AOS 17.05.01.00 Release Notes

ADTRAN

Release Notes	Release Date: April 13, 2009	Notes Revision: April 13, 2009

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*****	9700594-2A170501.biz	N/A	17.03.01.00
NetVanta 1238*****	9700594-2A170501.biz	N/A	17.03.01.00
NetVanta 1534	9700590-2A170501.biz	N/A	17.03.01.00
NetVanta 1544	9700544-2A170501.biz	N/A	17.05.01.00
NetVanta 1335	N/A	9950515-2A170501.biz	15.01.00
NetVanta 3120	N/A	9700600-2A170501.biz	14.04.00
NetVanta 3130	N/A	9700610-2A170501.biz	14.04.00
NetVanta 3200/3205 (3rd Gen.)*	9200860-2A170501.biz	9950860-2A170501.biz	17.02.01.00
NetVanta 3305**	9200880-2A170501.biz	9950880-2A170501.biz	04.02.00
NetVanta 3430	9200820-2A170501.biz	9950820-2A170501.biz	13.03.SB
NetVanta 3430 2nd Gen.	9202820-2A170501.biz	9952820-2A170501.biz	17.05.01.00
NetVanta 3448	9200821-2A170501.biz	9950821-2A170501.biz	13.03.SB
NetVanta 4305***	9200890-2A170501.biz	9950890-2A170501.biz	08.01.00
NetVanta 4430	9700630-2A170501.biz	9950630-2A170501.biz	17.04.01.00
NetVanta 5305	9200990-1A170501.biz	9950990-1A170501.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.
*****This version of firmware will not be released for the NetVanta 1234 and 1238 series.

New Features	Overview
L3 Switching on NV 1544	Layer 3 switching for NetVanta 1544. Provides enterprise class multilayer gigabit Ethernet switching, supporting up to 1,000 routes in hardware. *Supported Platforms* **NetVanta 1544**
Network Monitor / Port Scheduler	The Port Scheduler feature allows system administrators to configure ADTRAN switch products to automatically activate and deactivate switchports based on the time of day. *Supported Platforms* **NetVanta Switch Products, including NetVanta 1234, 1238, 1335, 1534, and 1544**
Security Dashboard	The Security Dashboard provides a general overview of network security status that allows the user to quickly and easily assess security threats and firewall status. The AOS Security Dashboard feature has been designed as a visual representation of the network security threats blocked by the AOS firewall. *Supported Platforms* **NetVanta 1335, NetVanta 3200/3205, NetVanta 3305, NetVanta 3400 Series, NetVanta 4000 Series, and NetVanta 5305**

Enhancements	Overview
Enhanced Ethernet QoS for FR, HDLC and ATM	Class-Based Traffic Shaping is supported on Ethernet interfaces and an enhancement has been added to incorporate Frame-Relay, HDLC and ATM. Some of the benefits of enhanced QoS are that a class can be an interface, VLAN, or any case that can be matched in a QoS map. 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 several 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. The 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 1335, NetVanta 3200/3205, NetVanta 3305, NetVanta 3400 Series, NetVanta 4000 Series, and NetVanta 5305**
IGMP Snooping	Internet group management protocol (IGMP) snooping is a way to take advantage of IGMP packets flowing through a switch to reduce unnecessary flooding of multicast traffic. Since multicast traffic isn't automatically learned by switch hardware, the switch must flood the multicast traffic out all its ports in the virtual local area network (VLAN) to ensure that a subscribed client receives the traffic. By using information learned by snooping IGMP packets, the Adtran unit can build a multicast address table and reduce the amount of flooding. This will allow multicast traffic to be forwarded only to ports on which multicast subscribers or multicast routers have been snooped using the IGMP protocol. This feature is now also available on the NetVanta 1234, 1238, and 1534. *Supported Platforms* **NetVanta 1234, NetVanta 1238, NetVanta 1534**

NQM MIB	This addition of the Network Quality Monitoring MIB will allow management platforms to access NQM capabilities via SNMP.
	Supported Platforms **NetVanta 1335, NetVanta 3200/3205 (3rd Gen), NetVanta 3305, NetVanta 3400 Series, NetVanta 4000 Series, and NetVanta 5305**
Mobile IP user profile	This adjustable setting will allow users to modify the user profile settings for 3G NIMs so that they can support private network connections over the EV+DO networks.
	Supported Platforms **All platforms that support the 3G NIMs**
2.5 Gbps SFP Transceiver Support	Addition of support for Singlemode and Multimode SFP Transceivers capable of running at speeds up to 2.5 Gbps.
	Supported Platforms **NetVanta 1544**

Errata

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

- Issuing a 'show run interface ethernet 0/1 verbose' on a NetVanta 3120 causes the unit to reboot.
    - o <u>Workaround</u> – Use the 'show run interface ethernet 0/1' command.

