AlliedWare Plus™ Software Maintenance Release Note

Software Version 5.4.1-2.12

For SwitchBlade x908, x900-12XT/S, x900-24 Series, x600 and x610 Series Switches

This document describes the new features, enhancements, and issues addressed in AlliedWare Plus software maintenance version 5.4.1-2.12. Version details are listed in the following table:

Models	Series	Release File	Date	GUI file
x600-24Ts, x600-24Ts/XP, x600-24Ts-POE, x600-48Ts, x600-48Ts/XP	x600	r6-5.4.1-2.12.rel	Dec 2012	gui_541_25.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	r7-5.4.1-2.12 rel	Dec 2012	gui_541_25.jar
SwitchBlade x908	SwitchBlade	r1-5.4.1-2.12.rel	Dec 2012	gui_541_25.jar
x900-12XT/S, x900-24, x900-12XT/S, x900-24XT, x900-24XT-N, x900-24XS	x900	r1-5.4.1-2.12.rel	Dec 2012	gui_541_25.jar

This Release Note includes:

Caution: *Information in this document 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.*

Contents

Installing and enabling this version

To use this version, your switch must already be running AlliedWare Plus. Contact your distributor or reseller for more information.

To install this version, perform the following:

1. Put the version file onto your TFTP server.
2. If necessary, delete or move files to create space in the switch's Flash memory for the new file.

   Note that you cannot delete the current boot file.

   To list files, use the command:

   ```
   awplus#dir
   ```

   To see the memory usage, use the command:

   ```
   awplus#show file systems
   ```

   To delete files, use the command:

   ```
   awplus#del <filename>
   ```
3. Copy the new release from your TFTP server onto the switch.

   To do this, enter Privileged Exec mode and use the command:

   ```
   awplus#copy tftp flash
   ```

   Follow the onscreen prompts to specify the server and file.
4. Set the switch to boot from the new release.

   Enter Global Configuration mode.

   On the x600 Series switches, use the command:

   ```
   awplus(config)#boot system r6-5.4.1-2.12.rel
   ```

   On the x610 Series switches, use the command:

   ```
   awplus(config)#boot system r7-5.4.1-2.12.rel
   ```

   On the x900 Series and SwitchBlade x908 switches, use the command:

   ```
   awplus(config)#boot system r1-5.4.1-2.12.rel
   ```

   If desired, check the boot settings by entering Privileged Exec mode and using the following command:

   ```
   awplus#show boot
   ```
5. Reboot.

   To do this, enter Privileged Exec mode and use the command:

   ```
   awplus#reload
   ```

New Features and Enhancements in 5.4.1-2.11

CR	Module	Description

CR00035017	**L2 Switching**	The **snmp-server enable trap** command now has a new **thrash-limit** option, which enables or disables the sending of MAC address thrash limiting traps:
		`snmp-server enable trap [thrash-limit] [<other-options>]`
		`no snmp-server enable trap [thrash-limit] [<other-options>]`

New Features and Enhancements in 5.4.1-2.9

Synchronise hardware ACLs: commit

A new commit command has been added to apply new access-list configuration to hardware immediately, and force the associated hardware and software ACLs to synchronize (CR00034077).

commit

Use this command to commit the ACL filter to hardware immediately, without exiting the Hardware ACL Configuration mode.

Syntax `commit`

Mode IPv4 or IPv6 Hardware ACL Configuration

Usage Normally, when a hardware ACL is edited, the new configuration state of the ACL is not written to hardware until you exit Hardware ACL Configuration mode. By entering this command you can ensure that the current state of a hardware access-list that is being edited is written to hardware immediately.

Scripts typically do not include the **exit** command to exit configuration modes, potentially leading to ACL filters in hardware not being correctly updated. Using this **commit** command in a configuration script after specifying a hardware ACL filter ensures that it is updated in the hardware.

Examples To update the hardware with the ACL filter configuration, use the command:

```
awplus(config-ipv6-acl)# commit
```

Related Commands access-list hardware
ipv6 access-list

New Features and Enhancements in 5.4.1-2.8

CR	Module	Description
CR00033931	**IPv6 DNS Relay**	DNS Relay debug has been enhanced to display IPv6 addresses in addition to the existing support for IPv4 addresses.
CR00032874	**QoS**	The processing speed of adding policy maps to multiple interfaces has been improved, enabling the CLI to respond to subsequent commands quicker.

CR00034174	**IGMP**	Previously, if no Source Specific Multicast (SSM) mapping was configured, IGMP packets for group addresses in the range of 232/8 were ignored. This was not configurable even though in PIM the SSM group addresses can be set to a non-default address range.
		This issue has been resolved with a new global configuration mode command to configure a non-default SSM range for IGMP:
		Command
		`ip igmp ssm (range {<accesslist>| <named-accesslist>})`
		
		`no ip igmp ssm (range {<accesslist>| <named-accesslist>})`
		Parameters
		`accesslist` <1-99> Simple access-list
		`named-accesslist` Named access-list
		Example
		Configure a non-default SSM range:
		`access-list 10 permit 224.1.1.0 0.0.0.255`
		`ip igmp ssm range 10`
		Return to default configuration:
		`no ip igmp ssm`

New Features and Enhancements in 5.4.1-2.7

SFP Digital Diagnostics Monitoring (DDM) (CR00031323)

x900 only. Support for SFP Digital Diagnostics Monitoring (DDM) has been added. A new **diagnostics** parameter has been added to the existing **show system pluggable** command. The command parameter instructs the system to read diagnostics information from installed SFP and SFP Plus pluggable devices that support the DDM feature and display the information.

The complete command is:

show system pluggable diagnostics

Additionally, an extra line of diagnostics output is now displayed via the existing command **show system pluggable detail**.

The new line of output serves to indicate whether or not the installed SFP supports diagnostics and is displayed as follows:

Diagnostic Calibration [Internal | External | -]

where a '-' character indicates that diagnostics is not supported by the SFP module.
Currently, the **show system pluggable diagnostics** command only supports those SFPs where diagnostics information is internally calibrated.

Example Output

```
awplus#show sys pluggable diagnostics
System Pluggable Information Diagnostics
Port1.1.1 Status Alarms Warnings
Reading Alarm Max Min Warning Max Min
Temp: (Degrees C) 36.461 - 0.000 0.000 - 0.000 0.000
Vcc: (Volts) 3.374 - 0.000 0.000 - 0.000 0.000
Tx Bias: (mA) 2.499 - 0.000 0.000 - 0.000 0.000
Tx Power: (mW) 2.193 - 0.000 0.000 - 0.000 0.000
Rx Power: (mW) 0.015 Low 0.000 0.000 Low 0.000 0.000
Rx LOS: Rx Down

awplus#show sys pluggable detail
System Pluggable Information Detail

Port1.1.1
==========
Vendor Name: ATI
Device Name: AT-SPSX
Device Type: 1000BASE-SX
Serial Number: A03240R082100004
Manufacturing Datecode: 08051900
SFP Laser Wavelength: 850nm
Link Length Supported
Single Mode Fiber : -
OM1 (62.5um) Fiber: 300m
OM2 (50um) Fiber : 550m
Diagnostic Calibration: Internal
-----------------------------------------------------------------
```

New Features and Enhancements in 5.4.1-2.6

Unless otherwise stated, each feature applies to all switches supported by this software version.

Announcing the release of the x610 family of 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.

Note: *All customers should ensure their x610 switches have Software Version 5.4.1-2.6 or later installed.*

Models and port specifications

The x610 switch models and port specifications are listed in the table below:

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*

x610 key features

The Allied Telesis x610 family of Layer 3+ switches offer an impressive set of features in a high-value package that is ideal for enterprise network applications.

x610 Family Features Include:

- VCStack
- Mixed-mode Stacking
- Long-distance Stacking
- Ethernet Protection Switching Rings (EPSRing)
- Industry-standard CLI
- Access Control Lists (ACLs)
- Industry-leading Quality of Service
- Terminal Access Controller Access–Control System Plus (TACACS+) Authentication
- Virtual Routing and Forwarding (VRF-Lite)

  An 802.1q switch port that is a tagged member of multiple VLANs can also span multiple VRF instances with this product family.
- Link Layer Discovery Protocol – Media Endpoint Discovery (LLDP – MED)
- Voice VLAN
- Open Shortest Path First (OSPFv3)
- Network Access Control (NAC)
- Tri-authentication
- sFlow
- Power over Ethernet Plus (PoE+)
- Eco-friendly support

  You can conserve power by enabling the eco-friendly feature. When enabled, this feature disables power to the port LEDs and a change of port status will not affect the display of the associated LED.

x610 Graphical User Interface (GUI)

The GUI simplifies network performance monitoring and network event troubleshooting. The x610 GUI file name is: **gui_541_25.jar**

x610 power supplies

The x610-24Ts-POE+, x610-24Ts/X-POE+, x610-48Ts-POE+ and x610-48Ts/X-POE+ switches are supplied with a factory installed blank panel on the power supply port.

The following power supplies (PSU) can be installed in these switches:

- 250W (AT-PWR250-xx) AC or DC PSU,
- 800W (AT-PWR800-xx) AC PSU, or
- 1200W (AT-PWR1200-xx) AC PSU

Note that the AT-PWR250-xx supplies system power only to the switch. Either an AT-PWR800-xx or an AT-PWR1200-xx is required to supply power to the PoE+ ports in addition to system power to the switch.

The Redundant Power Supply connector on an x610 switch rear panel can connect to an optional Redundant Power Supply (RPS), the AT-RPS3000. This RPS can provide power to the switch in the event of a failure of the switch's internal power supply.

AT-x6EM/XS2 x610 expansion module

The AT-x6EM/XS2 is a new expansion module that can be fitted to the x610 in order to support stacking over long distances using standard fibre connections.

The stacking links provided by the AT-x6EM/XS2 operate at 10 Gbps.

When stacking is disabled, the AT-Stack module provides and extra two 10 GbE network ports. For more detail on this, see Network Port Operation for AT-x6EM/XS2 and AT-StackXG, on page 10.

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.

Activity monitoring

There is one bi-color LED per port on the AT-x6EM/XS2 in addition to the corresponding stacking LED on the front of the x610 to indicate the link and activity of the SFP+ transceivers.

The x610 front panel LED indicates the following:

- Solid green – 10 Gbps link
- Flashing green – Activity
- Off – No link, no transceiver or invalid transceiver.

The rear LED on the AT-x6EM/XS2 indicates the following:

- Solid green – 10 Gbps link
- Flashing green – TX activity
- Off – No Link, no transceiver or invalid transceiver

Network Port Operation for AT-x6EM/XS2 and AT-StackXG

By **default,** the two ports AT-Stack modules are used for stacking. However, when stacking is disabled, the AT-Stack module provides an **extra two** 10 GbE **network** ports.To achieve this, you must disable stacking with the command **no stack <member-id> enable**, and then reboot the device to switch between stacking and network modes.

In network mode, the extra two 10 GbE ports are visible and configurable without the AT-Stack module present. The ports are named with a 1 in the board index member of the port triplet. For example, port1.1.1 and port1.1.2 in network-mode will correspond to stack ports 1.1.1 and 1.1.2 in stacking mode.

Note: *Provisioning will not be aware of the expansion module ports as they are not configurable in stacking-mode. However, the no stack <member-id> enable command can be used without a stack module being present in the switch. In network mode the ports will operate at 10Gbps for both AT-x6EM/XS2 and AT-StackXG stacking modules. When in stacking mode, the AT-StackXG operates at 12Gbps, whereas the AT-x6EM/XS2 still operates at 10Gbps.*

The AT-Stack module hardware is hot-swappable and allows up to eight units to be stacked. In network mode the AT-Stack modules will be fully hot-swappable. In stacking mode the AT-Stack modules will be hot-replaceable. If an ATStack module is inserted into a switch with stacking enabled the hot-insert event will be logged but stacking operation will not be available until the switch is restarted. In stacking mode it will not be possible to replace a AT-StackXG with an AT-x6EM / XS2, or vice versa, without restarting the unit. In both network and stacking mode the SFP+ transceivers in a AT-x6EM / XS2 will be hotswappable.

Module	Description
AT-x6EM/XS2-00	Expansion module (2 x SFP+)
AT-StackXG-00	Expansion module (2 x CX4) with one AT-StackXG/0.5-00 cable included
AT-StackXG/0.5-00	0.5 meter cable for stacking
AT-StackXG/1-00	1 meter cable for stacking

For additional 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.

Long distance stacking

Long distance stacking, in essence, currently allows up to four 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 customers to have a geographically separated stack of x610 units all managed as one switch. Any customer with a large or geographically separated site will benefit, including universities and high-rise offices.

Specifying a single stack member

The output of the commands **show cpu**, **show cpu history**, **show memory**, **show memory history**, and **show process** have been extended to allow you to specify a single stack member.

TACACS+ Accounting and Authentication improvements

AlliedWare Plus supports basic TACACS+ login Authentication and login Authorisation functionality from AW+ version 5.4.1 onwards.

TACACS+ services have been further enhanced to implement support for enable password authentication. Support for TACACS+ login accounting and command accounting has also been implemented.

New commands are documented in the following sections:

- “Define the method list for TACACS+ login authentication” on page 1.5
- “Define the method list for TACACS+ enable password authentication” on page 1.6
- “Define the method for TACACS+ login accounting” on page 1.6
- “Configure TACACS+ command accounting” on page 1.6
- “Troubleshooting TACACS+” on page 1.6

Additionally, TACACS+ has been updated to include support for the existing command aaa accounting update.

For full details regarding TACACS+ see:

- Appendix 1, TACACS+ Introduction and Configuration
- Appendix 2, TACACS+ Commands

For full details regarding AAA see:

- Appendix 3, AAA Introduction and Configuration
- Appendix 4, AAA Commands

Note: *TACACS+ authentication is not currently supported for GUI users.*

Privilege levels (CR32856 and CR33217)

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. See "enable password or enable secret" on page 15.
- The **enable** commands now take an optional **level** parameter that specifies which level you want to access. See "enable (Privileged Exec mode)" on page 17.
- A new command enables AAA authentication to determine the privilege level that you can access for passwords authenticated locally. See "aaa authentication enable default local" on page 18.
- Many **show** commands that were previously available at privilege level 7 are now available at privilege level 1 or 15 instead. This changes the mode from which you can access the commands. For more information, see Table 1, Table 2 and Table 3.
- As before, you can display your current privilege level. See "show privilege" on page 19.

Configuring passwords

The following commands specify **enable** passwords for levels 7 and 15. They also create three users with different configured privilege levels.

```
awplus#  configure terminal
awplus(config)#  enable password level 7 enable7
awplus(config)#  enable password level 15 enable15
awplus(config)#  username operator1 password pass1234
awplus(config)#  username operator7 privilege 7 password
                 pass5678
awplus(config)#  username admin privilege 15 password
                 passabcd
```

The following examples show how these three users would access the CLI.

Example 1 The user "operator1", with configured privilege of 1, must enter the correct enable password to access levels 7 and 15.

```
awplus login: operator1
Password:

AlliedWare Plus (TM) 5.4.1 08/29/11 16:16:02

awplus>show privilege
Current privilege level is 1
awplus>enable 7
Password:
awplus#show privilege
Current privilege level is 7
awplus#enable 15
Password:
awplus#show privilege
Current privilege level is 15
awplus#
```

Example 2 The user "operator7", with configured privilege of 7, can access level 7 without an enable password but must enter the correct password to access level 15. This example also shows that entering **enable** is the same as entering **enable 15**.

```
awplus login: operator7
Password:

AlliedWare Plus (TM) 5.4.1 08/29/11 16:16:02

awplus>enable 7
awplus#show privilege
Current privilege level is 7
awplus#enable
Password:
awplus#show privilege
Current privilege level is 15
awplus#
```

Example 3 The user "admin", with configured privilege of 15, can access any privilege level without having to enter an **enable** password. This example also shows that users can go directly from level 1 to level 15.

```
awplus login: admin
Password:

AlliedWare Plus (TM) 5.4.1 08/29/11 16:16:02

awplus>enable
awplus#show privilege
Current privilege level is 15
awplus#
```

enable password or enable secret

To set a local password to control access to various privilege levels, use the **enable password or enable secret** Global Configuration command. Use the **enable** form of the command to modify or create a password to be used, and use the **no** form of the command to remove the password.

Issuing a **no enable password** command removes a password configured with the **enable secret** command. The **enable password** command is shown in the running and startup configurations.

Note: *Do not use encrypted passwords for GUI users. The GUI requires unencrypted user passwords only - not encrypted user passwords. Do not use option 8 for GUI users.*

Syntax

```
enable password [<plain>|8 <hidden>|level <1-15> 8
   <hidden>]

no enable password [level <1-15>]

enable secret [<plain>|8 <hidden>|level <1-15> 8 <hidden>]

no enable secret [level <1-15>]
```

Parameter	Description
<plain>	Specifies the unencrypted password.
8	Specifies a hidden password will follow.
<hidden>	Specifies the hidden encrypted password. Use an encrypted password for better security where a password crosses the network or is stored on a TFTP server.
level	Privilege level <1-15>. Level for which the password applies. You can specify up to 16 privilege levels, using numbers 1 through 15. Level 1 is normal EXEC-mode user privileges for User Exec mode. If this argument is not specified in the command or the no variant of the command, the privilege level defaults to 15 (enable mode privileges) for Privileged Exec mode. A privilege level of 7 can be set for intermediate CLI security.

Default The privilege level for enable password is level 15 by default. Previously the default was level 1.

Mode Global Configuration

Usage This command enables the Network Administrator to set a password for entering the Privileged Exec mode when using the enable (Privileged Exec mode) command. There are three methods to enable a password: Plain, Encrypted, and Hidden. In the examples below, for each method, note that the configuration is different and the configuration file output is different, but the password string to be used to enter the Privileged Exec mode with the **enable** command is the same **mypasswd**.

From version 5.4.1, a user can have an intermediate CLI security level set with this command for privilege level 7 to access all the show commands in Privileged Exec mode and all the commands in User Exec mode, but not any configuration commands in Privileged Exec mode.

Note that the **enable password** command is an alias for the **enable secret** command and one password per privilege level is allowed using these commands. Do not assign one password to a privilege level with **enable password** and another password to a privilege level with **enable secret**.

Using plain passwords

The plain password is a clear text string that appears in the configuration file as configured.

```
        awplus#  configure terminal
awplus(config)#  enable password mypasswd
awplus(config)#  end
```

This results in the following show output:

```
awplus#show run
Current configuration:
hostname awplus
enable password mypasswd
!
interface lo
```

Using encrypted passwords

To configure an encrypted password using the **service password-encryption** command:

First, use the enable password command to specify the string that you want to use as a password (**mypasswd**).

