVITE.
- If the caller ID number received via MGCP was surrounded by quotation marks, the number displayed as **out of area**.

- When **ringback override 180** or **ringback override 183** were configured on a SIP trunk, modem passthrough did not function properly on calls involving that trunk.
- The output of the **show rtp quality-monitoring interface summary** command listed more completed calls than the unit was configured to store.
- In some cases, removing a voice trunk while calls were active resulted in the unit rebooting.

This section highlights the Switch specific bug fixes in products running AOS version R11.10.5.

- When using ActivChassis on a NetVanta 1638, false positive input errors may have been counted on the ports configured for ActivChassis.
- Port channel failover did not function properly on the NetVanta 1550-48 and 1550-48P.
- When using the Fluke LinkRunner AT 2000 Cable/Ethernet tester, PoE tests often failed.
- In rare cases, a reboot occurred on the NetVanta 1638.

This section highlights the Switch specific bug fixes in products running AOS version R11.10.4.

- On the NetVanta 1531 and 1550, two PC Config and RSTP threads may have been displayed in the output of **show process cpu**.
- SHA1 hashing for SNMPv3 did not function properly on the NetVanta 1531 and 1550.
- Occasionally, when powering a device that used the Power via MDI LLDP feature, if a different PoE device was disconnected from the switch or rebooted, all PoE devices connected to the same switch would lose power momentarily.
- In rare cases, an erroneous fan stalled message was shown or a reboot occurred on NetVanta 1638 switches.

This section highlights the Switch specific bug fixes in products running AOS version R11.10.3.

- The factory default IP address of 10.10.10.1 was not reachable if the switch had not obtained an IP address via DHCP.
- When using the 1700486F1 10GBase-LR SFP+ in a NetVanta 1550, the link was not restored if the peer was rebooted.
- In NetVanta 1638 ActivChassis applications AWCP frames were throttled, which caused errors and prevented firmware upgrades on NetVanta 150 and 160 Series access points.
- In some cases, the **shutdown** command was not properly applied to all switchports selected by the **interface range** command.

This section highlights the Switch specific bug fixes in products running AOS version R11.10.2.

- In some cases, when using the 1700485F1 10GBase-SR SFP+ on a NetVanta 1550, after a reboot the link failed to be established.
- PoE+ (IEEE 802.3at) capable switches sent a power class of 0 instead of 4 in LLDP.
- When inserted, the following SFP+ interconnect cables were reported as unsupported by NetVanta 1550 series switches, but the cables still functioned properly otherwise:

  1710484F1 - 1M Volex VSFPP30H-1M 10G DAC

  1710484F3 - 3M Volex VSFPP30H-3M 10G DAC

  1710484F5 - 5M Volex VSFPP26H-5M 10G DAC

- The active CPU process load percentages on the NetVanta 1531 and 1550, visible via the command **show processes cpu**, did not properly add up to 100 percent.

This section highlights the Switch specific bug fixes in products running AOS version R11.10.0.

- Sending jumbo frames to a NetVanta 1531 or NetVanta 1550 through a switchport configured with port-security caused the switches to become unresponsive until the jumbo frame traffic was removed.
- In R11.9.0, link LEDs on NetVanta 1531s did not change status after the switch was booted, although the switchports still functioned properly.
- If the VCID was changed on a line card in an ActivChassis stack, and the master was not rebooted afterward, configuration changes that would effect the previous VCID caused the master to reboot.
- Management traffic between line cards in an ActivChassis was given higher priority over other traffic. Without this added priority, certain types of traffic, when sent at high throughput rates, caused line cards to lose connectivity to the master. In certain cases, this caused a reboot of the ActivChassis master and backup switches.
- In rare cases, clearing a single dynamic MAC address entry using the **clear mac address-table dynamic address** <*MAC*> command caused the switch to become unresponsive and require a reboot.
- In rare cases, an ActivChassis could get into a state where some traffic would be routed via the CPU (rather than Layer 3 switched), which resulted in latency for that traffic.
- Hardware ACLs could not be used to block traffic destined for the management interface of a NetVanta 1638.

Errata

The following is a list of errata that still exist in all products running AOS version R11.10.5.

