Allied Telesis

Software Release Note

AlliedWare Plus Version 5.4.2-0.1

For SwitchBlade x908, x900 Series, x610 Series, and x600 Series Switches

Contents

Introduction

This release note describes the new features and enhancements in AlliedWare Plus software version 5.4.2-0.1 since version 5.4.1-0.1. For more information, see the Software Reference for your switch. Software and documentation and software can be downloaded from the Support area of our website at http://www.alliedtelesis.com. Note that to download software, you will need to log in to your account. You can request an account by filling in a form available from the User Login page. Software file details for this version are listed in Table 1 below.

Table 1: Switch models and software file names

Models	Series	Software File	Date	GUI File
x600-24Ts, x600-24Ts/XP, x600-48Ts, x600-48Ts/XP, x600-24Ts-POE, x600-24Ts-POE+	x600	x600-5.4.2-0.1.rel	Mar 2012	gui_542_16.jar
x610-24Ts, x610-24Ts-PoE+, x610-24Ts/X, x610-24Ts/X-PoE+, x610-48Ts, x610-48Ts-PoE+, x610-48Ts/X, x610-48Ts/X-PoE+	x610	x610-5.4.2-0.1.rel	Mar 2012	gui_542_16.jar
x900-12XT/S, x900-24XS, x900-24XT	x900	x900-5.4.2-0.1.rel	Mar 2012	gui_542_16.jar
SwitchBlade x908	SwitchBlade	SBx908-5.4.2-0.1.rel	Mar 2012	gui_542_16.jar

Caution: Using a software version file for the wrong switch model may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in, or omissions arising from, the use of this information.

Acknowledgements

This product includes software developed by the University of California, Berkeley and its contributors.
Copyright ©1982, 1986, 1990, 1991, 1993 The Regents of the University of California.
All rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).
Copyright ©1998-2008 The OpenSSL Project. All rights reserved.

This product includes software licensed under the GNU General Public License available from:
http://www.gnu.org/licenses/gpl2.html

Source code for all GPL licensed software in this product can be obtained from the Allied Telesis GPL Code Download Center at:
http://www.alliedtelesis.com/support/default.aspx

Allied Telesis is committed to meeting the requirements of the open source licenses including the GNU General Public License (GPL) and will make all required source code available.

If you would like a copy of the GPL source code contained in Allied Telesis products, please send us a request by registered mail including a check for US$15 to cover production and shipping costs and a CD with the GPL code will be mailed to you.

GPL Code Request
Allied Telesis Labs (Ltd)
PO Box 8011
Christchurch.
New Zealand

Hardware Support

This version provides the following new hardware support.

For more information on the x610 Series Layer 3+ switches, including Expansion modules, Cables, SFP+ modules and power supply accessories, see the *x610 Data Sheet* and *Hardware Reference*. For more information about the Allied Telesis XEMs, refer to the *High Speed Expansion Modules, XEM* data sheet.

Support for x610 Series Switches

The Allied Telesis x610 family of switches provide a high performing and scalable solution for today's networks, providing an extensive range of port density and uplink-connectivity options. The x610 family builds on the existing x600 family of products adding increased switching capacity and PoE+. With a choice of 24-port and 48-port versions and optional 10 Gigabit uplinks, plus the ability to stack up to eight units with the StackXG expansion module, the x610 family can connect anything from a small workgroup to a large business.

Table 2: x610 switch models and port specifications

Product	10/100/1000 Copper Ports	100/100x SFP Ports	1000X SFP Combo Ports	10Gigabit SFP+ Ports	Max PoE+ Ports
AT-x610-24Ts	24	–	4	–	2*	–
AT-x610-24Ts-PoE+	24	–	4	–	2*	24
AT-x610-24Ts/X	24	–	4	2	4*	–
AT-x610-24Ts/X-PoE+	24	–	4	2	4*	24
AT-x610-48Ts	48	–	4	–	2*	–
AT-x610-48Ts-PoE+	48	–	4	–	2*	48
AT-x610-48Ts/X	48	–	2	2	4*	–
AT-x610-48Ts/X-PoE+	48	–	2	2	4*	48

* with AT-x6EM/XS2 module in standalone switch

AT-x6EM/XS2 Expansion Module for Long Distance Stacking on x610 Series

The AT-x6EM/XS2 expansion module for the x610 Series supports stacking over long distances using standard fibre connections ("VCStack Long Distance Stacking for x610 Series" on page 5). The AT-x6EM/XS2 features 2 x 10 GbE SFP+ ports, which allow for long or short haul connections between each stack member, depending on the distance the inserted SFP+ transceiver supports. The stacking links provided by the AT-x6EM/XS2 operate at 10 Gbps.

Network Operation of Stacking XEM ports

By default, the two ports in the AT-x6EM/XS2 and AT-StackXG stacking modules are used for stacking. Now, when stacking is disabled, these modules provide an extra two 10 GbE network ports. For more information on the x610 Family of Layer 3+ switches, including Expansion modules, Cables, SFP+ modules and power supply accessories, see the *x610 Data Sheet* and *Hardware Reference*.

XEM-2XS Expansion Module for x900 and SBx908

The XEM-2XS features 2 x 10GbE SFP+ ports. Allied Telesis XEMs offer a high degree of flexibility that future-proofs your network investment against changes in network infrastructure, topologies, and physical link requirements.

Achieve high performance with the XEM-2XS 10 Gigabit Ethernet capable XEM. With true ten Gigabits per second throughput for each of the two 10 GbE ports, this XEM provides high-speed, high-capacity copper or fibre uplinks, with up to 20 Gbps of non-blocking throughput per XEM-2XS.

Increased Maximum LAGs and MAC Tables on SBx908 with XEM-2XP, XEM-2XT, XEM-2XS

If a SwitchBlade x908 has only XEM-2XP, XEM-2XT, and/or XEM-2XS XEMs installed (and no XEM-1XP, XEM-12T, or XEM-12S XEMs present), it can now be configured to use a new mode that:

■ increases the maximum number of link aggregators that can be configured to 128 (96 static channel groups and 32 dynamic (LACP) channel groups)

■ increases the maximum size of MAC tables

For more information, see the **platform silicon-profile** command in the *Switching Commands* chapter in the *Software Reference*.

New Features and Enhancements

This software version includes the following main new features in AlliedWare Plus version 5.4.2-0.1 since version 5.4.1-0.1. For a list of all new and enhanced features and commands, see "Changes in this Version" on page 8. For more information about all features on the switch, see the Software Reference for your switch. Unless otherwise stated, all new features and enhancements are available on all switch models running this version of AlliedWare Plus.

