New and enhanced features in AlliedWare Plus 5.4.6 major and minor versions (5.4.6-x.x)

AlliedWare Plus OPERATING SYSTEM

» SBx8100 Series » SBx908 » DC2552XS » x930 Series
» x610 Series » x510 Series » IE510 Series » IX5 » x310 Series
» IE300 Series » x230 Series » x210 Series » IE200 Series
» XS900MX Series » GS900MX/MPX Series
» AR2010V » AR2050V » AR3050S » AR4050S » AMF Cloud
» 5.4.6-1.x » 5.4.6-0.x

Acknowledgments

Getting the most from this manual

To get the best from this manual, we recommend using Adobe Acrobat Reader version 8 or later. You can download Acrobat free from **www.adobe.com/**

Contents

AlliedWare Plus Version 5.4.6-1.x

For:

SwitchBlade x8100 Series
SwitchBlade x908
DC2552XS/L3
x930 Series
x610 Series
x510 Series
IX5-28GPX
IE510-28GSX-80
x310 Series
IE300 Series
x230 Series
IE200 Series
x210 Series
XS900MX Series
GS900MX/MPX Series
AMF Cloud
AR4050S
AR3050S
AR2050V
AR2010V

Contents

Introduction

This release note describes the new features and enhancements in AlliedWare Plus software version 5.4.6-1.x. For more information, see the Command Reference for your switch or AR-series firewall. Software file details for this version are listed in Table 1 below.

Caution: Software version 5.4.6 requires a release license for the SBx908 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.6 license certificate before you upgrade.

If an SBx908 or SBx8100 switch already has a version 5.4.6 license installed, that license also covers 5.4.6-1.x versions. Such switches do not need a new license before upgrading to version 5.4.6-1.x.

Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- "Licensing this Software Version on an SBx908 Switch" on page 34 and
- "Licensing this Software Version on a Control Card for an SBx8100 Series Switch" on page 36.

The first 5.4.6-1.x software version is numbered 5.4.6-1.1, except for SBx8100 Series switches. The following table lists model names and software files for this version.

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
AT-GS924MX AT-GS924MPX AT-GS948MX AT-GS948MPX	GS900MX/MPX	07/2016	GS900-5.4.6-1.1.rel	GS900-gui_546_04.jar
AT-XS916MXT AT-XS916MXS	XS900MX	07/2016	XS900-5.4.6-1.1.rel	XS900-gui_546_11.jar
AT-IE200-6FT AT-IE200-6FP AT-IE200-6GT AT-IE200-6GP	IE200	07/2016	IE200-5.4.6-1.1.rel	ie200-gui_546_02.jar
AT-IE300-12GT AT-IE300-12GP	IE300	07/2016	IE300-5.4.6-1.1.rel	n/a
AT-IE510-28GSX-80	IE510	07/2016	IE510-5.4.6-1.1.rel	IE510-gui_546_04.jar
AT-x210-9GT AT-x210-16GT AT-x210-24GT	x210	07/2016	x210-5.4.6-1.1.rel	x210-gui_546_02.jar
AT-x230-10GP AT-x230-18GP AT-x230-18GT AT-x230-28GP AT-x230-28GT	x230	07/2016	x230-5.4.6-1.1.rel	x230-gui_546_11.jar
AT-x310-26FT AT-x310-50FT AT-x310-26FP AT-x310-50FP	x310	07/2016	x310-5.4.6-1.1.rel	x310-gui_546_03.jar
AT-IX5-28GPX	IX5	07/2016	IX5-5.4.6-1.1.rel	IX5-gui_546_04.jar

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
AT-x510-28GTX AT-x510-52GTX AT-x510-28GPX AT-x510-52GPX AT-x510-28GSX AT-x510-28GSX-80 AT-x510DP-28GTX AT-x510DP-52GTX AT-x510L-28GT AT-x510L-28GP AT-x510L-52GT AT-x510L-52GP	x510	07/2016	x510-5.4.6-1.1.rel	x510-gui_546_04.jar
AT-x610-24Ts AT-x610-24Ts-PoE+ AT-x610-24Ts/X AT-x610-24Ts/X-PoE+ AT-x610-24SPs/X AT-x610-48Ts AT-x610-48Ts-PoE+ AT-x610-48Ts/X AT-x610-48Ts/X-PoE+	x610	07/2016	x610-5.4.6-1.1.rel	x610-gui_546_04.jar
AT-SBx908 (see Table 2)	SBx908	07/2016	SBx908-5.4.6-1.1.rel	SBx908-gui_546_03.jar
AT-x930-28GTX AT-x930-28GPX AT-x930-52GTX AT-x930-52GPX AT-x930-28GSTX	x930	07/2016	x930-5.4.6-1.1.rel	x930-gui_546_02.jar
AT-DC2552XS/L3		07/2016	dc2500-5.4.6-1.1.rel	dc2500-gui_546_04.jar
AT-SBx81CFC400 AT-SBx81CFC960	SBx8100		Supported from 5.4.6-1.2 onwards: SBx81CFC400-5.4.6-1.2.rel SBx81CFC960-5.4.6-1.2.rel	SBx81CFC400-gui_546_06.jar SBx81CFC960-gui_546_06.jar
AT-AR4050S AT-AR3050S	AR-series firewall	07/2016	AR4050S-5.4.6-1.1.rel AR3050S-5.4.6-1.1.rel	n/a
AT-AR2050V AT-AR2010V	AR-series firewall	07/2016	AR2050V-5.4.6-1.1.rel AR2010V-5.4.6-1.1.rel	n/a
AMF Cloud		07/2016	vaa-5.4.6-1.1.iso	n/a

Under version 5.4.6, not all models of XEM are supported in the SwitchBlade x908. The following table lists which XEMs are and are not supported under version 5.4.6.

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.6-x.x

Product	Supported in version 5.4.6-x.x
XEM-1XP	No
XEM-2XP	Yes
XEM-2XS	Yes
XEM-2XT	Yes
XEM-12S	No

Product	Supported in version 5.4.6-x.x
XEM-12T	No
XEM-12Sv2	Yes
XEM-12Tv2	Yes
XEM-24T	Yes

Caution: Using a software version file for the wrong switch or AR-series firewall 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.

Obtaining User Documentation

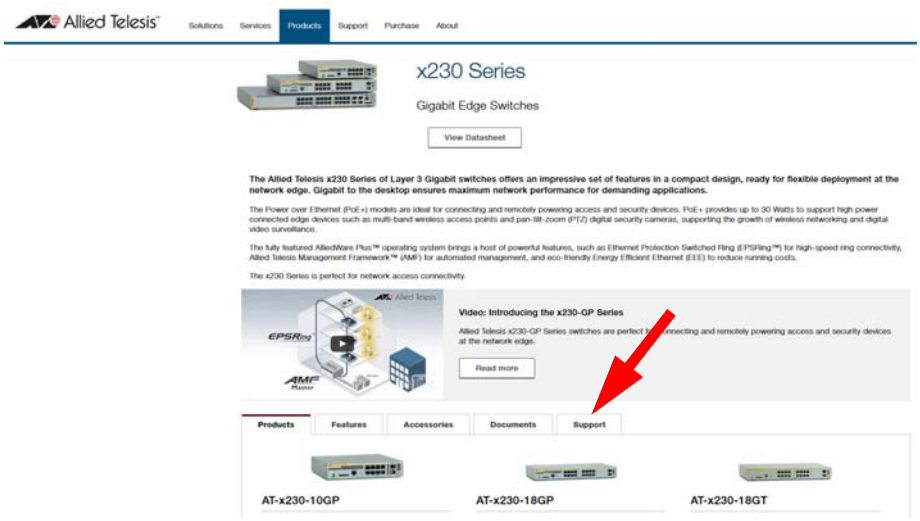
For full documentation about all features on your switch or AR-series firewall, see the Support tab of your product series web page. Product series web pages are available on our website from:

- alliedtelesis.com/products/switches (for switches) or
- alliedtelesis.com/products/securityapps (for AR-series firewalls)

For each product series, the Support tab includes the following documents:

- the **Installation Guide**,
- a detailed **Command Reference**, and
- **Feature Overview and Configuration Guides** for each supported feature.

