AOS 17.08.01.00 Release Notes

Release Notes **Release Date: May 10, 2010** **Notes Revision: May 11, 2010**

Introduction

NetVanta Series products support application image updates via the ADTRAN OS Web GUI, TFTP, X-Modem, and FTP. A detailed firmware upgrade guide with step-by-step instructions is available at: http://kb.adtran.com/article.asp?article=1630&p=2.
Prior to upgrading firmware, please ensure that your unit meets the minimum Boot ROM requirements, listed under "Supported Platforms."

Supported Platforms

	Standard Feature Pack	Enhanced Feature Pack	Minimum Boot ROM****
NetVanta 1234/1238	9700594-2A170801.biz	N/A	17.03.02.SB
NetVanta 1534	9700590-2A170801.biz	N/A	17.03.01.00
NetVanta 1534 2nd Gen.	9702590-2A170801.biz	N/A	17.08.01.00
NetVanta 1544/1544F	9700544-2A170801.biz	N/A	17.05.01.00
NetVanta 1544 2nd Gen.	9702544-2A170801.biz	N/A	17.08.01.00
NetVanta 1335	N/A	9950515-2A170801.biz	15.01.00
NetVanta 3120	N/A	9700600-2A170801.biz	14.04.00
NetVanta 3130	N/A	9700610-2A170801.biz	14.04.00
NetVanta 3200/3205 (3rd Gen.)*	9200860-2A170801.biz	9950860-2A170801.biz	17.02.01.00
NetVanta 3305	9200880-2A170801.biz	9950880-2A170801.biz	04.02.00
NetVanta 3430	9200820-2A170801.biz	9950820-2A170801.biz	13.03.SB
NetVanta 3430 2nd Gen.	9202820-2A170801.biz	9952820-2A170801.biz	17.05.01.00
NetVanta 3448	9200821-2A170801.biz	9950821-2A170801.biz	13.03.SB
NetVanta 3450	9200823-2A170801.biz	9950823-2A170801.biz	17.06.01.00
NetVanta 3458	9200824-2A170801.biz	9950824-2A170801.biz	17.06.01.00
NetVanta 4305* **	9200890-2A170801.biz	9950890-2A170801.biz	08.01.00
NetVanta 4430	9700630-2A170801.biz	9950630-2A170801.biz	17.04.01.00
NetVanta 5305	9200990-1A170801.biz	9950990-1A170801.biz	11.03.00

*1st generation NetVanta 3200/3205 routers (part numbers beginning '1200') and 2nd generation NetVanta 3200/3205 routers (part numbers beginning '1202') cannot run this version of AOS.
**1st generation NetVanta 3305 (Part number 1200880L1) cannot run this version of AOS.
***1st generation NetVanta 4305 (Part number 1200890L1) cannot run this version of AOS.
****To confirm the version of Boot ROM, telnet or console to the unit and issue the **show version** command. 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.

New Features	Overview
Microsoft® Desktop Auditing (NAP)	This AOS feature uses DHCP in conjunction with Microsoft® Network Access Protection Protocol (NAP) to monitor the health of client computers connected to an AOS network. When desktop auditing is enabled, the AOS device will collect NAP information by monitoring the DHCP messages between the client and server. The AOS device can also function as the DHCP server in the network where, on a per DHCP pool basis, it can act as the NAP server so that clients can then respond to the AOS device with its NAP information. ***Supported Platforms*** **NetVanta 1534 (1st and 2nd Gen) & NetVanta 1544 (1st and 2nd Gen)**
DHCP Network Forensics	This AOS feature uses DHCP to collect information about the network in which the AOS device resides. By passively monitoring DHCP requests from the clients, the AOS device is able to gather information about clients connected to the AOS device and provides information about them, such as Client MAC address, Client IP address, Client VLAN ID, location in the network, etc. ***Supported Platforms*** **NetVanta 1534 (1st and 2nd Gen) & NetVanta 1544 (1st and 2nd Gen)**
USB WWAN NIM	This USB wireless WAN network interface module works with AOS to provide support for USB cellular modems obtained from a service provider. The USB WWAN NIM will allow for an alternative method for providing primary or backup wide area network connections, utilizing cellular 3G networks. ***Supported Platforms*** **NetVanta 1335, NetVanta 3200/3205, NetVanta 3305, NetVanta 3430/3448, NetVanta 3450/3458, NetVanta 4305, NetVanta 4430**
2nd Generation Dual T1 NIM	The 2nd generation dual T1 NIM provides two T1/FT1 interfaces that have the added capability of being clocked independently of one another. ***Supported Platforms*** **NetVanta 1335, NetVanta 3200/3205, NetVanta 3305, NetVanta 3430/3448, NetVanta 3450/3458, NetVanta 4305, NetVanta 4430**

Enhancements	Overview
Mobile IP User Profile - Web GUI Support	This adjustable setting will allow users to modify the user profile settings for 3G NIMs so that they can support private network connections over the EV+DO networks. This feature is now configurable through the web GUI. ***Supported Platforms*** **All platforms that support the 3G NIM**

Errata

These are issues that were discovered during internal testing, but were unresolved at the time of release.