VCStack Long Distance Stacking for x610 Series

Long distance stacking allows up to eight units to be stacked over SFP+ fibre connections in conjunction with the AT-x6EM/XS2 module. This is in contrast to the shorter AT-StackXG cables used in conjunction with the AT-StackXG module CX4 interfaces.

Long distance stacking allows a geographically separated stack of x610 units to all be managed as one switch. Any organization with a large or geographically separated site will benefit, including universities and high-rise offices. For more information, see the *Stacking Introduction* chapter in the *Software Reference*.

EPSR Interconnected Rings with Superloop Protection

Where EPSR loops share a common segment and common data VLANs, a break in the common segment can result in a path loop existing across the rings. Superloop protection prevents the existence of these loops by applying priorities to the master nodes. Nodes attached to a common link will send link-down messages only to the highest priority master, thereby allowing only a single master node to unblock its secondary port. For more information, see the *EPSR Introduction and Configuration* chapter in the *Software Reference.*

PIM-SSM

Protocol Independent Multicast—Source Specific Multicast (PIM-SSM) is derived from Protocol Independent Multicast—Sparse Mode (PIM-SM) and is a simplified version of PIM-SM. While PIM-SM supports both a "many-to-many" and a "one-to-many" model, PIM-SSM only supports the "one-to-many" model, also known as a "broadcast application". PIM-SSM builds shortest path trees (SPT) that are directly rooted at the source. For more information, see the *PIM-SM Introduction and Configuration* chapter in the *Software Reference.*

Digital Diagnostics Monitoring (DDM) for SFPs, SFP+s and XFPs

You can now trouble-shoot fiber cable and pluggable issues with diagnostic information about installed pluggable transceivers:

- SFP pluggable transceivers, for SFPs and SFP+s that support DDM (Digital Diagnostic Monitoring)

- XFP pluggable transceivers, for XFPs that support DOM (Digital Optical Monitoring)

For more information, see the *Getting Started* chapter in the *AlliedWare Plus Software Reference*.

TACACS+ Enhancements

AlliedWare Plus now supports TACACS+ login and command accounting enhancements:

- TACACS+ login accounting

- TACACS+ command accounting

- enable password authentication

TACACS+ login and command accounting enables the logging of user sessions and CLI commands entered at the console to create an audit trail for user and console activity.

See the *TACACS+ Introduction and Configuration* and *TACACS+ Commands* chapters in the *Software Reference* for TACACS+ accounting configuration and command information.

Note: TACACS+ accounting and authentication is not supported in the AlliedWare Plus GUI.

IPv6 enhancements

IPv6 on the switches now supports:

- IPv6 RA Guard

  Because an entire IPv6 network configuration can be modified by what is contained in Router Advertisements, the network is vulnerable to rogue messages that are generated either through misconfiguration or due to a malicious attack. RA Guard (RFC6105) defends against these vulnerabilities by blocking RAs and redirects received from the untrusted hosts connected to untrusted ports. For more information, see the *IPv6 Introduction* chapter in the *Software Reference*.

- NTP over IPv6

  In addition to existing support for NTP via IPv4 addresses, NTP on the switch is now able to synchronize time via IPv6. NTP peer and NTP server addresses can now be specified in the form of IPv6 addresses. For more information, see the *NTP Introduction and Configuration* chapter in the *Software Reference.*

- DHCP Relay over IPv6

  While stateless address autoconfiguration is the IPv6 way of automatically configuring hosts' network information, it is not fully supported by some vendors, so Dynamic Host Configuration Protocol is still commonly used. Where the DHCPv6 server does not reside on the same IP subnet as its clients, a relay agent can act as an intermediate device between the two subnets. Alliedware Plus DHCP relay now supports IPv6 addresses, in addition to existing support for IPv4 addresses. For more information, see the *Dynamic Host Configuration Protocol (DHCP) Introduction* chapter in the *Software Reference.*

- DNS Relay over IPv6

  In addition to existing support for DNS relay via IPv4, you can now access a domain name server via an IPv6 network. For more information, see the *Internet Protocol (IP) Addressing and Protocols* chapter in the *Software Reference.*

Privilege level enhancements

AlliedWare Plus now supports 15 privilege levels, divided into 3 groups:

- levels 1-6 provide access to most show commands, in User Exec mode

- levels 7-14 provide access to some more show commands, in Privileged Exec mode

- level 15 provides access to some additional show commands and all configuration commands, in Privileged Exec mode

Network administrators can now control user access to each privilege level by configuring separate enable passwords for each privilege level, and configuring each user's initial privilege level (for locally configured users).

Users can move from their initial privilege level to a higher level by entering the enable command, specifying a privilege level, and entering that level's password.

These enhancements mean that network administrators can manage user access rights to network devices more effectively than was previously possible.

The command changes introduced to support these enhancements are:

- For the **username** command, the meaning of the **level** parameter has changed. This is now the maximum privilege level that you can access without having to enter an enable password.

- The **enable password** and **enable secret** commands now store up to 15 different passwords. You can enter these passwords to access privilege levels greater than their configured privilege level. You can not access levels above your configured privilege level unless an enable password has been configured for that level.

- The **enable** commands now take an optional level parameter that specifies which level you want to access.

- A new command enables AAA authentication to determine the privilege level that you can access for passwords authenticated locally. See the **aaa authentication enable default local** command in the *AAA Commands* chapter.

- Many show commands that were previously available at privilege level 7 are now available at privilege level 1 or 15 instead. To see changes for particular show commands, see **Table 4 on page 10**.

- As before, you can display your current privilege level. See the **show privilege** command in the *User Access Commands* chapter.

Changes in this Version

Table 3 below lists new and modified features in this version as documented in the Software References.

Table 4 on page 10 below lists all new and modified commands in this version, as documented in the Software References.