For example, the arrow in the following figure shows the location of the Support tab on the x230 Series web page.



Product datasheets are also available on the product series web pages, along with a range of helpful case studies, solution guides, whitepapers and videos.

New Products

AlliedWare Plus version 5.4.6-1.x supports the following recently-released products.

CentreCOM XS900MX Series

Layer 3 10G Stackable Managed Switches

The AT-XS916MXT and AT-XS916MXS switches offer cost effective, high-speed 10G connectivity for servers and storage, and support 100/1000 connections for existing networks. The XS900MX Series enable a highly flexible and reliable network, which can easily scale to meet increasing traffic demands.

For more information, see alliedtelesis.com/products/xs900mx-series.

AR2010V

Compact VPN Firewall

Allied Telesis Virtual Private Network (VPN) Firewalls are ideal for branch office and remote device connectivity, supporting the move towards smarter cities and the Internet of Things (IoT).

The compact AR2010V has a small form factor and extended temperature range, making it perfect for Machine to Machine (M2M) connectivity. Applications such as traffic control, video surveillance, vending and ticketing, and remote telemetry, provide real-time data to enhance the quality of urban services in today's Smart Cities.

For more information, see alliedtelesis.com/products/securityapps.

IE300 series

Industrial Ethernet, Layer 3 Switches

Our ruggedized IE300 Industrial Ethernet switches are built for enduring performance in harsh environments, such as those found in manufacturing, transportation and physical security. Offering high throughput, rich functionality and advanced security features, IE300 switches deliver the performance and reliability demanded by industrial deployments in the Internet of Things (IoT) age.

Ruggedized to meet the latest industrial Ethernet standards for temperature, vibration, and electrical noise, IE300 switches are certified to operate in temperatures ranging from -40°C (-40°F) to 75°C (-167°F).

For more information, see alliedtelesis.com/products/ie300-series.

New Features and Enhancements

This section describes the new features in 5.4.6-1.x.

Unless otherwise stated, all new features and enhancements are available on all switch and AR-series firewall models running this version of AlliedWare Plus.

For information about finding full documentation about all features on your product, see "Obtaining User Documentation" on page 5.

Managed L2TPv2 Peer-to-Peer tunnels

Available on AR-series firewalls

Version 5.4.6-1.x adds support for managed L2TPv2 Peer-to-Peer tunnels.

For more information and configuration examples, see the L2TP Feature Overview and Configuration Guide.

Support for RED curves in Traffic Control

Available on AR3050S and AR4050S NGFWs

Version 5.4.6-1.x adds support for RED (Random Early Dropping) curves to Traffic Control.

The goal of using RED curves in a traffic-control configuration is to cause TCP flows to back off early by occasionally dropping a packet, rather than causing all flows to back off at the same time when the queue overflows.

For more information and configuration details, see the Traffic Control Feature Overview and Configuration Guide.

SMTP support in Malware Protection

Available on AR3050S and AR4050S NGFWs

In Version 5.4.6-1.x, AlliedWare Plus Malware Protection provides MD5 scanning of SMTP. Malware Protection uses stream-based scanning to compare the MD5 hash to values provided by the Kaspersky Safestream II list of malicious objects. Streams that match the MD5 hash of known malware will be blocked. POP and IMAP do not use the MD5 hash, and are instead scanned by a byte-stream process signature analysis process.

For more information, see the Malware Protection Feature Overview and Configuration Guide.

IPsec enhancements

Available on AR-series firewalls

Version 5.4.6-1.x enables you to configure customizable user-defined ISAKMP and IPSEC profiles. These customizable profiles allow you to configure a specific set of non-default options to support interoperation with legacy devices using less secure cryptographic options.

The ability to configure negotiation of specific source and destination network address traffic selectors as the method to filter which traffic can traverse a VPN is also now supported.

Lastly, encrypted VPNs can also now be negotiated with Peers whose WAN address is dynamically allocated. This can be useful for Hub-and-spoke topologies where there is a central site with fixed IP negotiating encrypted VPNs to remote sites which have their WAN IP address dynamically allocated.

For configuration examples, see the Internet Protocol Security (IPsec) Feature Overview and Configuration Guide.

Support for terminating old PPPoE sessions with PADT

Available on AR-series firewalls

Version 5.4.6-1.x improves handling of old PPPoE sessions that are still considered active by the device at the other end of the link. Previously, if an AR-series firewall needed to reconnect a PPPoE session, for example because there was some data loss via the WAN connection, or because the ISP reset the PPP connection, the firewall might have to wait until the the device at the other end of the link timed the session out.

With version 5.4.6-1.x, the firewall will actively send a PADT (Active Discovery Terminate packet) to the source of the message to terminate that session. This allows PPPoE to reconnect faster because it does not have to wait for the device at the other end to time out the old session.

Secure Mode on x930 Series switches

Available on x930 Series switches

Version 5.4.6-1.x supports Secure Mode on x930 Series switches. When in Secure Mode, the following are disabled:

- Telnet
- SSHv1
- SNMPv1/v2
- All privilege levels except 1 and 15
- Weak cryptographic algorithms e.g. MD5, RSA1, DSA, etc.

Before entering secure mode, the flash should first be erased completely using the bootloader. To do this, on boot-up, use Ctrl-D to enter the diagnostic menu, select option 7 'Bootup stage 2 diagnostics menu', and then select option 4 'Erase FLASH (Filesystem only)').

The switch should be rebooted after completion of the erase process.

Use the following commands to enter secure mode:

```
awplus# configure terminal
awplus(config)# crypto secure-mode
awplus(config)# exit
awplus# write
awplus# reboot
```

Use the following command to confirm that the switch is in secure mode:

```
awplus# show secure-mode
```

The following message should be displayed:

```
Secure mode is enabled
```

Leaving Secure Mode

If you wish to leave secure mode, you should delete all sensitive information first. This means deleting all trustpoints (one by one), by using the commands:

```
awplus# configure terminal
awplus(config)# no crypto pki trustpoint <name>
```

Also, delete all public/private key pairs, by using the commands:

```
awplus# configure terminal
awplus(config)# crypto key zeroize all
```

Turn off secure mode, by using the commands:

```
awplus# configure terminal
awplus(config)# no crypto secure-mode
awplus(config)# exit
awplus# write
awplus# reboot
```

The switch ***must*** be rebooted after secure mode is turned off, and ideally Flash memory should be erased via the bootloader.

Enhancements to PKI Certificate Management

Available on all AlliedWare Plus devices

Version 5.4.6-1.x expands the PKI Certificate Management support, to support externally-signed X.509 root and device certificates, and multiple trustpoints. This allows for flexible use of security credentials for multiple Transport Layer Security (TLS) connections to different external systems.

For examples of configurations that use the new functionality, see the

- RADIUS Feature Overview and Configuration Guide
- Logging Feature Overview and Configuration Guide

RADIUS over TLS

Available on all AlliedWare Plus devices

Version 5.4.6-1.x supports RADIUS over TLS using Radsec Proxy , which is an extension to the RADIUS authentication protocol. It uses Transport Layer Security (TLS) protocol for encrypting all messages between the NACs and RADIUS Servers.

For more information and configuration examples, see the RADIUS Feature Overview and Configuration Guide and the Local RADIUS Server Feature Overview and Configuration Guide.

Syslog over TLS

Available on all AlliedWare Plus devices

Version 5.4.6-1.x supports Syslog over TLS, which secures the connection between the AlliedWare Plus device and a Syslog server.

For more information and a configuration example, see the Logging Feature Overview and Configuration Guide.

Remote-mirroring

Available on x230, x310, IX5, x510, x930 and SBx8100 Series switches

Remote-mirroring allows traffic being transmitted or received on a port on one device to be duplicated and forwarded over the network on a special VLAN to be analysed via a port on a remote switch. Remote-mirroring is also known as RSPAN.

For configuration examples, see the Remote-Mirroring Feature Overview and Configuration Guide.

