Software Maintenance Release Note

AlliedWare Plus Software Version 5.4.4-4.16

For SwitchBlade x8100, SwitchBlade x908, x900, x610, x510, IX5, x310, x230 and x210 Series Switches

Introduction

This document lists the issues addressed in AlliedWare Plus™ software maintenance version 5.4.4-4.16.

Read this maintenance release note in conjunction with the:

- *New and Enhanced Features in AlliedWare Plus 5.4.4 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 5.4.4* for your switch.

Contents

Introduction 1
Installing the GUI to your Switch using an SD Card or USB Device 3
Installing the GUI to your Switch via TFTP Server 5
Installing and Enabling this Version 7
Enhancements in 5.4.4-4.15 9
Enhancements in 5.4.4-4.13 10
Enhancements in 5.4.4-4.12 13
Enhancements in 5.4.4-4.11 14
Enhancements in 5.4.4-3.10 15
Enhancements in 5.4.4-3.9 16
Enhancements in 5.4.4-3.7 17
Issues Resolved in 5.4.4-4.16 19
Issues Resolved in 5.4.4-4.15 20
Issues Resolved in 5.4.4-4.14 25
Issues Resolved in 5.4.4-4.13 26
Issues Resolved in 5.4.4-4.12 28
Issues Resolved in 5.4.4-4.11 35
Issues Resolved in 5.4.4-3.10 37
Issues Resolved in 5.4.4-3.9 41
Issues Resolved in 5.4.4-3.7 43
Issues Resolved in 5.4.4-3.6 47
Issues Resolved in 5.4.4-3.5 49

Allied Telesis™

Supported switch models and software file names

Models	Series	Release File	Date	GUI file
x210 -9GT x210-16GT x210-24GT	x210	x210-5.4.4-4.16.rel	May 2017	x210-gui_544_08.jar
x230-10GP x230-18GP	x230	x230-5.4.4-4.16.rel	May 2017	x230-gui_544_03.jar
x310-26FT x310-50FT x310-26FP x310-50FP	x310	x310-5.4.4-4.16.rel	May 2017	x310-gui_544_08.jar
IX5-28GPX	IX5	IX5-5.4.4-4.16.rel	May 2017	IX5-gui_544_09.jar
x510-28GTX x510-28GPX x510-28GSX x510-52GTX x510-52GPX x510DP-52GTX	x510	x510-5.4.4-4.16.rel	May 2017	x510-gui_544_17.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	x610-5.4.4-4.16.rel	May 2017	x610-gui_544_07.jar
x900-12XT/S, x900-24XT, x900-24XS	x900	x900-5.4.4-4.16.rel	May 2017	x900-gui_544_10.jar
SwitchBlade x908	SBx908	SBx908-5.4.4-4.16.rel	May 2017	x900-gui_544_10.jar
SwitchBlade x8106 SwitchBlade x8112	SBx8100	SBx81CFC400-5.4.4-4.16.rel SBx81CFC960-5.4.4-4.16.rel	May 2017	SBx81CFC400_gui_544_09.jar SBx81CFC960_gui_544_05.jar

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

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.

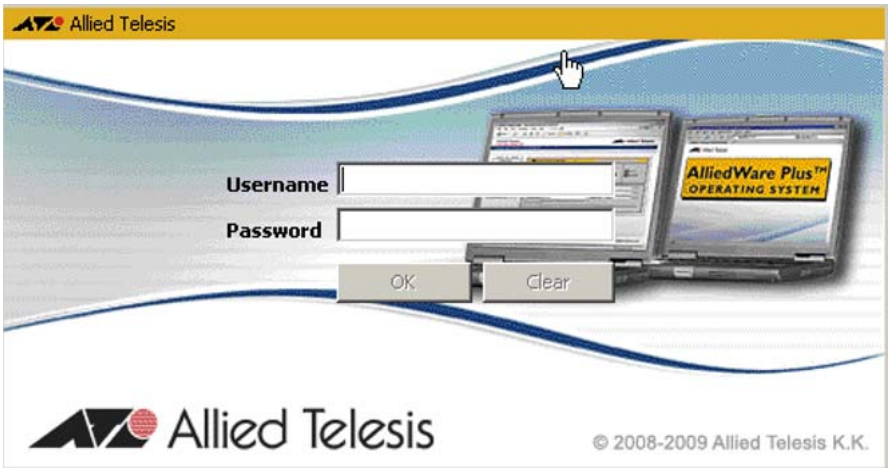
8. **Enter the URL in the Java Control Panel Exception Site List.**

   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 5.4.4 *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 x210-5.4.4-4.16.rel
   ```

   On the x230 Series switches, use the command:

   ```
   awplus(config)#boot system x230-5.4.4-4.16.rel
   ```

   On the x310 Series switches, use the command:

   ```
   awplus(config)#boot system x310-5.4.4-4.16.rel
   ```

   On the x510 Series switches, use the command:

   ```
   awplus(config)#boot system x510-5.4.4-4.16.rel
   ```

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

   ```
   awplus(config)#boot system ix5-5.4.4-4.16.rel
   ```

   On the x610 Series switches, use the command:

   ```
   awplus(config)#boot system x610-5.4.4-4.16.rel
   ```

   On the x900 Series switches, use the command:

   ```
   awplus(config)#boot system x900-5.4.4-4.16.rel
   ```

   On the SwitchBlade x908, use the command:

   ```
   awplus(config)#boot system SBx908-5.4.4-4.16.rel
   ```

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

   ```
   awplus(config)#boot system SBx81CFC400-5.4.4-4.16.rel
   ```

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

