



AlliedWare Plus™ Version 2.1.3

AT-9000 Layer 2-4 Gigabit Ethernet

EcoSwitches

Software Release Notes

Please read this document before you begin to use the management software. The document has the following sections:

- ☐ “Supported Platforms” on page 2
 - ☐ “Product Documentation” on page 2
 - ☐ “Introduction to Upgrading the Switch” on page 2
 - ☐ “What’s New in Version 2.1.3” on page 3
 - ☐ “Operational Notes” on page 3
 - ☐ “Resolved Issues” on page 4
 - ☐ “Known Issues” on page 7
 - ☐ “Contacting Allied Telesis” on page 8
 - ☐ Appendix A, New Feature Examples on Page 9
-

Caution:

The software described in this document contains certain cryptographic functionality and its export is restricted by U.S. law. As of this writing, it has been submitted for review as a “retail encryption item” in accordance with the Export Administration Regulations, 15 C.F.R. Part 730-772, promulgated by the U.S. Department of Commerce, and conditionally may be exported in accordance with the pertinent terms of License Exception ENC (described in 15 C.F.R. Part 740.17). In no case may it be exported to Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria. If you wish to transfer this software outside the United States or Canada, please contact your local Allied Telesis sales representative for current information on this product’s export status.

Supported Platforms

Version 2.1.3 of the AlliedWare Plus™ Management Software is supported on these switches:

- ❑ AT-9000/28
- ❑ AT-9000/28SP
- ❑ AT-9000/52

This version supports the following SFP modules:

- ❑ AT-SPTX (Supported only at a speed of 1G.)
- ❑ AT-SPEX
- ❑ AT-SPSX
- ❑ AT-SPFX/2
- ❑ AT-SPFX/15
- ❑ AT-SPLX10
- ❑ AT-SPLX40
- ❑ AT-SPZX/80
- ❑ AT-SPBD10-13
- ❑ AT-SPBD10-14
- ❑ AT-SPFXBD-LC-13
- ❑ AT-SPFXBD-LC-15

Product Documentation

For the AT-9000 Series documentation, refer to the following guides:

- ❑ *AT-9000 Series Installation Guide*
- ❑ *AT-9000 Series AlliedWare Plus Command Line User's Guide*
- ❑ *AT-9000 Series AlliedWare Plus Web Browser User's Guide*

Both documents are available from the Allied Telesis web site at **alliedtelesis.com/support**.

Introduction to Upgrading the Switch

You may upgrade your switch to version 2.1.3 using either the command line interface or web browser interface. If you want to use the command line interface, refer to the *AlliedWare Plus Command Line User's Guide*. If you want to use the web browser interface, refer to the *AlliedWare Plus Web Browser User's Guide*.

What's New in Version 2.1.3

This software version includes the following new features:

- ❑ Full AAA Services support for TACACS+ and RADIUS
- ❑ Restrict Remote Management Access - assign ACLs on VTYS

Note

See Appendix A, on page 9 for examples of these new features

Operational Notes

The AT-9000 Series switches behave in the following manner:

- ❑ The speed of the AT-SPFX/2 and AT-SPFX/15 modules has to be manually set to 100Mbps with the SPEED command. The following example of the command configures the speed of the AT-SPFX/2 or AT-SPFX/15 module in slot 1 of an AT-9000/28SP Switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# speed 100
```

- ❑ The assignment of an IPv6 management address to the switch must be performed manually using the IPV6 IPADDRESS command, because the switch cannot obtain an IPv6 address with stateless autoconfiguration or from a DHCP6 server.
- ❑ You cannot use the web browser interface to configure the following features:
 - Access control lists
 - Enhanced stacking
 - Quality of Service
 - SNMP
 - Voice VLANs
 - VLAN stacking

Use the command line interface to configure these features.

- ❑ The web browser interface has been tested and found to be compatible with the following web browsers:
 - Microsoft Internet Explorer 7 and 8
 - Mozilla Firefox 3.6.3
 - Apple Safari 4.0.5

Note:

If you are using Explorer 8 web browser and the pull-down menus in the switch's web browser interface do not work, open the Internet Options window in the web browser, select the Security tab, and set the custom settings to medium-high. Then refresh your page.

- ❑ You cannot change the configuration of a port, such as its VLAN assignment, after it is added to a static or an LACP trunk. The configuration of a port must be set before it is added to a trunk.
- ❑ You can create up to 4096 VLANs on the switch, but only 255 VLANs can be active at a time.
- ❑ Changing the SNMPv3 engine ID value is not recommended because the SNMP server on the switch may fail to operate properly.

Resolved Issues

The following issues have been resolved in this release.

- ❑ **AT-9000/28SP SFP Ports:** If you issue a “shutdown” command on SFP port 25, both SFP ports 25 and 27 are shutdown. If you issue a “shutdown” command on SFP port 26, SFP ports 26 and 28 are shutdown. This issue does not affect the copper ports 25 - 28. (9997)
- ❑ **AT-9000/52:**
 - ACL does not work on Ports 27 – 48. (10681)
 - On the AT-9000/52 only, when Private VLANs are configured, the switch reboots.
- ❑ **SNMP:**
 - LLDP and LLDP-MED SNMP traps do not work. (11241)
 - When port security violation mode is set to “restrict”, the switch does not send out a trap to the SNMP host when the threshold is exceeded. (11205)
 - First “get” on the Oid doesn't work from SNMPc MIB browser. (#10613)
 - Setting of vlan untag ports via NET-SNMP may change the information. (#10614)
 - The “snmpgetnext” command is getting incorrect info back. (#10615)
- ❑ **802.1x:**
 - When a “dot1x port-control auto” command is issued for a port, unauthorized clients can still communicate with CPU. (8095)
 - If the “show dot1x supplicant” command is issued at the same time a client is being authenticated, the switch crashes and reboots. (Customer issue# 101210-000013)
- ❑ **Syslog:** Syslog related to STP contains the wrong port number in message field. (11214)
- ❑ **Show Commands:**
 - “show platform table port” command doesn't have 1519-1522 size group of a transmit counter. (11176)
 - “sh sys” does not accurately show the version of the boot file (11231)
- ❑ **LLDP:** The default TLVs for LLDP are incorrectly set. (11220)
- ❑ **NTP:**

- Cannot configure UTC offset unless NTP server is reachable. (11080)
- If the NTP Server is NOT reachable, the commands are not written to running config file. (10895)
- ❑ **Bootup:** Traffic flows before config files are loaded. (10182)

❑ **WEB Interface:**

- The user is allowed to load an image and reboot without logging in. (10624)
- You can log in with any privilege level account and be able to load image files and reboot via the web. Loading images should be restricted to privilege level 15 login accounts.
- Subnet Masks are not displayed correctly in Web GUI. Customer issue# 101206-000016

❑ **TELNET Server:** Server sends malformed packets and numerical garble (10051)

❑ **CoS:**

- Switch prioritizes packets based on CoS value regardless of CoS Trust. Switch should not prioritize based on user-priority value unless “mls qos trust cos” command is configured on ingress ports.(11200)
- MLS qos map not written to running-config. (11125)

❑ **LACP:** LACP ID range and channel group range values are incorrect. (11168)

❑ **LLDP and LACP on Port 1.0.28:** If you configure LLDP notification on port 1.0.28, then the port becomes separated in the running configuration. If you configure an LACP aggregator to include port 1.0.28, it appears separately as a member. However, when you save and reboot the switch, the LACP configuration for port 1.0.28 is lost.

❑ **IGMP V3 Report:** The switch crashes if it received an IGMP V3 report with more than two groups.

❑ **New Command:** “sh running-config interface” now supported. This command can be used to view specific interface related configurations.

❑ **QoS Configurations:** Interface related QoS configurations are now retained when the switch is rebooted.

❑ **IGMP Snooping:** When you disable IGMP Snooping and the config is saved, this feature is not disabled after reboot.

❑ **New Image File on Web Interface:** SFP Port Speed: The configuration of port speed on SFP ports is now supported.

❑ **User Access:** User passwords now support special characters.

Note

The special characters that are supported include
0-9 a-z A-Z ~!@#\$%^&*()_+{}|:<>-=[]\;, except ‘ and “.

❑ **Port Authentication:** Dynamic VLANs are enabled by default. This feature should be disabled by default. (Customer Issue# 101223-000029)

Note

Note: If the user was previously using dynamic VLANs, they must enable it after the upgrade. If the Guest VLAN was not enabled and the “dot1x ports auto” command was not issued prior to enabling mac authentication, then mac authentication would not work. This issue has been resolved where the mac authentication is not dependent on the Guest VLAN status or issuing the “dot1x ports auto” command.

- ❑ **Configuration Files:** Large configuration files of 300 lines or more are not written or saved correctly. Customer Issue# 110113-000021
- ❑ **ACLs:** With IGMP snooping enabled, ACLs for Multicast Addresses do not work. (Customer Issue #110203-000038)
- ❑ **SSH:** Stale SSH sessions can possibly lock out management sessions. (Customer Issue #110201-000065)
- ❑ **IGMP Snooping:** IGMP snooping table displaying incorrect multicast groups (11187)

Known Issues

- ❑ There are no known issues in this release.

Contacting Allied Telesis

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

Online Support

You can request technical support online by accessing the Allied Telesis Knowledge Base: **www.alliedtelesis.com/support/kb.aspx**. 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.

Warranty

For hardware warranty information, refer to the Allied Telesis web site: **www.alliedtelesis.com/support/warranty**.

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. For instructions on how to obtain an RMA number, go to our web site at **www.alliedtelesis.com** and then select Support and Replacement Services.

Sales or Corporate Information

You can contact Allied Telesis for sales or corporate information through our web site: **www.alliedtelesis.com**.

Management Software Updates

New releases of management software for our managed products are available on our Allied Telesis web site at **<http://www.alliedtelesis.com/support/software>**.

Copyright © 2011 Allied Telesis, Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Allied Telesis and AlliedWare Plus are trademarks of Allied Telesis, Inc. 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.

Appendix A

New Feature Examples

Configuration examples are provided for the following new features:

- ❑ Full AAA Services support for TACACS+ and RADIUS
- ❑ Restrict Remote Management Access - assign ACLs on VTYS

RADIUS

Set up RADIUS Server & Accounting

Note

The manner of how the switch attempts to connect to each server is determined by the order they are displayed in the running configurations.

