AOS 17.01.01.00 Release Notes

Release Notes **Release Date: December 7, 2007** **Notes Revision: 12/7/2007**

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 340	9200422-2A170101.biz	9950422-2A170101.biz	10.01.00
NetVanta 344 Annex A (2nd Gen)*	9200426-2A170101.biz	9950426-2A170101.biz	
NetVanta 344 Annex B (2nd Gen)*	9200423-2A170101.biz	9950423-2A170101.biz	
NetVanta 1335	N/A	9950515-2A170101.biz	
NetVanta 1524ST	N/A	9950560-2A170101.biz	
NetVanta 3120	N/A	9700600-2A170101.biz	14.04.00
NetVanta 3130	N/A	9700610-2A170101.biz	14.04.00
NetVanta 3305	9200880-2A170101.biz	9950880-2A170101.biz	04.02.00
NetVanta 3430	9200820-2A170101.biz	9950820-2A170101.biz	
NetVanta 3448	9200821-2A170101.biz	9950821-2A170101.biz	
NetVanta 4305	9200890-2A170101.biz	9950890-2A170101.biz	08.01.00
NetVanta 5305	9200990-1A170101.biz	9950990-1A170101.biz	11.03.00

* Part numbers of 2nd generation NetVanta 344 routers end with 'E1'. 1st generation NetVanta 344 routers (part numbers ending 'L1') 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
Voice Quality Monitoring (VQM)	Voice Quality Monitoring (VQM) allows real time passive voice over IP (VoIP) quality measurements to be taken on all Realtime Transport Protocol (RTP) voice streams transmitted through an AOS device. VQM provides statistics and measurements vital for determining the quality of voice calls and the source of voice quality problems. VQM statistics can be sorted by call, interface, source IP address, RTP flows, and by date and time. ***Supported Platforms*** **NetVanta 3100 Series, NetVanta 3400 Series, NetVanta 4305, NetVanta 5305, and NetVanta 1335**
Cable Diagnostics	Cable diagnostics is a method of testing Ethernet cables connected to 10/100 Ethernet or 10/100/1000 Gigabit-Ethernet physical interfaces. By using the GUI, cable diagnostics can be run on multiple switch ports to determine if the cables stemming from the port(s) are functioning properly, have a short or an open connection, and either

	the total length of the cable or the length of the cable to the fault. This feature is not available on fiber ports, and can only be used through the Web GUI. ***Supported Platforms*** **NetVanta 1335**
Top Talkers (Integrated Traffic Monitoring Enhancement)	The Top Talkers feature incorporates the statistics of Top Talkers (top bandwidth users by source IP address), Top Listeners (top bandwidth users by destination IP address), and Port Lists (amounts of traffic observed on specific ports) into easily viewed output, accessed through either the command line interface (CLI) or Web-based graphical user interface (GUI). These statistics are captured by the metering process at the traffic flow observation point, and collected as traffic flow entries expire from the flow cache. These statistics allow the user to see the nature of traffic being processed by the router without having to configure a separate server to collect data. ***Supported Platforms*** **All Routers and Switches**
Flash Provisioning	Flash provisioning is a utility that automatically updates CompactFlash® capable units with new copies of Tcl scripts, configuration files, and binary images. Flash provisioning works in conjunction with AOS Tcl scripting capabilities, creating a powerful utility to easily upgrade code, create a standard default configuration, and require user input to answer site-specific questions. ***Supported Platforms*** **NetVanta 1335 and NetVanta 3400 Series**

Enhancements	Overview
Wireless Controller Support in NetVanta 4305	The NetVanta 4305 can now also act as Wireless LAN Access Controllers through Adtran Wireless Control Protocol for NetVanta 150 Access Points. ***Supported Platforms*** **NetVanta 4305**
VRRP Support in NetVanta 5305	The Virtual Router Redundancy Protocol (VRRP) is now also available on the NetVanta 5305 ***Supported Platforms*** **NetVanta 5305**
Output Modifiers	Allows you to specify a string of text to search for in the output of any show command and then only show lines that match, only show lines that don't match, or show the first line that matches and anything after. ***Supported Platforms*** **All Routers and Switches**
Firewall Improvements (Unique Source NAT)	Improvements were made to the firewall functionality to allow static 1:1 NAT to work with source port preservation. This allows for a scenario where two Private addresses are being NATed to two Public addresses, the source ports from the traffic originating from the Private IP can be the same and will be preserved as the source ports on the Public IP. For this to work properly, each 1:1 source NAT entry must have a matching destination NAT entry on the public interface. ***Supported Platforms*** **All Routers and Switches**
VRF Enhancements	In this new release, the implementation of VRF now allows for VRF-Aware DHCP Server and Firewall functionality. ***Supported Platforms*** **NetVanta 1335, NetVanta 3305, NetVanta 3400 Series, NetVanta 4305, NetVanta 5305**
IGMP Snooping added to NetVanta 1335	Internet group management protocol (IGMP) snooping is a way to take advantage of IGMP packets flowing through a switch to reduce unnecessary flooding of multicast

