RELEASE NOTES

AOS Converged Access
AOS version R12.1.0
July 29, 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 R12.1.0 is a major system release that adds new features and addresses customer issues that were uncovered in previous code releases.

This release is generally available code. Results obtained during internal testing have been evaluated and the code has been determined to be ready for general availability. Caveats discovered during testing but not addressed in this build are listed in *Errata on page 9*.

A list of new or updated documents for this release appears in *Documentation Updates on page 13*.

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 R12.1.0. 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

Platform	Standard Feature Pack	Enhanced Feature Pack	SBC Feature Pack	Minimum Boot ROM
NetVanta 3430 (2nd Gen.)	√	√	√	17.05.01.00
NetVanta 3448	√	√	√	13.03.SB
NetVanta 3450	√	√		17.06.01.00
NetVanta 3458	√	√		17.06.01.00
NetVanta 4305 (2nd Gen.)	√	√		08.01.00
NetVanta 4430	√	√	√	17.04.01.00
NetVanta 4660		√	√	R10.10.0.B5
NetVanta 5305	√	√		11.03.00
NetVanta 5660		√	√	R11.4.1.B2
NetVanta 6240		√	√	A5.01.00
NetVanta 6250		√	√	R10.9.0
NetVanta 6310/6330		√	√	A3.01.B2
NetVanta 6355		√	√	14.06.00
NetVanta 6360		√	√	R11.2.0
NetVanta 6410			√	R11.3.0
Total Access 900 Series (2nd Gen.)		√		14.04.00
Total Access 900e Series (2nd Gen.)		√	√	14.05.00.SA
Total Access 900e Series (3rd Gen.)		√	√	R10.9.0

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 R12.1.0 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 R12.1.0 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 R12.1.0.

- Added the ability to search the CLI for commands matching a specified pattern.

There are no Carrier Ethernet specific features, commands, or behavioral changes in AOS version R12.1.0.

This section highlights Voice specific features, commands, or behavioral changes in AOS version R12.1.0.

- Added support for the following to HMR:

  Call variables were added to allow the user to store data to and retrieve it from named variables in the same manner as is currently allowed with private and public HMR variables. However, the variables are scoped by the Call-ID from the SIP messages allowing per-call data to be stored. Additionally, for calls through the B2BUA, variables from one side of the call can be accessed by the other call leg.

  The new match function is a string function that allows the user to perform regular expression matching/substitution on a string expression.

  The new **renumber** CLI command was added to allow the user to automatically renumber message rules. This is primarily intended to allow the user to easily edit existing message rules.

This section highlights Switch specific features, commands, or behavioral changes in AOS version R12.1.0.

- The maximum number of static routes was increased to 32 and the maximum number of ARP entries to 1000 on the NetVanta 1550.

Fixes

This section highlights major bug fixes for all products running AOS version R12.1.0.

- 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.
- If the NTP server was under heavy load, a reboot could occur.
- In rare cases, a reboot occurred when the **show bgp ipv4 community-list** command was issued.
- The **http source-interface** command was missing from the NetVanta 4660, 5660, and 6360.

- 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 an configuration change that updated the CPU MAC address filter was made (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 through 13000.
- 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 using the GUI on a NetVanta 3140 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.
- /32 routes from loopback interfaces were always advertised by RIP even when **redistribute connected** was not configured.
- 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.
- The command **snmp trap link-status** was improperly enabled by default on Frame Relay subinterfaces.

This section highlights Carrier Ethernet specific bug fixes in AOS version R12.1.0.

- The **bonding** command set was missing from EFM group interfaces on the NetVanta 5660.
- 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 the **show interface gigabit-ethernet 0/x performance-statistic**s command was inaccurate.

This section highlights the Voice specific bug fixes in products running AOS version R12.1.0.

- The default value for the **early-cut-through** option on ISDN voice trunks was not set properly at boot.

- 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 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
- If an INVITE with a Replaces header was received while a call was still connecting, a reboot could occur.
- When the **clear sip resources** command was issued, the **max used** count for **CallLeg transcLists** was not cleared.
- 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.
- 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.
- 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.

This section highlights Switch specific bug fixes in AOS version R12.1.0.

- Port channel failover did not function properly on the NetVanta 1550-48 and 1550-48P.
- In R11.13.0, some configuration commands on port channels were silently discarded.
- 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.
- The factory default IP address of 10.10.10.1 was not reachable if the switch had not obtained an IP address via DHCP.
- In NetVanta 1638 ActivChassis applications, AWCP frames were throttled, which caused errors and prevented firmware upgrades on NetVanta 150 and 160 Series access points.
- 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.

Errata

The following is a list of errata that still exist in all products running AOS version R12.1.0.

- When using the firewall with policy-based routing (PBR) and WAN failover, changes to the next hop specified in a route map are not applied properly after the primary connection fails if **ip firewall fast-allow-failover** is not configured.
- The GUI accepts spaces in the text boxes for RADIUS and TACACS+ server hosts, which allows an invalid configuration to be applied.
- 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 on Total Access 900e (third generation) 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 R12.1.0.

- 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 R12.1.0**.**

- If an offered media stream from SDP is rejected, memory is leaked, which results in a reboot over time.
- 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 will report incorrect information for LocalURI, RemoteURI, and LocalCaller if a reINVITE that modifies the SDP is received from the callee 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.
- 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.
- 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 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.
- 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 R12.1.0.

- 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.

Documentation Updates

The following documents were updated or newly released for AOS version R12.1.0 or later. 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*

