AOS 13.01.00 Release Notes

Release Notes **Date: 7/31/06**

Introduction

NetVanta products support application image updates via the NetVanta Web GUI, TFTP, X-Modem, and FTP. A detailed firmware upgrade guide is available on our website for step-by-step instructions. Prior to upgrading firmware, please ensure that your unit meets the following Boot ROM Requirements

- **340 – Boot ROM version 10.01.00 or later is required to load this firmware.**
- **344 – Boot ROM version 10.04.00.SA or later is required to load this firmware.** NEW
- **1224R/STR – Boot ROM version 6.03.00 or later is required to load this firmware.**
- **3305 – Boot ROM version 4.02.00 or later is required to load this firmware.**
- **4305 – Boot ROM version 8.01.00 or later is required to load this firmware.**
- **5305 – Boot ROM version 11.03.00 or later is required to load this firmware.** NEW

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 Boot ROM upgrade, please contact ADTRAN Technical Support (support@adtran.com or 888-423-8726) for assistance.

New Features	Overview
Network Monitor	Network Monitor provides IP connectivity and performance testing, using ICMP ping probes, TCP connect probes, and/or HTTP probes. This provides dynamic detection of cases where Layer 1 and Layer 2 connectivity remain active, but Layer 3 connectivity is lost. For example, if a NetVanta is connected to a cable modem via Ethernet, and the cable link between the modem and service provider goes down, AOS can detect the link failure and remove any static routes that were associated with that link. Example: **ip local policy route-map PROBE_TRAFFIC** ! **probe PING_PROBE icmp-echo** **destination adtran.com** **period 5** **tolerance consecutive-failures 5** **no shutdown** ! **track TRACK** **test probe PING_PROBE** **no shutdown** ! ! **route-map PROBE_TRAFFIC permit 10** **match ip address Cable_Probe** **set ip next-hop 10.10.10.3** ! interface eth 0/1 ip address 10.10.10.1 255.255.255.0 no shutdown !

ip access-list extended Cable_Probe
 permit icmp any host 10.10.10.3
!
ip route 0.0.0.0 0.0.0.0 10.10.10.3 **track TRACK**

The router in this example will ping adtran.com every 5 seconds. If 5 consecutive pings fail, the associated track will be put into a "FAIL" state. The static default route will only be valid when the track is in a "PASS" state, so if the track fails, the route will be removed from the route table.

Network Monitor is configurable in both the CLI and the Web GUI.

Supported Platforms ***NetVanta 3300, 4000, and 5000 Series***

SNTP Server

ADTRAN OS devices can now act as Simple Network Time Protocol (SNTP) servers. This feature can be enabled from Global Config Mode with the command **ip sntp server**. (Note: In order to act a server, the AOS device must also be configured as an SNTP client for a remote server.)

Supported Platforms ***ALL***

Fast Forwarding Engine (FFE)

The Fast Forwarding Engine (FFE) increases routing throughput for many common applications, including:

- Firewall (no ALG traffic)
- NAT
- Static filters / access groups
- Per-destination load-sharing

When any of these applications are used without FFE, AOS runs several processes for every packet that is forwarded. With FFE enabled, these processes are only run on the initial packet of a "flow" or session. By reducing the number of required processes, the overall throughput through the router increases.

FFE is enabled on a per-interface basis with the command **ip ffe**. (Note: Fast Forwarding is currently unavailable on HDLC, GRE, and FDL interfaces.)

Supported Platforms ***NetVanta Routers***

SNMP Version 3

SNMP Version 3 updates previous versions of the Simple Network Management Protocol, by adding support for user authentication and packet encryption. SNMPv3 also adds a new message type, known as an *inform*, which allows routers and switches to reliably indicate to Network Management Systems when links go up or down.

Example:

ip snmp agent
!
snmp-server user ADMIN ADMIN-GROUP v3 auth md5 MYPASSWORD
snmp-server group ADMIN-GROUP v3 auth

The example above shows a user named "ADMIN," who is part of a group called "ADMIN-GROUP." Members of ADMIN-GROUP should use SNMPv3 and must authenticate themselves with a password. In this case, ADMIN will authenticate with an MD5 hash of the password "MYPASSWORD."