- The Verizon Novatel USB 551L USB LTE modem is not recognized by the NetVanta 3140.
- Making any changes in the GUI for an Ethernet interface configured for DHCP causes the DHCP client to perform a DHCP release/renew on that interface when the changes are applied.
- A few legacy cellular interface commands were incorrectly removed when USB LTE support was added. The removed commands include:

  snmp trap cellular

  snmp trap link-status

  snmp trap threshold-ecio

  snmp trap threshold-rssi
- When using the Novatel USB 551L modem with a NetVanta 3140, a small number of lost frames will occur with packets smaller than 512 bytes. The loss occurs in the modem and not the NetVanta 3140.
- Assigning the IP address 192.168.190.1 to a NetVanta 160 AP from an AOS controller prevents the AP from pulling a full configuration from the controller.
- On the NetVanta 6410, HTTP file transfers to the unit's flash memory can be up to 10 times slower than TFTP.
- If a track is configured to monitor the line protocol of an interface configured for 802.1q, the track will never go into a passing state even the interface is up. This issue does not affect the NetVanta 4660, 5660, or 6360. **Workaround:** Track the line protocol of the subinterface.

- In some command sets, the **exit** command is not visible even though it still functions properly.
- On the NetVanta 5305, VPN performance for 64 and 256 byte packets decreased moderately compared to R11.2.0.
- Speed and duplex settings are displayed with on MEF Ethernet interfaces in **show running-config verbose** command output, even though those options are not valid and cannot be configured for that type of interface.
- In the VQM RTP Monitoring menu, the refresh button refreshes the displayed graphic, but it also duplicates information in the lower part of the menu. In addition, when the cursor hovers over a data point, multiple instances of the same data display.
- In the VQM RTP Monitoring menu, the Source IPs and Interfaces menus have invisible data points that appear and display data when the cursor hovers over them. The invisible data point information duplicates a visible data point and can usually be found hidden above the visible data point.
- On the NetVanta 3430, the setup wizard in the GUI can freeze with a **Please Wait** message.
- The output of **show qos map interface** <*interface*> shows **ce-vlan-id** instead of **vlan-id** and **ce-vlan-pri** instead of **cos** on products other than the NetVanta 4660.
- On the NetVanta 6240, SNMP traps for warm start and cold start are reversed.
- On a NetVanta 4430, information for an inserted SFP does not display correctly.
- Ethernet interfaces in third generation Total Access 900e units are not visible in the Data > IP Interfaces GUI menu. These interfaces are visible and can be configured from the System > Physical Interfaces menu instead.
- The Total Access 900e (third generation) and NetVanta 6250 send a cold start SNMP trap on reload instead of a warm start trap.
- On very rare occasions, port T1 3/3 on an Octal T1 NIM can stop negotiating LCP when it is part of an MLPPP bundle. Rebooting the device will restore the interface.
- On the NetVanta 6310 or 6330, if a SHDSL circuit with a detected bad splice retrains to a different line rate, the distance of the bad splice will display incorrectly.
- On the NetVanta 6310 or 6330, if the top level ATM interface on a SHDSL ATM NIM2 module is disabled and re-enabled, the ATM circuit will no longer be able to pass traffic. The ADTRAN unit must be rebooted to correct the problem.
- When using a T1/E1 EFM NIM2 in the NetVanta 6310 or 6330, the EFM counters do not increment as traffic passes through the device.
- Removing a USB modem from the USB NIM while active could cause the AOS device to reboot. Shutting down the demand interface being used by the modem prior to removing the modem will prevent this reboot.
- Event messages indicating a firmware upgrade was attempted may appear in the AOS event log for NetVanta 160 APs that are not being upgraded.
- Having more than two entries in a Network Monitor ICMP probe test list will display **Tracked by: Nothing** in the **show probe** command output. This is merely a display error; the probes still function correctly.
- Accessing the GUI via HTTPS may be slow.
- VQM may show a loopback interface in the GUI when a loopback interface is not configured.
- The **called-number** command on a demand interface does not function properly.

