AOS 18.01.01.00 Release Notes

Release Notes **Release Date: Mar. 7, 2011** **Notes Revision: Mar. 7, 2011**

Introduction

NetVanta Series products support application image updates via the ADTRAN OS Web GUI, TFTP, X-Modem, and FTP. A detailed firmware upgrade guide with step-by-step instructions is available at: http://kb.adtran.com/article.asp?article=1630&p=2.
Prior to upgrading firmware, please ensure that your unit meets the minimum Boot ROM requirements, listed under "Supported Platforms."

Supported Platforms

	Standard Feature Pack	Enhanced Feature Pack	Minimum Boot ROM****
NetVanta 1234/1238	9700594-2A180101.biz	N/A	17.03.02.SB
NetVanta 1534	9700590-2A180101.biz	N/A	17.06.03.00
NetVanta 1534 2nd Gen.	9702590-2A180101.biz	N/A	17.08.01.00
NetVanta 1534P 2nd Gen.	9702590-2A180101.biz	N/A	17.09.01.00
NetVanta 1544/1544F	9700544-2A180101.biz	N/A	17.06.03.00
NetVanta 1544 2nd Gen.	9702544-2A180101.biz	N/A	17.08.01.00
NetVanta 1544P 2nd Gen.	9702544-2A180101.biz	N/A	17.09.01.00
NetVanta 1638	9700568-2A180101.biz	N/A	18.01.01.00
NetVanta 1638P	9700569-2A180101.biz	N/A	18.01.01.00
NetVanta 1335	N/A	9950515-2A180101.biz	15.01.00
NetVanta 3120	N/A	9700600-2A180101.biz	14.04.00
NetVanta 3130	N/A	9700610-2A180101.biz	14.04.00
NetVanta 3200/3205 (3rd Gen.)*	9200860-2A180101.biz	9950860-2A180101.biz	17.02.01.00
NetVanta 3305	9200880-2A180101.biz	9950880-2A180101.biz	04.02.00
NetVanta 3430	9200820-2A180101.biz	9950820-2A180101.biz	13.03.SB
NetVanta 3430 2nd Gen.	9202820-2A180101.biz	9952820-2A180101.biz	17.05.01.00
NetVanta 3448	9200821-2A180101.biz	9950821-2A180101.biz	13.03.SB
NetVanta 3450	9200823-2A180101.biz	9950823-2A180101.biz	17.06.01.00
NetVanta 3458	9200824-2A180101.biz	9950824-2A180101.biz	17.06.01.00
NetVanta 4305* **	9200890-2A180101.biz	9950890-2A180101.biz	08.01.00
NetVanta 4430	9700630-2A180101.biz	9950630-2A180101.biz	17.04.01.00
NetVanta 5305	9200990-1A180101.biz	9950990-1A180101.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.
***1st generation NetVanta 4305 (Part number 1200890L1) 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	
IPv6	IPv6 is the next generation of Internet protocols designed to replace IPv4. AOS implements this feature by incorporating one stack for IPv4 use and one stack for IPv6 use, often referred to as dual-stack, which can be run independently or in parallel. This allows for single feature upgrades from IPv4 to IPv6, as well as a method of transitioning from IPv4 to IPv6 on the network.	
	Supported Platforms	**2nd Gen NetVanta 3430, NetVanta 3448, NetVanta 3450, NetVanta 3458, NetVanta 4430, NetVanta 5305**
Strict Rate Policing	This AOS feature adds the ability to drop priority traffic that exceeds a specified limit, even when the egress interface is in a non-congested state.	
	Supported Platforms	**NetVanta 1335, NetVanta 3305, NetVanta 3430, NetVanta 3448, NetVanta 3450, NetVanta 3458, NetVanta 4305, NetVanta 4430, NetVanta 5305**
Backup Path Testing	This AOS feature uses demand routing, policy-based routing, and network monitoring to schedule a test of the backup path of a network. The feature allows the test to be scheduled, and allows a user to specify parameters to keep the test from running while the backup link is in use to ensure it does not adversely affect the network.	
	Supported Platforms	**NetVanta 1335, NetVanta 3200, NetVanta 3205, NetVanta 3305, NetVanta 3430, NetVanta 3448, NetVanta 3450, NetVanta 3458, NetVanta 4305, NetVanta 4430**