```
awplus(config)#boot system SBx81CFC960-5.4.4-4.16.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
   ```

Enhancements in 5.4.4-4.15

The following enhancements have been made:

ER-851	**SNMP**	For models: x210, x230, x310, x510, Ix5, x610, x900, SBx908, SBx81CFC400, SBx81CFC960 AlliedWare Plus MIBs now support SMIv1 version MIBs.
ER-879	**AMF**	For models: x210, x230, x310, x510, Ix5, x610, x900, SBx908, SBx81CFC400, SBx81CFC960 AMF can now be configured on LACP links.
ER-891	**Stacking**	For models: x230, x310, x510, x610 An extra diagnostic logging has been added to detect corruption of resiliency link healthcheck packets during transmission if such rare event should ever occur. Also on x510 and x930 stacks, this update prevents corrupted packets looping around the resiliency link VLAN.
ER-1089	**SNMP**	For models: x210, x230, x310, x510, Ix5, x610, x900, SBx908, SBx81CFC400, SBx81CFC960 This software updates provides the capability for the switch to generate an SNMP trap when the "syslog-ng" process unexpectedly fails.

Enhancements in 5.4.4-4.13

The following enhancement has been made:

Enhancement: 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 **msgtext**.
- 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>]
```

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.
...
```

Enhancements in 5.4.4-4.12

The following enhancement has been made:

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

Enhancements in 5.4.4-4.11

The following enhancement has been made:

Dynamic changes to policy-map content

Previously, on the x900 and x908 switches, QoS commands could not dynamically change 'class-maps' or 'policy-maps' that were attached to interfaces.

With this enhancement, it is now possible for policy-maps that are already applied to interfaces to be changed or updated dynamically.

Enhancements in 5.4.4-3.10

The following enhancement has been made:

ER-552	**Ping Polling, Triggers**	For the x210, x230, x310, Ix5, x510, x610, x900, x908, and SBx8100 with CFC400, CFC960. With this update, ping poll states are now correctly retained and reflected on the new stack master after a master fail over

Enhancements in 5.4.4-3.9

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

ER-528	**Hardware Health Monitoring**	For SBx8100 with CFC400 or CFC960 only. With this software update, a new command has been added to monitor SBx8100 line cards to reset or disable the card if a certain hardware issue is seen. **Note**: It is recommended to only enable this command if instructed to do so by Customer support. New Command: `no/system hw-monitoring packet-buffer (disable|reset (<1-10>|))"`
ER-544	**ARP**	For SBx8100 with CFC960 only. With this software update a new **unicast** parameter has been added to the **arp-mac-disparity** command. When configured, if a disparate unicast ARP reply is received, the switch will install a "**flood to vlan**" entry for the target MAC address. This option was added to support flooding of traffic to NLB clusters operating in unicast mode.
ER-554	**Aggregation - LACP, Aggregation - Static**	For the x510 switch only. With this software update, the hashing algorithm used to decide which port of an aggregation a packet should be sent to, has been reverted to the algorithm that was used in previous releases, unless the **platform load-balance** command is used.

Enhancements in 5.4.4-3.7

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

CR	Module	Description
ER-410	**ARP**	For x900, SBx908, and SBx8100 with CFC400 or CFC960 only. Previously, the **arp** command accepted only a single port to be entered and saved in the configuration file. With this update, the user can now specify multiple ports (for a multicast MAC address) for the packets to be forwarded out. The **arp** command has been changed to accept a port list for static ARPs with multicast MAC addresses: `arp <ip-addr> <multicast-mac-address> [<port-list>]` The entire port list is now stored in the configuration file when a multicast address is entered with the ARP command. (For a non-multicast MAC address, only a single port number can be configured, as before.) The **show arp** command has been updated to show all of the ports, rather than a single port, associated with the ARP entry with a multicast address. The **show mac address-table** command output has also been updated to handle multicast entries differently and reflect that these multicast entries are actually on a vidx rather than on the CPU on the CPU interface. With this update, a pre-existing issue has also been resolved that was related to aggregated ports being added to the vidx group for a multicast ARP. Specifically, the check for whether a port was enabled within a aggregator was incorrect. This would cause ports within the aggregator that were disabled to have their port added to the vidx group when they were no longer part of the aggregator (and hence they would forward packets). This issue has been resolved.

ER-9	**IGMP**	With this update, a new feature has been added to allow IGMP to control the reception of packets on certain trusted ports only.
		A new feature has been added to allow IGMP to control the reception of packets on certain trusted ports only.
		`[no] ip igmp trusted [all|query|report|routermode]`
		where:
		■ all allows IGMP to receive all IGMP and other routermode packets
		■ query allows IGMP to receive IGMP queries
		■ report allows IGMP to receive IGMP membership reports
		■ routermode allows IGMP to receive 'routermode' packets
		This command enables (and disables) the specified ports and/or aggregators to receive all, IGMP query or IGMP report or other 'routermode' packets. This command is used for disallowing specified packets being processed by the IGMP module if the packets are received on the specified ports/aggregator.
		By default, all ports and aggregators are all trusted interfaces, ie. IGMP is allowed to process all IGMP query, report, and router mode packets arriving on all interfaces.
		Example: to disallow processing of IGMP query packets arriving on port1.0.5 by IGMP module, use the command:
		`awplus(config)#int port1.0.5`