Supported Platforms ***ALL***

Enhancements	Overview
Port Mirroring Enhancements	When using port mirroring, the destination interface can now be configured to both transmit and receive data. Previously, such ports would transmit data to connected devices, but would not accept incoming data from those devices. To allow bidirectional communication, use the **monitor session 1 destination interface <interface-type> <slot/port> no-isolate** command. ***Supported Platforms*** ***NetVanta 1000 Series***
Web Interface Enhancements	▪ **Setup Wizard** for easy configuration of NetVanta 3200 and NetVanta 340 routers ▪ Added Italian language support to the Web GUI. o Added the **Language** page. o Added the **ip http language Italian** command. ▪ Added the ability to clear QoS map statistics in the Web GUI (Router Products) ▪ Added the ability to specify SNTP Wait Time and SNTP Retry Timeout from the **Time and Date** page ▪ Added warning to the **ip http authentication <list name>** command when an invalid list name is specified ▪ Added the ability to configure Ethernet Sub-Interfaces from the Web GUI (Router Products) ▪ Added the ability to configure OSPF Stub Areas, Total Stub Areas, and Inter-Area Route Summarization from the Web GUI (Router Products) ***Supported Platforms*** ***ALL, Unless Otherwise Specified***
Command Line Interface Enhancements	▪ Added AOS version, Boot Rom version, platform, serial number, flash memory size, DRAM size, and date/time stamp to the output of the **show run** command ▪ Added the ability to view Demand Interface statistics in real time, with the **show interface demand <interface number> realtime** command (Router Products) ▪ The **show flash** command now lists files in alphabetical order ▪ Added queuing information for ATM sub interfaces to the output of the **show interfaces** command (Router Products) ▪ Updated **debug ip <tcp | udp | icmp>** output to indicate new source IP addresses when Policy Based Routing is used on the local interface (**ip local policy <policy-name>**). Previously, the source address for these debug messages indicated "0.0.0.0" instead of the IP address of the egress interface (NetVanta 3300, 4000, 5000 Series) ***Supported Platforms*** ***ALL, Unless Otherwise Specified***
TFTP Server Overwrite	Added the ability to overwrite files that are sent to the unit via TFTP with the **ip tftp-server overwrite** command ***Supported Platforms*** ***ALL***
FTP Server	▪ Added the ability to view FTP server events with the **debug ip ftp-server** command ▪ Added the ability to specify the file system for the FTP server, on products that support Compact Flash. The default file system can be adjusted with the command **ip ftp server default-filesystem <cflash | flash>**. ***Supported Platforms*** ***ALL***
Quality of Service	In configurations that include PPPoE, PPPoA, or PPPoEoA, fair queuing should be applied to the lowest Layer 2 interface, while FIFO queuing should be applied to the corresponding PPP interface. Previously, users had to be aware of these stipulations and manually configure the proper queuing on the PPP interface, as well as the

	Ethernet, VLAN, or ATM interface. Now, the queue type is automatically changed to the appropriate type on all interfaces when applying a QoS map or making a cross-connect between a PPP interface and another logical interface type. ***Supported Platforms Router Products***
Firewall	Added a check to prevent users from configuring policy classes named "self" or "default." These policy class names are reserved by AOS and could cause confusion if users configured custom policies with either of these names. ***Supported Platforms Router Products***
Virtual Private Networking (VPN) Enhancements	▪ Added the ability to configure anti-replay window sizes, from 64 to 1024, in powers of 2. The Crypto Map Config Mode command is **antireplay <64 | 128 | 256 | 512 | 1024>** (the default is 64). ▪ The **show crypto ipsec sa** command now displays out-of-sequence errors on inbound Security Associations, to help determine the best anti-replay window size. ***Supported Platforms VPN Enabled Devices***
AAA Enhancements	▪ TACACS+ Exec Authorization – Allows users to enter directly into "enable" mode for new CLI sessions, with the **aaa authorization exec** command. ▪ TACACS+ Connection Accounting – Send accounting records for all outbound Telnet connections, with the **aaa accounting connection** command. ▪ TACACS+ Exec Accounting – Send accounting records for new connections or logins, with the **aaa accounting exec** command. ***Supported Platforms ALL***