Table 3: New and modified features in 5.4.2-0.1

Feature/MIB	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
Trouble-shoot fiber and pluggable issues	New	Y	Y	Y	Y	Getting Started	You can now trouble-shoot fiber cable and pluggable issues with diagnostic information about installed XFP and SFP pluggable transceivers, where SFPs are installed in the switch that support DDM (Digital Diagnostic Monitoring) functionality and XFPs are installed in the switch that support DOM (Digital Optical Monitoring) functionality.
Autoboot	New	Y	Y	Y	Y	Creating and Managing Files	The Autoboot feature enables the device to automatically load a specific release file and/or configuration file from external media, such as an SD card, into Flash memory. The Autoboot feature minimizes network downtime by avoiding the need for manual configuration of a replacement device. This feature is enabled only the first time the device is powered up. Subsequently, the Autoboot feature is disabled by default.
Load Balancing for Link Aggregation	New	Y	Y	Y	Y	Link Aggregation Introduction and Configuration	You can now select which packet fields are considered by the algorithm used for load balancing on link aggregators (include source and destination MAC data (Layer 2), or Source and Destination IP data (Layer 3)). This feature was previously available on x900 and SBx908 only; it is now also available on x600 and x610 Series.
Extended VRF-Lite Support Environments	Enhancement	–	Y	Y	Y	VRF-Lite Introduction and Configuration	VRF-Lite now also supports the following features: VCStack (Virtual Chassis Stacking), "route limits," and user-configurable static and dynamic routing resource limits that can be applied on a per-VRF basis. VRF-Lite now supports up to 64 VRF instances—an increase on the 8 instances previously supported.
PIM-SSM	New	Y	Y	Y	Y	PIM-SM Introduction and Configuration	Protocol Independent Multicast - Source Specific Multicast (PIM-SSM) is derived from Protocol Independent Multicast - Sparse Mode (PIM-SM) and is a simplified version of PIM-SM. While PIM-SM supports both a "many-to-many" and a "one-to-many" model, PIM-SSM only supports the "one-to-many" model, also known as a "broadcast application". PIM-SSM builds shortest path trees (SPT) that are directly rooted at the source.
TACACS+	Modified	Y	Y	Y	Y	TACACS+ Introduction and Configuration	AlliedWare Plus now supports TACACS+ login accounting, TACACS+ command accounting, and TACACS+ enable password authentication.

Table 3: New and modified features in 5.4.2-0.1

Feature/MIB	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
IP Multicast Enhancement	New	Y	Y	Y	Y	Multicast Introduction and Commands	You can now configure the switch to forward multicast traffic from a specific source and group ingressing on an upstream VLAN to a single or range of downstream VLANs. For more information, see the **ip multicast route** command.
AT-PRODUCT-MIB	Modified	Y	Y	Y	Y	SNMP MIBs	New object identifiers for Allied Telesis products have been added.
AT-BOARDS-MIB	Modified	Y	Y	Y	Y	SNMP MIBs	New object identifiers for base CPU and expansion boards have been added.
AT-FILEv2-MIB	Modified	Y	Y	Y	Y	SNMP MIBs	New objects have been added for copying, moving and deleting files from local, stack-member and remote sources.

If your existing configurations include commands modified or deprecated in this version (see the Status column), check whether you need to modify these configurations. For full command descriptions, modes and examples, see the appropriate Software Reference for your switch.

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
enable (Privileged Exec mode)	Modified	Y	Y	Y	Y	CLI Navigation Commands	You can now optionally set the privilege level for a session with this command, as well as entering the Privileged Exec mode. If the privilege level is omitted then only users with the maximum privilege level can access Privileged Exec mode without providing the password as specified by the enable password or enable secret commands. If no password is specified then only users with the maximum privilege level set with the username command can assess Privileged Exec mode.
show history	Modified	Y	Y	Y	Y	CLI Navigation Commands	You can now access this command from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
enable password	Modified	Y	Y	Y	Y	User Access Commands	You can now set a local password to control access to various privilege levels with this command. Note that the **enable secret** command is an alias for the **enable password** command, and the **no enable secret** command is an alias for the **no enable password** command.
enable secret	Modified	Y	Y	Y	Y	User Access Commands	You can now set a local password to control access to various privilege levels with this command. Note that the **enable secret** command is an alias for the **enable password** command, and the **no enable secret** command is an alias for the **no enable password** command. Note that if this command is entered then **enable password** is shown in the configuration.
show telnet	Modified	Y	Y	Y	Y	User Access Commands	You can now access this command from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
terminal resize	New	Y	Y	Y	Y	User Access Commands	Use this command to automatically adjust the number of rows of output on the console that the device will display before pausing, to the number of rows configured on the user's terminal.
autoboot enable	New	Y	Y	Y	Y	File Management Commands	Use this command to enable the device to restore a release file and/or a configuration file from external media.
create autoboot	New	Y	Y	Y	Y	File Management Commands	Use this command to create an autoboot.txt file on external media.

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
show autoboot	New	Y	Y	Y	Y	File Management Commands	Use this command to display the Autoboot configuration and status.
show boot	Modified	Y	Y	Y	Y	File Management Commands	This command now displays the status of the Autoboot feature.
show running-config show running-config interface show running-config lldp	Modified	Y	Y	Y	Y	File Management Commands	These commands are now available from the Privileged Exec command mode prompt (**awplus#**) and the Global Configuration prompt (**awplus(config)#**).
max-fib-routes	Modified	Y	Y	Y	Y	System Configuration and Monitoring Commands	This command now enables you to control the maximum number of FIB routes configured. It operates by providing parameters that enable you to configure preset maximums and warning message thresholds.
show cpu	Modified	Y	Y	Y	Y	System Configuration and Monitoring Commands	You can now display CPU processes for individual stack members.
show cpu history	Modified	Y	Y	Y	Y	System Configuration and Monitoring Commands	You can now display CPU process history for individual stack members.
show debugging show diagnostic monitor pcsping	Modified	Y	Y	Y	Y	System Configuration and Monitoring Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show memory	Modified	Y	Y	Y	Y	System Configuration and Monitoring Commands	You can now display CPU memory for individual stack members.
show memory history	Modified	Y	Y	Y	Y	System Configuration and Monitoring Commands	You can now display CPU memory history for individual stack members.
show process	Modified	Y	Y	Y	Y	System Configuration and Monitoring Commands	You can now run this command for individual stack members.
show router-id	Modified	Y	Y	Y	Y	System Configuration and Monitoring Commands	This command is now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show system pluggable	Modified	Y	Y	Y	Y	System Configuration and Monitoring Commands	Support for SFP DDM (Digital Diagnostics Monitoring) and XFP DOM (Digital Optical Monitoring) has been added. You can now select all pluggables on the switch, or a single pluggable on the switch, or a range of pluggables on the switch with the optional <port-list> placeholder.