- If there is a network situation where Spanning Tree topology changes happen frequently or constantly, the NetVanta 1544 may not keep L3 switching entries in its hardware, as these entries have to be completely flushed and then rebuilt any time there is a topology change. This may result in poor routing performance, and packets being dropped.
    - o <u>Workaround</u> – No known workaround.

- Port Mirroring on the NetVanta 1234, 1238, 1534, and 1544 does not include traffic sourced by the switch's CPU.
    - o <u>Workaround</u> – Use and external device to perform the port mirror if traffic sourced from the switch needs to be included.

- NetVanta 1335 may remove and/or add VLANs propagated by GVRP when unit is under heavy load.
    - o <u>Workaround</u> – Manually configure the VLANs.

- Changing the destination port for Port Mirroring in the GUI from "Destination" to "Disabled" returns a 503 Server Error.
    - o <u>Workaround</u> – Make Port Mirroring changes via the CLI.

- The NetVanta 1544 may reboot if the Bridge MIB is queried via SNMP to return the mac-address table and if a change in the table occurs simultaneously.
    - o <u>Workaround</u> - No known workaround.

- The Setup Wizard in the NetVanta 3120 freezes and has to be restarted if certain configurations are attempted.
    - o <u>Workaround</u> – Configure the unit without the Wizard.

- Under bursty traffic conditions, frames being switched by the NetVanta 1534 or NetVanta 1544 may be dropped. When this occurs, input discards will increment on the interfaces.
    - o <u>Workaround</u> – No known workaround.

- Issuing the command 'ip sntp server source-interface' on a NetVanta 4430 causes the unit to reboot.
  - <u>Workaround</u> – No known workaround.

- Upon boot-up, a block of 8 ports on a NetVanta 1238 may not function.
  - <u>Workaround</u> – Reboot the unit.

- SCP transfers fail when using WinSCP client.
  - <u>Workaround</u> – Transfer via FTP.

- A very small number of discards can be noted on interfaces on the NetVanta 1544. This amount is insignificant compared to the number of transferred packets, and should not disrupt traffic.
  - <u>Workaround</u> – No known workaround.

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.04.03)

Services and Viewers

- The setup wizard in the GUI does not allow the selection of VLAN interfaces as a Private or LAN interface.
- The output of 'show output-startup' is truncated before all information is displayed.
- Output of the "Input Packets" field from the 'show interface x' command is incorrect on a NetVanta 1534.
- Output of the "Output Packets" and "Output Bytes" fields from the 'show interface VLAN x' command is incorrect on the NetVanta 123x series.
- The AOS device may freeze upon boot-up if a 'run-tcl script' command is present in the startup-config.
- Deleting and adding VLAN interfaces can cause the device to incorrectly report those VLAN interfaces through SNMP.
- A WiFi PSK that contains space characters will not be inputted correctly after a reboot.
- ADSL interface/NIM firmware can not be upgraded directly from CFLASH.
- When 'tacacs-server host' entries are configured, they get arbitrarily reordered. They are not added to the configuration in the order entered, which can cause the ability to load balance between servers to not function properly.
- The unit may fail to boot upon initial boot-up, if there is any type of traffic being generated on the Ethernet port before Application code is loaded.

Routing, Switching and Bridging

- When redistributing routing protocols bidirectionally, such as BGP into OSPF and OSPF into BGP, the routing table may lock up, until the unit is rebooted.
- The AOS device may reboot if a new IP address is assigned to a PPP interface that is part of a Bridge group.

Network Interfaces and Quality of Service

- SHDSL NIM is unable to pass unfragmented packets larger than 1458 bytes.
- The NetVanta 3130 may reboot if the ADSL circuit is dropping cells at the end of an AAL5 frame.
- VQM may cause a reboot if two different streams use the same SSRC.
- If the NetVanta 4305's Ethernet port is negotiating to 100Mbps Half-duplex but the other end of link is hard-set to 100Mbps Full-duplex, prolonged transfers of data may cause the unit to stop transmitting traffic on that interface.
- Help text reflects 100Mbps as the maximum traffic-shape rate on a Gigabit interface, when the interface can actually traffic-shape up to 1Gbps.
- QoS policies are allowed to be applied to interfaces that have 'no fair-queue' applied (making the queuing method for the interface FIFO), which is misleading, as QoS will have no effect on a FIFO interface.

