



AT-S94 Version 1.1.0 Software

AT-8000S Switch

Software Release Notes

Please read this document before you begin to use the management software.

Supported Platforms

The following platforms are included in the AT-8000S family of devices:

- AT-8000S/16 – 16 FE ports with 1 combo 10/100/1000 SFP Port.
- AT-8000S/24 – 24 FE ports with modular configuration 2 x combo 10/100/1000 SFP ports and 2 RJ-45 10/100/1000 stacking ports.
- AT-8000S/24POE – 24 FE ports with modular configuration 2 x combo 10/100/1000 SFP ports and 2 RJ-45 10/100/1000 stacking ports, with support for Power over Ethernet on all ports.
- AT-8000S/48 – 48 FE ports with modular configuration 2 x combo 10/100/1000 SFP ports and 2 RJ-45 10/100/1000 stacking ports.
- AT-8000S/48POE – 48 FE ports with modular configuration 2 x combo 10/100/1000 SFP ports and 2 RJ-45 10/100/1000 stacking ports, with support for Power over Ethernet on up to 36 ports.

The AT-8000S/24, AT-8000S/24POE, AT-8000S/48 and AT-8000S/48POE can be combined together in a six-unit high stack.

Product Documentation

For description how to install the devices as standalone units or as members of a stack, refer to the following guide:

- ❑ *ATI 8000S Installation Guide*

For lists of CLI commands available to the user to configure the devices, refer to the following guide:

- ❑ *ATI 8000S CLI Reference Guide*

These documents are available from the Allied Telesis web site at www.alliedtelesis.com.

Newly Introduced Features

• Access Control Lists and Quality of Service Features

The system enables the user to define various services for specific traffic flows. This is achieved by two mechanisms: Classification (Access Control Lists) and Actions (Quality of Service Support).

Access Control Lists

Access Control Lists (ACLs) are a general mechanism to inspect incoming frames and classify them into named logical groups based on various criteria. Each such group may have specific actions that are carried out on each frame classified as a member of that group.

Quality of Service Support

To overcome unpredictable network traffic and optimize performance, you can apply Quality of Service (QoS) throughout the network to ensure that network traffic is prioritized according to specific criteria.

- **802.1x Support**

802.1x Port-Based Authentication

Port based authentication enables authenticating system users on a per-port basis via an external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the Remote Authentication Dial in User Service (RADIUS) server using the Extensible Authentication Protocol (EAP).

802.1x MAC Authentication

MAC authentication is an alternative to 802.1X that allows network access to devices (such as printers and IP phones) that do not have the 802.1X supplicant capability. MAC authentication uses the MAC address of the connecting device to grant or deny network access.

- **DHCP Snooping**

DHCP Snooping

DHCP snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database also referred to as a DHCP snooping binding table. DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. DHCP snooping differentiates between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch

Option 82 pass-through

Relay agent information option (option-82) in the DHCP protocol enables a DHCP relay or a switch to send the port number of a client, that request an IP address. The Relay agent information option specifies the port number from which the client's packet was received.

- **L2 Multicast Support**

Multicast forwarding allows one-to-many and many-to-many connections for information dissemination. In effect, Multicast service is a limited broadcast – the data is sent to all relevant ports, but ports that are known to have no need for the transmitted data do not get a copy of the data, conserving bandwidth and host resources on those links.

L2 Multicast Forwarding and Filtering

When a frame arrives on any switch port and its destination address is in an L2 multicast address it is forwarded to all relevant ports – that is, ports that are members of the relevant multicast group.

Static Multicast Groups

This feature allows the user to manually achieve what IGMP snooping can do automatically, as a replacement (when it is undesirable to use IGMP snooping) or as a supplement (e.g. to handle hosts that do not generate IGMP reports correctly).

IGMP Snooping

IGMP Snooping allows “snooping” (examining the contents of) IGMP frames as they are forwarded by the switch from stations to an upstream multicast router. This allows a switch to conclude the following:

- Where (on which ports) stations interested in joining a specific multicast group are located
- Where (on which ports) multicast routers sending multicast frames are located

This knowledge may be used to exclude irrelevant ports (ports on which no stations have registered to receive a specific multicast group) from the forwarding set of an incoming multicast frame

The system supports IGMPv3 as well as IGMPv1 and IGMPv2

- **IGMP Querier**

The IGMP Snooping Querier is used to support IGMP snooping where the multicast traffic does not have to be routed. A typical example is a local network where the multicast content is provided from a local server, and the router (if exists at all) of that network does not support multicast.

The network administrator can configure an IGMP snooping switch to be an IGMP Snooping Querier of a VLAN. If a VLAN is shared by more than one IGMP snooping switch, the user should verify that only one switch is configured as the IGMP Querier of a VLAN.

• 64 Bit SNMP Counters Support

The support of 64bit MIB counters is added to the system. This is in addition to the 32bit counters supported already.

