AOS 15.01.00 Release Notes

Release Notes **Release Date: April 27, 2007** **Notes Revision: 4/30/2007**

Introduction

NetVanta and Total Access 900 Series products support application image updates via the ADTRAN OS 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 minimum Boot ROM requirements, listed under "Supported Platforms."

Supported Platforms

	Standard Feature Pack	Enhanced Feature Pack	Minimum Boot ROM***
NetVanta 340	9200422-2A1501.biz	9950422-2A1501.biz	10.01.00
NetVanta 344 Annex A (2nd Gen)*	9200426-2A1501.biz	9950426-2A1501.biz	
NetVanta 344 Annex B (2nd Gen)*	9200423-2A1501.biz	9950423-2A1501.biz	
NetVanta 1335	N/A	9950515-2A1501.biz	
NetVanta 1524ST	N/A	9950560-2A1501.biz	
NetVanta 3120	N/A	9700600-2A1501.biz	14.04.00 NEW
NetVanta 3130	N/A	9700610-2A1501.biz	14.04.00 NEW
NetVanta 3200/3205 (2nd Gen)**	9200860-2A1501.biz	9950860-2A1501.biz	
NetVanta 3305	9200880-2A1501.biz	9950880-2A1501.biz	04.02.00
NetVanta 3430	9200820-2A1501.biz	9950820-2A1501.biz	
NetVanta 3448	9200821-2A1501.biz	9950821-2A1501.biz	
NetVanta 4305	9200890-2A1501.biz	9950890-2A1501.biz	08.01.00
NetVanta 5305	9200990-1A1501.biz	9950990-1A1501.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.
** Part numbers of 2nd generation NetVanta 3200/3205 routers begin with '1202'. 1st generation NetVanta 3200/3205 routers (part numbers beginning '1200') 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 Hardware	Description
G.SHDSL NIM	Supports 2-wire and 4-wire G.SHDSL, with speeds up to 4.608 Mbps. The NIM is only supported on NetVanta 3200 and NetVanta 3205 routers.
NetVanta 1335 PoE	Includes all features and functionality of the NetVanta 1335, in addition to both 802.3af and Cisco Legacy Power over Ethernet.
NetVanta 150 Wireless Access Point	Standalone Wireless Access Point (WAP), which can be controlled by a NetVanta router or switch acting as an Access Controller. Up to eight APs may be controlled by a single Access Controller.

New Features	Overview
Wireless LAN Access Controller	To coincide with the release of the NetVanta 150 Wireless Access Point, AOS devices may now act as Wireless LAN Access Controllers. A single Access Controller (AC) allows users to manage up to eight NetVanta Access Points from one central location. ***Supported Platforms*** **NetVanta 3100 Series, 3400 Series, and 1335**
Integrated Routing and Bridging (IRB)	IRB allows IP traffic to be bridged between interfaces and, optionally, routed to others. Previously, IP traffic could be bridged or routed between interfaces, but IP bridging and IP routing could not be enabled on a single AOS device simultaneously. For a practical example, consider a network requirement to bridge IP traffic between two sites that are connected via a T1/PPP link, while simultaneously routing traffic destined to the Internet over a second Ethernet interface at the host site. Main Site: ip routing ! **bridge irb** bridge 1 protocol ieee ! **int bvi 1** ! BVI Interface ID is the same as the Bridge Group **ip address 192.168.1.1 255.255.255.0** ! This IP address is the default gateway for hosts at both sites no shutdown ! int eth 0/1 **bridge-group 1** ! All traffic not intended for 192.168.1.1 will be bridged to PPP 1 ! int ppp 1 **bridge-group 1** ! All traffic not intended for 192.168.1.1 will be bridged to Eth 0/1 ! int eth 0/1 ip address 1.1.1.1 255.255.255.0 ! ip route 0.0.0.0 0.0.0.0 1.1.1.254 Remote Site: **no ip routing** ! The remote site does not need to bridge and route simultaneously, ! so IP routing is disabled ! bridge 1 protocol ieee ! int eth 0/1 **bridge-group 1** ! int ppp 1 **bridge-group 1**

