AlliedWare Plus Software Maintenance Release Note

Software Version 5.4.3-3.17 For SwitchBlade x8100, SwitchBlade x908, x900, x610, IX5, x510 and x210 Series Switches

Introduction

This document lists the issues addressed and enhancements in AlliedWare Plus software maintenance version 5.4.3-3.17. This document applies to the following switches:

Models	Series	Release File	Date	GUI file
x210 -9GT x210-16GT x210-24GT	x210	x210-5.4.3-3.17.rel	Jul 2015	x210-gui_543_05.jar
IX5-28GPX		IX5-5.4.3-3.17.rel	Jul 2015	x510-gui_543_16.jar
x510-28GTX x510-28GPX x510-28GSX x510-52GTX x510-52GPX x510DP-52GTX	x510	x510-5.4.3-3.17.rel	Jul 2015	x510-gui_543_16.jar
x610-24Ts x610-24Ts-POE+ x610-24Ts/X x610-24Ts/X-POE+ x610-24SPs/X x610-48Ts x610-48Ts-POE+ x610-48Ts/X x610-48Ts/X-POE+	x610	x610-5.4.3-3.17.rel	Jul 2015	x610-gui_543_11.jar
x900-12XT/S, x900-24, x900-12XT/S, x900-24XT, x900-24XT-N, x900-24XS	x900	x900-5.4.3-3.17.rel	Jul 2015	x900-gui_543_13.jar
SwitchBlade x908	SBx908	SBx908-5.4.3-3.17.rel	Jul 2015	x900-gui_543_13.jar
SwitchBlade x8106 SwitchBlade x8112	SBx8100	SBx81CFC400-5.4.3-3.17.rel	Jul 2015	SBx81CFC400_gui_543_14.jar

Contents

Installing the GUI to your Switch using an SD Card or USB Device

1. **Download a GUI Java applet.**

   The GUI Java applet file is available in a compressed (zip) file with the AlliedWare Plus Operating System software from the Software Download area of the Allied Telesis Website: http://www.alliedtelesis.com/support/software/restricted. Log in using your assigned Email Address and Password. Download the Java applet file. This file will have a `.zip` file name extension. You need to extract the Java `.jar` file from the compressed `.zip` file. The version number of the software applet file (`.jar`) gives the earliest version of the software file (`.rel`) that the GUI can operate with.

2. **Copy the GUI Java applet .jar file to an SD card or USB storage device.**

   Insert the SD card in the SD slot on the front of your switch or the USB device into the USB port on the switch. Connect to the management port, then login to the switch.

   Copy the GUI Java applet to your switch, using the below commands:

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

   or

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

   Where `<filename.jar>` is the GUI Java applet file you downloaded in Step 1.

Note: Where the GUI file is not in the root directory of the USB flash drive, you must enter the full path to the GUI file. For example, where the GUI file resided in the folder gui_files, you would enter the command: copy usb:/gui_files/filename.jar flash:/

3. **Assign IP addresses.**

   Use the following commands to assign the IP addresses for connecting to the Java applet.

   ```
   awplus# configure terminal

   awplus(config)# interface vlan1

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

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

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

4. **Configure the gateway.**

   Configure your switch with a default gateway, if necessary, using these commands:

   ```
   awplus(config-if)# exit

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

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

5. **Create a user account.**

   In order to log into the GUI, you must first create a user account. Use these commands to setup a user account:

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

   Note that you can create multiple users to log into the GUI. See the AlliedWare Plus Software Reference for information about the **username** command.

6. **Ensure HTTP service is enabled.**

   The HTTP service needs to be enabled on the switch before it accepts connections from a web browser. The HTTP service is enabled by default. However, if the HTTP service has been disabled, you must enable the HTTP service again. If the HTTP service is disabled, use the following command to enable it:

   ```
   awplus(config)# service http
   ```

   See the *AlliedWare Plus Software Reference* for information about the **service http** command.

7. **Log into the GUI.**

   Start a browser and enter the IP address you configured in Step 3 as the URL. You will be presented with a login screen after the GUI Java applet has started. Log in with the username and password that you defined in the earlier step, named **Create a user account.**

Note: Any configuration changes should be saved to ensure the device settings are retained.

Installing the GUI to your Switch via TFTP Server

1. **Download a GUI Java applet file from the support site.**

   The GUI Java applet file is available in a compressed (`.zip`) file with the AlliedWare Plus Operating System software from the Support area of the Allied Telesis Website: http://www.alliedtelesis.com. Download the Java applet file. This file will have a `.zip` file name extension. You need to extract the Java `.jar` file from the compressed `.zip` file. The version number of the software applet file (.jar) gives the earliest version of the software file (`.rel`) that the GUI can operate with.

2. **Copy the GUI applet.**

   Copy the GUI applet .jar file onto a TFTP server. Ensure this TFTP server is enabled and ready for the switch. Connect to the management port of the switch, then login to the switch. Do not connect to the management port of the TFTP server

3. **Assign the IP addresses.**

   Use the following commands to configure your switch with an appropriate IP address:

   ```
   awplus# configure terminal
   awplus(config)# interface vlan1
   awplus(config-if)# ip address 192.168.2.6/24
   ```

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

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

   Use the following commands to configure your switch with a default gateway:

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

4. **Configure the default gateway.**

   In necessary, use the following commands to configure the default gateway.

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

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

5. **Copy the GUI Java applet to your switch.**

   Use the following commands to copy the GUI Java applet to your switch:

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

   Where *<server-address>* is the IP address for the TFTP server, and where *<filename.jar>* is the GUI Java applet file you downloaded in Step 1.

6. Create a user account.

In order to log into the GUI, you must first create a user account. Use the following commands to setup a user account.

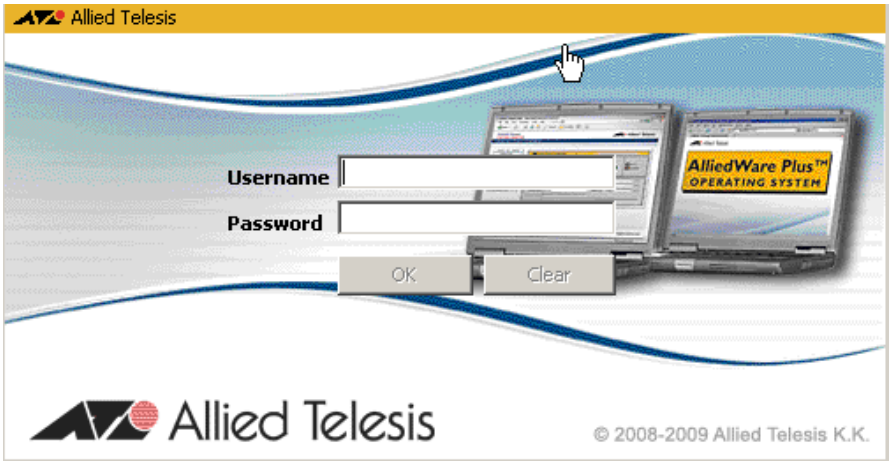
```
awplus(config)# username <username> privilege 15 password
    <password>

awplus(config)# exit
```

Note that you can create multiple users to log into the GUI. See the AlliedWare Plus Software Reference for information about the `username` command.

7. Log into the GUI.

Start a browser then enter the IP address you configured in Step 3 as the URL. You will then be presented with a login screen after the GUI Java applet has started. You can then Log in with the username and password that you defined previously in Step 6.



Note: Any configuration changes should be saved to ensure the device settings are retained.

For more information please refer to the 5.4.3 *Software Reference* available from the Support area of the Allied Telesis Website: *http://www.alliedtelesis.com/support*

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:

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 x210 Series switches, use the command:

   ```
   awplus(config)#boot system x210-5.4.3-3.17.rel
   ```

   On the x510 Series switches, use the command:

   ```
   awplus(config)#boot system x510-5.4.3-3.17.rel
   ```

   On the IX5-28GPX switch, use the command:

   ```
   awplus(config)#boot system ix5-5.4.3-3.17.rel
   ```

   On the x610 Series switches, use the command:

   ```
   awplus(config)#boot system x610-5.4.3-3.17.rel
   ```

   On the x900 Series switches, use the command:

   ```
   awplus(config)#boot system x900-5.4.3-3.17.rel
   ```

   On the SwitchBlade x908, use the command:

   ```
   awplus(config)#boot system SBx908-5.4.3-3.17.rel
   ```

   On the SwitchBlade x8100 Series switches, use the command:

   ```
   awplus(config)#boot system SBx81CFC400-5.4.3-3.17.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 Hardware Supported from 5.4.3-3.7

The following new hardware is supported by this software version:

IX5-28GPX High Availability Video Surveillance Switch

The Allied Telesis IX5-28GPX offers an impressive set of features in a high-value package, ideal for IP video surveillance environments.

IX5-28GPX

The IX5-28GPX is a high performing and scalable solution for today's networks. With 24 PoE+ enabled 10/100/1000Mbps ports, two 1/10 Gigabit uplinks, plus the ability to stack up to four units, the AT-IX5- 28GPX is an ideal solution for video surveillance applications where high performance and resilient PoE power are critical.

- Dual hot-swappable PSUs
- VCStackable up to 4 units
- High performance multicasting
- Up to 30W PoE+ power on every port
- AMF ready
- Supports Energy Efficient Ethernet
- 24 x 10/100/1000T (RJ-45) PoE+ copper ports
- 2 x 1/10 Gb SFP+ ports
- 2 x 10 Gb stacking ports

IX5 rear panel with two AT- PWR800 power supplies installed

x510DP-52GTX Stackable Gigabit Switch

This new member of the x510 Series provides 48 10/100/1000T ports in a stackable switch with 4 SFP+ ports. Two hot-swappable power supplies, with optimal reverse airflow, make it ideal for data center applications.

x510DP-52GTX

The power supplies for the x510DP-52GTX are:

- AT- PWR100R—100W AC system power supply (reverse airflow)
- AT- PWR 250—250W AC system power supply
- AT- PWR 250R—250W DC system power supply (reverse airflow)

SwitchBlade x8106 Next Generation Intelligent Layer 3+ Chassis Switch (6 slot)

This 6-slot chassis switch shares all the same features of AlliedWare Plus and supports the same line and controller cards as the 12-slot SwitchBlade x8112.

SwitchBlade x8106 with two SBx81GTX40 line cards and two SBx81CFC400 controller cards installed.

New Hardware Supported from 5.4.3-2.5

The following new hardware is supported by this software version:

x510-28GSX

AlliedWare Plus 5.4.3-2.5 supports a new model in the x510 Series of switches—like the others, it includes a full range of security and resiliency features, coupled with easy management, making them the ideal choice for network access applications.

The x510-28GSX provides:

- 24 x 100/1000X SFP ports
- 2 x 1/10 Gb SFP+ ports
- 2 x 10 Gb stacking ports—these stacking ports can be configured as additional 10G Ethernet ports when the unit is not stacked
- 128 Gbps switching fabric
- 95.2 Mpps forwarding rate

XEM24T

AlliedWare Plus 5.4.3-2.5 supports the new XEM-24T, providing 24 10/100/1000T copper ports, utilizing the latest RJ point five connectors to double the port density previously available. This expansion module can be installed in:

- x900-12XT/S and x900-24X Series switches
- SwitchBlade x908 in standard and extended silicon profile modes

SBx81GT40

AlliedWare Plus 5.4.3-2.5 supports the new SBx81GT40 40-port Gigabit copper line card, which maximizes port density, utilizing the latest RJ point five connectors. SwitchBlade x8112 can now provide up to 400 Gigabit copper ports in a single 7RU chassis.

x210 Series switches

AlliedWare Plus supports the x210 Series switches from version 5.4.3-1.4. The x210 Series is a reliable and value-packed solution for today's networks. With a choice of 9-, 16- and 24-port versions, each with one or more SFP uplinks, the x210 Series switches are ideal for applications at the edge of the network where security and manageability are the key requirements.

- x210-9GT—8 10/100/1000T (RJ45) copper ports, 1 100/1000X SFP port, 24GPS switching fabric
- x210-16GT—14 10/100/1000T copper ports, 4 SFP and 10/100/1000T combo ports, 36GPS switching fabric
- x210-24GT——20 10/100/1000T copper ports, 2 SFP and 10/100/1000T combo ports, 48GPS switching fabric

For information about the software features on these switches and how to configure them, see the *Software Reference for x210 Series Switches, AlliedWare Plus™ Operating System Version 5.4.3*, available from:

http://www.alliedtelesis.com/support/documentation_keyword_x210.aspx

Support for secure USB storage devices

x510 Series, SwitchBlade x8112. USB storage devices used as backup memory can be easily pulled out of a switch. You can use Secure USB storage devices to protect this data in the event that it is mislaid or in unauthorised hands. Secure USB devices provide password (PIN)-protected encryption to the data they store.

Note that if the switch reboots, the Secure USB key will be locked. After a VCStack failover, when a stack member recovers, the Secure USB device cannot be accessed until it is unlocked.

Features and Enhancements in 5.4.3-3.17

This version includes the following enhancement:

CR	Module	Description
ER-554	**Aggregation - LACP, Aggregation - Static**	**x510 only Enhancement**: With this software update, the hashing algorithm used to decide which port of an aggregation a packet should be sent to, has been reverted to the algorithm that was used in previous releases, unless the **platform load-balance** command is used.

Features and Enhancements in 5.4.3-3.16

This version includes the following enhancement:

CR	Module	Description
CR00042594	**Link Aggregation**	x510 only. This update adds more command parameter options that are used in the hash calculation for load balancing across LAGs. In particular, the additional options now allow ethertype and L4 ports to be turned on/off independently of each other, in addition to the existing options of using IP and MAC addresses for hash calculations. `platform load-balancing ({src-st-mac|src-dst-ip|`**`src-dst-port`**`|`**`ethertype`**`}`

Features and Enhancements in 5.4.3-3.13

This version includes the following enhancements:

CR	Module	Description
CR00041773	**SNMP**	Previously, the link up/down trap defined in RFC1157 included the interface ifindex in the trap, but it was not user-friendly for the user to figure out, from the iFIndex, which port the trap pertained to. To make it more user friendly, a new Allied Telesis Enterprise MIB has been created with MIB oid: 1.3.6.1.4.1.207.8.4.4.3.25. This new atSnmpTrap MIB, includes only 2 MIB variables: atLinkDown and atLinkUp. The information included in each of the traps is: ifIndex, ifAdminStatus, ifOperStatus, ifName (extra info from the standard link up/down trap).
CR00042228	**LDF**	With this update, the following command has been added for preventing ports from being blocked by LDF. `loop-protection loop-detect fast-block` The Default setting is none. (Disabled)
CR00042302	**Monitoring**	The output of the command: `show diagnostic channel-group` has been improved, so that it will now show the overall status of the aggregator, as well as the member-ports.

Features and Enhancements in 5.4.3-3.12

This version includes the following enhancements. Unless otherwise stated, these enhancements apply to all products.

Sending specific IGMP queries to member ports only (CR00041636)

IX5, x510, x610, x900, SBx908, and SBx8100 Series switches.

Previously, IGMP specific queries were always flooded to all VLAN member ports. A new enhancement has been added to allow specific queries to be sent only to multicast group member ports. The command description follows.

ip igmp flood specific-query

Syntax