Firewall and VPN

- VPN tunnels will fail to come up to another device when initiated by the NetVanta VPN device, if the crypto map lifetime is set between 32768 and 65535 seconds.
- If Auto-link is enabled and configuration is saved through the GUI, the AOS device may lockup while updating the N-command MSP server.
- URL filtering applied outbound on an interface may cause HTTP/XML SEARCH packets to not traverse the firewall properly.
- If certain IKE aggressive mode parameters are mis-configured, the AOS device may reboot.
- Certain soft VoIP clients fail to add a 'rinstance' parameter to the contact field inside the contact brackets when registering an extension, causing incorrect call routing by the SIP Proxy.

AOS 17.05.01.00.SA Release Notes

Release Notes	Release Date: May 4, 2009	Notes Revision: May 4, 2009

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	9700594-2A170501.biz	N/A	17.03.01.00
NetVanta 1238	9700594-2A170501.biz	N/A	17.03.01.00

*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

New Features	Overview
Network Monitor / Port Scheduler	The Port Scheduler feature allows system administrators to configure ADTRAN switch products to automatically activate and deactivate switchports based on the time of day. ***Supported Platforms*** **NetVanta Switch Products, including NetVanta 1234, 1238, 1335, 1534, and 1544**

Enhancements — Overview

Enhancements	Overview
IGMP Snooping	Internet group management protocol (IGMP) snooping is a way to take advantage of IGMP packets flowing through a switch to reduce unnecessary flooding of multicast traffic. Since multicast traffic isn't automatically learned by switch hardware, the switch must flood the multicast traffic out all its ports in the virtual local area network (VLAN) to ensure that a subscribed client receives the traffic. By using information learned by snooping IGMP packets, the Adtran unit can build a multicast address table and reduce the amount of flooding. This will allow multicast traffic to be forwarded only to ports on which multicast subscribers or multicast routers have been snooped using the IGMP protocol. This feature is now also available on the NetVanta 1234, 1238, and 1534. ***Supported Platforms*** **NetVanta 1234, NetVanta 1238, NetVanta 1534**

Errata

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

- Port Mirroring on the NetVanta 1234, 1238, 1534, and 1544 does not include traffic sourced by the switch's CPU.
  - <u>Workaround</u> – Use and external device to perform the port mirror if traffic sourced from the switch needs to be included.

- Changing the destination port for Port Mirroring in the GUI from "Destination" to "Disabled" returns a 503 Server Error.
  - <u>Workaround</u> – Make Port Mirroring changes via the CLI.

- Upon boot-up, a block of 8 ports on a NetVanta 1238 may not function.
  - <u>Workaround</u> – Reboot the unit.

- SCP transfers fail when using WinSCP client.
  - <u>Workaround</u> – Transfer via FTP.

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.04.03)

Services and Viewers

- The setup wizard in the GUI does not allow the selection of VLAN interfaces as a Private or LAN interface.
- The output of 'show output-startup' is truncated before all information is displayed.
- Output of the "Output Packets" and "Output Bytes" fields from the 'show interface VLAN x' command is incorrect on the NetVanta 123x series.
- The AOS device may freeze upon boot-up if a 'run-tcl script' command is present in the startup-config.
- Deleting and adding VLAN interfaces can cause the device to incorrectly report those VLAN interfaces through SNMP.
- A WiFi PSK that contains space characters will not be inputted correctly after a reboot.
- When 'tacacs-server host' entries are configured, they get arbitrarily reordered. They are not added to the configuration in the order entered, which can cause the ability to load balance between servers to not function properly.
- The unit may fail to boot upon initial boot-up, if there is any type of traffic being generated on the Ethernet port before Application code is loaded.

Network Interfaces and Quality of Service

- Help text reflects 100Mbps as the maximum traffic-shape rate on a Gigabit interface, when the interface can actually traffic-shape up to 1Gbps.
- QoS policies are allowed to be applied to interfaces that have 'no fair-queue' applied (making the queuing method for the interface FIFO), which is misleading, as QoS will have no effect on a FIFO interface.