- In the Web GUI, when stacking is configured on an AOS device, the stack master IP address may show up in the 'IP Interfaces' page or the 'Connectivity' page as 'ClusterInternal'. If this link is clicked, an error will be returned to the user.
    - Workaround: Do not click the 'ClusterInternal' IP.

- The NetVanta 1544F may not be able to pass traffic through links which are negotiated to half-duplex.
    - Workaround: No known workaround.

- Setting "qos trust cos" on a port-channel will function, but is not visible in the configuration.
    - Workaround: No known workaround. Display issue.

- When configuring port security with static MAC address entries, a NetVanta device may also learn and allow traffic from a dynamic MAC address not statically specified in the configuration.
    - Workaround: No known workaround.

- When uploading firmware via the Web GUI, the firmware will be uploaded and applied correctly, but may output a false error message stating, 'Error setting Primary Firmware. Firmware image successfully set – Please reboot for changes to take effect.'
    - Workaround: Display error only, no functional impact. Ignore the error.

- The output of the "show desktop-auditing dhcp brief" command may display false information.
    - Workaround: Use the "show desktop-auditing dhcp" command.

- When creating a DHCP pool, Microsoft Desktop Auditing (NAP) is enabled by default.
    - Workaround: Manually disable Microsoft Desktop Auditing (NAP).

- On a NetVanta 5305, if "ip ffe" is enabled on the PPP interface, issuing the command, "no ip address", may cause a reboot.
    - Workaround: Disable "ip ffe" prior to removing the IP address from the PPP interface.

- Even though the RAMdisk feature is not supported by the 2nd Gen. 1544, the commands may show up as valid commands in the CLI.
    - Workaround: RAMdisk feature is not supported.

- When using Network Forensics, a manual release on the client may not clear the DHCP information on the NetVanta device.
    - Workaround: No known workaround.

- When using Microsoft Desktop Auditing, releasing and renewing the IP address on a client may not cause the NetVanta device to properly read the NAP information correctly from the new DHCP request.
    - Workaround: Release and renew the client's IP address again.

- A hub connected to a NetVanta switch, may not be detected as a 'shared link' and may cause a packet storm to occur if there are multiple links between the switch network and the hub. This can eventually lead to a reboot of the NetVanta Switch.
    - Workaround: Do not use a hub to interconnect multiple switches.

- Configuring a 1st or 2nd Gen NetVanta 1544 or a 1st Gen 1534 as the stack master in the Web GUI may cause a reboot.
    - Workaround: Configure using the CLI.

- When using 802.1x MAC-based port authentication, the NetVanta device may not initiate an EAP-request when the link comes up.
    - Workaround: Have the supplicant initiate the session.

- If a switchport of an AOS device is set to trunk mode, attempting to run the 'Setup Wizard' may cause it to hang on the 'System Info' page.
    - Workaround: Configure using the GUI, outside of the Setup Wizard, or CLI.

- Stacking candidates may fail to create a Stack VLAN interface even when the Stack Master is known and the Stacking VLAN has been created.
    - Workaround: Do not use stacking.

- Removing and then re-adding a PPP cross-connect to a SHDSL interface may cause PPP not to come up.
    - Workaround: Bounce the SHDSL interface.

- The CLI may not allow ECIO threshold traps and RSSI threshold traps to be disabled on a cellular interface.
    - Workaround: No known workaround.

- On the NetVanta 5305, the clock may show the incorrect time and the output of "show version" may show the incorrect uptime.
    - Workaround – No known workaround. Display issue.

- SNMP traps generated by a NetVanta 1544 2nd Gen switch, may report a 'warm start' (soft reboot) as a 'cold start' (power cycle).
    - Workaround – No known workaround.

- Changing Radius or TACACS+ server settings in the Web GUI may cause the tabs under 'Service Authentication' on the 'Passwords' webpage to disappear.
    - Workaround – Make Radius and TACACS+ changes in the CLI.

- Issuing the "no ip address <IP address> <Subnet Mask> secondary" command or the "no ip address range <IP address> <Subnet Mask> secondary" may not remove the secondary IP address if there is more than one secondary IP address on an interface.
    - Workaround – Remove the secondary IP addresses by modifying the startup-config file and uploading to AOS device.