- When using XAUTH with a VPN client, an AOS device requests CHAP authentication from the client but does not send a CHAP challenge payload. This can cause issues with VPN clients that expect to receive this payload.
- If a USB modem is physically disconnected from a USB WWAN NIM while active NIM is active, the demand interface being used by the modem will not automatically shut down. The demand interface should be disabled before removing the modem to prevent this issue.
- On the NetVanta 6310/6330, with FFE enabled, passing traffic from the Ethernet 0/1 interface out an Ethernet NIM2 can cause the Ethernet 0/1 interface to fail. The interface is recovered with a reboot. Disabling FFE on the Ethernet 0/1 interface prevents the issue.
- The **vap-reference** command will not replicate VLAN IDs for an AP unless 802.1q encapsulation has been manually enabled on the AP expecting to receive the replicated configuration.
- Updating PRL values on a Sprint NetVanta 3G NIM may not function properly.
- A NetVanta 5305 can stop passing traffic for brief intervals when negotiating frequent VPN tunnels using Diffie Hellman Group 5.
- EAP Identity Responses from a wireless client that do not contain an Identity field can result in the NetVanta 150 creating a malformed RADIUS packet.
- NetVanta 150s may not properly handle immediate Access-Accept responses to Access-Request messages.
- The name of a deleted IPv4 ACL cannot be used to name a new IPv6 ACL.
- When a switchport on a NetVanta 3458 is configured for **port-security**, it does not receive BPDUs. If multiple connections between the NetVanta 3458 and another switch are made, a switching loop could occur because both ports will automatically enter a forwarding state even though the Spanning Tree protocol should cause one port to enter a blocking state.
- The output of the command **show ethernet cfm mep loca**l may display an incorrect maintenance association for a MEP ID if multiple maintenance associations are configured on the unit.
- The NetVanta 6240 should send warm_start SNMP traps when the unit is told to reboot by software. It should only send cold_start traps when the power is cycled. Instead, it is sending cold_start traps, even when reloaded by software.

The following is a list of Carrier Ethernet specific errata that exist in products running AOS version R11.10.5.

- The **efm-group** interface type option is missing from the **tunnel source** command on tunnel interfaces.

The following is a list of Voice specific errata that exist in products running AOS version R11.10.5.

- Enabling the SIP stack on a device allocates numerous resources. If this resource allocation fails, the device will reboot. Multiple sockets must be available and local SIP ports, typically UDP and TCP 5060, must be available as well, otherwise the resource allocation will fail and the device will reboot.
- TLS negotiation will fail when using ECDSA ciphers for SIP TLS.
- When using the SIP proxy with media anchoring, VQM reports incorrect information for LocalURI, RemoteURI, and LocalCaller if a reINVITE that modifies the SDP is received from the called party during a call.
- Issuing the command **clear voice call active** with active MGCP calls may result in a reboot.