Resolved Issues

- The Refresh button under the Port Security page in the web GUI only works when it is turned off (NetVanta 1224R / NetVanta 1224STR)
- DynDNS update timer is too long
- Adding a key to the **radius-server host** command may cause a unit to reboot
- Using the Web GUI to move stateless ACL entries above or below others will remove the **stateless** keyword
- The DHCP server lease expiration time is incorrect when viewed in the web GUI
- Units may lock up if they receive DHCP leases greater than 50 days
- Units may reboot if large configuration files are pasted in
- CLI does not allow deletion of specific or grouped SNMP server views
- The **show ip traffic** command incorrectly displays a negative number for established current sessions
- File system may become corrupt if rebooted during a file transfer
- The **service password-encryption** command does not encrypt DynDNS passwords
- The context sensitive help incorrectly displays "TFTP server packets" for the **debug tftp server events** command
- The **clear counters** command does not properly reset ATM statistics
- The command **framing esf** is displayed in the output of a **show run** even though it is the default framing format for T1 interfaces
- Using the VPN wizard in the Web GUI to configure remote peers with Xauth results in a 503 server error
- The **modem countrycode USA/Canada** command incorrectly appears as **modem countrycode usa** in the running configuration
- Users may configure more than one attribute set for Aggressive Mode IKE tunnels, which is not permitted by RFC 2408 (Section 4.7)
- The **debug atm oam** command does not show any output when OAM cells are transmitted or received
- Transmit counters do not increment as traffic passes over ATM Interfaces
- The "Modules" table heading is formatted differently in the Web GUI than in the CLI (NetVanta 5305)
- Routers may indicate high Kernel Stack Usage when configuring IPSec with Certificates and SCEP
- Maximum configurable MTU size on HDLC interfaces is too high

- The OSPF **default-information-originate** statement is inconsistent when comparing the output of the **show run** command and the **show run verbose** command
- The default metric associated with OSPF default routes is incorrectly set to 20 instead of 10
- The **show ip bgp <network address> <subnet>** command syntax is inconsistent with other parts of AOS
- The BGP Neighbor **update-source** command does not allow ATM or HDLC interfaces to be specified
- Switched Ethernet interface port statistics may indicate an artificially high load, in packets and bits per second (NetVanta 1000 Series)
- Configuring a static IP address on a VLAN interface that is currently tied to a PPPoE interface may cause the router to reboot (NetVanta 1224R, NetVanta 1224STR)
- Secondary addresses on a VLAN interface are not deleted after cross-connected the VLAN interface to a PPP interface (NetVanta 1224R, NetVanta 1224STR)
- Bridging on HDLC interfaces does not work correctly
- T1 interfaces do not respond to unframed loopback codes from remote devices
- SNMP reports a PPP interface as a Multilink PPP interface
- Mobile VPN with Certificates and XAUTH may cause a reboot
- Very large numbers of traffic flows through the Firewall may cause a reboot
- Demand interfaces may become unresponsive if an associated Modem interface fails
- Issuing the show tech command resets terminal length to default setting
- Inactive static routes appear in Route Table page of the Web GUI
- The T3 **test-pattern** command context help is displayed incorrectly (NetVanta 5305)
- The continuous refresh option on status pages in the Web GUI may not refresh at the proper timed interval
- A demand interface may not attempt to establish a new connection if it had previously disconnected a connection prior to establishing PPP
- The **signaling-mode none** command appears under the G.703 interface (interface e1 1/2) in the output of the **show running-config verbose** command
- A unit may respond to SNMP requests containing a blank community value
- The DHCP Server may not respond to DHCP Requests in a timely manner if numerous hosts request addresses simultaneously
- The **ip load-sharing** statement erroneously appears in the output of the show run verbose command on switch products
- Port mirroring on the NetVanta 1524 does not work unless **monitor session** commands are entered in a specific order