Enhancements	Overview	
PoE+	This AOS enhancement will now support a higher power version of PoE (802.3at). With PoE+ support, switches will be able to provide a maximum of 25.5 Watts on a given port and have the ability to power class 4 devices.	
	Supported Platforms	**2nd Gen NetVanta 1534P, 2nd Gen NetVanta 1544P, NetVanta 1638P**
Generic USB Modem Support	This AOS enhancement provides a generic implementation to detect and utilize 3G USB modems. AOS will attempt to automatically detect GSM or CDMA-based USB modems from Novatel, Sierra Wireless, and Huawei.	
	Supported Platforms	**NetVanta 1335, NetVanta 3305, NetVanta 3430, NetVanta 3448, NetVanta 3450, NetVanta 3458, NetVanta 4305, NetVanta 4430**
4-Byte ASN Support for BGP	This AOS enhancement in BGP will now support configurations where the ASN is required to be 32-bits (4-bytes). This is in addition to the 16-bit (2-byte) ASNs that are currently supported.	
	Supported Platforms	**NetVanta 1335, NetVanta 3305, NetVanta 3430, NetVanta 3448, NetVanta 3450, NetVanta 3458, NetVanta 4305, NetVanta 4430, NetVanta 5305**
BGP-4 MIB Support	AOS now provides BGP-4 MIB support to be used for adjacency monitoring in BGP networks.	
	Supported Platforms	**NetVanta 1335, NetVanta 3305, NetVanta 3430, NetVanta 3448, NetVanta 3450, NetVanta 3458, NetVanta 4305,**

		NetVanta 4430, NetVanta 5305
OSPF-4 MIB Support	AOS now provides OSPF-4 MIB support to be used for adjacency monitoring in OSPF networks.	
	Supported Platforms	**NetVanta 1335, NetVanta 3305, NetVanta 3430, NetVanta 3448, NetVanta 3450, NetVanta 3458, NetVanta 4305, NetVanta 4430, NetVanta 5305**
Increased SIP Buffer Size	AOS now supports a larger SIP buffer size which will allow routers to support more than 4 BLF lines in applications using Transparent SIP Proxy.	
	Supported Platforms	**NetVanta 1335, NetVanta 3430, NetVanta 3448, NetVanta 3450, NetVanta 3458, NetVanta 4305, NetVanta 4430, NetVanta 5305**

Errata

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

- The web GUI for the 5305 may display "Unknown" for the logical link status on the System Summary page, even though the PPP link is up.
  - Workaround: View the status in the CLI.
- VRF names containing spaces or other special characters may not restore correctly upon a reboot.
  - Workaround: Do not use VRF names with spaces or special characters.
- The statistics rate interval may not be modified to another value besides the default 5 minute interval.
  - Workaround: View statistics using the 5 minute interval.
- The output counters on a BVI interface may be inaccurate.
  - Workaround: No known workaround.
- When a frame-relay sub-interface is inactive or not cross-connected, the status may be incorrectly displayed as "IN LOOPBACK" in the output of 'show ip interface brief' in the CLI.
  - Workaround: This is a display issue.
- The output of 'show connection' may display invalid information when configured for PPP over Frame-relay.
  - Workaround: This is a display issue.
- A spanning tree broadcast storm lasting several hours may cause a reboot.
  - Workaround: Prevent spanning-tree loops and enable storm-control.
- The transmit and receive counters on a PPP interface may be inaccurate when using PPP over Frame-relay.
  - Workaround: No known workaround.
- The BGP 'maximum-paths <number of paths>' command may not allow multiple equal-cost paths to be added to the route table.
  - Workaround: No known workaround.
- A network monitor track may not be associated with an interface using the NetVanta 1638 web GUI.
  - Workaround: Associate the track and interface using the CLI.
- The debug command, 'debug ipv6 nd ar' may not generate any output.
  - Workaround: Use the debug command, 'debug ipv6 nd neighbor.'
- Enabling the 'port-authentication maximum requests' feature may not limit authorization attempts from an unauthorized supplicant.
  - Workaround: No known workaround.
- The 'no arp arpa' command may not block outbound ARPA-type requests.
  - Workaround: No known workarounds.
- The output of 'show dos counters' may show negative values.
  - Workaround: Clear the DoS counters to view the true values.
- On the 1638, the left management LED may blink green when it is supposed to be solid green to show link, and the right LED may not function.