SBx81XLEM: Support for more L3 routes, L3 hosts and forwarding database entries

Available on SBx8100 Series switches, from version 5.4.6-1.2 onwards

With version 5.4.6-1.x, you can increase the size of the switching and routing silicon tables of an SBx8100 system consisting of SBx81CFC960 controller cards and SBx81XLEM line cards. There are two new modes:

- L2 Switching / L3 Routing Mode
- Host Mode

These modes increase the number of host entries and routes, as shown in the following table:

	L2 Switching / L3 Routing Mode		Host Mode	
MAC address entries	maximum:	128K	maximum:	64K
IPv4 host entries	maximum: recommended:	22K (see note 1) 22K	maximum: recommended:	64K (see note 2) 32K
IPv6 host entries	maximum: recommended:	22K (see note 1) 16K	maximum: recommended:	32K (see note 2) 16K
Next hop for prefixes	maximum:	22K (see note 1)	maximum:	22K (see note 3)
IPv4 prefixes	maximum:	128K	maximum:	128K
IPv6 prefixes	maximum:	64K	maximum:	64K
OSPFv2 routes	maximum: recommended:	10,000 5,000	maximum: recommended:	10,000 5,000
OSPFv3 routes	maximum: recommended:	10,000 5,000	maximum: recommended:	10,000 5,000
BGP4 routes (for IPv4)	maximum: recommended:	100,000 50,000	maximum: recommended:	100,000 50,000
BGP4+ routes (for IPv6)	maximum: recommended:	50,000 25,000	maximum: recommended:	50,000 25,000

note 1: Entries are shared between IPv4 and IPv6 entries, and between hosts and nexthops for prefixes. Sharing is on a first-come-first-served basis.

note 2: Entries are shared between IPv4 and IPv6 hosts. Sharing is on a first-come-first-served basis.

note 3: A nexthop for prefixes will probably also consume a host entry.

There are a number of factors to be aware of with these new modes:

- The new modes are only available with SBx81CFC960 controller cards and SBx81XLEM line cards. If other line cards are present, they will be disabled.
- The modes are not available if the controller card or cards in the chassis are SBx81CFC400.
- The modes are mutually exclusive. Only one can be enabled at a time.
- By default, both modes are disabled.
- When either of these modes is enabled, the SBx81CFC960 front panel ports can only be used as stacking ports, not network ports. The front panel ports will not appear in **show interface** output.
- In Host Mode, if a host entry cannot fit into the FDB, the SBx81XLEM will put it into the Hardware Route Table. Therefore, it will consume a route entry.
- The **platform routingratio** command is not available with these modes.

Enabling L2 Switching / L3 Routing Mode

L2 Switching / L3 Routing Mode is the default mode under Silicon Profile 3. Therefore, changing to L2 Switching / L3 Routing Mode is simply a matter of enabling Silicon Profile 3. To do this, set the silicon profile to **profile3** and reboot, by using the commands:

```
awplus# configure terminal
awplus(config)# silicon-profile profile3
awplus(config)# exit
awplus# copy running-config startup-config
awplus# reboot
```

Enabling Host Mode

To change to Host Mode, use the following steps:

Step 1: Set the silicon profile to profile3 and reboot

Use the commands:

```
awplus# configure terminal
awplus(config)# silicon-profile profile3
awplus(config)# exit
```

Step 2: Turn on host mode

Use the commands:

```
awplus# configure terminal
awplus(config)# platform fdb-l3-hosts
awplus# copy running-config startup-config
awplus# reboot
```

Using the SBx81XLEM with BGP

The Premium License (AT-FL-CFC960-01) now supports up to 100,000 BGP routes in L2 Switching / L3 Routing Mode. If your license is older than August 3rd 2016, contact your Allied Telesis representative to obtain a new one.

If you are using large numbers of routes with BGP with silicon profile 3, then you need to set the graceful-restart timer to at least 400 seconds. To do this (for ASN 1 in this example), use the commands:

```
awplus# configure terminal

awplus(config)# router bgp 1

awplus(config-router)# bgp graceful-restart restart-time 400
```

Also, note that the **show tech** command may take a long time to run if the tables are very full.

Allied Telesis Management Framework (AMF) subscription licenses

Available on all AlliedWare Plus devices that can act as an AMF controller or master (SBx8100, SBx908, DC2552XS/L3, x930, x610, x510, IX5-28GPX-80, AR4050S, AMF Cloud)

Allied Telesis Management Framework (AMF) greatly reduces the time and cost of managing network infrastructure.

Version 5.4.6-1.x adds support for AMF subscription licenses. To see the available licenses, check your device's datasheet, which is available on our website at alliedtelesis.com.

To subscribe to AMF and manage your licenses, use the following steps.

Step 1: Obtain the serial number for your AMF master and/or controller devices

Subscription licenses are tied to the serial number of the device.

Use the **show system serialnumber** command to show the serial number:

```
awplus# show system serialnumber
A05050G144700002
```

Step 2: Obtain the subscription license

To buy a subscription license, contact your authorized Allied Telesis representative. You will need to supply the device serial number.

Step 3: Download the subscription license

Subscription licenses are contained in a Capability Response File (CRF).You can download the CRF from the Allied Telesis Download center by logging into your account.

Once you have reached the **Download Central Homepage**, you can locate your device type by clicking **Search Devices** from the **Devices** menu on the left. You can select your specific device by clicking the serial number from the **Serial Number** list.

From the **View Device** page, you can download a CRF by clicking the **Download Capability Response** link. CRFs are saved as .bin files.

Step 4: Load the subscription license onto the device

After you have downloaded your CRF, you can transfer it onto the device's Flash storage by any preferred method. For example, you can use the **copy** command to copy the CRF file from a USB device to your Flash storage:

```
awplus#copy usb flash
```

Output 1: Example from **copy usb flash**

```
awplus#copy usb flash
Enter source path with file name[]:A05050G144700002.bin
Copying...
Successful operation
```

Step 5: Activate the license

Display the filename of the CRF in Flash storage, by using the following command:

```
awplus#dir *.bin
```

Then activate it by using the following command.

```
awplus#license update <CRF-filename>
```

This command copies license entitlements from the CRF into the device's internal encrypted license library. You can then safely delete the CRF from the device.

For this command to successfully activate the license, the CRF must be valid and be tied to the serial number of the device.

Step 6: Verify your CRF activation

You can verify the license by using the following command:

```
awplus#show license external
```

This displays the license name, the serial number of the device, and the license's valid dates.

Updating subscription licenses

If a subscription license expires, the device immediately reverts to the 3-node AMF Starter license.

Warning messages will be printed in the device log 28 days, 21 days, 14 days, 7 days, and 1 day prior to a license expiring. The Allied Telesis Download Center will also send you an email reminder prior to your license expiring.

To renew your license, contact your Allied Telesis representative. You can use the command **show license external** to confirm the serial number of the device.

After renewing the license, follow steps 3-6 above to download and activate it.

Subscription licenses on VCStacks

If you are licensing a VCStack, you only need to purchase a license for one member of the stack. This does not need to be the VCStack master.

To load the license onto the stack, follow the steps above on the stack master. The software checks that the CRF is valid for one of the stack members and applies the license entitlement to all members of the stack. The command **show license external stored** shows which stack member is the source of the license entitlement.

Output 2: Example from **show license external stored**

```
awplus#show license external stored

Feature entitlements sourced from license file on local flash:

Stack member 1, serial A04435H101200015
No valid entitlements found


Stack member 2, serial C20YB7309

AMF Master

    Start date:                    25 Apr 2016 00:00
    Expiry date:                   19 Apr 2017 23:59
    Maximum nodes:                 10


Stack member 3, serial B04435H101200015
No valid entitlements found
```

If you need to modify the license, for example to extend the date or change the number of nodes under management, make sure you modify the license for the same device as the original license. Do not create a new license for a different stack member instead.

If a device leaves the stack

If the device that is the source of the license entitlement leaves the stack, the following happens:

- a warning message alerts you to this event. The message displays on the console, is logged, and appears in the **show license external** output
- the remaining members of the stack retain their entitlement and continue to operate as an AMF controller/master without any disruption in service
- if the remaining partial stack reboots, it loses access to the license when it restarts.