Known Issues

- A QoS queue designated to use the bandwidth remaining percent command does not properly obtain remaining bandwidth under heavy load
- Unit does not receive LLDP packets properly (NetVanta 344)
- The value specified by the **snmp-server chassis-id <value>** command does not appear in a SNMP walk
- Using the MSN ALG with new versions of MSN Messenger may cause routers to reboot

Special Hardware Notes

- Small form-factor pluggable (SFP) fiber modules only support gigabit (1000 Mbit/s) connections
- 1000R/STR support WAN NIMs (Network Interface Modules)
- 300, 2000 and 5000 Series do not support WAN NIMs
- 4000 Series support the Octal T1/E1 Wide Interface Module and WAN NIMs
- 5000 Series only support Wide Interface Modules
- 56k data channel rate is not supported by T1/FT1 NIM (1202862L1), a T1/FT1 + DSX-1 NIM (1202863L1) must be ordered

AOS 13.02.00 Release Notes

Release Notes **Date: 9/11/06**

Introduction

NetVanta products support application image updates via the NetVanta Web GUI, TFTP, X-Modem, and FTP. A detailed firmware upgrade guide is available on our website for step-by-step instructions. Prior to upgrading firmware, please ensure that your unit meets the following Boot ROM Requirements:

- **340 – Boot ROM version 10.01.00 or later is required to load this firmware.**
- **344 – Boot ROM version 10.04.00.SA or later is required to load this firmware.** NEW!
- **1224R/STR – Boot ROM version 6.03.00 or later is required to load this firmware.**
- **3305 – Boot ROM version 4.02.00 or later is required to load this firmware.**
- **4305 – Boot ROM version 8.01.00 or later is required to load this firmware.**
- **5305 – Boot ROM version 11.03.00 or later is required to load this firmware.** NEW!

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 Boot ROM upgrade, please contact ADTRAN Technical Support (support@adtran.com or 888-423-8726) for assistance.

New Features	Overview
New Hardware Support	Four new NetVanta 3000 Series routers were released with AOS 13.02.00. ▪ **NetVanta 3120** – includes Ethernet WAN port, analog Dial Backup (DBU), software-based VPN, and integrated four-port switch ▪ **NetVanta 3130** – includes ADSL WAN port, analog Dial Backup (DBU), software-based VPN, and integrated four-port switch ▪ **NetVanta 3430** – includes two routed Ethernet ports and one NIM slot; Compact Flash support; expandable RAM for memory-intensive applications ▪ **NetVanta 3448** – includes two routed Ethernet ports and one NIM slot; integrated eight-port switch; Compact Flash support; expandable RAM for memory-intensive applications ***Supported Platforms*** **See Above**

Enhancements	Overview
Fast Forwarding Engine (FFE) Enhancements	Optimized Fast Forwarding Engine operation for Ethernet to Ethernet routing in the NetVanta 4305. ***Supported Platforms*** **NetVanta 4305**
UDP Relay Conversion of Broadcast to Multicast	Added support for converting broadcast packets to multicast packets over a WAN connection, using UDP Relay. This can be used in Wake on LAN (WOL) applications. Example: **ip multicast-routing** ! **ip forward-protocol udp 2000** !

```
interface eth 0/1
  ip mcast-stub fixed
  ip igmp static-group 239.200.200.1
!
interface ppp 1
  ip helper-address  239.200.200.1
!
arp 239.200.200.1 FF:FF:FF:FF:FF:FF arpa
```

In this example, broadcast packets received on PPP 1, destined for UDP port 2000, will be forwarded to the 239.200.200.1 multicast group. Ethernet 0/1 is a static member of that group, and the IP address has been mapped to the broadcast MAC address (FF:FF:FF:FF:FF:FF), so packets will be flooded to the LAN segment attached to Ethernet 0/1.