Then, use the service password-encryption command to encrypt the specified string (**mypasswd**). The advantage of using an encrypted password is that the configuration file does not show **mypasswd**, it will only show the encrypted string fU7zHzuutY2SA.

Note: *Do not use encrypted passwords for GUI users. The GUI requires unencrypted user passwords only - not encrypted user passwords. Do not use option 8 for GUI users.*

```
        awplus#  configure terminal
awplus(config)#  enable password mypasswd
awplus(config)#  service password-encryption
awplus(config)#  end
```

This results in the following show output.

```
awplus#show run
Current configuration:
hostname awplus
enable password 8 fU7zHzuutY2SA
service password-encryption
!
interface lo
```

Using Hidden Passwords

To configure an encrypted password using the HIDDEN parameter (8) with the enable password or enable secret command. Use this method if you already know the encrypted string corresponding to the plain text string that you want to use as a password. It is not required to use the **service password-encryption** command for this method. The output in the configuration file will show only the encrypted string, and not the text string

```
awplus#  configure terminal
awplus(config)#  enable password 8 fU7zHzuutY2SA
awplus(config)#  end
```

This results in the following show output.

```
awplus#show run
Current configuration:
hostname awplus
enable password 8 fU7zHzuutY2SA
!
interface lo
```

Related Commands

enable (Privileged Exec mode)
enable secret
service password-encryption
privilege level
show privilege
username
show running-config

enable (Privileged Exec mode)

This command enters the Privileged Exec mode and optionally changes the privilege level for a session.

- If a privilege level is not specified then the maximum privilege level (15) is applied to the session.
- If the optional 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 command.
- If no password is specified then only users with the maximum privilege level set with the username command can assess Privileged Exec mode.

Syntax `enable [<privilege-level>]`

Parameter	Description
<privilege-level>	Specify the privilege level for a CLI session in the range <1-15>, where 15 is the maximum privilege level, 7 is the intermediate privilege level and 1 is the minimum privilege level. If the privilege level exceeds the user's privilege level, then the user will be prompted for a password. To configure a user's privilege level, use the **username** command. To configure an enable password for a privilege level, use the **level** parameter in the **enable password** command.

Mode User Exec

Usage Many of the Privileged Exec mode commands are used to configure operating parameters for the switch, so you should apply password protection to the Privileged Exec mode to prevent unauthorized use. Passwords can be encrypted but then cannot be recovered. Note that un-encrypted passwords are shown in plain text in configurations.

The username command sets the privilege level for the user. After login, you are given access to privilege level 1. You can access higher privilege levels with the enable command. If the privilege level specified is higher than your configured privilege level, then you are prompted for the password for that level.

Note that a separate password can be configured for each privilege level using the enable password or enable secret command from the Global Configuration mode. The service password-encryption command encrypts passwords configured by the enable password or the enable secret commands, so passwords are not shown in plain text in configurations.

Example The following example shows the use of the enable command to enter the Privileged Exec mode (note the change in the command prompt from > to #).

```
awplus> enable

awplus#
```

The following example shows the enable command which provides you with access the Privileged Exec mode with a privilege level of 7 or greater. With a a privilege level of 7 or greater you do not need to enter a password to access Privileged Exec mode. With a privilege level of 6 or less, you need to enter a password to access Privilege Exec mode. Use the enable password or the enable secret commands to set the password to enable access to Privileged Exec mode.

```
awplus> enable 7

awplus#
```

Related Commands disable (Privileged Exec mode)
enable password or enable secret
enable secret
exit
service password-encryption
username

aaa authentication enable default local

This command enables AAA authentication to determine what privilege level a user can access for passwords authenticated locally.

Syntax `aaa authentication enable default local`

Default Local privilege level authentication is enabled by default.

Mode Global Configuration

Usage The privilege level configured for a particular user in the local user database is the privilege threshold above which the user is prompted for an enable (Privileged Exec mode) command.

Example To enable local privilege level authentication command, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication enable default local
```

To disable privilege level authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication enable default
```

Related Commands
aaa authentication enable default group tacacs+
aaa authentication login
enable (Privileged Exec mode)
enable password
enable secret
tacacs-server host

show privilege

This command displays the current user privilege level, which can be any privilege level in the range <1-15>. Privilege levels <1-6> allow limited user access (all User Exec commands), privilege levels <7-14> allow restricted user access (all User Exec commands plus Privileged Exec show commands). Privilege level 15 gives full user access to all Privileged Exec commands.

Syntax `show privilege`

Mode User Exec and Privileged Exec

Usage From version 5.4.1, a user can have an intermediate CLI security level set with this command for privilege levels <7-14> to access all show commands in Privileged Exec mode and all commands in User Exec mode, but no configuration commands in Privileged Exec mode.

Example To show the current privilege level of the user, use the command:

```
awplus# show privilege
```

Output This results in the following show output.

```
awplus#show privilege
Current privilege level is 15
awplus#disable
awplus>show privilege
Current privilege level is 1
```

Related Commands privilege level

Show command privilege levels changes

This section contains three tables:

Some **show** commands had a privilege level of 1 and have retained that privilege level. These commands are not listed.

Table 1: **show** commands that were only available from Privileged Exec mode and are now available from both User Exec and Privileged Exec mode. These commands had a privilege level of 7 and now have a privilege level of 1

Command name	Syntax	Mode
AAA Commands		
show debugging aaa	show debugging aaa	User Exec and Privileged Exec
BGP Commands		
show bgp	show bgp <*other-parameters*>	User Exec and Privileged Exec
show ip bgp	show ip bgp [<*other-parameters*>]	User Exec and Privileged Exec
DHCP Commands		
show counter dhcp-client	show counter dhcp-client	User Exec and Privileged Exec
show counter dhcp-relay	show counter dhcp-relay	User Exec and Privileged Exec
show counter dhcp-server	show counter dhcp-server	User Exec and Privileged Exec
show ip dhcp binding	show ip dhcp binding [<*ip-address*>|<*address-pool*>]	User Exec and Privileged Exec
show ip dhcp pool	show ip dhcp pool [<*address-pool*>]	User Exec and Privileged Exec
show ip dhcp-relay	show ip dhcp-relay [interface <*interface-name*>]	User Exec and Privileged Exec
show ip dhcp server statistics	show ip dhcp server statistics	User Exec and Privileged Exec
show ip dhcp server summary	show ip dhcp server summary	User Exec and Privileged Exec
DHCP Snooping and ARP Security Commands		
show debugging arp security	show debugging arp security	User Exec and Privileged Exec
show debugging ip dhcp snooping	show debugging ip dhcp snooping	User Exec and Privileged Exec
show ip dhcp snooping	show ip dhcp snooping	User Exec and Privileged Exec
show ip dhcp snooping acl	show ip dhcp snooping acl show ip dhcp snooping acl [detail|hardware] [interface [<*interface-list*>]]	User Exec and Privileged Exec
show ip dhcp snooping agent-option	show ip dhcp snooping agent-option [interface <*interface-list*>]	User Exec and Privileged Exec
show ip dhcp snooping binding	show ip dhcp snooping binding	User Exec and Privileged Exec

Table 1: **show** commands that were only available from Privileged Exec mode and are now available from both User Exec and Privileged Exec mode. These commands had a privilege level of 7 and now have a privilege level of 1

Command name	Syntax	Mode
show ip dhcp snooping interface	show ip dhcp snooping interface [<*port-list*>]	User Exec and Privileged Exec
show ip dhcp snooping statistics	show ip dhcp snooping statistics [detail] [interface <*interface-list*>]	User Exec and Privileged Exec
show ip source binding	show ip source binding	User Exec and Privileged Exec
EPSR Commands		
show debugging epsr	show debugging epsr	User Exec and Privileged Exec
show epsr	show epsr	User Exec and Privileged Exec
show epsr word	show epsr <*epsr-name*>	User Exec and Privileged Exec
show epsr word counters	show epsr <*epsr-name*> counters	User Exec and Privileged Exec
show epsr counters	show epsr counters	User Exec and Privileged Exec
GVRP Commands		
show debugging gvrp	show debugging gvrp	User Exec and Privileged Exec
show gvrp configuration	show gvrp configuration	User Exec and Privileged Exec
show gvrp machine	show gvrp machine	User Exec and Privileged Exec
show gvrp statistics	show gvrp statistics [<*interface*>]	User Exec and Privileged Exec
show gvrp timer	show gvrp timer <*interface*>	User Exec and Privileged Exec
IGMP and IGMP Snooping Commands		
show debugging igmp	show debugging igmp	User Exec and Privileged Exec
show ip igmp groups	show ip igmp groups [<*ip-address*>|<*interface*> detail]	User Exec and Privileged Exec
show ip igmp interface	show ip igmp interface [<*interface*>]	User Exec and Privileged Exec
show ip igmp snooping mrouter	show ip igmp snooping mrouter [interface <*interface*>]	User Exec and Privileged Exec
show ip igmp snooping routermode	show ip igmp snooping routermode	User Exec and Privileged Exec
show ip igmp snooping statistics	show ip igmp snooping statistics interface <*interface-range*>	User Exec and Privileged Exec
IP Addressing and Protocol Commands		
show debugging ip dns forwarding	show debugging ip dns forwarding	User Exec and Privileged Exec
show debugging ip packet	show debugging ip packet	User Exec and Privileged Exec
show hosts	show hosts	User Exec and Privileged Exec
show ip dns forwarding	show ip dns forwarding	User Exec and Privileged Exec
show ip dns forwarding cache	show ip dns forwarding cache	User Exec and Privileged Exec
show ip domain-list	show ip domain-list	User Exec and Privileged Exec
show ip domain-name	show ip domain-name	User Exec and Privileged Exec
show ip forwarding	show ip forwarding	User Exec and Privileged Exec
show ip interface	show ip interface [<*interface-list*>] [brief]	User Exec and Privileged Exec
show ip irdp	show ip irdp	User Exec and Privileged Exec
show ip irdp interface	show ip irdp interface [<*interface-name*>]	User Exec and Privileged Exec
show ip name-server	show ip name-server	User Exec and Privileged Exec

Table 1: **show** commands that were only available from Privileged Exec mode and are now available from both User Exec and Privileged Exec mode. These commands had a privilege level of 7 and now have a privilege level of 1

Command name	Syntax	Mode
IP ACL Commands		
show access-group (x900 only)	show access-group [{<*3000-3699*>|<*4000-4699*>|<*access-list-name*>}]	User Exec and Privileged Exec
show access-list (IPv4 Software ACLs)	show access-list [<*1-99*>|<*100-199*>|<*1300-1999*>|<*3000-3699*>|<*4000-4499*>|<*access-list-name*>]	User Exec and Privileged Exec
show ip access-list	show ip access-list [<*1-99*>|<*100-199*>|<*1300-1999*>|<*2000-2699*>|<access-*list-name*>]	User Exec and Privileged Exec
show ip prefix-list	show ip prefix-list [<*name*>|detail|summary]	User Exec and Privileged Exec
IPv6 Commands		
show ipv6 forwarding	show ipv6 forwarding	User Exec and Privileged Exec
show ipv6 interface brief	show ipv6 interface [<*interface*>] brief	User Exec and Privileged Exec
show ipv6 neighbors	show ipv6 neighbors	User Exec and Privileged Exec
show ipv6 route	show ipv6 route [connected|database|ospf|rip|static|<*ipv6-address*>|<*ipv6-addr/prefix-length*>)]	User Exec and Privileged Exec
show ipv6 route summary	show ipv6 route summary	User Exec and Privileged Exec
IPv6 Software ACL Commands		
show ipv6 access-list (IPv6 Software ACLs)	show ipv6 access-list [<*access-list-name*>] show ipv6 access-list standard <*access-list-name*>	User Exec and Privileged Exec
Link Aggregation Commands		
show debugging lacp	show debugging lacp	User Exec and Privileged Exec
show diagnostic channel-group	show diagnostic channel-group	User Exec and Privileged Exec
show lacp-counter	show lacp-counter [<*1-65535*>]	User Exec and Privileged Exec
show lacp sys-id	show lacp sys-id	User Exec and Privileged Exec
show port etherchannel	show port etherchannel <*port*>	User Exec and Privileged Exec
LLDP Commands		
show debugging lldp	show debugging lldp [interface <*port-list*>]	User Exec and Privileged Exec
show lldp	show lldp	User Exec and Privileged Exec
show lldp interface	show lldp interface [<*port-list*>]	User Exec and Privileged Exec
show lldp local-info	show lldp local-info [base] [dot1] [dot3] [med] [interface <*port-list*>]	User Exec and Privileged Exec
show lldp neighbors	show lldp neighbors [interface <*port-list*>]	User Exec and Privileged Exec
show lldp neighbors detail	show lldp neighbors detail [base] [dot1] [dot3] [med] [interface <*port-list*>]	User Exec and Privileged Exec
show lldp statistics	show lldp statistics	User Exec and Privileged Exec
show lldp statistics interface	show lldp statistics interface [<*port-list*>]	User Exec and Privileged Exec
show location	show location {civic-location|coord-location|elin-location} show location {civic-location|coord-location|elin-location} identifier {<*civic-loc-id*>|<*coord-loc-id*>|<*elin-loc-id*>} show location {civic-location|coord-location|elin-location} interface <*port-list*>	User Exec and Privileged Exec
Local RADIUS Server Commands		

Table 1: **show** commands that were only available from Privileged Exec mode and are now available from both User Exec and Privileged Exec mode. These commands had a privilege level of 7 and now have a privilege level of 1

Command name	Syntax	Mode
show crypto pki certificates	show crypto pki certificates [local-ca|local]	User Exec and Privileged Exec
show crypto pki certificates local-radius-all-users	show crypto pki certificates local-radius-all-users	User Exec and Privileged Exec
show crypto pki certificates user	show crypto pki certificates user [<*user-name*>]	User Exec and Privileged Exec
show crypto pki trustpoints	show crypto pki trustpoints	User Exec and Privileged Exec
show radius local-server group	show radius local-server group [<*user-group-name*>]	User Exec and Privileged Exec
show radius local-server nas	show radius local-server nas [<*ip-address*>]	User Exec and Privileged Exec
show radius local-server statistics	show radius local-server statistics	User Exec and Privileged Exec
show radius local-server user	show radius local-server user [<*user-name*>] show radius local-server user <*user-name*> format csv	User Exec and Privileged Exec
Logging Commands		
show counter log	show counter log	User Exec and Privileged Exec
show exception log	show exception log	User Exec and Privileged Exec
show log	show log [tail [<*10-250*>]]	User Exec, Privileged Exec and Global Configuration
show log config	show log config	User Exec, Privileged Exec and Global Configuration
show log permanent	show log permanent [tail [<*10-250*>]]	User Exec, Privileged Exec and Global Configuration
MLD Snooping Introduction and Commands		
show ipv6 mld groups	show ipv6 mld groups [<*ipv6-address*> |<*interface*> detail]	User Exec and Privileged Exec
show ipv6 mld interface	show ipv6 mld interface [<*interface*>]	User Exec and Privileged Exec
show ipv6 mld snooping mrouter	show ipv6 mld snooping mrouter <*interface*>	User Exec and Privileged Exec
show ipv6 mld snooping statistics	show ipv6 mld snooping statistics interface <*interface*>	User Exec and Privileged Exec
Multicast Introduction and Commands		
show ip mroute	show ip mroute [<*group-addr*>] [<*source-addr*>] [{dense|sparse}] [{count|summary}]	User Exec and Privileged Exec
show ip mvif	show ip mvif [<*interface*>]	User Exec and Privileged Exec
show ip rpf	show ip rpf <*source-addr*>	User Exec and Privileged Exec
NTP Commands		
show counter ntp	show counter ntp	User Exec and Privileged Exec
show ntp associations	show ntp associations [detail]	User Exec and Privileged Exec
show ntp status	show ntp status	User Exec and Privileged Exec
OSPF Commands		
show debugging ospf	show debugging ospf	User Exec and Privileged Exec
show ip ospf	show ip ospf [<*process-id*>]	User Exec and Privileged Exec
show ip ospf border-routers	show ip ospf [<*process-id*>] border-routers	User Exec and Privileged Exec

Table 1: **show** commands that were only available from Privileged Exec mode and are now available from both User Exec and Privileged Exec mode. These commands had a privilege level of 7 and now have a privilege level of 1

Command name	Syntax	Mode
show ip ospf database	show ip ospf [<*process-id*>] database [self-originate|max-age]	User Exec and Privileged Exec
show ip ospf database asbr-summary	show ip ospf database asbr-summary [<*ip-addr*>] [self-originate|<*advrouter*>]	User Exec and Privileged Exec
show ip ospf database external	show ip ospf database external [<*ip-addr*>] [self-originate|<*advrouter*>]	User Exec and Privileged Exec
show ip ospf database network	show ip ospf database network [<*ip-addr*>] [self-originate|<*advrouter*>]	User Exec and Privileged Exec
show ip ospf database nssa-external	show ip ospf database nssa-external [<*ip-address*>] [self-originate|<*advrouter*>]	User Exec and Privileged Exec
show ip ospf database opaque-area	show ip ospf database opaque-area [<*ip-address*>] [self-originate|<*advrouter*>]	User Exec and Privileged Exec
show ip ospf database opaque-as	show ip ospf database opaque-as [<*ip-address*>] [self-originate|<*advrouter*>]	User Exec and Privileged Exec
show ip ospf database opaque-link	show ip ospf database opaque-link [<*ip-address*>] [self-originate|<*advrouter*>]	User Exec and Privileged Exec
show ip ospf database router	show ip ospf database router [<*ip-address*>] [self-originate|<*advrouter*>]	User Exec and Privileged Exec
show ip ospf database summary	show ip ospf database summary [<*ip-address*>] [self-originate|<*advrouter*>]	User Exec and Privileged Exec
show ip ospf interface	show ip ospf interface [<*interface-name*>]	User Exec and Privileged Exec
show ip ospf neighbor	show ip ospf [<*ospf-id*>] neighbor <*neighbor-ip-addr*> [detail] show ip ospf [<*ospf-id*>] neighbor detail [all] show ip ospf [<*ospf-id*>] neighbor [all] show ip ospf [<*ospf-id*>] neighbor interface <*ip-addr*>	User Exec and Privileged Exec
show ip ospf route	show ip ospf [<*ospf-id*>] route	User Exec and Privileged Exec
show ip ospf virtual-links	show ip ospf virtual-links	User Exec and Privileged Exec
show ip protocols ospf	show ip protocols ospf	User Exec and Privileged Exec
show ip ospf database asbr-summary	show ip ospf database asbr-summary [<*ip-addr*>] [self-originate|<*advrouter*>]	User Exec and Privileged Exec
show ip ospf database external	show ip ospf database external [<*ip-addr*>] [self-originate|<*advrouter*>]	User Exec and Privileged Exec
show ip ospf database network	show ip ospf database network [<*ip-addr*>] [self-originate|<*advrouter*>]	User Exec and Privileged Exec
show ip ospf database nssa-external	show ip ospf database nssa-external [<*ip-address*>] [self-originate|<*advrouter*>]	User Exec and Privileged Exec
show ip ospf database opaque-area	show ip ospf database opaque-area [<*ip-address*>] [self-originate|<*advrouter*>]	User Exec and Privileged Exec
show ip ospf database opaque-as	show ip ospf database opaque-as [<*ip-address*>] [self-originate|<*advrouter*>]	User Exec and Privileged Exec
show ip ospf database opaque-link	show ip ospf database opaque-link [<*ip-address*>] [self-originate|<*advrouter*>]	User Exec and Privileged Exec
show ip ospf database router	show ip ospf database router [<*ip-address*>] [self-originate|<*advrouter*>]	User Exec and Privileged Exec