```
ip igmp flood specific-query

no ip igmp flood specific-query
```

Description This command sets IGMP to send IGMP-specific queries to all ports in a VLAN, rather than to only the multicast group member ports.

In a Layer 2 switched network running IGMP, it is considered to be more robust to flood all specific queries. There are scenarios where the benefit of flooding specific queries to all VLAN member ports has been shown to outweigh the disadvantage. However, in certain scenarios, particularly ones involving hosts with very low CPU capability, even receiving specific queries for multicast groups they are not members of is enough to degrade the performance of the hosts.

In this situation, it is desirable for IGMP to be able to send specific queries to known member ports only. This will limit the performance degradation of such hosts to a minimum.

Default The default setting is for specific queries to be flooded to all VLAN member ports.

Mode Global Configuration

Examples To set IGMP to flood specific queries to all VLAN member ports, use the command:

```
awplus(config)# ip igmp flood specific-query
```

To set IGMP to flood specific queries to only multicast group member ports, use the command:

```
awplus(config)# no ip igmp flood specific-query
```

Validation Command show ip igmp interface <*interface-name*>

PoE service power inline configuration retained (CR00041679)

For PoE capable devices, the configuration command **service power-inline** controls whether the PoE service starts up. Prior to this change, if the last PoE capable device left the stack or chassis, the **service power-inline** command and the associated PoE port configuration was removed from the running configuration. After this change, when the last PoE capable device leaves, the **service power-inline** command and the associated PoE port configuration will not be removed as it is likely that the leaving device will rejoin in the future.

The following is a summary of the updated behaviour:

If a system starts with no configuration set and no PoE capable HW is present:

- The PoE service will be not be started.
- The **show running config** command will not display either **service power-inline** or **no service power-inline** as PoE has not been explicitly enabled or disabled.

If a PoE device joins after this point:

- The PoE service will start automatically.
- The **show running config** command will display **service power-inline**.

Once the PoE service has started, it will not be automatically stopped if the PoE capable device leaves the system. If the PoE configuration is no longer required, the user must actively disable PoE using the **no service power-inline** command.

If the **no service power-inline** command exists in the configuration and a PoE capable device joins the system, the PoE service will remain disabled. In this case, if PoE functionality is required, PoE must be enabled using the **service power-inline** configuration command.

IGMP snooping source timeout (CR00040711)

A new feature has been added to set the liveness timer for multicast groups created by unregistered multicast data using the command line.

ip igmp snooping source-timeout

This command sets the global IGMP Snooping source timeout value (in seconds) on a switch. The timeout determines how long an unregistered multicast entry will be kept for before it times out. If the value '0' is specified, then effectively all unregistered multicast entries will never time out, and can only be cleared by the command **clear ip igmp group** command. Use the **no** version of the command to disable global IGMP snooping source-timeout.

Caution: This command does not apply to existing unregistered groups in IGMP. To make existing group entries follow the new source-timeout setting, clear the groups by using the **clear ip igmp group *** command while keeping the data streaming.

Syntax `ip igmp snooping source-timeout <0-86400>`

`no ip igmp snooping source-timeout`

Default Global IGMP Snooping source timeout is disabled, and unregistered multicast will be timed-out like normal entries.

Mode Global Configuration

Usage This command is generally most useful when the source timeout is set to a much larger value than the current IGMP 'Group Membership Interval', which is derived from IGMP 'Query Interval'. Otherwise, the IGMP group will time out as soon as the last member of the group leaves, after the source-timeout expires earlier. This will cause a very brief period of multicast traffic flooding caused by the unregistered multicast learning process, similar to the initial unregistered multicast learning process. If the source timeout is set with the value of 0, the unregistered multicast group will never time out; the only way to delete the multicast groups that never time out is to use the command '**clear ip igmp group** (* | <*multicast-ip-address*>).

The most recently set IGMP snooping source timeout will only be effective for newly learned unregistered multicast groups. Existing unregistered multicast and registered multicast groups will not be affected. To apply new source timeout setting to existing multicast groups, use the command '**clear ip igmp group** (* | <*multicast-ip-address*>)' command to clear the existing groups. When the multicast data for the groups is detected again, the new source timeout setting will be applied.

The following table explains how the global and interface source-timeout interact.

Table 35: Global and interface source-timeout interaction

Global Timeout	Interface Timeout	Effective Timeout
off	off	None
off	on	Interface timeout
on	off	Global timeout
on	on	Interface timeout

Examples To enable IGMP Snooping source timeout on a switch:

```
awplus(config)# ip igmp snooping source-timeout 200
```

Validation Command show ip igmp snooping source-timeout <*interface-name*>

This command displays both the global and interface based IGMP Snooping source timeout settings on a switch.

Output To display the IGMP Snooping source timeout current settings:

```
awplus# sh ip igmp snooping source-timeout
Global IGMP snooping source-timeout is disabled

vlan1           enabled (0 secs)
vlan2           enabled (86400 secs)
vlan1000        disabled
```

Features and Enhancements in 5.4.3-3.10

This version includes the following enhancements:

CR	Module	Description
CR00041176	**Port Configuration**	This update allows the back pressure information to be displayed for x510 and x610 switches. The jam status information is now displayed by the **show platform port** command.

Two-step Authentication (CR00040819)

Support for Two-step Authentication has been added. Two-step Authentication improves security by requiring two forms of authentication. The single step authentication methods (either user or device authentication) have a potential security risk:

- an unauthorized user can access the network with an authorized device, or
- an authorized user can access the network with an unauthorized device

Two-step authentication solves this problem by authenticating both the user and the device. The supplicant will only become authenticated if both these steps are successful. If the first authentication step fails, then the second step is not started. The following authentication sequences are supported for two-step authentication:

- MAC Authentication followed by 802.1X Authentication
- MAC Authentication followed by Web Authentication
- 802.1X Authentication followed by Web Authentication.

To configure two-step authentication:

1. Configure the first authentication method.
2. Configure the second authentication method.
3. Specify the interface command **auth two-step enable**.
4. Make sure that both authentication steps require different authentication credentials.

MAC authentication followed by web authentication Port configuration could be as follows:

```
interface port1.0.1
switchport mode access
 auth-mac enable
 auth-web enable
 auth two-step enable
```

Ensuring All Authentication Methods Require Different Usernames and Passwords

If you configure a user or device to use multiple authentication methods, you need to set up your system to avoid a potential vulnerability.

The vulnerability occurs because there is no way for a RADIUS server to determine what authentication method you are using. Authentication simply queries a RADIUS server to see whether a username/password pair is valid.

This means that if you use the same RADIUS server for multiple authentication methods, a user can enter the *same* username/password pair for each of these authentication methods. If that username/password pair is valid for one of the methods, it will work for all of them.

This vulnerability is particularly significant for MAC authentication, because the default username and password is the MAC address of the supplicant device, which is easy to discover.

For example, if you set up two-step authentication of MAC authentication + 802.1x authentication, and both use the same RADIUS server, then an attacker does not need to know the 801.1x username and password. Instead, they can pass the 802.1x authentication step by entering the device's MAC address into the 802.1x username and password fields.

To avoid this vulnerability:

- Use different RADIUS servers for each authentication method, and/or
- Change the default password for MAC authentication, by using the **auth-mac password** command.

auth-mac password

This command changes the password for MAC-based authentication.

Use the **no** variant of this command to return the password to its default.

Syntax

```
show auth-web-server

no auth-mac password
```

Parameter	Description
`auth-mac`	MAC-Based Authentication
`encrypted`	Specify an encrypted password
`password`	Configure the password
`<password>`	The new password. Passwords can be up to 64 characters in length and can contain any printable characters except: ■ ? ■ "(double quotes) and ■ space

Default By default, the password is the MAC address of the supplicant

Mode Global configuration

Usage Changing the password increases the security of MAC-based authentication, because the default password is easy for an attacker to discover. This is particularly important if:

- some MAC-based supplicants on the network are intelligent devices, such as computers, and/or
- you are using Two-step authentication

Examples To change the password to very SecurePassword, use the commands:

```
awplus# configure terminal

awplus(config)# auth-mac password verySecurePassword
```

Validation Command **show running-config**

Related Commands **auth two-step enable**
show auth-mac

Features and Enhancements in 5.4.3-3.9

This version includes the new enhancement in the following table:

Enhancements

CR	Module	Description
CR00040196	**Flow Control**	Transmit flow control and back pressure are now supported on x510 Series switches.

Features and Enhancements in 5.4.3-3.7

This version includes the new features and enhancements in the following list and table:

- Web-authentication now supports:
  - Web Authorization Proxy (x510 and x610 Series switches)—enables Web Authentication to apply the supplicant's Web Proxy settings.
  - Two-step Authorization MAC and Web (x510 and x610 Series switches)—improves security by authenticating both the device and the user.
  - Web Authentication Timeout Connect (all platforms)—allows the timeout period to be set from 1-65535 seconds.

  For details, see the *Web Authentication Supplement, AlliedWare Plus™ Operating System Version 5.4.3-3.7*, downloadable from alliedtelesis.com/support/documentation_keyword_authentication.aspx.
- DHCP Relay and DNS Relay are now VRF-Lite aware. For details, see the *VRF-Lite Aware DHCP and DNS Relay Supplement for x610, x900, and SwitchBlade® x908 Series Switches, AlliedWare Plus™ Operating System Version 5.4.3-3.7*, downloadable from alliedtelesis.com/support/documentation_keyword_vrf.aspx.

CR	Module	Description
CR00039409	**QoS**	The buffer allocations have been changed on some SBx8100 line cards to give preference to high-priority traffic.
CR00040037	**L2 Switching**	x900, SBx908 Previously, congestion avoidance queuing limits were such that a TCP flow entering via a 10G port and egressing via a 1G port could end up with lower performance than expected. The limit has now been increased, thereby allowing more effective queuing per port. This significantly improves the throughput in the 10G-1G TCP flow.

Features and Enhancements in 5.4.3-2.6

This version includes the enhancements in the following table.

CR	Module	Description
CR00039430	**SNMP**	The switch can now generate a new log message that contains the source IP address when an SNMP request failed and an authenticationFailure trap is sent out.
CR00039536	**Port Authentication**	The maximum number of characters for the username/password that a user can enter for Web-authentication is now increased from 20 to 64.
CR00040037	**L2 Switching**	SBx908 and x900 only. Previously, congestion avoidance queuing limits were such that a TCP flow entering via a 10G port and egressing via a 1G port could end up with lower performance than expected. The limit has now been increased, thereby allowing more effective queuing per port. This significantly improves the throughput in the 10G-1G TCP flow.
CR00040091	**BGPv4**	SBx8100, SBx908, x900, x610, x510 only. The BGP command **neighbor remove-private-AS** is now supported for IPv4. `neighbor <address> remove-private-as` *Note:* For the filtering to apply, both peering devices must use either 2- or extended 4-byte ASN (same ASN type on both peers). For example, if a device (which defaults to use 4-byte ASN) is peered with a device that defaults to 2-byte ASN, then the device using 2-byte ASN also needs to be configured with the command **bgp extended-asn-cap** for the filtering to apply. For more details about this command, see the *Software Reference* for your switch.

Features and Enhancements in 5.4.3-2.5

This version includes the new features and enhancements in the following list and table:

- TACACS+ is now supported on the x210 Series switches. See the *TACACS+* chapters in the *Software Reference* for your switch.
- The following features are newly introduced in this release.
  - IPv6 hardware ACL supports x610 series switches.
  - You can use the new **ipv6 prefix-list** command to create an IPv6 prefix list or an entry in an existing prefix list.
  - You can use the new **platform hwfilter-size** command to control the configuration of hardware access control lists for x610 series switches, which determines the total available number and functionality hardware ACLs.

  For details, see the *IPv6 Hardware Access Control List (ACL) Commands* chapter in the *ACLs (Access Control Lists) Software Reference Supplement for x610 Series Switches, AlliedWare Plus™ Operating System Version 5.4.3-2.5*, downloadable from:

  http://www.alliedtelesis.com/support/documentation_keyword_ACL.aspx
- BGP4+ is now supported on x610 Series, x900 Series, SwitchBlade x908 and SwitchBlade x8112 switches. See the *BGP & BGP4+ (Border Gateway Protocol IPv4 & IPv6) Software Reference Supplement for x-Series Switches, AlliedWare Plus™ Operating System Version 5.4.3-2.5*, downloadable from

  www.alliedtelesis.com/support/documentation_keyword_BGP4.aspx
- "Silicon profile support for the SBx81GT40" on page 27

CR	Module	Description
CR00038136	**LPD**	Loop Detection action for a port can now be set to not expire by setting the timeout parameter to 0: `loop-protection timeout 0`
CR00039392	**Port Authentication**	x200 only: "Web-authentication gateway registration (CR00039392)" on page 29
CR00039394	**Port Authentication**	x200 only: "Customized message on Web-Authentication page (CR00039394)" on page 30
CR00039395	**Port Authentication**	x200 only: "Web-authentication configurable redirect-url delay time (CR00039395)" on page 30
CR00039465	**ACL**	x900 only: The storage of ACL rules now makes more efficient use of the available table space.

CR	Module	Description

CR00039698	**Layer 2 Switching**	A new global command has been added:
		`linkflap action shutdown`
		This command will disable any ports that flap more than 15 times in less than 15 seconds.
		To enable port flapping detection, use the command:
		`awplus(config)# linkflap action shutdown`
		To disable port flapping detection (default), use the command:
		`awplus(config)# no linkflap action`

Silicon profile support for the SBx81GT40

Support for the new SBx81GT40 line card ("SBx81GT40" on page 11) includes the command described below to configure the silicon profile for the switch.

platform silicon-profile (SBx8100)

Use this command to set the switch's switching and routing silicon tables to appropriate maximum sizes for the line cards that are installed in your switch, by selecting or removing a silicon profile. Changing the silicon profile changes the table limits, to match the line cards you wish to use.

Caution. *Use this command with caution, because setting the silicon profile stops some line cards from operating. We recommend that you consult your Allied Telesis support representative before using this command, to ensure the settings are suitable for your switch.*

The **no** variant of this command restores the memory to the default state when no silicon profile is set.

For this command or the no variant to take effect, you must copy it to the startup configuration using the **copy running-config** command and then reboot the switch.

You can also use the **platform routingratio** command to control how table capacity is shared between IPv4 and IPv6 entries, and/or unicast and multicast entries.

Syntax

```
platform silicon-profile {profile1|profile2}

no platform silicon-profile
```

Parameter	Description
profile1	This profile configures the switch silicon to store more MAC addresses and routes (both prefix and nexthop entries). Available for the SBx81GT40, SBx81GS24a and SBx81XS6 line cards. Do not use this option on a switch with SBx81GP24 and SBx81GT24 line cards installed - it will disable them.

Parameter	Description
profile2	Like profile1, this profile configures the switch silicon to store more MAC addresses and routes (both prefix and nexthop entries). Profile2 supports the same number of MAC addresses and prefixes as profile1 but further increases the number of nexthop entries. Available for the SBx81GS24a and SBx81XS6 line cards. Do not use this option on a switch with SBx81GT40, SBx81GP24, and SBx81GT24 line cards installed—it will disable them.

SBx8100 line cards supported by profile1 or profile2 parameter options

line card	profile1 support	profile2 support
SBx81GT40	supported	not supported
SBx81GP24	not supported	not supported
SBx81GT24	not supported	not supported
SBx81GS24a	supported	supported
SBx81XS6	supported	supported

Default By default, no silicon profile is set, and all line cards are allowed.

Mode Global Configuration.

Usage Changing the silicon profile changes the table limits, to make them match the line cards you wish to use.

For table size details and usage examples, see the Switching and Routing Tables Appendix of the SwitchBlade x8112 Internal Operation Technical Guide. You can download this guide from alliedtelesis.com.

Caution. *The silicon profile is only supported on line cards that meet the profile's minimum silicon specification. Unsupported line cards will not operate. If you wish to add an unsupported line card later, you will have to remove the silicon profile and then reboot the switch.*
Therefore, we recommend that you only set the silicon profile if the default route table size is insufficient.

To see which line cards are supported, see the table above.

The silicon profile setting in the startup configuration takes effect when the switch starts up. Therefore, for this command (or the no version) to take effect, you must copy it to the startup configuration using the copy running-config command and then reboot the switch:

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

Examples To apply profile2, use the commands:

```
awplus# configure terminal
awplus(config)# platform silicon-profile profile2
% The device needs to be restarted for this change to take
   effect.
```

To restore the silicon profile to its default setting (no profile), use the commands:

```
awplus# configure terminal

awplus(config)# no platform silicon-profile
```

Related Commands: copy running-config
platform routingratio
reboot
show platform

Web-authentication gateway registration (CR00039392)

x210 only. The Web-authentication feature first sends a Web-Auth login web page to the supplicant PC. But in most cases, the supplicant PC sends HTTP Get request packets to an external web host. So Web-authentication must intercept and use these HTTP Get request packets. The switch captures the ARP request packet from the supplicant to resolve the gateway address and sends an ARP response packet including its own MAC address. The supplicant identifies the switch's MAC address as the gateway address. In this way, the switch can capture the connection to the external web host.

Previously, Web-authentication could result in a mismatched ARP entry when an external DHCP server is used. Since the local WebAuth DHCP server leases short lifetime addresses, the supplicant resets its own address database (IP address and ARP table, e.t.c) after authentication succeeds. But if an external DHCP server is used instead of a local DHCP server, the server leases a long lifetime address and the supplicant keeps its address database based on the Web-authentication process. The ARP entry for the gateway address registered for the Web-authentication process would not be correct, resulting in the supplicant not being able to access hosts on an external subnet.

To resolve this issue, the switch now sends a gratuitous ARP message to the supplicant to refresh its ARP table when the supplicant is authorized. There is a now a new command **auth-web-server gateway** available to configure a gateway address for the Authentication Web Server.

auth-web-server gateway

Description Use this command to register the gateway IP address that supplicants should use after web authentication has succeeded. The switch finds the MAC address for this gateway device. Then, after a supplicant has authenticated, the switch sends out a gratuitous ARP advertising the gateway IP address with the MAC address that the switch has discovered belongs to that gateway device. This ensures the supplicant's gateway information is correct, and erases the fact that the switch had previously fooled the supplicant into thinking that the switch's MAC address was the MAC address of the gateway. By providing the supplicant with the correct MAC address for the gateway, the switch enables the supplicant to access external subnets.

Use the **no** version of this command to remove the gateway IP address from the Web-authentication server.

Syntax

```
auth-web-server gateway <gateway-ipaddr> vlan <1-4094>

no auth-web-server gateway <gateway-ipaddr>
```

Parameter	Meaning
<gateway-addr>	The IPv4 address of the Web-Authentication server gateway.
vlan <1-4094>	The VID of the local sub-net VLAN.

Default By default, there is no gateway entry.

Mode Global Configuration

Example To add the gateway IP address 192.168.1.1 and VLAN 10, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server gateway 192.168.1.1 vlan 10
```

To remove the gateway IP address 192.168.1.1 from the Authentication Web Server, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server gateway 192.168.1.1
```

Related Commands auth-web enable
auth-web-server mode
show auth-web-server
show running-config

Customized message on Web-Authentication page (CR00039394)

x210 only. You can now create a welcome message for the switch to display in the Web-Authentication Login Success page. Save the message in a text file (UTF-8 format) in the switch's Flash memory with a file name of either:

- success_page_msg.html, or
- message.html

If it finds both files in Flash memory, the switch gives priority to the **success_page_msg.html** file.

Web-authentication configurable redirect-url delay time (CR00039395)

x210 only. The existing 'redirect-url' auth-web feature allows the supplicant's web browser to be redirected to a user-configured Web page after the auth-web authentication is successful. In some cases a delay between the success message and the actual redirection may be required.

The amount of time that elapses between a successful login and the redirection to a configured URL can now be set to a period between 5-60 seconds. The authentication 'Success' page from the AlliedWare Plus switch is displayed to the user during the delay period.

The new **auth-web-server redirect-delay-time** command allows you to configure this delay time and the **show auth-web-server** command now displays its setting.

auth-web-server redirect-delay-time

Description Use this command to set the delay time in seconds before redirecting the supplicant to a specified URL when the supplicant is authorized.

Use the **no** version of this command to set the delay time back to the default.

Syntax

```
auth-web-server redirect-delay-time <5-60>

no auth-web-server redirect-delay-time
```

Parameter	Meaning
redirect-delay-time	The delay time in seconds before redirecting the supplicant to a specified URL when the supplicant is authorized.
<5-60>	The delay time in seconds.

Default The default redirect delay time is 5 seconds.

Mode Global Configuration

Example To set the delay time to 60 seconds for the web authentication server, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server redirect-delay-time 60
```

To reset the delay time to the default (5 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server redirect-delay-time
```

show auth-web-server

This command shows the web authentication server configuration and status on the switch.

Syntax show auth-web-server

Mode User Exec and Privileged Exec

Example To display web authentication server configuration and status, enter the command:

```
awplus# show auth-web-server
```

Output Figure 36: Example output from the show auth-web-server command