Supported Platforms **NetVanta Routers**

Command Line Interface Enhancements

- Added the ability to see destination port numbers when using TCP probes. This information can now be found as part of the **show probe <TCP-probe-name>** command.

Supported Platforms **NetVanta 3100, 3300, 3400, 4300, and 5300 Series**

Resolved Issues

- The **clear spanning-tree counters** command returns an error and does not properly reset STP counters (NetVanta 1000 Series)
- When **service password-encryption** is enabled, Dynamic DNS (DynDNS) passwords are re-encrypted after every reboot
- The SNTP Client feature cannot be configured via the Web GUI unless the SNTP Server is enabled
- The **Power Over Ethernet** page in the Web GUI displays power levels instead of voltage levels
- The **show tech** command resets CLI terminal length to the default setting
- The Web GUI allows secondary IP addresses to be set on VLAN interfaces of switch products, but this should only be allowed on router interfaces
- Using the MSN ALG with new versions of MSN Messenger may cause reboots, and there is no way to disable the ALG
- The **clear ip ospf process** command does not cause the local Router ID to be recomputed
- Using Network Monitor in conjunction with the AOS DHCP Client may cause probe traffic to establish erroneous firewall sessions
- The allowed values for probe **period** timers are not documented correctly
- Added the ability to see destination port numbers when using TCP probes. This information can be found with the **show probe <TCP-probe-name>** command.
- The **show track** command indicates that a track is tracking an item when it is not
  PPP Negotiated interfaces may be tracked, but they do not appear in the output of the **show track** command
- In the **track** command set, the **test probe** command should verify that a specified probe exists; the check occurs if only one probe is specified, but if a second is specified with an AND/OR, the check does not occur
- Changing the **expect status** parameter in an HTTP probe returns an error
- The **clear dump-core** command does not work on the NetVanta 344 platform
- Using RIP in conjunction with multicast routing may cause reboots without creating exception reports (NetVanta 4305)
- The Setup Wizard is missing images
- Adding a DNS Host Entry via the Web GUI returns a "503: Server Error" page
- Deleting a track may cause routers to lock up
- Configuring Layer 2 encapsulation on T3 interfaces via the Web GUI results in a "404: Not Found" page (NetVanta 5305)

- Using the Setup Wizard to configure the NetVanta 340 may result in a "503: Server Error" page
- The **show modules** command indicates an inaccurate Part Number for Slot 0 / Port 0 (NetVanta 5305)
- Added the ability to forward broadcast packets to multicast addresses using the **ip helper** command.
- Class-Based Weighted Fair Queuing (CBWFQ) does not work over Analog Dial Backup (NetVanta 4305)
- Route Table page in Web GUI has grammatical errors related to Network Monitor tracks
- Defining a static MAC Address Table entry causes CLI errors when loading or displaying configuration files (NetVanta 344)
- When used for Dial Backup, Analog Modem DIMs generate CRC and Abort errors on the NetVanta 4305 platform
- Pasting DHCP Pool commands into the running configuration may result in a host-only DHCP Pool instead of a network DHCP Pool
- The description for the Source IP Address in the **General Monitor** Web GUI page is misleading
- Line Status traps are not generated for T1 interfaces
- Analog Modem DIMs may send incorrect digits when placing calls (NetVanta 1224R / STR)
- PPPoE Service Names and AC Names are deleted after a reboot
- Cisco IP phones running software version 07-05-00 do not work with the AOS SIP ALG (updated ALG to accommodate new Cisco behavior)
- Applying the ip address dhcp command to ATM Sub-Interfaces may cause a reboot
- When configuring Demand Routing via the Web GUI, a resource pool priority must be specified; this does not match the behavior of the CLI, which uses a default priority of 1 if another value is not specified
- The Technology field of the Demand Routing **Connect Sequence** page in the Web GUI does not work when any "forced" technology is selected
  The Technology field of the Demand Routing **Connect Sequence** page in the Web GUI incorrectly shows an option called "busy-threshold"
- The Physical Interfaces page in the Web GUI returns a "503: Server Error" when T1 interfaces are in Yellow Alarm
- Route table changes may cause active firewall sessions to not be reset properly
- Changing a probe tolerance from consecutive-failure to rate-of-failure causes the probe to fail for several probe periods
- Configuring two probes with the same name and different probe types is allowed
- ICMP probe periods of less than 60 seconds are not allowed in the Web GUI
- The Network Monitor ACLs generated by the Web GUI allow all traffic of the chosen probe type, instead of specifying the proper destination hostname, IP address, or port number
- Some SIP call features (hold, transfer, conference) do not work with the SIP ALG in some applications
- Source NAT statements that reference interfaces that no longer exist cannot be removed with the **no nat source list <listname> int <interface> overload** command
- The Fast Forwarding Engine may cause routers to reboot if interfaces go up and down frequently
- The LLDP interface number is not advertised correctly on 802.1q interfaces
- The ip crypto fast-failover ? command is not formatted properly
- IKE Main Mode requires Remote IDs to be IP addresses, but other ID types should be allowed when using certificates
- In rare cases, routers may reboot when IPSec Security Associations are deleted