Table 1: **show** commands that were only available from Privileged Exec mode and are now available from both User Exec and Privileged Exec mode. These commands had a privilege level of 7 and now have a privilege level of 1

Command name	Syntax	Mode
show ip ospf database summary	show ip ospf database summary [<*ip-address*>] [self-originate|<*advrouter*>]	User Exec and Privileged Exec
show ip ospf interface	show ip ospf interface [<*interface-name*>]	User Exec and Privileged Exec
show ip ospf neighbor	show ip ospf [<*ospf-id*>] neighbor <*neighbor-ip-addr*> [detail]	User Exec and Privileged Exec
	show ip ospf [<*ospf-id*>] neighbor detail [all]	
	show ip ospf [<*ospf-id*>] neighbor [all]	
	show ip ospf [<*ospf-id*>] neighbor interface <*ip-addr*>	
show ip ospf route	show ip ospf [<*ospf-id*>] route	User Exec and Privileged Exec
show ip ospf virtual-links	show ip ospf virtual-links	User Exec and Privileged Exec
show ip protocols ospf	show ip protocols ospf	User Exec and Privileged Exec
OSPFv3 for IPv6 Commands		
show debugging ipv6 ospf	show debugging ipv6 ospf	User Exec and Privileged Exec
show ipv6 ospf	show ipv6 ospf [<*process-id*>]	User Exec and Privileged Exec
show ipv6 ospf database	show ipv6 ospf [<*process-id*>] database	User Exec and Privileged Exec
show ipv6 ospf database external	show ipv6 ospf database external [adv-router <*adv-router-id*>]	User Exec and Privileged Exec
show ipv6 ospf database network	show ipv6 ospf database network [adv-router <*adv-router-id*>]	User Exec and Privileged Exec
show ipv6 ospf database router	show ipv6 ospf database router [adv-router <*adv-router*>]	User Exec and Privileged Exec
show ipv6 ospf interface	show ipv6 ospf interface [<*interface-name*>]	User Exec and Privileged Exec
show ipv6 ospf neighbor	show ipv6 ospf [<*process-id*>] neighbor <*neighbor-id*>	User Exec and Privileged Exec
	show ipv6 ospf [<*process-id*>] neighbor detail	
	show ipv6 ospf [<*process-id*>] neighbor <*interface*> [detail]	
show ipv6 ospf route	show ipv6 ospf [<*process-id*>] route	User Exec and Privileged Exec
PIM-DM Commands		
show debugging pim dense-mode	show debugging pim dense-mode	User Exec and Privileged Exec
show ip pim dense-mode interface	show ip pim dense-mode interface	User Exec and Privileged Exec
show ip pim dense-mode interface detail	show ip pim dense-mode interface detail	User Exec and Privileged Exec
show ip pim dense-mode mroute	show ip pim dense-mode mroute	User Exec and Privileged Exec
show ip pim dense-mode neighbor	show ip pim dense-mode neighbor	User Exec and Privileged Exec
show ip pim dense-mode neighbor detail	show ip pim dense-mode neighbor detail	User Exec and Privileged Exec
show ip pim dense-mode nexthop	show ip pim dense-mode nexthop	User Exec and Privileged Exec
PIM-SM Commands		

Table 1: **show** commands that were only available from Privileged Exec mode and are now available from both User Exec and Privileged Exec mode. These commands had a privilege level of 7 and now have a privilege level of 1

Command name	Syntax	Mode
show debugging pim sparse-mode	show debugging pim sparse-mode	User Exec and Privileged Exec
show ip pim sparse-mode bsr-router	show ip pim sparse-mode bsr-router	User Exec and Privileged Exec
show ip pim sparse-mode interface	show ip pim sparse-mode interface	User Exec and Privileged Exec
show ip pim sparse-mode interface detail	show ip pim sparse-mode interface detail	User Exec and Privileged Exec
show ip pim sparse-mode mroute	show ip pim sparse-mode mroute [<*group-address*>] [<*source-address*>] show ip pim sparse-mode mroute [<*source-address*> <*group-address*>]	User Exec and Privileged Exec
show ip pim sparse-mode mroute detail	show ip pim sparse-mode mroute [<*group-address*>|<*source-address*>] detail show ip pim sparse-mode mroute [<*group-address*> <*source-address*>] detail show ip pim sparse-mode mroute [<*source-address*> <*group-address*>] detail	User Exec and Privileged Exec
show ip pim sparse-mode neighbor	show ip pim sparse-mode neighbor [<*interface*>] [<*ip-address*>] [detail]	User Exec and Privileged Exec
show ip pim sparse-mode nexthop	show ip pim sparse-mode nexthop	User Exec and Privileged Exec
show ip pim sparse-mode rp-hash	show ip pim sparse-mode rp-hash <*group-addr*>	User Exec and Privileged Exec
show ip pim sparse-mode rp mapping	show ip pim sparse-mode rp mapping	User Exec and Privileged Exec
Ping Polling Commands		
show counter ping-poll	show counter ping-poll [<*1-100*>]	User Exec and Privileged Exec
show ping-poll	show ping-poll [<*1-100*>|state {up|down}] [brief]	User Exec and Privileged Exec
Power over Ethernet Commands		
show debugging power-inline	show debugging power-inline	User Exec and Privileged Exec
show power-inline	show power-inline	User Exec and Privileged Exec
show power-inline counters	show power-inline counters [<*port-list*>]	User Exec and Privileged Exec
show power-inline interface	show power-inline interface [<*port-list*>]	User Exec and Privileged Exec
show power-inline interface detail	show power-inline interface [<*port-list*>] detail	User Exec and Privileged Exec
QoS Commands		
show class-map	show class-map <*class-map name*>	User Exec and Privileged Exec
show mls qos aggregate-policer (SBx908 and x900 series)	show mls qos aggregate-policer [<*name*>]	User Exec and Privileged Exec
show mls qos fabric-queue (SBx908 and x900 series)	show mls qos fabric-queue	User Exec and Privileged Exec
show mls qos interface	show mls qos interface [<*port*>]	User Exec and Privileged Exec

Table 1: **show** commands that were only available from Privileged Exec mode and are now available from both User Exec and Privileged Exec mode. These commands had a privilege level of 7 and now have a privilege level of 1

Command name	Syntax	Mode
show mls qos interface policer-counters	show mls qos interface <*port*> policer-counters [class-map <*class-map*>]	User Exec and Privileged Exec
show mls qos interface queue-counters	show mls qos interface <*port*> queue-counters queue [<*0-7*>]	User Exec and Privileged Exec
show mls qos interface storm-status	show mls qos interface <*port*> storm-status	User Exec and Privileged Exec
show mls qos maps cos-queue	show mls qos maps cos-queue	User Exec and Privileged Exec
show mls qos maps fabric-queue (SBx908 and x900 series)	show mls qos maps fabric-queue	User Exec and Privileged Exec
show mls qos maps policed-dscp (SBx908 and x900 series)	show mls qos maps policed-dscp [<*0-63*>]	User Exec and Privileged Exec
show mls qos maps premark-dscp	show mls qos maps premark-dscp [<*0-63*>]	User Exec and Privileged Exec
show mls qos queue-set (SBx908 and x900 series)	show mls qos queue-set [<*1-4*>]	User Exec and Privileged Exec
show policy-map	show policy-map [<*name*>]	User Exec and Privileged Exec
RADIUS Commands		
show debugging radius	show debugging radius	User Exec and Privileged Exec
show radius	show radius	User Exec and Privileged Exec
show radius statistics	show radius statistics	User Exec and Privileged Exec
RIP Commands		
show debugging rip	show debugging rip	User Exec and Privileged Exec
show ip protocols rip	show ip protocols rip	User Exec and Privileged Exec
show ip rip	show ip rip	User Exec and Privileged Exec
show ip rip database	show ip rip database [full]	User Exec and Privileged Exec
show ip rip interface	show ip rip interface [<*interface*>]	User Exec and Privileged Exec
show ip rip vrf database (x610, SBx908, x900)	show ip rip {vrf <*vrf-name*>|global} database [full]	User Exec and Privileged Exec
show ip rip vrf interface (x610, SBx908, x900)	show ip rip {vrf <*vrf-name*>|global} interface [<*interface-name*>]	User Exec and Privileged Exec
RIPng Commands		
show debugging ipv6 rip	show debugging ipv6 rip	User Exec and Privileged Exec
show ipv6 protocols rip	show ipv6 protocols rip	User Exec and Privileged Exec
show ipv6 rip	show ipv6 rip	User Exec and Privileged Exec
show ipv6 rip database	show ipv6 rip database	User Exec and Privileged Exec
show ipv6 rip interface	show ipv6 rip interface [<*interface*>]	User Exec and Privileged Exec
RMON Commands		
show rmon alarm	show rmon alarm	User Exec and Privileged Exec
show rmon event	show rmon event	User Exec and Privileged Exec
show rmon history	show rmon history	User Exec and Privileged Exec

Table 1: **show** commands that were only available from Privileged Exec mode and are now available from both User Exec and Privileged Exec mode. These commands had a privilege level of 7 and now have a privilege level of 1

Command name	Syntax	Mode
show rmon statistics	show rmon statistics	User Exec and Privileged Exec
Routing Commands		
show ip route	show ip route [bgp|connected|ospf|rip|static|<*ip-addr*>|<*ip-addr/prefix-length*>] show ip route {vrf <*vrf-name*>|global} [bgp|connected|ospf|rip|static]	User Exec and Privileged Exec
show ip route database	show ip route database [bgp|connected|ospf|rip|static] show ip route [vrf <*vrf-name*>|global] database [bgp|connected|ospf|rip|static]	User Exec and Privileged Exec
show ip route summary	show ip route summary [vrf <*vrf-name*>|global]	User Exec and Privileged Exec
sFlow Commands		
show debugging sflow	show debugging sflow [interface <*port-list*>]	User Exec and Privileged Exec
SNMP Commands		
show counter snmp-server	show counter snmp-server	User Exec and Privileged Exec
show debugging snmp	show debugging snmp	User Exec and Privileged Exec
Secure Shell (SSH) Commands		
show crypto key hostkey	show crypto key hostkey [dsa|rsa|rsa1]	User Exec, Privileged Exec and Global Configuration
show crypto key pubkey-chain knownhosts	show crypto key pubkey-chain knownhosts [vrf <*vrf-name*>|global] [<*1-65535*>]	User Exec, Privileged Exec and Global Configuration
show crypto key pubkey-chain userkey	show crypto key pubkey-chain userkey <*username*> [<*1-65535*>]	User Exec, Privileged Exec and Global Configuration
show crypto key userkey	show crypto key userkey <*username*> [dsa|rsa|rsa1]	User Exec, Privileged Exec and Global Configuration
show ssh	show ssh	User Exec, Privileged Exec and Global Configuration
show ssh client	show ssh client	User Exec, Privileged Exec and Global Configuration
show ssh server	show ssh server	User Exec, Privileged Exec and Global Configuration
show ssh server allow-users	show ssh server allow-users	User Exec, Privileged Exec and Global Configuration
show ssh server deny-users	show ssh server deny-users	User Exec, Privileged Exec and Global Configuration
Stacking Commands		
show counter stack	show counter stack	User Exec and Privileged Exec
show debugging stack	show debugging stack	User Exec and Privileged Exec
show provisioning (stack-member)	show provisioning	User Exec and Privileged Exec
Spanning Tree Commands		
show debugging mstp	show debugging mstp	User Exec and Privileged Exec
show spanning-tree	show spanning-tree [interface <*port-list*>]	User Exec, Privileged Exec and Interface Configuration

Table 1: **show** commands that were only available from Privileged Exec mode and are now available from both User Exec and Privileged Exec mode. These commands had a privilege level of 7 and now have a privilege level of 1

Command name	Syntax	Mode
show spanning-tree brief	show spanning-tree brief	User Exec, Privileged Exec and Interface Configuration
show spanning-tree mst	show spanning-tree mst	User Exec, Privileged Exec and Interface Configuration
show spanning-tree mst config	show spanning-tree mst config	User Exec, Privileged Exec and Interface Configuration
show spanning-tree mst detail	show spanning-tree mst detail	User Exec, Privileged Exec and Interface Configuration
show spanning-tree mst detail interface	show spanning-tree mst detail interface <*port*>	User Exec, Privileged Exec and Interface Configuration
show spanning-tree mst instance	show spanning-tree mst instance <*instance*>	User Exec, Privileged Exec and Interface Configuration
show spanning-tree mst instance interface	show spanning-tree mst instance <*instance*> interface <*port*>	User Exec, Privileged Exec and Interface Configuration
show spanning-tree mst interface	show spanning-tree mst interface <*port*>	User Exec, Privileged Exec and Interface Configuration
Switching Commands		
show debugging loopprot	show debugging loopprot	User Exec and Privileged Exec
show debugging platform packet	show debugging platform packet	User Exec and Privileged Exec
show flowcontrol interface	show flowcontrol interface <*port*>	User Exec and Privileged Exec
show loop-protection	show loop-protection [interface <*port-list*>] [counters]	User Exec and Privileged Exec
show mirror	show mirror	User Exec and Privileged Exec
show mirror interface	show mirror interface <*port*>	User Exec, Privileged Exec and Interface Configuration
show provisioning (xem-bay) (x900 and SBx908)	show provisioning	User Exec and Privileged Exec
show storm-control	show storm-control [<*port*>]	User Exec and Privileged Exec
System Configuration and Monitoring Commands		
show debugging	show debugging	User Exec and Privileged Exec
show diagnostic monitor pcsping (x900 and SBx908)	show diagnostic monitor pcsping	User Exec and Privileged Exec
show continuous-reboot-prevention	show continuous-reboot-prevention	User Exec and Privileged Exec
show process	show process [sort {cpu|mem}]	User Exec and Privileged Exec
show reboot history	show reboot history	User Exec and Privileged Exec
show router-id	show router-id	User Exec and Privileged Exec
TACACS+ Commands		
show tacacs+	show tacacs+	User Exec and Privileged Exec
User Access Commands		
show telnet	show telnet	User Exec and Privileged Exec
VLAN Commands		
show vlan	show vlan {all|brief|dynamic|static|<*1-4094*>}	User Exec and Privileged Exec

Table 1: **show** commands that were only available from Privileged Exec mode and are now available from both User Exec and Privileged Exec mode. These commands had a privilege level of 7 and now have a privilege level of 1

Command name	Syntax	Mode
show vlan classifier group	show vlan classifier group [<*1-16*>]	User Exec and Privileged Exec
show vlan classifier interface group	show vlan classifier interface group [<*1-16*>]	User Exec and Privileged Exec
show vlan classifier rule	show vlan classifier rule [<*1-256*>]	User Exec and Privileged Exec
show vlan private-vlan	show vlan private-vlan	User Exec and Privileged Exec
show vlan statistics (x600 and x610)	show vlan statistics [name <*instance_name*>]	User Exec and Privileged Exec
VRF-Lite Commands		
show ip vrf	show ip vrf <*vrf-name*>	User Exec and Privileged Exec
show ip vrf detail	show ip vrf detail <*vrf-name*>	User Exec and Privileged Exec
show ip vrf interface	show ip vrf interface <*vrf-name*>	User Exec and Privileged Exec
VRRP Commands		
show debugging vrrp	show debugging vrrp	User Exec and Privileged Exec
show vrrp	show vrrp [brief]	User Exec and Privileged Exec
show vrrp counters	show vrrp counters	User Exec and Privileged Exec
show vrrp (session)	show vrrp <*vrid*> <*interface*>	User Exec and Privileged Exec

Table 2: **show** commands that are still only available from Privileged Exec mode. These commands had a privilege level of 7 and now have a privilege level of 15.

Command name	Syntax
Running-Config Commands	
show running-config	show running-config [<*other-parameters*>]
Switching Commands	
show port-security interface	show port-security interface <*port*>
show port-security intrusion	show port-security intrusion [interface <*port*>]
System Configuration and Monitoring Commands	
show boot	show boot
show file	show {<*filename*>|<*url*>}
show startup-config	show startup-config
show tech-support	show tech-support [all] [outfile <*filename*>]
	show tech-support {[bgp] [dhcpsn] [epsr] [igmp] [ip] [ipv6] [ospf] [pim] [rip] [rinpng] [mld] [stack] [stp] [system]} [outfile <*filename*>]
User Access Commands	
show security-password configuration	show security-password configuration
show security-password user	show security-password user

Table 3: **show** commands that are still only available from Privileged Exec mode. These commands still have a privilege level of 7.

Command name	Syntax
show auth-mac	show auth-mac [<*other-parameters*>]
show auth-web	show auth-web [<*other-parameters*>]
show auth-web-server	show auth-web-server
show dhcp lease	show dhcp lease [<*interface*>]
show dot1x	show dot1x [<*other-parameters*>]
show ecofriendly	show ecofriendly
show mail	show mail
show platform	show platform [<*other-parameters*>]
show sflow	show sflow [<*other-parameters*>]
show snmp-server	show snmp-server [<*other-parameters*>]
show test	show test [count]
show trigger	show trigger [<*1-250*>|counter|full]

Increased MAC Auth Capabilities

On the x600 and x610 platforms, it is possible to dynamically allocate multiple different untagged VLANs to different supplicants attached to the same port.

This is achieved by using the MAC-based VLAN capability within the switching capability. This capability makes use of a table which holds a mapping from a MAC address to a VLAN.

This table can hold over 1000 entries. But, for performance reasons, it uses a hashing algorithm to achieve rapid lookup of table entries. Performance is very important in this capability - for every packet that arrives on a port that is using MAC-based VLANs, a lookup must be performed to determine the VLAN to associate with the packet's source MAC address.

By their very nature, hash-based table storage algorithms can lead to sub-optimal utilisation of the available table space. If too many entries resolve to the same hash value, then the table space allocated to entries with that hash value can become over-subscribed, and entries will be unable to be stored, even though the rest of the table is not completely full.