- In the Web GUI, a static MAC entry may appear not to be removed from the MAC address table when deleted.
    - Workaround – Refresh the webpage.

- In the Web GUI, under Network Monitoring, setting a Probe and a Schedule as test objects for a Track may output in an incorrect error, 'You must enter Probe 2.'
    - Workaround – Configure Network Monitoring in the CLI.

- In the Web GUI, changing a port's membership from a Vlan to "Stack" will be applied, but may output an incorrect error message stating, 'ERROR: Could not set switchport mode.'
    - Workaround – Display issue, error message can be ignored.

- In the Web GUI, a schedule may show as inactive when it is, in fact, active.
    - Workaround – No known workaround. Display issue.

- Executing the "show desktop-auditing dhcp interface <interface>" command, may return an error.
    - Workaround – Use the "show desktop auditing dhcp" command and view all interfaces.

- A topology change may cause the stacking VLAN interface to not come back up after going into a down state.
    - Workaround – No known workaround.

- Issuing the “show desktop-auditing dhcp” command may show ‘Unknown’ for the ‘Client Automatic Updates’ state for a Vista NAP-enabled client.
    - Workaround – No known workaround.

- If a PPP interface is deleted via the CLI and it is cross-connected to an Ethernet port, the AOS device may reboot.
    - Workaround – Delete the cross-connect before deleting the PPP interface or delete the PPP interface in the Web GUI.

- In the Web GUI, the ‘Port-Mirroring’ webpage will not allow the selection of a destination port.
    - Workaround – Configure port-mirroring in the CLI.

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.07.02)

Services and Viewers

- Executing multiple successive SNMP walks on a NetVanta device may cause a reboot.
- NetVanta 3120s, 3130s, and 3rd Gen 3200s/3205s may be unable to upgrade their firmware using N-Command Enterprise Edition.
- The auto-link client may incorrectly utilize a secondary IP address rather than the primary IP of the interface when registering to N-Command MSP.
- When using the DBU daughterboard and a DIM holder module, the DBU LED may not light up when a dial-backup connection is up.
- Using the up/down arrows keys within the CLI under specific circumstances may cause the AOS device to reboot.
- Certain configurations may cause a NetVanta device's CLI to appear to lock-up when show commands are issued and the terminal length is set to a value higher than 0.
- The "System Summary" page in the GUI can return a 503 server error if the unit is unable to retrieve LLDP information from the neighbor.
- The L3 Switching "Enabled" checkbox in the Web GUI of the NetVanta 1335 is permanently grayed out under the VLAN interface page, thus not allowing the user to enable this feature from the Web GUI.
- The Wireless wizard may not be able to setup a new Access Point if an interface named 'dot11ap 24' already exists.
- The Web GUI may not allow TDM groups with different channel specifications to be added to the same multilink PPP interface.
- The "Specified Port" field under the "UDP Forward Protocol" section of the UDP Relay page in the GUI does not allow more than 3 characters to be entered, prohibiting ports with more than 3 characters from being forwarded.
- The command, 'ip rtp firewall-traversal policy-timeout x', will properly accept the configured timeout value, but may display 'no ip rtp firewall-traversal policy-timeout' when a 'show run' command is issued.
- Gigabit-ethernet switchports may show the SFP media type as "Small Form-factor Pluggable" when copper connections are used.
- In the Web GUI, placing switchports into "auto" or "mac-based" authentication mode may cause a 503 server error.
- In the Web GUI, viewing the VPN configuration page for a remote-ID that contains special characters may cause a 503 server error.
- Initiating an SNMP GET on a VLAN interface may return an invalid number of discards.
- LLDP commands configured by default can randomly appear in a 'show run' output.
- The command 'power inline 2-point' may not be displayed as an option under the help text until it is fully typed out. Once the command is applied, it functions as expected.
- LLDP may not properly advertise a link's speed and duplex when operating at 2.5 Gbps. This is merely a cosmetic error, and has no functional impact.

- When utilizing an external WebSense server, DNS queries held in the buffer may be lost awaiting a reply. This adds a few seconds of delay to each new session created.
- Running a port mirror for long periods of time while switchport link changes are occurring, may cause the port mirror to stop functioning until the destination port is moved to another switchport, or the switch is rebooted.