- Workaround: No known workarounds.
- The 3305 may not display any LLDP neighbors.
  - Workaround: No known workarounds.
- The "refresh" button on the PoE page of the NetVanta 1638 web GUI may need to be clicked twice to disable the automatic refreshing of PoE statistics.
  - Workaround: Click the "refresh" button twice.
- The NetVanta 1638 may display incorrect LLDP peer information for neighbors connected over a 20 Gbps (2x10Gbps) port-channel.
  - Workaround: No known workarounds.
- In resetting the policy-timeouts, the "seconds" parameter may be required instead of accepted at the end of the 'no ip policy-timeout <udp/tcp>' command.
  - Workaround: Include the "seconds" parameter in the command.
- Manually entered duplicate IPv6 link-local addresses may show up in Neighbor Solicitation (NS) or Neighbor Advertisement (NA) messages even though duplicate address detection (DAD) has failed.
  - Workaround: Do not manually enter duplicate IPv6 link-local addresses.
- The 'show usb attached-devices' command may appear in the CLI even though there are no USB ports.
  - Workaround: No known workaround. Command is not functional.
- The CLI may allow IPv6 ND options under the 'ipv6 nd' command subset to be entered in multiple times.
  - Workaround: Enter each preferred option once.
- The command, 'show spanning-tree detail' may display incorrect Port IDs for frame-relay sub-interfaces.
  - Workaround: This is a display issue.
- Ping options in IPv6 may not be removed from the command options list after they are entered.
  - Workaround: This is a display issue.
- Shutting an Ethernet interface down that is associated with a BVI interface, may cause the BVI interface to go down.
  - Workaround: No known workaround.
- Rebooting an integrated switch/router AOS device while traffic is routing between VLAN interfaces may prevent traffic from flowing once the device has booted.
  - Workaround: Stop traffic flow between VLAN interfaces before rebooting device.
- Extra zeroes may appear in the output of 'debug rip events' on the 1638.
  - Workaround: This is a display issue.
- The NetVanta 1638 may send an incorrect source IP address in its SNMP packets.
  - Workaround: No known workaround.
- When viewing the web GUI using Windows 7, some of the entry boxes may be misaligned on the Access Point configuration page.
  - Workaround: This is a display issue.
- On the NetVanta 1638, the DHCP client information under the Network Forensics web GUI page may not contain the server MAC address.
  - Workaround: Information can be viewed through the CLI.
- Having a track name that is longer than 20 characters may cause a 503 server error when browsing to the Network Monitor configuration page in the web GUI.
  - Workaround: Use a track name that contains less than 20 characters.
- An AOS device may not always send port-authentication replies causing valid supplicants to be unauthorized.
  - Workaround: Attempt to authenticate again.
- The AOS device may drop GVRP packets when first configured.
  - Workaround: Bounce the uplink connections.
- On the Netvanta 1335 w/ WiFi, browsing from "Port Security" configuration page to the "Switchports"configuration page may cause a 503 server error.
  - Workaround: Switchports configuration page on the web GUI can be viewed by browsing from another point in the web GUI.
- The web GUI on the 2nd Gen 1544 may not reflect when a TACACS server is being used to authenticate FTP.
  - Workaround: This information can be viewed in the CLI.
- AWCP may show as a configurable option under the gigabit-switchport command set on an AOS switch.
  - Workaround: AWCP is configurable from the VLAN interface.