	traffic. Since multicast traffic isn't automatically learned by switch hardware, the switch must flood the multicast traffic out all its ports in the virtual local area network (VLAN) to ensure that a subscribed client receives the traffic. By using information learned by snooping IGMP packets, we can build a multicast address table and reduce the amount of flooding. This will allow multicast traffic to be forwarded only to ports on which multicast subscribers or multicast routers have been snooped using the IGMP protocol. This feature is now also available on the NV 1335. ***Supported Platforms*** **NetVanta 1335**

Errata

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

Services and Viewers

- **Using Flash Provisioning to back up image takes longer than expected.**
  - Description: Copying firmware images from Flash to Compact Flash can take longer than 20 minutes to complete.
  - Workaround: No known workaround.

- **If DNS Proxy is configured on a non-default VRF, and the proxy points to a DNS server on the default VRF, the DNS lookup will not be NAT'd.**
  - Description: This will occur when traffic from one or more LAN VRFs to the Internet VRF must change VRFs with NAT, and DNS Proxy must be used so that lookups will first be attempted on the LAN VRF before being proxied to an external DNS server out the Internet VRF. DNS proxy requires both the internal DNS server and client to reside on the same VRF. Also, DNS proxy requests can not change VRFs via NAT since they will be sourced from an internal IP address and the SELF policy class cannot be configured.
  - Workaround:
    1) LAN hosts can statically configure their DNS server as the external server out the Internet VRF rather than the router or the DHCP server pools on the router can hand out the external DNS server IP address.
    2) DHCP server pools hand out the Internet interface IP address as the DNS server, and DNS requests to that address get source NAT'ed to the Internet VRF.
    3) Create separate encapsulating GRE tunnels and decapsulating GRE tunnels from the LAN VRFs to the Internet VRF. Designate the internal DNS server in the Internet VRF as the LAN VRFs" name-server and the external DNS out the Internet VRF as the Internet VRF"s name-server.

- **Long duration conference calls between VRFs, using the SIP ALG may lead to a reboot.**
  - Description: When a public phone on the default VRF conferences in a private phone on the default VRF and a private phone on the non-default VRF, and the call lasts for several hours, routers may reboot.
  - Workaround: No known workaround

- **The 5305's Flash Filesystem may become corrupt when loading files onto it.**
  - Description: When copying firmware onto Flash, the Filesystem may become corrupt. The CLI reports errors acquiring and writing to sectors of the Filesystem. This only affects NetVanta 5305 units manufactured since July 2007.
  - Workaround: No known workaround. If this occurs, recovery requires reformatting the filesystem

- **503 error on AP config page and VAP config page**
  - Description: A 503 error will result when browsing to the AP or VAP configuration pages on a NetVanta 3430.

- Workaround: Configure the AP or VAP via the CLI.

- **Issuing the "no bridge 1 protocol ieee" returns an error message**
  - Description: In the CLI, when you attempt to remove bridging functionality by issuing the "no bridge 1 protocol ieee" command, an error message indicating that the operation could not be performed is returned, although the command actually takes effect and disables the bridge.
  - Workaround: Ignore the error message.

- **Navigating from VQM page to other pages causes Firefox to crash.**
  - Description: After observing the statistics in the Voice Quality Monitoring utility in the GUI, browsing to a different page causes Firefox to crash.
  - Workaround: Use a different browser.