```
awplus#show auth-web-server
Web authentication server
  Server status: enabled
  Server mode: intercept
  Server address: 192.168.1.1/0
  HTTP Port No: 80
  Security: disabled
  Certification: default
  SSL Port No: 443
  Redirect URL: --
  Redirect Delay time: default
  HTTP Redirect: enabled
  Session keep: disabled
  Blocking mode: disabled (cur session: 0)
  PingPolling: disabled
  PingInterval: 30
  Timeout: 1
  FailCount: 5
  ReauthTimerRefresh: disabled
```

Features and Enhancements in 5.4.3-1.4

CR	Module	Description
CR00038868	**Software Licensing**	x510 only: OSPF-256 and OSPFv3-256 licensing have been implemented in this release as part of x510 premium license.

CR00039055	**Layer 2 switching**	x900 and SBx908: In certain configurations of over-subscription, there could be inefficient throughput. A new buffer drop mode has been added that allows back pressure to build and work with flowcontrol to improve through put under certain configurations.
		The new configuration command is:
		`platform buffer-drop-mode lossless (new behaviour)`
		`platform buffer-drop-mode tail-drop (default and existing behaviour)`

Issues Resolved in 5.4.3-3.17

AlliedWare Plus maintenance version 5.4.3-3.17 includes the resolved issues in the following table.

CR	Program	Description	x210	IX5	x510, x510L	x610	x900 / SBx908	SBx8100 CFC400
CR00052167	**System**	Previously, after receiving approximately 4 billion multicast packets on a VLAN, the VLAN could be deleted unexpectedly. This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00050788	**IPv6** **OSPFv3**	Previously, when an OSPF graceful restart was performed in an event such as a stack master failover, the default route on the device could be incorrectly removed from the OSPF route database. This issue has been resolved.	–	–	Y	Y	Y	Y
CR00052083	**Loop protection**	Previously, stack members could reboot unexpectedly if a port that had loop protection enabled was removed from an aggregation. This issue has been resolved.	–	Y	Y	Y	Y	Y
CR00052319	**IGMP**	Previously, IGMP proxy would still report an IGMP Join in response to an IGMP Query, even if the multicast group had already left. This issue has been resolved.	–	Y	Y	Y	Y	Y
CR00051900	**VLAN**	Previously, when a port with VLAN classification enabled was added to an aggregation, the aggregation would not join that VLAN. This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00052135	**802.1x**	Previously, restarting the port authentication process would result in FDB entries associated with the wrong VLAN. This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00042750	**802.1X**	Previously, a possible memory corruption would occur during the processing of authentication packets. This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00051839	**VCStack**	Previously, when learning a large number of nexthop entries for the first time after booting up, it was possible for the switch to restart unexpectedly. This issue has been resolved.	–	–	Y	Y	Y	Y
CR00041499	**SNMP**	Previously, when two Power Supply Units (PSUs) were present in a VCStack member and only one of the PSUs was powered off, the switch would fail to send an SNMP trap notification. This issue has been resolved.	–	–	Y	Y	Y	Y

CR	Program	Description	x210	IX5	x510, x510L	x610	x900 / SBx908	SBx8100 CFC400
CR00041866	**L2 Switching**	Previously, disparity of MAC address entries between hardware and software table of x210, IX5, x510 and x610 switches could occur. This issue has been resolved.	Y	Y	Y	Y	–	–
CR00042323	**Multicast**	Previously, the switch forwarding could stop under multicast stress conditions. This issue has been resolved.	–	–	–	–	–	Y
CR00042363	**RSTP**	Previously, on XEMv2 products, when spanning tree had set a port's state to discarding, it was still possible for IGMP packets to be sent to the device's CPU for processing when IGMP snooping was enabled. Processing these packets could cause more packets to be generated by the device in response, which could result in a packet storm. This issue has been resolved, so that IGMP packets will now always obey the spanning tree port state.	–	–	–	–	Y	–
CR00042413	**System**	Previously, on rare occasions, an x210 device could restart due to some initialisation errors. This issue has been resolved.	Y	–	–	–	–	–
CR00042498	**Logging**	Previously, the switch could fail to clear invalid IGMP packets which resulted in excessive log messages being generated and IGMP would then fail to correctly process subsequent IGMP packets. This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00042506	**Provisioning**	Previously, if a master of a stack was powered down while a stack member was joining the stack, the running-configuration on the master associated with the stack member could be lost. This issue has been resolved.	–	Y	Y	Y	Y	Y
CR00042710	**Switching**	Previously, executing the command **clear mac address-table dynamic vlan <vid>** would cause an unexpected restart if the VLAN specified in the command did not exist. This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00042717	**VCStack**	Previously, on very rare occasion, it was possible for the VCStack resiliency-link to fail during normal operation and never recover. This issue has been resolved.	–	Y	Y	Y	Y	Y
CR00050313	**DHCP Server, IPv6**	Previously, the DHCPv6 Relay agent failed to add routes for the assigned or delegated prefixes. This issue has been resolved.	–	Y	Y	Y	Y	Y

CR	Program	Description	x210	IX5	x510, x510L	x610	x900 / SBx908	SBx8100 CFC400
CR00051693	**Port authentication, VCStack**	Previously, it was possible for ARP packets ready for transmission to be dropped when their egress was via ports that were members of a static aggregation on x510. This issue has been resolved.	–	–	Y	–	–	–
CR00051777	**IGMP**	Previously, if a high rate of traffic was arriving at the switch CPU, it was possible for an expiring IGMP group to cause an unexpected restart of the switch. This issue has been resolved.	Y	Y	Y	Y	Y	Y

Issues Resolved in 5.4.3-3.16

AlliedWare Plus maintenance version 5.4.3-3.16 includes the resolved issues in the following table.

CR	Module	Description	x210	IX5	x510	x610	x900 / SBx908	SBx8100 CFC400
CR00042613	**RADIUS**	Previously, a supplicant could fail to be authenticated by a RADIUS server due to incorrect reuse of data transmitted in a prior RADIUS request. This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00042413	**System**	Previously, on rare occasions, an x210 device could restart due to some initialisation errors. This issue has been resolved.	Y	–	–	–	–	–

Issues Resolved in 5.4.3-3.15

AlliedWare Plus maintenance version 5.4.3-3.15 includes the resolved issue in the following table.

CR	Module	Description	x900/x908	x610	x510	IX5	x210	SBx8100
CR-50838	**SSL** **SHTTP**	SSL 3.0 cryptography protocol was vulnerable to interception of encrypted data (CVE-2014-3566, 'Poodle bug'). Previously, SSL on the device was vulnerable to this attack. This issue has been resolved. The openSSL version included in this AlliedWare Plus version includes mitigation against SSL. Support in shttpd for SSLv3 has been disabled.	Y	Y	Y	Y	Y	Y

Issues Resolved in 5.4.3-3.14

AlliedWare Plus maintenance version 5.4.3-3.14 includes the resolved issues in the following tables.

The issues addressed in this section 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.

No level 1 issues

No level 2 issues

Level 3 issues

CR	Module	Description	x900/x908	x610	x510	IX5	x210	SBx8100
CR00042516	**LLDP**	Previously, when new ports were added (when a XEM is inserted, or from a joining VCStack member) to a device that had been running for longer than 248.5 days, LLDP transmission would be incorrectly disabled, that is, the **no lldp transmit** command would appear in the running config. Executing the **lldp transmit** command on such new ports would fail. In addition, the LLDP reinit timer mechanism did not work on ports that had been continuously present from when the device had been up for 248.5 days. These issues have been resolved.	Y	Y	Y	Y	Y	Y

No level 4 issues

Issues Resolved in 5.4.3-3.13

AlliedWare Plus maintenance version 5.4.3-3.13 includes the resolved issues in the following tables.

Level 1 issues

CR	Module	Description	x900/x908	x600	x610	x510	IX5	x210	SBx8100
CR00050059	**Security SSH**	This update fixes an OpenSSH security vulnerability. OpenSSH before version 6.6 allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character - CVE-2014-2532 also CVE-2014-2653. This issue has been resolved.	Y	–	Y	Y	–	Y	Y

Level 2

CR	Module	Description	x900/x908	x600	x610	x510	IX5	x210	SBx8100
CR00038435	**VCStacking**	Previously, a rejoining member would fail to sync with the stack after it had more than five failovers. This issue has been resolved.	–	–	Y	Y	–	–	–
CR00039879	**ATMF**	Previously, if a stacked node left an AMF network, the AMF process on other nodes would occasionally experience an unexpected restart. This issue has been resolved.	Y	–	Y	Y	–	–	Y
CR00040756	**VCStacking**	Previously, a stack would not revert from the disabled master state even after all stack members had joined. This issue has been resolved.	–	–	Y	Y	–	–	–
CR00042031	**VCStacking**	Previously, on a stack with at least four members, it was possible for a stack member to not join the stack correctly if another stack member had joined and left within a short period of time. This issue has been resolved.	–	–	Y	Y	–	–	–
CR00042404	**IGMP**	Previously, IGMP Proxy would fail to send IGMP reports for a multicast group on behalf of the members in the downstream interfaces. This issue has been resolved.	Y	–	Y	Y	–	–	Y

Level 3

CR	Module	Description	x900/x908	x600	x610	x510	IX5	x210	SBx8100
CR00041856	**EPSR**	Previously, on rare occasions a delayed or missing hello packet would cause an EPSR ring to go into the failed state (and the master's secondary port to start forwarding) even though no links in the ring had been broken. This issue has been resolved.	Y	–	–	–	–	–	–
CR00041931	**OSPFv3**	Previously, OSPFv3 may have sent fragmented LSUs when many LSAs were held in the LS-database. Also, AS-external LSAs would include a tag of 0x00000000 when the T-bit was not set (no tags were specified). These issues has been resolved. Now, OSPFv3 will make sure that the number of LSAs packed into an LSU do not exceed the MTU of the interface where the LSU is sent through.	Y	–	Y	Y	–	–	Y
CR00042211	**QoS**	Previously, on the SBx8100 switch, IPv6 VRRPv3 packets were incorrectly received by the CPU on queue 2. This issue has been resolved. The IPv6 VRRPv3 packets are now received on queue 4.	Y	–	Y	Y	–	–	Y
CR00042261	**IGMP**	Previously, when an SSM mapping was removed, the corresponding mapped IGMP group entries would not be deleted. This issue has been resolved.	Y	–	Y	Y	–	–	Y
CR00042309	**QoS**	When a port disable action had been triggered by storm protection traffic was not always passing through the switch once the disable timeout had expired. This issue has been resolved.	Y	–	Y	Y	–	Y	Y
CR00042394	**Port auth**	Previously, broadcast packets would cause a network loop if **port-disable** and **fast-block** were used at the same time. This issue has been resolved.	Y	–	Y	Y	–	Y	Y

Level 4

CR	Module	Description	x900/x908	x600	x610	x510	IX5	x210	SBx8100
CR00041758	**Port Configuration**	Previously, the **ecofriendly lpi** and **no ecofriendly lpi** commands were not visible in the ?-help output. Moreover, the commands could not be entered in shortened form or by using TAB-completion. This issue has been resolved.	Y		Y	Y	Y	Y	Y
CR00042349	**Environmental Monitoring**	Previously, the process of adjusting fan speed as the temperature changed did not operate as expected on the following products: - x510-28GTX - x510-52GTX - x510-28GSX This issue has been resolved.	–	–	–	Y	–	–	–
CR00042387	**IGMP**	Previously, issuing the **clear ip igmp group *** command would result in an error: "[IGMP-ENCODE] : Invalid Rexmit HRT (3)!" showing in the log - but no operational issues were observed. This erroneous log issue has been resolved.	Y	–	Y	Y	–	Y	Y

Issues Resolved in 5.4.3-3.12

No level 1 issues

Level 2

CR	Module	Description	x900 / x908	x610	x510	IX5	x210	SBx8100
CR00042190	**PIM-SSM v4**	Previously, SSM-mapped IGMPv2 membership remained even when the last member left the multicast group. The membership remained until the group live timer expired. As a result, multicast data was being forwarded unnecessarily. This issue has been resolved. Now, when members leave the group, their membership will be removed properly at the appropriate time.	Y	Y	Y	Y	Y	Y
CR00042000	**IGMP Snooping**	Previously, if **ip igmp snooping source-timeout** was configured either globally or on a VLAN interface, and some multicast UDP packets were then received, subsequently executing the command **clear ip igmp groups** could cause the switch to reboot unexpectedly. This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00041968	**Port Authentication**	When a backup switch joins a stack, and existing authenticated port-auth supplicants are attached to the stack, then the information about those existing supplicants needs to be copied to the newly-joined stack member. Previously, when port authentication copied this information to a new stack member, the bringing up of LAG ports on the new stack member was delayed. As a result, the supplicants on the LAG port were deleted. This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00041759	**Port Authentication**	Previously, if 2-step authentication, using dot1x and web-auth, was configured on a port that was also configured as a critical port, then after a supplicant had been authenticated once on that port, every subsequent supplicant attaching to that port was automatically passed through the second step of the 2-step authentication, irrespective of whether or not they entered correct credentials. This issue has been resolved.	Y	Y	Y	Y	Y	Y

Level 2 (cont.)

CR	Module	Description	x900 / x908	x610	x510	IX5	x210	SBx8100
CR00041569	**ACL**	Previously, on the SBx8100 switches, ACLs matching on TCP flags could incorrectly match against UDP packets if the UDP packets had the right bit patterns set at the same location as the flags appear in TCP packets. This issue has been resolved.	–	–	–	–	–	Y
CR00041467	**NTP**	This update is to address the security vulnerability as disclosed by CVE-2013-5211 (http://www.us-cert.gov/ncas/alerts/TA14-013A). To mitigate the risk of attacks, the NTP monitor functionality has been disabled.	Y	Y	Y	Y	Y	Y
