AOS 17.02.01.00 Release Notes

Release Notes **Release Date: April 7, 2008** **Notes Revision: 4/7/2008**

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 1335	N/A	9950515-2A170201.biz	
NetVanta 1524ST	N/A	9950560-2A170201.biz	
NetVanta 3120	N/A	9700600-2A170201.biz	14.04.00
NetVanta 3130	N/A	9700610-2A170201.biz	14.04.00
NetVanta 3200/3205 (3rd Gen.)*	9203860-2A170201.biz	9700860-2A170201.biz	17.02.01.00
NetVanta 3305**	9200880-2A170201.biz	9950880-2A170201.biz	04.02.00
NetVanta 3430	9200820-2A170201.biz	9950820-2A170201.biz	
NetVanta 3448	9200821-2A170201.biz	9950821-2A170201.biz	
NetVanta 4305	9200890-2A170201.biz	9950890-2A170201.biz	08.01.00
NetVanta 5305	9200990-1A170201.biz	9950990-1A170201.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
Network Quality Monitoring	Expanding on the functionality of the existing Network Monitor feature, Network Quality Monitoring will now offer the ability to measure loss, latency, and jitter between two endpoints. This goes beyond just testing for reachability to actually measuring the quality of service that the intervening network provides. It also included the ability to execute a Two-way Active Measurement Probe (TWAMP) ping to measure packet loss, delay, and IPDV-abs from the web GUI. ***Supported Platforms*** **NetVanta 1335, NetVanta, NetVanta 3100 Series, NetVanta 3200 Series, NetVanta 3305, NetVanta 3400 Series, NetVanta 4305, and NetVanta 5305**
Generic Email Client	This Mail Client provides an abstract way to add e-mail notifications to AOS with the

	ability to determine the content of the sent message. The client consists of four major components: capture trigger, output, send trigger, and email. When a *capture trigger* occurs, the mail agent will gather *output* from running commands that the user specifies (normally, "show" commands but "tcl" commands may also be useful). When the *send trigger* indicates that the proper time has come, the mail client will send an *email* with the configured options. Multiple agents can be configured to work in parallel. ***Supported Platforms*** **NetVanta 1335, Netvanta, NetVanta 3100 Series, NetVanta 3200 Series, NetVanta 3305, NetVanta 3400 Series, NetVanta 4305, and NetVanta 5305**
3G EV-DO NIM Support	A NIM module that provides connectivity to the Verizon Wireless network for dial backup as well as primary connectivity applications. ***Supported Platforms*** **NetVanta 1335, NetVanta 3200 Series, NetVanta 3305, NetVanta 3400 Series, and NetVanta 4305**
LLDP-MED	LLDP-MED (also known as either LLDP for Media Endpoint Devices or LLDP-Media Endpoint Discovery) extends basic LLDP functionality, by providing useful network policy information to devices such as VoIP phones. In particular, it allows switches to tell attached devices what VLAN tags, Layer 2 CoS, and DSCP values to use. In addition to VoIP-specific information, LLDP-MED also requires support of the 802.3 MAC/PHY Configuration/Status TLV. This allows network devices to inform each other whether they support auto-negotiation, the speed/duplex combinations they support, and at what speed/duplex they are currently operating. ***Supported Platforms*** **NetVanta 1335, NetVanta 1524ST, NetVanta 3100 Series, and NetVanta 3448 Series**
Enhanced Ethernet QoS	Class-Based Traffic Shaping is supported on Ethernet Interfaces. This allows the product to perform as a CPE router in Metro-Ethernet applications. Some of the benefits of this new feature are that a class can be an interface, VLAN, or any case that can be matched in a QoS map. Multiple independent shapers on an Ethernet, 802.1q, or VLAN interface can be configured. Also, the addition of child maps allows for subdividing a shaped class into multiple subclasses and applying QoS actions such as class-based queuing and low latency queuing to each subclass. There are new matching options as well. Matching up to eight DSCP values with one statement, matching outgoing VLAN, or matching any are all available options. When multiple match statements are configured in a QoS map class, the default behavior is matching any of the statements results in applying the configured action. Now the new match-all option can be used when it is desirable to require a packet to match all configured match statements in order to be considered part of the QoS map class. ***Supported Platforms*** **NetVanta 3100 Series, NetVanta 3305, NetVanta 3400 Series, NetVanta 4305, NetVanta 5305, and NetVanta 1335**
Top Talkers Graphing (Integrated Traffic Monitoring Enhancement)	The Top Talkers Graphing 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 an easily viewed output graph, accessed through the 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 **NetVanta 3100 Series, NetVanta 3305, NetVanta 3400 Series, NetVanta 4305, NetVanta 5305, and NetVanta 1335**
Network Time Protocol (NTP)	The Network Time Protocol (NTP) is used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver or modem. NTP (version 3) has developed into the standard Internet time synchronization protocol. It is extremely efficient and needs no more than about one packet a minute to synchronize systems on a LAN to within 1 millisecond, and systems across WANs to within about 10 milliseconds. ***Supported Platforms*** **NetVanta 1335, NetVanta, NetVanta 3100 Series, NetVanta 3200 Series, NetVanta 3305, NetVanta 3400 Series, NetVanta 4305, and NetVanta 5305**
WLAN - Automatic Security Key Generation	This feature adds the ability to generate WEP keys based on a WEP key seed (passphrase). It generates a WEP key using a standard md5 key generator that is compatible with a clients WEP key generator. It is useful for quickly producing keys if the passphrase or seed is known. Most clients have this ability and now the Virtual Access Point will be able to produce the same keys. ***Supported Platforms*** **NetVanta 3200 Series, NetVanta 3305, NetVanta 3400 Series, NetVanta 4305, NetVanta 5305, and NetVanta 1335**
ATM QOS (SHDSL NIM Only)	This feature provides the ability to define ATM QOS for VBR-RT, VBR-NRT, and UBR VC's. VBR-rt class of service is characterized using three traffic parameters, parameter cell rate (PCR), sustained cell rate (SCR) and maximum burst size (MBS). This type of channel is allowed to transmit at PCR for MBS cells and SCR on average. The service must guarantee a maximum cell delay variation. VBR-NRT is much like VBR-rt with the maximum cell delay variation requirement removed. UBR VC's class of service is characterized by PCR which defines the maximum bandwidth available to this channel. The PCR is not guaranteed by the service provider. ***Supported Platforms*** **NetVanta 3200 Series, NetVanta 3400 Series, NetVanta 4305, NetVanta 5305, and NetVanta 1335**