Routing, Switching and Bridging

- **Using Top Talkers in combination with the Firewall can potentially cause a reboot.**
  - Description: It is possible for units configured with both Top Talkers and Firewall to reboot, with a core dump indicating "Invalid Address for Read."
  - Workaround: No known workaround
- **RADIUS Client can get stuck in a loop and consume 90+% of the CPU**
  - Description: The AOS RADIUS Client can potentially get stuck in a loop and drain CPU resources. The only way to recover is to manually cycle power.
  - Workaround: No known workaround.
- **Configuring stacking on the 3448 can cause the unit to become unresponsive and subsequently reboot.**
  - Description: -
  - Workaround: No known workaround

- **DHCP Relay in IPSEC VPN**
  - Description: DHCP does not get relayed over an IPSEC VPN tunnel.
  - Workaround: No known workaround.

- **Bridging between an Ethernet port and a VLAN interface on the same bridge group does not work.**
  - Description: When trying to create a bridge between an Ethernet interface and a VLAN interface that belong to the same bridge group, the end devices on the interfaces cannot communicate.
  - Workaround: No known workaround.

System and Drivers

- **During broadcast storms, the NetVanta 1335 may reboot due to PacketRouting congestion.**
  - Description: PacketRouting may become congested during packet storms, causing a reboot. The exception report will indicate PacketRouting was congested for 120 seconds; also, the top item under Buffer Users in the report will not be "fixedsize."
  - Workaround: Be careful to not allow broadcast storms in a network. The BPDU Filter feature should only be enabled on ports that will not be connected to other switches.
- **The TFTP Client can consume all CPU resources, causing packets to not be routed.**
  - Description: Copying files to Flash via TFTP can cause the CPU to reach 100%. This has only been observed on NetVanta 3100 series units with part numbers ending in "G2."
  - Workaround: Copy files to the unit via FTP or HTTP.
- **Tracks may become stuck in a Fail state when an associated Probe is in the Pass state.**
  - Description: In rare cases, a Network Monitor track may fail even if the probe(s) it tracks is/are in a

pass state. Disabling and re-enabling the track will make it recover.
  - Workaround: If this occurs, do a 'shut', 'no shut' on the track to make it recover.

Firewall and VPN

- **The SIP ALG does not support overlapping addresses on different VRFs.**
  - Description: The SIP ALG supports VRFs, but does not work when there are overlapping IP addresses.
  - Workaround: Do not use overlapping IP addresses in different VRFs.

Resolved Issues

These are issues that have been resolved since the previous AOS release (16.03.00)

Services and Viewers

- SMTP Extended Hello (EHLO) messages do not have brackets around system address literals, as recommended in RFC 2821 section 4.1.3.
- Units reboot when a Compact Flash card is removed while files are being copied to or from Compact Flash.
- HDLC interface descriptions are not returned via SNMP.
- System events for insertion and removal of Compact Flash cards use inconsistent capitalization.
- SMTP client port selection does not override the default port (25).
- The 'copy http' command returns the message "No Error" when an HTTP Server sends a response that does not include an HTTP Header.
- An empty line is placed at the end of Ethernet sub-interface configuration blocks in configuration files.
- When configuring Switch Stacking in the GUI, configuring member switches with a VLAN that is out of the acceptable range will return a blank web page instead of providing a warning.
- Using the Web GUI to change Radio Modes from 802.11 BG to either 802.11B or 802.11G may result in invalid speeds being left in the configuration.
- The context-sensitive help for 'access-point-controller' under 'dot11ap' is too long to fit on one line.
- The WiFi Wizard accepts spaces in preshared keys, although spaces should not be permitted.
- The WiFi Wizard does not check key lengths.
- Access Point names are not retained when manually configured in the Web GUI.
- Using long banners in conjunction with TACACS requires manually paging through the banner prior to receiving a login prompt. This can cause problems for automated management tools, such as nCommand.
- The context-sensitive help for the 'no terminal length' command indicates a range of 0-512, but the acceptable range is actually 0-480.
- When Syslog is configured with a facility value of "local3," the Web GUI displays the facility as "auth."
- The Troubleshooting page reports IP addresses of 0.0.0.0 for interfaces that acquire addresses through DHCP.
- Configuring excluded-domains from the Top Websites statistics page does not work.
- Access Point Radio Speed Default Basic Set settings are not correctly applied to the CLI if changed in the Web GUI (despite a message indicating that the settings have been successfully applied).
- The 'show interface description' command does not work for switchports.
- Hitting ESC or CTRL+C to escape from context sensitive help, and then hitting '?' to get the same context sensitive help, produces an incomplete list of available commands.
- VRF and VPN are mutually exclusive features. However, if VRF is enabled, the VPN Wizard in the Web GUI does not indicate this to users.
- If an access list with a name that is numerical is entered using the web interface a 503 server error will be returned.
- When using port-auth and having ports in a force-authorized state, the authentication status in the web interface shows as “Unauthorized."
- Context sensitive help for 'port-channel load-balance' crosses column 80 and wraps to next line.
- The context-sensitive help for the 'interface' command shows "ethernet" as an option, however the product's