		`awplus((config-if)#no ip igmp trusted query`
		Please use the command 'show running-config interface' to display the IGMP trusted port status.

CR	Module	Description
ER-472	**Port Security**	With this update, when a port-security violation occurs, the MAC address that caused the violation is now logged as part of the existing log message.
ER-450	**SNMP**	With this software update, the command **snmp port-polling timeout <1-65535>** is added to allow a user to configure the IF-MIB polling rate from the default 5s to 1s.
CR00041773	**SNMP**	Previously, the link up/down trap defined in RFC1157 included the interface ifindex in the trap, but it was not user-friendly for the user to figure out, from the iFIndex, which port the trap pertained to. To make it more user friendly, a new Allied Telesis Enterprise MIB has been created with MIB OID: 1.3.6.1.4.1.207.8.4.4.3.25. This new atSnmpTrap MIB, includes only 2 MIB variables: atLinkDown and atLinkUp. The information included in each of the traps is: ifIndex, ifAdminStatus, ifOperStatus, ifName (extra info from the standard link up/down trap).

Issues Resolved in 5.4.4-4.16

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

CR number format: A new issue tracking system is being introduced. The CRs in the new system use a new format (CR-5xxxx). 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	x900	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960
CR-53412	**Multicasting**	Previously, if rendezvous points (RPs) were moved then it could cause the multicast forwarding cache entry to be removed incorrectly from the switch hardware table, resulting in switches that acted as RPs not sending register-stop packets. This issue has been resolved.	–	–	Y	–	Y	Y	Y	–	Y	Y	Y

Issues Resolved in 5.4.4-4.15

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

CR	Module	Description	x210	x230	x310	IX5	x510, 510L	x610	x900	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960
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
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
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	Y	Y

CR	Module	Description	x210	x230	x310	IX5	x510, 510L	x610	x900	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960
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 its 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
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
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

CR	Module	Description	x210	x230	x310	IX5	x510, 510L	x610	x900	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960
CR-53989	**DHCP Snooping**	Previously, if DHCP snooping was being used with DHCP Relay on the same switch, DHCP replies were not processed correctly. As a result, no DHCP Snooping bindings would be added. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
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
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
CR-54355	**IPv4**	Previously, executing the command **set ip next-hop** could result in an internal process restarting unexpectedly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	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
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	–	–	–	–
CR-51885	**Loop Protection**	Previously, on the x230 Series switches, the loop detection packets were sent out with incorrect Ethernet type, VID, and port-ID. This issue has been resolved.	–	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

CR	Module	Description	x210	x230	x310	IX5	x510, 510L	x610	x900	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960
CR-53237	**Multicast Routing**	Previously, when the switch chip driver encountered an error adding a multicast route, it allocated a route-entry index but returned an error without freeing the route index. This resulted in one less multicast route available for use. If the problem happened frequently enough, then the route table was full of unusable entries. 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-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	–	–	–	–	–
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. SSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	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
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-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
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

CR	Module	Description	x210	x230	x310	IX5	x510, 510L	x610	x900	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960
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-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. ISSU: Effective when ISSU complete	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y
CR-54863	**System**	Previously, on x510 or x310 variant 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	–	–	–	–	–	–

Issues Resolved in 5.4.4-4.14

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

CR	Module	Description	x210	x230	x310	x350	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
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	Y	Y	Y	Y
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 5.4.4-4.13

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

CR	Module	Description	x210	x230	x310	x350	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
CR-53180	**AMF System**	Previously, in rare circumstances, a switch could reboot unexpectedly after the **show tech-support** command was entered. This issue has been resolved.	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
CR-53166	**IGMP**	Previously, setting the IGMPSnooping router mode to IP with a set of custom addresses could result in incorrect flooding of multicast data non-member ports. This issue has been resolved.	Y	Y	Y	–	Y	Y	Y	–	–	Y	Y	Y
CR-53497	**IGMP**	Previously, when all downstream ports of multicast groups went down during a stack failover, the multicast forwarding information could get out of sync between stack members, resulting in some multicast traffic failing to be forwarded. This issue has been resolved.	–	–	–	–	–	–	–	–	–	Y	Y	Y