CR00041393	**Port Authentication**	Previously, if the switch had port authentication configured on a LAG, and multiple ports of the LAG linked up at the same time while a high rate of data was arriving on the links, some packets from unauthenticated supplicants would be forwarded. This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00040560	**Pluggable Transceivers**	Previously, on an x210 switch, plugging in or removing an SFP caused the link on other SFPs to drop and re-establish within a sub-second period. This issue has been resolved.	–	–	–	–	Y	–
CR00040215	**ARP**	Previously, it was possible for packets to be incorrectly hashed to ports on an aggregator if **arp-mac-disparity** was configured and an ARP was being resolved to a multicast MAC address. This issue has been resolved.	–	–	–	–	–	Y
CR00042137	**VCStack**	Previously, on an x510 stack, the resiliency link health check would fail when IGMP packets were received. This issue has been resolved.	–	–	Y	–	–	–

Level 3

CR	Module	Description	x900 / x908	x610	x510	IX5	x210	SBx8100
CR00042175	**IGMP Snooping**	Previously, if all members left a given group, but the device continued to receive data destined to the group's multicast address (that is, unregistered multicast addressed to this group), then the device would send IGMPv2 reports in response to IGMPv2 queries for this group. Sending these reports was incorrect, as there were actually no members still wishing to receive that group. This was due to the snooping switch incorrectly handling the group entry's status from registered to unregistered. This issue has been resolved. In addition, the command: `show ip igmp snooping statistics interface <interface-name>` now displays the "Last Reporter" field correctly "Router Port" entries (that is, entries for the "group address" 224.0.0.2). The address displayed as the "Last Reporter" is the address of the last device from which an IGMP query was received on the port in question.	Y	Y	Y	Y	Y	Y
CR00042097	**VCStack**	Previously, if a large number of IP packets were sent at a high rate to a large number of non-existent IP addresses in locally connected subnets, then a CFC failover could occur. This issue has been resolved.	–	–	–	–	–	Y
CR00042081	**System**	Previously, if there were more than 255 processes running, a small amount of memory would be lost when running the **show cpu** command. This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00042076	**802.1X**	Previously, if port authentication had assigned a dynamic VLAN ID to a LAG that spanned multiple members of a stack, and one of the backup stack members whose ports were included into the LAG restarted, then the restarted switch would subsequently believe that the dynamically assigned VLAN ID had been statically configured on the LAG port(s) in question. When the supplicant's session finished, the port(s) in question would not return to their original VLAN, but would stay in the dynamically assigned VLAN. This issue has been resolved.	Y	Y	Y	Y	Y	Y

Level 3 (cont.)

CR	Module	Description	x900 / x908	x610	x510	IX5	x210	SBx8100
CR00041795	**File System**	Previously, TFTP file transfers from an AlliedWare Plus device to an external server would add a leading '/' to the filename, which is not supported by some TFTP servers. This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00041724	**VCStack**	Previously, the **copy** <name> **web-auth-https-file** command did not install the SSL certificate correctly on a stack if the stack had been reduced to just one member. This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00041718	**VLAN**	Previously, if the **switchport trunk allowed vlan except** command was entered for a switchport, it could cause problems if the switchport was not already a member of the VLAN that the command was specifying to be excluded. For example, the switch may fail to respond to ARP requests on that VLAN. This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00041699	**IPv4 Multicast Route Manager**	Previously, processing around 64 IGMP leaves and 64 IGMP joins in layer-3 switched multicast configuration every 5 seconds resulted in some multicast streams not being forwarded. This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00041534	**Environment Monitoring**	Previously, the low limit voltage threshold was not recognized in hardware monitoring. This issue has been resolved.	–	–	Y	Y	–	–
CR00041370	**VCStack**	Previously, if multiple VCStack members or SBx8100 cards were rebooted at the same time, and a large configuration file was present, then it was possible that it would take a long time for them to finish loading the configuration. This issue has been resolved. Also, with this update, the status of the atFilev2InfoTable MIB objects in the at-filev2.mib file has changed from deprecated to obsolete. These MIB objects are no longer supported and the atFilev2FileViewer MIB objects should be used instead.	Y	Y	Y	Y	–	Y

Level 4

CR	Module	Description	x900 / x908	x610	x510	IX5	x210	SBx8100
CR00042016	**IPv4**	Previously, deleting a VLAN interface would not also delete the IP helper configuration on that interface. This resulted in the IP helper referencing a non-existent interface, which could cause undefined behaviour. This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00041447	**MLD Snooping**	Previously, superfluous warning log messages indicating IGMP Group-Source report retransmission failures may have been filling up logs, obscuring other more useful logs. This issue has been resolved by downgrading the warning level log to a debugging level log.	Y	Y	Y	Y	Y	Y
CR00041347	**Port Configuration**	Previously, JAM state was displayed as an invalid value on 10G port. This issue has been resolved.	–	Y	Y	–	–	–
CR00040976	**System**	Previously, command modifiers would have no effect on certain commands when used in an ATMF working-set. This has been resolved. Command modifiers now behave as expected.	Y	Y	Y	Y	Y	Y
CR00040862	**IGMP**	Previously, IGMP produced excessive log messages displaying text: `[IGMP-ENCODE] : Failed to find real Src-Rec from a Clone!` This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00041713	**Environment Monitoring**	The fan RPM on the SBxSYSPWR1-80 was incorrectly reported. This issue has been resolved.	–	–	–	–	–	Y

Issues Resolved in 5.4.3-3.11

AlliedWare Plus maintenance version 5.4.3-3.11 includes the resolved issues in the following tables.

No level 1 issues

Level 2

CR	Module	Description	x900/x908	x600	x610	x510	IX5	x210	SBx8100
CR00041731	**STP**	Previously, if a device configured with spanning-tree (RSTP or MSTP) received repeated BPDU's with the "proposal" flag set, it would set its designated ports back to discarding and they would then have to progress back to forwarding. This would potentially cause regular traffic loss. This situation arises if the device sending the proposal BPDU's ignores the agreements sent back to it. This issue has been resolved. Now if the device receives a BPDU with repeated information that it has already agreed to, it will not change the state of its designated ports. This behaviour is in accordance with the IEEE standards.	Y	–	Y	Y	Y	Y	Y

No Level 3 issues

No Level 4 issues

Issues Resolved in 5.4.3-3.10

AlliedWare Plus maintenance version 5.4.3-3.10 includes the resolved issues in the following tables.

No level 1 issues

Level 2

CR	Module	Description	x900/x908	x600	x610	x510	IX5	x210	SBx8100
CR00039926	**ATMF**	Previously, ATMF Neighbour relationships and ATMF working-sets failed to operate correctly after the failover of a stack in the ATMF network. This issue has been resolved.	Y	–	–	–	–	–	Y
CR00040157	**IGMP Snooping**	Previously, the command **ip igmp snooping routermode** could cause an x210 switch to restart unexpectedly. This issue has been resolved.	–	–	–	–	–	Y	–
CR00040590	**L2 switching**	Previously, an attempt to boot an XS16 (unsupported) in an SBx8100 chassis, resulted in other cards to stop forwarding traffic. This issue has been resolved. The XS16 will now be disabled once it is detected.	–	–	–	–	–	–	Y
CR00040669	**QoS**	Previously, when the command **service-policy input xxx** was used, followed by the command **aaa authentication auth-web** an unexpected reboot would occur. This issue has been resolved.	–	–	Y	Y	Y	Y	–
CR00041344	**ARP**	Previously, when a XEM-2XS, XEM-2XT, XEM-12Sv2, XEM-12Tv2 or XEM-24T was hotswapped out from an **x908** switch, traffic destined to the CPU would not be processed by the newly elected XEM CPU packet processor if that newly elected processor was a XEM-12S, XEM-12T or XEM-1XP. This issue has been resolved.	Y	–	–	–	–	–	–
CR00041412	**IPv6**	Previously, when a disabled master became a VCS master, some global IPv6 addresses on interfaces on the stack might not have been configured properly, causing communication failure. This issue has been resolved.	Y	–	Y	Y	–	Y	Y

Level 2 (cont.)

CR	Module	Description	x900/x908	x600	x610	x510	IX5	x210	SBx8100
CR00041470	**OSPFv3**	Previously, when a switch that was preparing to perform an OSPFv3 Graceful Restart received an implicit grace-LSA acknowledgment from a DR (and the DR was its only OSPFv3 neighbor), the switch would fail to execute the Graceful Restart. Instead, it would keep resending the grace-LSA until it received an explicit grace-LSA acknowledgment. This issue has been resolved.	Y	–	Y	Y	–	Y	Y
CR00041642	**Port Authentication**	Previously, if **HTTP-redirect** and **session-keep** were enabled on web-authentication, and a Windows7 supplicant accessed the web-authentication page, then the HTTPredirect process could unexpectedly restart. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y

Level 3

CR	Module	Description	x900/x908	x600	x610	x510	IX5	x210	SBx8100
CR00039848	**OSPFv3**	Previously, when a route map which did not include a **set metric** clause, was used as the route map for OSPFv3 redistribution, the metric value of the redistributed route would be set to the original metric of the route from the RIB, even if the redistribution command specified a different metric value. This issue has been resolved. The metric configured on the redistribute command will be correctly applied, unless a route map with a **set metric** clause is used.	Y	–	Y	Y	–	Y	Y
CR00040442	**Port Authentication**	Previously, when a supplicant was authorised, and moved to a different VLAN, an internal error, '*VCS sync timeout for lock-step operation*' would be displayed and the supplicant would fail to authenticate. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y

Level 3 (cont.)

CR	Module	Description	x900/x908	x600	x610	x510	IX5	x210	SBx8100
CR00040630	**Port Authentication**	Previously, on a stack, if the HTTPS feature was enabled just after the certificate file was removed (by the entering the **erase system:web-auth-https-file** command) from all backup nodes during the stack sync event, the stack would reboot unexpectedly. This issue has been resolved.	Y	–	Y	Y	–	–	Y
CR00040804	**System**	Previously there was a memory leak in an internal software process on x510 and Ix5 switches. This issue has been resolved.	–	–	–	Y	Y	–	–
CR00041023	**BGPv4**	Previously, the configuration commands **address-family ipv6** and **exit-address-family** would be added by default to BGP configuration. This issue has been resolved. These commands are now only added when a **address-family ipv6** subcommand has been entered.	Y	–	Y	Y	–	–	Y
CR00041081	**Port Authentication**	Previously, when a port's authentication status changed from "Authorized" to "Unauthorized", e.g. the supplicant logged out and the authenticating port went link-down, the FDB entry associated with the supplicant was not deleted. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y
CR00041153	**Port Authentication**	Previously, when the supplicant MAC was configured as port-control skip-second-auth, and critical port was used together with 2nd-step authentication, the port-control skip-second-auth would not work correctly. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y
CR00041185	**VCStack**	Previously, on rare occasions, an **x908** switch could reboot unexpectedly due to an internal system error. This issue has been resolved.	Y	–	–	–	–	–	–
CR00041521	**Policy-based Routing**	Previously, when a VLAN was repeatedly brought up and down by adding the VLAN to and removing it from a static aggregator, the VLAN could go into a permanent down state. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y
CR00041566	**Exception Handling**	Previously, an x510 switch might unexpectedly restart on rare occasions without generating any core file. This issue has been resolved.	–	–	–	Y	–	–	–

Level 3 (cont.)

CR	Module	Description	x900/x908	x600	x610	x510	IX5	x210	SBx8100
CR00040062	**IPv6**	Previously, the interface state of a tunnel interface was not changed when its underlying VLAN interface went up and down. This issue has been resolved.	Y	Y	Y	Y		Y	Y

Level 4

CR	Module	Description	x900/x908	x600	x610	x510	IX5	x210	SBx8100
CR00039657	**EEE**	Previously, on an SBx8100 switch, the ecofriendly settings would get cleared after CFC failover. This issue has been resolved.	–	–	–	–	–	–	Y
CR00039729	**TACACS+**	Previously, commands executed under the command **show tech-support** were not sent to the TACACS+ server. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y
CR00040062	**IPv6**	Previously, the interface state of a 6-to-4 tunnel interface would not change when the VLAN associated to it went up and down. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y
CR00041022	**L2 Switching**	Previously, the transmit pause frame counter of a 10G port on the x610 and x510 switches was not displaying the correct values. This issue has been resolved.	–	–	Y	Y	–	–	–
CR00041364	**IGMP**	Previously, if there was an IGMP querier with a higher priority (lower IP address) on another device in the subnet and IGMP snooping was disabled, the command **show ip igmp groups** would show the IP address of the other querier as 0.0.0.0. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y
CR00041386	**Triggers**	Previously, the **show atmf trigger** command would not display USB trigger counters. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y

Level 4

CR	Module	Description	x900/x908	x600	x610	x510	IX5	x210	SBx8100
CR00041788	**System**	Previously, an unnecessary kernel warning was printed on the console when removing a port from a channel group. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y