```
awplus(config)# radius-server host { host-name | <ip4addr> } [acct-port <0-65535>] [auth-port <0-65535>] [key <key-string>]
```

(Optional) RADIUS hosts order can also be configured by inputting the order option by which the switch will attempt to connect to each server.

```
awplus(config)# radius-server host { host-name | <ip4addr> } order [1|2|3] [acct-port <0-65535>] [auth-port <0-65535>] [key <key-string>]
```

RADIUS AAA Accounting

```
awplus(config)# aaa accounting login default start-stop|stop-only|none
group radius|tacacs
awplus(config)# no aaa accounting login default
```

The accounting event to send to RADIUS server is configured with the following options:

start-stop - sends a start accounting message at the beginning of a session and a stop accounting message at the end of the session.

stop-only - sends a stop accounting message at the end of a session.

none - disables accounting.

Enable AAA RADIUS Authentication

Use this command to enable or disable RADIUS authentication on all terminals (local and remote).

```
awplus(config)# aaa authentication login default group radius [local]
awplus(config)# no aaa authentication login default
```

This command enables server-based authentication on all terminals local|remote:

```
awplus(config)# server-based authentication radius
```

Negating server-based authentication radius reverts authentication method back to local user database.

```
awplus(config)# no server-based authentication radius
```

Specify RADIUS Global Secret Key

```
awplus(config)# radius-server key <shared secret b/w 802.1x client and radius server>
awplus(config)# no radius-server key
```

Specify RADIUS Server Timeout

```
awplus(config)# radius-server timeout <1-300>
awplus(config)# no radius-server timeout
```

Note

Default radius-server timeout is set to 5(s)

Enable|Disable authentication on Console & Remote Terminals

If you want to disable any Remote authentication (TACACS+,RADIUS) on Console or VTY lines, use the 'NO LOGIN AUTHENTICATION' command in the line mode. To run this command, your user ID needs to be authenticated on the local switch.

```
awplus(config)# line [console 0|vty 0 9]
awplus(config-line)# login authentication
awplus(config-line)# no login authentication
```

Show RADIUS

```
awplus# show radius
RADIUS Global Configuration
  Source Interface      : 192.168.3.97
  Timeout               : 5 sec
  Server Host : 192.168.1.75
  Authentication Port : 1812
  Accounting Port    : 1813
```

TACACS+

Configure TACACS+

By default, TACACS+ sends out PAP requests.

Note

The manner of how the switch attempts to connect to each server is determined by the order they are displayed in the running configurations.