CR-53132	**Multicast**	Previously, in a VCStack Plus setup with a lot of multicast entries, the VCStack Plus fail over (for example, due to a power outage) would result in a large number of EXFX log messages being generated, and could cause the switch to incorrectly detect that the L3 multicast route table was full. This issue has been resolved.	–	–	–	–	–	–	–	–	–	Y	Y	Y
CR-53371	**NTP**	Previously, the command **no NTP server x.x.x.x** would fail to de-configure the NTP server on a switch. This issue has been resolved.	Y	Y	Y	–	Y	Y	Y	–	–	Y	Y	Y

CR	Module	Description	x210	x230	x310	x350	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
CR-52366	**QoS**	Previously, with 100% utilization on an ACL and QoS configured, a stack master could restart unexpectedly when the command **show platform classifier statistics utilization brief** was entered. Previously, 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-53418	**Switching**	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-52987	**System**	Previously, when a switch was running continuously for more than 248.5 days, the **show interface <*port*>** command would incorrectly show an extrememly large "Time since last state change" value. This issue has been resolved.	Y	Y	Y	–	Y	Y	–	–	–	Y	Y	Y
CR-53391	**System**	Previously, when a system restart occurred, the resulting core dump may not have been correctly stored to allow for later retrieval. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-53284	**VCStack**	Previously, a VCStack Plus would not reform due to the stacking (DAC) ports not coming back up after the backup member reset. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y

Issues Resolved in 5.4.4-4.12

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

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
CR-52276	**802.1x**	Previously, HTTP redirect of Web authentication would 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-51387	**ACL, Mirroring, QoS**	Previously, configuring QoS on mirror ports could cause an unexpected restart. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	–	Y	Y	Y
CR-50943	**AMF**	Previously, the command **atmf distribute-firmware** could occasionally result in an unexpected restart. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	–	Y	Y	Y
CR-52239	**AMF**	Previously, on rare occasions it was possible for AMF neighbour relationships to go through several unnecessary 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-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-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	–	–	–	–

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
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-52240	**CLI, Tunnel**	Previously, there was a reference count leak in ARP which could result in a "unregister_netdevice" error message and CLI unresponsiveness. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	–	Y	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 “triplane” option configured, the server configuration will need to be updated to support the correct values with this release.	–	–	–	–	–	–	–	–	Y	Y
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
CR00042694	**IGMP**	Previously, clearing IGMP groups could result in a memory leak. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	–	Y	Y	Y
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	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
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
CR00036542	**MLD**	Previously, packets arriving on interfaces which did not have MLD support (only the first 100 VLANs are MLD capable), warning messages would be reported. This issue has been resolved. ISSU: Effective when CFCs upgraded.	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.	–	–	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-51374	**Port Security**	Previously, when port security was enabled on a switch port, the FDB entries for that port were incorrectly registered in the hardware table as dynamic entries rather than static entries. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	–	–
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	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
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 back into the RIP table. 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. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52762	**RIP**	Enhancement: 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-53270	**RIP**	Previously, RIPv2 would incorrectly reject routes that it received on an interface if the route was a super-net of the network configured on that interface. Eg., if a RIP interface was configured with IP subnet 192.168.1.0/24, a route such as 192.168.0.0/16 would be incorrectly rejected when received on that RIP interface. This issue has been resolved. Now only a route that exactly matches the network of the interface on which the route is received will be rejected by RIP. ISSU: Effective when CFCs upgraded.	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	IX5	x510, x510L	x610	x930	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
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
CR-53287	**Storm protection**	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-52004	**Switching**	Previously, a XEM-12T, XEM-12S or XEM-1XP in a SBx908 could occasionally produce a very low rate of packet corruption. This issue has been resolved.	–	–	–	–	–	–	–	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.	–	–	–	–	–	–		–	–	–
CR-52250	**System**	Previously, during a stack failover, an unexpected restart could occur if there were a large number of routes. This issue has been resolved.	–	–	Y	Y	Y	Y	Y	–	–	–
CR-52850	**System**	Previously, executing a **show tech-support** command during a VRRP transition would result in a lock up. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	Y	Y	Y	–	Y	Y	Y
CR-52851	**System**	With this software update, the unregister_netdevice log message will no longer result in a switch lock-up. 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
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 then static default route was rendered un-useable. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52727	**Unicast Routing**	Previously, dynamic route entries were not being installed into hardware correctly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	Y