Enhancements	Overview
Wireless Controller Support in NetVanta 5305	The NetVanta 5305 can now also act as Wireless LAN Access Controllers through Adtran Wireless Control Protocol for NetVanta 150 Access Points. ***Supported Platforms*** **NetVanta 5305**

Ping Improvements	There were a few of modifications to the CLI for a ping test. AOS now allows the user to run a ping test towards a destination with an infinite number of pings. If an infinite ping test is issued, the verbose option will not be allowed. The user will only see the overall result (display character) of each individual ping. To issue an infinite ping, specify the count as 0. AOS now also allows a timeout between 1-60 seconds, instead of 1-5 seconds. There is also a new user-specified parameter added to the CLI called "wait". The wait parameter is the minimum amount of milliseconds that will elapse in between sending test packets. This was added to guarantee that every result is obtained, stored, and displayed prior to deletion of the result. ***Supported Platforms*** **NetVanta 3100 Series, NetVanta 3200 Series, NetVanta 3305, NetVanta 3400 Series, NetVanta 4305, NetVanta 5305, and NetVanta 1335**
Show IP Route Refactoring	The "show ip route <IP>" command now shows more detailed information. The previous implementation of the "show ip route <IP>" command's output has now been changed to be displayed when the command "show ip route <IP> longer-prefixes" is issued. Also, instead of performing a search on the route table for a route specifically matching the given IP, the next hop route for the given IP address in the route table will be found. ***Supported Platforms*** **All Routers and Switches**

Errata

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

Services and Viewers

- The 'ntp server ADDRESS prefer' command does not cause the specified server to be preferred over other servers.
  - Workaround – No known workaround.
- The command 'clear qos map' does not clear all statistics.
  - Workaround – No known workaround.
- SNMP Informs do not work.
  - Workaround – No known workaround.
- On the NetVanta 1524ST, the System Summary page warns that a problem was detected by the device, but the Troubleshooting Page shows no problem.
  - Workaround – Ignore the error message.
- In the Web GUI, following the steps in the Getting Started page to configure bridging results in loss of IP connectivity to the unit.
  - Workaround - Assign the IP address of the router to the Bridge Virtual Interface, and put the physical interfaces in the bridge group.
- XML reports generated in the Web GUI for Voice Quality Monitoring stats are not formatted in proper XML format. There are more than one top level elements. Firefox and Internet Explorer will not display the file, due to this.
  - Workaround – No known workaround.
- Clearing ATM interface statistics results in invalid input/output rates, as reported in both the CLI and Web GUI.