Known Issues

- Without a startup configuration, the Ethernet 0/2 LED is active until the **show run** command is executed (NetVanta 4305)
- Specifying an invalid probe period returns an error of "%" instead of indicating that the value is invalid
- Using Multilink Frame Relay Link Integrity Protocol under heavy traffic loads may cause MLFR to drop
- Configuring a Raw HTTP probe in the Web GUI may require horizontal scrolling to read HTTP strings
- Configuring two probes with the same name and different probe types in the Web GUI returns a "503: Server Error" instead of indicating that the action is not allowed
- Units may reboot if the Fast Forwarding Engine is configured in conjunction with Demand or GRE Interfaces

- A QoS queue designated to use the **bandwidth remaining percent** command does not properly obtain remaining bandwidth under heavy load.
- The value specified by the **snmp-server chassis-id <value>** command does not appear in a SNMP walk.

Special Hardware Notes

- Small form-factor pluggable (SFP) fiber modules only support gigabit (1000 Mbit/s) connections
- 1000R/STR support WAN NIMs (Network Interface Modules)
- 300, 2000 and 5000 Series do not support WAN NIMs
- 4000 Series support the Octal T1/E1 Wide Interface Module and WAN NIMs
- 5000 Series only support Wide Interface Modules
- 56k data channel rate is not supported by T1/FT1 NIM (1202862L1), a T1/FT1 + DSX-1 NIM (1202863L1) must be ordered

AOS 13.03.00 Release Notes

Release Notes **Date: 10/20/06**

Resolved Issues

- NV 344: Reallocated memory to better support VPN applications.
- Addressed issue that could cause reboots when configuring nat source
- Addressed problem with using HDLC as an SNMP source interface
- Resolved reboot with respect to DNS
- (Switch) Adjusted MAC table to prevent reboots
- Executing a clear mac address-table dynamic command may clear static entries as well
- NV1524 Reboots when TACACS+ is configured.
- WEB: Addressed web setup wizard errors.
- NV 3430/3448: ETH 0/1 and 0/2 go dark instead of red when link is lost
- Addressed reboot that could happen under extensive demand routing scenario
- Addressed issue where setting global max FFE sessions did not take effect.
- Web: Addressed 503 error when adding ethernet sub-interface.
- Corrected issue that required a reboot to get back to default view when SNMP community string is deleted.
- Unit will intermittently reboot if traffic is flowing and IP FFE is enabled on a layer 2 interface when either the IP address is deleted ('no ip address') or the interface is deleted ('no interface ppp 1' , 'no interface fr 1').
- Addressed internal broadcast issue that were causing VPN tunnels to not renegotiate properly
- Addressed reboot for unit under extensive througput performance testing
- BGP - Default network is not advertised when default route is removed from and re-added to route table
- With demand routing, if a NAT session is created before the demand interface is up, it will not NAT the packets to the proper address--must clear or time out before the traffic will pass.
- 'show queue' only displays packets for PPP & frame relay
- Timestamp in the running-config comments causes running and startup configs to have different MD5 hashes
- Addressed SNMP errors when sysName was over 80 characters.
- Corrected issue where DRI_AdminStatusCell does not work correctly for SNMP
- Add support for ipNetToMediaTable in IP MIB
- Add Latin American Spanish option for the web server does not appear in the running-config.
- Unit will intermittently reboot if traffic is flowing and IP FFE is enabled on a layer 2 interface when either the IP address is deleted ('no ip address') or the interface is deleted ('no interface ppp 1' , 'no interface fr 1').