The number of actual entries that this table will hold is dependant on what MAC addresses are in use on a network, and the hash algorithm used to assign locations to the table entries.

A different hashing algorithm, used with the same MAC addresses, can sometimes allow a different number of entries to be added to the table.

There is now a new command platform mac-vlan-hashing-algorithm which will allow the network administrator to try 4 different algorithms and select the most appropriate one. This enables the network administrator to tune the table's storage algorithm to best fit with the set of MAC addresses that happen to be in use on their network.

platform mac-vlan-hashing-algorithm

This command enables you to change the MAC VLAN hash-key-generating algorithm.

The **no** variant of this command returns the hash-key algorithm to crc32l.

Syntax

```
platform mac-vlan-hashing-algorithm
   {crc16l|crc16u|crc32l|crc32u}

no platform mac-vlan-hashing-algorithm
```

Parameter	Description
`platform`	The global settings for the platform processor.
`mac-vlan-hashing-algorithm`	L2 MAC VLAN hash control.
`crc16l`	The algorithm that will apply to the lower bits of crc16
`crc16u`	The algorithm that will apply to the upper bits of crc16
crc32l	The algorithm that will apply to the lower bits of crc32
crc32u	The algorithm that will apply to the upper bits of crc32

Default crc32l

Mode Config

Usage Occasionally, when using the Multiple Dynamic VLAN feature, a supplicant cannot be authenticated because a collision occurs within the VLAN MAC table. This can happen when more than four different MAC addresses produce the same hash-key.

When this situation occurs, you can sometimes work around it by changing the hashing algorithm from its default of crc32l. You may need to try several different algorithms to rectify the problem.

You must restart the switch for this command to take effect.

Note that this command is intended for technical support staff, or advanced end users.

Example To change the hash-key generating algorithm to one that applies to the lower bits of the crc16, use the command:

```
awplus#          configure terminal
awplus(config)#  platform mac-vlan-hashing-algorithm crc16l
```

Increased maximum LAGs on x908 with XEM-2XP, XEM-2XT, XEM-2XS

This enhancement is supported on:

- SwitchBlade x908

For the SwitchBlade x908 with only XEM-2XP and / or XEM-2XT, and / or XEM-2XS XEMs installed (and no XEM-1XP, XEM-12T, or XEM-12S XEMs present), a new platform enhanced mode option **extended** increases the maximum number of link aggregators that can be configured to 128 (96 static channel groups and 32 dynamic (LACP) channel groups).

The following commands are modified:

- platform enhanced-mode command on page 34
- show platform command on page 36
- channel-group command on page 37
- static-channel-group command on page 37

platform enhanced-mode

On a SwitchBlade x908 with XEM-2XP and / or XEM-2XT, and / or XEM-2XS XEMs installed (and no XEM-1XP, XEM-12T, or XEM-12S XEMs present), a new enhanced mode option **extended** increases the maximum number of static and dynamic link aggregators.

Use this command to rearrange memory in the switch's silicon hardware, to provide differing numbers of table entries for different uses. For a new enhanced mode setting to take effect, it must be in the startup configuration when the switch starts up. For more details about the limits that are modified by this command, see Table 5 on page 35.

The no variant of this command restores the memory to the default state: no enhanced mode set. For the default mode setting to take effect, you must restart the switch with the **no** version of the command in the startup config.

Syntax SBx908

```
platform enhanced-mode
   {nexthop|qoscounters|qospolicers|extended}

no platform enhanced-mode
```

Table 4: New parameter in the **platform enhanced-mode** command

Parameter	Description
extended	SBx908 with only XEM-2XP and/orXEM-2XT, and/or XEM-2XS XEMs installed: This mode increases the maximum number of: ■ static channel groups ■ LACP channel groups

Default By default, no enhanced mode is set.

Mode Global Configuration

Usage Memory in the switch hardware silicon can be allocated in various ways when the switch starts up. The memory allocations that can be made depend on the hardware (which switch model and which XEMs are installed). On some hardware platforms, using this command to increase the allocation for one use reduces the memory available for other uses.

Before you configure QoS storm protection (**storm-protection** command.), you must set the silicon profile to either **extended** or **qoscounters**.

The enhanced mode setting in the startup configuration takes effect when the switch starts up. Once you have entered this **platform enhanced-mode** command (or the **no** version), you can copy the running-config to the startup-config (**copy running-config** command) and reboot the switch (**reboot** command):

```
awplus# copy running-config startup-config

awplus# reboot
```

SBx908 only: The switch will only start up with the platform enhanced mode set to **extended** if all the XEMs installed are XEM-2XP and / or XEM-2XT, and / or XEM-2XS XEMs. When the switch is running in the extended mode, you cannot install any of the other XEMs (XEM-1XP, XEM-12T, or XEM-12S). If you insert one of these XEMs, the XEM will not start up. To install one of these XEMs, you must remove the extended mode setting from the startup config, and restart the switch. This results in the maximum numbers of link aggregators being reduced to the default settings.

Before connecting switches into a stack, all stack members must be operating in the same mode (enhanced or default / none).

Table 5: Memory allocation for silicon profiles with routing ratio IPv4 and IPv6

	Silicon profile options				
	None (default)	**nexthop**	**qoscounters**	**qospolicers**	**extended**
Route Entry/Policer Limits					
Unicast nexthop entries	2500	5060	2500	2500	2500
Multicast nexthop entries	2048	256	2048	1280	2048
QoS policers (traffic classes)	713	329	475	1097	475
FDB Limits					
Forwarding Database entries (MAC addresses)	16384	16384	16384	16384	16384
Link Aggregation Limits					
Link aggregators: total	31	31	31	31	128
Link aggregators: LACP (dynamic)	31	31	31	31	32
Link aggregators: static	31	31	31	31	96
QoS Counters Enabled					
QoS counters	No	No	Yes	No	Yes

Examples On a SwitchBlade x908 with XEM-2XP and / or XEM-2XT, and / or XEM-2XS XEMs installed (and no XEM-1XP, XEM-12T, or XEM-12S XEMs present), to increase table sizes, use the commands:

```
awplus# configure terminal

awplus(config)# platform enhanced-mode extended
```

Related Commands: copy running-config
channel-group
reboot
show platform
static-channel-group
storm protection

show platform

This command displays the platform enhanced-mode setting, including the new **extended** option, in addition to other platform settings.

Syntax `show platform`

Mode Privileged Exec

Usage This command displays the settings in the running config. For changes in some of these settings to take effect, the switch must be rebooted with the new settings in the startup config.

Output Figure 1: Example output from the **show platform** command on a SwitchBlade x908

```
awplus# show platform

Load Balancing                  src-dst-mac, scr-dst-ip
Control-plane-prioritization    Max 60 Mbps
L2MC overlapped group check     off
enhanced-mode                   extended
Jumboframe support              off
Vlan-stacking TPID              0x8100
Routing ratio                   IPv4 and IPv6
```

Table 6: Modified parameter in the output of the **show platform** command

Parameter	Description
enhanced-mode	The enhanced-mode setting (**platform enhanced-mode** command) for the switch hardware; one of: ■ nexthop ■ qoscounters ■ qospolicers ■ **extended (SBx908 only)** ■ None (default)

channel-group

SBx908 only: If the platform enhanced mode is set to the new option **extended platform enhanced-mode** command, the maximum number of dynamic (LACP) channel groups is increased to 96.

Syntax `channel-group <dynamic-channel-group-number> mode {active|passive}`

Table 7: Modified parameter in the **channel-group** command

Parameter	Description
<dynamic-channel-group-number>	<1-32> Specify a dynamic channel group number for an LACP link. If the switch enhanced-mode is not set to **extended**, you can create up to 31 channel groups (dynamic and/or static channel groups). SBx908 only: If the switch's silicon profile is set to **extended**, you can create up to 32 dynamic (LACP) channel groups (as well as up to 96 static channel groups). Each channel group can include up to 8 ports. The enhanced modes are hardware dependent—see the platform enhanced-mode command.

Mode Interface Configuration

static-channel-group

SBx908 only: If the platform enhanced mode is set to the new option **extended platform enhanced-mode** command, the maximum number of static channel groups is increased to 96.

Syntax `static-channel-group <static-channel-group-number>`

Table 8: Modified parameter in the **static-channel-group** command

Parameter	Description
<static-channel-group-number>	<1-96> Static channel group number. If the platform enhanced-mode is not set to **extended**, you can create up to 31 channel groups (dynamic and/or static channel groups). SBx908 only: If the switch's silicon profile is set to **extended**, you can create up to 96 static channel groups (as well as up to 32 dynamic (LACP) channel groups). Each channel group can include up to 8 ports. The platform enhanced-modes are hardware dependent—see the platform enhanced-mode command.

Mode Interface Configuration

IPv6 RA Guard

This enhancement is supported on all AlliedWare Plus Layer 3 switches. The following command has been added:

- ipv6 nd raguard command on page 39

Overview

Router Advertisements (RA) and Router Redirects are key to the Network Discovery Protocol (NDP) used to manage IPv6 networks. RA messages advertise a router's presence and specify network parameters that are used by hosts as part of address auto-configuration and next hop routers for particular destinations.

RAs are periodically transmitted by routers. This allows networks to be reconfigured easily by changes to the router only. Routers can also send redirects to hosts suggesting they use a different next-hop for a particular traffic stream. But because the entire network configuration can be modified by what is contained in RAs and redirects, the network is vulnerable to rogue messages that are generated either through misconfiguration or due to a malicious attack.

RA Guard defends against these vulnerabilities. RA Guard on the switch simply considers each of its ports as either trusted or untrusted. Any host connected to a port is considered trusted or untrusted depending on the port status. A trusted port will accept RAs and redirects and will forward RAs and redirects on trusted ports. An untrusted port will block and discard all RAs and redirects received from the untrusted host. RA Guard is specified in RFC6105 - IPv6 Router Advertisement Guard.

Important concepts

Rogue RAs A rogue RA is an RA that contains invalid information that could cause unwanted changes in the network configuration. These could be generated unintentionally through misconfiguration or maliciously by someone wanting to disrupt or gain access to the network.

Router Redirects Router redirects are sent from routers to hosts to inform the host that it should use a different next-hop for a particular destination. These can also cause instability in the network by influencing hosts' internal routing decisions, though misconfiguration or with malicious intent.

RA Guard Classifiers The actual security enforcement of RA Guard is handled through hardware classifiers, which are dynamically added when a port is marked as trusted or untrusted. RA Guard blocks unintentionally generated RAs and router redirects with filters for ICMPv6 type 134 and 137.

RA Guard Support

RA Guard operates on all AlliedWare Plus Layer 3 switches, including stacked environments. It is supported on:

- standalone ports
- individual ports in a dynamic (LACP) aggregator, but is not supported on a dynamic aggregator
- a static aggregator, but is not supported on individual ports in a static aggregator

Commands

ipv6 nd raguard

Use this command to apply the Router Advertisements (RA) Guard feature from the Interface Configuration mode for a switch port. This blocks all RA messages received on a switch port.

Use the no parameter with this command to disable RA Guard for a specified switch port.

Syntax `ipv6 nd raguard`

`no ipv6 nd raguard`

Default RA Guard is disabled by default.

Mode Interface Configuration for a switch port interface.

Usage Router Advertisements (RAs) are used by routers to announce themselves on the link. Applying RA Guard to a switch port disallows Router Advertisements and redirect messages. RA Guard blocks RAs from untrusted hosts. Blocking RAs stops untrusted hosts from flooding malicious RAs and stops any misconfigured hosts from disrupting traffic on the local network.

Enabling RA Guard on a port blocks RAs from a connected host and indicates the port and host are untrusted. Disabling RA Guard on a port allows RAs from a connected host and indicates the port and host are trusted. Ports and hosts are trusted by default i.e. the default is to allow the reception of RAs on a port.

Example To enable RA Guard on switch ports port1.0.2-1.0.12, use the following commands:

```
awplus#configure terminal

awplus(config)#interface port1.0.2-1.0.12

awplus(config-if)#ipv6 nd raguard
```

To verify RA Guard is enabled on switch port interface port1.0.2, use the command:

```
awplus#show running-config interface port1.0.2
```

Output Example output from a **show running-config interface port1.0.2** to verify RA Guard:

```
!
interface port1.0.2
 switchport mode access
 ipv6 nd raguard
!
```

To disable RA Guard on switch ports port1.0.2-1.0.12, use the following commands:

```
awplus#configure terminal

awplus(config)#interface port1.0.2-port1.0.12

awplus(config-if)#no ipv6 nd raguard
```

Related Commands show running-config interface

NTP over IPv6 (CR00033256)

This enhancement is supported on:

- x600 Series
- x610 Series
- x900 Series
- SwitchBlade x908

NTP is a service that allows networked devices to solicit their system time from a central source. This can either be internal to a company, or derived from one of a handful of atomic clocks who provide this time as a service to the Internet community. NTP on Alliedware Plus can accept time from upstream devices, synchronize with peers, and pass the time on to downstream devices. NTP over IPv6 is identical to NTP over IPv4, with IPv6 as the network protocol.

In addition to existing support for NTP via IPv4 addresses, NTP on the switch is now able to synchronise time via IPv6. NTP peer and NTP server addresses can now be specified in the form of IPv6 addresses.

The following commands are modified:

- ntp peer command on page 41
- ntp server command on page 41
- show ntp associations command on page 42

ntp peer

Use this command to configure an NTP peer association. An NTP association is a peer association when one system is willing to synchronize its system time to another system.

Use the no variant of this command to remove the configured NTP peer association.

Syntax

```
ntp peer {<peeraddress>|<peername>}
ntp peer {<peeraddress>|<peername>} [prefer] [key <key>]
   [version <version>]
no ntp peer {<peeraddress>|<peername>}
```

Table 9: Modified parameter in the **ntp peer** command

Parameter	Description
<peeraddress>	Specify the IP address of the peer, entered in the form `A.B.C.D` for an IPv4 address, or in the form `X:X::X.X` for an IPv6 address.
<peername>	Specify the peer hostname. The peer hostname can resolve to an IPv4 and an IPv6 address.

Mode Global Configuration

Examples See the following commands for options to configure NTP peer association, key, and NTP version for the peer with an IPv6 address of: `2001:0db8:010d::1`:

```
awplus# configure terminal
awplus# ntp peer 2001:0db8:010d::1
awplus# ntp peer 2001:0db8:010d::1 prefer
awplus# ntp peer 2001:0db8:010d::1 prefer version 4
awplus# ntp peer 2001:0db8:010d::1 prefer version 4 key 1234
awplus# ntp peer 2001:0db8:010d::1 version 4
awplus# ntp peer 2001:0db8:010d::1 version 4 key 1234
awplus# ntp peer 2001:0db8:010d::1 key 1234
```

To remove an NTP peer association for this peer with an IPv6 address of: `2001:0db8:010d::1`, use the following commands:

```
awplus# configure terminal
awplus# no ntp peer 2001:0db8:010d::1
```

ntp server

Use this command to configure an NTP server. The effect of this command is that it informs the switch of the address of a server that is operating as an NTP time source. So, the switch will then set its system time based on the information it receives from that server. This means that this system will synchronize to the server, and not vice versa.

Use the **no** variant of this command to remove the configured NTP server.

Syntax

```
ntp server {<serveraddress>|<servername>}
ntp server {<serveraddress>|<servername>}
    [prefer] [key <key>] [version <version>]
no ntp server {<serveraddress>|<servername>}
```

Table 10: Modified parameters in the **ntp server** command

Parameter	Description
<serveraddress>	Specify the IP address of the peer, entered in the form `A.B.C.D` for an IPv4 address, or in the form `X:X::X.X` for an IPv6 address.
<servername>	Specify the server hostname. The server hostname can resolve to an IPv4 and an IPv6 address.

Mode Global Configuration

Examples See the following commands for options to configure an NTP server association, key and NTP version for the server with an IPv6 address of: `2001:0db8:010e::2`:

```
awplus# configure terminal
awplus(config)# ntp server 2001:0db8:010e::2
awplus(config)# ntp server 2001:0db8:010e::2 prefer
awplus(config)# ntp server 2001:0db8:010e::2 prefer version 4
awplus(config)# ntp server 2001:0db8:010e::2 prefer version
4 key 1234
awplus(config)# ntp server 2001:0db8:010e::2 version 4 key
1234
awplus(config)# ntp server 2001:0db8:010e::2 version 4
awplus(config)# ntp server 2001:0db8:010e::2 key 1234
```

To remove an NTP peer association for this peer with an IPv6 address of: `2001:0db8:010e::2`, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp server 2001:0db8:010e::2
```

show ntp associations

Use this command to display the status of NTP associations. Use the detail option for displaying detailed information about the associations.

Syntax `show ntp associations [detail]`

Mode User Exec and Privileged Exec

Output

Example output from the **show ntp associations** command

```
awplus# show ntp associations

address ref clock st when poll reach delay offset disp
*~2001:0db8:010e::2 10.32.16.105 5 8 64 377 0.0 0.0 3.9
-~172.134.2.1 172.30.1.251 5 11 64 377 0.0 0.0 3.7
-~172.205.2.1 10.32.16.105 5 37 64 377 0.0 0.0 3.4
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

Example output from the **show ntp associations detail** command

```
awplus# show ntp associations detail

2001:0db8:010e::2 configured, sane, valid, our_master, leap_sub, stratum 5
ref ID 10.32.16.105, time d1ef0db4.a75ed6ef (14:25:56.653 NZST Fri Aug 12 2011)
our mode active, peer mode active, our poll intvl 64, peer poll intvl 64
root delay 4.88 msec, root disp 0.00, reach 037,
delay 0.00 msec, offset -0.0004 msec, dispersion 0.93
precision 2**-20,
org time 00000000.00000000 (18:28:16.000 NZST Thu Feb 7 2036)
rcv time d1ef12fd.a19882fc (14:48:29.631 NZST Fri Aug 12 2011)
xmt time 00000000.00000000 (18:28:16.000 NZST Thu Feb 7 2036)
filtdelay = 0.84 6.72 0.84 6.73 3.61 0.84 0.84 0.84
filtoffset = -0.39 -3.43 -0.58 -3.61 -2.13 -0.75 -0.76 -0.76
filterror = 0.00 1.02 2.04 3.05 3.92 3.95 3.98 4.01
172.134.2.1 configured, sane, valid, selected, leap_sub, stratum 5
ref ID 172.30.1.251, time d1ef1242.fda7e308 (14:45:22.990 NZST Fri Aug 12 2011)
our mode active, peer mode passive, our poll intvl 64, peer poll intvl 64
root delay 5.55 msec, root disp 0.00, reach 377,
delay 0.00 msec, offset -0.0003 msec, dispersion 1.20
precision 2**-18,
org time 00000000.00000000 (18:28:16.000 NZST Thu Feb 7 2036)
rcv time d1ef131c.63a1c639 (14:49:00.389 NZST Fri Aug 12 2011)
xmt time 00000000.00000000 (18:28:16.000 NZST Thu Feb 7 2036)
filtdelay = 0.96 1.05 1.05 1.07 1.03 1.13 1.40 1.03
filtoffset = -0.34 -0.41 -0.51 -0.62 -0.71 -0.85 -1.08 -0.99
filterror = 0.01 1.00 2.95 3.94 4.90 5.87 6.88 7.84
172.205.2.1 configured, sane, valid, selected, leap_sub, stratum 5
ref ID 10.32.16.105, time d1ef0db4.a75ed6ef (14:25:56.653 NZST Fri Aug 12 2011)
our mode active, peer mode active, our poll intvl 64, peer poll intvl 64
root delay 4.88 msec, root disp 0.00, reach 377,
delay 0.00 msec, offset -0.0004 msec, dispersion 0.98
precision 2**-20,
org time 00000000.00000000 (18:28:16.000 NZST Thu Feb 7 2036)
rcv time d1ef12e0.a1951279 (14:48:00.631 NZST Fri Aug 12 2011)
xmt time 00000000.00000000 (18:28:16.000 NZST Thu Feb 7 2036)
filtdelay = 0.79 0.81 0.81 0.83 0.83 0.83 0.73 0.83
filtoffset = -0.41 -0.51 -0.61 -0.71 -0.80 -0.89 -1.04 -1.06
filterror = 0.00 1.01 2.03 3.06 4.05 5.06 6.09 6.95
```

Table 11: Parameters in the output from the **show ntp associations** command

Parameter	Description
address	Peer IP address—IPv4 or IPv6 address
ref clock	IP address for reference clock
st	Stratum. The number of hops between the server and the accurate time source.
poll	Time between NTP requests from the device to the server.
reach	Shows whether or not the NTP server responded to the last request.
delay	Round trip delay between the device and the server.
offset	Difference between the device clock and the server clock.
disp	Lowest measure of error associated with peer offset based on delay.