CR-52468	**VCStack**	Previously, under unusual circumstances, it was possible for a stack member or SBx8100 card to falsely detect a duplicate master situation and cause the rest of the stack or the SBx8100 card to reboot unintentionally. With this software update, extra processing checks have been added to ensure that units do not reboot unnecessarily.	–	–	Y	Y	Y	Y	Y	–	Y	Y
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-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.	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
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-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 5.4.4-4.11

CR	Module	Description	x210	x230	x310	x350	IX5	x510, x510L	x610	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
CR-50743	**AMF**	Previously, it was possible for 10 logins anywhere on an AMF network to accumulate resources on switches that were not part of the working-set, resulting in an effective limit of 10 AMF users on the network. This issue is now resolved, so that AMF allows more than 10 users, and instead limits any one switch to be added to a maximum of 10 working-sets.	Y	Y	Y	–	Y	Y	Y	Y	Y	Y
CR-51188	**AMF, SNMP**	Previously, the SNMP AMF trigger counter MIB object: (1.3.6.1.4.1.207.8.4.4.4.53.10.11.0) was unrecognized in the Allied Telesis trigger MIB. This issue has been resolved.	Y	Y	Y	–	Y	Y	Y	Y	Y	Y
CR-52652	**ARP**	Previously, if a static ARP was configured on multiple ports, the ARP entry would not get re-added correctly into the hardware table after a failover. This issue has been resolved.	–	–	–	–	–	–	–	Y	Y	Y
CR-51026	**IPv6**	Previously, in an AMF environment, it was possible for a CFC960 controller card to restart unexpectedly after all nodes in another AMF area were rebooted. This issue has been resolved.	–	–	–	–	–	–	–	–	–	Y
CR-50755	**Licensing**	Previously, there was a feature license display issue whereby an x230 switch would list unsupported features in its base license. This issue has been resolved.	–	Y	–	–	–	–	–	–	–	–
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	–	–	–
CR-51008	**Port Auth VCStack**	Previously, when a master failover occured repeatedly, it would result in web-page login failures via web-authentication. This issue has been resolved.	Y	Y	Y	–	Y	Y	Y	Y	Y	Y

CR	Module	Description	x210	x230	x310	x350	IX5	x510, x510L	x610	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
CR00020313	**QoS**	Previously, the VLANdisable action of QoS storm protection was not effective in disabling a VLAN on a port where a storm was detected. This issue has been resolved.	Y	Y	Y	–	Y	Y	Y	Y	Y	Y
CR-51851	**QoS**	Previously, the QoS on SBx908 and SBx8100 switches would not match the DSCP value in IPv6 traffic. This issue has been resolved.	–	–	–	–	–	–	–	Y	Y	Y
CR-51822	**SNMP**	Previously, the x510-28GTXR and x510-56GTXR switch MIB object contained incorrect board OID values. This issue has been resolved.	–	–	–	–	–	Y	–	–	–	–
CR-50941	**Switching**	Previously, when running the command **show platform mem QosBufferConfig** either directly or via **show tech-support** under a high load of traffic, the SBx81GT40, SBx81XS16, or SBx81CFC960 might restart unexpectedly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	Y
CR-52227	**VLAN**	Previously, removing an IPv4 VLAN classifer rule from a VLAN interface would incorrectly remove the port from the VLAN regardless of whether there were other rules configured on that VLAN. This issue has been resolved.	Y	Y	Y	–	Y	Y	Y	Y	Y	Y

Issues Resolved in 5.4.4-3.10

CR	Module	Description	x210	x230	x310	x350	IX5	x510, x510L	x610	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
CR-50898	**802.1x**	Previously, executing the **no dot1x port-control** command would incorrectly clear all Port-Auth interface configuration. This issue has been resolved.	Y	Y	Y	–	Y	Y	Y	Y	Y	Y
CR-52135	**802.1x**	Previously, restarting the port authentication process would result in FDB entries associated with the wrong VLAN. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	–	Y	Y	Y	Y	Y	Y
CR-50824	**AMF**	Previously, if an AMF master within a ring of AMF links in a network was disconnected, an undesirable loop could occur in the network. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	–	Y	Y	Y	Y	Y	Y
CR-51799	**AMF**	Previously, when using the command **atmf provision node NAME delete** in combination with an ATMF remote file server, it was possible for the command to fail with a "***Directory not empty"*** error This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	Y	Y	Y	Y
CR-52539	**ARP**	Previously, a static ARP configured on a VRF instance would not be saved to the running configuration correctly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	Y	Y	Y	Y
CR-52541	**ARP**	Previously, it was not possible to configure the maximum of 8 ports on a static ARP entry with a multicast MAC address. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	Y	Y	Y
CR-52555	**ARP** **Neighbor Discovery** **VCStack**	Previously, static ARP entries with a multicast MAC address would not be added correctly if a flooding entry already existed due to arp-mac-disparity This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	Y	Y	Y

CR	Module	Description	x210	x230	x310	x350	IX5	x510, x510L	x610	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
CR-52569	**ARP VCStack**	Previously, after a Master failover, an ARP entry with multiple egress ports could be overwritten by an entry that included only one port. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	Y	Y	Y
CR-52574	**ARP VCStack**	Previously, during a LIF reboot, an ARP entry with multiple egress ports could temporarily disappear until the card had finished rebooting, resulting in unnecessary VLAN flooding. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	Y	Y	Y
CR-51452	**BGP, BGP4+**	Previously, the BGP process would restart when the BGP neighbour configuration was removed. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	Y	Y	Y	Y