- Downloading the configuration from the web GUI may misalign the configuration.
  - Workaround: This is a display issue.
- LLDP may not function on interfaces where 802.1q is enabled.
  - Workaround: No known workaround.
- The NetVanta 1638 may output the following message “Failed to initialize semaphore” while in an idle state.
  - Workaround: No known workaround.
- The output of ‘debug ntp’ may produce an output in hexadecimal characters instead of decimal digits.
  - Workaround: No known workaround.
- 802.1x may not allow RADIUS servers to dynamically assign VLANs to supplicants.
  - Workaround: Manually assign VLANs.
- An AOS product may reboot after several failed 802.1x authentication attempts when using a RADIUS server.
  - Workaround: Do not allow RADUS servers to dynamically assign VLANs to supplicants.
- The command, ‘no storm-control all-types’ is missing from the CLI.
  - Workaround: Disable storm-control types individually.
- The NetVanta 1335 w/WiFI may reboot after a call has been made using the WWAN NIM.
  - Workaround: No known workaround.
- Xmodem transfers on a NetVanta 1638 may generate bad checksums.
  - Workaround: Upload bootcode using TFTP. Upload firmware using web GUI or TFTP.

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.09.02)

Services and Viewers

- The NTP hardware and software clock on an AOS device may drift resulting in event messages stating, “NTP frequency error -500 PPM exceeds tolerance of 500 PPM.”
- Issuing the command "show tech" simultaneously from two separate sessions may cause the unit to lockup.
- The DHCP server may incorrectly respond to a DHCP Request message from a client that it already gave an address to on a different interface.
- When a large number of DHCP pools are configured, issuing the ‘show run’ command may cause the unit to become unresponsive for a period of time.
- “ClusterInternaMember” may be displayed as an interface in the “IP Interfaces” page of the web GUI.
- SSH access may lock up when large amounts of data are being sent to a client from an AOS device.
- Administrative access may be lost if the space bar is hit followed by CTRL+W at the enable prompt.
- The self-signed HTTPS certificate will now be based off the SHA1 algorithm as opposed to the MD5 algorithm.
- The CLI may allow a user name in SNMP to be set that is also being used as a community name.

- Netflow may incorrectly reference Ethernet sub-interfaces by always referencing the first sub-interface.
- DNS servers that are learned via DHCP may not be removed if the DHCP client renews a lease that has modified DNS settings.
- The System page in the Web GUI will display a 503 error if there is a PPP interface present and the Ethernet interface was chosen as the public interface in the Setup Wizard.
- Using the HTTP secure server to access the web GUI on a non-standard port may cause a memory leak.
- The demand interface may not be populated in the web GUI interface assignment list.
- Issuing a 'shut' command on an HTTP or TCP probe may not cause a state change. This is inconsistent with ICMP probes which will transition to a "PASS" state when administratively shutdown.
- Setting a ping probe period to greater than 2147 seconds may cause a flood of ping packets to be transmitted.

