AlliedWare Plus™ Version 2.1.2.10 Patch
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:

Caution

The software described in the documentation 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 2.1.2.10 Patch 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 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

Upgrading the AT-9000 Switch to AlliedWare Plus Version 2.1.2.10 Patch from AlliedWare Plus Version 2.1.2

Upgrade Requirements

The upgrade procedure has the following requirements:

- The switch must already have AlliedWare Plus Version 2.1.2 Management Software. For upgrade instructions, refer to the *AlliedWare Plus Version 2.1.2 Software Release Notes*.
- There must be a TFTP server on your network.
- The switch must have an IP address. For instructions, refer to the *AT-9000 AlliedWare Plus Version 2.1.2 User's Guide*.

Caution

The upgrade process causes the switch to reset. The switch will not forward network traffic during the reset.

Upgrade Procedure

To upgrade the switch to AlliedWare Plus Version 2.1.2.10 Patch from AlliedWare Plus Version 2.1.2:

1. Store the AlliedWare Plus Version 2.1.2.10 Patch Management Software on the TFTP server on your network.
2. Start the TFTP server.
3. Start a local or remote management session on the switch.
4. Use the ENABLE command to move to the Privileged Executive mode.

   ```
   awplus> enable
   awplus#
   ```

5. Use the COPY command to download the AlliedWare Plus Version 2.1.2.10 Patch Management Software from the TFTP server to the switch. Here is the format of the command:

   `copy tftp flash` *`ipaddress filename`*

   The IPADDRESS parameter specifies the IP address of the TFTP server on your network.

The FILENAME parameter specifies the filename of the AlliedWare Plus Version 2.1.2.10 Patch Management Software stored on the TFTP server. The extension must include the ".img" extension. The name cannot contain spaces. In this example, the IP address of the TFTP server is 149.157.18.78 and the name of the management software file is "ats-9000-2.1.2.10_patch.img:"

```
awplus# copy tftp flash 149.157.18.78 ats-9000-2.1.2.10_patch.img
```

After receiving the file from the TFTP server, the switch writes it to flash memory and resets. The entire process takes several minutes. The switch is now running the new software.

Troubleshooting the Upgrade Procedure

If you have a problem downloading the management software to the switch from your TFTP server, here are a few suggestion on how to resolve it:

- Check to be sure that the TFTP server on your network is active.
- Use the SHOW IP INTERFACE command in the User Exec or Privileged Exec modes to verify that the switch has an IP address.
- Use the PING command in the Privileged Exec mode to ensure that the switch has an active link to your TFTP server.
- Verify that you entered the upload or download command correctly. Be sure to include the ".img" extension in the filenames of the management software files.
- If you are using a TFTP server that is case sensitive, be sure to use upper and lowercase characters when specifying filenames in the commands.
- If you experience a problem downloading a management software file to the switch from your TFTP server, check to be sure the file is stored in the correct directory, as required by the server.

New Feature

- **Configuration Format Optimization** - Interface and VTY related commands are no longer entered into the configuration as separate entries. These commands are all grouped together in one area of the configuration file. Where ports are configured the same ranges are displayed. This feature is backwards compatible with existing configurations, so no re-entry of the configuration is required for this feature to take affect.

Operational Notes

- The speed on the AT-SPFX/2 or AT-SPFX/15 module has to be manually set to 100Mbps with the SPEED command. This example of the command configures the speed of an 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
```

- If you want to assign an IPv6 management address to the switch, you must assign it manually using the IPV6 IPADDRESS command. The switch cannot obtain an IPv6 address with stateless auto-configuration or from a DHCP6 server.
- You cannot use the web browser interface to configure these features:
  - Access control lists

- Enhanced stacking
- Quality of Service
- SNMP
- Voice VLANs

Use the command line interface to configure the 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 the pull-down menus in the switch's web browser interface do not work with the Explorer 8 web browser, 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 LACP trunk. For this reason, you must configure a port before adding it to a trunk.
- You can create up to 4096 VLANs on the switch, but only 255 active VLANs are supported.
- The user guide states that a port that has more than one access control list (ACL) performs the ACLs according to their ID numbers, in ascending order. This is incorrect. ACLs are performed in the order in which they are applied to the port. Thus, permit ACLs should be applied first to the port, followed by specific deny ACLs and, finally, general deny ACLs. This example configures ports 22 and 23 to accept only ingress packets with destination addresses in the 149.124.47.0 subnet. The permit ACL, ID number 3011, specifies the 149.124.47.0 subnet and the deny ACL, ID number 3020, defines all traffic. Since the permit access list is added to the port first, the ingress packets are compared against it first.

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3011 permit ip any 149.124.47.0/24
awplus(config)# access-list 3020 deny ip any any
awplus(config)# interface port1.0.22,port1.0.23
awplus(config_if)# ip access-group 3011
awplus(config_if)# ip access-group 3020
```

This example is the same as the previous one, except that the deny ACL is added to the port before the permit ACL, causing the port to discard all ingress traffic:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3011 permit ip any 149.124.47.0/24
awplus(config)# access-list 3020 deny ip any any
awplus(config)# interface port1.0.22,port1.0.23
awplus(config_if)# ip access-group 3020
awplus(config_if)# ip access-group 3011
```

- The Net-SNMP command "snmpwalk" may deliver unexpected results. To insure proper results, always precede each "snmpwalk" command with an "snmpgetnext" command of the first desired object.

Resolved Issues For Patch Version 2.1.2.10

- **LLDP and LACP on Port 1.0.28**
  This patch resolves the following issue on port 1.0.28 of all three AT-9000/xx models:

  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 will appear separately as a member. However, when you save and reboot the switch, the LACP configuration will be lost for port 1.0.28.

Resolved Issues For Patch Versions 2.1.2.1 through 2.1.2.9

ACLs on the AT-9000//52

For the AT-9000/52, prior to this release, ACL's were effective on only ports 1 -25. This issue has been resolved and ACL's can now be applied to ports 1 through 52.

SNMP

Each of the following issues has been resolved:

- 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)
- snmpgetnext is getting incorrect info back. (#10615)

Private VLAN

- Private VLANs were previously not supported on the AT-9000/52. When configured, the switch would reboot. This issue is now fixed.

IGMP V3 Report

- The issue has been resolved where the switch would crash 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 upon reboot.

IGMP Snooping

- When you disable IGMP Snooping and the config is saved, this feature now remains disabled after reboot.

New Image File on Web Interface

- You must now log in with a privilege 15 account to be able to load image files and reboot via the web.

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

- Customer Issue# 101223-000029 - Dynamic VLANs were previously enabled by default. This issue has been resolved by disabling the Dynamic VLANs by default.

> **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.
- Customer issue# 101210-000013 - Previously, if the “show dot1x supplicant” command was issued at the same time a client was being authenticated, the switch would crash and reboot. This issue has been resolved.

Web GUI

- Customer issue# 101206-000016 - Subnet Masks were not being display correctly in Web GUI. This issue has been resolved and the correct Subnet Mask is now displayed.

Configuration

- Customer Issue# 110113-000021 - Large configuration files of 300 lines or more were not written or saved correctly. This issue has been resolved.

ACLs

- Customer Issue #110203-000038 - With IGMP snooping enabled, ACLs for Multicast Addresses did not work. This issue has been resolved.

SSH

- Customer Issue #110201-000065 - Stale SSH sessions could lock out management sessions. This issue has been resolved.

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 at **www.alliedtelesis.com/supportcenter**. 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/support**. 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 at **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.

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/purchase/direct**.
To find an office near you, select **www.alliedtelesis.com/office**.

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**.