AOS 17.03.01.00 Release Notes

Release Notes **Release Date: August 4, 2008** **Notes Revision: 8/4/2008**

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	9200594-2A170301.biz	N/A	17.03.01
NetVanta 1238	9200598-2A170301.biz	N/A	17.03.01
NetVanta 1534	9200590-2A170301.biz	N/A	17.03.01
NetVanta 1335	N/A	9950515-2A170301.biz	
NetVanta 1524ST	N/A	9950560-2A170301.biz	
NetVanta 3120	N/A	9700600-2A170301.biz	14.04.00
NetVanta 3130	N/A	9700610-2A170301.biz	14.04.00
NetVanta 3200/3205 (3rd Gen.)*	9203860-2A170301.biz	9700860-2A170301.biz	17.02.01.00
NetVanta 3305**	9200880-2A170301.biz	9950880-2A170301.biz	04.02.00
NetVanta 3430	9200820-2A170301.biz	9950820-2A170301.biz	
NetVanta 3448	9200821-2A170301.biz	9950821-2A170301.biz	
NetVanta 4305	9200890-2A170301.biz	9950890-2A170301.biz	08.01.00
NetVanta 5305	9200990-1A170301.biz	9950990-1A170301.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.
*** 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
SIP Transparent Proxy with Survivability	ADTRAN developed its AOS Transparent Proxy feature by incorporating RFC 3261 compliant stateful SIP proxy functionality to provide a new way for AOS products to transport IP voice traffic. Using Transparent Proxy, the SIP proxy server allows AOS voice products to forward SIP messages between endpoints (phones and softswitches) without being required to interpret the messages as with back-to-back user agent (B2BUA) devices. When using Transparent Proxy, customers are not restricted to using ADTRAN-compatible (B2BUA) phone models. Unlike the B2BUA, the Transparent Proxy server

	is not feature dependent. As a result, adding new phone or softswitch features does not require corresponding features in the AOS product, or further configuration to support customer endpoints. Configuration is simplified because creating voice users, voice trunks, and dial plans is not required on the AOS product. In addition to increased interoperability, Transparent Proxy is switchboard independent and increases survivability options. ***Supported Platforms*** **NetVanta 1335, NetVanta 3100 Series, NetVanta 3200 Series, NetVanta 3305, NetVanta 3400 Series, NetVanta 4305, and NetVanta 5305**
TFTP directly to compact Flash	Provide the ability to TFTP to and from Compact Flash card. ***Supported Platforms*** **All AOS devices with Compact Flash,** NetVanta **1335,** NetVanta **3430,** NetVanta **3448**

Enhancements	Overview
Wireless Controller Support in NetVanta 1234, 1238, and 1534	The NetVanta 1234, 1238 and 1534 can also act as Wireless LAN Access Controllers through Adtran Wireless Control Protocol for NetVanta 150 Access Points. ***Supported Platforms*** **NetVanta 1234, NetVanta 1238 and NetVanta 1534**
DHCP Improvements	The AOS based DHCP server is now capable of sending up to four DNS server entries to DHCP clients. ***Supported Platforms*** **All Devices with DHCP functionality**
Voice Quality Monitoring Support on the 3rd Generation NetVanta 3200 Series	Voice Quality Monitoring was introduced in AOS in revision 17.1 but is now also available on the Third Generation NetVanta 3200 and NetVanta 3205. ***Supported Platforms*** **NetVanta 3200/3205**
VRRP Support on the 3rd Generation NetVanta 3200 Series	The Virtual Router Redundancy Protocol was introduced in AOS in revision 16.1 but is now also available on the Third Generation NetVanta 3200 and NetVanta 3205. ***Supported Platforms*** **NetVanta 3200/3205**

Errata

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

- The average CPU utilization on the NetVanta 123X series is higher than other NetVanta products.
  - Workaround – No known workaround.

- Boot code for the NetVanta 1534 and 123X series allows users to attempt to configure an IP address, as well as initiate TFTP firmware downloads, however neither of these actions is supported in current boot code. The CLI should not accept these commands rather than accepting them and then returning errors.
  - Workaround – N/A.

- Access to an AOS device's console may be lost after entering the command 'logging email receiver-ip' followed by a hostname, rather than an IP address.
  - Workaround – No known workaround.