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
show system pluggable detail	Modified	Y	Y	Y	Y	System Configuration and Monitoring Commands	Support for SFP DDM (Digital Diagnostics Monitoring) and XFP DOM (Digital Optical Monitoring) diagnostics has been added. You can now select all pluggables on the switch, or a single pluggable on the switch, or a range of pluggables on the switch with the optional <port-list> placeholder. Additional DDM and DOM information is displayed, such as OMA (Optical Module Amplitude) and FEC BER (Forward Error Correction Bit Error Rate) and Internal Diagnostic Calibration, if the SFP or XFP pluggable transceiver supports DDM or DOM.
show system pluggable diagnostics	New	Y	Y	Y	Y	System Configuration and Monitoring Commands	Support for SFP DDM (Digital Diagnostics Monitoring) and XFP DOM (Digital Optical Monitoring) diagnostics has been added. This command displays diagnostic information about the pluggable transceivers that are currently installed in your switch. See your Allied Telesis dealer for more information about supported pluggables for your switch.
show counter log show exception log	Modified	Y	Y	Y	Y	Logging Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show log show log config show log permanent	Modified	Y	Y	Y	Y	Logging Commands	These commands are now available from the User Exec command mode prompt (**awplus>**), the Privileged Exec command mode prompt (**awplus#**) and the Global Configuration command mode prompt (**awplus(config)#**).
card provision	New	–	–	–	–	Switching Commands	Use this command to pre-configure a specific empty slot within a chassis ready for inserting a particular card type.
clear mac address-table dynamic	Modified	Y	Y	Y	Y	Switching Commands	Use this command to clear the filtering database of all entries learned for a selected MAC address, an MSTP instance, a switch port interface or a VLAN interface. This command now includes an optional MSTI instance for the switch port.
platform enhancedmode (deprecated)	Deprecated	–	–	Y	Y	Switching Commands	This command has been replaced by the new platform silicon-profile command.

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
platform silicon-profile	New	–	–	Y	Y	Switching Commands	This command replaces the deprecated command platform enhanced-mode. A new silicon profile option for a SwitchBlade x908 with all XEM-2XP, XEM-2XT, and XEM-2XS XEMs installed increases hardware table sizes.
show debugging loopprot show debugging platform packet show flowcontrol interface show loop-protection show mirror show storm-control	Modified	Y	Y	Y	Y	Switching Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show mirror interface	Modified	Y	Y	Y	Y	Switching Commands	This command is now available from the User Exec command mode prompt (**awplus>**), the Privileged Exec command mode prompt (**awplus#**) and the Interface Configuration command mode prompt (**awplus(config-if)#**).
show provisioning (xem-bay)	Modified	–	–	Y	Y	Switching Commands	This command is now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show vlan classifier group interface	New	Y	Y	Y	Y	VLAN Commands	Use this command to display information about all switch port interfaces or a single switch port interface for all configured VLAN classifier groups.
show vlan show vlan classifier group show vlan classifier interface group show vlan classifier rule show vlan private-vlan	Modified	Y	Y	Y	Y	VLAN Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show vlan statistics	Modified	Y	Y	–	–	VLAN Commands	This command is now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
vlan classifier activate	Modified	Y	Y	Y	Y	VLAN Commands	This command can now optionally associate a VLAN identifier with a VLAN classifier group. This command primarily associates and removes VLAN classifier groups with switch port interfaces in Interface Configuration.
clear spanning-tree statistics	Modified	Y	Y	Y	Y	Spanning Tree Commands	You can now optionally specify an MSTI (Multiple Spanning Tree Instance) instance to clear MSTP BPDU statistics with this revised command.

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
instance priority (MSTP)	Modified	Y	Y	Y	Y	Spanning Tree Commands	You can now specify <1-63> MSTIs for a switch port with this revised command to set the priority for the switch to become the root bridge for the specified MSTI.
instance vlan (MSTP)	Modified	Y	Y	Y	Y	Spanning Tree Commands	The range of MSTIs for a switch port has increased from <1-15> to <1-63>. Use this command to create an MST Instance (MSTI), and associate the specified VLANs with it. An MSTI is a spanning tree instance that exists within an MST region (MSTR). An MSTR can contain up to 63 MSTIs.
show debugging mstp	Modified	Y	Y	Y	Y	Spanning Tree Commands	This command is now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show spanning-tree show spanning-tree brief show spanning-tree mst show spanning-tree mst config show spanning-tree mst detail show spanning-tree mst detail interface show spanning-tree mst instance show spanning-tree mst instance interface show spanning-tree mst interface show spanning-tree mst detail interface	Modified	Y	Y	Y	Y	Spanning Tree Commands	These commands are now available from the User Exec command mode prompt (**awplus>**), the Privileged Exec command mode prompt (**awplus#**) and the Interface Configuration mode prompt (**awplus(config-if)#**).
show spanning-tree statistics	New	Y	Y	Y	Y	Spanning Tree Commands	This command displays BPDU (Bridge Protocol Data Unit) statistics for all spanning-tree instances, and all switch ports associated with all spanning-tree instances. Previously, separate show spanning-tree statistics commands were applied to specify particular instances or interfaces, not all instances and interfaces.
show spanning-tree statistics instance	Modified	Y	Y	Y	Y	Spanning Tree Commands	The range of MSTI instances for a switch port increased from <1-15> to <1-63>. This command displays BPDU (Bridge Protocol Data Unit) statistics for the specified MST instance, and all switch ports associated with that MST instance.

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
show spanning-tree statistics instance interface	Modified	Y	Y	Y	Y	Spanning Tree Commands	The range of MSTI instances for a switch port has increased from <1-15> to <1-63>. This command displays BPDU (Bridge Protocol Data Unit) statistics for the specified MST (Multiple Spanning Tree) instance and the specified switch port associated with that MST instance.
show spanning-tree statistics interface	Modified	Y	Y	Y	Y	Spanning Tree Commands	The range of MSTI instances for a switch port increased from <1-15> to <1-63>. This command displays BPDU (Bridge Protocol Data Unit) statistics for the specified switch port, and all MST instances associated with that switch port.
show spanning-tree vlan range-index	New	Y	Y	Y	Y	Spanning Tree Commands	Use this new command to display information about MST (Multiple Spanning Tree) instances and the VLANs associated with them including the VLAN range-index value for the switch.
spanning-tree mst instance spanning-tree mst instance path-cost spanning-tree mst instance priority	Modified	Y	Y	Y	Y	Spanning Tree Commands	The range of MSTIs for a switch port has increased from <1-15> to <1-63>.
spanning-tree mst instance restricted-role	New	Y	Y	Y	Y	Spanning Tree Commands	Use this new command to enable the restricted role for an MSTI (Multiple Spanning Tree Instance) on a switch port. Configuring the restricted role for an MSTI on a switch port prevents the switch port from becoming the root port in a spanning tree topology. Use the no variant of this command to disable the restricted role for an MSTI on a switch port. Removing the restricted role for an MSTI on a switch port allows the switch port to become the root port in a spanning tree topology.
spanning-tree mst instance restricted-tcn	New	Y	Y	Y	Y	Spanning Tree Commands	Use this new command in Interface Configuration mode to set the restricted TCN (Topology Change Notification) value to TRUE for the specified MSTI (Multiple Spanning Tree Instance). Use the no variant of this command in Interface Configuration mode to reset the restricted TCN for the specified MSTI to the default value of FALSE.