Issues Resolved in 5.4.3-3.9

AlliedWare Plus maintenance version 5.4.3-3.9 includes the resolved issues in the following tables.

No level 1 issues

Level 2

CR	Module	Description	x900/x908	x610	x510	IX5	x210	SBx8100
CR00040572	**PoE**	x510-GPX, IPX-GPX only. Previously, the switch would sometimes erroneously stop supplying PoE power to connected powered devices. This issue has been resolved.	–	–	Y	Y	–	–
CR00040614	**VCStack**	Previously, traffic was not well shared across aggregated links that spanned different members of a stack. This issue has been resolved, so that the sharing of traffic across such links is now more even.	–	Y	Y	–	–	–
CR00040647	**RSTP**	Previously, interoperation of ATMF with STP could cause thrashing of a MAC address in a switch's FDB. This was because a port could learn an AMF neighbor's MAC address from a BPDU even when the BPDU was received via a port that was blocked by STP. This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00040659	**Hot Swap**	Previously, hot insertion of XEMs sometimes resulted in traffic loss. This issue has been resolved.	Y	–	–	–	–	–
CR00040701	**ATMF**	Previously, changing the hostname of a node via AMF caused the console to lock up. This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00040960	**Flow Control**	Previously, when a new SFP+ was inserted into a port, any pause frames subsequently sent from the port had a source MAC address of all zeros. This issue has been resolved.	–	–	Y	Y	–	–
CR00041146	**VCStack**	Previously, when at least one of the following XEMs were present: XEM-2XP, XEM-2XT, XEM-2XS, XEM-12Tv2, XEM12Sv2, XEM-24T, and when the switch was under high MAC processing load (i.e., a storm), a system lockup leading to a system reboot could occur. This issue has been resolved.	Y	–	–	–	–	–

Level 3

CR	Module	Description	x900/x908	x610	x510	IX5	x210	SBx8100
CR00039370	**VLAN**	Previously, vlan4091 and vlan4092 could be configured as network VLANs on a unit booted at factory default, but packets would not be forwarded in those VLANs. This is because those VLANs are reserved for the use of AMF, which is enabled by default. This issue has been resolved—it is no longer possible to configure vlan4091 and vlan4092 on a switch that is booted from factory-default. AMF must be explicitly disabled before those VLANs can be configured.	Y	Y	Y	Y	Y	Y
CR00040512	**Port Authentication**	Previously, the Web Authentication login page would not display after failing web authenticate once. This issue has been resolved.	Y	Y	Y	Y	Y	Y
CR00040710	**VCStack**	Previously, on rare occasions, it was possible for the VCStack master to stop sending healthchecks over the stacking resiliency link. This issue has been resolved.	Y	Y	Y	Y	–	Y
CR00040757	**Environment Monitoring**	Previously, if the temperature detector in the SBx8100 that feeds data to the fan controller ever reached maximum temperature, the fan would remain at the maximum speed even after the temperature had returned to a normal value. This issue has been resolved.	–	–	–	–	–	Y
CR00040799	**IPv6 Filter**	Previously, if IPv6 storm protection was configured on an aggregated link, the storm protection action would be incorrectly triggered if a stack member rejoined the stack. This issue has been resolved.	–	Y	Y	–	–	–
CR00040822	**QoS**	Previously, it was possible for a log message: `audit inconsistencies detected - stack member 1 should reboot` to be generated if QoS storm control was enabled on an aggregator port when a stack member rejoined a stack. This issue has been resolved.	–	Y	Y	–	–	–
CR00041251	**IGMP Snooping**	Previously, even when the IGMP snooping was turned off in a standalone switch, that is, the switch was neither an IGMP querier nor an IGMP snooper, L2 multicast traffic was not being flooded, even though it should be. This issue has been resolved.	Y	Y	Y	Y	Y	Y

Level 4

CR	Module	Description	x900/x908	x610	x510	IX5	x210	SBx8100
CR00040396	**IPv6**	Previously, the **show ipv6 route summary** command would not show the correct number of connected routes in the connected route counters. This issue has been resolved.	Y	Y	Y	–	–	Y
CR00040717	**ATMF**	Previously, the **show trigger counter** command displayed incorrect data for 'atmf node leave and join events'. This issue has been resolved.	Y	Y	Y	Y	–	Y
CR00040086	**L2 Switching**	Previously, the counter for frames with sizes between 1523 and 2047 bytes was erroneously used to count frames with sizes between 1519 and 2047 bytes. This issue has been resolved—the correct frame counter range is now displayed.	–	Y	Y	Y	Y	–
CR00041149	**DHCPv4**	Previously, when a DHCP client included a MAC address client-ID option in its DHCP request, the **show ip dhcp binding** command output on the AlliedWare Plus DHCP server could sometimes show an incorrect value in the ClientId column for the corresponding lease. This issue has been resolved.	Y	Y	Y	Y	Y	Y

Issues Resolved in 5.4.3-3.8

AlliedWare Plus maintenance version 5.4.3-3.8 includes the resolved issues in the following tables.

No level 1 issues

Level 2

CR	Module	Description	x900/x908	x610	x510	x210	SBx8100
CR00040452	**ATMF**	Previously, the AMF node recovery master selection process was incorrectly selecting the last master node contacted, instead of the one with the best backup. This issue has been resolved.	Y	Y	Y	Y	Y
CR00040484	**Pluggable Transceivers**	Previously, under certain conditions it was possible that an SFP would not correctly link up. This issue has been resolved.	Y	–	–	–	Y
CR00040552	**Auto-negotiation**	Previously, with certain combinations of direct attach copper cables and link partners, the ports on SBx81XS6 would fail to link up. This issue has been resolved.	–	–	–	–	Y
CR00040561	**BGPv4**	Previously, if the local BGP peer was set with the 4-Byte ASN capability (enabled by default since 5.4.3-2.5), and a BGP update with an empty AS-path attribute arrived from a non-4-Byte-capable peer and the switch was using a routemap to filter AS paths, the BGP process would restart. This issue has been resolved.	Y	Y	Y	–	Y

Level 3

CR	Module	Description	x900/x908	x610	x510	x210	SBx8100
CR00035900	**Pluggable transceivers**	Previously, certain third-party SFPs would be rejected by the switch due to strange values in the serial EEPROM data. This issue has been resolved. Note that this does not guarantee interoperability with these SFPs, only that the switch does not reject them outright.	Y	Y	Y	–	Y

Level 3 (cont.)

CR	Module	Description	x900/x908	x610	x510	x210	SBx8100
CR00039387	**OSPFv3**	Previously, the OSPFv3 **default-information originate** command would only work if the command was issued when the IP route table already contained the default route. The command did not handle dynamic addition/ deletion of a ::/0 route very well. This issue has been resolved.	Y	Y	Y	–	Y
CR00039434	**ATMF**	Previously, there were circumstances where the **atmf working-set** command was not working for a leaving node. When the node rejoined, it would cause an internal system process (imish) to exit unexpectedly. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039634	**ACL**	Previously, it was not possible to remove an ACL rule from the IPv6 hardware access list by specifying a sequence number. This issue has been resolved.	–	Y	Y	–	–
CR00040397	**VCStack**	Previously, OSPFv3 would sometimes fail to send a grace LSA upon stack failover. This resulted in fast failover taking more time than usual. This issue has been resolved.	Y	Y	Y	–	Y
CR00040417	**ATMF**	Previously, when entering an Interface Configuration mode command into a multiple-node AMF working-set in which the specified interface did not exist locally, the command line could become unresponsive. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039980	**System**	Previously if more than 20 different users had logged into the switch by Telnet or SSH, and had been authenticated by RADIUS, then the next login would fail, and a system process (IMI) would restart. This issue has been resolved.	Y	Y	Y	Y	Y
CR00040323	**ARP**	Previously, if the **switchport trunk allowed vlan none** command was entered for a switchport, it could cause problems for VLANs that the switchport was not a member of. For example, the switch may have failed to respond to ARP requests on those VLANs. This issue has been resolved.	Y	Y	Y	Y	Y
CR00040441	**Port Authentication**	Previously, if a port was part of an LACP aggregation, and the port was configured with single-host mode authentication, traffic would not be allowed in, even after the supplicant was successfully authenticated. This issue has been resolved.	Y	–	–	–	Y

Level 4

CR	Module	Description	x900/x908	x610	x510	x210	SBx8100
CR00040292	**IPv6**	Previously, an unnecessary log message, indicating that IPv6 multicasting was not enabled, would be generated when the device processed MLD joins. This happened when IPv6 multicast routing was disabled. This issue has been resolved.	Y	–	–	–	Y
CR00040309	**NTP**	Previously, unnecessary NTP log messages were generated when an AMF node left the network. This issue has been resolved—the log message no longer appears.	Y	Y	Y	Y	Y
CR00040086	**L2 Switching**	Previously, the counter for frames with sizes between 1523 and 2047 bytes was erroneously used to count frames with sizes between 1519 and 2047 bytes. This issue has been resolved—the correct frame counter range is now displayed.	–	Y	Y	Y	–
CR00040444	**Pluggable Transceivers**	Previously, when manually setting speed/duplex of an SFP combo port in an x210 switch to 1000M/Full, the SFP port appeared to be 'not connected', while the link partner considered the link to still be up. This issue has been resolved.	–	–	–	Y	–

Issues Resolved in 5.4.3-3.7

AlliedWare Plus maintenance version 5.4.3-3.7 includes the resolved issues in the following tables.

No level 1 issues

Level 2

CR	Module	Level	Description	x900/x908	x610	x510	x210	SBx8100
CR00040143	**EPSR**	**2**	Previously, on an x900 or SBx908 VCStack, a joining member could incorrectly drop packets. This issue has been resolved.	Y	–	–	–	–
CR00039293	**IPv4 Multicast Route Manager**	**2**	Previously, clearing the IP mroute table (**clear ip mroute ***) would not result in the mroute table being refreshed properly. This issue has been resolved.	Y	Y	Y	–	Y
CR00039838	**ATMF**	**2**	Previously, AMF automatic node recovery would sometimes fail to work. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039942	**Port authentication**	**2**	Previously, Web-authentication did not work on the ports of the following products: XEM-12Tv2, XEM-12Sv2, XEM-2XT, XEM-2XS, XEM-1XP, XEM-2XP, SBx81GT24, SBx81GP24, SBx81GS24a, SBx81XS9, SBx81GT40. This issue has been resolved.	Y	–	–	–	Y
CR00040009	**802.1x**	**2**	Previously, 802.1x authentication did not work on the ports of the following XEM models: XEM-12Tv2, XEM-12Sv2, XEM-2XT, XEM-2XS, XEM-1XP, XEM-2XP. This issue has been resolved.	Y	–	–	–	–
CR00040126	**ATMF**	**2**	Previously, if a user was connected to an AMF node in Interface Configuration mode at the same time as another node left the AMF network, an unexpected system reboot occurred. This issue has been resolved.	–	Y	Y	Y	–
CR00040169	**VLAN**	**2**	Previously, communication from a Private VLAN promiscuous port to the switch's CPU would fail. This issue has been resolved.	–	Y	Y	Y	–
CR00040191	**OSPFv3**	**2**	Previously, if one of the OSPFv3 interfaces on a VCStack backup member changed status to 'DOWN', the OSPF6d process running on that member would restart. This issue has been resolved.	Y	Y	Y	–	Y

Level 2 (cont.)

CR	Module	Level	Description	x900/x908	x610	x510	x210	SBx8100
CR00040312	**IPv4**	**2**	Previously, some UDP packets were being forwarded with incorrect UDP checksums. This could result in packets being dropped by host devices. This issue has been resolved.	Y	Y	Y	Y	Y
CR00040320	**RIP**	**2**	Previously, a static default route with a nexthop in a connected network would become unreachable when the nexthop was also advertised as a host-specific route by a routing protocol neighbour (such as RIP neighbour). This issue has been resolved.	Y	Y	Y	Y	Y

Level 3

CR	Module	Level	Description	x900/x908	x610	x510	x210	SBx8100
CR00040106	**Policy-based Routing**	**3**	Previously, the removal and re-addition of a policy map to a port could cause the policy rules to be applied to hardware in the wrong order. The correct order of the rules would not be restored until the unit was rebooted. This issue has been resolved.	–	Y	Y	–	–
CR00040112	**Port Authentication**	**3**	Previously, if a supplicant re-authentication happened before the RADIUS server timeout on the deleted supplicant, the authd process would end unexpectedly. This issue has been resolved.	Y	Y	Y	Y	Y
CR00040176	**ACL**	**3**	Previously, with an access-list configured and attached to a port, rebooting a single SBx908 or x900 stack member could lead to issues when attempting to alter the access-list while it remained attached to the port. This issue has been resolved.	Y	–	–	–	Y
CR00040190	**QoS**	**3**	Previously, on a VCStack, the running configuration could report incorrect values for the **wrr-queue egress-rate-limit** command. This issue has been resolved.	Y	Y	Y	–	Y
CR00039376	**SNMP**	**3**	Previously, the license indices reported by SNMP and the CLI were different. This issue has been resolved—both the CLI and SNMP now report the same index value for each license.	Y	Y	Y	Y	Y

Level 3 (cont.)

CR	Module	Level	Description	x900/x908	x610	x510	x210	SBx8100
CR00039892	**QoS**	**3**	There is a limitation with the switch chip in SBx908, x900 and SBx8100 switches. The limitation is that the chip requires a minimum value for the CBS and EBS thresholds in a policing configuration. This minimum threshold could result in the committed burst rate being rounded down to zero, resulting in all non-red traffic being marked as yellow. This issue has been resolved. The rounding of the police committed burst rate now favours marking traffic as green instead of yellow.	Y	–	–	–	Y
CR00039968	**OSPFv3**	**3**	Previously, the OSPF6d process sometimes unexpectedly restarted when the switch was redistributing IPv6 routes into OSPFv3. This issue has been resolved.	Y	Y	Y	Y	Y
CR00040214	**DNS**	**3**	Previously, DNS would occasionally fail to allocate memory to cache. As a result, after rebooting, the resolved names were not stored in the cache. This issue has been resolved.	Y	Y	Y	Y	Y