Ethernet interfaces are called "switchports."
- The "Netvanta" Web GUI heading on the 5305 is not consistent with the "NetVanta" heading on other platforms.
- The IP Flow Statistics Web GUI page (under the Cache tab) displays an incorrect value for "Last aging poll occurred."
- The output from the 'show output-startup' command is truncated for startup configs that are larger than 20309 bytes.

Routing, Switching and Bridging

- Routers configured as DNS Proxy servers in a non-default VRF do not respond to DNS requests.
- Removing VRF from a Frame Relay sub-interface leads to a reboot.
- Host table entries cannot be cleared on a non-default VRF.
- While bridging is configured on a PPP interface, manually rebooting units may cause them to reboot with a core dump upon reloading.
- AOS continues to route packets when 'no ip routing' command is issued, but 'ip route-cache' is enabled.
- Removing 'default-information-originate' from an OSPF process may lead to a reboot.

Network Interfaces and Quality of Service

- When changing speed and duplex on Ethernet ports from auto-negotiate to forced, the new settings may not be properly applied to the Ethernet hardware, causing errors and low throughput.
- The NetVanta 5305 may reboot if it has high volumes of traffic running over multiple DS3s with Multi-Link Frame Relay configured.
- When neither routing nor bridging are enabled, attempts to assign IP addresses to PPP interfaces are unsuccessful. Subsequent attempts to use these IP addresses on other interfaces are also unsuccessful.
- Hard-setting the interface speed/duplex on the switchports of the 3448 and 3100 series platforms will cause interface errors even when the other end of the link is hard-set.
- Deleting a QoS map while it is still applied to a logical interface may cause a reboot.
- When an Ethernet link on a NetVanta 3430 is auto-negotiated and then switched to 100Mbps/full-duplex, throughput may degrade, but no errors will appear on the interface.

Firewall and VPN

- The Web GUI does not clearly describe the differences in Top Websites reports when Allow Mode is enabled vs. disabled. When Allow Mode is enabled, reports indicate successful visits to web sites; when it is disabled, reports indicate blocked attempts to access web sites.
- IKE configuration accepts a peer IP address of 0.0.0.0, which is an invalid address.
- IKE messages are not always freed after being allocated. Each platform has a predefined number of messages that may be allocated, and if enough messages are not available, units may reboot.
- Cannot Flow Data over 3120 VPN Tunnel with Sec Assoc Life at Max Value. With the Security Association Lifetime Set to the maximum value in kBytes, the 3120 will not allow data to be transmitted over a VPN tunnel.
- When multiple VPN clients behind an AOS device performing NAT connect to a single public VPN concentrator, returning traffic may be sent to the incorrect client.
- When using URL Filtering with Websense, missing Host fields received from clients should be populated with the destination IP address prior to sending to Websense. The host field is included in packets sent to Websense, but the Host field does not contain the destination IP.
- Running 100 registrations with 100 simultaneous calls (the maximum allowable values for both) can cause the SIP ALG to fail during periods of re-registration.
- The 'show access-lists' command does not show the correct number of matches for standard ACL entries (extended ACLs are unaffected).
- Receiving ICMP error messages for uninitiated sessions causes the firewall to leak memory.
- The SIP ALG may attempt to free unused NAT ports when phones are used that re-use source ports for RTP.