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
show debugging lacp show diagnostic channel-group show etherchannel detail show etherchannel summary show lacp-counter show lacp sys-id show port etherchannel	Modified	Y	Y	Y	Y	Link Aggregation Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show debugging power-inline	Modified	Y	Y	–	–	Power over Ethernet Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show power-inline	Modified	Y	Y	–	–	Power over Ethernet Commands	
show power-inline counters	Modified	Y	Y	–	–	Power over Ethernet Commands	
show power-inline interface	Modified	Y	Y	–	–	Power over Ethernet Commands	
show power-inline interface detail	Modified	Y	Y	–	–	Power over Ethernet Commands	
show debugging gvrp show gvrp configuration show gvrp machine show gvrp statistics show gvrp timer	Modified	Y	Y	Y	Y	GVRP Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
arp opportunistic-nd	New	Y	Y	Y	Y	IP Addressing and Protocol Commands	Use this command to enable opportunistic neighbor discovery for the global ARP cache, or a specified named VRF instance. Use the no variant of this command to disable opportunistic neighbor discovery for the global ARP cache, or a specified named VRF instance. Opportunistic neighbor discovery changes the behavior for unsolicited ARP packet forwarding on the switch.
ip name-server	Modified	Y	Y	Y	Y	IP Addressing and Protocol Commands	This command now adds the IPv6 address of a DNS server to the device's list of servers. The DNS client on your device sends DNS queries to devices on this list when trying to resolve a DNS hostname.

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
show debugging ip dns forwarding show debugging ip packet show hosts show debugging ip dns forwarding show ip dns forwarding cache show ip domain-list show ip domain-name show ip forwarding show ip interface show ip irdp show ip irdp interface show ip name-server	Modified	Y	Y	Y	Y	IP Addressing and Protocol Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show ip interface vrf	Modified	–	Y	Y	Y	IP Addressing and Protocol Commands	This command is now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
ipv6 address	Modified	Y	Y	Y	Y	IPv6 Commands	You can now use this command to set the IPv6 address of a VLAN interface and enable IPv6 with an optional eui64 parameter to apply the MAC address of the interface. Note that the MAC address of the default VLAN is applied if the interface does not have a MAC address of its own when specifying the eui64 parameter.
ipv6 address autoconfig	New	Y	Y	Y	Y	IPv6 Commands	Use this new command to enable IPv6 stateless address autoconfiguration (SLAAC) on an interface This configures an IPv6 address on an interface derived from the MAC address on the interface.
ipv6 enable	Modified	Y	Y	Y	Y	IPv6 Commands	This revised command now enables IPv6 with a IPv6 link-local address not with an IPv6 global address. Use this command to enable IPv6 on an interface without an IPv6 global address set for the interface.
ipv6 nd current-hoplimit	New	–	–	Y	Y	IPv6 Commands	Use this new command to specify the advertised current hop limit used between IPv6 Routers.

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
ipv6 nd minimum-ra-interval	New	Y	Y	Y	Y	IPv6 Commands	Use this new command in Interface Configuration mode to set a minimum Router Advertisement (RA) interval for a VLAN interface. Use the no variant of this command in Interface Configuration mode to remove the minimum RA interval for a VLAN interface.
ipv6 nd prefix	Modified	Y	Y	Y	Y	IPv6 Commands	The no-autoconfig and offlink parameters have been added to this command. The all parameter has been added to the no variant of this command. Use this command to specify the IPv6 prefix information that is advertised by the router advertisement for IPv6 address auto-configuration. Use the no parameter with this command to reset the IPv6 prefix.
ipv6 nd ra-interval	Modified	Y	Y	Y	Y	IPv6 Commands	The Router Advertisements (RA) interval range has changed from <3-1800> seconds to <4-1800> seconds. Use this revised command to specify the interval between IPv6 RA transmissions. The no variant of this command resets the IPv6 RA interval to the default of 600 seconds.
ipv6 nd retransmission-time	New	Y	Y	Y	Y	IPv6 Commands	Use this new command to specify the advertised retransmission interval for Neighbor Solicitation in milliseconds between IPv6 Routers.
ipv6 opportunistic-nd	New	Y	Y	Y	Y	IPv6 Commands	Use this new command to enable opportunistic neighbor discovery for the global IPv6 ARP cache. Use the no variant of this command to disable opportunistic neighbor discovery for the global IPv6 ARP cache. Opportunistic neighbor discovery changes the behavior for unsolicited ARP packet forwarding on the switch.
show ipv6 forwarding show ipv6 interface brief show ipv6 neighbors show ipv6 route show ipv6 route summary	Modified	Y	Y	Y	Y	IPv6 Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show ip route show ip route database show ip route summary	Modified	Y	Y	Y	Y	Routing Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
show debugging rip show ip protocols rip show ip rip show ip rip database show ip rip interface	Modified	Y	Y	Y	Y	RIP Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show ip rip vrf database show ip rip vrf interface	Modified	–	Y	Y	Y	RIP Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show debugging ipv6 rip show ipv6 protocols rip show ipv6 rip show ipv6 rip database show ipv6 rip interface	Modified	Y	Y	Y	Y	RIPng Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show debugging ospf show ip ospf show ip ospf border-routers show ip ospf database show ip ospf database asbr-summary show ip ospf database external show ip ospf database network show ip ospf database nssa-external show ip ospf database opaque-area show ip ospf database opaque-as show ip ospf database opaque-link show ip ospf database router	Modified	Y	Y	Y	Y	OSPF Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show ip ospf database summary show ip ospf interface show ip ospf neighbor show ip ospf route show ip ospf virtual-links show ip protocols ospf	Modified	Y	Y	Y	Y	OSPF Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
show debugging ipv6 ospf show ipv6 ospf show ipv6 ospf database show ipv6 ospf database external show ipv6 ospf database network show ipv6 ospf database router show ipv6 ospf interface show ipv6 ospf neighbor show ipv6 ospf route	Modified	Y	Y	Y	Y	OSPFv3 for IPv6 Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
debug bgp undebug bgp	Modified	Y	Y	Y	Y	BGP Commands	Use these commands to turn on or of one or more BGP debug options. These commands now have the option to debug for BGP NHT (Next Hop Tracking). You can also now issue this command from Privileged Exec and Global Configuration command modes at the **awplus#** and **awplus(config)#** prompts respectively.
show bgp nexthop-tracking show bgp nexthop-tree-details show debugging bgp show ip bgp show ip bgp attribute-info show ip bgp cidr-only show ip bgp community show ip bgp community-info show ip bgp community-list show ip bgp dampening show ip bgp filter-list	Modified	Y	Y	Y	Y	BGP Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
show ip bgp inconsistent-as show ip bgp longer-prefixes show ip bgp neighbors show ip bgp neighbors connection-retrytime show ip bgp neighbors hold-time show ip bgp neighbors keepalive show ip bgp neighbors keepalive-interval show ip bgp neighbors notification show ip bgp neighbors open show ip bgp neighbors rcvd-msgs show ip bgp neighbors sent-msgs show ip bgp neighbors update show ip bgp paths show ip bgp prefix-list show ip bgp quote-regexp show ip bgp regexp show ip bgp route-map	Modified	Y	Y	Y	Y	BGP Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show ip bgp scan show ip bgp summary show ip bgp view show ip bgp view neighbors show ip bgp view summary show ip community-list show ip extcommunity-list show ip protocols bgp	Modified	Y	Y	Y	Y	BGP Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show route-map	Modified	Y	Y	Y	Y	Route Map Commands	This command is now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
max-fib-routes (VRF)	Modified	–	Y	Y	Y	VRF-Lite Commands	This command now enables you to control the maximum number of FIB routes configured for a VRF Instance. It operates by providing parameters that enable you to configure preset maximums and warning message thresholds.