	Supported Platforms **All Routers**
Schedules (Absolute and Periodic)	Added support for absolute and periodic time schedules. Absolute schedules can be used to influence the behavior of Network Monitor Tracks during specific time periods (for example, "From 5:00PM on April 30, 2007 to 7:00AM on May 5, 2007 do X.") Example: **schedule S** **absolute start 17:00 30 april 2007 end 07:00 5 may 2007** no shutdown Periodic schedules can be used to influence the behavior of Network Monitor Tracks during recurring time periods (for example, "From 8:00AM to 5:00PM every weekday do X.") Example: **schedule T** **periodic weekday 08:00 to 17:00** no shutdown ***Supported Platforms*** **NetVanta 1335, 3000 Series (except 3200/3205), 4305, 5305**
Route Tagging	Route tags give users accurate and easy control over redistribution between routing protocols. Users may assign tags to static routes and routes inserted into the routing table via VPN Reverse Route Injection. Additionally, routes learned via BGP have tags associated with them and are set to the AS number of the last Autonomous System in the path to the destination network. Example: ip route 192.168.254.0 255.255.255.0 ppp 1 **tag 10** ! This associates tag 10 with the static route to 192.168.254.0 /24 ! route-map REDISTRIBUTE permit 10 **match tag 10** ! This matches all routes in the route table associated with tag 10 ! router ospf redistribute static route-map REDISTRIBUTE ! Because of the route map configuration, static routes with tag 10 are ! redistributed into OSPF. Other static routes are not. ***Supported Platforms*** **All Routers**
VPN Reverse Route Injection	Reverse Route Injection (RRI) allows an AOS router to add remote VPN networks to its route table when the VPN tunnel is up. By adding the route to its local route table, the router can then redistribute the route into a routing protocol, so that other routers can dynamically learn how to reach the remote network. This is useful when setting up redundant VPN gateways at a host site, which multiple remote sites will connect to. Example:

	! IKE Configuration, IPSec Transform Set, and VPN Selectors Omitted ! crypto map VPN 10 ipsec-ike match address VPN-10-vpn-selectors set peer 1.1.1.1 set transform-set esp-3des-esp-md5-hmac **set security-association idle-time 60** ! After 60 seconds of inactivity, the VPN tunnel will be torn down, and ! any associated routes that were injected into the route table will be removed. ! See "Crypto Map Idle-Time" under "Enhancements" for more information. **reverse-route tag 10** ! When the VPN tunnel is active, the remote private network(s) – as defined ! by the VPN selectors that were used to bring up the tunnel – will be added ! to the IP route table with a tag value of 10. ike-policy 100 ***Supported Platforms*** **All Routers (Requires Enhanced Feature Pack)**

Enhancements	Overview
802.1X Port Authentication	Added support for 802.1X Port Authentication to the NetVanta 3448 platform. ***Supported Platforms*** **NetVanta 3448**
VLAN 'Show' Commands	Added realtime viewing of the commands 'show vlan id <VLAN-ID>' and 'show vlan name <VLAN-NAME>'. ***Supported Platforms*** **NetVanta 344, 1000 Series, 3100 Series, and 3448**
Port Mirroring	Added the ability to remove VLAN tags from the destination port of a Monitor Session on the NetVanta 344 and NetVanta 3100 Series. This is enabled with the 'monitor session 1 destination interface <interface-ID> no-tag' command. ***Supported Platforms*** **NetVanta 344, 3100 Series**
Switchport Range Configuration	Added the 'interface range switchport' command to the NetVanta 3100 Series. ***Supported Platforms*** **NetVanta 3100 Series**
DHCP Client on Ethernet Sub-Interfaces	802.1Q encapsulated Ethernet sub-interfaces can now obtain IP addresses via DHCP. ***Supported Platforms*** **NetVanta 3000, 4000, and 5000 Series Routers**
SSLv3 / TLS 1.0 Support in Web GUI	The Web GUI now supports SSLv3 / TLS 1.0 for HTTPS connections. ***Supported Platforms*** **All**
SMTP Authentication for System E-mail	AOS now supports SMTP authentication for outgoing system-generated e-mails (e-mail logging and e-mail notification of voicemail). The command 'logging email receiver-ip <e-mail server address> auth-username <username> auth-password <password>' is used to configure authentication. ***Supported Platforms*** **All**
Quality of Service	▪ Added a fifth queue for Class Based Weighted Fair Queuing (CBWFQ)