If you need to permanently replace the device that is the source of the license entitlement, you can transfer the license to another stack member. To do this:

1. On the Allied Telesis Download center, transfer the license to the other stack member's serial number
2. Follow steps 3-4 above to transfer the CRF to the stack member
3. Force the stack to re-synchronise its license entitlement by using the command:

```
awplus#license redistribute
```

Multiple copies of a license on a stack

As said above, you only need to purchase a single license for multiple stack members, and therefore you only need to activate one CRF for the whole stack.

However, if you activate multiple CRFs for the same feature on the stack, the stack will obtain its license entitlements from the device with the lowest stack-ID. Note that stack-ID is the only factor that determines which license is used; factors such as license expiry date are not checked.

This means that it is possible (but not recommended) to have multiple CRFs for the same feature, where those CRFs have different expiry dates or support a different number of nodes. In that situation, it is possible for the stack to obtain the wrong license entitlements.

If the stack obtains the wrong license entitlements, enter the **license redistribute** command.

If that does not resolve the issue, then renumber the stack members so that the device with the preferred license entitlements has the lowest stack-ID amongst the devices that have any license installed, and reboot the renumbered devices. Once the stack has fully re-formed, if licenses are still not as desired, enter the **license redistribute** command again.

Support for renaming the AMF network without rebooting

Available on all AlliedWare Plus devices

In earlier software versions, if you renamed the AMF network on an AlliedWare Plus device, we recommended you reboot your device. Version 5.4.6-1.x removes the need to reboot.

To rename the AMF network, use the command:

```
node_1(config)# atmf network-name <new-name>
```

Improved AMF support for x600 Series switches

Available on all AlliedWare Plus devices

AMF networks that are running Version 5.4.6-1.x are now more seamlessly integrated with AlliedWare Plus x600 Series switches, as long as the x600 Series switch is running version 5.4.2-3.16 or later[1].

The x600 Series switch must be directly connected to an AMF node that is running 5.4.6-1.x or later.

The x600 Series switch provides the following information to the AMF node that it is connected to:

- The MAC address of the port connected to the AMF node
- The IPv4 address
- The IPv6 address
- The name/type of the device (Allied Telesis x600)
- The name of the current firmware
- The version of the current firmware
- The configuration name

Previous software versions made most of this information available from x600 Series switches, but it was necessary to configure the x600 as an AMF Guest Node (so it needed to be configured with DHCP and/or LLDP). With version 5.4.2-3.16 or later, as soon the x600 is connected to an appropriately configured port of an AMF node, it is immediately integrated into the AMF network.

1. Available soon from www.alliedtelesis.com/support/software

To configure the new functionality, use the following steps.

Step 1: Upgrade the software version on the x600 Series switch

The x600 Series switch must be running version 5.4.2-3.16 or later.

Step 2: Configure the link to the x600 Series switch

On the AMF node to which the x600 Series switch is connected, configure the link to the x600, using the command:

```
node_1(config-if)# switchport atmf-agentlink
```

Step 3: Monitor the x600 Series switch

On the AMF node to which the x600 Series switch is connected, you can see the details of the x600 by running the following command:

```
node_1# show atmf links guest detail
```

NTP enhancements

Available on all AlliedWare Plus devices

Version 5.4.6-1.x includes enhancements to NTP to increase the security options and make it easier to configure.

Restricting NTP functionality

Version 5.4.6-1.x enables you to restrict NTP functionality for a host or hosts, and to ignore NTP messages if they arrive at greater than a specified frequency. To configure this, use the new commands:

```
awplus(config)# ntp restrict
   {default-v4|default-v6|<host-address>|<host-subnet>} ignore

awplus(config)# ntp restrict
   {default-v4|default-v6|<host-address>|<host-subnet>}
   [limited [kod]] {nomodify|noquery|nopeer|noserve|notrust}

awplus(config)# ntp discard minimum <1-60>

awplus(config)# ntp discard average <1-16>
```

In the **ntp discard** commands, the parameters have the following meanings:

Parameter	Description
`minimum <1-60>`	The minimum time between NTP packets, in seconds.
`average <1-16>`	The minimum average time between NTP packets, in units of log2(value).

In the **ntp restrict** commands, the parameters have the following meanings:

Parameter	Description
`default-v4`	Apply this restriction to all IPv4 hosts.
`default-v6`	Apply this restriction to all IPv6 hosts.
`<host-address>`	Apply this restriction to the specified IPv4 or IPv6 host. Enter an IPv4 address in the format A.B.C.D. Enter an IPv6 address in the format X:X::X:X.
`<host-subnet>`	Apply this restriction to the specified IPv4 subnet or IPv6 prefix. Enter an IPv4 subnet in the format A.B.C.D/M. Enter an IPv6 prefix in the format X:X::X:X/X.
`ignore`	Block all NTP connections, including time polls, from matching hosts.
`limited`	Apply frequency limits to matching hosts. To specify the frequency limits, use the command **ntp discard**.
`kod`	Send kiss-of-death packets when the rate limit is exceeded. If you do not specify this, NTP packets are dropped without further processing.
`nomodify`	Prevent matching hosts from modifying the NTP configuration, even if they have a trusted key.

Parameter	Description
noquery	Prevent matching hosts from querying this device's NTP status. This option does not block time queries. We recommend using this option on publicly-accessible systems, because it blocks ntpq and ntpdc queries, which can be used in amplification attacks.
nopeer	Prevent matching hosts from becoming NTP peers of this device.
noserve	Do not serve the time to matching hosts.
notrust	Require that matching hosts authenticate NTP sessions with this device. If you use this option, the device will drop all unsigned NTP packets from matching hosts.

To prevent all hosts from using NTP except for the host 192.0.2.1 and the subnet 192.168.1.0/16, use the commands:

```
awplus# configure terminal
awplus(config)# ntp restrict default-v4 ignore
awplus(config)# ntp restrict default-v6 ignore
awplus(config)# no ntp restrict 192.0.2.1
awplus(config)# no ntp restrict 192.168.1.0/16
```

To force the host 192.0.2.1 and the subnet 192.168.1.0/16 to authenticate NTP sessions with this device, use the commands:

```
awplus# configure terminal
awplus(config)# ntp restrict 192.0.2.1 notrust
awplus(config)# ntp restrict 192.168.1.0/16 notrust
```

To ignore NTP messages from the 192.168.1.0/16 subnet if they arrive more frequently than every 5 seconds, and also send kiss-of-death messages, use the commands:

```
awplus# configure terminal
awplus(config)# ntp discard minimum 5
awplus(config)# ntp restrict 192.168.1.0/16 limited kod
```

To silently ignore all NTP messages if they arrive more frequently than once a second on average (log2(2)), use the commands:

```
awplus# configure terminal
awplus(config)# ntp discard average 2
awplus(config)# ntp restrict default-v4 limited
awplus(config)# ntp restrict default-v6 limited
```

Authentication keys

Version 5.4.6-1.x enables you to authenticate NTP sessions with SHA1 keys instead of MD5.

Also, previously, it was necessary to configure authentication keys and then separately specify a list of trusted keys. Now you can declare that a key is trusted at the time you configure it, by using one of the following commands:

```
awplus(config)# ntp authentication-key <keynumber> md5 <key> trusted
awplus(config)# ntp authentication-key <keynumber> sha1 <key> trusted
```

Default stratum value

When entering the command **ntp master**, if you do not enter a stratum value, a default of **12** is now used and displayed in output of the **show running-config** command. Previously, the default value was either 12 or 14 depending on the device.

Improved show commands

The following **show** commands have been improved:

Command	Improvement
show ntp assocation	Format of output improved
show ntp status	Format of output improved
show ntp counters	Replaced by **show ntp counters**
show ntp counters associations	New command

Deprecated commands

The following commands have been deprecated as part of this project:

Command	Replacement
ntp trustedkey	ntp authentication-key
ntp access-group	ntp restrict
show ntp associations detail	show ntp association show ntp counters associations

Support for user-created web authentication login page

Available on all AlliedWare Plus devices

Version 5.4.6-1.1 enables you to create your own web authentication login page. Prior to this, you could only customise the logo and some of the text on the page.