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
max-static-routes	Modified	–	Y	Y	Y	VRF-Lite Commands	This command now enables you to set the maximum number of static routes (excluding FIB—Forwarding Information Base routes) for VRF Instances.
show ip vrf show ip vrf detail show ip vrf	Modified	–	Y	Y	Y	VRF-Lite Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
ip multicast route	New	Y	Y	Y	Y	Multicast Introduction and Commands	Use this command to add a static multicast route for a specific multicast source and group address to the multicast Routing Information Base (RIB).
ip multicast wrong-vif-suppression	New	Y	Y	Y	Y	Multicast Introduction and Commands	Use this command to prevent unwanted multicast packets received on an unexpected VLAN being trapped to the CPU.
show ip mroute show ip mvif show ip rpf	Modified	Y	Y	Y	Y	Multicast Introduction and Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
ip igmp ssm	New	Y	Y	Y	Y	IGMP and IGMP Snooping Commands	Use this command to define a non-default Source Specific Multicast (SSM) range of IP multicast addresses in IGMP. Incoming IGMPv1 and IGMPv2 join requests are ignored if the multicast IP address is in the SSM range and no SSM mapping is configured for these addresses. By default, the SSM range is 232/8.
ip igmp ssm-map enable	New	Y	Y	Y	Y	IGMP and IGMP Snooping Commands	Use this command to enable Source Specific Multicast (SSM) mapping on the device.
ip igmp ssm-map static	New	Y	Y	Y	Y	IGMP and IGMP Snooping Commands	Use this command to specify the static mode of defining Source Specific Multicast (SSM) mapping. SSM statically assigns sources to IGMPv1 and IGMPv2 groups to translate such (*,G) groups' memberships to (S,G) memberships for use with PIM-SSM.
ip igmp startup-query-count	New	Y	Y	Y	Y	IGMP and IGMP Snooping Commands	Use this command to configure the IGMP startup query count on a VLAN interface in Interface Configuration mode. The IGMP startup query count is the number of general query messages sent at startup. The default IGMP startup query count is 2.

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
ip igmp startup-query-interval	New	Y	Y	Y	Y	IGMP and IGMP Snooping Commands	Use this command to configure the IGMP startup query interval for a VLAN interface in Interface Configuration mode. The IGMP startup query interval is the amount of time in seconds between successive IGMP General Query messages sent by a querier during startup. The default IGMP startup query interval is one quarter of the IGMP query interval value.
show debugging igmp	Modified	Y	Y	Y	Y	IGMP and IGMP Snooping Commands	This command is now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show ip igmp groups show ip igmp interface show ip igmp proxy show ip igmp snooping mrouter show ip igmp snooping routermode show ip igmp snooping statistics	Modified	Y	Y	Y	Y	IGMP and IGMP Snooping Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
ip pim ssm	New	Y	Y	Y	Y	PIM-SM Commands	Use this command to define the Source Specific Multicast (SSM) range of IP multicast addresses.
show debugging pim sparse-mode show ip pim sparse-mode bsr-router show ip pim sparse-mode interface show ip pim sparse-mode interface detail show ip pim sparse-mode mroute show ip pim sparse-mode mroute detail show ip pim sparse-mode neighbor show ip pim sparse-mode nexthop show ip pim sparse-mode rp-hash show ip pim sparse-mode rp mapping	Modified	Y	Y	Y	Y	PIM-SM Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
show debugging pim dense-mode show ip pim dense-mode interface show ip pim dense-mode interface detail show ip pim dense-mode mroute show ip pim dense-mode neighbor show ip pim dense-mode neighbor detail show ip pim dense-mode nexthop	Modified	Y	Y	Y	Y	PIM-DM Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show ipv6 mld groups show ipv6 mld interface show ipv6 mld snooping mrouter show ipv6 mld snooping statistics	Modified	Y	Y	Y	Y	MLD Snooping Introduction and Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show access-group	Modified	–	–	Y	Y	IPv4 Hardware Access Control List (ACL) Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show access-list (IPv4 Hardware ACLs)	Modified	Y	Y	Y	Y	IPv4 Hardware Access Control List (ACL) Commands	This command is now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show access-list (IPv4 Software ACLs) show dos interface show ip access-list show ip prefix-list	Modified	Y	Y	Y	Y	IPv4 Software Access Control List (ACL) Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show ipv6 access-list (IPv6 Hardware ACLs)	Modified	–	–	Y	Y	IPv6 Hardware Access Control List (ACL) Commands	This command is now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
ipv6 access-list extended proto	New	Y	Y	Y	Y	IPv6 Software Access Control List (ACL) Commands	Use this command when configuring an IPv6 extended access-list for filtering frames that permit or deny packets with a specific value based on the IP protocol number specified. The no variant of this command removes a specified IPv6 extended access-list with an IP protocol number.
show ipv6 access-list (IPv6 Software ACLs)	Modified	Y	Y	Y	Y	IPv6 Software Access Control List (ACL) Commands	This command is now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
police-aggregate	Modified	–	–	Y	Y	QoS Commands	Use this command to apply a previously created aggregate-policer to the class-map. The command keyword has changed from police aggregate to police-aggregate. Note that a console message is displayed indicating the previous command keyword police aggregate is deprecated and is available as an alias to the police-aggregate keyword.
show class-map show mls qos aggregate-policer show mls qos interface policer-counters show mls qos interface queue-counters show mls qos interface storm-status show mls qos maps cos-queue show mls qos maps premark-dscp show policy-map	Modified	Y	Y	Y	Y	QoS Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show mls qos fabric-queue show mls qos maps policed-dscp show mls qos aggregate-policer show mls qos fabric-queue show mls qos queue-set	Modified	–	–	Y	Y	QoS Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show debugging dot1x	Modified	Y	Y	Y	Y	802.1X Commands	This command is now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
platform mac-vlan-hashing-algorithm	New	Y	Y	–	–	Authentication Commands	This command enables you to change the MAC VLAN hash-key-generating algorithm. It is used when MAC hash collisions occur.
aaa accounting commands	New	Y	Y	Y	Y	AAA Commands	With this command you can configure and enable TACACS+ command accounting.
aaa accounting login	Modified	Y	Y	Y	Y	AAA Commands	With this command you can now configure TACACS+ accounting for login shell sessions.
aaa accounting update	Modified	Y	Y	Y	Y	AAA Commands	This command now enables periodic accounting reporting to a TACACS+ accounting server.