Enhancements	▪ QoS Maps can now be used to set 802.1p Class of Service (CoS) values on Ethernet sub-interfaces for improved Layer 2 quality of service ▪ Added support for input QoS maps on Ethernet interfaces. Input QoS can be used to set DSCP/IP Precedence values. ▪ QoS Maps can now match DSCP aliases. Rather than inputting decimal values, such as "46," alias strings, such as "ef," can be used. ***Supported Platforms*** **All Routers**
Configurable Administrative Distance for OSPF and RIP	OSPF and RIP administrative distances may now be changed from their default values. From router configuration mode, the 'distance' command is used to accomplish this. ***Supported Platforms*** **All Routers**
Network Monitor Enhancements	▪ **Probe Pass/Fail Tolerance**: Users may now specify different tolerance values to put probes into the PASS state or the FAIL state. This is useful for users who wish to only use a link if it is very reliable; for example, if the probe should pass only after 5 consecutive successes, but fail after only 2 failures, the Probe Config Mode command 'tolerance consecutive pass 5 fail 2' would be used. ▪ **Increased Number of Track Test Objects**: The number of probes that can be tested by a single Track has been increased from 2 to 60,000. ▪ **Multiple Track Test Objects**: Schedules may now be tested in addition to probes. ▪ **Inverse Track Test Logic**: Tracks can now be put into a PASS state when a test fails, using the 'not' keyword. ▪ **Weighted Track Test Logic**: Users may now assign weights to test objects, putting the Track into either a PASS or FAIL state based on the cumulative weight of all objects. Example: track T **test list weighted** **if probe A weight 100** ! When the probe is in a PASS state, it will contribute a weight of 100 ! to the total weight of the test. **if probe B weight 100** **if probe C weight 100** **threshold 100** ! When the combined weight of the three probes under test is equal to ! or greater than 100, the track is in a PASS state. When the combined ! weight is less than 100, the track is in a FAIL state. ***Supported Platforms*** **NetVanta 1335, 3000 Series (except 3200/3205), 4305, 5305**
Track Control of ACLs	Access Control List entries may now be controlled by tracks by appending the 'track <TRACK-NAME>' keywords to the end of 'permit' or 'deny' statements. This is available for both Standard and Extended ACLs. ***Supported Platforms*** **NetVanta 1335, 3000 Series (except 3200/3205), 4305, 5305**
Diffie-Hellman Group 5	Added support for Diffie-Hellman Group 5, for use with IKE policies and IPSec Perfect Forward Secrecy (PFS). ***Supported Platforms*** **All Routers (Requires Enhanced Feature Pack)**

Crypto Map Idle-Time	VPN tunnels may be torn down before the expiration of the tunnel's hard lifetime, using the VPN Idle-Time option. If no data is received from a VPN peer within the time specified by the idle-time, the tunnel will be torn down. Any routes added to the IP route table by Reverse Route Injection will also be removed from the route table. From Crypto Map Config Mode, an Idle Time may be configured with the command 'set security-association idle-time <IDLE-TIME>'. (Note: The Idle Time value is measured in seconds.) ***Supported Platforms*** **All Routers (Requires Enhanced Feature Pack)**
H.323 ALG Timeout	Users may now configure the timeout value for H.323 signaling policy sessions. The default value is 8 hours. ***Supported Platforms*** **All Routers**

Errata

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

Services and Viewers

- **NetVanta 1335: Issuing the 'show interface switchport <interface-ID>' command may cause a reboot if the interface is a member of a Port Channel**
  - Description: When a Port Channel is enabled and interfaces are assigned to the channel, attempting to look at physical switchport statistics with the 'show interface switchport <interface-ID>' command may result in a reboot. The generic 'show interface' command will also cause a reboot to occur.
  - Workaround: No known workaround