- Workaround – No known workaround.

- The Web GUI allows users to configure Ethernet sub-interfaces, whose sub-interface numbers are out of range. The valid range is 1-4095, but higher numbers are allowed. In the Web GUI, a 503 server error is returned if users then try to apply a VLAN ID to the interface. The CLI will not allow users to change the configuration of this sub-interface.
  - Workaround - Configure Ethernet sub-interfaces via the CLI between the range of 1-4095.

- When two routes to the same destination are configured, but load sharing is disabled, only one path is used for forwarding. This is reflected in the CLI with the 'show ip route' command, but both routes are shown in the Web GUI.
  - Workaround – If the unit is configured for multiple routes to the same destination, only view the 'show ip route' command in the CLI.

- 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.
  - Workaround - When going through the wizard a second time, be certain to manually delete the original default route.

- The number of Port Security violations displayed in the Web GUI is inconsistent with the number displayed in the CLI.
  - Workaround – View the violations in the CLI or manually refresh the web page.

- 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.
  - Workaround – Configure ATM PVCs for ADSL interfaces via the CLI.

- Using the Setup Wizard to configure a unit for Internet access after the unit has already had several interfaces configured leads to invalid configurations.
  - Workaround - Use the Setup Wizard to configure Internet access only if the unit is in its factory default configuration.

- The Setup Wizard will not complete if users attempt to configure ATM Routed-Bridged Encapsulation (RBE).
  - Workaround - Manually configure ADSL with ATM Routed-Bridged Encapsulation in the Web GUI, or else use the CLI.

- The Setup Wizard cannot be used to configure bridging.
  - Workaround - Manually configure bridging either in the Web GUI, under Bridging, or configure it in the CLI.

- Top Talkers graphs in the Web GUI do not always display complete IP addresses. For example, 10.22.110 may be displayed instead of 10.22.110.30.
  - Workaround - If you are unable to see an address in the Web GUI, view the statistics in the CLI.

- For routers that have a large number of Top Talkers statistics, if you view the 5 minute Top Talkers graph, navigate to another graph, and come back, the graph does not display.
  - Workaround – No known workaround.

- 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. Other host platforms are unaffected.
  - Workaround – Wait until the 3G NIM firmware upgrade is complete to use the CLI.

- The Web GUI of the 3rd generation NetVanta 3200/3205 suggests that 16 ATM PVCs are supported on the platform, but this number is too high based on performance testing. Performance degradation can be seen with

only eight PVCs.
    - Workaround – Configure less than eight PVC, for desired performance.

Firewall and VPN

- The MSN Messenger ALG appears to modify MSN fields that are not supposed to be modified. These fields include: IP-Address-Internal and PortX-Internal.
    - Workaround – No known workaround.
- MSN Messenger file transfers are unsuccessful through the AOS firewall, regardless of whether the MSN ALG is enabled or not.
    - Workaround – No known workaround.
- The MSN Messenger Phone feature is unsuccessful through the AOS firewall, regardless of whether the MSN ALG is enabled or not.
    - Workaround – No known workaround.

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.01.03)

