The Network Access Company

Corporate Office
Adtran, Inc.
901 Explorer Boulevard
Huntsville, AL 35806

U.S. Mail
P.O. Box 140000
Huntsville, AL 35814-4000

General Information
800 9ADTRAN
info@adtran.com
www.adtran.com

Pre-Sales
Technical Support
800 615-1176
application.engineer@adtran.com
www.adtran.com/support

Post-Sales
Technical Support
888 423-8726
support@adtran.com
www.adtran.com/support

ACES Help Desk
888 874-ACES
aces@adtran.com
www.adtran.com/support

Release Notes
AOS Voice Products

AOS Release A1.01.00
February 25, 2007

Contents

Purpose and Supported Platforms

AOS Voice Products release A1.01.00 is a major system release that adds many new features and addresses customer issues that have been uncovered in previous code releases.

Release A1.01.00 is Generally Available code, meaning that it has been subjected to both Design Verification and Product Qualification testing. Results obtained during this testing have been evaluated and the code has been determined to be ready for General Availability. Caveats discovered during testing but not addressed in this build are listed in Appendix A.

A listing of available documents for this release appears in Appendix B. Configuration guides, white papers, data sheets, and other documentation may be found on Adtran's knowledge base, http://kb.adtran.com.

The contents of these release notes will focus on the Netvanta 6355/1355 and the Total Access 900/900e series platforms. Netvanta 7100 release notes are available on the Adtran knowledge base:

http://kb.adtran.com/article.asp?article=2299&p=2

Supported Platforms for A1.01.00

- **NetVanta 7100** – Converged IP Office in a Box
- **NetVanta 6355/1355** – Multiservice Access Gateway
- **TA 900 Series** – VoIP Multiservice Access Gateway, single T1 interface
- **TA900e Series** – VoIP Multiservice Access Gateway, multi-T1 interface

Summary of New Features

This section highlights the major features, commands and behavioral changes for AOS A1.01.00. For a list of related documents, please see Appendix B.

Additions for All Voice Products:

VQM – Voice Quality Monitoring

Ability to make VoIP quality measurements on RTP media flows terminated or passed through the IAD. Results will estimate MOS scores for particular calls as well as jitter buffer performance.

Loopback Accounts

When the loopback account call is connected, the RTP audio is looped back. This will provide an easy method to verify proper operation and configuration during install, and can be used with VQM to troubleshoot network issues. This feature includes the ability to initiate SIP calls via the CLI.

AWCP - ADTRAN Wireless Control Protocol

AWCP is a Layer 2 Control and Management protocol that enables the platform to act as a Wireless Access Controller for the Netvanta 150 Access Point. Up to eight Netvanta 150 Access Points can be configured and managed by the AC.

Top Talkers

The NetFlow flows that are generating the heaviest system traffic are known as the "top talkers." The NetFlow MIB and Top Talkers feature can be used for security monitoring or accounting purposes for top talkers, and matching and identifying key users of the network.

Full PRI support

All 23 B channels of a PRI can be used simultaneously. The number DSP resources are increasing from 16 to 24 channels on the RoHS-E1 units.

Top visited websites

The top websites feature is designed to report top websites requested by users to system administrators. This feature is intended to be used in conjunction with the *ip urlfilter* command so that customers without a Websense server will have a simple URL filtering package.

Additional Features

- VRF aware DHCP server
- VRF aware firewall
- Portal-List(s) to assign username access to different portals (system applications such as http, telnet, ssh, ftp, and console). Previously, a username for ftp could also telnet or ssh into the unit.

Summary of Bug Fixes

This section highlights major bug fixes in AOS version A1.01.00.

Pasting config with timezone change could cause reboot

Issue Detail

- When a new unit is configured out of the box and a config is loaded the changes the timezone region to -1 or greater, the IAD is susceptible to a memory leak that could cause a core dump. This would only happen on a new unit that has the factory date and time or a unit that was factory defaulted.

Corrective Action

- Units without real timeservers save the system time in a file on the filesystem. When this file is being restored on startup, the RTC and the kernel''s system clock would get out of sync. We changed the way we restore the file to prevent the clocks from getting out of sync, which ultimately caused the memory leak.

T.38 fax causes a reboot

Issue Detail

- If T.38 is configured in the codec list and a T.38 fax call is place, the IAD will reboot.

Corrective Action

- There was an error in the GUI that would allow a user to configure T.38 as an acceptable codec in the codec list. This was not configurable from the CLI. The option has been removed from the GUI. T.38 should not be configurable as an acceptable voice codec.

Dial string longer then 20 characters could cause reboot

Issue Detail

- If a dial string in the URI or contact field of an INVITE is longer then 20 characters, the IAD will reboot.