To create your own login page, follow these steps:

Step 1: Create the page

Write the page in HTML. Note that it must include the following login form code:

```
<form action="/index.cgi" autocomplete="off" target="_self" name="AUTH" method="POST">

<div>User name</div>
<div><input size="30" type="text" maxlength="64" name="USERNAME"></div>
<div>Password</div>
<div><input size="30" type="password" maxlength="64" name="PASSWORD"></div>

<div>
<input type="submit" name="ACTION" value="login">
<input type="reset" name="RESET" value="Reset">
</div>

</form>
```

If you do not include the above login form, the page will display in the client browser but will not perform web authentication.

Step 2: Save the page onto the switch

Name the file **login_page.html** and save it in the folder **/flash/web-auth/**

Configure VLAN classifiers on aggregators

Available on SBx8100, SBx908, DC2552XS/L3, x930, x610, x510, IE510, IX5, x310, IE300, XS900MX and GS900MX/MPX Series switches

Version 5.4.6-1.x enables you to activate VLAN classifier rules on link aggregation groups. Previously, you had to activate them on each individual port in the aggregator instead.

For example, to activate VLAN classifier group 1 on the LACP aggregator po3, use the commands:

```
awplus# configure terminal
awplus(config)# interface po3
awplus(config-if)# vlan classifier activate 1
```

Clear the PPPoE Access Concentrator statistics counters

Available on AR-series firewalls only

Version 5.4.6-1.x enables you to zero the PPPoE Access Concentrator statistics counters, by using the new command **clear pppoe-ac statistics**. This command sets all the counters to zero and restarts the statistics counting.

For example, to clear the PPPoE AC statistics counters, use the command:

```
awplus# clear pppoe-ac statistics
```

Ensure that MAC addresses are learnt by all VCStack members

Available on x930, x610, x510, IX5, and x310 Series switches

MAC addresses are automatically learnt by stack members when a packet is seen by that stack member. Normally this is sufficient to make sure that all stack members that need the MAC address learn it.

If aggregators are used, it is possible for the path taken by packets travelling from host A to B to traverse different stack members than packets travelling from host B to A. In this case, the MAC addresses may not be learnt and traffic could be flooded. Even in this case, a broadcast packet from each unit, such as an ARP packet, would be enough to cause all stack members to learn these MAC addresses.

However, in very unusual cases, the automatic learning can still lead to some flooding. Version 5.4.6-1.x adds a new command that allows a MAC address learnt on one stack member to be used on any other stack member. This will prevent the flooding that would otherwise occur in these unusual cases.

To enable this feature, use the command:

```
awplus# mac address-table vcs-sync-mode
```

Note that enabling this feature has a small impact on CPU performance, because it slightly increases the numbers of packets sent to the CPU.

Limit the number of IGMP group entries per port

Available on all AlliedWare Plus devices except AR2010V firewalls

Version 5.4.6-1.x enables you to set a limit, per switch port, on the number of IGMP groups clients can join. This stops a single client from using all the switch's available group-entry resources, and ensures that clients on all ports have a chance to join IGMP groups.

To set the limit, go into interface mode for the switch port or ports and use the command:

```
awplus(config-if)# ip igmp maximum-groups <0-65535>
```

The default is 0, which means no limit.

We recommend using this with IGMP snooping fast leave on the relevant VLANs. To enable fast leave, use the command:

```
awplus(config-if)# ip igmp snooping fast-leave
```

The device keeps count of the number of groups learned by each port. This counter is incremented when group joins are received via IGMP reports. It is decremented when:

- Group leaves are received via leave messages or reports
- Group memberships time out

Also, the port's group counter is cleared when:

- The port goes down
- You run the command **clear igmp groups ***
- The port is removed from a VLAN
- The port is on a VCStack back-up member, and that member reboots or otherwise leaves the stack.

You can see the current value of the group counter by using either of the commands:

```
awplus# show ip igmp snooping statistics interface <port-list>
```

```
awplus# show ip igmp interface <port>
```

For example, to display information about port1.0.3, use either of the following commands:

```
awplus# show ip igmp snooping statistics interface port1.0.3
```

```
IGMP Snooping statistics for port1.0.3
Maximum groups limit set: 10
Number of groups port belongs to: 0
```

```
awplus# show ip igmp interface port1.0.3
```

```
IGMP information for port1.0.3
Maximum groups limit set: 10
Number of groups port belongs to: 0
```

Enhancement to EPSR Superloop Protection

Available on all AlliedWare Plus devices that can act as an EPSR master

Version 5.4.6-1.x extends EPSR Superloop Protection (SLP) to allow multiple ring EPSR scenarios where there are multiple ring masters on a common segment, as long as none of the master secondary ports are on the common segment.

However, in such scenarios, it is not advisable to use EPSR Enhanced Recovery on transit nodes.

Support 100 local RADIUS server users on x230 and x310 Series switches

Available on x230 and x310 Series switches. Already supported in earlier software versions on AR-series firewalls, SBx8100, SBx908, DC2552XS/L3, x930, x610, IX5, IE500 and x510 Series switches.

Version 5.4.6-1.x increases the supported number of local RADIUS server users to 100 on x230 and x310 Series switches.

For more information about the local RADIUS server, see the Local RADIUS Server Feature Overview and Configuration Guide.

Restrict access to “show log” command

Available on all AlliedWare Plus devices

Version 5.4.6-1.x makes the command **show log** only available to users at privilege level 7 and above. This change enhances network security.

To set a user’s privilege level, use the command

```
awplus(config)# username <name> privilege <1-15>
```

Combine ARP security and Private VLANs

Available on all AlliedWare Plus switches

Version 5.4.6-1.x enables you to configure ARP security and Private VLANs at the same time, for Type-2 Private VLANs only. Previously, this combination was not supported.

IE200: Support for IPv6 Hardware ACLs

Newly supported on IE200 switches

Version 5.4.6-1.x adds support for IPv6 hardware ACLs on IE200 Series switches. Hardware ACLs are ACLs that you can apply directly to an interface, or use for QoS classifications

For more information and configuration details, see the ACL Feature Overview and Configuration Guide.

DC2552XS/L3: Support for new features

Version 5.4.6-1.x adds support for the following features on DC2552XS/L3 switches:

- "Active Fiber Monitoring"
- "AMF restricted-login"
- "Support for services like Microsoft Network Load Balancing (MS-NLB)" on page 26

Active Fiber Monitoring

Newly supported on DC2552XS/L3 switches.

Version 5.4.6-1.x enables DC2552XS/L3 switches to support active fiber monitoring.

The active fiber monitoring feature monitors fiber ports to see if the received optical power falls below a configurable baseline by a threshold amount. This may indicate physical bending of the fiber cable, which could arise when there is a physical intrusion. If this happens, the device can perform a configurable action.

For more information and a configuration example, see the Pluggables and Cabling Feature Overview and Configuration Guide.

AMF restricted-login

Newly supported on DC2552XS/L3 switches.

Version 5.4.6-1.x enables DC2552XS/L3 switches to support AMF restricted-login.

By default, a user logged into any node on an AMF network is able to manage any other node by using either working-sets or AMF remote login (provided the login username exists on all nodes). Where the access provided by this feature is too wide, or contravenes network security restrictions, this access can be limited by running the command **atmf restricted-login**.

This command will not be saved in the running configuration; it is a network property that can be enabled or disabled from any AMF Master. The status of restricted login will be retained over a reboot.

When restricted login is enabled on the Area, only the AMF Master nodes are able to create working-sets or manage other devices via AMF remote-logins. Other nodes may remote login to the AMF Master, but they will require password authentication on that Master, and will then be able to create working-sets originating from the Master.

Note that once you have run the command **atmf restricted-login**, certain other commands that utilize the AMF working-set command will operate only on Master nodes. Such commands include the **atmf reboot-rolling** and **show atmf group members** commands.

Support for services like Microsoft Network Load Balancing (MS-NLB)

Newly supported on DC2552XS/L3 switches.

Version 5.4.6-1.x enables DC2552XS/L3 switches to support services like Microsoft Network Load Balancing (MS-NLB).

Such services use ARP with disparate MAC addresses to ensure that packets destined for a server cluster virtual address are sent to all servers in the cluster. Disparate MAC addresses mean that the MAC address in the "sender hardware address" field of an ARP reply is different to the MAC address in the "Source MAC address" field of the Ethernet header that the ARP packet is encapsulated in.

