Software Maintenance Release Note

AlliedWare Plus™ Software Version 5.4.5-3.12

For SwitchBlade x8100, SwitchBlade x908, DC2552XS/L3, x930, x610, x510, IX5, x310, x230, and x210 Series Switches, AR2050V, AR3050S and AR4050S NGFWs, and VAA

Introduction

This document lists the issues addressed in AlliedWare Plus™ software maintenance version 5.4.5-3.12.

Read this maintenance release note in conjunction with the:

- *New and Enhanced Features in AlliedWare Plus 5.4.5 Major and Minor Versions*, Available from: http://alliedtelesis.com/support/documentation_keyword_new and enhanced.aspx, which describes new and enhanced features in this and previous minor and major versions since AlliedWare Plus 5.4.4.
- *Software Reference for AlliedWare Plus™ Operating System Version 5.4.5* for your switch.

Allied Telesis

Contents

Supported Models and Software File Names

Table 1: Supported switch models and software file names

Models	Series	Release File	Date	GUI file
x210-9GT x210-16GT x210-24GT	x210	x210-5.4.5-3.12.rel	Mar 2017	x210-gui_545_10.jar
x230-10GP x230-18GP x230-28GP	x230	x230-5.4.5-3.12.rel	Mar 2017	x230-gui_545_13.jar
x310-26FT x310-50FT x310-26FP x310-50FP	x310	x310-5.4.5-3.12.rel	Mar 2017	x310-gui_545_11.jar
IX5-28GPX	IX5	IX5-5.4.5-3.12.rel	Mar 2017	IX5-gui_545_07.jar
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510	x510-5.4.5-3.12.rel	Mar 2017	x510-gui_545_11.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	x610-5.4.5-3.12.rel	Mar 2017	x610-gui_545_11.jar
SwitchBlade x908*	SBx908	SBx908-5.4.5-3.12.rel	Mar 2017	SBx908-gui_545_10.jar
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	x930-5.4.5-3.12.rel	Mar 2017	x930-gui_545_13.jar
DC2552XS/L3		dc2500-5.4.5-3.12.rel	Mar 2017	n/a
SBx81CFC400 SBx81CFC960	SBx8100	SBx81CFC400-5.4.5-3.12.rel SBx81CFC960-5.4.5-3.12.rel	Mar 2017	SBx81CFC400_gui_545_10.jar SBx81CFC960_gui_545_11.jar

Table 1: Supported switch models and software file names

Models	Series	Release File	Date	GUI file
AR2050V	NGFW	AR2050V-5.4.5-3.12.rel	Mar 2017	n/a
AR3050S AR4050S		AR3050S-5.4.5-3.12.rel AR4050S-5.4.5-3.12.rel		
VAA (Virtual AMF Appliance)		vaa-5.4.5-3.12.iso	Mar 2017	n/a

Table 2: *Expansion modules for the SwitchBlade x908 from version 5.4.5

Product	Supported in version 5.4.5
XEM-1XP	No
XEM-2XP	Yes
XEM-2XS	Yes
XEM-2XT	Yes
XEM-12S	No
XEM-12T	No
XEM-12Sv2	Yes
XEM-12Tv2	Yes
XEM-24T	Yes

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

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. **Start the Java Control Panel, to enable Java within a browser .**

   On your PC, start the Java Control Panel by opening the Windows Control Panel from the Windows Start menu. Then enter Java Control Panel in the search field to display and open the Java Control Panel.

   Next, click on the 'Security' tab. Ensure the 'Enable Java content in the browser' checkbox is selected on this tab.

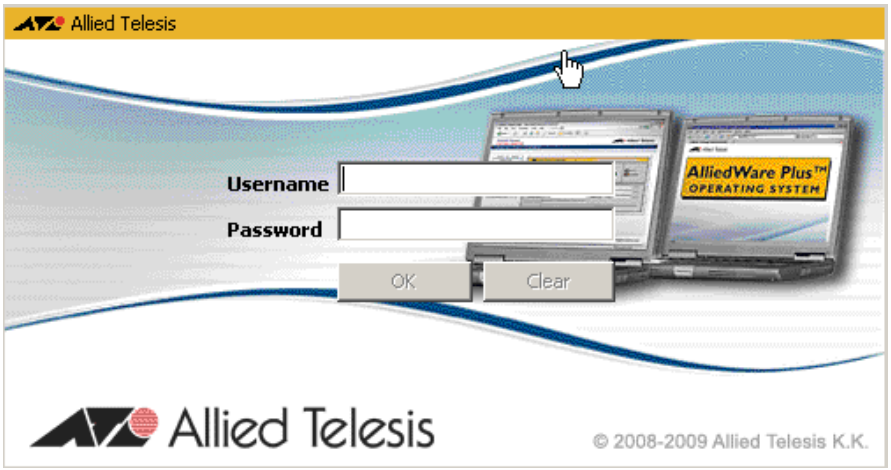
8. **Enter the URL in the Java Control Panel Exception Site List.**

   Click on the 'Edit Site List' button in the Java Control Panel dialog Security tab to enter a URL in the Exception Site List dialog. In the 'Exception Site List' dialog, enter the IP address you configured in Step 4, with a http:// prefix.

   After entering the URL click the Add button then click OK.

9. **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 5.4.5 *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 x210-5.4.5-3.12.rel
   ```

   On the x230 Series switches, use the command:

   ```
   awplus(config)#boot system x230-5.4.5-3.12.rel
   ```

   On the x310 Series switches, use the command:

   ```
   awplus(config)#boot system x310-5.4.5-3.12.rel
   ```

   On the x510 Series switches, use the command:

   ```
   awplus(config)#boot system x510-5.4.5-3.12.rel
   ```

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

   ```
   awplus(config)#boot system ix5-5.4.5-3.12.rel
   ```

   On the x610 Series switches, use the command:

   ```
   awplus(config)#boot system x610-5.4.5-3.12.rel
   ```

   On the SwitchBlade x908, use the command:

   ```
   awplus(config)#boot system SBx908-5.4.5-3.12.rel
   ```

   On the x930 Series switches, use the command:

   ```
   awplus(config)#boot system x930-5.4.5-3.12.rel
   ```

   On the DC2552XS/L3 switch, use the command:

   ```
   awplus(config)#boot system dc2500-5.4.5-3.12.rel
   ```

   On the SwitchBlade x8100 Series switches with a SBxCFC400 controller card installed, use the command:

```
awplus(config)#boot system SBx81CFC400-5.4.5-3.12.rel
```

On the SwitchBlade x8100 Series switches with a SBxCFC960 controller card installed, use the command:

```
awplus(config)#boot system SBx81CFC960-5.4.5-3.12.rel
```

On the ARxx series (NGFW) security appliances, use the commands for each product as follows:

```
awplus(config)#boot system AR2050v-5.4.5-3.12.rel
awplus(config)#boot system AR3050S-5.4.5-3.12.rel
awplus(config)#boot system AR4050S-5.4.5-3.12.rel
```

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

```
awplus#show boot
```

5. Reboot.

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

   ```
   awplus#reload
   ```

Upgrading the Software of a VAA

VAA does not need to be the same release as the products it is managing, however, as VAA is intended to be used as an AMF Master or Controller, it is recommended it be on the latest release. Before you begin, you will first need to upload a VAA ISO image to a data store on your ESXi server. For the complete set of instructions on uploading a VAA ISO image, please refer to the VMware vSphere 6.0 Documentation Centre.

To upgrade or downgrade the current installed image, you will need to change the current.iso software image in the virtual-machine configuration, then reboot the virtual-machine.

To change the current .iso software image:

- Power off the virtual-machine you wish to upgrade/downgrade.
- Edit the settings of the virtual-machine.
- Select CD/DVD Drive 1 item
- Ensure that **Connect at power on** check-box is ticked.
- Select the **Datastore ISO File** radio button.
- **Browse** for the desired VAA iso image.

Start the virtual machine, during boot you will see a menu that looks like this:

```
Alliedware+
Boot from CD
```

- Select the **Boot from CD** option.

You will only have 5 seconds to select "Boot from CD" before the boot continues with the previously installed release.

This will boot using the new .iso software image, and next time you login using the console you will be presented with the *"Install this release to disk? (y/n)"* option.

ISSU (In-Service Software Upgrade) on SBx8100 with CFC960

ISSU is available on standalone SBx8100 Series switches with dual CFC960 control cards, and on switches using VCStack Plus™ to create a single virtual unit out of two chassis (where each chassis has a pair of CFC960 control cards). ISSU allows you to upgrade the software release running on the CFCs with no disruption to network traffic passing through the chassis.

This maintenance release cannot be upgraded from any previous release using ISSU.

For each issue resolved on these platforms, the resolution will take effect as indicated when:

- CFCs upgraded: The issue will be resolved once all CFCs have rebooted and are running the same SW version.
- ISSU Complete: The issue will be resolved once all cards in the system are running the same SW version.

Please refer to the ISSU compatibility matrix below to determine ISSU release compatibility. C= Compatible, I = Incompatible.

		TO											
FROM	RELEASE	5.4.5-2.1	5.4.5-2.2	5.4.5-2.3	5.4.5-3.4	5.4.5-3.5	5.4.5-3.6	5.4.5-3.7	5.4.5-3.8	5.4.5-3.9	5.4.5-3.10	5.4.5-3.11	5.4.5-3.12
	5.4.5-2.1	C	C	I	I	I	I	I	I	I	I	I	I
	5.4.5-2.2			I	I	I	I	I	I	I	I	I	I
	5.4.5-2.3				I	I	I	I	I	I	I	I	I
	5.4.5-3.4					C	I	I	I	I	I	I	I
	5.4.5-3.5						C	I	I	I	I	I	I
	5.4.5-3.6							C	I	I	I	I	I
	5.4.5-3.7								C	I	I	I	I
	5.4.5-3.8									C	I	I	I
	5.4.5-3.9										C	I	I
	5.4.5-3.10											C	I
	5.4.5-3.11												C

Additional information

For more information about ISSU, see the *New and Enhanced Features in AlliedWare Plus 5.4.4 Major and Minor Versions. ISSU Introduction* and *ISSU Commands* in the *Software Release Note* for *AlliedWare Plus Version 5.4.4-1.1*. ISSU is not supported on other platforms.

You may also find the following How To Note useful:

- How to Use the In-Service Software Upgrade (ISSU) Feature

Enhancements in 5.4.5-3.12

The following enhancement has been made in this software version.

CR	Module	Description
ER-1089	**SNMP**	For: x210, x230, x310, IX5, x510, x610, x930, DC2500, SBx908, SBx81CFC400, SBx81CFC980, AR2010V, AR2050V, AR3050S, AR4050S With this software update, a new SNMP trap will be generated if an SNMP process is killed.

Enhancements in 5.4.5-3.7

The following enhancements have been made in this software version. Unless otherwise stated, these enhancements apply to all models.

CR	Module	Description

ER-1007	**IGMP**	With this software update, a user can now limit the number of IGMP group joins on any particular port.
		To configure the maximum number of IGMP groups on a port, use the following new command:
		`switchport igmp maximum-groups <1 - 65535>`
		`no switchport igmp maximum-groups`
		To remove the maximum IGMP group limit from a port, use the command:
		`no switchport igmp maximum-groups`
		By default, there is no maximum group limit set on a port.
		The following show commands are extended to display the current group counter value for a port:
		`show ip igmp snooping statistics interface <port-list>`
		`show ip igmp interface <port>`

ER-1046	**EPSR**	AR-Series switches, not AR-Series firewalls Switches only. With this software update, EPSR topologies with masters deployed on a common segment are now supported, but only if their secondary ports are not on the common segment.
ER-1089	**Logging**	With this software update, an SNMP notification (trap) can now be generated when the syslog-ng process dies.
ER-1090	**Logging**	With this software update, the **show log** command is only available for a user with privilege level 7 or above.

Enhancements in 5.4.5-3.5

The following enhancements have been made:

CR	Module	Description
ER-887	**ICMP**	x210, x230, x310, x510, x610, x930, IX5, DC2552XS/L3, x900, SBx908, SBx8100 CFC400, SBx8100 CFC960, AR2050, AR3050, AR4050, VAA With this software update, ICMP IPv4 and IPv6 messages can now be rate limited in order to prevent performance being affected by an overwhelming number of ICMP messages generated or processed by a switch, for example, in a worm attack.

ER-888	**ICMP**	x210, x230, x310, x510, x610, x930, IX5, DC2552XS/L3, x900, SBx908, SBx8100 CFC400, SBx8100 CFC960, AR2050, AR3050, AR4050, VAA
		With this software update, it is now possible to disable the generation of IPv4 and IPv6 ICMP Destination Unreachable messages in response to a packet that cannot be delivered to its destination for reasons other than congestion. This prevents an attacker from using destination unreachable messages to discover the topology of your network. If ICMP unreachable messages are disabled, any application that depends on them will not work. Traceroute, for example, does not work when ICMP unreachable messages are disabled.
		Command syntax:
		`ip unreachables`
		`no ip unreachables`
		`ipv6 unreachables`
		`no ipv6 unreachables`
		Default:
		ICMP destination unreachable messages are enabled by default
		Mode:
		Global Configuration.
		Example
		To **disable** ICMP unreachable messages on IPv6, use the commands:
		`awplus#configure terminal`
		`awplus(config)#no ipv6 unreachables`
		To **enable** ICMP unreachable, messages for IPv6, use the commands:
		`awplus# configure terminal`
		`awplus#(config) ipv6 unreachables`

Enhancements in 5.4.5-3.4

The following enhancements have been made:

CR	Module	Description
ER-839	**OpenVPN**	Products: AR2050. AR3050, AR4050 With this update, it is now possible to allow multiple iOS clients to connect via OpenVPN.
ER-848	**ARP**	Products: x210, x230, x310, x510, x610, x930, IX5, DC2552XS/L3, x900, SBx908, SBx8100 CFC400, SBx8100 CFC960, AR2050. AR3050, AR4050 With this update, a new feature has been added to allow ARP replies sent to a L2 broadcast destination MAC to be learnt by a AlliedWare Plus device. This feature is disabled by default and can be enabled by the command **arp-reply-bc-dmac.**
ER-851	**SNMP**	Products: x210, x230, x310, x510, x610, x930, IX5, DC2552XS/L3, x900, SBx908, SBx8100 CFC400, SBx8100 CFC960, AR2050. AR3050, AR4050 With this update, AlliedWare Plus MIBs can now support SMIv1 version MIB.
ER-891	**Stacking**	Products: x310, x510, x610, x930, IX5, DC2552XS/L3 With this update, an extra diagnostic logging has been added to detect resiliency link healthcheck packet corruption during transmission, if such a rare event should ever occur. Also on x510 and x930 stacks, silicon firmware has now been updated to prevent the corrupted packets looping around the resiliency link VLAN.

Enhancements in 5.4.5-2.3

The following enhancements have been made for all supported models, unless otherwise stated.

CR	Module	Description
ER-483	**Logging**	Logging now supports **exclude** filters for log messages in addition to the previously available **include** filters. See below.
ER-840	**NAT, ARP**	With this software update, a user is now able to specify addresses for which the device will respond to ARP requests, using the device's own MAC address. See **"Limited Local Proxy ARP (ER-840)" on page 19**

Exclude filters for log messages (ER-483)

Logging now supports **exclude** filters for log messages in addition to the previously available **include** filters.

- The user can enter a command to prevent certain log message from being sent to a certain log output.
- The command that creates such a filter (called an "exclude filter") can use any combination of existing log parameters, that is, **program**, **facility**, **level** and **sextet**.
- Exclude filters can be applied to the buffered log, permanent log, console log, host log, email log and terminal.
- All log messages will be filtered by existing log filters (called "include filter") first. Any message not matching the include filters will be thrown away. Messages that pass through the Include Filters will be filtered by the exclude filters, if any are configured. Any message matching the exclude filter(s) will be thrown away. Message left will be sent to their log destination.
- A counter of the number of messages filtered out by exclude filters has been added to the output of the **show log config** command.
- The exclude filter will not be implemented for event log, as it currently only logs ATMF topology events and these events has predefined log parameters.

New commands for:

```
log buffered exclude [level <level>]
   [program <program-name>] [facility <facility>]
   [msgtext <text-string>]

no log buffered exclude [level <level>]
   [program <program-name>] [facility <facility>]
   [msgtext <text-string>]



log permanent exclude [level <level>]
   [program <program-name>] [facility <facility>]
   [msgtext <text-string>]
```

```
no log permanent exclude [level <level>]
   [program <program-name>] [facility <facility>]
   [msgtext <text-string>]


log console exclude [level <level>]
   [program <program-name>] [facility <facility>]
   [msgtext <text-string>]

no log console exclude [level <level>]
   [program <program-name>] [facility <facility>]
   [msgtext <text-string>]


log monitor exclude [level <level>]
   [program <program-name>] [facility <facility>]
   [msgtext <text-string>]

no log monitor exclude [level <level>]
   [program <program-name>] [facility <facility>]
   [msgtext <text-string>]


log host <ip-addr> exclude [level <level>]
   [program <program-name>] [facility <facility>]
   [msgtext <text-string>]

no log host <ip-addr> exclude [level <level>]
   [program <program-name>] [facility <facility>]
   [msgtext <text-string>]


log email <email-address> exclude [level <level>]
   [program <program-name>] [facility <facility>]
   [msgtext <text-string>]

no log email <email-address> exclude [level <level>]
   [program <program-name>] [facility <facility>]
   [msgtext <text-string>]
```

Figure 35: Example output from **show log config**

```
awplus# show log config

Host 10.37.76.1:
Time offset .... +0:00
Offset type .... Local
Filters:
1 Level ..... notices
Program .... any
Facility ... any
Msg text ... any
Type ..... include
2 Level ..... any
Program .... any
Facility ... kern
Msg text ... any
Type ..... exclude
3 Level ..... any
Program .... imish
Facility ... any
Msg text ... any
Type ..... exclude
Statistics ..... 12584 messages received, 13 accepted, 33
excluded (2015 Dec 2 10:25:01)
Email joe.blogs@alliedtelesis.com:
Time offset .... +0:00
Offset type .... Local
Filters:
1 Level ..... notices
Program .... any
Facility ... any
Msg text ... any
Type ..... include
2 Level ..... any
Program .... any
Facility ... any
Msg text ... started
Type ..... exclude
3 Level ..... any
Program .... imish
Facility ... any
Msg text ... any
Type ..... exclude
Statistics ..... 12584 messages received, 8 accepted, 38
excluded (2015 Dec 2 10:25:01)
Meaning of the counters are:
12584 messages received before any filtering
8 appear in the log destination
38 have been dropped by the exclude filter.
...
```

Limited Local Proxy ARP (ER-840)

Limited Local Proxy ARP is a feature to support Static NAT configurations where the public address in the NAT configuration is not an address that is configured as an interface address on the device. On Ethernet interfaces the device needs to respond to ARP requests for the public address so that it will then receive packets targeted at that address. This is especially useful where a number of 1-1 NAT configurations exist and each public address falls within

the subnet of the public interface. With the feature enabled on the public interface and suitable addresses specified, the device will respond to ARP requests for those addresses, as long as the addresses are routed out the interface the ARP requests are received on. The device responds with it's own MAC address.

With this software update, a user is now able to specify addresses for which the device will respond to ARP requests, using the device's own MAC address. Such replies will be made when the target IP address is reachable via the same interface on which the ARP request is received. This is the same behaviour as the existing Local Proxy ARP feature but for a user-specified set of addresses.

ip limited-local-proxy-arp

Description Sets an interface into a mode where the device will respond to ARP requests for a specified set of IP addresses if those addresses are reachable via the interface.

The behaviour is the same as the existing **ip local-proxy-arp** command, except that the behaviour only occurs with addresses that are specified via the new **local-proxy-arp** command

Syntax ip limited-local-proxy-arp

Mode Interface mode

Default Off by default.

Example To enable the device to be able to make ARP responses to ARP requests for specified addresses, when the ARP requests are received on interface eth1 and that addresses are routed out that interface, use the following commands:

```
awplus(config)#interface eth1
```

```
awplus(config-if)#ip limited-local-proxy-arp
```

Default Off by default

Related commands local-proxy-arp

local-proxy-arp

Specifies a subnet of IPv4 addresses for which the device should respond to ARP requests when the "Limited Local Proxy ARP" feature is enabled on an interface.

Description Specifies a subnet of IPv4 addresses for which the device should respond to ARP requests when the "Limited Local Proxy ARP" feature is enabled on an interface. The behaviour is similar to "Local Proxy ARP", where the response is made if the target address is reachable via the interface the request was received on. The difference is that responses are on given for addresses in the subnet specified and any others instances of the command.

Syntax local-proxy-arp A.B.C.D/M

Parameters: A.B.C.D/M

An IPv4 address and mask length specifying a subnet of IP addresses for which the device should send ARP responses.

Mode Global Configuration mode

Default No local proxy arp is created by default.

Example To configure the device to respond to ARP requests for all addresses in the 172.22.200.0/24 subnet, when the ARP requests are received on interface eth1 and that subnet is routed out that interface, use the following commands:

```
awplus(config)#interface eth1

awplus(config-if)#ip limited-local-proxy-arp

awplus(config-if)#exit

awplus(config)#local-proxy-arp 172.22.200.0/24
```

Related commands `ip limited-local-proxy-arp`

Enhancements in 5.4.5-1.4

The following enhancements have been made for all supported models, unless otherwise stated.

ER-506	**Loop Protection**	Previously, when log messages were generated by Loop Protection disabling a port or MAC learning the diagnostic message only gave the ifindex of the port concerned, with x210, x310, x510, x930 switches not logging any learning disable/re-enable events. With this enhancement, the thrash loop protection log messages now detail the MAC and VLAN which instigates the event along with the port name affected and x210, x310, x510, x930 switches will log whenever learning is disabled or re-enabled ISSU: Effective when CFCs upgraded.
ER-659	**QoS**	x930 only. This enhancement addresses the following issues: ? Previously, the 'remark new-cos internal/both' command changed the CPU queue for remarked packets to the 'new-cos'. Now all remarked packets use CPU queue 0. ? Previously, **match dscp 0** was matching on L2 traffic, which was incorrect because DSCP is part of the L3 header. This issue has been resolved. ? Previously, QoS rules had a higher priority than hardware ACLs. Now ACLs have the highest priority.

Enhancements in 5.4.5-1.3

The following enhancements have been made for all supported models, unless otherwise stated.

CR	Module	Description
ER-278	**VRRP**	Previously, VRRPv3 on AlliedWare Plus was limited to 32 IPv4 VRRP instances, and 32 IPv6 VRRP instances. This has now been increased to a maximum of 255 VRRP instances, regardless if they are IPV4 or IPv6, or a combination of both IPv4 and IPv6 VRRP instances.
	Policy-based Routing	This software update enables PBR routing on SBx8100 series, limited to only 128 PBR routes. This 128 route limitation is the same limitation that already applies to all existing switches that support PBR.

Enhancements in 5.4.5-0.3

The following enhancements have been made for all supported models, unless otherwise stated.

CR	Module	Description
ER-551	**PoE**	With this software update, the default state for PoE RPS Boost Mode has been changed from Enabled to **Disabled** on the **x930**.

Issues Resolved in 5.4.5-3.12

This AlliedWare Plus maintenance version includes the resolved issues in the following table, ordered by feature (Module).

CR number format: A new issue tracking system is being introduced. The CRs in the new system use a new format (CR-5xxxx). The previous system used the format: CR000xxxx.

For the next while, both systems will be used and both formats may appear in these tables. When referring to CRs, use the full CR format, e.g. CR-5xxxx.

CR	Module	Description	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050V	AR3050S/AR4050S	AMF Cloud
CR--55327	**802.1x**	Previously, a supplicant that was connected to a switch via MAC-based authentication would only be successfully authenticated once. If the MAC authentication failed, then the supplicant could fail to be re-authenticated unless the **clear mac** or **dot1x init** command was issued. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–
CR-56293	**802.1x**	Previously, in a port configuration with **auth dynamic-vlan-creation type multi** configured, hitting the limit of the number of times of authorisation and un-authorisation would stop packets being forwarded on x903 variant switches. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–	–	–
CR-56377	**802.1x**	Previously, the interface reference counter could increase incorrectly after port authentication events. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-55222	**802.1x** **Unified Wireless Controller**	Previously, the WMD process would restart unexpectedly when it failed to access a secondary RADIUS server. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	Y	–	–	–	Y	–	–	–
CR-56049	**ACL** **DHCP Snooping**	Previously, the DHCP Snooping database would not be correctly written to non volatile memory on x210 and x230 variant switches. This issue has been resolved.	Y	Y	–	–	–	–	–	–	–	–	–	–	–	–
CR-55191	**Anti-virus**	With this software update, Antivirus will now handle long running HTTP connections more efficiently. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-56062	**ARP Neighbor Discovery**	Previously, IPv4 ARP and IPv6 ND entries that used port-groups or flood to a VLAN, would not be correctly synchronized across stack members during a stack failover. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–
CR-56168	**BGP**	Previously, when BGP password authentication was configured on an AR-Series Firewall, the BGP session with its peer would not be successfully established. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–
CR-55250	**Bootup**	Previously, it was possible for continuous reboot prevention to fail to detect process failures. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	–	Y	Y	Y	Y	Y	Y	Y	–	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-56201	**CPU**	Previously, the average CPU utilisation output of the **show CPU** command would display abnormally high values if the device was running for a prolong period of time. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-55278	**DPI** **Firewall**	Previously, if there were DNS changes while under excessive load, it could cause Antivirus or Web Control to block all HTTP traffic. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-56294	**Environmental Monitoring**	Previously, upon boot up, the initial fan speed was below the minimum documented fan speed of 4700 RPM. With this software update, the initial fan speed is now set to 5500 RPM, which is a higher value than the minimum documented speed. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–	–	–
CR-56300	**EPSR**	Previously, when adding a data VLAN to an EPSR domain on a stacked switch, the VLAN would fail to be blocked. This issue has been resolved.	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-55406	**Firewall**	Previously, changing the configuration of an entity used in a firewall rule would not trigger an update of the rule. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-56272	**Firewall NAT**	Previously, when using the WebAPI to configure a Firewall NAT rule, it was possible to create a **portfwd rule** in the running config that was invalid. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–

CR	Module	Description	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-54640	**Flow Control**	Previously, back pressure and flow control on x510 variant switches did not work. This issue has been resolved.	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-55385	**Flow Control**	Previously, when a port was configured with Pause "receive", it was not working correctly on x210 variant switches. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-55185	**IDS/IPS** **Web Control**	Previously, if an HTTP request for the same URL from two different clients occurred at the same time, and that URL was not in the Web Control cache, then once the URL was categorised, the cache could become corrupted. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-55249	**IPv4**	Previously, the **dot1q ETH** sub-interfaces could occasionally fail to forward traffic. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–
CR-55901	**IPv4**	Previously, when a VLAN was configured to be 'shutdown' after the first port in that VLAN was linked up, the switch would incorrectly add an interface route to the hardware table, resulting in high CPU load. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–
CR-55820	**Logging**	Previously, parity error messages were being logged every 5 minutes. However, this was not affecting the functionality and performance of the switch. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-56140	**NTP**	Previously, the hardware clock was not always synchronised correctly with NTP time. This issue has been resolved.	Y	–	Y	–	Y	–	–	–	–	–	–	Y	Y	–

CR	Module	Description	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-55466	**Ping Polling**	Previously, on a stack, traffic generated on the CPU of the stack master would egress on the queue assigned to that type of traffic (i.e. queues 4 to 6). However, if the egress port was on one of the stack slaves, then the packets would actually egress on queue 2. With this software update, the traffic generated on a stack master permanently egresses on queue 4. If the egress port is on the stack slave and if the egress port is on the master, then it will maintain queue 4 to 6. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-56188	**Pluggable Transceivers**	Previously, certain QSFP DAC cables were not being detected correctly by the system. This issue has been resolved.	–	–	–	Y	Y	–	–	Y	–	Y	Y	–	–	–
CR-55255	**PoE**	Previously, the **disable service power-inline** command did not work on PoE switches. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	Y	Y	–	Y	Y	–	–	Y	Y	–	–	–
CR-56299	**PoE**	Previously, PoE devices would sometimes be disconnected by an unexpected PoE hardware restart. This issue has been resolved.	–	–	–	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-55067	**Policy-based Routing**	Previously, when a multiple recursive PBR was configured, the policy-rule TCAM entry in hardware would fail to update correctly, resulting in PBR traffic being redirected to the CPU. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-54545	**Port Configuration**	Previously, a fibre SFP in an SFP+ port would not work correctly after disconnecting and reconnecting its cable. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	Y	Y	–	Y	–	–	–	Y	–	–	–
CR-56006	**Port Configuration**	Previously, manual 10M speed and full duplex would not be accepted in x930 variant switches when the SFP and copper ports were not populated. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–	–	–
CR-55661	**Provisioning**	Previously, when a VRRP role was changed from backup to master, traffic could occasionally be routed to the CPU rather than forwarded by hardware. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-54620	**QoS-hardware**	Previously, if QoS twin-rate policers were used, yellow marked packets were incorrectly being dropped. This issue has been resolved.	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-56112	**RMON**	Previously, the AlarmValue and AlarmThreshold were incorrectly displayed as "0" in the SNMP trap. This issue has been resolved.	–	Y	–	–	–	–	–	–	–	–	–	–	–	–
CR-55913	**Stacking**	Previously, if a member of a stack was restarted from the CLI, there was a chance that one of the stack ports would fail to re-join the stack. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	Y	–	–	–	Y	–	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-55672	**Stacking** **Port Authentication** **Static Aggregation**	Previously, port authentication would not work on a port configured with link-aggregation. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-56296	**xSTP**	Previously, adding a VLAN into an existing MST instance could result in a broadcast storm. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-56076	**Switch**	Previously, if a VLAN was shut down and then the command **no shutdown** was used, then the hardware entries for connected routes would be added even if no ports on the VLAN were up. This could result in traffic being forwarded by the CPU, thus causing high CPU utilisation. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-55821	**System**	Previously, an uncorrected "L3 Parity Error" would result in the "parity log" error to be displayed continuously, unnecessarily filling up the log table. This type of parity error can be automatically corrected and the issue has been resolved without flooding the log table.	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-56327	**System**	Previously, a parity error on the register table used for multicast would not be corrected on x510 variant switches. This issue has been resolved.	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-55342	**Triggers**	Previously, there was a short delay before linkdown triggers would execute their associated script(s). This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	Y	–	–	–	–	–	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-56393	**Triggers**	Previously, a protocol module disconnection could result in a failure of a link-down trigger to activate. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-55109	**VCStack Trigger**	Previously, when triggers were used to change configuration on a stack, it was possible for part of the configuration to be lost in an failover event. Any OSPF, RIP and BGP configuration would be affected. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–
CR-55605	**VRRP**	Previously, when the VRRP role was changed from backup to master, traffic could occasionally be routed to the CPU rather than being forwarded by hardware. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-54273	**Web Control**	Previously, a long running HTTP connection could potentially cause Web Control to halt all HTTP connections. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-55451	**Web Control**	With this software update, Web Control now consumes less system resources whilst blocking an HTTP POST.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–

Issues Resolved in 5.4.5-3.11

This AlliedWare Plus maintenance version includes the resolved issues in the following table, ordered by feature (Module).

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050/AR4050
CR-56062	**ARP Neighbor Discovery**	Previously, IPv4 ARP and IPV6 ND entries that used port-groups or flood to a VLAN would not be correctly synchronised across stack members during a stack failover. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	–	Y	Y	Y	Y	Y	Y	Y	–	–