CR-50533	**BGP, IPv4**	Previously, BGP peers would incorrectly advertise a default route with a next-hop of IP address of 0.0.0.0, which resulted in BGP session termination. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	Y	Y	Y	Y
CR-52611	**Hotswap**	Previously, performing a XEM hot-swap after a failover could result in a XEM initialization failure. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	Y	Y	Y
CR-51127	**IGMP, IPv4**	Previously, clearing IGMP groups using the **clear ip igmp group *** command in an IGMP snooping switch would not result in leave messages being sent by the switch to the IGMP querier. 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	x350	IX5	x510, x510L	x610	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
CR-51019	**IPv4, IPv6, Multicast Routing, PIMv6, PIM-SMv4**	Previously, an x900, x908 or x8100 switch would display higher than normal CPU usage when it was connected to a LAN containing a multicast source sending multicast data to the following groups: 225.0.0.x and 225.128.0.x 226.0.0.x and 226.128.0.x ... 238.0.0.x and 238.128.0.x 239.0.0.x and 239.128.0.x This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	Y	Y	Y
CR-51421	**IPv4, IPv6, Unicast Forwarding - HW**	Previously, adding a host route to the host table would incorrectly remove interfaces from the egress multipath objects used for multiple ECMP forwardng. This issue has been resolved.	Y	Y	Y	–	Y	Y	Y	–	–	–
CR-52301	**Multicast Forwarding (HW)**	Previously, an unnecessary error message would appear after L2 multicast entries were cleared as a result of a stack failover This issue has been resolved. ISSU: Effective when ISSU completed.	–	–	–	–	–	–	–	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.	Y	Y	Y	–	Y	Y	Y	Y	Y	Y
CR-52491	**System**	Previously, learning an ARP with a multicast MAC address, even with the **arp-mac-disparity** feature enabled, would not cause the switch to flood traffic destined for the IP address. This issue has been resolved.	–	–	–	–	–	–	–	Y	–	–
CR-52565	**System**	Previously, when VRRP was enabled and a host sent an IPv6 ping to the real IPv6 address of the interface, the device might undergo a system 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	x350	IX5	x510, x510L	x610	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
CR-51594	**VCStack**	Previously, a switch in a stack with 4 or more members could restart unexpectedly if multiple backup members rejoined the stack simultaneously. This issue has been resolved.	–	–	–	–	–	Y	Y	–	–	–

Issues Resolved in 5.4.4-3.9

CR	Module	Description	x210	x230	x310	IX5	x510, x510L	x610	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
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	–	–	–
CR-52241	**ARP** **Neighbor discovery**	Previously, when a static ARP, using a multicast MAC address, was configured, the switch would not reply to ARP requests with that MAC address. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	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-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-50788	**IPv6** **OSPFv3**	Previously, when an OSPF graceful restart was performed in an event such as a stack master failover, the default route on the device could be incorrectly removed from the OSPF route database. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	–	Y	Y	Y	Y	Y
CR-52083	**Loop protection**	Previously, stack members could reboot unexpectedly if a port that had loop protection enabled was removed from an aggregation. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	Y	Y	Y	Y	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	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
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-51045	**Port Authentication** **Stacking**	Previously, if an aggregated link was created, and the first port of the aggregation was on a provisioned unit, the MAC address of the aggregation was set to 0000.0000.0000, resulting in port authentication failure. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	Y	Y	Y	Y	–	–	–
CR-51552	**Stacking**	Previously, when the Master of a VCS+ stack was powered off, the new Master failed to remove entries from its hardware tables, which resulted in traffic loss associated with the old entries. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	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.	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-52363	**System**	Previously, on rare occasions, a 2-unit VCS Stack of x510 switches might restart unexpectedly during a power-cycle. This issue has been resolved.	–	–	–	–	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-52354	**VLAN**	Previously, on rare occasions, a VLAN could be deleted unexpectedly when web-authentication, DHCP snooping, or ARP-security were enabled. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y

Issues Resolved in 5.4.4-3.7

CR	Module	Description	x210	x230	x310	IX5	x510	x610	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
CR00042730	**802.1x**	Previously, when MAC authentication and the Loop detection feature were being used, a loop in the network would still result in an authentication flapping even after the loop was detected by LDF. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	–
CR-52064	**ATMF**	Previously, in a large AMF network, upgrading from an AlliedWare Plus 5.4.4 version to a 5.4.5 version failed on some switches due to remote sync errors. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00042747	**DHCP Snooping**	Previously, DHCP snooping had not been snooping egressing traffic, so DHCP snooping was not operating fully and ARP security was not operating correctly. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00042477	**DHCPv4**	Previously, unrecoverable parity errors might occur. This issue has been addressed to allow the switch to recover from parity errors. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	–
CR-51651	**DNS**	This update addresses the CVE-2015-0235 GHOST vulnerability. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-51777	**IGMP**	Previously, under very rare circumstances, it was possible for an expiring IGMP group to cause the device to restart. This issue has been resolved.	Y	Y	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.	–	–	–	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.	–	–	Y	Y	Y	Y	Y	Y	Y