Routing

- **NetVanta 1335: OSPF and BGP routing performance may suffer with large route tables**
  - Description: Performance appears to be affected when the route table approaches 3,000 OSPF routes or 10,000 BGP routes. Comparative testing indicates 64 byte and 256 byte packet throughput is considerably lower than a NetVanta 3305 with an OSPF or BGP route table of similar size. (1518 byte packet throughput is similar between platforms.)
  - Workaround: No known workaround

Network Interfaces and Quality of Service

- **NetVanta 5305: PPP or MLPPP interface may drop packets with over 24 RTP streams of traffic per T1**
  - Description: PPP or MLPPP may drop packets when more than 24 RTP streams per T1 are active. The problem only affects the NetVanta 5305 with Octal T1 Module. This does not affect routers with T1, Dual T1, or T1+DSX NIMs, nor does it affect the NetVanta 4305 with Octal T1 Module.
  - Workaround: No known workaround

- **G.SHDSL line rate may be invalid when changing from 4-wire to 2-wire**
  - Description: If the G.SHDSL interface line-mode is configured for 4-wire with a line-rate of 4608, and the line-mode is changed to 2-wire, then the line-rate will still be 4608 (which is invalid for 2-wire mode). This would prevent any QoS configuration from working properly, however it will still pass data in this state.
  - Workaround: Configure the line-rate for 2304 before changing from 4-wire to 2-wire.

VPN

- **Encryption errors may occur when terminating high number of VPN tunnels with heavy traffic**
  - Description: Units with VPN Accelerator Modules installed that terminate a high number of VPN tunnels (64+) with heavy traffic on the tunnels may experience errors in encryption. When such an error occurs, an event is displayed: "Internal error in udm_pkt_sync." The unit will recover from this error and continue encrypting/decrypting packets properly.
  - Workaround: Since the unit automatically recovers from the error, no action needs to be taken.

Wireless LAN

- **MAC ACL filtering on an Access Point does not work until the AP is rebooted**
  - Description: When a MAC ACL is applied to an AP interface, clients with MAC addresses not permitted by the ACL can still connect to the AP and pass traffic. The ACL only goes into effect after the AP is rebooted.
  - Workaround: Reboot Access Point(s) after configuring MAC ACLs.

Resolved Issues

These are issues that have been resolved since the previous AOS release (14.04.00).

Services and Viewers

- TFTP uploads to AOS devices may fail, with the error "Received Past Block ID."
- CLI: When a console session times out, the CLI may get stuck in a loop requesting users to "Press RETURN to get started" instead of providing the expected "hostname>" prompt.
- SSH with RADIUS authentication: When a RADIUS server rejects a user's login credentials, AOS continues to send requests to the server until the maximum retry value is reached.
- DHCP Server: AOS does not reliably send DHCP Offers when acting as the DHCP server for a remote network.
- Web GUI: The "Debug" page allows users to 'debug ppp packet', although this is not a valid debug.
- Config Files: There are two blank lines between eth 0/1 and VLAN 1 under the 'show ip interface' command. (NetVanta 3120)
- Config Files: Interface descriptions are omitted from the 'show interface' command on gigabit interfaces. (NetVanta 1524ST, NetVanta 1300 Series)

Switching and Bridging

- CLI: The help for the 'switchport port-security violation' command does not adequately describe the differences between 'protect' and 'restrict'.
- CLI: 'show vlan' help indicates that 'realtime' output is available, but it is not.
- When creating a Monitor Session, if you choose a source interface that does not exist, the unit will crash.
- The interface-level 'ip route-cache express' command overrides the global 'no ip route-cache express' command, making it difficult to disable Layer 3 switching once it has been enabled. (NetVanta 1335)
- The hardware route table supports 32 Layer 3 interfaces (VLANs), but there is no warning that the maximum has been surpassed if more than 32 VLAN interfaces are created. (NetVanta 1335)
- When a Port Channel is configured as an 802.1Q trunk, and more than one Ethernet interface in the channel is active, Native VLAN traffic is tagged, but should not be. (NetVanta 1335)
- The Monitor Session 'no-isolate' keyword does the opposite of what is expected. (NetVanta 3100 Series)