DHCP Relay over IPv6

This enhancement is supported on:

- x600 Series
- x610 Series
- x900 Series
- SwitchBlade x908

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.

The following commands are modified:

- ip dhcp-relay server-address command on page 44
- show ip dhcp-relay command on page 45

ip dhcp-relay server-address

This command adds a DHCP server for the DHCP relay agent to forward client DHCP packets to on a particular interface. You can add up to five DHCP servers on each device interface that the DHCP relay agent is listening on.

The **no** variant of this command deletes the specified DHCP server from the list of servers available to the DHCP relay agent.

For introduction and configuration information about DHCP relay agent see "*DHCP Relay Agent Introduction*" and "*Configuring the DHCP Relay Agent*" in the *Dynamic Host Configuration Protocol (DHCP) Introduction* chapter in the *Software Reference*.

Syntax

```
ip dhcp-relay server-address {<ipv4-address>|
   <ipv6-address> <server-interface>}

no ip dhcp-relay server-address {<ip-address>|
   <ipv6-address> <server-interface>}
```

Table 12: New parameters in the **ip dhcp-relay server-address**

Parameter	Description
<ipv6-address>	Specify the IPv6 address of the DHCP server for DHCP relay agent to forward client DHCP packets to, in hexadecimal notation.
<server-interface>	Specify the interface via which the DHCP server may be reached, i.e. the interface out which the switch should transmit the packets it is sending to the DHCP server. This parameter is required when the DHCP server has an IPv6 address, but not required when the DHCP server has an IPv4 address.

Mode Interface Configuration for a VLAN interface.

Usage For a DHCP server with an IPv6 address you must specify the interface for the DHCP server. See examples below for configuration differences between IPv4 and IPv6 DHCP relay servers.

See also the **service dhcp-relay** command to enable the DHCP relay agent on your device. The **ip dhcp-relay server-address** command defines a relay destination on an interface on the device, needed before the DHCP relay agent relays DHCP client packets to a DHCP server.

Examples To enable the DHCP relay agent on your device to relay DHCP packets on interface `vlan10` to the DHCP server with the IPv6 address `2001:0db8:010d::1` on interface `vlan20`, use the following command sequence:

```
awplus# configure terminal

awplus(config)# service dhcp-relay

awplus(config)# interface vlan10

awplus(config-if)# ip dhcp-relay server-address
   2001:0db8:010d::1 vlan20
```

To remove the DHCP server with the IPv6 address `2001:0db8:010d::1` on interface `vlan20` from the list of servers available to the DHCP relay agent on interface `vlan10`, use the following command sequence:

```
awplus# configure terminal

awplus(config)# interface vlan10

awplus(config-if)# no ip dhcp-relay server-address
   2001:0db8:010d::1 vlan20
```

Related Commands service dhcp-relay
show ip dhcp-relay

show ip dhcp-relay

This command shows the configuration of the DHCP relay agent on each interface, including any servers configured to IPv4 **or IPv6 addresses**.

Syntax `show ip dhcp-relay [interface <interface-name>]`

Parameter	Description
<interface-name>	Name of a specific interface. This displays the DHCP relay configuration for the specified interface only.

Mode User Exec and Privileged Exec

Example To display the DHCP relay agent's configuration on the interface vlan100, use the command:

```
awplus# show ip dhcp-relay interface vlan100
```

DNS Relay over IPv6

This enhancement is supported on:

- x600 Series
- x610 Series
- x900 Series
- SwitchBlade x908

DNS (Domain Name System) translates domain names meaningful to humans into the numeric identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide. Alliedware Plus has the ability to resolve domain names for internally generated commands (DNS client) as well as providing the DNS information to connected hosts (via DNS relay). The DNS client is enabled automatically when at least one DNS server is configured. This internal DNS client allows you to use domain names instead of IP addresses when using commands on your device. The DNS relay provides a local virtual DNS server, which can service DNS lookup requests sent to it from local hosts, by forwarding the requests to the configured DNS server.

Alliedware Plus now supports Domain Name translation for internal switch applications using remote DNS servers over an IPv6 network via the following modified commands:

- ip name-server command on page 46
- show ip name-server command on page 47

The existing command **ip dns forwarding** has been enhanced and now inherently supports the ability for connected hosts to resolve domain names via a remote DNS server over an IPv6 network.

The **ip name server** command is required in addition to the **ip dns forwarding** command to ensure DNS requests from connected hosts can be relayed to the DNS server.

ip name-server

This command adds the IPv4 or 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. Your device cannot resolve a hostname until you have added at least one server to this list. There is no limit on the number of servers you can add to the list.

The no variant of this command removes the DNS server from the list of servers.

Syntax

```
ip name-server <ip-addr>

no ip name-server <ip-addr>
```

Table 13: Modified parameter in the **ip name-server** command

Parameter	Description
<ip-addr>	The IP address to be advertised with the specified preference value, entered in the form `A.B.C.D` for an IPv4 address, or in the form `X:X::X.X` for an IPv6 address.

Mode Global Configuration

Usage When your device is using its DHCP client for an interface, it can receive Option 6 from the DHCP server. This option appends the name server list with more DNS servers. For more information about DHCP and DHCP options, see the *Dynamic Host Configuration Protocol (DHCP) Introduction* chapter in the Software Reference.

For more information about DNS Relay to map IPv4 and IPv6 addresses to name servers to maintain a a database of hostname-to-address mappings, see "*DNS Relay*" in the *Internet Protocol (IP) Addressing and Protocols* chapter. For information about DNS Client configuration commands, see "*DNS Client*".

Example To allow your device to send DNS queries to a DNS server with the IPv6 address `2001:0db8:010d::1`, use the commands:

```
awplus# configure terminal

awplus(config)# ip name-server 2001:0db8:010d::1
```

Related Commands
ip domain-list
ip domain-lookup
ip domain-name
show ip name-server

show ip name-server

This command displays the list of DNS servers that your device sends DNS requests together with assigned IPv4 and IPv6 addresses. This is a static list configured using the **ip name-server** command.

Syntax
```
show ip name-server
```

Mode User Exec and Privileged Exec

Example To display the list of DNS servers that your device sends DNS requests to, use the command:

```
awplus# show ip name-server
```

Output Figure 2: Example output from the **show ip name-server** command

```
Nameservers:
 10.10.0.123
 10.10.0.124
 2001:0db8:010d::1
 2001:0db8:010d::2
```

Related Commands
ip domain-lookup
ip name-server

AutoBoot from External Media

The Autoboot feature enables your switch to automatically load a specific release file and / or configuration file from external media into Flash memory, providing there is enough free dynamic memory space available. If there is not enough free memory space, the autoboot feature will exit and booting will revert to that previously set by the CLI. This feature is enabled only the first time the device is powered up. Subsequently, the Autoboot feature is disabled by default.

The autoboot feature minimizes network downtime by avoiding the need for manual configuration of a replacement device.

If you use prepared external media for the first time boot, the autoboot feature gives you the ability to easily ensure the device boots with your desired release and configuration files. You must prepare the external media for this purpose using an initiation file, **autoboot.txt**, and accompanying release and configuration files.

Use the command create autoboot, on page 54 to create an `autoboot.txt` file on external media. This command will automatically ensure that the keys and values that are expected in this file are correct. After the file is created the **create autoboot** command will automatically copy the current release and configuration files across to the external media. The `autoboot.txt` file is read / writable by any desktop operating system currently supported by the AlliedWare Plus™ Operating System. Note that the external media file system is not case sensitive.

When the Autoboot feature is enabled, the device on boot-up:

- checks for a special file called `autoboot.txt` on external media, and if this file exists,
- checks in the file for the “key=value” pair “`Copy_from_external_media_enabled=yes`”, and if this enable flag is set,
- loads the release file and / or configuration file from external media.

An example of a valid `autoboot.txt` file is shown below.

```
; J Smith,  x600-24Ts/XP,  16 July 2011
[AlliedWare Plus]
Copy_from_external_media_enabled=yes
Boot_Release=r6-5.4.2-0.1.rel
Boot_Config=network1.cfg
```

If external media is not present, cannot be read, or the internal enable flag is not set to **yes** in the switch, the switch will boot as normal. Incompatible release files are prevented from loading onto the device, even if the enable flag is set on the switch. If there is an incompatible release file then the configuration file referenced in the autoboot.txt file is also not loaded onto the device.

Restoring a switch using AutoBoot from external media

The example shown below describes the sequence of events when a switch in the field fails and is restored using this feature:

1. By using the command create autoboot, a network engineer has previously, manually created a restore media card. This media card contains the following components:
   - An autoboot.txt file with required contents
   - An appropriate release file
   - A configuration file
2. A switch fails in the field.
3. A replacement switch of same model is installed.

Note: *This replacement switch must already have a xx541-2.6 or later release or bootloader version 1.1.6 or later pre-installed to be able to detect and interpret the* `autoboot.txt file`*.*

4. A previously created external media device is placed into the replacement switch.
5. The switch powers up using its pre-installed release if present. It automatically checks the external media card for the autoboot.txt file.
6. The device finds a valid autoboot.txt file on the external media card, with the value Copy_from_external_media_enabled set. The release file and configuration file both exist on the external media card.
7. The MD5sum of the pre-installed flash release file is compared to the MD5sum of the release file stored in the external media device. If they do not match (because the release file in the replacement switch is either missing or different), then the release will be restored from the external media card. If the release files match, then the release file is not copied from the external media.
8. The MD5sum of the flash config file default.cfg (if pre-installed in the replacement switch) is compared to the MD5sum of the config file stored in the external media. If they do not match (because the config file in the replacement switch is either missing or different), then the config file will be restored from the external media card. If the config files already match, then the config file is not copied from the external media.
9. The memory space available in the switch flash is checked to ensure the release and config file stored in the external media will fit. If there is not enough space the Autoboot program will exit.
10. The release file and config files are automatically copied from the external media card to switch flash memory. The switch .release and .config files are updated to contain the appropriate names.
11. The switch automatically reboots.
12. The replacement switch is now running the restored release and configuration files. Subsequent reboots will be based on the restored release and config files stored in the switch flash memory.
13. If you want to autoboot from external media, on this specific device, in the future, you must now manually enable the autoboot feature in the configuration menu via the `autoboot enable` command. This command resets the enable flag stored internally in the switch NVS memory.

Allied Telesis recommends that no directories are present on external media used to hold the `autoboot.txt` file. In addition, large numbers of files on external media may slow the booting process.

Notes

Note: The Autoboot feature is not supported in a stacked configuration.

Note: Do not remove external media part way through the copy process, as this may leave the device in an unstable state.

Note: Configuration files placed on external media reduce security. Therefore, ensure adequate security precautions are taken with external media holding configuration files.

Note: Configuration commands that rely on the presence of a feature license will fail when executed in the replacement switch if the replacement switch does not have the same feature license present.

Note: The bootloader version on the switch must be 1.1.6 or greater to support appropriate external media. An *autoboot.txt* file on an external SD card will not be detected on a device with a bootloader version less than 1.1.6.

Configuration procedures for the Autoboot feature

Create an Autoboot file (autoboot.txt)	
awplus#	
create autoboot [card|usb]	Create an autoboot.txt file on external media.
Enable the Autoboot feature	
awplus#	
configure terminal	Enter Global Configuration mode.
awplus(config)#	
autoboot enable	The Autoboot feature is enabled by default the first time the device is powered up in the field. Use this command to enable the feature subsequently.

Configuration procedures for the Autoboot feature (cont.)

Disable the Autoboot feature	
awplus(config)#	
no autoboot enable	Use this command to disable the Autoboot feature.
Display Autoboot configuration and status	
awplus#	
show autoboot	Display detailed information about the current Autoboot configuration and status.
awplus#	
show boot	Display the status of the Autoboot feature; either enabled or disabled.

autoboot enable

This command enables the device to restore a release file and / or a configuration file from external media. When the Autoboot feature is enabled, the device looks for a special file called `autoboot.txt` on the external media. If this file exists, the device will check the key and values in the file and recover the device with a new release file and / or configuration file from the external media. An example of a valid `autoboot.txt` file is shown below.

Example autoboot.txt file

```
; J Smith,  x600-24Ts/XP,  16 July 2011
[AlliedWare Plus]
Copy_from_external_media_enabled=yes
Boot_Release=r6-5.4.2-0.1.rel
Boot_Config=network1.cfg
```

Use the no variant of this command to disable the Autoboot feature.

Note: *This command is not supported in a stacked configuration.*

Syntax `autoboot enable`

`no autoboot enable`

Default The Autoboot feature operates the first time the device is powered up in the field, after which the feature is disabled by default in the switch.

Mode Global Configuration

Example To enable the Autoboot feature, use the command:

```
awplus# configure terminal
awplus(config)# autoboot enable
```

To disable the Autoboot feature, use the command:

```
awplus# configure terminal
awplus(config)# no autoboot enable
```

Related Commands

create autoboot
show autoboot
show boot

show autoboot

This command displays the Autoboot configuration and status.

Syntax

```
show autoboot
```

Mode

Privileged Exec

Example

To show the Autoboot configuration and status, use the command:

```
awplus# show autoboot
```

Output

Example output from the **show autoboot** command

```
awplus#show autoboot
Autoboot configuration
------------------------------------------------------------
Autoboot status                  : enabled
SD Card file autoboot.txt exists : yes

Restore information on SD card
Autoboot enable in autoboot.txt  : yes
Restore release file             : r6-main-20110624-3.rel
(file exists)
Restore configuration file       : network_1.cfg (file
exists)
```

Example output from the **show autoboot** command when an external media source is not present

```
awplus#show autoboot
Autoboot configuration
------------------------------------------------------------
Autoboot status                  : enabled
External media source            : SD card not found.
```

show boot

This command displays the current boot configuration. This command now displays the status of the autoboot feature.

Syntax `show boot`

Mode Privileged Exec

Example To show the current boot configuration, use the command:

```
awplus# show boot
```

Output Example output from the **show boot** command

```
awplus#show boot
Boot configuration
-----------------------------------------------------------
Current software   : r1-5.4.1.rel
Current boot image : card:/r1-5.4.1.rel
Backup  boot image : flash:/r1-5.3.4.rel
Default boot config: flash:/default.cfg
Current boot config: card:/my.cfg (file exists)
Backup  boot config: flash:/backup.cfg (file not found)
Autoboot status    : enabled
```

Parameters in the output of the **show boot** command

Parameter	Description
`Current software`	The current software release that the device is using.
`Current boot image`	The boot image currently configured for use during the next boot cycle.
`Backup boot image`	The boot image to use during the next boot cycle if the device cannot load the main image.
`Default boot config`	The default startup configuration file. The device loads this configuration script if no file is set as the startup-config file.
`Current boot config`	The configuration file currently configured as the startup-config file. The device loads this configuration file during the next boot cycle if this file exists.
`Backup boot config`	The configuration file to use during the next boot cycle if the main configuration file cannot be loaded.
`Autoboot status`	The status of the Autoboot feature; either enabled or disabled.

Related Commands
autoboot enable
boot backup (Deprecated)
boot config-file
boot system
show autoboot

create autoboot

Use this command to create an `autoboot.txt` file on external media. This command will automatically ensure that the keys and values that are expected in this file are correct. After the file is created the create autoboot command will copy the current release and configuration files across to the external media. The external media is then available to restore a release file and/or a configuration file to the device.

Syntax `create autoboot [card|usb]`

Mode Privileged Exec

Example To create an `autoboot.txt` on external media, use the command:

```
awplus# create autoboot card
```

Related Commands autoboot enable
show autoboot
show boot

Other Enhancements in 5.4.1-2.6

CR	Module	Description

CR00017854	**Command Shell**	Hardware flow control is now supported on async serial ports. Hardware flow control makes use of the RS232 RTS and CTS signals to control the flow of data between the transmitter and receiver. This assists in the uninterrupted flow of data if the rate of transmission is faster than the rate of receiving.
		`awplus(config)#line console 0`
		`awplus(config-line)#flowcontrol ?`
		`hardware RTS/CTS hardware flow control`
		`awplus(config-line)#flowcontrol hardware`

CR00032352	**IP Multicasting**	A new command **ip multicast route** has been provided to forward multicast traffic from a specific source and group ingressing on an upstream VLAN to a single or range of downstream VLANs. See below for more detail.

ip multicast route (CR00032352)

Use this command to add a static multicast route for a specific multicast source and group address to the multicast Routing Information Base (RIB). This multicast route is used to forward multicast traffic from a specific source and group ingressing on an upstream VLAN to a single or range of downstream VLANs.

Use the no variant of this command to either remove a static multicast route set with this command or to remove a specific downstream VLAN interface from a static multicast route for a specific multicast source and group address.