To configure this, use the following command.

Syntax

```
arp-mac-disparity {multicast|multicast-igmp|unicast}
no arp-mac-disparity {multicast|multicast-igmp|unicast}
```

Parameter	Description
`multicast`	Enables support of server clusters operating in multicast mode. Packets destined for the server cluster are flooded to all ports in the VLAN.
`multicast-igmp`	Enables support of server clusters operating in multicast/IGMP mode. In multicast/IGMP mode, the MS-NLB server cluster uses IGMP reports to forward server traffic to a limited set of ports.
`unicast`	Enables support of server clusters operating in unicast mode. Packets destined for the server cluster are flooded to all ports in the VLAN.

Default ARP-MAC disparity support is disabled and:

- If the disparate ARP has a multicast MAC address in the ARP reply, the switch drops the ARP reply and does not learn any associated addresses
- If the disparate ARP has a unicast MAC address in the ARP reply, the switch learns the address in the ARP reply. The learned ARP entry points to the single port that the ARP reply arrived on. Matching traffic will go out this port.

Mode Interface Configuration for a VLAN interface.

Usage When you are using **multicast** mode, you can limit the number of ports that packets are flooded to, instead of flooding to all ports in the VLAN. To do this, specify the list of ports when creating the ARP entry.

For example, to flood only port1.0.1 to port1.0.3, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# arp 10.10.1.100 010e.11ff.2222 port1.0.1-port1.0.3
```

Examples

To enable support for MS-NLB in unicast mode on interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# arp-mac-disparity unicast
```

To disable support for MS-NLB in unicast mode on interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no arp-mac-disparity unicast
```

Further information about Multicast Mode with IGMP

In multicast mode with the IGMP option selected, the only difference to standard multicast mode is that the reception of IGMP reports now controls the ports to which the L3 switch floods traffic. That is, rather than simply flooding each packet destined for the NLB cluster IP address to all ports on the egress VLAN, those packets are only sent to the switchports in the VLAN that have received IGMP reports for the multicast group corresponding to the NLB cluster MAC address.

This mode is enabled by using the command **arp-mac-disparity multicast-igmp**.

Like the command **arp-mac-disparity multicast**, the command **arp-mac-disparity multicast-igmp** puts the switch into a mode where it will accept disparate ARP responses. Similarly, upon receiving a disparate ARP response, an ARP entry is created for the IP/MAC in the content of the ARP packet. The difference with the **arp-mac-disparity multicast-igmp** command is that the egress port is set to the subset of ports in the VLAN that have received IGMP reports for the NLB cluster MAC address. Note that the ARP entry is updated as ports join/leave the IGMP group.

If no ports have received IGMP reports for the NLB cluster MAC address then the ARP entry will have no egress ports and will simply drop packets destined for the NLB cluster IP address.

Again, no FDB entry is created in response to receiving the ARP packet. However, since the NLB server is operating in multicast mode with the IGMP option set and is sending IGMP reports, an FDB entry will already exist for the IGMP group (and, as a result, the NLB cluster MAC address).

When the **arp-mac-disparity multicast-igmp** command is configured on the VLAN, ARP entries appear in the output of the command **show arp** like this:

```
awplus#show arp
IP Address    MAC Address      Interface  Port         Type
10.100.0.56   0100.5e7f.0038   vlan200    igmp-group   dynamic
```

Support for multiple circuit-failover interfaces per VRRP instance

Available on all AlliedWare Plus devices that support VRRP.

Version 5.4.6-1.x enables VRRP to use Circuit Failover to monitor up to 32 interfaces per VRRP instance, by using the **circuit-failover** command.

If a VRRP instance is configured to monitor multiple interfaces, the VRRP priority will be cumulatively decremented by the configured delta for each interface as it goes down.

For example, if VRRP is configured to monitor VLAN2 and VLAN3 with the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip address 192.168.1.1/24
awplus(config-if)# exit
awplus(config)# router vrrp 1 vlan1
awplus(config-router)# virtual-ip 192.168.1.10 backup
awplus(config-router)# priority 100
awplus(config-router)# circuit-failover vlan2 10
awplus(config-router)# circuit-failover vlan3 20
```

then the following examples explain the effect of each VLAN going down:

- If only VLAN2 fails, then the VRRP priority will be decremented by 10. VRRP priority would be adjusted to become 90, because 100 - 10 = 90.
- If only VLAN3 fails, then the VRRP priority will be decremented by 20. VRRP priority would be adjusted to become 80, because 100 - 20 = 80.
- If both VLAN2 and VLAN3 fail, then the VRRP priority will be decremented by the cumulative delta values of all monitored interfaces. VRRP priority would therefore be adjusted to become 70, because 100 - 10 - 20 = 70.

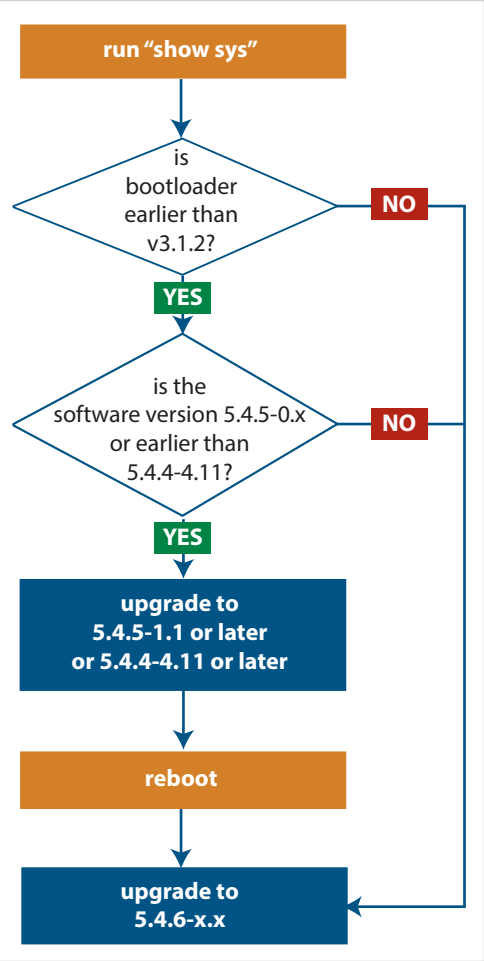
As each monitored interface recovers, the VRRP priority is incremented by the same delta value.

When you configure the delta values of the monitored interfaces, make sure their sum is high enough to ensure that the VRRP priority stays above zero if all the interfaces go down.

Important Considerations Before Upgrading

Bootloader compatibility for SBx81CFC960

On the AT-SBx81CFC960, please check your bootloader and current software version before you upgrade to AlliedWare Plus software version 5.4.6.



If your bootloader is older than 3.1.2, you can only upgrade to 5.4.6 from the following software versions:

- 5.4.5-1.1 or higher (including 5.4.5-2.x and 5.4.5-3.x)
- 5.4.4-4.11 or higher

If your bootloader is older than 3.1.2, your switch must be running one of the above versions when you upgrade to 5.4.6.

Note that you cannot upgrade to 5.4.6 directly from 5.4.5-0.x.

To see your bootloader and current software version, check the "Bootloader version" and "Software version" fields in the command:

```
awplus# show system
```

If you experience issues when upgrading, please contact your Allied Telesis support team. See our website at alliedtelesis.com/support.

Licensing

From software version 5.4.4-0.4 onwards, AlliedWare Plus software releases need to be licensed for SBx908 and SBx8100 switches.

If you are upgrading to 5.4.6-1.x on your SBx908 or SBx8100 switch, please ensure you have a 5.4.6 license on your switch. To obtain a license, contact your authorized Allied Telesis support center. You will need to provide the MAC addresses of the switches you want to license. For details, see:

- "Licensing this Software Version on an SBx908 Switch" on page 34 and
- "Licensing this Software Version on a Control Card for an SBx8100 Series Switch" on page 36.

Upgrading a VCStack

This version supports VCStack "reboot rolling" upgrades. With the **reboot rolling** command, you can reduce downtime when upgrading a VCStack.