Corrective Action

- Added a check in the trunk account to accommodate for longer dial strings.

Blind transfer fails when using sip grammar domain to/from through stateful proxy

Issue Detail

- When a REFER from a SIP phone behind the IAD passes through the stateful proxy, the Refer-To domain is changed to that of the SBC instead of the configured domain setting.

Corrective Action

- Made change to Refer-To to inherit the from/to grammar functionality.

Network SBC could detect NAT when NAT is not configured on IAD

Issue Detail

- It’s possible that an SBC could detect NAT when an IAD is configured for transparent mode/no NAT due to the layer 3 source IP address of the SIP packet (the IAD’s WAN address) being different then the IP in the VIA (the IP of the SIP Phone).

Corrective Action

- Added a NAT simulation mode with “ip sip proxy transparent nat-simulate”. This will change the appropriate IPs in the SIP packet to the WAN address of the IAD, without changing any other data traffic passing through the IAD.

Using “show media-gateway channel” stats every second could cause a memory leak

Issue Detail

- If using a script to log in and check DSP channel stats every second, it is possible that there will be a memory leak causing a reboot over time.

Corrective Action

- Fixed database error related to deleting status table after show command is issued.

Contact header not followed after upgrade from 14 to 16

Issue Detail

- If the IAD receives a 200ok from the Sip server during call setup, the corresponding ACK will be sent to the URI IP for the 200ok, not the IP in the Contact field. This worked in correctly in rev 14.

Corrective Action

- Added functionality to reset the about-to-be-sent ACK’s destination as well as changing the appropriate call-leg transitions in the SIP trunk.

Possible SIP parsing error in contact field

Issue Detail

- If the contact field contains a transport value longer then 3 characters, the SIP parser will fail to properly parse the SIP message.

Corrective Action

- Made appropriate changes to the SIP parser.

Using non-authoritative DNS servers can cause failed calls when using SRV records to resolve the SIP server IP

Issue Detail

- If a DNS server that is non-authoritative for SRV records is used, there can be windows of time where calls will fail because the SIP stack can’t resolve the FQDN configured for the outbound proxy or sip-server. This is due to the TTL on non-authoritative DNS servers decrementing until it reaches 0 (or some threshold where it will perform a new query to the authoritative server).

Corrective Action

- The DNS client in the IAD has trouble when we send a query and receive a TTL that is less then 60 seconds. Implemented cache behavior in the DNS table so that for the brief interval that we have a response that has a very low TTL, it will persist in the cache long enough for the SNS to refresh it without exceeding the lower bound value.

Possible one-way audio with SIP endpoints behind the IAD proxy that respond to UPDATE with 200 w/ SDP

Issue Detail

- We have seen an implementation error with some SIP endpoints where upon receiving an UPDATE with no SDP, the SIP endpoint responds with a 200 with SDP. The one-sided SDP causes a new port pair to be allocated from the firewall in the IAD’s proxy when source NAT applies to the same direction. The SIP proxy does not connect the call because an offer/answer pair was not seen on the dialog; hence media begins to flow to a port pair that has not been opened and one-way talkpath occurs.

Corrective Action

- Implemented a workaround that detects this case and removes the SDP from the 200 before forwarding the message from the offending endpoints.

“Unknown” sent as ANI in feature group D / E&M wink trunk

Issue Detail

- If the From field of an inbound INVITE contains “unknown” as the ANI, the IAD generates (*Unknown*5555*) out the E&M wink trunk for FGD.

Corrective Action

- The IAD now correctly sends (**5555*)

SDP in 200 to reINVITE does not include T.38 attributes

Issue Detail

- Outbound T.38 calls fail due to the IAD not sending the T.38 attributes in the SDP of the 200ok. This only happens when responding to a reINVITE from the softswitch.

Corrective Action

- Modified SDP attribute generation to always include the same attributes when responding to reINVITE.

Reboot when a call into a ring group is placed on hold from the Sip server

Issue Detail

- If a call is placed into a ring group and is then placed on hold from the network side, the IAD will reboot. This does not happen if you call the analog user directly and place the call on hold.

Corrective Action

- The switchboard resource was not getting set in the RTP channel. If an existing RTP channel was already in the CS, the resource wasn’t set properly.

Reboot when doing a “show run” after deleting non-default VRF

Issue Detail

- Creating a non-default VRF, assigning it to a frame-relay subinterface, deleting the non-default VRF, and then doing a “show run” will cause the IAD to reboot.

Corrective Action

- The frame-relay interface was not being deconstructed properly when “no ip vrf” was entered. Made appropriate changes to properly remove VRF.