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
aaa authentication enable default group tacacs+	New	Y	Y	Y	Y	AAA Commands	This command enables AAA authentication to determine the privilege level a user can access for passwords authenticated against the TACACS+ server.
aaa authentication enable default local	New	Y	Y	Y	Y	AAA Commands	This command enables AAA authentication to determine the privilege level a user can access for passwords authenticated locally.
show debugging aaa	Modified	Y	Y	Y	Y	AAA Commands	This command is now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show debugging radius show radius show radius statistics	Modified	Y	Y	Y	Y	RADIUS Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show tacacs+	Modified	Y	Y	Y	Y	TACACS+ Commands	This command is now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show crypto pki certificates show crypto pki certificates local-radius-all-users show crypto pki certificates user show crypto pki trustpoints show radius local-server group show radius local-server nas show radius local-server statistics show radius local-server user show crypto key hostkey show crypto key pubkey-chain knownhosts show crypto key pubkey-chain userkey show crypto key userkey	Modified	Y	Y	Y	Y	Local RADIUS Server Commands	These commands are now available from the User Exec command mode prompt (**awplus>**), the Privileged Exec command mode prompt (**awplus#**) and the Global Configuration prompt (**awplus(config)#**).
show running-config ssh show ssh show ssh client show ssh server show ssh server allow-users show ssh server deny-users	Modified	Y	Y	Y	Y	Secure Shell (SSH) Commands	These commands are now available from the User Exec command mode prompt (**awplus>**), the Privileged Exec command mode prompt (**awplus#**) and the Global Configuration prompt (**awplus(config)#**).

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
show debugging arp security show debugging ip dhcp snooping show ip dhcp snooping show ip dhcp snooping acl show ip dhcp snooping agent-option show ip dhcp snooping binding show ip dhcp snooping interface show ip dhcp snooping statistics show ip source binding	Modified	Y	Y	Y	Y	DHCP Snooping Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
interface (VRRP) (deprecated)	Deprecated	Y	Y	Y	Y	VRRP Commands	The interface (VRRP) command has been deprecated. Use the router vrrp (interface) command to configure VRRP and define the interface that will participate in virtual routing to send and receive advertisement messages.
router vrrp (interface)	Modified	Y	Y	Y	Y	VRRP Commands	Use this command to configure VRRP and define the interface that will participate in virtual routing to send and receive advertisement messages. This command allows you to enter the Router Configuration mode. Note that the interface must be specified, and that the interface (VRRP) command has been deprecated from this version.
show debugging vrrp show vrrp show vrrp counters show vrrp (session)	Modified	Y	Y	Y	Y	VRRP Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
epsr priority	New	Y	Y	Y	Y	EPSR Commands	This command sets the priority of an EPSR instance on an EPSR node. Priority is used to prevent superloops forming under fault conditions with particular ring configurations.
show debugging epsr show epsr show epsr word show epsr word counters show epsr counters	Modified	Y	Y	Y	Y	EPSR Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show counter ntp show ntp associations show ntp status	Modified	Y	Y	Y	Y	NTP Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
show counter dhcp-client show counter dhcp-relay show counter dhcp-server show dhcp lease show ip dhcp binding show ip dhcp pool show ip dhcp-relay show ip dhcp server statistics show ip dhcp server summary	Modified	Y	Y	Y	Y	Dynamic Host Configuration Protocol (DHCP) Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show counter snmp-server show debugging snmp	Modified	Y	Y	Y	Y	SNMP Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
lldp port-number-type	New	Y	Y	Y	Y	LLDP Commands	This command sets the type of port identifier used to enumerate, that is to count, the LLDP MIB local port entries. This command also enables you to optionally set an interface index to enumerate the LLDP MIB local port entries, if required by your management system.
show lldp	Modified	Y	Y	Y	Y	LLDP Commands	This command is now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**). This command now displays the Port Number Type, which is the type of port identifier to enumerate LLDP MIB local port entries. Port Number Type is set by the new lldp port-number-type command.
show debugging lldp show lldp interface show lldp local-info show lldp neighbors show lldp neighbors detail show lldp statistics show lldp statistics interface show location	Modified	Y	Y	Y	Y	LLDP Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show rmon alarm show rmon event show rmon history show rmon statistics	Modified	Y	Y	Y	Y	RMON Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).

Table 4: New and modified commands in 5.4.2-0.1

Command	Status	x600	x610	x900	SBx908	Software Reference Chapter	Description
type stack master-fail	New	–	–	–	–	Trigger Commands	This command initiates the action of a pre-configured trigger to occur when the Control Fabric Card enters the fail-over state.
type usb	New	–	–	–	–	Trigger Commands	Use this command to configure a trigger that activates on either the removal or the insertion of a USB storage device.
show counter ping-poll show ping-poll	Modified	Y	Y	Y	Y	Ping Polling Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show debugging sflow	Modified	Y	Y	Y	Y	sFlow Commands	This command is available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show counter stack show debugging stack show provisioning (stack-member)	Modified	Y	Y	Y	Y	Stacking Commands	These commands are now available from the User Exec command mode prompt (**awplus>**) and the Privileged Exec command mode prompt (**awplus#**).
show stack resiliencylink	New	Y	Y	Y	Y	Stacking Commands	Use this command to display information about the current status of the resiliency-link across the members of the stack.
stack mixed-mode	New	–	Y	–	–	Stacking Commands	Use this command to combine x610 and x600 switches in a VCStack.
switch provision	Modified	–	Y	–	–	Stacking Commands	Two additional parameters have added that allow you to provision either an x610-24 or an x610-48 switch as a stack member.