- If a TFTP download is initiated from a CLI session, and that session is closed, administrative access is lost. Console, Telnet, SSH, and Web sessions are unsuccessful.
  - Workaround – Reboot the Unit.

- LEDs for ports on the NetVanta 1238 flicker a weak orange/green when they are not connected to anything. This only occurs when roughly half of the ports on the switch are currently connected.
  - Workaround – No known workaround.

- In the Web GUI, a WEP transmit key cannot be changed when the security mode includes MD5.
  - Workaround – Make change via the CLI.

- On the NetVanta 123X and 1534, traffic generated by the CPU is not detected via port mirroring. Users will be unable to see things like LLDP and Spanning Tree BPDUs.
  - Workaround – No known workaround.

- The distribution of bandwidth between flows within the same WRR queue on the NetVanta 123X and 1534 is not as even as it is in older switch products.
  - Workaround – No known workaround.

- The Save button in the Web GUI does not work with Firefox 3.
  - Workaround – Save via the CLI command “write” or use different web browser.

- SIP server failover does not work properly when SIP Transparent Proxy is enabled.
  - Workaround – No known workaround.

- Changing the speed to 10Mbps on the NetVanta 1238's gig ports causes the duplex to be set to half.
  - Workaround – Manually re-set duplex to Auto or Full.

- NetVanta 123X switches forward during boot-up, while their startup configurations are being applied and spanning tree is disabled. This can cause traffic storms.
  - Workaround – If Spanning-tree is disabled, boot unit before connecting devices.

- Shutting down a VLAN (note: not a VLAN interface) causes an invalid command to show in the running configuration.
  - Workaround - No known workaround.

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.02.03)

Services and Viewers

- In the Web GUI, checking and un-checking the interval statistics checkbox for SHDSL interfaces can cause the statistics to not display correctly.
- SSH sessions are listed as authentication in progress under the command 'show users' even when SSH users have authenticated and logged into the CLI.
- In the Web GUI, when a VPN is configured without VQM (therefore, making it stateless) and VQM is subsequently configured for the VPN, the private policy class is made stateful, but the public policy class is not.
- Entering a URL Filter server via the CLI without specifying a port and timeout, leads to these values being set to '0'. This is an invalid value for these options.
- The 'show modules' command does not show the ADSL application code version.
- It is possible for users to be given the unprivileged exec mode prompt (>) but still have access to enable mode commands if AAA is enabled. This occurs when a user is in enable mode, enters the command 'enable', and enters the incorrect enable password.
- Running the maximum number of TWAMP probes with the maximum number of packets and the minimum period between them can cause routers to lock up. A manual power cycle is required to recover.
- Issuing the command 'reload in' and subsequently entering the 'reload in' command again before the reboot causes units to reload in approximately half the expected time. For example, 'reload in 120' should cause units to reload in two hours, but if this had occurred, the reload would happen in one hour.
- Configuring a source interface for a NTP Server in the Web GUI does not always update the running configuration correctly.
- Storm control values cannot be configured in the Web GUI on the NetVanta 1524.
- The Web GUI Port Configuration page does not allow manual configuration of gigabit ports for 1000Mbps operation.
- On the Shape Class Traffic page of the Web GUI, if users input an invalid value for Average or Burst, the Wizard continues to the next page, but should stay on the Shape Class Traffic page.
- In the Web GUI, following the steps in the Getting Started page to configure bridging results in loss of IP connectivity to the unit.
- A burst value cannot be set for traffic shape rates on Ethernet and VLAN interfaces in the Web GUI.
- Using the Setup Wizard to configure a unit for Internet access after the unit has already had several interfaces configured leads to invalid configurations.
- If users go through the Setup Wizard more than once and specify a different Layer 2 WAN encapsulation the second time through, the wizard returns an error at the end. The original default route is not removed, which causes a conflict.
- The Setup Wizard does not apply the configured ATM PVC to the running configuration for ADSL interfaces. Regardless of what users put into the Setup Wizard, it applies a VPI/VCI of 8/35.
- The HTTP Request probe Web GUI page implies that a text string must be entered for all HTTP requests, but it is only required for HTTP Raw.
- When configuring a Demand interface via the Web, the number of connect-sequence attempts is put into the running configuration as 1082567232.
- The Demand Routing Web GUI pages reference Acl instead of ACL - this is inconsistent with other Web GUI pages.
- The Telnet client always uses source port 23, even if a different source is specified.
- When hovering over a bar in the Top Talkers graphs, the time interval displayed in the pop-up information bubble is not correct. This happens intermittently and appears to require a large number of stats before it occurs.
- Configuring QoS Map entries in the Web GUI, which each use bandwidth percentages, may cause an error message to be generated when the total percentage for the map is 100%. For example, if four classes were to be configured for 25% of the available bandwidth, the first three could be configured; the fourth would generate an error in the GUI.
- The T1 configuration page becomes sluggish when viewing the page for awhile. This can be alleviated by