Routing

- CLI: The 'show track' command does not reflect tracks applied to static routes.
- The PacketRouting thread may become congested and lead to a reboot when debugging is enabled. (NetVanta

1335)

- Web GUI: Configuring the data field on the probe configuration leads to a URL that ends with #error. No error actually results, but the potentially confusing anchor name has been changed.
- ICMP Probes fail when type and code are specified in the associated Route-Map ACL.
- Deleting a track or probe from within that track or probe's configuration mode does not return users to Global Config Mode.
- Proxy ARP replies to ARP requests on interfaces without IP addresses.
- The 'clear arp-cache' command should only delete dynamic ARP entries, but deletes static and permanent entries as well.

Network Interfaces and Quality of Service

- Input/Output Rate statistics are incorrect on Modem Interface.
- Flow Control is not initialized properly on Modem Interfaces, causing CRC and Abort errors (NetVanta 3100 Series)
- Packets in the PPP Transmit Queue are not deleted when a PPP interface goes down, which can lead to reboots.
- Demand Interfaces retain negotiated IP addresses after the associated physical interface returns to "idle" if configured with 'ip address negotiated no-default' (does not affect interfaces without 'no-default' keyword).
- The 'interface range' command fails on gigabit-switchports.
- Changing the bandwidth statement on a PPP interface causes the interface to bounce.
- CLI: Users may configure secondary IP addresses on an interface that are identical to the interface's primary IP address.
- Changing T1 timeslot allocation for interfaces that are cross-connected to a Layer 2 protocol (PPP, HDLC, Frame Relay) may cause the Layer 2 protocol to drop and not come back up until the router is rebooted.
- Collisions on an interface can cause Ethernet interfaces to stop padding small frames to the minimum allowable size of 64 bytes. This affects ARP (in addition to other traffic types), which effectively means the interface locks up after devices on the LAN segment clear their ARP caches. (NetVanta 4305)
- DBU should not be a valid resource pool name on a Demand Interface because "DBU" is reserved for Legacy Dial Backup by AOS.
- When calculating the bandwidth available on an Ethernet or VLAN interface, QoS treats the 'bandwidth' interface command as if it were in bits per second instead of kilobits per second.
- Configuring two interfaces for IP Unnumbered to one another will cause routers to reboot.
- Administratively shutting down a Demand Interface while there is an active data call (both ISDN and Analog) for that interface causes a reboot.
- During periods of high traffic, the NetVanta 3130 ADSL interface may stop processing inbound traffic until the router is rebooted.
- Web GUI: From the DSX configuration page, clicking the "WAN-T1" link in the "DSX-1 Map" field returns a "404: Page Not Found" error page.

Firewall

- Firewall route lookups contain two memory leaks (most likely to be seen with very high traffic levels).
- The MSN Messenger ALG can cause routers to reboot.
- Web GUI: Using the up and down arrows to re-order port forwards with port translation causes the destination port to be set to 0.
- Web GUI: If no subnet mask is specified for source or destination address while modifying a port forward, the GUI returns a "503: Server Error" page instead of a warning message.
- Web GUI: There is a typo in the "General Firewall" page under "Access Control Lists" ("Allows you modify…" instead of "Allows you to modify…").

VPN

- Using both AH and ESP in the same IPSec Transform Set may lead to a reboot.
- Web GUI: Under "Certificates," the Web GUI fails to generate a valid Self Certificate Request when using Fully Qualified Domain Names as Subject Name identifiers.

System and Drivers

- Transferring files to Compact Flash may cause devices to reboot.
- Units may reboot without exception reports or core dumps, indicating that they were returned to ROM by "JTAG Reset." (NetVanta 3400 Series)
- When there is a high traffic volume on a switchport at the time of bootup, units may enter a continuous reboot cycle. (NetVanta 1335)
- A repair case was added to the Compact Flash filesystem to address a potential problem with an invalid first allocation unit.
- Heavy traffic loads may cause routers to lock up, requiring a manual reboot (NetVanta 3130, NetVanta 344).