CR-56188	**Pluggable Transceivers**	Previously, certain QSFP DAC cables would not be detected correctly on an x930 switch. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-54545	**Port Configuration**	Previously, a 1G fibre SFP on a SFP+ port on a x930 switch could fail to link up after disconnecting and re-connecting. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-56006	**Port Configuration**	Previously, a port speed command would not be accepted on a x930 switch if SFP and copper ports were not populated. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-55913	**Stacking**	Previously, if a member of a x930 stack was rebooted, there was a chance that one of the stack ports could become stuck in an inoperative state. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–	–

Issues Resolved in 5.4.5-3.10

This AlliedWare Plus maintenance version includes the resolved issues in the following table, ordered by feature.

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050/AR4050
CR-54620	QoS	Previously, if QoS twin-rate policers were used, packets marked as yellow would be incorrectly dropped. This issue has been resolved.	–	–	–	Y	Y	–	–	–	–	–	–	–	–

Issues Resolved in 5.4.5-3.9

This AlliedWare Plus maintenance version includes the resolved issues in the following table, ordered by feature.

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050/AR4050
CR-55605	**VRRP**	Previously, a VRRP role change from backup to master would occasionally cause packets to be routed via the CPU rather than in hardware, and hence severely impact the performance of the switch. This issue has been resolved.	–	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	–	Y

Issues Resolved in 5.4.5-3.8

This AlliedWare Plus maintenance version includes the resolved issues in the following table, ordered by feature.

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050/AR4050
CR-55109	**VCStack Trigger**	Previously, when triggers were used to change configuration on a stack, it was possible for part of the configuration to be lost in an failover event. Any OSPF, RIP and BGP configuration would be affected. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–

Issues Resolved in 5.4.5-3.7

This AlliedWare Plus maintenance version includes the resolved issues in the following table, ordered by feature.

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050/AR4050	AMF Cloud
CR-54392	**VCStack**	Previously, when a stack backup member rejoined the stack, it was possible that rejoining unit would restart unexpectedly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–
CR-54132	**AMF**	Previously, if an AMF virtual link down time was longer than the interval between link database updates being sent and less than the time taken for the AMF master to realise the link was down, then the node would miss all of the link database updates from the AMF master. As a result, the node would have an incorrect view of the other nodes in the AMF network. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-54633	**AMF**	Previously, after a stack reboot, AMF packets were not being correctly forwarded from a stack backup member to the stack master, resulting in an AMF network not forming correctly. This issue has been resolved.	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050/AR4050	AMF Cloud
CR-54669	**AMF**	Previously, a re-joining CFC would not form an AMF neighbour relationship with the Master CFC and consequently did not learn anything about AMF from the Master CFC. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–
CR-53339	**AMF**	Previously, when an AMF node was replaced and automatically recovered, it occasionally failed to communicate with the adjoining AMF node for recovery file retrieval, causing the recovery to fail. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–
CR-54357	**AMF**	Previously, the ‘no valid release license’ error message would be displayed at login on an AMF Cloud Master or Controller even though there was a proper license installed. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y
CR-54836	**CLI**	Previously, executing the command **boot system backup *.rel** repeatedly would cause unnecessary memory consumption. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-54806	**EPSR**	Previously, shutting down a single port on an aggregator on an EPSR ring caused the ring to flap. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050/AR4050	AMF Cloud
CR-54636	**Flow Control**	Previously, if *flowcontrol* was configured in the startup configuration for a 10G pluggable port, the configuration would not be applied. This issue has been resolved.	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-54438	**Hotswap**	Previously, the license mismatch error message would be displayed when an active CFC was replaced by another CFC that was running an older firmware version. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–
CR-54695	**IDS/IPS**	Previously, on an AR-Series firewall with IPS enabled, packets with the ICMP/UDP/TCP/IP checksums 0xFFFF would be incorrectly marked as invalid checksums, resulting in transmission delay for packets. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–
CR-53748	**IGMP**	Previously, static IGMP entries could not be successfully configured on ETH ports of the AR-Series firewalls. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–
CR-55041	**IGMP**	Previously, a switch configured with IGMP proxy would restart unexpectedly when multi-source IGMP entries on the downstream side expired. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050/AR4050	AMF Cloud
CR-54389	**IGMP**	Previously, repeated IGMP group join and leave events could cause a slow memory leak. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-54488	**IGMP, Multicast Routing**	Previously, a switch would unnecessarily log info-level messages like ‘Stopping STAT timer’ and ‘Starting STAT timer with 210 seconds’ when static IGMP groups were configured. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-54746	**IPsec, ISAKMP**	With this software update, IPSEC NAT-T is now interoperating between AR-Series firewalls running AlliedWare Plus and those running AlliedWare. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-54355	**IPv4**	Previously, executing the command **set ip next-hop** could result in an internal process restarting unexpectedly. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-55043	**Switch**	Previously, the policer metering entries were incorrectly initialized to default values when Storm Control was configured on a port. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050/AR4050	AMF Cloud
CR-53486	**Log**	Previously, when a burst of log messages were generated and were emailed out with the **log email** command, some of the emails created would have missing 'To:' or 'Subject:' fields. This resulted in 'failing to send' log messages being generated. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-54723	**NTP**	Previously, when the command **ntp source <*ip-address*>** was used, all subsequent NTP commands would fail to execute. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-53705	**OSPFv3**	Previously, adding an IPsec authentication on a VLAN interface with already established OSPFv3 neighbours would cause a 'Failed to write IPSec interface configuration' error message being logged, although the IPSec configuration had been successfully implemented. The error message was spurious. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	-	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050/AR4050	AMF Cloud
CR-52980	**OSPFv3, IPv6, Stacking**	Previously, there was a small chance that IPv6 routes leant by OSPFv3 could be installed without the link-local nexthop address set. This affected the traffic forwarding for all intra-area and AS external prefixes associated with that missing nexthop. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-54432	**PoE**	Previously, the PoE Firmware Updater on the SBx81GP24 Line card might fail to run a firmware update. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–
CR-53474	**Port Auth 802.1x**	Previously, an unexpected port authentication process restart due to, for example, a disconnected physical link, would result in incorrect operation of port authentication after the restart. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-55004	**Port Authentication**	Previously, neither the **clear arp-cache** command nor a port down event cleared all internal copies of the neighbor information, causing an inconsistency in the information available to users. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050/AR4050	AMF Cloud
CR-54518	**QoS (Hardware)**	Previously, on x210-series switches, an user was unable to attach a policy-map to a port. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-54553	**RIP**	Previously, the RIP metric was not updated correctly upon receiving a RIP update packet. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-54279	**SNMP**	Previously, the power supply alarm traps were not sent from backup members in a stack after a master fail over. This issue has been resolved.	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–
CR-54366	**Static Aggregation**	Previously, the command **show diagnostic channel-group** (run as part of **show tech support**) would result in link flaps on some SFP+ ports on the SBx8100 variant switches if the ports were part of an aggregator. This issue has been resolved.	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–
CR-54863	**System**	Previously, on x510 or x310 switches, under rare circumstances, the internal software watchdog process would not always produce a core-dump file when it detected an internal process lock up. This issue has been resolved.	–	–	Y	–	Y	–	–	–	–	–	–	–	–	–
CR-53549	**System**	Previously, under rare circumstances, removing a XEM from an SBx908 switch could cause an unexpected system restart. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	–	–	–	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050/AR4050	AMF Cloud
CR-54660	**System**	This software update includes resolution for the vulnerability listed under CVE-2016-4805, which affects the PPP feature. Before the resolution, the PPP driver might suffer memory corruption due to a use-after-free problem. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–
CR-54407	**System**	Previously, the device would send packets from the CPU via an incorrect CPU priority queue. This issue has been resolved.	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-55063	**Web Authentication**	Previously, WEB-AUTH login with username and password of over 64 characters would result in buffer overflow, causing the authentication process to restart unexpectedly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–
CR-54718	**Web Control**	Previously, an AlliedWare Plus router with the Web Control feature enabled would suffer from a memory leak under high HTTP load. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–

Issues Resolved in 5.4.5-3.6

This AlliedWare Plus maintenance version includes the resolved issues in the following table, ordered by feature.

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050	AR4050	VAA
CR-54349	**Provisioning**	This software update provides support for the Revision B XEM-12Tv2. The mapping of external port numbering in this revision of the XEM is different to the previous revision. Without this software change, to support the new port mapping, the wrong ports are displayed as "running" in the output of the **show interface brief** command. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–

Issues Resolved in 5.4.5-3.5

This AlliedWare Plus maintenance version includes the resolved issues in the following table, ordered by feature.

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050	AR4050	VAA
CR-53378	**ARP, Neighbor Discovery, STP**	Previously, if a switch had a static neighbour entry configured, a spanning tree topology change notification could result in the neighbour entry being incorrectly deleted. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–
CR-53614	**Bootup**	Previously, x210, IE200, x230, x310, x510, x610, x930 would fail to boot up in extremely rare cases. This issue has been resolved.	Y	Y	Y	–	Y	Y	Y	–	–	–	–	–	–	–	–
CR-53619	**CLI**	Previously, prior to 5.4.5-2.x releases, it was not possible to log in to a switch console if TACACS+ was used for both login authentication and enabling Privileged Exec mode. This issue has been resolved. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-53695	**LACP**	With this software upgrade, a warning message will be logged if member ports of an LACP aggregation link together with different port speeds. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR-53787	**Switching**	Previously, the **show platform port** command could take a long time to complete on a stack of x310, x510, x610 or x930 switches. This issue has been resolved.	–	–	Y	–	Y	Y	Y	–	–	–	–	–	–	–	–
CR-53962	**ARP** **Neighbor Discovery**	Previously, on an AT-x610 switch, the next hop table entry counter under the **show platform ip table** command displayed an incorrect value. This issue has been resolved.	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-54054	**IPv6**	Previously, an IPv6 address would not be re-applied after disabling and then re-enabling an interface by the **shutdown/no shutdown** command if the interface had the maximum IPv6 neighbours. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-54107	**RADIUS**	Previously, a VLAN could not be removed from a port if Web-authentication or MAC authentication was configured on that port. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-54139	**PoE**	Previously, if an AT-IX5-28GPX unit had two Power Supply Units installed in it, it would not deliver PoE power to powered devices that were connected to its network ports. This issue has been resolved.	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–
CR-54177	**PoE**	Previously, the PoE functionality was unintentionally removed from combo ports on AT-x610 series PoE devices. As a result, the AT-x610 series PoE devices were not marked as being PoE capable devices. This issue has been resolved.	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–

CR-54256	**SFlow**	Previously, when a switch was configured with sFLOW, an unexpected reboot could occur if the switching hardware was running close to full capacity. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y