CR	Module	Description	x210	x230	x310	IX5	x510	x610	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
CR-51693	**Port authentication, VCStack**	Previously, broadcast traffic would be dropped or duplicated across static aggregators on a x510 stack. This issue has been resolved.	–	–	–	–	Y	–	–	–	–
CR00042131	**Port Security**	With this software update, a port violation is now carried out if a static mac is configured for a port but then the source mac is seen on another port with port-security enabled. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-51901	**QoS**	Previously, executing the command **show mls qos interface <ifname> storm-state** would cause the device to restart if the specified ifname was over 21 characters. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00033382	**SNMP**	Previously, MIB walks of the ARP cache would sometimes fail when more than 1024 ARP entries were present. x210, x230, x310, Ix5, x510, x610, x900, x908, x8106, x8112 This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-51454	**SSL**	This update addresses the following OpenSSL security vulnerabilities: * CVE-2014-3569 * CVE-2014-3570 * CVE-2014-3571 * CVE-2014-3572 * CVE-2014-8275 * CVE-2015-0204 * CVE-2015-0205 * CVE-2015-0206 These issues have been resolved.	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.	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00042413	**System**	Previously, on rare occasions, an x210 device could restart due to some initialisation errors. This issue has been resolved.	Y	–	–	–	–	–	–	–	–

CR	Module	Description	x210	x230	x310	IX5	x510	x610	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
CR-51310	**System**	Previously, it was possible for card synchronisation keep-alive packets to be lost when executing show commands such as **show platform mem** or **show tech-support**. This issue has been resolved.	–	–	–	–	–	–	–	Y	Y
CR00042717	**VCStack**	Previously, it was possible for the VCS resiliency-link to fail during normal operation and never recover. This problem was only ever observed once and is extremely rare. This issue has been resolved.	–	–	Y	Y	Y	Y	Y	Y	Y
CR-51056	**VCStack**	Previously, it was possible to assign the resiliency link a VLAN ID that was in use by VCS management, causing the stack to separate. This issue has been resolved — it is now not possible to use the reserved VCS management VLAN for the resiliency link.	–	–	Y	Y	Y	Y	Y	Y	Y
CR-51228	**VCStack**	Previously, on a stacking capable switch, the resiliency link would not work correctly with some members that had joined the already-formed stack. This issue has been resolved.	–	–	Y	Y	Y	Y	Y	Y	Y
CR-51320	**VCStack**	Previously, under high load, a stack could potentially separate due to a high number of protocol packets. This issue has been resolved.	–	–	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 VCS+ setup. This issue has been resolved.	–	–	–	–	–	–	–	–	Y
CR00042710	**VLAN**	Previously, executing the **clear mac address-table dynamic VLAN <vid>** command for an unknown VID would result in the device restarting. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	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.	–	–	–	–	–	–	Y	Y	Y

CR	Module	Description	x210	x230	x310	IX5	x510	x610	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
CR-51305	**VLAN**	Previously, on AW+ release 5.4.4-2.3 and later, if the **switchport trunk allowed vlan all** command was configured for an aggregator port, this command would not work as intended. It would add all existing VLANs to the aggregator port, but any new VLANs created would not be automatically added. This issue only affected aggregators, not individual switchports. This issue has been resolved.	–	–	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.	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.	–	–	Y	Y	Y	Y	Y	Y	Y

Issues Resolved in 5.4.4-3.6

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

CR number format: A new issue tracking system is being introduced. The CRs in the new system use a new format (CR-5xxxx). 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	x610	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
CR-50957 CR-50990	**IPv6, Unicast forwarding**	If multiple IPv6 addresses in the same subnet are assigned to the same VLAN interface, and if the last IPv6 address (that was assigned to the VLAN interface) is deconfigured, then the prefix entry for the whole subnet could have been removed from the switch HW table. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00042594	**Link Aggregation**	**Enhancement**: This update adds more command parameter options that are used in the hash calculation for load balancing across LAGs. In particular, the additional options now allow ethertype and L4 ports to be turned on/off independently of each other, in addition to the existing options of using IP and MAC addresses for hash calculations. `platform load-balancing ({src-st-mac|src-dst-ip|`**`src-dst-port`**`|`**`ethertype`**`}`	–	–	–	–	Y	–	–	–	–
CR-51103	**PoE**	Previously, there was a problem with x230 PoE ports not coming up even though the total allocated power was within the nominal power budget. This issue has been resolved.	Y	Y	–	–	Y	–	–	–	–
CR00042581	**Port Security**	**Enhancement**: Previously, when port-security was enabled, the only way to clear the port-security intrusion status after an intrusion was detected, was by temporarily removing the port-security configuration on a port. By doing so, it posed a security risk as it would allow "all traffic" to go through. With this update, a new command: ***clear port-security intrusion [interface <port>]*** is implemented to allow users to clear the intrusion list, reset the security violation count and clear the last violation source address, without changing the port status ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR-50603	**QoS**	**Enhancement**: QoS Storm Proctection can now be configured on static aggregators if the LAG includes ports on devices other than switch instance 0.	–	–	–	–	–	–	Y	Y	Y