Routing, Switching and Bridging

- When using the 'summary-address' command in OSPF, the router may still transmit an additional route of a subnet that should be included in the summary route. This causes no routing problems, and only adds an unnecessary route to the route table.
- Constant changes to the MAC or ARP table may cause packets to be delayed or dropped, when Layer 3 switched through the NetVanta 1544 (1st Gen).
- IGMP Snooping feature may cause a memory leak, eventually resulting in a reboot.
- With IGMP snooping enabled, a NetVanta 1335 may reboot upon receiving a membership query.
- Multicast traffic addressed to 224.0.1.16/28 may cause some units to stop or transmitting and receiving on the Ethernet port of the NetVanta.
- Enabling IGMP snooping on a specific VLAN interface may cause the NetVanta switch to reboot.
- Certain AOS devices acting as a wireless Access Controller may reboot when a WiFi client disassociates from an attached AP.
- When an inbound route map is applied to a BGP neighbor that filters based on a match community list statement, learned prefixes that do not include a standard community string may incorrectly be deemed invalid, preventing them from being exported to the route table.
- UDP relay can insert a bad ARP entry into the ARP table which can cause the VLAN interface to stop responding.
- Under high traffic load, with processor load above 80%, ARP entries may stop being updated until the box is reloaded. During this time, a "show arp" will yield entries with TTL of 0.

Network Interfaces and Quality of Service

- If 'ip ffe' is enabled on a PPP interface, and PPP changes states while data is flowing through the interface, the router may reboot.
- Packets fragmented by FRF 12 do not preserve the protocol type. This may cause adverse effects when attempting to classify traffic for QoS.
- PAP/CHAP encrypted passwords may not be retained in the configuration after a reboot.
- When utilizing 4 wire mode (standard or enhanced) on a SHDSL NIM, the second loop may fail to complete training.
- When using a Sprint 3G NIM, the log message, "OTASP Initial programming required," may appear even though OTASP programming is only required for the Verizon 3G NIM.
- Enabling multilink PPP fragmentation may cause a minute amount of packet loss if small packets arrive at a slow interval.
- Ethernet interfaces may not transition into the "Test" state when looped.

Firewall and VPN

- After a VPN tunnel times out, the tunnels may be unable to reestablish, outputting an error stating the upper watermark has been reached, even if no tunnels are up.
- SIP Transparent Proxy may block SIP messages that contain an extra "/" at the end of the "Content-Type" field.

AOS 17.08.02.00 Release Notes

Release Notes **Release Date: July 6, 2010** **Notes Revision: July 6, 2010**

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.08.01.00)

Deleting a route on a NetVanta 1544 may cause any routing additions that occur afterwards to be software routed instead of being Layer 3 switched.

Modifying a route-map that is used on an interface where FFE is enabled and is attempting to update may cause the NetVanta device to reboot.

If traffic traversing a NetVanta device is using gigabit-ethernet interfaces, a Netflow packet may mark the input and output interfaces as "0" instead of its correct IfIndex number.

Excessive unresolved ARP entries on the NetVanta 1544 may cause it to reboot.

Configuring BVI interfaces for "ip unnumbered" before configuring the logical interfaces that will participate in the BVI interface may cause those logical interfaces to lose their configuration upon a reboot.

In the GUI, adding a sub-interface on a NetVanta router with 802.1q encapsulation enabled may cause a lock up.

Policy timeout values for port 443 (HTTPS) may be lost after a reboot.

The output of a 'show qos map interface <interface>' may not report any packets matched, even though packets are being matched and prioritized appropriately.

ARP table entries may not properly be refreshed after half of their TTL has elapsed, potentially leading to a small number of dropped packets while the entry is being updated.

Switchports that are part of a port-channel may remain in a suspended state after going down and then coming back up, causing traffic to be incorrectly directed through the port-channel.

Disabling DoS protection against threat ID 6 (TCP SYNs with a source port less than 1024) may not take effect until the NetVanta device is rebooted.

Issuing the SNTP server 'source-interface' command may not properly source the SNTP packet from the specified interface's source IP address.

SIP Transparent Proxy may not release RTP ports when a call completes, possibly resulting in the inability of those RTP ports to be mapped for future calls.

The 'test if interface <interface>' command may be removed from the configuration after a reboot.

Configuring a 1st or 2nd Gen NetVanta 1544 or a 1st Gen 1534 as the stack master in the Web GUI may cause a reboot.

	If a switchport of an AOS device is set to trunk mode, attempting to run the ‘Setup Wizard’ may cause it to hang on the ‘System Info’ page.
	When the SIP Proxy is enabled, Bridged Line Appearance phone calls may not function properly.
	In a large Ethernet network, a NetVanta router may delete more ARP entries than expected, causing a perceived network outage for those users to whom the deleted ARP entries belong.
	With VRRP configured, the AOS device may respond to an ARP request with the incorrect MAC address after transitioning from VRRP master to VRRP backup.