Issues Resolved in 5.4.5-3.4

This AlliedWare Plus maintenance version includes the resolved issues in the following table, ordered by feature.

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050	AR4050	VAA
CR-52149	**802.1x**	Previously, rapid link up and down transitions of a switch port could cause the port to be incorrectly associated with the Guest VLAN. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-53661	**802.1x**	Previously, the HTTP redirect process would not be cleaned up after illegal connections. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-52598	**Aggregation-Static Switching**	Previously, the source MAC address of an ingress link-aggregated switch port on a router was incorrectly learnt on the switch port rather than on the link-aggregated port. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050	AR4050	VAA
CR-53615	**AMF**	Previously, the execution of a manual AMF backup on a device would not be allowed even if the device was configured as a master/controller and had external storage available. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	–
CR-53947	**AMF**	Previously, if commands for configuring zones were sent to AR-series firewalls via an AMF working set connection, the commands were not executed. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-53378	**ARP, Neighbor Discovery, STP**	Previously, if a switch had a static neighbour entry configured, a spanning tree topology change notification could result in the neighbour entry being incorrectly deleted. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–
CR-53715	**BGP**	Previously, if two eBGP peers were configured in a single AS, disconnecting one of the peers by bringing the interface down would cause the remaining peer to start flapping, resulting in an unstable BGP network. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050	AR4050	VAA
CR-53722	**BGP**	Previously, when BGP received a prefix update with an AS path of a moderate length that included ASN4 byte segments, the BGP process could restart unexpectedly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050	AR4050	VAA
CR-53775	**BGP**	With this update, several issues with **graceful-reset** for BGP have been resolved: 1. When the **clear ip bgp** command is used to clear a BGP neighbor, the device will now set the ***graceful restart on*** flag in the subsequent OPEN message. 2. The device will only assume the neighbor is gracefully restarting when it receives a Cease notification with error codes 6/0 or 6/6; now notifications with other error codes such as 4/0 will not cause the device to assume the neighbor is gracefully restarting. 3. If the device has assumed its neighbor is gracefully restarting, but the neighbor does not set the ***graceful restart on*** flag in their OPEN message, the device will no longer permanently remain in graceful restart helper mode, but will exit graceful restart helper mode when it receives End Of Rib from the neighbor. 4. For standard BGP graceful-restart, an optimization has been made so that if the device which is helping it's neighbor restart detects that the hold down timer for its neighbor has expired, it will immediately clear any stale routes learned from that neighbor and exit graceful restart. This allows the device to more quickly re-converge to a stable routing state. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050	AR4050	VAA
CR-54042	**BGP**	Previously, when BGP received an update containing an ASN4 path from a neighbor, a small amount of memory was consumed and never released. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-53730	**BGP** **OSPF**	Previously, BGP and OSPF graceful restart could sometimes be delayed by up to 10 minutes during a stack failover event, if device configuration changed due to a script being run simultaneously with the stack failover. This issue has been resolved, now simultaneous configuration via script and stack-failovers will not prevent BGP and OSPF from gracefully restarting. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–
CR-53556	**DHCP**	Previously, if an incoming DHCP packet did not match any of the configured DHCP pools, a log message would be generated stating that there were "***no free leases***". With this update, the log message is now stating "***no permitted pools***" under this circumstance. The message no longer appears in the log files but will be displayed on the console when "terminal monitor" is enabled. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-53767	**GRE, IPsec, L2TP**	Previously, dynamic peer IPSEC Tunnels would not work on L2TPv3 or GRE Protected Tunnels. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050	AR4050	VAA
CR-53582	**IPv6**	Previously, an x210, x230, x310, x510, x610 or x930 would fail to send "Packet Too Big" ICMP messages if the device tried to forward packets that were larger than the MTU of the outgoing interface. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–
CR-53608	**LACP**	Previously, on an AR-series Firewall, the command **show diagnostic channel-group** would result in errors being displayed. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-53313	**LACP Switch**	Previously, if a packet ingressed via a switch port that was a member of a link aggregation, the packet's source MAC address was incorrectly learnt on the switch port rather than on the link aggregation. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-52335	**LACP Switching**	Previously, the output of the command: **show mac address-table** displayed an incorrect port ID on AR-series Firewalls. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050	AR4050	VAA
CR-53493	**Logging**	Previously, if a very large number of log messages were recorded over a brief period, it was possible for the buffered log to fill up completely and not recover. This meant that any subsequent events that occurred on the device would not be recorded properly when using the command: **show log**. This problem was more likely to affect an SBx8100 or VCStack+ stack, as there is potential for a lot more log messages to be generated when there are more cards in the system. This issue has been resolved, when the buffered log becomes more than 90% full, the messages in the buffered log will now be automatically truncated to free up more space. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–
CR-53922	**Multicast**	Previously, when a multicast client sent a join for a multicast group to a switch operating as an IGMP Proxy, the client might receive a small number of "out of order" multicast packets. As a result, there could be a noticeable pixelation. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050	AR4050	VAA
CR-53565	**Multicast Forwarding**	Previously, missing fragments of multicast traffic could result in PIM failing to register the multicast groups. This issue has been resolved, now PIM can register these groups if the new command **ip multicast allow-register-fragments** is used. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–
CR-53527	**Open VPN, RADIUS**	Previously, a change of the configuration of the shared secret for a radius server being used for validating OpenVPN clients would not be passed through to the RADIUS client module correctly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-53790	**OpenVPN**	Previously, when a custom radius group was configured for validating OPenVPN clients, the OpenVPN tunnel would always say "Tunnel is not yet fully configured." This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-54040	**Pluggable Transceivers**	Previously, the revision E AT-SP10TW1 cables were incorrectly disallowed as stacking cables on x310, x510 and SBx8100 series switches. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	–	Y	–	–	–	–	Y	Y	–	–	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050	AR4050	VAA
CR-54098	**Pluggable Transceivers**	Previously, the output of **show system pluggable diagnostics** incorrectly transposed the "transmit power thresholds" and "receive power thresholds" for SFP and SFP+ modules. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–
CR-53739	**Port Authentication**	Previously, a switch could send out an "unknown" service type attribute when **auth radius send service-type** was configured. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-53704	**Port Configuration**	Previously, manually editing the configuration file and adding port ranges that did not exist could result in a boot up failure. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-53755	**QoS**	Previously, on a x930 switch, CPU originated traffic could incorrectly egress the switch on queue 2 even when the traffic was intended to use queue 4. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-53828	**QoS**	Previously, the command **no mls qos cpu-queue rx-rate-limit** would cause the default transmit queue limit to be overridden. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050	AR4050	VAA
CR-53651	**RIP Unicast Routing**	Previously, on an x230 switch, if a route's nexthop was not resolved (via ARP) the route would not be added to hardware correctly. It should have been added with the traffic sent to the CPU in order to resolve the ARP. This issue has been resolved.	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-53652	**SNMP**	This update adds the following SBx8100 power supplies, PWRSYS1/DC and PWRSYS2/AC, to the **at-boards mib**. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–
CR-53698	**SNMP**	Previously, the value of the MIB **object ifType** returned incorrect values for VLAN interfaces and tunnel interfaces. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-53872	**SNMP**	Previously, when an SNMP GET Request included multiple variable binding and at least one of the variables was a counter64 type, then the operation would fail. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-53838	**SSL**	With this update, OpenSSL is upgraded to the latest version to address vulnerabilities stated in CVE-2016-0701, CVE-2015-3197, and CVE-2015-4000. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050	AR4050	VAA
CR-53809	**Stacking**	Previously, if both stacking cables on an x930 switch were disconnected and reconnected again, the stack ports might fail to link up, causing the stack to not reform. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-53418	**System**	Previously, if a member of a static aggregation momentarily dropped immediately after coming up during boot, there was a small chance that the aggregation would be locked out, stopping all traffic passing through. This issue has been resolved. 545-3.4: ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-53516	**System**	This update fixes the vulnerability reported in CVE-2015-8215 - namely that IPv6 stack in Linux kernel versions before v4.0 did not validate attempts to change MTU values, thereby opening up possible DDoS attacks. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-53529	**Unicast Routing**	Previously, an AR-Series firewall could restart unexpectedly if under heavy load.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050	AR4050	VAA
CR-53502	**VTI System**	Previously, if an AR-series firewall received packets addresses to its local interface (lo) or that arrived via an ECMP route, it was possible that the reply may not have a source address that matched the destination address of the original packet. Instead it would sometimes choose the address that was configued on the egress interface. This issue has been resolved, so that the AR-series firewall will always reply with the address correct source address.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–

Issues Resolved in 5.4.5-2.3

Note that ISSU cannot be used to upgrade to this version.

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050	AR4050	VAA
CR-53538	**File System, User Management**	Previously, when a device was upgraded to either 5.4.5-2.1 or 5.4.5-2.2 from 5.4.5-1.x or an earlier release, and flash was full and the login authentication method was “local”, no users were able to log in. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-53483	**GUI**	Previously, when accessing the GUI on an AlliedWare Plus device, the user was required to log in twice. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–
CR-53497	**IGMP**	Previously, when all downstream ports of multicast groups went down during stack failover, the multicast forwarding information could get out of sync between stack members for a late joining member, resulting in the multicast traffic failing to be forwarded. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–
CR00042694	**IGMP**	Previously, clearing IGMP groups could result in a memory leak. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050	AR4050	VAA
CR-53582	**IPv6**	Previously, x230 and x310 switches would fail to send ICMPv6 Packets if they were larger than the egress interface MTU. This issue has been resolved.	–	Y	Y	–	–	–	–	–	–	–	–	–	–	–	–
CR-53572	**IPv6**	Previously, IPv6 on x230 and x310 series switches would not send ICMP Redirects properly when forwarding IPv6 packets from an interface out the same interface. This issue has been resolved.	–	Y	Y	–	–	–	–	–	–	–	–	–	–	–	–
CR-53507	**Static aggregation, VLAN**	Previously, when deleting rules from VLAN classifiers, if a port had multiple classifier rules assigned to it that referenced the same VLAN, the VLAN registration could either be prematurely deleted from the port or in some circumstances not deleted when it should have been. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-53418	**System**	Previously, a port that was a member of a static aggregator on an x210 switch would sometimes fail to link up at bootup, even though the port was connected to another active Ethernet port. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-52996	**ATMF, EPSR**	Previously, when AMF and EPSR were being configured on a switch, the connection of AMF link between the AMF master and AMF member would not recover after the AMF link type was changed. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050	AR4050	VAA