CR00040243	**NSM**	**3**	Previously, when a route had multiple ECMP recursive nexthops, and the interface connecting to the first recursive nexthop went down, the whole route would be removed from the software table, even when it was still reachable via the remaining active nexthops. This issue has been resolved. In addition, a display error in the output of the command **show ipv6 route database** has also been resolved.	Y	Y	Y	Y	Y
CR00040257	**Hot swap**	**3**	Previously, hotswapping the second PSU on an x510-28GPX or x510-52GPX switch would result in turning off the PoE power supply. This issue has been resolved.	–	–	Y	–	–
CR00040342	**Pluggable Transceivers**	**3**	Previously, detection of an SBx81XS6 card with pluggables connected on all ports would occasionally fail on power up. This issue has been resolved.	–	–	–	–	Y
CR00040293	**IGMP Snooping**	**3**	Previously, when an empty IGMP snooping entry timed out and router ports were present in the VLAN, a few packets may have been dropped incorrectly. This issue has been resolved.	Y	Y	Y	Y	Y

Level 4

CR	Module	Level	Description	x900/x908	x610	x510	x210	SBx8100
CR00039350	**PIM-DMv4**	**4**	Previously, excessive log messages would be generated during the learning phase of a PIM border router. This issue has been resolved.	Y	Y	Y	–	Y
CR00039992	**ATMF**	**4**	Previously, AMF did not display the full 64 characters of a hostname correctly. This issue has been resolved.	Y	Y	Y	Y	Y
CR00040271	**Logging**	**4**	Previously, inappropriate error log messages would be produced if the hardware route entry table became full. This issue has been resolved. These error log messages have been replaced with more meaningful warnings when the hardware route entry table is full.	Y	–	–	–	Y
CR00039824	**File System**	**4**	Previously, when deleting a file from an ASK-256-8G USB flash stick, the USB stick's LED would not stop flashing even when the deletion had completed. This issue has been resolved.	–	–	Y	–	Y

Issues Resolved in 5.4.3-2.6

AlliedWare Plus maintenance version 5.4.3-2.6 includes the resolved issues in the following tables.

No level 1 issues

Level 2

CR	Module	Description	x900/x908	x610	x510	x210	SBx8100
CR00039123	**OSPFv3**	Previously, shutting down multiple interfaces that were nexthops for an OSPFv3 route sometimes caused an unexpected reboot. This issue has been resolved.	Y	Y	Y	–	Y
CR00039221	**IPv6**	Previously, IPv6-over-IPv4 tunnelling would not work correctly over aggregated links. This issue has been resolved.	Y	Y	Y	Y	Y

Level 2 (cont.)

CR	Module	Description	x900/x908	x610	x510	x210	SBx8100
CR00039299	**Storm Control**	When MAC thrashing (MAC addresses rapidly moving from one port to another) is occurring, the switch chip will send packets to the CPU to inform the CPU of the MAC movement. Previously, the packets being sent to the CPU for this reason were being sent on a high-priority queue, and could drown out more important traffic. This issue has been resolved by sending the MAC-movement indication packets to the CPU on queue 0.	–	–	Y	–	–
CR00039816	**Pluggable Transceivers**	Previously, an AT-SPSX/I was not detected correctly when inserted into an SFP+ port. This issue has been resolved.	–	Y	Y	–	–
CR00039854	**IGMP Snooping**	Previously, a system reboot could occur when configuring an IGMP proxy. This issue has been resolved.	Y	Y	Y	–	Y
CR00040093	**Port Configuration**	Previously, SFP ports would not work correctly at 100Mbps on the x210. This issue has been resolved.	–	–	–	Y	–
CR00040161	**IGMP Snooping**	Previously, PIM would stop receiving group membership from IGMP when IGMP Version 2 was used. This issue has been resolved.	Y	Y	Y	Y	Y
CR00040167	**VCStack**	Previously, when the user attempted to stack x900 or SBx908 units that were running incompatible software versions, instead of entering disabled master state, the second stack member would reboot indefinitely. This issue has been resolved.	Y	–	–	–	Y

Level 3

CR	Module	Description	x900/x908	x610	x510	x210	SBx8100
CR00039474	**VCStack**	Previously, it was possible for CoS 7 traffic to cause stack separations because the stacking management traffic also used this CoS value. This issue has been resolved. The stacking management traffic is now placed into a high priority internal queue.	–	Y	Y	–	–
CR00039565	**Switching**	Previously, an SBx8100 could experience an unexpected reboot when a large number of MAC movements occurred. This issue has been resolved.	–	–	–	–	Y

Level 3 (cont.)

CR	Module	Description	x900/x908	x610	x510	x210	SBx8100
CR00039753	**Port Authentication**	Previously, when a WebAuth supplicant's status moved from REAUTHENTICATING to AUTHENTICATED, the authenticated page was not displayed to the user. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039841	**IPv6**	Previously, an interface link down did not always clear the IPv6 state fully on that interface. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039893	**Pluggable Transceivers**	Previously, when a port on an SBx81XS6 line card was connected to a link partner via a Direct Attach Cable (DAC), the link sometimes failed to come up on bootup. This issue has been resolved.	–	–	–	–	Y
CR00040083	**Command Shell**	Previously, copying a file from a switch to a TFTP server that did not exist would cause a memory leak. This issue has been resolved.	Y	Y	Y	Y	Y
CR00036389	**OSPFv3**	Previously, on a stack with OSPFv3 configured, master failover would sometimes cause traffic to be disrupted. This would only affect traffic that used routes learnt from an OSPFv3 neighbour. This issue has been resolved.	Y	Y	Y	–	Y
CR00040042	**OSPFv3**	Previously, OSPFv3 would generate an AS-External LSA with a random prefix if a redistributed default route was no longer present, but **default-information-originate** was configured. This issue has been resolved.	Y	Y	Y	–	Y
CR00040062	**IPv6**	Previously, the interface state of a tunnel interface was not changed when its underlying VLAN interface went up and down. This issue has been resolved.	Y	Y	Y	Y	Y
CR00040064	**Triggers**	Previously, if a trigger was deconfigured, the configuration was not completely removed from the configuration file. This issue has been resolved.	Y	Y	Y	Y	Y
CR00040139	**TFTP**	Previously, when trying to copy multiple files via TFTP, only the first file would be copied. This issue has been resolved.	Y	Y	Y	Y	Y

Level 4

CR	Module	Description	x900/x908	x610	x510	x210	SBx8100
CR00039545	**Hot swap**	Previously, under some circumstances when using Direct Attach Cables (DAC), the LEDs on the SBx81XS6 line card would not light up. This issue has been resolved.	–	–	–	–	Y
CR00039824	**File System**	Previously, when deleting a file from an ASK-256-8G USB flash stick, the USB stick's LED would not stop flashing, even when the deletion had completed. This issue has been resolved.	–	–	Y	–	Y
CR00039826	**OSPFv3**	Previously, the log messages of OSPFv3 authentication did not have a return character at the end of the messages. This issue has been resolved.	Y	Y	Y	–	Y
CR00039857	**Telnet**	Previously, the IP address of a device that connected via Telnet was absent in the log entries. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039969	**TFTP**	Previously, when copying multiple files from a switch via TFTP, the message 'Successful operation' was displayed even if there was a copying error. This issue has been resolved. Now 'Successful operation' will only be displayed if the TFTP copy of the multiple files completes successfully.	Y	Y	Y	Y	Y
CR00039618	**EPSR**	Previously, a warning message would not be displayed when the EPSR control VLAN was assigned to a third port. This issue has been resolved.	–	–	Y	–	–

Issues Resolved in 5.4.3-2.5

AlliedWare Plus maintenance version 5.4.3-2.5 includes the resolved issues in the following tables.

No level 1 issues

Level 2

CR	Module	Description	x900/x908	x610	x510	x210	SBx8100
CR00039255	**CLI**	Previously, issuing the command: `card enable` for a CFC or line card that was already enabled would result in a system reboot. This issue has been resolved.	–	–	–	–	Y
CR00039462	**Layer 3 switching**	Previously, when a switch was learning recursive summary routes through a routing protocol, the switch might undergo a system reboot. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039677	**DHCPv6**	Previously, if MLD snooping was disabled, then DHCPv6 relay would not relay DHCPv6 client requests. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039564	**SNMP**	Previously, when a switch was configured to use VLAN 4094, performing an SNMP GET for on object in the VLAN4094 dot1q MIB table would cause an expected reload. This issue has been resolved.	Y	Y	Y	Y	Y

Level 3

CR	Module	Description	x900/x908	x610	x510	x210	SBx8100
CR00038277	**QoS**	X908 with XEM. Previously, the egress queue for OSPF unicast control packets were not given sufficiently high priority when egressing from ports on XEM-2XP, XEM-12Tv2 or XEM-12Sv2. This issue has been resolved.	Y	–	–	–	–

Level 3 (cont.)

CR	Module	Description	x900/x908	x610	x510	x210	SBx8100
CR00039296	**EPSR**	X908 with XEMv2 installed. Previously, with certain combinations of XEMs, VLAN tags were failing to be added to packets egressing ports on XEM-1XP, XEM-12T and XEM-12S. This issue has been resolved.	Y	–	–	–	–
CR00039386	**VCStack**	Previously, the egress-rate-limit settings would not be retained on all stack members after reboot or failover. This issue has been resolved.	–	Y	Y	–	–
CR00039393	**Web authentication**	Previously, if a user was successfully authenticated via web-authentication, then moved to another subnet, then the Logout button was not operating as expected. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039412	**Layer 2 switching**	Previously, Jumbo frames of size 10233 - 10240 bytes were not being forwarded between two line cards. This issue has been resolved.	–	–	–	–	Y
CR00039436	**Port Authentication**	Previously, an internal software race condition could lead to ports configured for MAC-AUTH and dynamic VLAN assignment not being assigned the dynamic VLAN, and remaining in the native VLAN. This issue has been resolved.	–	Y	Y	Y	–
CR00039452	**PIM-SM v4**	Previously, it was possible for some multicast streams to stop being Layer 3 forwarded after a stack failover. This issue has been resolved.	–	Y	Y	–	–
CR00039539	**File System**	Previously, port numbers specified in the command: `scp copy` were being incorrectly interpreted as filenames. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039547	**VCStack**	Previously, there was a chance of a late joining x510-24GSX becoming a duplicate Master. This issue has been resolved.	–	–	Y	–	–
CR00039548	**PIM-SMv4**	Previously, if a PIM border router received a stream (S,G) from the PIM-DM domain, it could fail to send register packets for this stream to the RP of the PIM-SM domain. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039569	**Triggers**	Previously, interface triggers would not work on x210 switches. This issue has been resolved.	–	–	–	Y	–
CR00039581	**ACL**	Previously, ACLs would fail to match IP, TCP, UDP, and ICMP packets when the source and destination IPv4 addresses were specified in the ACL. This issue has been resolved.	Y	–	–	–	–

Level 3 (cont.)

CR	Module	Description	x900/x908	x610	x510	x210	SBx8100
CR00039653	**Pluggable Transceivers**	Previously, when a copper SFP was inserted into the switch, the Pause control setting of the port could disagree with the setting that had been configured for the port. This mismatch would persist even if the copper SFP was replaced by a fibre SFP. This issue has been resolved.	–	Y	Y	Y	–
CR00039674	**RADIUS**	Previously, accounting packets sometimes failed to be sent to the RADIUS server after a reload. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039699	**Port Configuration**	Previously, copper SFPs were not always being initialised correctly. This could result in incorrect link status. This issue has been resolved.	–	Y	Y	Y	–
CR00039702	**Port Authentication**	Previously, port-authentication sent only a RADIUS accounting START packet, and no STOP packet, when re-authentication was successful. This issue has been resolved, now both START and STOP packets are sent upon successful re-authentication.	Y	Y	Y	Y	Y
CR00039703	**Scripting**	Previously, when interactive commands such as **copy** or **delete** were used in a script, they caused an early exit of the script. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039728	**VCStack**	Very occasionally (i.e. 1 in 1000) one of the units could fail to join the stack. Instead, it would boot as a standalone unit. When this problem occurred, the command: `show stack detail` would display the stack ports as down on the standalone unit, but the stacking ports would be up on the other directly-connected stack members. This issue has been resolved.	–	Y	Y	–	–
CR00039760	**Port Authentication**	Previously, the command: `erase web-auth-https-file` did not correctly erase the certificate being used by the Web-Auth server. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039717	**SNMP**	Previously, an SNMP GET for an object in the dot1Q MIB could result in a memory leak if VLAN 4094 was configured. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039641	**IGMP**	Previously, if the downstream side of a IGMP proxy was configured before the upstream side, an unexpected system reboot could occur. This issue has been resolved.	Y	Y	Y	Y	Y

Level 3 (cont.)

CR	Module	Description	x900/x908	x610	x510	x210	SBx8100
CR00039568	**IPv6**	Previously, on rare occasions, where a switch was used in an IPv6 multicast network without configuring a VLAN with the command: `IPv6 enable` and there were other switches in the VLAN, it was possible for the switch to re-forward an MLD protocol packet back to an originating switch using the original MAC address. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039564	**SNMP**	Previously, when a switch was configured to use VLAN 4094, performing an SNMP GET for on object in the VLAN4094 dot1q MIB table would cause an unexpected system restart. This issue has been resolved	Y	Y	Y	Y	Y
CR00039952	**Layer 3 switching**	Previously, if a connected route matched another route (e.g. a static route or a route learnt by RIP), then if the connected route was removed by shutting down the egress interface, it would not be re-added to the hardware route table when the interface was re-enabled. This issue has been resolved.	–	Y	Y	–	–