```
awplus(config)# tacacs-server host { host-name | <ip4addr> } [key <key-string>]
```

(Optional) TACACS+ hosts order can also be configured by inputting the order option by which the switch will attempt to connect to each server.

```
awplus(config)# tacacs-server host { host-name | <ip4addr> } order [1|2|3] [key <key-string>]
```

Enable TACACS+ Login Access

Use this command to enable or disable TACACS login authentication on all terminals (local and remote).

```
awplus(config)# aaa authentication login default group tacacs [local]
awplus(config)# no aaa authentication login default
```

Note

[local] indicates that authentication is attempted using the local user database if the TACACS+ server is not accessible. By default, username: manager password: friend

Enable TACACS+ Enable Access

Use this command to enable or disable tacacs enable authentication on all terminals (local and remote). You can set the TACACS protocol to determine whether a user can access the privileged EXEC level. To do so, perform the following task in global configuration mode:

```
awplus(config)# aaa authentication enable default group tacacs [local]
awplus(config)# no aaa authentication enable default
```

Note

[local] indicates that authentication is attempted against the local 'ENABLE PASSWORD' if the TACACS+ server is not accessible.

Enable|Disable authentication on Console & Remote Terminals

To disable any Remote authentication (TACACS+,RADIUS) on Console or VTY lines, use the 'NO LOGIN AUTHENTICATION' command in the line mode. To run this command, your user ID needs to be authenticated on the local switch.

```
awplus(config)# line [console 0|vty 0 9]
awplus(config-line)# login authentication
awplus(config-line)# no login authentication
```

AAA Accounting Login

This command configures TACACS+ accounting for login shell sessions.

```
awplus(config)# aaa accounting login default {start-stop} group tacacs
awplus(config)# no aaa accounting login default
```

The accounting event to send to TACACS+ server is configured with the following parameters:

start-stop - sends a start accounting message at the beginning of a session and a stop accounting message at the end of the session.

stop-only - sends a stop accounting message at the end of a session.

none - disables accounting.

tacacs-server timeout

This command configures timeout parameter for TACACS+ servers globally. The no version of this command resets the global timeout parameter for TACACS+ servers to the default value (5s).

Syntax

```
awplus(config)#tacacs-server timeout <1-1000>
awplus(config)#no tacacs-server timeout
```

show tacacs+

```
show tacacs+
awplus# show tacacs+
TACACS+ Global Configuration
Timeout : 5 sec
Server Name/ Server
IP Address Status
-----
192.168.1.10 Alive
192.168.1.11 Dead
The following are the two server status used:
    ALIVE      : Server working correctly
    DEAD       : Server has timed out or is unreachable
```

Restrict Remote Management Connections

You can create a numbered or named ACL to restrict Telnet, SSH, and HTTP/S sessions to certain hosts and apply the ACL to all the VTY lines.

Use following command to apply an ACL to VTY's.

Example:

To deny all access to switch to any host but give full access to host 10.0.0.3, configure like below.

1. Configure Switch management IP and create ACLs.

```
awplus# conf t
awplus(config)#interface vlan10
awplus(config-if)#ip address 10.0.0.20/24
awplus(config-if)# q
awplus(config)#access-list 3000 permit ip host 10.0.0.3 host 10.0.0.20 <--
Full access to 10.0.0.3
awplus(config)#access-list 3001 deny ip any host 10.0.0.20<--No access at
all to everybody else
```

2. Apply configured ACLs to VTY lines in the same order as shown in this example.

```
awplus(config)# line vty 0 9
awplus(config-line)# access-class 3000
awplus(config-line)# access-class 3001
```

show users

```
awplus# show users
```

Example

```
awplus#sh users
```

Line	User	Host(s)	Idle	Location
con 0	manager	idle	00:02:36	ttyS0
vtty 0	manager	idle	00:09:08	10.4.8.146
vtty 1	manager	idle	00:01:32	10.4.9.36
vtty 2	manager	idle	00:00:00	10.4.9.36