- If **sip tls** is configured while **sip** is disabled, **no sip tls** must be issued before **sip** can be enabled, otherwise the following error will be displayed: %Error: Failed to modify SIP Access-class with new VRF.
- If a CA profile is removed while SIP TLS calls using that profile are active, BYE messages will not be sent for any of the active calls.
- The ERL tool is not functional on the NetVanta 6360.
- On the NetVanta 6360, if the onboard FXO port is configured to receive digits, a 500 ms delay is required after answering before receiving the first DTMF digit.
- Receiving an initial INVITE with both audio and T.38 SDP will result in the call being placed on hold.
- In AOS R10.4.0 and higher, modem-passthrough will fail to send a reINVITE to G.711 if the endpoint is configured with a codec-list that doesn't contain G.711.
- The command **ip mgcp qos dscp** <*value*> will not take effect until either **ip mgcp** is disabled and then re-enabled or the AOS device is reset.
- When the SIP server monitor clears the primary SIP server from a delayed state due to a failure of the secondary SIP server, there will be a 60-second delay until a SIP registration is attempted to the primary SIP server. This delay will not occur if the SIP server monitor is clearing the secondary SIP server from a delayed state due to a failure of the primary SIP server.
- On the Total Access 900e (third generation) and NetVanta 6250, SIP must be enabled in the running configuration whenever MGCP is used for voice.
- If an ADTRAN unit is configured with single call appearance mode, forwarded calls on a PRI trunk will fail.
- When using media anchoring, receiving a 183 Session Progress after a previous 183 on hairpinned calls can result in no early media if the SDP in the second 183 differs from the first.
- Echo cancellation is not enabled on three-way calls when using the local conferencing feature.
- On NetVanta 644 and NetVanta 6240 Series units, V.21 messages will sound overly amplified when listening to the TX output of a T.38 DSP capture. This is a flaw of the capture utility and does not represent how the audio actually sounds.
- DSP captures on the NetVanta 6240 and 644 platforms consume large amounts of memory while in progress. The unit could become unstable if a DSP capture is active for an unusually long period of time.
- With the ADTRAN unit set for **voice flashhook mode transparent**, the conference originator must wait for the third-party to answer before executing the flashhook to initiate the conference.
- On the NetVanta 6240 Series, over an extended period of use, T.38 calls can cause DSP channels to cease producing a dial tone and have poor voice quality. Rebooting the unit will correct the problem.
- NetVanta 6240 only: While running 29 or more simultaneous calls using E&M Immediate, Wink, or Feature Group D, it is possible to get in a state where DTMF tone detection will not function on any outbound (DSX to SIP) call using DSP 0/1.15 or higher. While in this failed state, all calls will continue to function in either call direction on DSP 0/2, as well as all calls on DSP0/1 in the inbound direction. With a load of 28 or fewer calls, all calls will function reliably in both directions on both DSPs. No consistent work around has been identified at this time. A unit reboot will typically solve the problem.
- The NetVanta 6240 Series IP business gateways can reboot if 60 simultaneous calls are placed through the DSP.
- The Total Access 900e Series (second generation) cannot properly handle more than 40 simultaneous E&M RBS calls. More than 40 simultaneously active calls could result in no dial tone or no audio on the last 8 channels.

- On the NetVanta 6310/6330 Series, if a SIP trunk is trying to register a large number of users and the registration fails, activating **debug sip trunk-registration** will cause the Telnet and console connection to become unresponsive. A reboot clears the condition.

The following is a list of Switch specific errata that exist in products running AOS version R11.10.5.

- On a NetVanta 1544F, a switchport interface with a connected SFP interconnect cable cannot be shut down properly.
- The idle process on a NetVanta 1638, visible with the command **show processes cpu**, is named **procnto-600-,** rather than **Idle**, like other AOS platforms.
- Certain NetVanta PoE switches require the command **power inline 2-point** be configured on applicable switchports in order to power Polycom VVX phones with three attached color expansion modules.
- In an ActivChassis configuration utilizing port channels that are distributed among individual line cards, if more than 1 Gbps is sent across the port channel the ActivChassis will sometimes discard some traffic.
- Traffic destined for devices that match static ARP entries in a Layer 3 switch will experience extra latency if a static MAC entry is not present for the same device.
- ICMP responses from a VLAN interface on the NetVanta 1531 may be periodically latent. ICMP routed or switched through the unit is not affected.
- When running R11.1.0 boot ROM on a NetVanta 1531 and attempting to apply a backup firmware image from bootstrap, the switch will print out benign errors indicating packets are being dropped due to congestion.
- Creating a hardware ACL with the same name as a previously created and deleted IP ACL will result in the creation of an IP ACL with an implicit permit.
- Removing port channels from the configuration while an ActivChassis is under a heavy load could cause the ActivChassis to reboot.
- On NetVanta 1638s in ActivChassis mode, spanning tree will reconverge at non-rapid spanning tree rates (about 30 seconds) if there are spanning tree topology changes in the network.
- If an ActivChassis line card has NetVanta APs physically attached, and the line card is removed and added back to the ActivChassis stack, the NetVanta APs will not properly indicate the AC that controls them. Bouncing the switchport on the line card or rebooting the ActivChassis master will resolve this issue.
- Certain OIDs in the Bridge-MIB may not return a value on AOS switches.
- Port mirroring on a NetVanta 123x (second and third generation) 1534, and 1544 cannot send transmit mirrored frames without a VLAN tag.

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.