Syntax

```
ip multicast route <source-addr> <group-addr> <upstream-vlan-id> [<downstream-vlan-id>]

no ip multicast route <source-addr> <group-addr> [<upstream-vlan-id> <downstream-vlan-id>]
```

Parameter	Description
<source-addr>	Source IP address, in dotted decimal notation in the format `A.B.C.D`.
<group-addr>	Group IP address, in dotted decimal notation in the format `A.B.C.D`.
<upstream-vlan-id>	Upstream VLAN interface on which the multicast packets ingress.
<downstream-vlan-id>	Downstream VLAN interface or range of VLAN interfaces to which the multicast packets are sent.

Default By default, this feature is **disabled**.

Mode Global Configuration

Usage Only one multicast route entry per IP address and multicast group can be specified. Therefore, if one entry for a static multicast route is configured, PIM will not be able to update this multicast route in any way.

If a dynamic multicast route exists you cannot create a static multicast route with same source IP address, group IP address, upstream VLAN and downstream VLANs. An error message is displayed and logged. To add a new static multicast route, either wait for the dynamic multicast route to timeout or clear the dynamic multicast route with the clear ip mroute * command.

To update an existing static multicast route entry with more or a new set of downstream VLANs, you must firstly remove the existing static multicast route and then add the new static multicast route with all downstream VLANs specified. If you attempt to update an existing static multicast route entry with an additional VLAN or VLANs an error message is displayed and logged.

To create a black hole or null route where packets from a specified source and group address coming from an upstream VLAN are dropped rather than forwarded, do not specify the optional *<downstream-vlan-id>* parameter when entering this command.

To remove a specific downstream VLAN from an existing static multicast route entry, specify the VLAN you want to remove with the *<downstream-vlan-id>* parameter when entering the no variant of this command.

Example To create a static multicast route for the multicast source IP address `2.2.2.2` and group IP address `224.9.10.11`, specifying the upstream VLAN interface as `vlan10` and the downstream VLAN interface as `vlan20`, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast route 2.2.2.2 224.9.10.11
vlan10 vlan20
```

To create a blackhole route for the multicast source IP address `2.2.2.2` and group IP address `224.9.10.11`, specifying the upstream VLAN interface as `vlan10`, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast route 2.2.2.2 224.9.10.11
vlan10
```

To create a static multicast route for the multicast source IP address `2.2.2.2` and group IP address `224.9.10.11`, specifying the upstream VLAN interface as `vlan10` and the downstream VLAN range as `vlan20-25`, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast route 2.2.2.2 224.9.10.11
vlan10 vlan20-25
```

To remove the downstream VLAN 23 from the static multicast route created with the above command, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip multicast route 2.2.2.2 224.9.10.11
vlan10 vlan23
```