AOS 13.04.00 Release Notes

Release Notes **Date: 11/30/06**

Resolved Issues

- WEB: Addressed issue that prohibited setting of SNMP trap host from GUI.
- FIREWALL: 'show ip policy-sessions' gets stuck in loop
- 3400: When 256M DRAM is installed, 'show version' output does not display app/boot code version
- Addressed a routing loop when an AOS device redistributes that it has a default route that was learned from OSPF.
- Dead peer detection messages causing error in peer router. Adjusted DOI value to address
- WEB: GUI Download mobile VPN policy file gives an error
- Addressed issue with a garbled host value in VIA line of SIP message. Resulted in one way audio.
- NetVanta returns invalid value for dot3pauseAdminMode and dot3pauseOperMode for the NetVanta 3120/3130 and NetVanta 3430/3448
- Added support for ipNetToMediaTable in the IP-MIB.

AOS 13.09.00 Release Notes

Release Notes **Release Date: September 4, 2007** **Notes Revision: 9/5/2007**

Enhancements	Overview
Network Interface Enhancements	Added support to allow an ATM sub-interface as a source interface for packets including SNTP, HTTP, and FTP. ***Supported Platforms*** **All routers and switches supporting DSL network interfaces**
IGMP Enhancements	IGMP Snooping has been added to NetVanta 1224s with integrated routers. ***Supported Platforms*** **NetVanta 1224R, NetVanta 1224STR**
SNMP Enhancements	Added SNMP support for BRIDGE-MIB dot1dBasePortIfIndex (OID 1.3.6.1.2.1.17.1.4.1.2). ***Supported Platforms*** **All routers and switches supporting AOS 13.9**

Resolved Issues

These are issues that have been resolved since the previous AOS release (13.04.00)

- A 503 Server Error is returned by the web interface when attempting to view VPN Peers.
- A high number of SNMP requests can cause SNMP to stop responding.
- QoS maps cannot be applied to VLAN interfaces with the web interface.
- An error will occur if the Remote ID and crypto map names are not the same.
- The VPN wizard gets stuck in "Loading" when using Microsoft Internet Explorer version 7.
- The Firewall wizard gets stuck in "Loading" when using Microsoft Internet Explorer version 7.
- New Daylight Savings Time standard is not supported.
- If a console or telnet session was ended before the username/password was entered completely while using TACACS+, a resource was not released. If this was repeated enough times TACACS+ would not be able to process any new requests.
- ADSL interface statistics show wrong value for Last Failed statistic when viewed through the CLI.
- An error is returned to an SNMP GET for ifInNUcastPkts and ifOutNUcastPkts on a PPP interface.
- A flood of ARP requests can cause a unit to reboot.
- When changing a password using the web interface, a 503 server error is returned.
- If there is a remote-id that is not associated with a crypto map, the VPN Peers page of the web interface will return a 503 server error.
- IGMP Snooping does not work correctly over Gigabit Ethernet Ports on a NetVanta 1224.
- Switchports may lock up on a NetVanta 1224 under heavy congestion.
- A lockup may occur when using IPSEC.
- Mode config does not properly remove a route when a VPN tunnel goes down.
- Entering the command 'no routed-bridge ip' on an ATM sub-interface causes the unit to reboot.
- The Physical Interfaces page of the web interface returns a 503 server error.
- Spanning tree may cause switches to reboot.
- Secondary IP addresses are not reported via SNMP.
- Policy classes applied to Ethernet sub-interfaces are not applied correctly after a reboot.
- The web interface shows the wrong value for ADSL Last Failed statistic.
- The 'snmp-server source-interface' command no longer effects SNMP traps that get sent.