AOS 17.01.02.00 Release Notes

Release Notes **Release Date: January 28, 2008** **Notes Revision: 2/28/2008**

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.01.01.00)

- 503 Server Error on System Summary Page in 1524
- "Undefined" returned as result of cable diagnostics test in web GUI
- Adding static routes or VPN clients connecting to a router running OSPF and redistributing the default route would sometimes cause the OSPF neighbors to lose the redistributed default route
- Demand interface dial string does not honor all ASCII characters
- Incorrect output on the DMT Bits Per Bin with the 'show interface adsl' command
- Not returning NUcastPkts from PPP interface via SNMP
- HDLC Interface statistics not retrieved with SNMP Walk
- Ethernet not responding in Frame Relay Unnumbered Config when the 'ip unnumbered' command was issued before configuring the DLCI value
- When the router is acting as a DNS client and receives a response code 2(Server Failure) from a non authoritative server, the router does not append the domain name and query again
- Frame Relay Fragmentation not accepting Begin and End bit of a Frame Relay header when the frame length is less than the MTU
- DHCP Relay traffic not sent through a VPN tunnel

AOS 17.01.03.00 Release Notes

Release Notes **Release Date: March 5, 2008** **Notes Revision: 03/20/2008**

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.01.02.00)

The command "logging email priority-level warning" does not show up in the running configuration.

Removing Loopback IP address on a NetVanta 1335 can cause the unit to reboot.

Top Websites Reporting causes Memory leak which can lead to a reboot.

Web GUI returns a 503 server error on 3100 series products when Radius is enabled.

Netvanta 1335 may reboot when FFE is enabled and the PPP interface changes state.

In OSPF, if the 'default-information-originate' command is manually entered before the network statements, the router will not advertise a default route

5305 can reboot if a shutdown command is issued to the T3 interface when it is under heavy traffic load.

Unable to cross connect a VLAN with a ppp interface on the NetVanta 3448

Configuring UDP relay to forward any UDP port will prevent DHCP pools from being configured.

TACAS+ session maintained whenever console session is logged out

SSH Executive Authorization not being sent in TACACS+

Creating a new username/password combination in the GUI without a portal-list, causes an invalid login

GUI stops responding when a user tries to login leaving the password field blank when using TACACS+

Switch Stacking Does Not Work After Reboot.

AOS 17.01.04.00 Release Notes

Release Notes **Release Date: April 24, 2008** **Notes Revision: April 28, 2008**

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.01.03.00)

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 tag is removed.

When the firewall and e-mail logging are enabled, with logging set to priority level of info, a deadlock may occur.

When VPN tunnel timeout values are mismatched between the peers, a few seconds of disruption in service during times of re-negotiation can occur.

Troubleshooting page in the GUI displays an error about not NATing to a public IP, when the IP address is public.

When using SCP to transfer files whose filenames are larger than 24 bytes, the transfer will not work properly. The file is transferred but is truncated to the shorter length.

E1 interfaces GUI page report to be using only the first channel, regardless of the actual number of channels being used.

Using the 'Separate Firewall Device' option with the GUI setup wizard, a browser freezes and gives an error.

Unable to statically assign an IP address to a specific MAC address from the DHCP options in the GUI.

NetVanta 5305 will not perform multicast routing with PIM Sparse enabled.

NetVanta 1524 stops port mirroring after a reboot.

Applying a Crypto Map to a PPPOE interface in the Web GUI does not work.

AOS 17.01.05.00 Release Notes

Release Notes **Release Date: June 12, 2008** **Notes Revision: June 13, 2008**

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.01.04.00)

On the Ethernet 0/1 interface of the NetVanta 3120, when the IP type is changed from static to DHCP, the crypto map statement is removed from that interface, but only when being done via the web GUI.

If, during IKE negotiation with a dynamic client, the NetVanta sends an IKE message to the client out an interface other than that on which the VPN tunnel would terminate (this could be due to load sharing, for example), the message will use the source address of the interface it was sent out of rather than that of the terminating interface, which causes the negotiation to fail.

SNR is not displayed correctly on the NetVanta 340.

When a track disables a crypto map entry and the NetVanta switches from a backup tunnel to the primary tunnel multiple times, intermittently only IPSec SAs get deleted, which causes dead pear detection to still use the backup tunnel's IKE SA, preventing routes on the peer from getting removed.

Issuing the command 'show qos interface switchport 0/x' returns a value of ‘0’ regardless of what the value should be.

When high traffic-rates force late collisions, due to duplex setting mismatches between a NetVanta 4305's Ethernet port and the directly connected device, the port may cease transmitting; although, it remains up and receives traffic.

Having multiple secondary IP addresses configured will cause the IP addresses to be associated with the wrong interfaces inside the Public IP Address drop down box when setting up a Port Forward policy type in the web GUI.

The System Summary page in the NetVanta 1524 GUI reports an error that does not exist.

Web GUI reports a track as passing regardless of the actual state.

Applying a Policy-Class on an interface, which does not have an IP address configured, will block data.