CR-53620	**Pluggable transceivers**	Previously, if a pluggable-based line card was used in bay 12 of the SBx8100 switch, it was not possible to get link up on ports for that card. The output from the **show system pluggable** command would show the pluggables associated with an incorrect chassis ID. This issue has been resolved.	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–

Issues Resolved in 5.4.5-2.2

This AlliedWare Plus maintenance version includes the resolved issues in the following table, ordered by feature.

CR	Module	Description	x210	x230	DC2552XS/L3	x310	x350	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050	AR4050
CR-53503	**System**	Previously, software version syncronization between two CFC400 units or two CFC960 units could occassionally fail. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–
CR-52366	**QoS**	Previously, with 100% utilization on ACL and QoS configured, a stack master would restart unexpectedly when the command **show platform classifier statistics utilization brief** was entered. The backup member in a VCStack would reboot after a master failover with 100% Qos and ACL utilization. This issue has been resolved.	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–
CR-53512	**System**	Previously, the write protect function was incorrectly enabled on the x230 switch SD card slot. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	x210	x230	DC2552XS/L3	x310	x350	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR3050	AR4050
CR-53330	**VLAN**	Previously, when a VLAN classifier was attached to an aggregator (via the member ports), and when the rule list in the classifier was changed either by adding or deleting the rules, then the VLAN membership of the aggregator was not being properly updated to reflect the new classifier rules. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–

Issues Resolved in 5.4.5-1.4

This AlliedWare Plus maintenance version includes the resolved issues in the following table, ordered by feature.

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52276	**802.1x**	Previously, HTTP redirect of Web authentication could cause a memory leak if a client tried to access it repeatedly. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	–	–
CR-52629	**802.1x, Switching**	Previously, Multiple Dynamic VLAN (MDV) would not work with port authentication on a x210 switch. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–	–
CR-52042	**802.1x VCStack**	Previously, roaming authentication was not possible on stacks if dynamic VLAN assignment was being used. This issue has been resolved.	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-53021	**ACL**	Previously, when setting an IPv6 access-list to be a management ACL and if the IPv6 address specified in the access-list was over 15 characters long, this access-list or filter in this access-list would not work correctly in the management ACL. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	–	–
CR-52239	**AMF**	Previously, it was possible for AMF neighbour relationships to go through several create and destroy cycles which in turn could lead to a storm on the AMF VLAN. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52597	**AMF**	Previously, AMF remote login could fail after a device has been reincarnated. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52867	**AMF, EPSR**	Previously, an EPSR topology change within an AMF network could put an AMF blocking port into a faulty state. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	–	–
CR-52093	**AMF** **VCStack**	Previously, in rare circumstances, the AMF process would exit unexpectedly after a stack master failover. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52339	**Antivirus, Deep Packet Inspection, Firewall, IDS/IPS, IP Reputation,**	Previously, the output from the tech-support command generated for the AR3050 and AR4050 did not contain all the details for the NGFW features. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-52903	**Board Management, Environment Monitoring, Hardware ISSU**	Previously, if the "SBxPWRSYS2" was present at boot up or inserted with no AC input connected, it could cause the SBx8100 switch to lock up, environmental monitoring to fail, or insertion of other cards to be missed. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	Y	Y	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-51954	**GUI**	Previously, when an HTTP "GET" request was received for "/gui/" and the "host:" line was not specified, the switch could send "400 Bad Request" in response. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	–	–
CR-53031	**HTTP service, User management**	Previously, attempting to enable **service http** on an AR3050 or AR4050 would open up a security risk because low privilege users did not have appropriate restrictions placed on them when accessing the device through the HTTPs interface. The GUI is not supported on AR3050 and AR4050 products with previous 5.4.5 and 5.4.5-1 releases, but the command **service http** was still present. This issue has been resolved —the **service http** command now reports an error and does not attempt to start the web server on AR3050 and AR4050 routers.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-51636	**IPSEC, PPP, RIP**	Previously, bringing an interface down and up would cause route entries no to be cleared out of memory properly, and some invalid entries being added, resulting in packets loss. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52550	**IPv6**	Previously, the global **ip redirect** command was not working as expected on a x510 or x930 switch family. This issue has been resolved. Now when the global **ip redirect** command is issued, all redirected packets will also be mirrored to the CPU correctly and will be processed accordingly.	–	–	–	Y	Y	–	Y	–	–	–	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52763	**IPv6, Logging**	Previously, a spurious error message would be logged after executing the command **show platform table ipv6**. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	Y	Y	Y	–	–
CR-52365	**Logging**	Previously, when NTP adjusted time backwards, "show log" would fail to operate. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	–	–
CR-52902	**Multicast Routing**	Previously, if a multicast group was learnt at a particular time during the late joining of a member to a stack, the event could result in unnecessary attempts to send multicast hello packets, resulting in a "send failed" error message appearing in the log. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	Y	–	Y	Y	–	Y	Y	Y	Y	Y
CR-52382	**Pluggable Transceivers**	Previously, some SFP media types were not recognized by the switch. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	–	–	Y	Y	–	Y	Y	Y	–	–
CR-52860	**Port authentication**	Previously, packets from unauthorised supplicants would occasionally be allowed to reach their destination by ARP resolution. This issue has been resolved.	Y	Y	Y	Y	Y	–	Y	–	–	–	–	–
CR-52909	**QoS**	Previously, the command **show mls qos interface port<port-number> queue-counters** did not count unicast traffic queued for the egress port on an x930 switch. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52829	**RADIUS**	Previously, "no nas 127.0.0.1" would still appear in the configuration even when the local RADIUS NAS entry was removed. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	–	–
CR-52847	**Removable media**	Previously, insertion of an SD/USB card on a backup stack member was not recognised by the ATMF software. This meant that after a failover the ATMF backup and synchronization software would fail because it was not aware that it had any external media. (This would not affect remote file servers and could be worked around by removing and re-inserting the SD/USB media.) This update correctly assesses the status of the SD/USB media with regards to ATMF backups and synchronization. This issue has been resolved. The device now correctly assesses the status of the SD/USB media with regards to ATMF backups and synchronization and the AMF backup function will operate accordingly. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	Y	Y	Y	Y	–	–
CR-52762	**RIP**	With this software update, an additional parameter **invalid-routes** is added to the command **clear ip rip routes**. This parameter clears the routes with metric 16, waiting to be cleared when the timer goes to 0. Command syntax: **clear ip rip route invalid routes** ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-53287	**Storm protection**	With this software update, the log messages for thrash limiting have been reworded. Previously they were in the format: `Thrash: Loop Protection has...` Now they are in the format: `Thrash-limiting: ...` ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-52919	**Switching**	With this software update, the memory corruption caused by the "show platform" command has been resolved ISSU: Effective when ISSU complete.	–	–	–	–	–	–		Y	Y	Y	–	–
CR-52312	**System, Unicast Forwarding - CPU**	Previously, when an interface was destroyed and recreated, this could result in invalid entries being installed into the routing table. As a result, traffic would not flow as expected. Previously, when a route with multiple nexthops (ECMP) was deleted, it was possible for not all nexthops to be removed from the hardware table. As a result, when a route with potentially different nexthops was reinstalled, the old nexthops would be used instead of the new ones. These issues have been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52401	**Unified Wireless Controller**	The default channel-bandwidth calculation has been updated to be based on the maximum allowable channel-bandwidth for the new mode, instead of using the old modes default bandwidth calculation. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	Y	Y	–	Y	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-53099	**VCStack**	Previously, on SBx8100 VCStack Plus stacks it was possible for a stack separation to occur when a card was rebooted and was rejoining the chassis stack. This could cause the stack Backup Member chassis to reboot. This problem was characterized by a log message similar to the following: EXFX[1234] DBG:exfx_stack_syncDataExport 427: Failed to export data FDB. This problem would only occur when the SBx8100 stack was flooding traffic at the CPU level, for example if MLD or IGMP snooping was enabled globally, but disabled on a VLAN. Or if loop-protection was enabled on the SBx8100 and on other switches in the network. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	Y	Y	–	–
CR-52896	**VCStack**	With this software update, Tyco DACs are added to the list of supported VCStack cables for the x310 switch.	–	–	Y	–	–	–	–	–	–	–	–	–
CR-52737	**VLAN**	Previously, when removing a VLAN classifier group from an interface, it incorrectly removed classifiers on other interfaces as well. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-52400	**VRRP**	Previously, directed broadcast packets could be duplicated on a VRRP master. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	Y	Y	Y	–	Y	Y	Y	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52932	**VRRP**	Previously, if a VRRP instance transitioned to "Master" and then transitioned back to "Backup-member" in a very quick succession (sub-second interval), the device might retain the virtual MAC address ownership, causing it to act as a forwarder for traffic to be routed by the VRRP master This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	Y	Y	–	–	Y	Y	Y	–	–

Issues Resolved in 5.4.5-1.3

This AlliedWare Plus maintenance version includes the resolved issues in the following table, ordered by feature.

Note: This release does not support ISSU.

CR	Module	Description	x210	x230	x310	x350	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52042	**802.1x** **VCStack**	Previously, roaming authentication was not possible on stacks if dynamic VLAN assignment was being used. This issue has been resolved.	–	–	Y	–	Y	Y	Y	Y	Y	Y	Y	–	–
CR-52824	**ACL, DHCP Snooping**	Previously, the static source address binding for a DHCP snooping ACL was not updated onto non-master stack members during stack bootup. As a result, the traffic from the static binding host could be dropped. This issue has been resolved.	–	–	Y	–	Y	Y	Y	Y	–	–	–	–	–
CR-52464	**AMF**	Previously, a SBxCFC960 controller card could restart unexpectedly if the configuration of an AMF controller was removed and then re-added. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	–
CR-52093	**AMF** **VCStack**	Previously, in rare circumstances, the AMF process would exit unexpectedly after a stack master failover. This issue has been resolved.	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Description	x210	x230	x310	x350	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52797	**ARP Neighbor Discovery**	Previously, the output for the **show arp** command would incorrectly display as **flood** even if the ARP was already resolved for a multicast MAC address. This issue has been resolved.	Y	Y	Y	–	Y	Y	Y	Y	–	–	–	–	–
CR-52740	**Bridge**	Previously, when bridging was used on an AlliedWare Plus router with more than two interfaces in the bridge, one of them being a VLAN interface, broadcast packets could be forwarded to some interfaces with incorrect source and destination MAC addresses. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-52159	**DHCP Snooping**	Previously, when using the "vlantriplet" option for the circuit-ID for DHCP Snooping option 82 on an SBx8100 chassis, the value was incorrect. For example, for port 1.8.1 the value would be 08000100 instead of the expected 01080100. This issue has been resolved. If the current DHCP server or NMS configuration is using the previous incorrect values generated by an SBx8100 switch with the "vlantriplet" option configured, the server configuration will need to be updated to support the correct values with this release.	–	–	–	–	–	–	–	–	–	Y	Y	–	–
CR-52514	**Enviro Monitoring**	Previously on a SBx8100 switch, a single low fan tray temperature sensor reading would slow down all the fans in the chassis to their minimal speed. This issue has been resolved and the fans will only run at minimal speed when all three temperature sensors report a low read-out.	–	–	–	–	–	–	–	–	–	Y	Y	–	–