Services and Viewers

- HTTP and HTTPS Access Classes cannot be deleted with the command '[no] ip http [secure-access-class | access-class] in'.
- Added a checkbox to the VPN Wizard and VPN Peers Web GUI pages to make it easier to use Voice Quality Monitoring over a VPN. VQM requires stateful firewall inspection, but VPN tunnels created in the GUI are stateless by default.
- The SNMP Web GUI page contains a link to firewall pages on platforms that don't include firewall functionality (such as switches).
- When using 802.1x MAC-based port authentication, you may not change the port control type. This is expected behavior. However, when attempting to make this change in the Web GUI, the warning message that is generated is ambiguous and offers no advice on why the change to port control type was rejected.
- Incorrect output on the DMT Bits Per Bin with the 'show interface adsl' command
- The context-sensitive help for 'logging email sender' contains a registered domain and should have an example domain instead.
- The command 'no periodic' does not remove periodic items from a schedule. (Users are required to enter 'no' plus the entire command as it reads in the configuration to remove the item from the configuration.)
- Under probe config mode, the command 'no data ' returns an error, even though it successfully removes the command from the configuration.
- The context-sensitive help for the probe configuration mode 'timeout' command displays an invalid range.
- ICMP Echo Probes accept packet sizes that are outside the range indicated in context sensitive help.
- The 'show run interface shdsl' command does not work.
- If the same QoS map is applied more than once to the same interface, the CLI returns a warning that reads %No Error. The warning should indicate that the map has already been applied.
- The context-sensitive help for 'show qos map interface' and 'show qos map interface atm' refers to vcls instead of sub-interfaces.
- Hitting Ctrl-Z while prompted for a password breaks from password prompt, but does not insert a new line beforehand.
- The Telnet to Unit link in the Web GUI does not work if the Telnet server port has been changed to anything but port 23.
- The Web GUI for Access Controllers does not indicate when Access Points are disconnected.
- Bridge Virtual Interfaces are not persistent across reboots.
- The Web GUI does not provide a warning when users attempt to change the authentication mode of a Demand

interface from None to either PAP or CHAP without also entering a username and password.

- The tabs at the top of the Firewall / ACLs Web page intermittently do not show any content until one of the tabs is clicked.
- If a MAC Access List is created in the Web GUI and given a name that includes spaces, the ACL name that is inserted into the running configuration should be enclosed in quotation marks, but is not. As a result, the configuration will not be properly restored upon a reload.
- Invalid probe tolerance values are accepted in the Web and CLI.
- TCP Connect probes do not display correctly in the Web GUI.
- In the Network Monitor Wizard, the interface used to monitor the destination is not saved in such a way that users can later click the back button to return to the screen and have the interface remain the same. Users have to manually re-set the interface to the appropriate setting.
- The Network Monitor Wizard occasionally freezes after users click Next or Finish.
- The framing for G.703 interfaces on E1/G.703 NIMs cannot be properly configured in the Web GUI.
- For modem interfaces, if Caller-ID Override is set to Normal, the Web GUI should not display the Override Number textbox. However, the textbox is displayed in Internet Explorer.
- The firewall must be enabled for URL Filtering to work. If URL has been configured, but the firewall is disabled, there is no warning in the Web GUI to inform users that their filtering configuration will not be active until the firewall is enabled.
- The direction for URL Filters is not clearly described in the Web GUI.
- If the maximum allowed number of ATM PVCs has already been configured, and users attempt to add an additional PVC via the Web GUI, the GUI returns a 503 server error.
- Disabling an ATM sub-interface in the Web GUI produces an error message that refers to Routed-Bridged Encapsulation, even if RBE is not configured for the sub-interface.
- When configuring interfaces in the Web GUI, a checkbox is displayed for RTP Monitoring even if there is no IP address on the interface. Upon clicking Apply, a warning is returned to indicate that the RTP Monitoring settings were unable to be saved. This occurs for all interface types, but could be particularly troublesome on ATM interfaces that are to be configured for any operation mode besides IP over ATM (for example, PPPoA or PPPoEoA).
- There is a 503 server error if a bridge group is assigned to an interface, and IRB is subsequently enabled in the Web GUI.
- The Web GUI does not check to ensure users have entered a sequence number before attempting to add a new sequence.
- The AC / AP Web GUI page does not update the status of previously discovered access points when communication with one of the access points has been lost. Users are required to leave the page and return in order to see up-to-date information.
- Attempting to remove a bridge group via the Web GUI results in a 503: Server Error page.
- The default dampening interval for Network Monitor tracks configured in the Web GUI is 1000 seconds instead of 1 second.
- The WAN Summary section of the System Summary Web GUI page shows interfaces that are a part non-default VRFs. However, the Web GUI is supposed to be limited to the default VRF.
- The acceptable size for ICMP-Echo probes is different in the Web GUI (64-1500 bytes) than in the CLI (0-1462 bytes).
- Clicking on the RTP Monitoring link on the 3120/3130 platforms results in a 404 error (the page is not found).
- The Setup Wizard's description of the requirement for a T1 NIM in order to configure an external firewall is too vague.
- If a QoS map has been configured to mark DSCP by alias instead of numeric value (for example, EF instead of 46), the marking cannot be changed to a numeric value via the Web GUI.
- When users apply default DSCP to COS mapping on a switch via the Web GUI and then attempt to disable it, the Default DSCP to COS checkbox remains checked. This is expected behavior when specific mappings have not been changed, and it is intended to show the user that the default mappings are still in effect. However, it would be easier to understand what is happening if the specific DSCP to COS fields were grayed out when the Default DSCP-COS checkbox is checked (to show that they cannot be changed) and were not grayed out when the checkbox is unchecked (to show that they can - and should - be changed from their default values).
- Static MAC address table entries cannot be configured for Gigabit Switchport interfaces via the Web GUI.