Resolved Issues from PH1

- ❑ MAC groups mapping was not working for IGMP packets; references: 89459
- ❑ Virtual Cable Test is not accessible from the web; reference: 55277
- ❑ SNTP - Using unicast client SNTP long run failed; reference: 57562
- ❑ SNTP - Configuration of SNTP using Web GUI not works; reference: 57509
- ❑ The commands 'Interface Configuration command *port security mode dynamic*;' and 'show qos map dscp-dp' are documented in the CLI Reference Guide, but should not appear: reference: 51805, 59467

Known Issues

- ❑ SFP 100 - Switch over back to fiber fails after fiber link restored. It happens when an LCP155A4HSR 100M SFP is used when backup Copper link is 1G. **Recommended User Workaround:** Works fine when fiber and Copper speeds are similar and there are no issues with different SFP model.
- ❑ Port Mirroring - Port mirroring closes the port and opens it again. **Recommended User Workaround:** not required
- ❑ TAB functionality - Use of the Tab key does not complete the command Interface range VLAN all and the command Switchport general allowed VLAN **Recommended User Workaround:** type in the full command.
- ❑ SNMP - EWS > SNMP > Notify > Filters: cannot add or modify filter with name containing special characters **Recommended User Workaround:** do not use special characters
- ❑ Time - EWS > System > System Time: current day becomes undefined after changing Time Zone Offset **Recommended User Workaround:** this is fixed after next reset
- ❑ IGMP - the MAC groups mapping is not working for igmp packets
- ❑ Flow Control - Flow control does not work on Giga ports **Recommended User Workaround:** no workaround
- ❑ Encryption - It is impossible to add MD5/SHA keys via EWS **Recommended User Workaround:** use CLI

Software Upgrade Procedure

The new software requires additional FLASH sectors beyond the current amount of FLASH sectors which are currently allocated for the image. Therefore the FLASH sectors must be reordered before downloading the new software. This will be accomplished by first downloading an interim version, and only after that loading the actual released version.

The interim version provided reorders the FLASH allocation without the need to erase the FLASH and downloading the new software via the serial cable using XMODEM. Hence, the AT-8000S software upgrade procedure can be performed via TFTP server.



Note

Due to new Board Support Package (BSP) there is also an updated Boot code; version 1.0.1.06. This can be uploaded regardless of the SW image (ROS version) running on the device. Therefore, boot upgrade can be performed before or after the 2-stage procedure described below

The user will have to run the following steps in order to successfully completing the upgrade procedure:

1. Back up configuration files to an external device.
2. Delete startup configuration file from the device.

3. Download to the device the ats94-Interim image drop via TFTP.
4. Switch active image for next reboot
5. Reboot the device. By the end of the reboot process (which may take a few minutes), the interim code drop version will be running on the device, and it will automatically rearrange the FLASH sectors as needed.
6. Download the final code drop via TFTP.
7. Switch active image for next reboot
8. Reboot the device. By the end of the reboot process, the final code drop is running.
9. Download to the device saved configuration (if needed).



Note

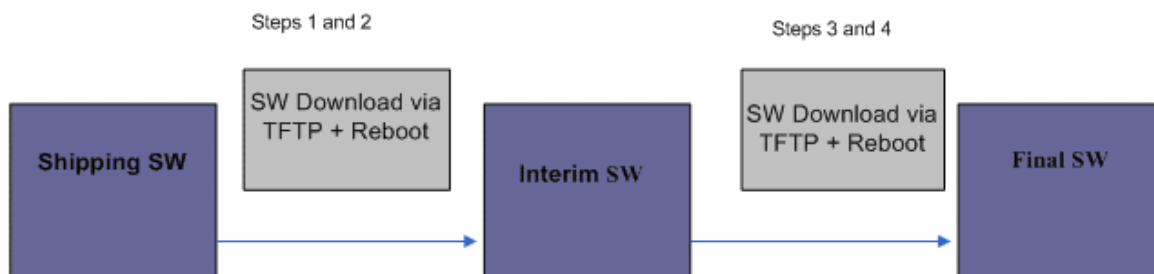
In case of a stack both the interim version and the final version should be downloaded to **ALL** the units in the stack at the same time.



Note

Following this procedure and uploading the interim code drop is required only once. The next S/W upgrade will not require the additional upload of the interim code drop.

Figure 1: Software Upgrade Process



The existing configuration is retained including MAC address and serial number.



Note

During the software upgrades ensure the following:

- Ensure that the device is not powered down or that a power cable is not disconnected during the software upgrade. If the device is powered down or if a cable is disconnected, once device is reconnected the software upgrade must be downloaded via XMODEM
- Ensure to back up the device configuration to an external server/station.
- Do not use the interim code drop for Quality Assurance testing, field upgrades etc; use only the final code drop
- When running the interim version, the initialization stage takes a relatively long time

Contacting Allied Telesis

This section provides Allied Telesis contact information for technical support as well as sales and corporate information.

Online Support

You can request technical support online by accessing the Allied Telesis Knowledge Base: www.alliedtelesis.com/support. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Support & Services section of the Allied Telesis web site: www.alliedtelesis.com. Select your country from the list displayed on the website. Then select the appropriate menu tab.

Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesis without an RMA number will be returned to the sender at the sender's expense. To obtain an RMA number, contact the Allied Telesis Technical Support group at our web site: www.alliedtelesis.com/support/rma. Select your country from the list displayed on the website. Then select the appropriate menu tab.

Sales or Corporate Information

You can contact Allied Telesis for sales or corporate information through our web site: www.alliedtelesis.com. Select your country from the list displayed on the website. Then select the appropriate menu tab.

Obtaining Management Software Updates

New releases of management software for our managed products are available from our Allied Telesis web site: www.alliedtelesis.com.

Warranty

The AT-8000S has a Lifetime Warranty (two years fan and PSU). Go to www.alliedtelesis.com/warranty for the specific terms and conditions of the warranty and for warranty registration.

Copyright © 2008 Allied Telesis, Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc. Allied Telesis is a trademark of Allied Telesis, Inc. Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation. Netscape Navigator is a registered trademark of Netscape Communications Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.