To delete a static multicast route for the multicast source IP address 2.2.2.2 and group IP address 224.9.10.11, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip multicast route 2.2.2.2 224.9.10.11
```

Related Commands show ip mroute

New Features and Enhancements in 5.4.1-1.5

AlliedWare Plus version 5.4.1-1.5 includes the following new enhancements. Unless otherwise stated, this feature applies to all switches supported by this software version.

Announcing the release of the XEM-2XS expansion module

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.

Cables for use with XEM-2XS

Description

- AT-SP10TW1 - 1 meter SFP+ Direct Attach cable
- AT-SP10TW3 - 3 meter SFP+ Direct Attach cable
- AT-SP10TW7 - 7 meter SFP+ Direct Attach cable

10GBE SFP+ modules for use with XEM-2XS

Description

- AT-SP10SR 10GBASE-SR 850nm short-haul, 300m with MMF
- AT-SP10LR 10GBASE-LR 1310nm medium-haul, 10 km with SMF

For additional information about the Allied Telesis XEM family please refer to the High Speed Expansion Modules, XEM data sheet.

Enhancements

CR	Module	Description
CR00032709	**IP**	The **show ip interface** command lists the primary IP addresses for each interface. This has been enhanced to also show any secondary IP addresses which exist on each interface. To show only the primary addresses, use the brief command: **show interface brief**.
CR00032029	**System**	On rare occasions, a system reboot could occur as a result of internal bit errors causing a hardware subsystem to lock up. The software has been enhanced to detect this fault condition, and recover from the condition automatically, preventing a system reboot.

New Features and Enhancements in 5.4.1-1.4

AlliedWare Plus version 5.4.1-1.4 includes the following new enhancements. Unless otherwise stated, this feature applies to all switches supported by this software version.

Enhancements

CR	Module	Description

CR00031398	**Link Aggregation**	x600 only
		The existing x900 command **platform load-balancing** (which allows the user to select a hashing criteria for LAGs) is now supported in the x600 switch with the following options:
		`platform load-balancing src-dst-mac`
		`platform load-balancing src-dst-ip`
		Note: The configuration use of the load balancing options in x600 are a Boolean "OR" whereas for the x900 the use of the load balancing options are a Boolean "AND".

New Features and Enhancements in 5.4.1-1.3

AlliedWare Plus version 5.4.1-1.3 includes the following new enhancements. Unless otherwise stated, this feature applies to all switches supported by this software version.

Enhancements

CR	Module	Description

CR00030163	**SFP**	Support has been added to the x900 Series and SBx908 switches for the RAD MiRICi GE SFPs (Gigabit Ethernet-to-DS3 bridge-on-an-SFP). These commands:
		`speed 1000`
		`duplex full`
		can be used to provision and configure these RAD SFPs.

CR00030562	**IGMP**	Previously, you could display mrouter interface information for a specified interface. You can now also display this information for all interfaces (VLANs), by using a single command: `show ip igmp snooping mrouter` The output from this command is also included in the output from the **show tech-support** command.
CR00032289	**VRF-Lite, BGPv4**	VRF-Lite now supports the BGPv4 command **local-as**. This will allow internal BGP loopback connections between named VRFs and the default global routing instance to be configured to act as eBGP connections, instead of only iBGP.
CR00030008	**IGMP**	Previously, the transmission of IGMP Query Solicit messages could not be disabled on an EPSR Master or xSTP Root node. This issue has been resolved. A new pair of VLAN interface mode commands have been added: **ip igmp snooping tcn query solicit**, and the '**no**' version, to allow Enable/Disable of IGMP Query Solicit messages on a per-VLAN basis.

Issues Resolved in 5.4.1-2.12

The issues addressed in this document include a level number. This number reflects the importance of the issue that has been resolved. The levels are:

Level 1 This issue will cause significant interruption to network services, and there is no work-around.

Level 2 This issue will cause interruption to network service, however there is a work-around.

Level 3 This issue will seldom appear, and will cause minor inconvenience.

Level 4 This issue represents a cosmetic change and does not affect network operation.

Level 1

No level 1 issues.

Level 2

CR	Module	Description	x900/x908	x600	x610
CR00036756	**ARP**	Previously, if a nexthop remained valid for longer than 25 days, then moved port or became unreachable for a short period and then returned, there was a chance that the ARP entry for that nexthop would not be successfully relearnt. As a workaround, an entry in this state could be successfully relearnt by momentarily shutting down the VLAN and then renabling the VLAN. This issue has been resolved; the workaround is no longer necessary.	Y	Y	Y

Level 3 & 4

No level 3 or 4 issues

Issues Resolved in 5.4.1-2.11

Level 1

CR	Module	Description	x900/x908	x600	x610
CR00035515	**Boot Setup**	Previously, in rare cases the switch could get into an unresponsive state when a syslog restart occurred. This issue has been resolved.	Y	Y	Y

Level 2

CR	Module	Description	x900/x908	x600	x610
CR00032447	**OSPFv2** **OSPFv3**	Previously, if the switch had invalid OSPFv2 and OSPFv3 configuration in which an area that shared an ABR with the backbone area also had a virtual link configured, making itself a transit area to the backbone area, a system reboot could occur. This issue has been resolved.	Y	Y	Y
CR00033749	**IGMP**	Previously, under some circumstances (depending on the IP addresses assigned), an IGMP proxy interface could become the IGMP querier. This issue has been resolved—now the IGMP proxy interface will never become the querier.	Y	Y	Y
CR00034925	**OSPFv2**	Previously, if a stack was under heavy load, occasionally during a master failover event, OSPF would not correctly perform graceful restart. This would result in a longer convergence time. This issue has been resolved—OSPF will now correctly performs graceful restart under these conditions.	Y	Y	Y
CR00034936	**DHCPv4 Relay**	Previously, in an IPv4/IPv6 dual stack environment, when a switch operating as a DHCP relay lost both the IPv4 and IPv6 routes to the DHCP server, when the route was recovered, packets could not be relayed or sometimes a DHCP relay exception occurred. This issue has been resolved.	Y	Y	Y
CR00035075	**BGPv4**	Previously, when BGP was configured on a VCStack with a resiliency link, sometimes a master failover resulted in traffic interruption for several seconds. This issue has been resolved.	Y	Y	Y
CR00035100	**VLAN**	Previously, nested VLANs (also known as QinQ or VLAN double-tagged), did not function correctly via XEM-2XP, XEM-2XS, or XEM-2XT. This issue has been resolved.	Y	–	–
CR00035135	**IPv6 Neighbour Discovery**	Previously, using the command **ipv6 nd suppress-ra** on a shutdown VLAN could cause an exception to be generated. This issue has been resolved.	Y	Y	Y

CR	Module	Description	x900/x908	x600	x610
CR00035164	BGPv4	Previously, on a VCStack with an inter-VRF BGP configuration, master failover sometimes resulted in traffic interruption. This issue has been resolved.	Y	Y	Y
CR00035166	DHCPv4 Relay	Previously, DHCP relay occasionally exited during VLAN startup. This issue has been resolved.	Y	Y	Y
CR00036268	PIM-SMv4	Previously, when PIM-SM and the multicast Routing Information Base (RIB) engine was under heavy load sometimes local multicast joins failed to be added as downstream interfaces on the relevant multicast routing entry, causing data not to be forwarded to the interface correctly. This issue has been resolved.	Y	Y	Y
CR00036327	VCStack, Triggers	Previously, if a trigger was setup to run a script on a master failover, then this sometimes caused a system reboot. This issue has been resolved.	Y	Y	Y
CR00036360	PIM-DMv4	Previously, a newly added PIM-DM interface was always added as a downstream interface of existing multicast route entries regardless of the existence of local joins or neighbouring router on this interface. As a result, data might have flowed unnecessarily to the switch from the upstream router and never be pruned. This issue has been resolved.	Y	Y	Y
CR00036432	System	Previously, static routing entries that overlapped directly connected routes could sometimes be lost from hardware, and were not re-added automatically, when a port unrelated to those static routes was shut down. This issue has been resolved.	Y	Y	Y
CR00032939	VCStack	Previously, if a stack member joined a stack and then left the stack within 10 secs of joining, then the stack would not let any more stack members join. This issue has been resolved.	Y	Y	Y
CR00035006	Command Shell	Previously, use of the small selection of commands that support the ability to accept an interface range could have resulted in a memory leak, or in rare cases a process termination. This issue has been resolved.	Y	Y	Y
CR00035296	OSPFv2	Previously, OSPF routers on a common Ethernet network could occasionally, under very rare circumstances, get into a state where the **show ip ospf route** command would show no routes and new routes were not being added correctly. The circumstances were: ■ two neighbours lose 2-way connectivity ■ other neighbours (especially the Designated Router) do not lose connectivity ■ no other changes in the routing state of the network occur (route recalculation would clear the error state) This issue has been resolved.	Y	Y	Y

CR	Module	Description	x900/x908	x600	x610
CR00035780	SNMP MIB Support	Previously, using SNMPWALK on the AT-LOG MIB in a VCStack could result in a system reboot. This issue has been resolved.	Y	Y	Y

Level 3

CR	Module	Description	x900/x908	x600	x610
CR00035090	Pluggable Transceivers	Previously, during bootup, 10G SFP+ ports came up and went down unnecessarily. This could slightly increase convergence time when a new stack member joined a VCStack. This issue has been resolved.	–	–	Y
CR00036346	Triggers	Previously, an interface trigger on a VCStack sometimes failed after master failover. This issue has been resolved.	Y	Y	Y
CR00034979	Pluggable Transceivers	Previously, flow control could be on momentarily when the configuration for flow control was off. This issue has been resolved.	Y	Y	Y
CR00035054	VLAN	Previously, hosts in an isolated VLAN could ping the IP address of the primary VLAN of the switch. This issue has been resolved.	–	Y	–
CR00035165	ACL	Previously, deleting an interface with an access group attached and attaching the group to a new interface could produce misleading error messages. This issue has been resolved.	Y	–	–
CR00035246	Pluggable Transceivers	The transmit and receive power values and thresholds displayed by DDM (Digital Diagnostics Monitoring) in **show system pluggable** diagnostics were incorrectly interpreted. This issue has been resolved.	Y	Y	Y
CR00035249	Pluggable Transceivers	Previously, when an 10G SFP+ installed in an x610 series switch with 7m passive cables connected and under full load, a very small amount of packet loss may have occurred. This issue has been resolved.	–	–	Y
CR00035288	Logging	When the **log email** command was configured on a stack, both the master and backup members tried to send emails to the SMTP Server. Since only the master is actually able to send emails, the backup members were using up Flash memory to store the unsent emails and unterminated processes. This caused unnecessary log messages and memory leaks on the backup members. This issue has been resolved.	Y	Y	Y

CR	Module	Description	x900/x908	x600	x610
CR00035319	DHCPv4	Previously, the DHCP server would not NAK (Negatively Acknowledge) some lease renewal requests from a client that had been moved to a different subnet. This issue has been resolved. Most DHCP clients, upon physically being moved to a new subnet, go to the INIT-REBOOT state and immediately request a lease reconfirmation, in which case this issue does not occur. However, some clients, e.g. Windows XP DHCP client, do not change state when moved to a new subnet, and it is for these clients that this change has been made.	y	y	y
CR00035389	OSPFv3	Previously, static IPv6 blackhole routes (with a Null destination interface) failed to be redistributed to routing protocols. This issue has been resolved.	Y	Y	Y
CR00036033	PIM-SM v4	Previously in mixed mode PIM-DM and PIM-SM networks, when a switch acting as RP for a PIM-SM domain received a (*,*,RP) join from a directly connected border PIM router which was forwarding a multicast group from a PIM-DM domain, the interface receiving the group could be incorrectly added to the outgoing interface list, resulting in a multicast loop between the RP and PIM border router. This issue has been resolved.	Y	Y	Y

Level 4

CR	Module	Level	Description	x900/x908	x600	x610
CR00034776	VRF-Lite	4	Previously, if there was no BGP feature licence present, the commands **show ip vrf**, **show ip vrf brief**, and **show ip vrf detail** did not display the relevant information. This issue has been resolved.	–	Y	Y
CR00035222	Logging	4	Previously, any unsent email messages were stored in memory until memory ran out. This could produce a memory leak. This issue has been resolved. Now the maximum allowable memory storage size is 5% of total RAM for emails. A memory check ensures that new messages are not added to the queue when the limit is reached. This will prevent emails from consuming too much of the system resource.	Y	Y	Y
CR00035410	BGPv4	4	Previously, the switch would not accept 0 as a valid parameter in the **ip community-list** command (in the form of X:0 nor 0:X). This issue has been resolved.	Y	Y	Y

CR	Module	Level	Description	x900/x908	x600	x610
CR00035613	**SNMP MIB Support**	**4**	Previously, when performing SNMP GETNEXT for objects with large instance-IDs in the AT-LOG-MIB, lexicographic ordering of the returned values failed. This issue has been resolved.	Y	Y	Y
CR00035624	**Scripting, VCStack**	**4**	Previously, remote-login to a back-up stack member failed if the user was remotely authenticated via either TACACS+ or RADIUS. This issue has been resolved.	Y	Y	Y

Issues Resolved in 5.4.1-2.10

Level 1

No level 1 issues.

Level 2

CR	Module	Description	x900/x908	x600	x610
CR00034463	**L2 Switching** **VCStack**	Previously, on a VCStack, a broadcast storm with a large number of MAC addresses sometimes resulted in excessive memory use, which could eventually lead to a system reboot. This issue has been resolved.	–	Y	Y
CR00034512	**IPv6**	Previously, when ECMP was used with static IPv6 routes, sometimes not all routes were used—sometimes only one route was used, resulting in ECMP not distributing traffic across all routes that have been configured to use ECMP. This issue has been resolved.	Y	Y	Y
CR00034696	**Policy-based Routing** **Link aggregation**	Previously, if a VCStack of x900 or SBx908s had a late-joining member configured with Policy-based Routing over link aggregators, a master failover sometimes resulted in the polic-based routes for these link aggregators being lost. This issue has been resolved.	Y	–	–
CR00034922	**Console**	Previously, running the command **clear line console 0** resulted in the speed of the console port, and the console ports on units in the same stack, being reset to 9600, and therefore appearing to lock up. Rebooting was required to restore the speed of console ports. This issue has been resolved.	Y	Y	Y
CR00034976	**Link Aggregation**	Previously, running the **show etherchannel detail** command used a small amount of memory that was not freed. This issue has been resolved.	Y	Y	Y
CR00034988	**PBR**	Previously, it was possible to specify an ACL that used the **copy-to-mirror** action in combination with Policy-Based Routing. In 5.4.1, this combination was incorrectly rejected. This issue has been resolved. It is now again possible to use **copy-to-mirror** ACL actions in conjunction with PBR.	Y	–	–
CR00035051	**VCStack**	After a VCStack master fails, and an auth-supplicant moves to another port by roaming authentication, entries in the auth-supplicant and MAC address tables are updated to the new port. Previously, the switch failed to update the ARP table accordingly, stopping connectivity to the supplicant. This issue has been resolved.	–	Y	Y

Level 3

CR	Module	Description	x900/x908	x600	x610
CR00034101	**L3 Switching**	Previously, if maximum-sized multicast ethernet frames arrived into an interface on a XEM-2XS, XEM-2XP or XEM-2XT, a number of log messages of the form "Puma but i (1) != 0" were created. This issue has been resolved.	Y	–	–
CR00034111	**Port Authentication**	Previously, when a supplicant failed twice at 802.1X port authentication by RADIUS, port authentication sometimes stopped responding. This issue has been resolved.	Y	Y	Y
CR00034471	**IPv6**	Previously, when using 6to4 tunnels, if the tunnel source IP address was unset and then re-set (**tunnel source** command), when the tunnel was destroyed, the device sometimes became unresponsive and eventually (after about 10 minutes) a system reboot could occur. This issue has been resolved.	Y	Y	Y
CR00034575	**IGMP snooping**	Previously, IGMP snooping with the querier feature enabled failed to send group-specific queries when a leave message was received from multicast clients. This issue has been resolved.	Y	Y	Y
CR00034578	**IGMP snooping**	Previously, when IGMP snooping with the querier feature was enabled, the snooping switch did not cease to be a querier when it saw a query from a router with a lower IP address. This issue has been resolved.	Y	Y	Y
CR00034586	**OSPFv2**	Previously, OSPF sometimes failed to properly execute a graceful restart during a master failover. This issue has been resolved.	Y	Y	Y
CR00034612	**Command line**	Previously, a small number of commands (including the **show interface status** command) resulted in very small memory leaks. This issue has been resolved.	Y	Y	Y
CR00034653	**Link Aggregation**	Previously, in a VCStack environment, when the switch was under stress the switch failed to get the correct channel group information from the stack member. This issue has been resolved.	Y	Y	Y
CR00034713	**IPv6**	Previously, there was a small amount of traffic loss for tunnelled IPv6to4 traffic via a XEM-2XP, XEM-2XT, or XEM-2XS. This issue has been resolved.	Y	–	–
CR00034745	**DNS**	Previously, when all external DNS servers were not reachable, DNS relay could fail on reception of a DNS query from a clients. This issue has been resolved.	Y	Y	Y

CR	Module	Description	x900/x908	x600	x610
CR00034793	**SNMP**	By default, the SNMP server is enabled for both IPv4 and IPv6. Previously, disabling the SNMP server for IPv6 (**no snmp-server ipv6** command) and then re-enabling it (**snmp-server ipv6** command) incorrectly resulted in the SNMP server for IPv4 being disabled. This issue has been resolved. The SNMP server can now be independently disabled and enabled for IPv4 and IPv6.	Y	Y	Y
CR00034800	**SNMP**	Previously, snmpwalk on the LLDP MIB sometimes failed on switches that support VRF. This could affect the information available to some SNMP manager applications. This issue has been resolved.	Y	–	Y
CR00034866	**User**	Previously, if an SNMP user logged in and out via Telnet or SSH, or if the **show ntp status** command was used, a small memory leak sometimes occurred. This issue has been resolved.	Y	Y	Y
CR00034919	**SNMP**	Previously, the GUI user authentication password was not changed by specifying a new password with the **username** command. This issue has been resolved—the GUI user password can now be changed.	Y	Y	Y
CR00034947	**EPSR**	Previously, when the EPSR process stopped responding, the EPSR Enhanced Recovery Config (**epsr enhancedrecovery enable** command) was lost from the running-config. This issue has been resolved.	Y	Y	Y

Level 4

No level 4 Issues.

Issues Resolved in 5.4.1-2.9

Level 1

No level 1 issues.

Level 2

CR	Module	Description	x900/x908	x600	x610
CR00032344	**OSPFv2** **VCStack**	Previously, if a VCStack failover occurred immediately after an OSPF graceful restart on the stack master, then the new master sometimes failed to restart the OSPF process This issue has been resolved.	Y	Y	Y
CR00032665	**VCStack**	Previously, in a busy multicast environment, sometimes a new member joining an existing VCStack would fail to join. This issue has been resolved.	Y	Y	Y
CR00034013	**SNMP**	Previously, unsetting the backup config via SNMP sometimes resulted in a system reboot. This issue has been resolved.	Y	Y	Y
CR00034031	**IGMP** **PIM**	Previously, on x610 switches, multicast packets with TTL=1 were L2 switched correctly; however they were also unnecessarily copied to the device CPU, causing high CPU utilisation. This issue has been resolved.	–	–	Y
CR00034216	**IPv6** **vlan**	Previously, it was possible for every 30th VLAN with an IPv6 address not to contain a link local address. This issue has been resolved.	Y	Y	Y
CR00034316	**PIM-DM**	Previously, in rare cases PIM-DM became inconsistent across a VCStack. If a failover occurred in this inconsistent state, then it could take up to 30 seconds for the affected multicast traffic to fully recover. This issue has been resolved.	Y	Y	Y
CR00034352	**QOS**	Previously, the QOS police rate configuration was sometimes removed from the running-config after a master failover. This issue has been resolved.	Y	Y	Y

CR	Module	Description	x900/x908	x600	x610
CR00034468	VCStack ARP	Previously, a problem could occur on VCStack failover in a Layer 3 switched network environment. The problem occurred if the switches in the stack had a large number of dynamic nexthops associated with ARP entries that needed to change egress port to continue forwarding, and there was also a high rate of traffic. The problem was that the software and hardware ARP tables could get out of sync. This resulted in software forwarding of IP traffic. Previously, the problem could be avoided by manually using the **clear arp-cache** command. This issue has been resolved—the ARP tables are now kept in sync automatically, without needing to manually enter the **clear arp cache** command.	Y	Y	Y
CR00034700	EPSR	Previously, a VCStack consisting of x600 or x610 units running as an EPSR master node with EPSR secondary ports on a VCStack backup member sometimes dropped traffic for a short time when EPSR topology changed, especially under heavy load (e.g. many ARPs to re-learn). This issue has been resolved.	–	Y	Y
CR00034752	PIM-SMv4	Previously, in a network where two PIM-SM switches connect to the same VLAN and only one has a multicast client connected, the same multicast stream received on both switches was copied to the CPU of the switch without a multicast client. This caused a high load on the CPU and extensive internal messaging between internal software modules in the switch which did not have the multicast client connected. This issue has been resolved.	Y	Y	Y

Level 3

CR	Module	Description	x900/x908	x600	x610
CR00034339	GUI	Previously, when a GUI user was created, the SNMP-server **user** command did not appear in the running configuration. If the running configuration was saved and the device was rebooted, then no SNMP user was created for the GUI application. This issue has been resolved.	Y	Y	Y
CR00031473	SNMP MIB Support	Previously, aggregator interfaces were not assigned an SNMP bridge port number when they were created. The result was that an SNMP query for the STP states of the switch's interfaces would not return the STP state of aggregator interfaces. This issue has been resolved.	Y	Y	Y
CR00033955	TACACS+ RADIUS Accounting	Previously, interim update packets were sent to a TACACS+ server even if login accounting was only configured for RADIUS. This issue has been resolved.	Y	Y	Y

CR	Module	Description	x900/x908	x600	x610
CR00034108	**System**	Previously, when a file was copied to a remote directory by SCP, the filename was not preserved. This issue has been resolved. Now, the copied file on the remote SCP server has the same file name as the source.	Y	Y	Y
CR00034256	**ACL**	Previously, if the command: `ipv6 access-list extended <name> permit proto <number>` included the **protocol** parameter, it was sometimes inadvertently removed from the device running-config after a reboot. This issue has been resolved.	Y	Y	Y
CR00034394	**VCStack** **OSPF**	Previously, stack members totally disconnected from the master sometimes prematurely caused protocols such as OSPF to initiate the fast failover procedure by starting the graceful restart mechanism before the stack members became disabled masters. This issue has been resolved.	Y	Y	Y
CR00034424	**System**	Previously, an x610 switch connected to an RPS unit sometimes generated unnecessary RPS log messages if the RPS cable was repeatedly plugged and unplugged in quick succession. This issue has been resolved.	–	–	Y
CR00034541	**DHCPv4**	Previously, if a **client-id** had been specified on the switch when configuring a DHCP client, and a reboot occured, this information was sometimes lost. This issue has been resolved.	Y	Y	Y
CR00034587	**IGMP Snooping**	Previously, if IGMP snooping was globally disabled, then re-enabled, the VLAN interfaces sometimes did not restart IGMP snooping. This prevented groups/query information being learnt on the interface. This issue has been resolved.	Y	Y	Y
CR00033524	**ARP**	Previously, repeatedly received gratuitous ARPs sometimes caused an unnecessary delay in writing the ARP information to hardware. This unnecessarily increased the traffic that was routed via software instead of hardware switching. This issue has been resolved.	Y	Y	Y
CR00034230	**NTP**	Previously, the command prompt was not displayed on a new line after executing the **show ntp associations** command. This issue has been resolved.	Y	Y	Y
CR00034436	**DHCPv4**	Previously, deleting a lease from the DHCP server (using the **clear ip dhcp binding** command) could under certain conditions result in other leases that did not match the command also being deleted. This issue has been resolved.	Y	Y	Y

CR	Module	Description	x900/x908	x600	x610
CR00034742	System	In 5.4.1-2.8, sometimes a GUI user created via the **username** commmand could not log into the switch, and an error message like the following was generated: `user.err awplus snmpd[1848]: /etc/snmpd.conf: line 9: Error : could not generate localized authentication key (Kul) from the master key (Ku)` The issue did not occur in 5.4.1-2.7 or earlier versions. This issue has been resolved.	Y	Y	Y
CR00034762	VCStack, Core	Previously, on a VCStack of four x600 or x610 Series switches, repeated reboots sometimes resulted in incorrect multicast group details being displayed by the **sh ip igmp group** command. This issue has been resolved.	–	Y	Y

Level 4

CR	Module	Description	x900/x908	x600	x610
CR00032858	LLDP	Previously, on startup, an erroneous LLDP message was sometimes displayed: `LLDP{ID] Unable to send PDU on portx.x.x, error` This was because the port was not yet in the LINKUP state at the time the first LLDPDU was generated. This issue has been resolved.	Y	Y	Y
CR00033037	Link Aggregation (Channel Groups)	Previously, ports were sometimes displayed out of sequence by the command **show etherchannel detail**. This issue has been resolved.	Y	Y	Y
CR00033620	Port Authentication	Previously, a small memory leak sometimes occurred if there was packet loss during the Web Authentication procedure—if the loss occurred after the initial TCP connection was established, but before the HTTP Get request. For example, if remote clients attempting web authentication were wirelessly connected and were migrating from one access point to another, and this was detected by the switch as a MAC station movement from one switch port to another on the physical LAN. This issue has been resolved.	Y	Y	Y
CR00033735	Switching	Previously, packets with a length between 1507 and 1518 were counted as oversize on the internal ports, as shown by the **show platform xbar** command. This issue has been resolved. Only packets larger than 1518 bytes are now counted as oversize.	Y	Y	Y

CR	Module	Description	x900/x908	x600	x610
CR00033893	**License**	Previously, if users tried to add a temporary licence when the clock was not correct, a message was sometimes generated that said the licence was invalid. This issue has been resolved. A message now explicitly tells the user when a licence has expired.	Y	Y	Y
CR00034098	**Pluggable**	Hotswapping the x6EM/XS2 module with an SFP+ module inserted could cause the following erroneous error message to be generated: `serial Id read Operation timed out` This issue has been resolved.	–	–	Y
CR00034411	**TACACS+**	Previously, when periodic TACACS+ accounting was configured, after several days of continuous operation, the erroneous log message "Too many open files" was sometimes generated. This issue has been resolved.	Y	Y	Y
CR00034605	**MLD Snooping**	Previously, when MLD snooping was globally disabled and an interface also had MLD snooping disabled, the **running config** and **show ipv6 mld interface** commands still displayed this interface as enabled. This issue has been resolved.	Y	Y	Y
CR00034667	**Port Authentication**	Previously, the web-authentication interface displayed the year as '2010'. This has been updated to '2011'.	Y	Y	Y
CR00033950	**ETH**	Previously, the output from the **show arp** command did not display ARP information for the eth0 management interface. This issue has been resolved.	Y	–	–

Issues Resolved in 5.4.1-2.8

The following issues were resolved in this release.

Level 1

No level 1 issues.

Level 2

CR	Module	Description	x900/x908	x600	x610