- When a username has been configured and a subsequent similar username (for example, Bob and bob) is configured and assigned a portal list in the Web GUI, the previously-created user is also assigned to the portal list.
- In the Web GUI, when editing a QoS map that is configured to match a DSCP value, if you click the link to add another DSCP value and then click the delete button for the pre-existing DSCP value, you can no longer configure any DSCP values without navigating to another page and then returning to the QoS map page. (Note: This applies to the QoS map pages as they are organized in AOS 17.02 and does not affect earlier releases.)
- The Web Setup Wizard does not create DHCP excluded ranges to limit the start and end addresses. As a result, all addresses in the subnet of the LAN interface will be offered to clients.
- Using the Setup Wizard to configure a unit for Internet access after the unit has already had several interfaces configured leads to invalid configurations. Workaround: Use the Setup Wizard to configure Internet access only if the unit is in its factory default configuration.
- If bridging is configured prior to starting the Setup Wizard, the wizard does not work.
- The Setup Wizard returns an ambiguous error when users attempt to configure primary or secondary DNS servers that are the same as those already learned dynamically from DHCP. Additionally, the wizard does not offer a Back button to allow users to go back to change their DNS server, forcing them to begin the wizard from the beginning.
- When configuring DHCP in the Setup Wizard, if users enter the broadcast address for their configured subnet, the wizard returns an error upon completing the wizard.
- The Web GUI Troubleshooting page attempts to detect errors on non-default VRFs, but it should only work for the default VRF.
- For IP over ATM configurations, the Web GUI Troubleshooting page warns that ATM sub-interfaces are not cross-connected to any PPP interfaces. For this type of configuration, they do not need to be.
- ATM interface hold-queue and fair-queue threshold values are visible in the Web GUI, but should be removed to prevent users from accidentally breaking Class Based Queueing configurations.
- A warning is displayed above the page heading at the top of the Web GUI if a HDLC interface is administratively up but operationally down.
- When configuring Ethernet sub-interfaces in the Web GUI, sub-interfaces may be set to the Native VLAN even if the appropriate checkbox is not checked.
- The 'show interface tunnel X' command displays sequence and checksum statistics even if sequencing and checksums are disabled.
- The 5 minute statistics for PPP, Frame Relay, and HDLC interfaces cannot be cleared via the CLI or Web GUI.
- The 'show interface' command for SHDSL interfaces reports that the EOC is down.
- Removing an IP address from an interface that is the source for a GRE Tunnel causes routers to reboot.
- Deleting ATM interfaces or ATM cross-connects can cause units to reboot. Additionally, if there are 16 ATM sub-interfaces, and one of the sub-interfaces is deleted, the router reboots.
- When a NetVanta is configured to initiate an IPSec VPN tunnel with only transform sets that include Authentication Header, the unit sends a malformed first message of Quick Mode. The responder may reboot upon receipt of the malformed packet.
- Troubleshooting page in the GUI displays an error about not NATing to a public IP, when the IP address is public.

Routing, Switching and Bridging

- IP addresses cannot be assigned to routed interfaces when IRB is enabled.
- Static MAC Address Table entries for switchport interfaces are not persistent across reboots.
- Additional debug information regarding processing of LSAs has been added to the 'debug ip ospf flood' command.
- Routers do not respond to RIP requests.
- Removing an IP address from a Bridge Virtual Interface corrupts the running configuration.
- Extended ping commands do not work with non-default VRFs.
- The 'no-alg' keyword is omitted from the running config for NAT destination lists on the default VRF.