AOS 17.08.03.00 Release Notes

Release Notes **Release Date: August 5, 2010** **Notes Revision: August 5, 2010**

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.08.02.00)

Secondary IP addresses may be unable to be removed from Ethernet sub-interfaces.

The Security Dashboard may incorrectly display the “Projected Average” of threat occurrences per day.

Security scanners (i.e. Nessus) may report an NTP DoS vulnerability within AOS.

The mail-client may not send an email notification if there are no capture commands configured and the body of that email is empty.

The ATM sub-interface may not retain its VPI/VCI settings when configured through the web GUI.

SMTP messages originating from an AOS device may be rejected by some mail servers.

The “no nap” command in the DHCP pool settings may intermittently be removed from the running-configuration.

An Ethernet interface with 802.1q encapsulation enabled may discard valid packets as giants.

The modem on a 3G NIM may not initialize if a T1 NIM is also installed.

In the web GUI, the troubleshooting page may incorrectly display an error when GRE tunnels are configured stating, "Warning: tunnel 1 has a private IP Address, but NAT is not enabled on its policy class."

An Annex B ADSL link may not be able to train up properly.

The count under ‘Packets’ when viewing Top Traffic Statistics may be displayed incorrectly.

A PPPoE link may take an excessive amount of time (several hours) to come up.

The AOS chassis may incorrectly recognize a Verizon 3G NIM as a Sprint 3G NIM when attempting to go through the activation process.

The local-user list may be deleted from the running-configuration when TACACS+ is configured in a certain manner.

The URL filter may improperly allocate memory causing the AOS device to reboot.

An AOS device may lose the command to track a gigabit-ethernet interface after a reboot.

On a 1544, ARP entries for multiple IP addresses that use the same MAC address may not properly be indexed for Layer 3 switching.

The AOS device may improperly handle a frame that is sourced from an all zeroes MAC address and potentially cause a reboot.

Desktop-auditing may inadvertently be enabled when the no desktop-auditing command is issued from within an interface

AOS 17.08.04.00 Release Notes

Release Notes	Release Date: November 29, 2010	Notes Revision: November 29, 2010

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.08.03.00)

The NTP hardware and software clock on an AOS device may drift resulting in event messages stating, “NTP frequency error -500 PPM exceeds tolerance of 500 PPM.”

The NetVanta 4305 may display an incorrect reset cause.

When AAA is enabled, the FTP server may be unable to authenticate users via the default AAA list.

Issuing the command "show tech" simultaneously from two separate sessions may cause the unit to lockup.

When downloading the configuration file from the web GUI, the AOS device may download the HTML script instead.

Certain encrypted packets by the Shrew VPN client may be dropped when the packet is decrypted.

The telnet client may function improperly when being sourced from non-default VRFs.

The cellular interface may be brought down due to short-term signal dropouts.

The switchport interface statistics may show an incorrect and very high number of unicasts.

An AOS device may reboot if an IGMP packet is received on a non-default VRF.

The web GUI of the NetVanta 4430 may accept a gigabit-ethernet as a next-hop even though the option is invalid.

The NetVanta 2nd Gen 1534 and 2nd Gen 1544 may reboot without an exception report or core dump message.

SNMP source interface may not source an SNMP packet from the specified IP address.

Removing a cross-connect for a PPPoE connection may cause a reboot.

Receiving an invalid DHCP packet may cause a reboot.

When configuring the ATM sub-interface through the GUI, when the interface mode is set to PPPoE, the GUI will redirect to the ATM configuration page instead of the PPP configuration page.

Loopback interfaces may not be populated in the Layer 3 hardware table.

The output of 'show ip policy-sessions' may not display all active GRE sessions.

When PPP fragmentation is enabled, fragments may traverse the same link instead of being transmitted equally between all the links.

Enabling email-logging may cause the AOS device to reboot.

Bridged frames across a PPP link with the "LAN FCS" bit set were given an extra CRC, which can cause an invalid packet to be transmitted and may result in errors.

A PPP interface may get stuck in loopback if the far end transmits LCP frames that do not include "magic numbers."

The DHCP server may incorrectly respond to a DHCP Request message from a client that it already gave an address to on a different interface.

The 123x switches may not honor static MAC address assignments.

On the 123x switches, if port security with sticky MAC addresses is used, the sticky MAC addresses may be removed after a certain period of time.

On a re-INVITE where both the remote IP and port number have changed, the SDP information is not properly processed by the SIP ALG, which may create an invalid policy session and result in one-way or no audio.