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.05.01.00)

Issuing a 'show run interface ethernet 0/1 verbose' on a NetVanta 3120 can cause the unit to reboot.

Issuing the command 'ip sntp server source-interface' on a NetVanta 4430 may cause the unit to reboot.

After disabling Port Mirroring using the "no monitor session 1" command, this feature may not work again until the unit is rebooted.

Referencing the MSP server by hostname causes the Auto-link client to fail to connect with the server.

NetVanta 123x PoE switches will not provide power to Ruckus PoE Wifi access points.

Adding a second T1 to an already existent unnumbered MLPPP interface may cause loss of IP connectivity to the interface referenced by the 'ip unnumbered' command..

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

In the CLI, the help text for the "traffic-shape rate" command on a Gigabit interface incorrectly specifies the maximum traffic-shape rate that can be set as 100 Mbps.

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.05.02.00)

SNMPv3 polls can fail when SHA authentication and DES encryption are used.

The PPTP ALG can improperly create an active GRE association which may cause the session to incorrectly timeout.

Using the 'nonegotiate' command when defining a static speed setting on a Fiber connection of a NetVanta 1534 or 1544 switch may result in incorrect behavior.

SDP information contained within a '180 Ringing' SIP message may not be properly parsed by the SIP ALG which may result in one-way audio on the call.

Loss in connectivity between a NetVanta 150 Access Point and a NetVanta Access Controller may cause the Access Controller to reboot.

Multiple ISDN error conditions can cause the DIM to exhibit inconsistent behavior when call attempts are made.

When AAA is enabled and TACACS server is being utilized for authentication, the user may be disconnected after only one failed login attempt.

An error may be returned when parsing the adGenAosCommon.mib.

If an interface contains no MAC (i.e. address of 00:00:00:00:00:00), the router may reboot after a period of time.

The 'SNTP wait-time' setting can cause a unit to lockup if it is configured to use a larger than default wait-time.

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

Top websites and exception report email clients may send a naked LF without a preceding CR. This is in violation of RFC 2822 section 2.3.

AOS units, acting as SNTP servers, do not respond correctly to clients' SNTP queries.

IGMP snooping may allow for a spanning tree loop, which may lead to a reboot if an extensive amount of multicast traffic traverses the switch.

Unframed T1 loopbacks can cause false bit errors to appear on the Netvanta router.

Resolved Issues

These are issues that have been resolved since the previous AOS release (17.05.03.00)

The help text for the dampening-interval of a track is unclear in stating under which conditions it would be enforced.

On the NetVanta 123x switches, shutting down the gigabit fiber port may not power down the SFP module.

When configuring a schedule, if the schedule name includes spaces, the schedule name will not persist after a reboot.

If the startup configuration on an AOS device contains certain specific characters, the config may not fully load during bootup.

Auto-link client may report a false "success" of a job back to the MSP server, leading the user to believe the task was successful, when it may not have been.

If an interface contains no MAC (i.e. address of 00:00:00:00:00:00), the router may reboot after a period of time.

The SNTP server may cease to function and possibly cause a reboot if the 'source-interface' or 'send-unsynced' options are being used.

Entering the 'run-tcl' command with the 'on-pass' track option may cause the TCL script to execute immediately regardless of the track status.

The troubleshooting wizard may display an error when the source IP that traffic is being NAT'd to is a private IP address instead of a public IP address.

When AAA is enabled and a TACACS server is being utilized for authentication, the user may be disconnected after only one failed login attempt.

Executing a test-pattern on a T1 interface while it is in the "Down" state may falsely indicate that the test-pattern is transmitting with no errors.

An error may be returned when parsing the adGenAosCommon.mib.

Multiple ISDN error conditions can cause the DIM to exhibit inconsistent behavior when call attempts are made.

Enabling the Auto-link client may cause a slow memory leak, which can lead to a reboot.

Removing the 'shape average' command from a parent map may leave the child map assigned to it even though assigning a child map to a parent map without the 'shape average' command is an invalid configuration.

The packet count for the Top Traffic Statistics may be displayed incorrectly in the GUI.

Accessing a NetVanta device using Telnet or SSH when AAA is enabled may cause a reboot.

Multiple SSH sessions to a NetVanta device if authenticated in a different order than they were created, may cause one or more of those sessions not to connect and output the message, "********SSH Session Blocked********."