You can use the **reboot rolling** command to upgrade to any 5.4.6-1.x version from:

- 5.4.6-0.x, or
- 5.4.5-x.x, or
- 5.4.4-1.x or later.

You cannot use rolling reboot to upgrade directly to 5.4.6-1.x from 5.4.4-0.x or earlier versions. If you wish to use rolling reboot, follow these steps:

- For releases 5.4.3-x.x or earlier, first upgrade to 5.4.4-0.x
- Next, upgrade from 5.4.4-0.x to any 5.4.5-x.x version
- Finally, upgrade from 5.4.5-x.x to 5.4.6-1.x.

Forming or extending a VCStack

If you create a VCStack from switches that are running different software versions, auto-synchronization ensures that all members will run the same software version when they boot up.

The following versions are compatible with 5.4.6-1.x for auto-synchronization:

- 5.4.6-0.x, and
- 5.4.5-x.x, and
- 5.4.4-2.x or later.

Auto-synchronization is not supported between 5.4.6-1.x and 5.4.4-1.x or 5.4.4-0.x.

Before you add a new switch to a stack, make sure the new switch's software version is compatible with the stack's version. If the new switch is running an incompatible version, it cannot join the stack until you have manually upgraded it.

AMF software version compatibility

We strongly recommend that all nodes in an AMF network run the same software release.

If this is not possible, nodes running version 5.4.6-1.x are compatible with nodes running:

- 5.4.6-0.x
- 5.4.5-x.x
- 5.4.4-x.x, and
- 5.4.3-2.6 or later.

However, if you are using Vista Manager and any AMF members are running 5.4.6-x.x, the AMF Master or Controller must also run 5.4.6-x.x. Otherwise Vista Manager will not operate correctly.

Upgrading all switches in an AMF network

This version supports upgrades across AMF networks. There are two methods for upgrading firmware on an AMF network:

- Reboot-rolling, which upgrades and reboots each node in turn
- Distribute firmware, which upgrades each node, but does not reboot them. This lets you reboot the nodes at a minimally-disruptive time.

You can use either of these methods to upgrade to this software version.

You can use these methods to upgrade to this version from 5.4.3-2.6 and later.

In summary, the process for upgrading firmware on an AMF network is:

1. Copy the release .rel files for each product family to the media location you intend to upgrade from (Flash memory, SD card, USB stick etc).
2. Decide which AMF upgrade method is most suitable.
3. Initiate the AMF network upgrade using the selected method. To do this:
    a. create a working-set of the nodes you want to upgrade
    b. enter the command **atmf reboot-rolling <*location*>** or **atmf distribute-firmware <*location*>** where **<*location*>** is the location of the .rel files.
    c. Check the console messages to make sure that all nodes are “release ready”. If they are, follow the prompts to perform the upgrade.

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.

You cannot use ISSU to upgrade to 5.4.6-1.2 from any previous software version.

Verifying the Release File for x930 Series Switches

On x930 Series switches, to ensure that the release file has not been corrupted or interfered with during download, you can verify the release file. To do this, use the following command:

```
awplus# crypto verify x930-5.4.6-1.1.rel
66d22003b876b2ac993251df29d326697f3e2fcbfe170357c62feba5d4815899
```

This command compares the SHA256 checksum of the release file with the correct checksum for the file.

All x930 Series switch models run the same release file and therefore have the same checksum. See Table 1 on page 3 for a list of models.

Licensing this Software Version on an SBx908 Switch

Release licenses are applied with the **license certificate** command, then validated with the **show license** or **show license brief** commands. Follow these steps:

- Obtain the MAC address for a switch
- Obtain a release license for a switch
- Apply a release license on a switch
- Confirm release license application

Step 1: Obtain the MAC address for a switch

A release license is tied to the MAC address of the switch.

Switches may have several MAC addresses. Use the **show system mac license** command to show the switch MAC address for release licensing:

```
awplus# show system mac license

MAC address for licensing:

eccd.6d9d.4eed
```

Step 2: Obtain a release license for a switch

Contact your authorized Allied Telesis support center to obtain a release license.

Step 3: Apply a release license on a switch

Use the **license certificate** command to apply a release license to your switch.

Note the license certificate file can be stored on internal flash memory, or an external SD card, or on a server accessible by the TFTP, SCP or HTTP protocols.

Entering a valid release license changes the console message displayed about licensing:

```
11:04:56 awplus IMI[1696]: SFL: The current software is not licensed.
awplus#license certificate demo1.csv
A restart of affected modules may be required.
Would you like to continue? (y/n): y
11:58:14 awplus IMI[1696]: SFL: The current software is licensed. Exiting
unlicensed mode.

Stack member 1 installed 1 license

1 license installed.
```

Step 4: Confirm release license application

On a stand-alone switch, use the commands **show license** or **show license brief** to confirm release license application.

On a stacked switch, use the command **show license member** or **show license brief member** to confirm release license application.

The **show license** command displays the base feature license and any other feature and release licenses installed on AlliedWare Plus switches:

```
awplus# show license
OEM Territory : ATI USA
Software Licenses
------------------------------------------------------------------------
Index                          : 1
License name                   : Base License
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 20-Mar-2016
License expiry date            : N/A
Features included              : EPSR-MASTER, IPv6Basic, MLDSnoop, OSPF-64,
                                 RADIUS-100, RIP, VRRP

Index                          : 2
License name                   : 5.4.6-rl
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 20-Mar-2016
License expiry date            : N/A
Release                        : 5.4.6
```

Licensing this Software Version on a Control Card for an SBx8100 Series Switch

Release licenses are applied with the **license certificate** command, then validated with the **show license** or **show license brief** commands. Follow these steps:

- Obtain the MAC address for a control card
- Obtain a release license for a control card
- Apply a release license on a control card
- Confirm release license application

If your control card is in a stacked chassis, you do not need to perform these steps on each chassis in the stack, only on the stack master.

If your license certificate contains release licenses for each control card present in a stacked chassis, entering the **license certificate** command on the stack master will automatically apply the release licenses to all the control cards within the stack.

Step 1: Obtain the MAC address for a control card

A release license is tied to the control card MAC address in a chassis.

Chassis may have several MAC addresses. Use the **show system mac license** command to show the control card MAC address for release licensing. Note the MAC addresses for each control card in the chassis. The chassis MAC address is not used for release licensing. Use the card MAC address for release licensing.

```
awplus#show system mac license

MAC address for licensing:


Card                MAC Address
-----------------------------------
1.5                 eccd.6d9e.3312
1.6                 eccd.6db3.58e7

Chassis MAC Address eccd.6d7b.3bc2
```

Step 2: Obtain a release license for a control card

Contact your authorized Allied Telesis support center to obtain a release license.

Step 3: Apply a release license on a control card

Use the **license certificate** command to apply a release license to each control card installed in your chassis or stack.

Note the license certificate file can be stored on internal flash memory, a USB drive, or on a server accessible by the TFTP, SCP or HTTP protocols.

Entering a valid release license changes the console message displayed about licensing:

```
11:04:56 awplus IMI[1696]: SFL: The current software is not licensed.
awplus# license certificate demo1.csv
A restart of affected modules may be required.
Would you like to continue? (y/n): y
11:58:14 awplus IMI[1696]: SFL: The current software is licensed. Exiting
unlicensed mode.

Stack member 1 installed 1 license

1 license installed.
```

Step 4: Confirm release license application

On a stand-alone chassis, use the commands **show license** or **show license brief** to confirm release license application.

On a stacked chassis, use the command **show license member** or **show license brief member** to confirm release license application.

The **show license** command displays the base feature license and any other feature and release licenses installed on AlliedWare Plus chassis:

```
awplus# show license
OEM Territory : ATI USA
Software Licenses
------------------------------------------------------------------------
Index                          : 1
License name                   : Base License
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 20-Mar-2016
License expiry date            : N/A
Features included              : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100
                                 Virtual-MAC, VRRP

Index                          : 2
License name                   : 5.4.6-rl
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 20-Mar-2016
License expiry date            : N/A
Release                        : 5.4.6
```

Installing this Software Version

Caution: Software versions 5.4.6-x.x require a release license for the SBx908 and SBx8100 switches. Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- "Licensing this Software Version on an SBx908 Switch" on page 34 and
- "Licensing this Software Version on a Control Card for an SBx8100 Series Switch" on page 36.