AOS 15.02.00 Software Release

Release Notes **Date: 6/8/07**

Resolved Issues

- Making changes to modem interface configuration via the Web GUI when AAA is enabled leads to a "503: Server Error" page.
- Secondary IP addresses may not be added to an interface if the secondary IP address is in a network that overlaps with another IP address.
- OSPF does not converge reliably when configured on a Bridge Virtual Interface.
- MTU cannot be changed on routed Ethernet interfaces (NetVanta 3400 Series)
- The NetVanta 1335 only supports 128MB RAM modules, but should also support 256MB and 512MB modules (NetVanta 1335, NetVanta 1335 PoE).
- System generated e-mails are not sent if the SMTP server offers (but does not require) authentication, and the AOS device is not configured for authentication.
- Wireless configuration Web GUI pages are inaccessible on the NetVanta 3430.
- Collisions on routed Ethernet interfaces can cause the interface to stop transmitting packets. (NetVanta 3400 Series)
- The 'ip route-cache' command is not persistent after a reboot on Bridge Virtual Interfaces.
- If the G.SHDSL interface line-mode is configured for 4-wire with a line-rate of 4608, and the line-mode is changed to 2-wire, then the line-rate will still be 4608 (which is invalid for 2-wire mode).
- Fan noise may be excessive for small office environments. (NetVanta 3400 Series)
- Using VPN Reverse Route Injection (RRI) may cause routers to reboot.
- SIP ALG: When using a SIP Gateway on a private LAN, a callee on the private LAN may not be able to put an external caller on hold.
- SIP ALG: With two calls present, both initiated from the private LAN toward the WAN, the first external callee can hang up and a BYE message is passed through the private caller; however, the second external callee's BYE message is not passed through the firewall to the caller.
- The Setup Wizard deletes the PPP interface in the default config, resulting in an unusable configuration. (NetVanta 340)
- The Route Table Web GUI page displays a "503: Server Error" when a route is configured destined for a Null Interface.

AOS 15.05.00 Release Notes

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

Enhancements	Overview
Firewall Enhancements	Added ability to disable the IRC ALG. This can be accomplished using the command 'no ip firewall alg irc'. ***Supported Platforms*** **All Routers supporting AOS 15.05**

Errata

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

- **DNS Proxy does not use all configured name servers**
  - Description: When the NetVanta is used as a DNS Proxy with more than two configured name servers, only two name servers will be tried for each request. This will only be observed if requests to both name servers fail.
  - Workaround: No known workaround.
- **Abnormally terminated SSH sessions can not be terminated**
  - Description: If a link is lost while an SSH session is active, the session does not timeout and cannot be terminated. If this happens five times, SSH will be unresponsive until the unit has been rebooted..
  - Workaround: No known workaround.
- **One way audio during transfer when using the SIP ALG**
  - Description: NAT source ports are not preserved when a 183 Session Progress is processed by the SIP ALG, resulting in one-way audio during an attended transfer.
  - Workaround: No known workaround.
- **One way audio after retrieving a held call when using the SIP ALG**
  - Description: If the SIP ALG is in use and a call is placed on hold, then retrieved, one way audio will result if a Re-Invite is received for that call.
  - Workaround: No known workaround.

Resolved Issues

These are issues that have been resolved since the previous AOS release (15.02.00)

- When performing an SNMP walk, units will reboot if there is no startup configuration.
- Reboot caused by VPN Nat-Traversal Version 2.
- Cannot add multiple VLANs to a bridge-group.
- Inbound SIP calls using the SIP ALG experience one-way audio.
- Default Demand Route is removed from running configuration after Idle-timeout.
- Inbound SIP calls using the SIP ALG fail if port 5060 is port forwarded.
- NetVanta 5305 under heavy load may reboot.
- White highlight bar is missing from wireless configuration selections in the Web Interface.
- Showing the status of a Port Channel causes a reboot.
- HTTP probes are not successful.
- The web interface returns a 503 Server Error when trying to view VAP with PSK longer than 40 characters.
- A WPA preshared key is truncated to 40 characters when entered through the web interface.
- NetVanta 3100 Series only supports VLAN Ids up to 510.