Network Interfaces and Quality of Service

- To remove Demand Routing connect sequences, users cannot copy the existing connect sequence from their config, and then enter 'no' plus the existing line.
- Port descriptions are not communicated via LLDP.
- If a QoS map is applied to a PPP interface that is configured for PPPoA, PPPoEoA, or PPPoE, the PPP interface's 'cross-connect' command is not persistent across reboots. (Note: QoS maps should be applied to the lowest possible Layer 2 interface -- in these cases, either ATM or Ethernet/VLAN interfaces.)
- If a QoS map is deleted while the map is applied to an interface, the map may not be removed from the interface configuration.
- Exceeding the five class-based queue limit in a QoS map results in an entry that still appears to be part class-based when viewed.
- Inbound QoS maps on 802.1q interfaces do not work.
- If users create an ATM interface (with a cross-connect to a SHDSL interface and is shutdown) before the 2nd SHDSL pair comes out of LOS, then the 2nd pair will never come out of alarm until after the unit is reloaded.
- 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.

Firewall and VPN

- Changing a standard ACL while debugging the ACL can cause the match delta to go negative.
- IKE may attempt to save a hash value for a Security Association that was previously deleted by XAuth (for example, if XAuth times out before a SA completely comes up). In very rare cases, this behavior leads to a reboot.
- Users may enter the 'log-input' keyword for ACLs, although this functionality is not supported.
- Configuring excluded-domains from the Top Websites statistics page can cause a string of url15 delete to be printed on the screen.
- URL Filtering does not allow HTTP POST messages, whose content length is zero.
- WEP ASCII keys do not work.

AOS 17.02.02.00 Release Notes

Release Notes **Release Date: May 7, 2008** **Notes Revision: May 9, 2008**

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.02.01.00)

A reboot may occur if a child QOS map is applied to a parent map, which has a priority statement applied.

IKE SAs are not being cleared when the crypto map is disabled by a track, resulting in routes through the VPN tunnel not being removed.

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

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

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

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.

DDS NIM reports line status as UP, regardless of actual state. When this occurs, no traffic traverses the NIM even though the line status shows to be UP.

AOS 17.02.03.00 Release Notes

Release Notes **Release Date: July 7, 2008** **Notes Revision: July 15, 2008**

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.02.02.00)

When running URL filtering, users accessing websites that generate malformed HTTP segments may cause the router to reboot.

TCP flows are not reported correctly via NetFlow.

'Clear counters' command for HDLC protocol interfaces does not clear out queue statistics.

NV1335 reboots when an ATM PVC interface mode is changed from PPPoE to PPP via the GUI.

When a crypto map is applied to an interface, enabling or disabling traffic-shaping on that same interface, from the GUI, will also remove the crypto map entry from that interface.

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), then the message was given the source address of the interface it was sent out of rather than that of the terminating interface, which causes the negotiation to fail.

ADSL downlink interface statistics incorrectly calculated and displayed when a "show" command is issued

AOS 17.02.04.00 Release Notes

Release Notes **Release Date: September 29, 2008** **Notes Revision: October 1, 2008**

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.02.03.00)

Changing the data length for an active ICMP-echo probe with the 'size' command may cause the unit to reboot.

There is a memory leak that can lead to reboots when TACACS+ is invoked.

In Network Monitor, changing the default probe period does not correctly effect when the probes are actually transmitted.

NetVanta 3430 presents a 503 error while accessing the System Summary page from the GUI when the 'ip unnumbered eth 0/1' command is set on 'interface PPP 1'.

NetVanta 3400 series routers with SNMP Traps enabled will provide a Cold Start Trap after reboot regardless of whether reload was a cold or warm start.

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.

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

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

Configuring SNMP through the GUI results in an incomplete command, which causes the tarps not to be sent out.

AOS allows configuration of invalid static routes, which cause other features to not function properly.

Issuing the 'show ip mroute' command can cause the unit to reboot.

Using a port that is reserved by the Microsoft Zone Gaming ALG can cause the unit to reboot.

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

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.

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.

Rebooting a unit that has 'bridge-group 1 vlan-transparent' in the configuration may result in the unit continuously rebooting.

Performing a SNMP Walk on the DS1 performance intervals either errors out, or skips the first few OIDs.

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