disabling the refresh of statistics.

- If users make changes to the Public interface of a NetVanta 3120 by going to IP Interfaces / eth 0/1, the left-hand menu disappears. The only way to bring the menu back is to click the ADTRAN logo in the upper left-hand corner, or to otherwise navigate away from the Web GUI and back to it again.
- The formatting of input and output packet statistics for cellular interfaces in the Web GUI are inconsistent with those of other interfaces.
- Stub OSPF areas cannot be configured via the Web GUI.
- Area IDs that are formatted as IP addresses do not show up in the Web GUI OSPF page, under the 'Add an Area and Range' section.
- The Setup Wizard will not complete if users attempt to configure ATM Routed-Bridged Encapsulation (RBE).
- Upgrading the firmware on a 3G NIM that is installed in a 1335 causes the CLI session to the 1335 to lock up until the firmware upgrade is complete.
- DNS lookups are case-sensitive, which violates RFC 4343. For example, if an AOS device is configured as a DNS Proxy, has a host entry for www.adtran.com, and a client sends a DNS request for www.ADTRAN.com, the AOS device will query its name server instead of using the existing host entry.
- VPN Peer page does not correctly change the access-list entries for the VPN allow policy through the firewall, according to the checkbox in the GUI.
- The Web GUI does not clearly explain that TWAMP source ports of 0 refer to random source ports and not an actual port value of 0.
- The NetVanta 5305 System Summary web page does not show the System Temperature.
- When a security zone that includes VPN selectors is assigned to an interface it can not be changed in the Web GUI.
- The Web GUI returns an error when users attempt to add a secondary IP address to an interface that is configured as the IP unnumbered source of another interface.
- Message of the day (MOTD) banners have an extra line feed prepended to them upon boot-up. Therefore, if users frequently reboot units, then make changes, the MOTD can grow to be very long, with extra line feeds at the beginning.
- There is a memory leak that can lead to reboots when TACACS+ is invoked.

Routing, Switching and Bridging

- When a route uses a device's own IP address as a next-hop, traffic to the destination is passed up the device's IP stack. The device will respond to this traffic, although it should not. For example, if a router had the following in its configuration: ip route 9.9.9.9 /32 10.22.41.4 where 10.22.41.4 was a local IP address, the router would respond to pings to 9.9.9.9. This could give users a false impression that network connectivity existed. (Note: When configuring routers, users should not use a device's own IP address as a next-hop address.)
- Routers may reboot if Fast Cache is enabled with IP Load Sharing, and there is a large volume of route changes between parallel paths.

Network Interfaces and Quality of Service

- When a network interface has an IP address assigned to it, but it is shut down, a router may still keep its interface's network in the route table. When the interface is down, its network should not be in the route table.
- When 802.1q sub-interfaces are configured on the NetVanta 3448, the sub-interfaces are listed twice in the running configuration.
- Changing the Default-Cos on a Switchport interface does not result in the modification of the COS value of frames that enter that port and then exit a Dot1Q interface.
- Interfaces on the Octal T1 Module can get into a state where traffic cannot be received in the interface. This is more likely to affect port 8 than other ports.
- The default queueing method for PPP interfaces that are cross-connected to DS3s is Weighted Fair Queueing, but it should be FIFO.
- The default queueing method for PPP interfaces that are cross-connected to HSSI interfaces is Weighted Fair Queueing, but it should be FIFO.

- The MRRU on MLPPP interfaces (1520 bytes) prevents proper interoperability with equipment from Turin Networks.