CR	Module	Description	x210	x230	x310	x350	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52769	**IGMP, MLD, VRF-lite**	Previously, a specific configuration and series of commands using VRF, VLANs and aggregators could result in corrupted multicast-related show output or an unexpected restart of the device. This issue has been resolved.	–	–	–	–	–	–	Y	Y	Y	–	Y	–	–
CR-52780	**IPv4**	With this software update, the output of the command **show platform table ip** will now include an **LTT** (Lookup Translation Table) column on a SBx908 switch.	–	–	–	–	–	–	–	–	Y	–	–	–	–
CR-52550	**IPv6**	Previously, the global **ip redirect** command was not working as expected on a x510 or x930 switch family. This issue has been resolved. Now when the global **ip redirect** command is issued, all redirected packets will also be mirrored to the CPU correctly and will be processed accordingly.	–	–	–	–	Y	Y	–	Y	–	–	–	–	–
CR-52902	**Multicast Routing**	Previously, if a multicast group was learnt at a particular time during the late joining of a member to a stack, the event could result in unnecessary attempts to send multicast hello packets, resulting in a “send failed” error message appearing in the log. This issue has been resolved.	–	–	Y	–	–	Y	Y	–	Y	Y	Y	Y	Y
CR-52251	**Multicast routing** **VLAN**	Previously, if subnet-VLAN classifiers were used with fully populated multicast routing tables, then the subnet-VLAN classification would fail to work. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	Y	Y	–	–

CR	Module	Description	x210	x230	x310	x350	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52835	**Port Auth**	Previously, IP traffic was software routed to an authenticated port, resulting in high CPU utilisation. This issue has been resolved, so the traffic is now routed (L3 switched) in hardware.	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	–	–
CR-52911	**Port Config**	Previously, packets would be discarded incorrectly by an x210 switch on a port linked up in half-duplex mode. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–	–	–
CR-52712	**RIP**	Previously, when RIP was configured to redistribute connected routes, and it received a route from a neighbor that had an identical destination subnet and next-hop as a connected route it had redistributed, the learnt route would replace the redistributed route in RIP table. If the learnt route was eventually withdrawn with a metric of 16, the redistributed route would never be re-added. This issue has been resolved. RIP will now keep redistributed routes in its table, and identical routes received from neighbors will be added as additional paths (visible via the command **show ip rip database full**') instead of over-writing the redistributed route. When the learnt route becomes unreachable with metric 16, the redistributed connected route will remain in RIP's RIB, undisturbed.	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52337	**SNMP**	Previously, SNMP traps sent from a CFC used the stack member ID, whereas the node ID should have been used. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	Y

CR	Module	Description	x210	x230	x310	x350	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52488	**SNMP**	Previously, there was a security issue whereby a switch would still respond to SNMPv3 requests even when the corresponding SNMPv3 user was deleted. This issue has been resolved.	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52481	**SSL**	With this software update, SSL has been updated to protect against potential security vulnerabilities identified by the following CERT advisories: CVE-2015-4000 CVE-2015-1793 CVE-2015-1792 CVE-2015-1791 CVE-2015-1790 CVE-2015-1788	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52161	**System**	With this software update, the vulnerability described in CERT advisory CVE-2015-1465 has been resolved.	Y	Y	Y	_	Y	Y	Y	Y	Y	Y	Y	–	–
CR-52852	**Unicast Forwarding**	Previously, if a "non-forwarding" Ethernet management interface on a switch unexpectedly received IP packets matching a static default route (where the static default route is associated with a completely unrelated L3 forwarding interface), and the matching IP packets were received before the default route had been used for routing packets originating from forwarding interfaces, then static default route was rendered un-useable. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Description	x210	x230	x310	x350	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52401	**Unified Wireless Controller**	The default channel-bandwidth calculation has been updated to be based on the maximum allowable channel-bandwidth for the new mode, instead of using the old modes default bandwidth calculation.	–	–	–	–	–	–	–	Y	Y	–	Y	–	–
CR-52822	**User Management**	Previously, there were some inconsistencies in the behaviour of a switch when a user used the “enable” command if the user was below privilege level 15 and no password was configured for level 15 privilege. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52468	**VCStack**	Previously, it was possible for a stack member to falsely detect a duplicate master situation, resulting in an unnecessary reboot of the whole stack. This issue has been resolved.	–	–	Y	–	Y	Y	Y	Y	–	Y	Y	–	–
CR-52817	**VCStack**	Previously, the x930 switch could fail to recognise a particular type of Tyco stacking cable. This issue has been resolved.	–	–	–	–	–	–	–	Y	–	–	–	–	–
CR-52737	**VLAN**	Previously, when removing a VLAN classifier group from an interface, it incorrectly removed classifiers on other interfaces. This issue has been resolved.	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	–	–

Issues Resolved in 5.4.5-0.4

This AlliedWare Plus maintenance version includes the resolved issue in the following table, ordered by feature.

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52108	**AMF**	Previously, AMF automatic recovery relied on a physical or a virtual link between two devices and recovery over aggregated links was not supported. There was a time window (during the initialisation of the remote node when it activated its aggregated links) that the initiating device was unable to identify that they were aggregated links. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52228	**ARP** **Neighbor discovery**	Previously, the **arp-mac-disparity** command could cause the console to lockup. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-52242	**ARP** **Neighbor discovery**	Previously, when a stack failed over, it would incorrectly delete all multicast FDB entries - both static and dynamic entries. This issue has been resolved. Now a stack failover will just remove all dynamic multicast FDB entries. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	Y	Y	Y	–	–
CR-52112	**Deep Packet Inspection**	Previously, DPI sometimes would not identify applications in flows that consisted of only a few packets (e.g. DNS). This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52269	**Firewall**	Previously, in a given firewall zone, there was a limitation of 8 networks. The number of networks is now dynamically calculated. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-52271	**Firewall, NAT**	Previously, NAT rules would display incorrect firewall entries when a NAT rule and a firewall rule were configured simultaneously. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-52319	**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. ISSU: Effective when CFCs upgraded.	–	–	Y	Y	Y	Y	–	Y	Y	Y	–	–
CR-52260	**IPv6**	Previously, the NGFW would fail to send an ICMP error message if it encountered problems processing fragmented IPv6 packets. This issue has been resolved. Now ICMP errors are correctly generated when there is a problem with fragmented packets.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-52274	**IPv6**	Previously, the NGFW would occasionally fail to disable an IPv6 interface when it detected that the IPv6 address used by the interface was also used by another device in the network. This detection of already-used addresses is part of the DAD process and required by the RFC. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-50744	**MAC Thrashing**	Previously, a **mac-thrashing port down** action on a SBx8100 CFC960 could result in the restart of a line card. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	Y	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52251	**Multicast routing** **VLAN**	Previously, if subnet-VLAN classifiers were used with fully populated multicast routing tables, then the subnet-VLAN classification would fail. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	Y	Y	–	–
CR-51331	**NTP**	Some security vulnerabilities related to NTP have been resolved. (CERT Vulnerability Note VU#852879) ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52226	**SNMP**	Previously, when SNMP was configured on a NGFW router, unnecessary SNMP error messages would occur whenever the device was polled. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-52264	**Unified Wireless Controller**	x908 only. Previously, on a SBx908 with no supported XEMs, the wireless manager process could restart unexpectedly at bootup. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	–	–	–
CR-52298	**Unified Wireless Controller**	Previously, the command **no channel auto-eligible 132** could not be applied at device startup due to an incorrect configuration order. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	Y	Y	–	Y	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52299	**Unified Wireless Controller**	Previously, changing the channel-bandwidth of a unified wireless manager capable device resulted in inconsistency between the running configuration and the output of the **show wireless ap profile radio auto-eligible** command. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	Y	Y	–	Y	–	–
CR-52371	**Unified Wireless Controller**	Previously, the wireless manager could fail to operate after a CFC master failover. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	Y	–	–
CR-51585	**VLAN**	Previously, subnet-based VLAN classifiers did not work at all on x230 and x310 switches. This issue has been resolved.	–	Y	Y	–	–	–	–	–	–	–	–	–
CR-51900	**VLAN**	Previously, when a port with VLAN classification enabled was added to an aggregation, the aggregation would not be successfully added to the VLAN. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-51900	**VLAN**	Previously, the switch would fail to register MAC addresses into the FDB table on ports in a LAG on which a protocol VLAN had been configured. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	–	Y	Y	Y		

Issues Resolved in 5.4.5-0.3

This AlliedWare Plus maintenance version includes the resolved issue in the following table, ordered by feature.

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52108	**AMF**	Previously, AMF automatic recovery relied on a physical or a virtual link between two devices and recovery over aggregated links was not supported. There was a time window (during the initialisation of the remote node when it activated its aggregated links) that the initiating device was unable to identify that they were aggregated links. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52228	**ARP** **Neighbor discovery**	Previously, the **arp-mac-disparity** command could cause the console to lockup. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-52242	**ARP** **Neighbor discovery**	Previously, when a stack failed over, it would incorrectly delete all multicast FDB entries - both static and dynamic entries. This issue has been resolved. Now a stack failover will just remove all dynamic multicast FDB entries. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	Y	Y	Y	–	–
CR-52112	**Deep Packet Inspection**	Previously, DPI sometimes would not identify applications in flows that consisted of only a few packets (e.g. DNS). This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52269	**Firewall**	Previously, in a given firewall zone, there was a limitation of 8 networks. The number of networks is now dynamically calculated. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-52271	**Firewall, NAT**	Previously, NAT rules would display incorrect firewall entries when a NAT rule and a firewall rule were configured simultaneously. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-52319	**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. ISSU: Effective when CFCs upgraded.	–	–	Y	Y	Y	Y	–	Y	Y	Y	–	–
CR-52260	**IPv6**	Previously, the NGFW would fail to send an ICMP error message if it encountered problems processing fragmented IPv6 packets. This issue has been resolved. Now ICMP errors are correctly generated when there is a problem with fragmented packets.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-52274	**IPv6**	Previously, the NGFW would occasionally fail to disable an IPv6 interface when it detected that the IPv6 address used by the interface was also used by another device in the network. This detection of already-used addresses is part of the DAD process and required by the RFC. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-50744	**MAC Thrashing**	Previously, a **mac-thrashing port down** action on a SBx8100 CFC960 could result in the restart of a line card. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	Y	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52251	**Multicast routing** **VLAN**	Previously, if subnet-VLAN classifiers were used with fully populated multicast routing tables, then the subnet-VLAN classification would fail. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	Y	Y	–	–
CR-51331	**NTP**	Some security vulnerabilities related to NTP have been resolved. (CERT Vulnerability Note VU#852879) ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52226	**SNMP**	Previously, when SNMP was configured on a NGFW router, unnecessary SNMP error messages would occur whenever the device was polled. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-52264	**Unified Wireless Controller**	x908 only. Previously, on a SBx908 with no supported XEMs, the wireless manager process could restart unexpectedly at bootup. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	–	–	–