Routing, Switching and Bridging

- Loopback interfaces may not be populated in the Layer 3 hardware table.
- Bridged frames across a PPP link with the "LAN FCS" bit set were given an extra CRC, which can cause an invalid packet to be transmitted and may result in errors.
- On the 123x switches, if port security with sticky MAC addresses is used, the sticky MAC addresses may be removed after a certain period of time.
- Issuing the command 'set metric 0' within a route-map may not be displayed in the running-configuration.
- In the 123x switch GUI, the "Default Gateway" link may be missing.
- Issuing the 'show mac address-table dynamic' command may cause a reboot.
- The Web GUI may display a switchport speed as "10 Mbps / full" even if it has been manually set to "2500 Mbps / full" in the CLI.
- Under very high traffic loads, Spanning-tree may enter a state where it is unable to transmit BPDUs which may result in a reboot.
- BGP may not re-advertise a local route if the AOS device's corresponding local interface bounces.
- The BGP and OSPF "maximum-path" CLI option may incorrectly appear on AOS Layer 3 switches.
- When stacking is configured, the stacking VLAN may not come up after the switchport stack mode is modified on a stack member.
- Traffic may not pass over a link that is configured to bridge over Frame-Relay.
- Under certain conditions, an AOS device which has 802.1x configured may allow an unauthorized supplicant, which is authenticating using an incorrect password, to pass traffic.
- Configuring stacking may cause the AOS device to reboot.
- Using HDLC to do bridging with IRB may cause a reboot.
- Loopback interface addresses with 32-bit subnet masks may not be properly redistributed into OSPF or RIP when 'redistribute connected' is specified.
- Port-channels which are in a spanning-tree "blocking" state may not be displayed in the spanning-tree database.
- Issuing the 'no ip routing' on an AOS switch/router combo unit may not disable routing through the default gateway or to another connected subnet.
- Routing unicast traffic destined for a very large number of hosts residing in a directly connected subnet may cause a reboot.
- If an AOS device learns a route from both an internal and external BGP neighbor with an AS_PATH attribute that differs only by the next-hop address, the first route determined to have the best path may be used, even if a better route is learned later.

Network Interfaces and Quality of Service

- When PPP fragmentation is enabled, fragments may traverse the same link instead of being transmitted equally between all the links.
- A PPP interface may get stuck in loopback if the far end transmits LCP frames that do not include "magic numbers."
- When configuring 'match-all' QoS maps in the CLI, an invalid error message of, "%Cannot add multiple 'match

dscp' statements to a map with 'match-all' enabled." may be displayed.

- Configuring a QoS map to match on an ACL that has a space in its name may disappear upon a reboot.
- When 'service password-encryption' is enabled, a username or password configured for a PPP connection may display in clear text when it should be encrypted.
- A QoS map that is matching a DLCI value may display an invalid error stating, "%Can only assign this QoS map to a frame relay interface." when applied to a frame-relay interface.
- The WWAN NIM may not recognize the Verizon USB760 USB modem.
- Adding multiple cross-connect statements for TDM-groups that are part of the same T1 on an octal NIM may cause a reboot.
- Configuring ATM with routed-bridged sub-interfaces while the firewall or ip crypto is enabled may cause a reboot.
- The bandwidth command may be displayed twice under the PPP interface configuration in the CLI.
- When doing PPPoE with authentication, CHAP/PAP packets that contain extra padding may be discarded causing the connection to not fully establish.
- The NetVanta 3120/3130 may fail to answer incoming calls on the DBU interface.
- The 3G and WWAN NIM may stop responding resulting in the error message on the demand interface that states, "No data call resource."
- Deleting an ATM interface in AOS may cause the device to reboot.
- Configuring the demand interface through the web GUI may erroneously set the MTU to 0.
- LLDP may not be able to be disabled on the native VLAN of an Ethernet interface acting in 802.1q mode.
- When issuing the 'debug interface adsl events' command, the following output may be displayed, "ADSL.EVENTS: AdslDrv: WARNING!!! Memory Priority is not correctly set!"
- The PPP output queue in a PPPoE configuration may get into a state where it starts "holding" packets resulting in increasing latency in the network.
- When configuring PPP authentication, the CLI may not display an error message when the command 'password encrypted <password>' is entered and may appear as if it was accepted.

Firewall and VPN

- On a re-INVITE where both the remote IP and port number have changed, the SDP information is not properly processed by the SIP ALG, which may create an invalid policy session and result in one-way or no audio.
- Policy-sessions created using an 'allow' policy-class entry may not be cleared when 'fast-nat-failover' is enabled.
- When using the SIP proxy, if the soft switch is using a port other than 5060 for SIP, the Contact header in a 200 OK may get updated with the wrong port when the 200 OK is sent to the phone.