V.21 pre-amble detection turns echo can off w/ modem-passthrough

Issue Detail

- If a V.21 preamble event is received from a fax machine, the echo canceller in the IAD is fully disabled (data mode). This could cause problems with certain fax machines.

Corrective Action

- In order to comply with V.21 spec, we now leave the echo canceller on and turn off NLP (non-linear suppression).

Upgrade Instructions

Several steps need to be taken to assure a valid upgrade. First, save your existing configuration to a tftp server. The command to execute this step is

```
Router# copy start tftp
```

You will be prompted for file names and the server address in the process.

Next, download AOS version A1.01.00 from the ADTRAN support website. When properly installed on your tftp server, the file will have the form "*product-version.*biz*"* where *product* is the platform name, and *version* is the AOS image version (A1.01.00) separated by hyphens instead of decimals.

From your privileged prompt:

```
Router# copy tftp flash
```

During the tftp download you will be prompted for the tftp server name, the tftp server file name, and finally the name you want to give the file once it is transferred to the on-board flash. The flash can hold up to eight megabytes of files, whether AOS or configuration files. Now from the Configuration prompt:

```
Router (config)# boot system flash filname.biz
```

The boot command tells the router which software on the flash to use as the boot up AOS. The router should now be rebooted with the privileged command

```
Router (config)# reload
```

When the unit reboots, it will be running AOS version A1.01.00.

Appendix A – Errata for A1.01.00

The following is a list of errata that still exists in A1.01.00.

1. Multiple T.38 calls will fail instead of failing over to G.711

If more then one T.38 call is placed through the IAD at one time, the second and subsequent calls will fail without failing over to G.711. This will be addressed in A1.02.

2. Missed digits when dialing from certain analog phones

The DSP may have trouble picking up digits from certain analog phone sets. This is not a new issue and will not be caused by an upgrade to A1.01. If you currently have analog sets that are working on previous releases of firmware, then there is no risk of seeing this issue after upgrade. This will be addressed in A1.02.

3. SRV records to not update change of priorities

If DNS server changes SRV record priorities, the IAD will not properly update the new priorities in the DNS table. This will be addressed in A1.02.

4. Password encryption does not work with sip-identity on a ring group

If password authentication is configured for the sip-identity of a ring group, the password will say it is encrypted in the running config, but the password itself will still show as un-hashed. This will be addressed in A1.02

5. DSP reboot during T.38 fax call

During the setup of a T.38 fax, it is possible that the IAD will reboot. This is due to a memory corruption error in the DSP. This will be addressed in A1.02.

6. Caller-id name override doesn’t work for inbound calls on a trunk

Caller-id number override for voice trunks works properly; however, the CID name field cannot be manipulated. This previously worked in version 12. This will be addressed in A2.01.

7. INVITE not properly changed after 302 ‘moved temporarily’

If a 302 is used to change the destination port for subsequent calls to a specific user, the URI generated by the IAD contains the requested port number, but the destination port for the SIP packet still contains the original port number. This will be addressed in A2.01.

8. URI matching for SIP PUD needs to be tweaked to handle certain SIP endpoints

If a SIP endpoint sends a REGISTER through the proxy containing an rinstance but does not send the ristnance in the INVITE, the PUD lookup in the proxy will think that the two contact headers don’t match. This violates RFC 3261. This will be addressed in A2.01.

9. Trunk appearance leak on E&M wink trunk w/ dialtone enabled

If dialtone generation is enabled on an E&M wink trunk without saving the change to the startup-config and then rebooting the IAD, a trunk appearance could lockup and by unavailable. Rebooting the IAD will permanently clear up the issue. This will be addressed in a future release of code.

Appendix B – Related Documents

For configuration guides, installation guides, white papers and more, visit ADTRAN's knowledge base at http://kb.adtran.com.

AOS A1.01 Command Line Reference Guide (13MB file) –
http://kb.adtran.com/article.asp?article=2219&p=2

Voice Quality Monitoring Config Guide -
http://kb.adtran.com/article.asp?article=2262&p=2

[Video]Understanding Voice Quality Monitoring in AOS -
http://kb.adtran.com/article.asp?article=2296&p=2

Integrated Traffic Monitoring Config Guide (Top Talkers Support) -
http://kb.adtran.com/article.asp?article=2157&p=2

Multi-VRF Config Guide –
http://kb.adtran.com/article.asp?article=2156&p=2

URL Filtering/Top Websites Reporting Config Guide -
http://kb.adtran.com/article.asp?article=2158&p=2

AOS Wireless Config Guide –
http://kb.adtran.com/article.asp?article=2078&p=2