Firewall and VPN

- When a SIP call ends, it is possible for an association to be left in the firewall by the SIP ALG longer than it should be. If another SIP transaction matches this passive association, the new transaction fails. Additionally, if a SIP packet is received that matches a newly-deleted old SIP association, the old association is used, rather than creating a new one. The first packet is discarded, but subsequent packets get through.
- AOS currently supports only 20 policy classes at a time. Attempting to configure a 21st policy class via the CLI generates an error, as it should, however it still moves the user into policy-class configuration mode.
- When initiating a tunnel using Aggressive Mode, after IKE and IPSec both come up, the initiator re-sends the initial message of Aggressive Mode three more times.
- When URL Filtering is enabled, Yahoo Messenger clients behind a router may not work. This results from the fact that Yahoo Messenger clients will send non-HTTP traffic to port 80 if attempts on other ports fail. The URL Filter intercepts this traffic as HTTP, determines that it is not HTTP traffic, and discards the traffic.
- It is possible for memory to erroneously be overwritten by the SIP ALG when calls end.

AOS 17.03.02.00 Release Notes

Release Notes **Release Date: September 17, 2008** **Notes Revision: Sep. 17, 2008**

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.03.01.00)

The Adtran unit fails to TFTP a configuration from the server upon bootup when using Auto-Config, because the DHCP client does not ask for options 66 and 67; this only occurs when the DHCP server is configured in a way that it only replies with parameters requested from the client.

Removing a VRRP statement followed by removing a corresponding track statement, from the NetVanta 3400 series, will cause a reboot.

When using the ShoreTel 530 or 560 speakerphone connected to a NetVanta 1238 PoE switch, if the remote caller speaks loudly while the local 530/560 phone is on speakerphone, the local 530/560 may reboot.

A Cisco IP phone can not download a screen logo through the AOS stateful firewall because the phone sends an ACK even though it does not see a SYN/ACK from the server.

Pasting large amounts of non-command text, with little or no carriage returns, into a SSH session will cause an Adtran unit to lockup.

When a child map is applied to the parent map, the unit will drop prioritized traffic, if specifying the priority as a percentage with the 'priority percent' command rather than using 'priority xxx (in kbps)' command.

Entering a password exceeding 256 characters at the enable prompt, or web login, combined with service password-encryption enabled will result in a reboot.

A 202 Accepted response to a SUBSCRIBE, is treated as an unknown response by the SIP ALG.

Top websites email client and exception report email client send a naked LF without a preceding CR. This is in violation of RFC 2822 section 2.3.

When a TCP packet is missing from a TCP stream, the MLPPP stack will wait 500ms for the missing packet to arrive before continuing to process the TCP stream, which is normal behavior for MLPPP, but may cause poor throughput because the Adtran will buffer the following packets for 500ms.

AOS 17.03.02.00 SA Release Notes

Release Notes **Release Date: September 17, 2008** **Notes Revision: Sep. 17, 2008**

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.03.01.00)

The Adtran unit fails to TFTP a configuration from the server upon bootup when using Auto-Config, because the DHCP client does not ask for options 66 and 67; this only occurs when the DHCP server is configured in a way that it only replies with parameters requested from the client.

Removing a VRRP statement followed by removing a corresponding track statement, from the NetVanta 3400 series, will cause a reboot.

When using the ShoreTel 530 or 560 speakerphone connected to a NetVanta 1238 PoE switch, if the remote caller speaks loudly while the local 530/560 phone is on speakerphone, the local 530/560 may reboot.

A Cisco IP phone can not download a screen logo through the AOS stateful firewall because the phone sends an ACK even though it does not see a SYN/ACK from the server.

Pasting large amounts of non-command text, with little or no carriage returns, into a SSH session will cause an Adtran unit to lockup.

When a child map is applied to the parent map, the unit will drop prioritized traffic, if specifying the priority as a percentage with the 'priority percent' command rather than using 'priority xxx (in kbps)' command.

Entering a password exceeding 256 characters at the enable prompt, or web login, combined with service password-encryption enabled will result in a reboot.

A 202 Accepted response to a SUBSCRIBE, is treated as an unknown response by the SIP ALG.

Top websites email client and exception report email client send a naked LF without a preceding CR. This is in violation of RFC 2822 section 2.3.

When a TCP packet is missing from a TCP stream, the MLPPP stack will wait 500ms for the missing packet to arrive before continuing to process the TCP stream, which is normal behavior for MLPPP, but may cause poor throughput because the Adtran will buffer the following packets for 500ms.