CR00033959	**VCStack ARP**	Previously, in a VCStack, if a station movement occurred on a backup member, the ARP entries were not always flushed. This issue has been resolved.	Y	Y	Y
CR00034196	**IGMP**	Previously, IGMP packets could have been lost or delayed in heavy traffic to the CPU. This issue has been resolved. Internal processing of IGMP messages has been enhanced to ensure there is no risk of IGMP processing delays under high software traffic conditions.	–	–	Y

Level 3

CR	Module	Description	x900/x908	x600	x610
CR00033768	**OSPFv2**	Previously, NSSA LSAs failed to be translated to AS-External LSAs and be propagated to the backbone. This occurred when NSSA LSAs were advertised by advertising the router together with the router-LSA of the advertising router before SPF calculation for the NSSA area in the ABR took place. This issue has been resolved.	Y	Y	Y

CR	Module	Description	x900/x908	x600	x610
CR00033775	**OSPFv3**	During a certain sequence of events— including when a link between neighbouring OSPF routers became active, routes advertised via an intra-prefix-LSA may have failed to be added to the routing table. This issue has been resolved as follows: When the intra-prefix-LSA ages out (maxaged), SPF is recalculated as specified in RFC 5340, Section 4.5.3, which states: "When an LSA's contents have been changed, the following parts of the routing table must be recalculated based on the LSA's LS type: Router-LSAs, Network-LSAs, Intra-Area-Prefix-LSAs, and Link-LSAs - The entire routing table is recalculated, starting with the shortest-path calculation for each area" Recalculating the SPF will make sure that the newer (but higher cost) LSA will be promoted and selected as a path (hence the route is added to the routing table).	Y	Y	Y
CR00033874	**VLAN**	If a dynamic IGMP group was received on a private VLAN host port, an IGMP HW table entry may not have been created. This resulted in unnecessary flooding of the multicast stream. This issue has been resolved.	Y	Y	Y
CR00033041	**VCStack**	Previously, if a **no channel-group** or **no static-channel-group** command was entered, and rapidly followed by a command that created the same channel-group, an error would be output indicating that the previous deletion was still in progress. This error could result in synchronization problems on stacked systems. This issue has been resolved.	Y	Y	Y
CR00033836	**SFlow**	Using sflow on x900/x908 devices (on 5.4.1) would over time result in loss of IP connectivity, system reboots and duplicate master states in stacks. The associated log messages are: ■ 2011 Aug 31 10:21:07 kern.warning H002_SVHUB01 kernel: dst cache overflow ■ 2011 Aug 31 10:21:05 user.err H002_SVHUB01 SFLOWD[1287]: sfl_agent_sysError: receiver: socket sendto error (errno = 105 - No buffer space available) This issue has been resolved.	Y	–	–
CR00034261	**OSPF VCStack**	Previously, the OSPF graceful restart process may not have closed properly during a topology change in an non-redundant VCStack topology setup. This could lead to unnecessary delays in synchronizing LSA tables with neighbours. This issue has been resolved.	Y	Y	Y
CR00034281	**ARP**	On rare occasions when a high number of received ARP messages were being processed, it was possible for some ARP entries to fail to be written to HW tables, resulting in unnecessary traffic handling in software. This issue has been resolved.	Y	Y	Y
CR00033348	**VRF-Lite**	Previously, when a VLAN interface was deleted, the static VRF route which used that interface as a gateway was not deleted. This issue has been resolved.	Y	Y	Y

CR	Module	Description	x900/x908	x600	x610
CR00033350	BGPv4	The configured BGP **maximum-prefix** was missing from the running config, although it was displayed correctly in the **show bgp neighbor** command output. This prevented the command from being saved if entered into the CLI dynamically. This issue has been resolved.	Y	Y	Y

Level 4

CR	Module	Description	x900/x908	x600	x610
CR00033939	VCStack	Previously, when a VCStack backup member was powered off, the stack link port down notification may not have been generated. This issue has been resolved.	Y	Y	Y
CR00033947	NTP	Previously, when an IPv6 address was configured as an NTP source master, then the **show ntp status** command would display the NTP reference as an IPv4 address. This issue is resolved. The command now displays the actual IPv6 address used by the NTP source.	Y	Y	Y
CR00034221	System	The following erroneous bootup log message is no longer generated: `kernel: of:fsl-pq_mdio: probe of ffe24520.mdio failed with error -16`	–	–	Y
CR00033888	System	When a 250W PSU was used in a RPS connected to the x610 PoE switch, which also had an 800W PSU installed, the fault LED would flash although the PSU combination is valid for some situations. This issue has been resolved.	–	–	Y
CR00032670	Log EPSR	Previously, an EPSR "Complete' log message failed to be logged, even though EPSR ring topology had been established. This issue has been resolved.	Y	Y	Y
CR00034083	VCStack	Previously, when a four-unit stack was powered up there was a chance that an erroneous log message— **Unable to start job** was generated. This issue has been resolved.	–	Y	Y

Issues Resolved in 5.4.1-2.7

The following issues were resolved in this release.

Level 1

No level 1 issues.

Level 2

CR	Module	Description	x900/x908	x600	x610
CR00033869	**System**	Excessive amounts of system generated environmental events (such as high rates of fan failure messages, temperature over alarms etc.) could result in inefficient memory usage, which on rare occasions could eventually result in a system reboot. This issue has been resolved.	Y	Y	Y
CR00033820	**QOS**	Applying Policy Based Routing (PBR) policy-maps to a large number of ports at once via a port range could result in a system reboot. This issue has been resolved.	Y	Y	Y
CR00033891	**Swi**	Previously, if a stack of x600 or x610 series switches was forwarding a large number of L3 multicast streams, and a stack failure occured, thereafter the stack would stop forwarding a small subset of the streams. This issue has been resolved.	–	Y	Y

Level 3

CR	Module	Description	x900/x908	x600	x610
CR00033812	**VCStack**	Previously if login accounting was enabled, then remote-login to a backup member could fail. This issue has been resolved.	Y	Y	Y
CR00034080	**OSPFv2**	Previously, OSPF neighbour stability could be impacted when a device recieved a heavy continuous load of non IP multicast traffic that was processed in software . This issue has been resolved.	-	Y	Y

Level 4

No level 4 issues.

Issues Resolved in 5.4.1-2.6

Level 1

No level 1 issues.

Level 2

CR	Module	Description
CR00032436	**VCStack**	When a continuous reboot was detected, and the required action was linkdown, the action to disable eth0 interface could fail. This issue has been resolved.
CR00032749	**IGMP**	Previously, IGMPv2 reports from a downstream interface could sometimes fail to be proxied across an IGMPv3 upstream proxy interface. This issue has been resolved.
CR00032931	**VLAN**	Previously, in a VCStack, if a master failover occurred with private VLAN functionality configured, it could cause the new master to also failover. This issue has been resolved.
CR00032939	**VCStack**	Previously, if a stack member joined a stack and then left the stack within 10secs of joining, then the stack would not let any more stack members join. This issue has been resolved.
CR00033253	**RADIUS**	If the loopback interface was specified as the source interface for RADIUS packets using the command **ip radius source-interface lo**, and login was configured for RADIUS authentication, then a user's login attempt was only checked against the switch's local user database - it did not send the request to the RADIUS Server. Accounting information was also not sent to the RADIUS Server. This issue has been resolved. Now, when the loopback interface is set as the RADIUS source interface using the command **ip radius source-interface lo**, AW+ switches use the first assigned loopback interface address.

CR	Module	Description
CR00033275	**IGMP VCS**	Previously, existing multicast clients on backup members of a VCstack would fail to receive multicast data when other clients or a router was detected on ports of the stack master. This was because multicast entries on the VCS backup member were not being re added/updated properly when the port membership for a particular entry changed. This issue has been resolved.
CR00033289	**PIM-DM v4**	Previously, multicast traffic could be lost when many multicast clients and multiple PIM-DM devices shared the same VLAN. This issue has been resolved.
CR00033295	**VCStack**	When a VCS Master and backup member(s) were rebooted at the same time, VCS may have failed to reform and a VCS sync timeout occurred. When this occurred, the following log message could be displayed when the startup configuration was loading: *HSL[1124]: Internal error: VCS sync timeout for lock-step operation* However, this problem would not have had any significant impact on network traffic or on the VCS operation. This issue has been resolved.
CR00033313	**VCStack**	**x600 stack:** Previously, when a late-joined backup member later became a new master on a x600 stack, OSPF routes were not being fully synchronised to all backup members. This issue has been resolved.
CR00033334	**IPv6 ICMP**	**x900/SBx908:** If any of XEM-2XP, XEM-2XT, or XEM-2XS XEMs were combined with any of XEM-1XP, XEM-12T, or XEM-12S XEMs installed into x900/SBx908 switches, then certain ICMPv6 requests could solicit 2 replies. This has now been resolved so that only 1 reply is generated.
CR00033370	**VCStack**	If a stack was receiving a large amount of traffic that had to be learned while another stack member joined, then it was possible for the port information to be out of sync across the stack members for an unnecessary period of time, before synchonizing. Now the ports are kept consistent across the stack without delay. This issue has been resolved.

CR	Module	Description
CR00033384	Port Auth	**x600 stack:** Previously, with many L2 entries changing and stack members joining/leaving the stack, it was possible for an internal race condition to lead to a system reboot. This issue has been resolved.
CR00033410	VCStack	Using x600 (4-stacked) device, filled up with ACLs and running IXIA stream (MAC Addresses), there is a critical process failure occur after performing master failover. This issue has been resolved.
CR00033518	BGPv4	BGP could fail if an RD was configured in the default VRF, and the same RD was then configured in a VRF instance. This issue has been resolved.
CR00033528	ACL	**x900/SBx908:** When access-lists were applied to a XEM-2XT, XEM2XP, or XEM-2XS as a global rule, sometimes the rule wouldn't match, whereas it would match when applied directly to a port. This issue has been resolved.
CR00033599	Pluggable Transceivers	If hardware errors were detected with SFP+ modules, the error message was only logged on the local stack member. This issue has been resolved. Now the message is logged to all stack members.
CR00033640	Swi	Previously, after hotswapping a XEM in a VCStack environment, MACs learnt on that XEM were being aged out by VCStack members that the XEM was not in. This could result in unnecessary flooding of traffic. This issue has been resolved.

Level 3

CR	Module	Description
CR00031232	QoS	Previously, in QoS class maps, the match tcp-flags rule was only matching on 5 out of the 6 TCP flags (PSH was missing). This issue has been resolved. QoS class-maps now match on PSH TCP flags.

CR	Module	Description
CR00031297	**SNMP**	Previously, the following SNMP MIB counters from the dot3Stats Table (OID (1.3.6.1.2.1.10.7.2.1) did not reflect the CLI port counter output: ■ dot3StatsAlignmentErrors ■ dot3StatsSingleCollisionFrames ■ dot3StatsDeferredTransmissions ■ dot3StatsSymbolErrors ■ dot3StatsCarrierSenseErrors This issue has been resolved.
CR00031482	**VLAN**	If a switch port was associated with a private vlan (PVLAN), and if a user changed the VLAN ID associated with the switch port, the switch port moved to the new VLAN ID without first warning the user that the port needed to be removed from the PVLAN first. This issue has been resolved, by rejecting the invalid command with a message, to ensure the user first removes the port from the PVLAN.
CR00032400	**Trigger**	Previously, if two event triggers were used to send email notifications and the triggers were executed at the same time, one email would be duplicated (sent twice) and the other lost. This issue has been resolved.
CR00032445	**OSPFv3**	Previously if an OSPFv3 process was set with an ABR type of 'ibm', the OSPFv3 **show running configuration** command output would display the ABR type for the OSPFv3 process inappropriately. This was only an output display issue and did not affect operation of the OSPFv3 process. This issue has been resolved.
CR00032861	**RMON**	On rare occasions, dynamically removing existing RMON alarm monitoring could result in a system reboot. This issue has been resolved.
CR00032863	**SNMP**	Entering a single character for the SNMP user encrypted password caused a system restart. This issue has been resolved.
CR00033100	**PIM-SMv4**	Under certain circumstances - such as when a second client joins to the same (S,G) multicast stream as an existing client, but the second client joins on a different VLAN, the multicast HW table entry created by PIM-SM was not always being updated properly, resulting in the multicast stream failing to be delivered on some occasions. This issue has been resolved.

CR	Module	Description
CR00033168	**VCStack**	**x600:** Previously, when a stack of x600s was learning a lot of new MAC addresses, the speed of processing port up/down events was reduced. This issue has been resolved.
CR00033310	**Ping Polling**	When deactivating or removing ping polls via a script (not via the command line), some ping poll counters were still visible in the output of **show counter ping-poll**, and the ping polling daemon stopped sending pings for any remaining ping polls. This issue has been resolved.
CR00033333	**RADIUS**	Previously it was possible for a user to configure a service like RADIUS or SSH to use a TCP or UDP port that was in use by another protocol. This issue has been resolved.
CR00033458	**SNMP MIB Support**	Previously, when a new VRRP master was elected, an SNMP trap was sent containing an incorrect OID. This issue has been resolved, to ensure the trap contains the correct OID 1.3.6.1.2.1.68.0.1
CR00033459	**LAG Channel Groups**	It was possible for a brief L2 loop on to occur when a stack member joined a VCStack and Cisco **keepalive** messages were being sent in on a link aggregator. This issue has been resolved.
CR00033659	**TACACS+**	Previously, configuring a TACACS+ key greater than 64 characters, could result in the existing global key being deleted. This issue has been resolved.
CR00033704	**SSH**	Previously, if the internal SSH/telnet server listen port was changed to a non default port number for incoming management connections, then the internal ssh/telnet client would attempt to use the same non-default port number for outgoing connections, instead of using the default port number. This issue has been resolved.
CR00033722	**Mirroring**	Previously, if a port was configured as a mirror port and default VLAN 1 was removed from that same port, a system reboot could occur. This issue has been resolved.
CR00033739	**Ping Polling**	Adding and removing/deactivating 12 or more ping-polls resulted in a failure of the ping-poll mechanism, and each iteration of adding a previously removed ping-poll resulted a small amount of unnecessary memory usage. These issues has been resolved.
CR00033827	**User Management**	Usernames starting with the unsupported '#' character are now deprecated.

Level 4

CR	Module	Description
CR00032375	Logging	An error message was appearing in the log after the **boot system** command was run, even though the command succeeded. This issue has been resolved. The erroneous log message no longer appears.

Issues Resolved in 5.4.1-1.5

Level 1

No level 1 issues.

Level 2

CR	Module	Description
CR00032706	IGMP Snooping	Previously when an unexpected dynamic IGMP multicast group entry, equal to an existing static entry, was received at a port, then after 260 seconds the static entry was removed when the dynamic entry aged out. This prevented multicast traffic from being forwarded to the port. This issue has been resolved.
CR00032920	Authentication	Previously, the “Authenticated” web page failed to open when web authentication and a guest-vlan were used together. This issue has been resolved.

Level 3

CR	Module	Description
CR00032676	OSPFv3	Previously, when OSPFv3 executed a graceful restart, it could sometimes fail to re- advertise the connected routes for non-OSPF interfaces. This issue has been resolved.
CR00032782	L2 switching	On rare occasions with x600 VCS, some MAC authentication attempts could fail when many hundreds of MAC addresses were learned and authenticated simultaneously. This issue has been resolved.

CR	Module	Description
CR00032422	OSPFv3	Previously, when an OSPFv3 interface was created over an IPv6 interface which was still in the DOWN state, when the IPv6 interface changed state to UP, the OSPFv3 interface sometimes did not activate properly. This issue has been resolved.
CR00032532	VLAN	The behavior of the command **switchport trunk allowed vlan except** has been enhanced to allow for the future creation of VLANs. The previous implementation added all current VLANs to the port except for the list passed in by the above command. However, when a new VLAN was created it was not automatically added to this port. This issue has been resolved, so that appropriate future VLANs will be automatically added to the port.
CR00032539	IGMP Report	An IGMPv3 to_ex{} and to_ex{s1...} packets were not recognized as joins, when a multicast group was operating in V2 compatibility mode. This issue has been resolved.
CR00032630	Authentication	On rare occasions a system restart could occur when an excessively long hostname was configured for the RADIUS-server or TACACS-server commands. This issue has been resolved.
CR00032752	OSPF	Previously, an OSPF graceful restart in a non-fully redundant topology (i.e. master and backup member(s) were not necessarily connected to all interfaces in LAGs) and connected to the neighboring routers via Layer 2 switches, could fail to detect topology change(s) during a master failover. This caused a late graceful restart exit by the graceful restart process **timeout** mechanism, which ultimately resulted in the routing table not being updated in a timely manner (up to 120 seconds delay). This issue has been resolved.
CR00033014	Switch	Previously, the **storm-control** command would fail when applied to a port that was down. This issue has been resolved.
CR00033258	Pluggable Transceivers	x600-48 only. Previously, ports connected to a copper SFP would not go **link-down** when the unit was restarted. This issue has been resolved.

CR	Module	Description
CR00033296	Switch	Previously, when multiple silent Layer 2 station MAC movements from one switch port to another occurred in a VCStack environment, it was possible for some station movements to be ignored, resulting in entries timing out. This issue has been resolved.
CR00031457	SSH	Previously, if the TCP port specified via the command **ssh server <TCPport>** was already in use by another protocol, the command was always accepted. This issue has been resolved. The command is now only accepted when the TCP port specified is not already in use by another protocol.

Level 4

CR	Module	Description
CR00032534	Ping-poll	Previously, if the command **show counter ping-poll** was used in a configuration involving more than 12 ping-poll instances, then the counters for instances beyond the 12th did not always display correctly. This issue has been resolved.
CR00033278	SNMP	The following SNMP enterprise MIB files have been updated to prevent erroneous log messages: ■ at-filev2.mib ■ at-sysinfo.mib ■ at-setup.mib

Issues Resolved in 5.4.1-1.4

Level 1

No level 1 issues.

Level 2

CR	Module	Description
CR00032742	Core	Previously, when the command **switchport trunk allowed vlan all** or **switchport trunk allowed vlan none** was issued in port interface configuration mode, a core module restart could occur. This issue has been resolved.

CR	Module	Description
CR00032760	SSH	Previously, SFTP connections were not being established correctly due to the way non-interactive shell sessions were internally handled. This issue has been resolved.

Level 3

CR	Module	Description
CR00032408	OSPFv2 VCStack	Previously, if a failover occurred in a VCStack using OSPFv2, the implicit grace-LSA-ACKs from the designated router could sometimes cause the restarting router to resend grace-LSAs needlessly. This issue has been resolved.
CR00032400	Trigger	Previously, if two event triggers were used to send email notifications and the triggers were executed at the same time, one email would be duplicated (sent twice) and the other lost. This issue has been resolved.
CR00032676	OSPFv3	Previously, when an OSPFv3 device executed a graceful restart, it could sometimes fail to re advertise the connected routes for non-OSPF interfaces. This issue has been resolved.
CR00032782	L2 switching	On rare occasions with a x600 VCS, sometimes MAC authentication could fail when many hundreds of MAC addresses were learnt and authenticated simultaneously. This issue has been resolved.

Level 4

No level 4 issues.

Issues Resolved in 5.4.1-1.3

Level 1

No level 1 issues.

Level 2

CR	Module	Description
CR00030509	**LACP**	Previously, if ports in trunk mode were members of an LACP aggregator and port configuration included the command: `switchport trunk allowed vlan all` then if a new VLAN was created, it was possible that the LACP link could sometimes go down briefly, resulting in a short traffic interruption. This issue has been resolved.
CR00031840	**VCStack**	Previously, after the VCStack master with a large configuration file failed-over (restarted) multiple times in quick succession, it could eventually fail to start up correctly. This issue has been resolved.

CR	Module	Description
CR00032208	**OSPFv2** **OSPFv3**	Previously: ■ With OSPF Graceful enabled, if a VCStack failover occurred while running OSPF, the new Stack Master sometimes failed to advertise correct external-summary-LSAs to its neighbours causing the neighbours to lose some routes and be unable to forward traffic. ■ In the rare event of an SPF calculation being scheduled to happen during a suspended ASExternal calculation, the SPF calculation could fail to execute - resulting in loss of routes associated with the SPF calculation being added to the IP route table. ■ OSPF neighbours failed to establish a full OSPF neighbour adjacency during a graceful restart on non-stacking units if both neighbours were restarted together. In this situation, both devices transitioned to a DROther state. This situation has been resolved, and DR/BDR election will now occur resulting in full neighbour relationships being established. ■ If a stack running OSPF was also connected to more than one OSPF area, for example, area 0.0.0.0 and area 0.0.0.3, and if there were two OSPF interfaces connected to area 0.0.0.3 (one connection via the current master, and one connection via the current backup member), then when failover occurred, i.e. the master went down and stayed down - effectively bringing down the only OSPF interface to area 0.0.0.3 via the former master. Then sometimes the summary-LSA for the down interface remained in the OSPF route table of the stack member and other neighbours in the backbone area. These previous OSPFv2 software improvements have now been applied to OSPFv3.
CR00032209	**OSPFv3**	Previously, after a graceful restart, OSPFv3 sometimes incorrectly advertised an AS-external LSA containing OSPF IPv6 interface routes. This issue has been resolved.
CR00032383	**IPv4** **VRF-lite**	Previously, when a route was configured and selected in a VRF and the nexthop was resolved recursively with other routes, the prefix was not able to be removed from the FIB in certain cases, which could cause network disruption. This issue has been resolved.
CR00032384	**VRRP** **VRF-lite**	Previously, when multiple VRRP routers were configured in two or more VRFs, then ARP Requests from some VRRP interfaces were not handled correctly. This issue has been resolved.

CR	Module	Description
CR00032562	**802.1x**	Previously, occasionally, an x600 VCStack under high system load could cause auth-mac supplicants to lose communication with the network. This issue has been resolved.
CR00032614	**TACACS+**	Previously, TACACS+ authentication requests were sometimes sent with incorrect service type and session ID. This issue has been resolved—the TACACS+ authentication requests now use the correct service type and session ID requests.
CR00032653	**DHCPv4 relay**	Previously, issuing the command: `shutdown` for a VLAN interface sometimes resulted in DHCP relay failure. This issue has been resolved.
CR00032659	**VRRP**	Previously, the command: `show vrrp brief` sometimes resulted in a system reboot. This issue has been resolved.
CR00032699	**ARP** **VRF-Lite**	Previously, when a static ARP entry for a VRF instance was created, it was not added to the running config with the associated vrf_name, although the ARP table entry remained correct. This issue has been resolved.
CR00032177	**ARP**	Previously, when an arp-ageing-timeout was configured this was not obeyed the first time an ARP entry was learned, also stale ARP entries could be retained for up to 5 minutes even when the arp-ageing-timeout was configured. Also, when L3 traffic was interrupted and restarted via a different port, traffic would not resume immediately under some circumstances. These issues have been resolved.

Level 3

CR	Module	Description
CR00030448	**DHCP snooping, QoS, VCStack**	Previously, in some circumstances, DHCP snooping filters for IP source binding were not applied via QoS to ports on x600 VCStack backup members. This could result in blocked traffic. This issue has been resolved—DHCP snooping filters are now correctly applied to all the ports on all the stack members.

CR	Module	Description

CR00031010	**MLD**	Previously, the IPv6 SSM-mapping commands were documented and included in the CLI, but were unsupported. These commands have now been removed from the CLI:
		`ipv6 mld ssm-map enable`
		`ipv6 mld ssm-map static`
		`ipv6 mld static-group <ipv6-group-address> [source <ipv6-source-address>|ssm-map] [interface <port>]`

CR00031394	**QoS**	Previously, repeatedly adding and removing policy maps to or from an interface many times could eventually lead to a low level memory leak. This issue has been resolved.
CR00032042	**VCStack**	During the transition to Disabled Master, it was possible for FDB lookups to fail for a brief period, resulting in corresponding error messages in the log. This issue has been resolved.
CR00032410	**VLAN** **VCStack**	Previously, in a VCStack, if a master failover occurred then some private VLAN settings associated with aggregators were not being replayed into the configuration correctly. This issue has been resolved.
CR00032423	**SNMP MIB**	The SNMP manager revision history in the AT-Boards enterprise MIB file was not ordered correctly in strict accordance with SNMP standards. This issue may have prevented SNMP management stations from compiling the AT-Boards enterprise MIB file. This issue has been resolved
CR00032482	**QoS**	x600 only. Previously, when creating a single-rate or twin-rate policer, the running config would display the value entered in the CLI, but not the actual nearest rounded value used in HW. This issue has been resolved to ensure the CLI now displays the same value used in HW.
CR00032484	**PoE**	x600-POE+ only. Devices now conform to the 802.3af specification. This means that if PoE ports are in an over-current condition during classification, the POE+ (type 2) PSE units will not supply power to external powered devices attached to these PoE switch ports.

CR	Module	Description
CR00032500	**VRF-Lite**	Previously, it was possible to create static inter-VRF routes using the command: `ip route vrf <vrf-name> <subnet&mask> <interface>` even though static inter-VRF routes had been disabled via the non default **no ip route static inter-vrf** command. This issue has been resolved—attempting to create a static inter-VRF route using this command will now fail if static inter-VRF routes have been disabled.
CR00032505	**VRF-Lite**	When static inter-VRF routes were removed by command, ARP entries associated with the static route were not always removed correctly if a similar ARP entry with the same next-hop existed in a different VRF instance. This issue has been resolved.
CR00032526	**Ping**	Previously, the **clear ping-poll** command was not clearing the ping-poll counters correctly. This issue has been resolved.

Level 4

CR	Module	Description
CR00032405	**VLAN**	Previously, on rare occasions, enabling a disabled VLAN could sometimes result in an incorrect VLAN status. This issue has been resolved.
CR00032452	**OSPFv3**	Previously, the value '0' (zero) was displayed as the default IPv6 OSPF restart grace period when the command **show ipv6 ospf** was issued. This has been changed so that the output correctly reflects the current **default** grace period of 120 seconds.

CR00032530	**OSPFv3**	A spelling mistake in the output of the **show ipv6 ospf** command has been corrected. The previous output line:
		`Number of incomming current DD exchange neighbors`
		now reads:
		`Number of incoming current DD exchange neighbors`