Installing this Software Version

To use this software version, your switch must already be running AlliedWare Plus. Contact your distributor or reseller for more information. The software file is available from the Support area of the Allied Telesis website at: http://www.alliedtelesis.com.

To install and enable this software version, use the following steps:

1. **Copy the software version file (.rel) onto your TFTP server.**

2. **If necessary, delete or move files to create space in the switch's Flash memory for the new file.**

   To see the memory usage, use the command:

   awplus# `show file systems`

   To list files, use the command:

   awplus# `dir`

   To delete files, use the command:

   awplus# `del <filename>`

   You cannot delete the current boot file.

3. **Copy the new release from your TFTP server onto the switch.**

   awplus# `copy tftp flash`

   Follow the onscreen prompts to specify the server and file.

4. **Set the switch to reboot with the new software version:**

   for x610 series switches:

   awplus#`configure terminal`

   awplus(config)# `boot system x610-5.4.2-0.1.rel`

   for x600 series switches:

   awplus#`configure terminal`

   awplus(config)# `boot system x600-5.4.2-0.1.rel`

   for x900 series switches:

   awplus#`configure terminal`

   awplus(config)# `boot system x900-5.4.2-0.1.rel`

   or for SwitchBlade x908 switches:

   awplus# `configure terminal`

   awplus(config)# `boot system SBx908-5.4.2-0.1.rel`

   Return to Privileged Exec mode and check the boot settings, by using the commands:

   awplus(config)#`exit`

   awplus# `show boot`

5. **Reboot using the new software version.**

   awplus# `reload`

Installing the GUI

This section describes how to install and set up the AlliedWare Plus GUI using an SD card or a TFTP server. The GUI Java applet file is available in a compressed (**.zip**) file from the Support area of the Allied Telesis website: http://www.alliedtelesis.com. The version number in the GUI Java applet filename (**.jar)** gives the earliest version of the software file (**.rel**) that the GUI can operate with.

To install and run the AlliedWare Plus GUI requires the following system products and setup:

- PC Platform:
  Windows XP SP2 and up / Windows Vista SP1 and up

- Browser: (must support Java Runtime Environment (JRE) version 6)
  Microsoft Internet Explorer 7.0 and up / Mozilla Firefox 2.0 and up

To install the GUI on your switch, use the following steps:

1. **Copy to the GUI Java applet file (.jar extension) onto your TFTP server or SD card.**

2. **Connect to the switch's management port, then log into the switch.**

3. **If necessary, delete or move files to create space in the switch's Flash memory for the new file.**
   To see the memory usage, use the command:

   awplus# `show file systems`

   To list files, use the command:

   awplus# `dir`

   To delete files, use the command:

   awplus# `del <filename>`

   You cannot delete the current boot file.

4. **Assign an IP address for connecting to the GUI. Use the commands:**

   awplus# `configure terminal`

   awplus(config)# `interface vlan1`

   awplus(config-if)#`ip address <address>/<prefix-length>`

   Where <address> is the IP address that you will subsequently browse to when you connect to the GUI Java applet. For example, to give the switch an IP address of 192.168.2.6, with a subnet mask of 255.255.255.0, use the command:

   awplus(config-if)# `ip address 192.168.2.6/24`

5. **If required, configure a default gateway for the switch.**

   awplus(config-if)# `exit`

   awplus(config)# `ip route 0.0.0.0/0 <gateway-address>`

   Where <gateway-address> is the IP address for your gateway device. You do not need to define a default gateway if you browse to the switch from within its own subnet.

6. **Copy the GUI file onto your switch from the TFTP server or SD card.**

   TFTP server: Use the command:

   ```
   awplus# copy tftp://<server-address>/<filename.jar> flash:/
   ```

   where *<server-address>* is the IP address of the TFTP server, and where *<filename.jar>* is the filename of the GUI Java applet.

   SD card: Insert the SD card into the SD slot on the front of your switch, and use the command:

   ```
   awplus# copy card:/<filename.jar> flash:/
   ```

   where *<filename.jar>* is the filename of the GUI Java applet.

7. **Create a user account for logging into the GUI.**

   ```
   awplus(config)# username <username> privilege 15 guiuser password
                   <password>
   ```

   You can create multiple users to log into the GUI. For information about the **username** command, see the AlliedWare Plus Software Reference.

8. **Log into the GUI.**

   Start a browser and enter the switch's IP address. The GUI starts up and displays a login screen. Log in with the username and password specified in the previous step.

Errata to the Software Reference

The following update is a correction to the *Software Reference for AlliedWare Plus 5.4.2*

ping ipv6

This command sends a query to another IPv6 host (send Echo Request messages).

> **Note** Use of the `interface` parameter keyword, plus an interface or an interface range, with this command is only valid when pinging an IPv6 link local address.

Syntax
```
ping ipv6 [<host>|<ipv6-address>] [repeat {<1-2147483647>|
    continuous}] [size <10-1452>] [interface <interface-list>]
    [timeout <1-65535>]
```

Parameter	Description
`<ipv6-addr>`	The destination IPv6 address. The IPv6 address uses the format X:X::X:X.
`<hostname>`	The destination hostname.
`repeat`	Specify the number of ping packets to send.
`<1-2147483647>`	Specify repeat count. The default is 5.
`size <10-1452>`	The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).
`interface <interface-list>`	The interface or range of configured IP interfaces to use as the source in the IP header of the ping packet.
`timeout <1-65535>`	The time in seconds to wait for echo replies if the ARP entry is present, before reporting that no reply was received. If no ARP entry is present, it does not wait.
`repeat`	Specify the number of ping packets to send.
`<1-2147483647>`	Specify repeat count. The default is 5.
`continuous`	Continuous ping.
`size <10-1452>`	The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).
`timeout <1-65535>`	The time in seconds to wait for echo replies if the ARP entry is present, before reporting that no reply was received. If no ARP entry is present, it does not wait.

Mode User Exec and Privileged Exec

Example

```
awplus# ping ipv6 2001:0db8::a2
```

Related Commands traceroute ipv6