If two SSH connections to the unit are attempted simultaneously, the same session ID may be assigned to both sessions, which can cause SSH to lockup until the unit is rebooted.

AOS 17.03.03.00 Release Notes

Release Notes **Release Date: November 6, 2008** **Notes Revision: Nov. 7, 2008**

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.03.02.00)

Issuing a 'show qos map' command may cause the unit to reboot if there is a single sequence within a QoS map in the configuration.

Utilizing the 'ip unnumbered' command on a WAN interface may cause the directly connected route for the LAN interface, which has the IP address configured, to be removed. This can prevent the user from being able to access the device when connected to it via the LAN.

DHCP server does not update the client name in the lease when it receives a DHCP request from a client already in its lease list.

The DHCP server command 'netbios-node-type h-node' is added automatically and cannot be removed from the running config.

AOS VPN routers may reboot if mode configuration negotiations are initiated by a client including more than 16 attributes.

A TACACS+ session is maintained when console session is logged out.

TACACS+ accounting reporting back to the server contains a minor memory leak, which can cause the unit to reboot after an extended period of time.

IGMP snooping may allow for a spanning tree loop, which may lead to a reboot if an extensive amount of multicast traffic traverses the switch.

Referencing a prefix-list that does not exist in a BGP neighbor configuration and then removing the reference may cause the unit to reboot.

Receiving L2TP traffic on a stateless policy-class entry may cause the unit to reboot.

If two SSH connections to the unit are attempted simultaneously, the same session ID may be assigned to both sessions, which can cause SSH to lockup until the unit is rebooted.

Receiving 5,000+ routes from two or more eBGP neighbors can unveil a slow memory leak that can cause the unit to reboot.

Web GUI and help text in CLI give the impression that any interface can have the QOS 'match-all' clause, when in reality only EEQoS interfaces support this clause at this time.

If, during normal router operation on a unit running VPN, the router enters a state where an inbound SA does not have a corresponding outbound SA, the unit may reboot.

AOS 17.03.04.00 Release Notes

Release Notes **Release Date: January 6, 2009** **Notes Revision: Jan. 13, 2009**

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.03.03.00)

Changing the MTU on an 802.1q Ethernet sub-interface returns an error.

Slow fan speeds, when unit is idle in a below average temperature environment, can cause the NetVanta 1534 to display a false "Chassis fan has failed" message.

When used with certain non AOS switches, 802.1q tagged packets generated by the AOS device may be dropped if the packet is smaller than 64 bytes after the tag is removed.

IGMP Snooping may consume extensive CPU resources, and may cause the unit to reboot after an extended period of time.

If a DS3 interface remains saturated for an extended period of time, HDLC keepalives may not be transmitted, thus causing the HDLC interface to bounce.

Using VQM and the SIP ALG simultaneously can cause a reboot when specific SIP communication patterns are processed by the router.

A WPA pre-shared key on a VAP containing spaces will be operational after being configured, but will not be restored when the unit was rebooted.

Attempting to delete a tcl script from flash memory after the script has been executed with the 'run-tcl' command, can cause unit to lockup.

Setting a Port Description from the GUI causes the Speed/Duplex setting to change on the NetVanta 1534.

If the unit is congested and receives a frame on the Layer 2 interface, the T1 may drop (port 1 only, on a dual T1 NIM).

Some of the SIP Proxy Pool Elements are incorrectly incremented, and may cause the SIP Proxy functionality to fail after an extended period of time.

AOS 17.03.05.00 Release Notes

Release Notes **Release Date: January 6, 2009** **Notes Revision: Jan. 13, 2009**

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.03.04.00)

In the CLI, the command 'ip forward-protocol udp domain' or 'ip forward-protocol udp 53' will return an error that states "%Could not perform operation." In the GUI, when trying to add port 53 or the well-known port labeled as "domain" in the DHCP Relay webpage, the following error is returned, "Error: Could not add UDP Forward Protocol."

When using AAA to authenticate an SSH session, in certain situations, the unit may lock up or reboot.

In the Web GUI, if IP unnumbered is used on a frame-relay interface, the system summary page returns a '503 server error.'

AOS units, acting as SNTP servers, do not respond correctly to clients' SNTP queries.