- E-mail logging cannot be configured from the web interface.
- Cannot set the MTU on an ATM sub-interface.
- Disabling bridging on an interface causes a reboot.
- Secondary IP addresses are not preserved after a PPP link goes down if the primary IP address is assigned dynamically via IPCP.
- PBR does not properly route packets if the policy routes the packet to a Frame Relay sub-interface.
- If a MLFR interface is created and not cross-connected to a physical interface, a reboot will occur when walking the frame relay MIB with SNMP.
- VPN Peers page in the web interface can display a 503 server error.
- Frame relay DLCIs cannot be set on a sub-interface if there is a frame relay interface with a sequentially lower number that does not have any sub-interfaces associated with it.
- A dial in modem will lock up when a session is closed due to a modem disconnect.
- The dial in modem on a NetVanta 3448 can get into a state where it will not answer calls.
- IGMP snooping on VLANs can be disabled, but will be re-enabled upon reboot.
- Reordering port forwards with port translation in the web interface results in the destination port being set to 0.
- IP Addresses reported via SNMP may be associated with the wrong interface.
- Performing an SNMP walk on a unit with no community name set will cause the unit to reboot.
- Clearing ARP Cache causes DHCP Server to fail.
- When configuring PPPoE authentication the web interface returns a 503 server error.

AOS 13.10.00 Release Notes

Release Notes **Release Date: December 3, 2007** **Notes Revision: 12/5/2007**

Resolved Issues

These are issues that have been resolved since the previous AOS release (13.09.00)

- PoE: PoE devices may randomly loose power when connected to a port and result in the device rebooting.
- AAA: When TACACS+ executive authorization is configured the logins are always executive authorized instead of according to the configured privilege level.
- AAA: When the authorization commands <enable level> <method> command is applied to a telnet, console, or ssh interface it will not be saved or viewable in a show running-configuration.
- CLI: The T1 DSX NIM CLI help for the tdm-group command implied noncontiguous DSOs are supported.
- Long banner messages may trigger the "Waiting on TACACS Server" prompt on units configured for AAA requiring user input before being able to login, which causes problems for N-Command.
- SNMP: The ifIndex variable is missing from link up and link down traps.

AOS 13.11.00 Release Notes

Release Notes **Release Date: March 20, 2008** **Notes Revision: 03/28/2008**

Resolved Issues

These are issues that have been resolved since the previous AOS release (13.10.00)

SSH Executive Authorization not being sent in TACACS+

T1 and Dual T1 NIMs experience false loop ups.

D4 Framing is removed from config after reboot.

RTP passives not created properly in destination NATs, causing one-way Audio for SIP Phones depending on the order calls are placed.

AOS 13.12.00 Release Notes

Release Notes **Release Date: May 7, 2008** **Notes Revision: 05/13/2008**

Resolved Issues

These are issues that have been resolved since the previous AOS release (13.11.00)

If the firewall receives an ICMP or UDP echo response for which it can find no association for the initial request, this is detected as a smurf attack, and the packet is dropped, regardless of policy being set to stateless.

Sending a high-speed stream of 64 byte packets through a NetVanta 1224r may cause a reboot.

If the WAN interface drops while files are being transferred via FTP, the router may reboot.

Applying a policy-class on the default VRF interface, with no IP address, blocks data, even after IP is added to interface.

HTTPS does not work with Internet Explorer 7 on Windows Vista for the NetVanta 1224 series.

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.

RTP passives not created properly in destination NAT case.

AOS 13.13.00 Release Notes

Release Notes **Release Date: September 17, 2008** **Notes Revision: 09/18/2008**

Resolved Issues

These are issues that have been resolved since the previous AOS release (13.12.00)

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

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.

Accessing the QoS pages in the GUI causes the unit to reboot, when one or more Switchports are configured as part of a Port-Channel.

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.