- Reboot caused by ADSL NIM running firmware prior to version 10.
- Reboot caused by mis-configuration of Integrated Routing and Bridging.
- QoS maps applied inbound on a VLAN interface do no work.
- Event history does not show up in the web interface.
- The web interface does not properly setup bridging.
- A 503 server error is returned when accessing the port security settings of the Gigabit Ethernet ports of a NetVanta 1335.
- The sent time field is incorrect in logs forwarded by e-mail.
- Local Preference is not taken into consideration when BGP devises a path to a network.
- Removing a VLAN interface and then modifying a QoS map that was applied to that VLAN interface will cause a reboot.
- Unable to change QoS map bandwidth or priority setting while applied to a VLAN interface.
- The domain name is not appended to a DNS query originated from the NetVanta if the original query fails.
- Issuing the command 'show crypto IPSec sa' with hundreds of IKE tunnels causes a reboot.
- Cannot set the speed of a switchport on a NetVanta 1524 to 1000Mbps with the web interface.
- Creating an 802.1q sub-interface with the web interface of a NetVanta 3448 causes the unit to reboot.

AOS 15.07.00 Release Notes

Release Notes **Release Date: November 5, 2007** **Notes Revision: 11/6/2007**

Resolved Issues

These are issues that have been resolved since the previous AOS release (15.05.00)

- If a link is lost while an SSH session is active, the session does not timeout and cannot be terminated
- If the SIP ALG is in use and a call is placed on hold, then retrieved, one way audio will result if a Re-Invite is received for that call.
- Connected routes with a 31-bit or 32-bit subnet mask are not redistributed into BGP.
- 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.
- SNMP Link Down Traps do not include the instance portion of the OID resulting in inconclusive reporting of alarms by some SNMP agents.

AOS 15.08.00 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 (15.07.00)

TACACS+ Session maintained whenever console is logged out.

Port security on a NV1524 causes the port to stop passing traffic when a single sticky mac-address is defined.

AOS 15.09.00 Release Notes

Release Notes **Release Date: January 31, 2008** **Notes Revision: 2/29/2008**

Resolved Issues

These are issues that have been resolved since the previous AOS release (15.08.00)

Setup Wizard in the web GUI will hang when loading the routing page.

Ethernet not responding in Frame Relay Unnumbered Config when the 'ip unnumbered' command was issued before configuring the DLCI value.

Demand interface dial string does not honor all ASCII characters.

Frame Relay Fragmentation not accepting Begin and End bit of a Frame Relay header when the frame length is less than the MTU

HDLC Interface statistics not retrieved with SNMP Walk

AOS 15.10.00 Release Notes

Release Notes **Release Date: December 1, 2008** **Notes Revision: 12/2/2008**

Resolved Issues

These are issues that have been resolved since the previous AOS release (15.09.00)

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

The Web GUI returns an error when users attempt to add a secondary IP address to an interface that is configured as the IP unnumbered source of another interface.

When bridging is configured, changing a PPP interface through the GUI to MLPPP, and then proceeding to add a second T1 to the MLPPP bundle can cause the unit to reboot.

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

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

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

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.

AOS 15.11.00 Release Notes

Release Notes **Release Date: June 16, 2009** **Notes Revision: June 17, 2009**

Resolved Issues

These are issues that have been resolved since the previous AOS release (15.10.00)

Multiple-value GET-BULK SNMP requests may return incorrect values.

AOS 15.12.00 Release Notes

Release Notes **Release Date: June 28, 2010** **Notes Revision: June 28, 2010**

Resolved Issues

These are issues that have been resolved since the previous AOS release (15.11.00)

Performing an SNMP GET using the ifPhysAddress OID may return an integer value of "1" instead of a string value of the MAC address.

Using the up/down arrow keys within the CLI under specific circumstances may cause the AOS device to reboot.

Failed SNMP GETs may cause a memory leak leading the NetVanta device to reboot.