CR00039568	**IPv6**	Previously, on rare occasions, where a switch was used in an IPv6 multicast network without configuring a VLAN with **IPv6 enable** and there were other switches in the VLAN, it was possible for the switch to re-forward an MLD protocol packet back to an originating switch using the original MAC address. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039641	**IGMP**	Previously, if the downstream side of a IGMP proxy was configured before the upstream side, an unexpected system reboot could occur. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039717	**SNMP**	Previously, an SNMP GET for an object in the dor1Q MIB could result in a memory leak if VLAN 4094 was configured. This issue has been resolved.	Y	Y	Y	Y	Y

Level 4

CR	Module	Description	x900/x908	x610	x510	x210	SBx8100
CR00039336	**Find Me**	Previously, the port LED on the x510-GPX switch would not be lit up by the command: `findme` This issue has been resolved.	–	–	Y	–	–
CR00039348	**DHCPv4**	Three issues have been resolved in the output of the command: `show ip dhcp binding` ■ With some timezone offset configurations, the **show ip dhcp binding** command would fail to show dynamic leases that have infinite expiry. ■ The **show ip dhcp binding** command would show dynamic infinite leases as having an expiry of "19 Jan 2038 03:14:06" Such leases are now shown with an expiry of "Infinite". ■ Expired leases with an expiry date with a single digit day of month were being shown in the **show ip dhcp binding** output. Such leases are now not shown.	Y	Y	Y	Y	Y
CR00039407	**802.1x**	Previously, when a switch was operating as an 802.1x authenticator, and had sent a maximum number of unanswered EAP-Request/Identity packets, and then received an EAPOL-Start, it would not send another EAP-Request/Identity immediately. Instead, it would wait for tx-period (default 30sec), before sending the EAP-Request/Identity. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039490	**Port Configuration**	x510 with SFP support. Previously, after fast insertion and removal of an SFP there was a possibility of not being able to read or detect future SFP hot swaps. This issue has been resolved.	–	–	Y	–	–
CR00039491	**Port Configuration**	Previously, on very rare occasions, a fiber link could fail to come up on a SBx81GS24a. This issue has been resolved.	–	–	–	–	Y
CR00039635	**Pluggable Transceivers**	For AlliedWare Plus products with SFP support. Previously, SPF type AT-SPBD20-A/B would not display pluggable diagnostics information due to an incorrect checksum. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039845	**PoE**	Previously, on specific x510 PoE switches (x510-28GPX and x510-52GPX), the PoE LED was incorrectly displayed as duplex. This issue has been resolved.	–	–	Y	–	–

Issues Resolved in 5.4.3-1.4

AlliedWare Plus maintenance version 5.4.3-1.4 includes the resolved issues in the following tables.

No level 1 issues

Level 2

CR	Module	Description	x900/x908	x600	x610	x510	SBx8100
CR00038390	**VCStack**	Previously, on x908 and x900 stacks, if a late-joining stack member contained a version 2(v2) XEM (12Tv2, 12Sv2, 24T, 2XP, 2XS, etc.) there was a small chance that during the joining of the new stack member, broadcast packets received by other stack members on VLAN 1 might form a loop within the switching silicon of the XEM on the joining unit, which could result in a flood of duplicate packets being sent out other ports on the stack. This issue has been resolved - V2 XEMs will no longer induce broadcast packet storms during stack late-join.	Y	–	–	Y	–
CR00039028	**VCStack**	Previously, adding a static route that conflicted with the stack management network could cause associated repeating error messages such as *"Route x.x.x.x/x not added as it interferes with the Stack Management Network"* flooding the log if the VLAN was restarted. This issue has been resolved.	Y	Y	Y	Y	Y
CR00033963	**NTP**	Previously, configuring NTP on a stacked device could cause a warning message to be logged in error. This issue has been resolved.	Y	Y	Y	Y	Y
CR00036511	**IPv6**	Previously, when the port associations of a IPv6 tunnel source subnet VLAN was changed, the hardware tunnel entry was not updated appropriately. Therefore, Link Aggregation (Static) did not take effect immediately on a 6to4 tunnel until the configuration change was saved and the device was rebooted. This issue has been resolved. 6to4 tunnelling now properly supports these dynamic configuration changes.	Y	Y	Y	Y	Y
CR00036541	**OSPFv6**	Previously, OSPFv6 would fail to redistribute routes for metric and interface route-maps. This issue has been resolved.	Y	Y	Y	Y	Y
CR00036978	**IGMP Snooping**	Previously, a static multicast router port would be removed upon receiving an IGMP query message. This issue has been resolved.	Y	Y	Y	Y	Y

Level 2 (cont.)

CR	Module	Description	x900/x908	x600	x610	x510	SBx8100

CR00037178	**IGMP**	Previously, when unknown multicast traffic was being forwarded to a VLAN, the multicast traffic would flood the CPU rather than flooding all ports on that VLAN.
		This issue has been resolved.
		The following new command has been implemented:
		`platform stop-unreg-mc-flooding`
		`no platform stop-unreg-mc-flooding (default value)`
		The command stops the periodic flooding of unknown or unregistered multicast packets when the Group Membership interval timer expires and there are no subscribers to a multicast group.
		If there is multicast traffic in a VLAN without subscribers, multicast traffic temporarily floods out of the VLAN when the Group Membership interval timer expires, which happens when the switch does not get replies from Group Membership queries.
			–	Y	Y	–	–

CR00037625	**QoS**	Previously, the following command did not work on the AT- x510 switch: `remark new-cos internal` This issue has been resolved.	–	–	–	Y	–
CR00037702	**MLD Snooping**	Previously, if the startup configuration contained commands which disabled MLDSnooping, enabling MLDSnooping after the system started up would fail to fully enable it. This issue has been resolved.	Y	Y	Y	Y	Y
CR00038712	**Pluggable Transceivers**	Previously, some SFP+ modules were incorrectly being reported as having locked up. This issue has been resolved	–	–	–	–	Y
CR00038828	**Layer 2 Switching**	Previously incorrect MAC address entries were showing up on the GT40 MAC address table during learning or aging of MAC addresses. This issue has been resolved.	–	–	–	–	Y
CR00038950	**SMTP**	Previously, a memory leak could occur when a high rate of log email was generated. This issue has been resolved.	Y	Y	Y	Y	Y
CR00038981	**MLD Snooping**	Previously the x510 switch would incorrectly forward and/or would not flood MLD packets when the reserved IPv6 multicast group address was used. This issue has been resolved.	–	–	–	Y	–
CR00039080	**VCStack**	Previously, on an x908 stack, A system reboot could occur when new MAC addresses were learnt after a stack failover. This issue has been resolved.	–	–	–	–	Y

Level 2 (cont.)

CR	Module	Description	x900/x908	x600	x610	x510	SBx8100
CR00039132	**IGMP**	Previously, in certain limited circumstances, the **ip multicast forward-first-packet** command would not work as expected. This issue has been resolved.	Y	–	–	–	Y
CR00039163	**802.1x**	Previously, during 802.1X authentication, if the authenticator port received another EAP Response/ Identity, while waiting for a RADIUS response, it would abort the current authentication request, and start again. This cycle could continue indefinitely. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039261	**VLAN**	Previously, when a range of VLANs were created and tagged into a switchport with the command **switch trunk allow vlan all**, the VLANs would not be added correctly if one of the VLANs was disabled. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039300	**Policy-based routing**	Previously, if the interface used to resolve a next hop went down, then the default route was not being used to recursively resolve the next hop. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039332	**IGMP**	Previously, a system reboot would occur when static SSM mapped groups were joining and leaving. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039333	**ACL**	Previously, some switches would not match against the VLAN ID in ACLs, even though the hardware was capable of doing so. This issue has been resolved. ACLs can now optionally have a VLAN parameter, allowing them to only match traffic on a specified VLAN ID.	–	Y	Y	Y	–
CR00039341	**IGMP**	Previously, static IGMP group entries would not be propagated correctly to PIM when a switch started up. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039403	**802.1x**	Previously, when a combination of 802.1X EAPOL-Version 2 and AuthFailVLAN were used, the authenticator would not correctly respond to an authentication request from a supplicant that had just recently had a login failure. This issue has been resolved.	Y	Y	Y	Y	Y

Level 3

CR	Module	Description	x900/x908	x600	x610	x510	SBx8100
CR00038465	**ARP**	When an ARP entry on a switch transitioned from REACHABLE to PROBE and at the same time a gratuitous ARP request for the same address was received on a different port, the ARP entry would get stuck in the STALE state. This has been resolved by probing (sending ARP requests) to the device that sent the gratuitous ARP in this scenario.	–	–	–	–	Y
CR00034770	**Loop Detection**	Previously, the time displayed in "Last LDF Rx" in the output of **show loop-protection counters** was incorrect. This issue has been resolved.	Y	Y	Y	Y	Y
CR00038901	**IPv6**	Previously, the state of a tunnel interface would fail to be updated when the assigned port VLAN interface went up and down. This issue has been resolved.	Y	Y	Y	Y	Y
CR00038917	**IGMP**	Previously, IGMP would not start properly if IGMP snooping was disabled. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039006	**System**	Previously, packets arriving at the CPU were discarded after loop-protection link-down action and timeout were repeatedly executed. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039126	**BGPv4**	Previously, executing the BGP command **no network A.B.C.D** prior to configuring the network address would return an unclear error message. This issue has been resolved, with an appropriate error message "*Can't find specified network address*"	Y	Y	Y	Y	Y
CR00039200	**Pluggable Transceivers**	Previously, the SP10LRM SPF+ module would return an incorrect integer value as SFP+ 10LRM via SNMP rather than SFP+ 10LR This issue has been resolved.	–	–	–	Y	Y
CR00039222	**OSPFv2**	Previously, a combination of the transition from Active Master to Disabled Master on a stack and the graceful restart of OSPF would cause the removal of OSPF configuration. This issue as been resolved.	Y	Y	Y	Y	Y
CR00039232	**ATMF**	Previously, on rare occasions it was possible for the ATMF neighbour relationship between a rebooted node and a node connected via a downlink to not form correctly This issue has been resolved.	Y	–	–	Y	Y

Level 3 (cont.)

CR	Module	Description	x900/x908	x600	x610	x510	SBx8100
CR00039349	**RADIUS**	Previously, a small memory leak would occur upon successful web-authentication. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039362	**Command Shell**	Previously, disabling *default-information origination* on a device with this **already disabled** might result in incorrect default-information origination configuration. This issue has been resolved. Now, *default-information originate* is only available if manually configured. Which means, a user can only disable *default-information origination* if it is already enabled. This issue has been resolved.	Y	Y	Y	Y	Y

Level 4

CR	Module	Description	x900/x908	x600	x610	x510	SBx8100
CR00038884	**IPv6**	Previously, when a VLAN interface with IPv6 configured went from link down to link up, it would only start Duplicate Address Detection (DAD) on the link local address the first time. This issue has been resolved - DAD on the link local will now be started every time the link goes up.	Y	–	–	Y	Y
CR00038938	**Loop detection**	Previously, the length field value of an LDF frame was incorrect. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039101	**L2 Switching**	Previously, MAC addresses would not age when a **GP24** line card was used. This issue has been resolved.	–	–	–	–	Y

Issues Resolved in 5.4.3-0.2

AlliedWare Plus maintenance version 5.4.3-0.2 includes the resolved issues in the following tables.

No level 1 issues

Level 2

CR	Module	Description	x900/x908	x600	x610	x510	SBx8100
CR00039073	**ATMF**	Previously, when a VCS member that was part of an EPSR ring in an ATMF network was rebooted, a situation could occur that would prevent nodes further from the core rejoining the ATMF network. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039150	**VCStack**	Previously, adding an address to a VLAN that overlaps with the stack management subnet would result in an error, and the IP address was not added to the VLAN. That error has now been replaced by a warning, so that it is now possible to give a VLAN an IP subnet that overlaps with the stack management subnet (192.168.255.0/27). For example, addresses such as 192.0.0.1/8 may be applied to a VLAN. Note: If a device on the subnet 192.0.0.1/8 has an IP address falling inside 192.168.255.0/27, communication with that device will not work.	Y	Y	Y	Y	Y

Level 3

CR	Module	Description	x900/x908	x600	x610	x510	SBx8100
CR00039013	**Memory Monitoring**	Previously, a memory leak could occur when multicast routes were deleted. This issue has been resolved	–	–	–	–	Y
CR00039030	**Chassis Management**	Previously, on a SBx8100, when a high rate of traffic was received at the CPU via both network ports and management ports, it was possible for a CFC (Centralized Forwarding Card) failover to occur. This issue has been resolved.	–	–	–	–	Y
CR00039052	**ARP**	Previously, SBx8100 switches could not resolve the ARP for a device that had performed a silent station movement. This issue has been resolved.	–	–	–	–	Y

Level 3 (cont.)

CR00039172	**DHCPv6 Relay**	Previously, the DHCPv6 relay would exit immediately whenever it was started, or restarted (e.g. after a relay configuration change), when any of its server facing interfaces had no IPv6 address. This issue has been resolved.	Y	Y	Y	Y	Y
CR00039242	**VCStack**	Previously, if a stack failover event occurred, and the member that re-joined the stack as a backup unit contained a 12Sv2 XEM, then some SFP ports on the 12Sv2 XEM might not link-up. This issue has been resolved.	Y	–	–	–	Y

No level 4 issues