CR-52298	**Unified Wireless Controller**	Previously, the command **no channel auto-eligible 132** could not be applied at device startup due to an incorrect configuration order. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	Y	Y	–	Y	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52299	**Unified Wireless Controller**	Previously, changing the channel-bandwidth of a unified wireless manager capable device resulted in inconsistency between the running configuration and the output of the **show wireless ap profile radio auto-eligible** command. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	Y	Y	–	Y	–	–
CR-52371	**Unified Wireless Controller**	Previously, the wireless manager could fail to operate after a CFC master failover. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	Y	–	–
CR-51585	**VLAN**	Previously, subnet-based VLAN classifiers did not work at all on x230 and x310 switches. This issue has been resolved.	–	Y	Y	–	–	–	–	–	–	–	–	–
CR-51900	**VLAN**	Previously, when a port with VLAN classification enabled was added to an aggregation, the aggregation would not be successfully added to the VLAN. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-51900	**VLAN**	Previously, the switch would fail to register MAC addresses into the FDB table on ports in a LAG on which a protocol VLAN had been configured. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	–	Y	Y	Y		

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-51397	**AMF**	Previously, if a stack failed-over or had members added to it and an AMF working-set command involving the stack was issued, the console might lock up and the message *No such VR* would appear on the stack master console. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-51462	**AMF**	The ATMF backup process will backup as many devices as was possible for the available external memory. Previously, the process mistakenly ran until it exhausted the external memory, which then caused undesirable effects. This software update ensures that there is enough external memory for each device before continuing with the backup for that device. A check will be performed on all devices and logs indicating the exhaustion of memory will be generated. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-51865	**AMF**	Previously, an erroneous critical AMF error message: *user.crit MR2 ATMF[918]: ATMF local area id (120) does not match that set on MR2* would occasionally appear on remote area Masters. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	Y	Y	Y	Y	–	–
CR-51934	**AMF**	Previously, after a rolling reboot was successfully performed on a local master, the local master would become unreachable from the AMF controller core network even though it was reachable via IPv6. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	Y	Y	Y	Y	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52011	**AMF**	Previously, when executing the command **atmf distribute firmware** to update the firmware on routers, the incorrect software would be used for the update. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-52045	**AMF**	Previously, it was possible that after a VCS master failover on an AMF node, the node would fail to join a working-set. This issue has been resolved. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52141	**AMF**	Previously, on rare occasions after device startup, AMF would not function and the command **show atm detail** would show **Domain State: Init** and Management and Domain VIDs of 0. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52186	**AMF**	This software update improves encryption for ATMF areas (ATMF remote Masters and ATMF Controllers) which are supported from 5.4.5-0.1 release onwards. The change is not backwards compatible. If an ATMF Controller is running 5.4.5-0.1 and it is upgraded to 5.4.5-0.3, Remote ATMF Masters will need to be upgraded to 5.4.5-0.3 before areas will authenticate. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52199	**CLI**	Previously, if a device started with unknown commands in Interface Configuration mode, the use interface process would restart unexpectedly during startup. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR00042477	**DHCPv4**	Previously, unrecoverable parity errors might occur. This issue has been addressed to allow the switch to recover from parity errors.	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-51980	**Eth**	Previously, if duplex speed or polarity was set on an Ethernet port in the startup configuration, these settings would not take effect on an SBx908 or SBx81CFC400. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	Y	Y	Y	Y	–	–
CR-51637	**HA**	Previously, the high availability LED would not flash amber when an HA-VRRP device failed over due to circuit monitoring. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-52034	**HSL**	Previously, in extremely rare cases, a port down event which was the last port in a VLAN, could cause an unexpected restart due to an internal race condition. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	Y
CR-51960	**IP-Reputation Update manager**	Previously, in rare circumstances, the IP-Reputation update manager would update features that only had their provider set. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-52055	**IPsec**	Previously, running many IPSEC tunnels over a long period of time could result in unexpected reboot. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52113	**IPsec**	Previously, when there were many IPsec tunnels configured in the startup configuration that were all simultaneously trying to connect, some tunnels could end up with mismatching SPIs after startup during Security Association negotiation, resulting in encrypted traffic failing to pass through those tunnels. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-51978	**IPv6**	Previously, class-maps configured to match on DSCP or IP-PREC would correctly match IPv4 packets, but failed to match IPv6 packets. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-51978	**IPv6, QoS**	Previously, class maps configured to match on DSCP or IP-Precedence did not match IPv6 traffic. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	Y	Y	Y	–	Y	Y	Y	–	–
CR-52114	**IPV6, VRRP**	Previously, configuring an IPv6 address on a VLAN interface with VRRP, followed by removing the IPv4 address from that VLAN would cause a device to restart. This issue has been resolved. SSU: Effective when CFCs upgraded.	–	–	Y	Y	Y	Y	–	Y	Y	Y	–	–
CR-51896	**ISAKMP**	Previously, a small amount of memory was leaked when adding and deleting ISAKMP policies. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-51660	**L2TP**	Previously, when the device started up, it could take up to 5 minutes to establish communication over an L2TPv3 link. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR00042741	**Layer 3 switching**	Previously, a host connected to an isolated or community port on a secondary VLAN of a private VLAN was able to communicate with a host on a conventional VLAN configured on the same switch. This was however incorrect, as the purpose of secondary VLANs is to prevent the host port from directly communicating with any other port outside the private VLAN. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	Y	Y	Y	–	–
CR-51441	**MLD**	Previously, when an interface that was not configured for MLD received an MLD packet, a warning log: *NO MLD-IF for interface <name>* would be generated. With this software update, the MLD log message has been downgraded to INFO level. The error message can still be seen by enabling MLD debug: **debug MLD all**. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52081	**MLD** **RIPng**	Previously, MLD snooping was not correctly processing MLD packet received on switch ports that had previously received an IPv6 RIP packet. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-51979	**NGFW**	Previously, the TCP ports 3128 (proxy) and 111 (non-stacking targets) were responding to packets when they shouldn't have been doing so. This issue has been resolved - those ports are now blocked.	–	–	–	–	–	–	–	–	–	–	Y	Y

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52063	**NGFW**	Previously, both Antivirus and Deep Packet Inspection (DPI) features used the same address for marking packets. As a result, when both features were enabled, packets would be handled incorrectly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-52110	**NGFW**	Previously, the combination of Firewall, DPI, and traffic shaping features would not work as expected, as they were overwriting the same internal table resource. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-51579	**OSPF**	Previously, executing the command **clear ip ospf process** when the same OSPF networks were configured in multiple VRF instances would cause an unexpected error. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	Y	–	–	Y	–	–
CR-51950	**Ping-poll**	Previously, the ping-poll process would restart unexpectedly when an IPv6 address longer than 15 characters was used as the ping-poll target. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-51230	**Pluggable**	Previously, if an SFP was inserted into an SFP+ socket on an x930, a link would be established, but if the cable was subsequently removed and reconnected, the link would fail to re-establish. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52089	**Pluggable**	Previously, repeated linkup/linkdown events on a pluggable port of an x510 port could cause the port to start corrupting packets if it was operating at 100Mbps. This issue has been resolved.	–	–	–	Y	Y	Y	Y	–	–	–	–	–
CR-52104	**Port Auth**	Previously, an unexpected restart could occur when 1024 authenticated MAC addresses were cleared from the hardware table. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR00042753	**STP**	Previously, under some circumstances RSTP and MSTP would send, from designated ports, BPDUs that contained the bridge ID of the neighbouring device rather than its own bridge ID. This issue has been resolved. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00042477	**Swi**	Previously, on rare occasions, the switch would be affected by unrecovered parity errors. With an update to the switch chip driver, these parity errors are now automatically recovered. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-52167	**System**	Previously, after receiving approximately 4 billion multicast packets on a VLAN, the VLAN could be deleted unexpectedly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52062	**Traffic Shaping**	Previously, there was a problem with virtual-bandwidth not applying correctly to an interface. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52029	**Unified Wireless Controller**	There are two command variations: 1. For the command, **qos station-edca** ... ? The value range for parameter **aifs** is changed to <1-15> from <1-255>. ? The help string for it is changed from "*Enter valid time in milliseconds"* to *"Enter valid slot number*". 2. For the command, **qos ap-edca** ... ? The value range for parameter **aifs** is changed to <1-15> from <1-255>. ? The help string for it is changed from *"Enter valid time in milliseconds"* to *"Enter valid slot number"*. ? The value range for parameter **max-burst** is changed from <0-999900> to <0-999000> ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	Y	–	–	Y	–	–
CR-51915	**Update manager**	Previously, after executing the command **no <*feature*>** while the feature downloadable resource was being downloaded, subsequent **show resource** command output would show invalid information for the resource. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-52002	**Update manager**	Previously, error messages would be generated if *IP Reputation* and *Malware Protection* had their resources updated in a quick succession. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52053	**VCStack**	Previously, packets whose headers had been corrupted in a very specific manner could cause an internal packet storm in a VCStack Plus setup. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	Y	–	–
CR-52073	**VCStack**	Previously, when a VCStack member rejoined the stack, there was a small possibility that the stack would separate and a stack member could reboot unexpectedly. This issue has been resolved.	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–
CR-52053	**VCStack**	Previously, packets whose headers had been corrupted in a very specific manner could cause an internal packet storm in a VCStack setup. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	Y	Y	–	–
CR00042741	**VLAN**	Previously, a host on a secondary VLAN could communicate with a host on the conventional VLAN configured on the same switch. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	Y	Y	Y	–	–
CR-51476	**VRRP**	Previously, pinging a VRRP instance on a device where the instance was on a different subnet to the ping source would result in no ping reply being received. This issue has been resolved. ISSU: Effective when CFCs upgraded	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52114	**VRRP**	Previously, removing an IPv4 address on a VRRP interface configured with an IPv6 address could cause an unexpected restart. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-51476	**VRRP**	Previously, with VRRPv3, pinging a VRRP instance on a device where the instance was on a different subnet to the ping source would result in lost replies. This issue has been resolved. ISSU: Effective when CFCs upgraded	–	–	Y	Y	Y	Y	–	Y	Y	Y	–	–
CR-52019	**Web control**	Previously, Web Control was unable to classify HTTP requests by source interface. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y

Issues Resolved in 5.4.5-0.2

This AlliedWare Plus maintenance version includes the resolved issue in the following table, ordered by feature.

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR3050	AR4050
CR-52143	**Environment Monitoring**	Previously, an x930 with two power supplies installed would fail to generate a fault message if one of those supplies became faulty or was unplugged. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–