CR-51511	**QoS**	**Enhancement**: With this update, a new command ***static-channel-group [1-96] member filters*** is introduced. This allows the user to configure static aggregators in such a way that QoS Storm Protection can be configured on the individual ports, in the same way as it is done with LACP aggregators. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00042654 **CR00042726**	**UPnP**	Previously, a USB memory device would become either unrecognized or inaccessible after it was removed and re-inserted into a **CFC960** controller card. This issue has been resolved.	–	–	–	–	–	–	–	–	Y

Issues Resolved in 5.4.4-3.5

CR	Module	Description	x210	x230	x310	IX5	x510	x610	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
CR-50652	**AMF**	Previously, after an AMF core domain split, it was possible for some nodes to become isolated from the ATMF network. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-50817	**AMF**	Previously, a TCP port used by AMF was open regardless of AMF status. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00042614	**ARP**	Previously, multicast routed traffic received on an SBx8100 backplane port might incorrectly be source-filtered if it was destined for an aggregator interface that matches the source aggregator interface. Also, in a system with two SBx81CFC960s, unicast traffic destined to a multicast MAC (MS-NLB) could be duplicated. This issue has been resolved.	–	–	–	–	–	–	–	Y	Y
CR-50753	**BGP**	Previously, BGP packets generated by an SBx8100 switch would be transmitted on CPU queue 2. This could result in these packets being dropped in cases of network congestion. This issue has been resolved. The BGP packets generated by the switch will now be transmitted on CPU queue 5.	–	–	–	–	–	–	–	Y	Y
CR-50887	**BGP**	Previously, stale BGP routes learned from a peer would not be deleted if the BGP neighbor connection was administratively shut down using the **neighbor A.B.C.D shutdown** command after the peer had undergone a graceful restart and if the shutdown occurred before the BGP connection reached the Established state. This issue has been resolved.	–	–	–	–	–	Y	Y	Y	Y
CR00042619	**EPSR**	Previously, the processing of large numbers of MAC learning events on a disabled VLAN of the blocked port of an EPSR ring could cause high CPU utilisation on the EPSR master switch. This issue has been resolved.	–	–	–	–	–	–	Y	–	–

CR	Module	Description	x210	x230	x310	IX5	x510	x610	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
CR00042634	**GVRP**	Previously, on rare occasions, a node being configured for GVRP could suffer an unexpected reboot. This issue has been resolved.	–	–	–	Y	Y	Y	Y	Y	Y
CR00042663	**GVRP**	Previously, GVRP neighbors might have seen intermittent removal of the dynamic VLANs from its SBx8100 neighbour. This issue has been resolved.	–	–	–	–	–	–	–	Y	Y
CR-50833	**Healthcheck**	Previously, an SBx8100 would sometimes reboot unexpectedly in a network storm condition. This issue has been resolved.	–	–	–	–	–	–	–	Y	Y
CR-50777	**IPv4**	Previously, directed IP broadcast did not work correctly with IP subnet broadcast traffic. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-50807	**IPv4**	Previously, the default routes were not getting installed properly due to the presence of one or more routes for a non-routable interface that did not get added to the hardware table. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00042632	**Switch**	Previously, if an SBx8100 or VCStack was under high system load, such as in a network storm, it was possible that the switch would reboot unexpectedly. If this problem occurred, then a 'CPG Error: Invalid message size' message would always be recorded in the log. This issue has been resolved.	–	–	–	–	–	–	–	Y	Y
CR00042621	**NTP**	Previously, there was a problem whereby the real time hardware clock could drift away from the software clock. This could mean that on a reboot NTP would need to re-adjust the time again. This issue has been resolved, now if NTP is running, the real-time clock will not drift.	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00042650	**PIM-SMv4**	Previously, if a user configured more than one PIM Rendezvous Point Candidate with a non-default group range (i.e. via an access list), only the last configured Candidate RP would have the correct group range applied to it. The other Candidate RPs would advertise candidacy for the full 224.0.0.0/4 range. This issue has been resolved.	–	–	–	Y	–	Y	Y	Y	Y

CR	Module	Description	x210	x230	x310	IX5	x510	x610	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960
CR00042652	**PIM-SMv4**	Previously, PIM register packets were not being forwarded by the RP as required by the RFC. This issue has been resolved.	–	–	–	Y	–	Y	Y	Y	Y
CR-50796	**Policy-based Routing**	Previously, the policy-based routing would not work as expected on an x900 or SBx908 switch. If the policy rule matched on a range of port numbers, then a rule to match on port numbers less-than/greater-than <*value*> would include <*value*> in the match, and port number not-equal <*value*> would not work. This issue has been resolved.	–	–	–	–	–	–	Y	–	–
CR-50678	**Port Authentication**	Previously, HTTP Redirect would not work when HTTPS was used on WEB authentication. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00042608	**Port Configuration**	Previously, on x900, SBx908 or SBx8100 switches, if NTP made a significant time adjustment at the same time as ports were coming up, there was a small chance that the links would not link up correctly. This issue has been resolved.	–	–	–	–	–	–	Y	Y	Y
CR-50776	**Port Configuration**	Previously, in an SBx8106, the backplane ports from CFC in Bay 5 to a LIF in Bay 6 were not correctly enabled. This issue has been resolved.	–	–	–	–	–	–	–	Y	Y
CR00042633	**Storm Control**	Previously, when configuring storm control, it was possible in rare cases for the switch to reboot unexpectedly. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00042644	**VLAN**	Previously, a port tagged in VLAN1, and with no native VLAN set, would be incorrectly flooded with broadcast packets. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021
alliedtelesis.com