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

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

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

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

   ```
   awplus# del <filename>
   ```

   You cannot delete the current boot file.

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

   ```
   awplus# copy tftp flash
   ```

   Follow the onscreen prompts to specify the server and file.

4. Move from Privileged Exec mode to Global Configuration mode, using:

   ```
   awplus# configure terminal
   ```

   Then set the switch to reboot with the new software version. For example, for 5.4.6-1.1, use one of the following commands:

Product	Command
GS900MX/ MPX series	`awplus(config)# boot system GS900-5.4.6-1.1.rel`
XS900MX series	`awplus(config)# boot system XS900-5.4.6-1.1.rel`
x210 series	`awplus(config)# boot system x210-5.4.6-1.1.rel`
x230 series	`awplus(config)# boot system x230-5.4.6-1.1.rel`
IE200 series	`awplus(config)# boot system IE200-5.4.6-1.1.rel`
x310 series	`awplus(config)# boot system x310-5.4.6-1.1.rel`
IE300 series	`awplus(config)# boot system IE300-5.4.6-1.1.rel`
IX5-28GPX	`awplus(config)# boot system IX5-5.4.6-1.1.rel`
x510 series	`awplus(config)# boot system x510-5.4.6-1.1.rel`
IE510-28GSX	`awplus(config)# boot system IE510-5.4.6-1.1.rel`
x610 series	`awplus(config)# boot system x610-5.4.6-1.1.rel`
SBx908	`awplus(config)# boot system SBx908-5.4.6-1.1.rel`

Product	Command
x930 series	`awplus(config)# boot system SBx930-5.4.6-1.1.rel`
DC2552XS/L3	`awplus(config)# boot system DC2500-5.4.6-1.1.rel`
SBx8100 with CFC400[1]	`awplus(config)# boot system SBx81CFC400-5.4.6-1.2.rel`
SBx8100 with CFC960[1]	`awplus(config)# boot system SBx81CFC960-5.4.6-1.2.rel`
AR2010V	`awplus(config)# boot system AR2010V-5.4.6-1.1.rel`
AR2050V	`awplus(config)# boot system AR2050V-5.4.6-1.1.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.4.6-1.1.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.4.6-1.1.rel`

1. Supported from version 5.4.6-1.2 onwards

5. Return to Privileged Exec mode and check the boot settings, using:

```
awplus(config)# exit
awplus# show boot
```

6. Reboot using the new software version.

```
awplus# reload
```

Installing the Switch GUI

This section describes how to install and set up the java-based GUI for switches. The GUI enables you to monitor andmanage your AlliedWare Plus switch from your browser.

To install and run the GUI, you need the following system products and setup:

- PC Platform:
  Windows XP SP2 and up / Windows Vista SP1 and up
- Browser: (must support Java Runtime Environment (JRE) version 6)
  Microsoft Internet Explorer 7.0 and up / Mozilla Firefox 2.0 and up

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

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

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

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

   To see the memory usage, use the command:

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

   ```
   awplus# del <filename>
   ```

   You cannot delete the current boot file.

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

   ```
   awplus# configure terminal
   awplus(config)# interface vlan1
   awplus(config-if)#ip address <address>/<prefix-length>
   ```

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

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

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

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

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

6. Copy the GUI file onto your switch from the TFTP server, SD card, or USB storage device.

   TFTP server: Use the command:

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

   SD card: use the command:

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

   USB storage device: use the command:

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

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

7. Ensure the HTTP service is enabled on your switch. Use the commands:

   ```
   awplus# configure terminal
   ```

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

   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 has been disabled then you must enable the HTTP service again.

8. Create a user account for logging into the GUI.

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

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

9. 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.

10. 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.

11. Log into the GUI.

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

AlliedWare Plus Version 5.4.6-0.x

For:

SwitchBlade x8100 Series
SwitchBlade x908
DC2552XS/L3
x930 Series
x610 Series
x510 Series
IX5-28GPX
IE510-28GSX-80
x310 Series
x230 Series
IE200 Series
x210 Series
AMF Cloud
AR4050S
AR3050S
AR2050V

Contents

Introduction

This release note describes the new features and enhancements in AlliedWare Plus software version 5.4.6-0.x. For more information, see the Command Reference for your switch or AR-series firewall. Software file details for this version are listed in Table 1 below.

Caution: Software version 5.4.6 requires a release license for the SBx908 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.6 license certificate before you upgrade.

Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- "Licensing this Software Version on an SBx908 Switch" on page 67 and
- "Licensing this Software Version on a Control Card for an SBx8100 Series Switch" on page 69.

The first 5.4.6-0.x software version is numbered 5.4.6-0.1. The following table lists model names and software files for this version.

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
x210-9GT x210-16GT x210-24GT	x210 Series	03/2016	x210-5.4.6-0.1.rel	x210-gui_546_02.jar
x230-10GP x230-18GP x230-28GP	x230 Series	03/2016	x230-5.4.6-0.1.rel	x230-gui_546_05.jar
x310-26FT x310-50FT x310-26FP x310-50FP	x310 Series	03/2016	x310-5.4.6-0.1.rel	x310-gui_546_03.jar
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200 Series	03/2016	IE200-5.4.6-0.1.rel	ie200-gui_546_02.jar
IX5-28GPX		03/2016	IX5-5.4.6-0.1.rel	IX5-gui_546_04.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 Series	03/2016	x510-5.4.6-0.1.rel	x510-gui_546_04.jar
IE510-28GSX-80		03/2016	IE510-5.4.6-0.1.rel	IE510-gui_546_04.jar

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
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 Series	03/2016	x610-5.4.6-0.1.rel	x610-gui_546_04.jar
SwitchBlade x908 (see Table 2)	SBx908	03/2016	SBx908-5.4.6-0.1.rel	SBx908-gui_546_03.jar
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930 Series	03/2016	x930-5.4.6-0.1.rel	x930-gui_546_02.jar
DC2552XS/L3		03/2016	dc2500-5.4.6-0.1.rel	n/a
SBx81CFC400 SBx81CFC960	SBx8100 Series	03/2016	SBx81CFC400-5.4.6-0.1.rel SBx81CFC960-5.4.6-0.1.rel	SBx81CFC400-gui_546_06.jar SBx81CFC960-gui_546_06.jar
AR4050S AR3050S AR2050V	AR-series firewall	03/2016	AR4050S-5.4.6-0.1.rel AR3050S-5.4.6-0.1.rel AR2050V-5.4.6-0.1.rel	n/a - use the web-based GUI instead
AMF Cloud		03/2016	vaa-5.4.6-0.1.iso	n/a

Under version 5.4.6, not all models of XEM are supported in the SwitchBlade x908. The following table lists which XEMs are and are not supported under version 5.4.6.

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.6-x.x

Product	Supported in version 5.4.6-x.x
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 or AR-series firewall 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.

New Features and Enhancements

This section describes the new features in 5.4.6-0.x.

For more information about all features on the switch or AR-series firewall, see the Command Reference for your switch or AR-series firewall.

Unless otherwise stated, all new features and enhancements are available on all switch and AR-series firewall models running this version of AlliedWare Plus.

AMF guest nodes

Available on all AlliedWare Plus devices - a guest node can be connected to any AMF edge node

The AMF guest node feature provides an extension to AMF's management capabilities by providing a limited degree of management capability to devices (guest nodes) that either do not run the AlliedWare Plus operating system or run a version that does not support AMF. This feature offers guest nodes limited participation in an AMF network without the need to modify their operating systems. Essentially any device that has either an IPv4 or IPv6 address can become an AMF guest node.

AMF nodes within the network can recognize the presence of a guest node either dynamically, if they use protocols such as DHCP or LLDP, or statically, from the switchport atmf-guestlink command. Once recognized, the AMF node is then able to provide some, albeit limited, level of management support to these devices.

For details, see your device's Command Reference and the AMF Feature Overview and Configuration Guide.

AMF Cloud on Amazon Web Service

Available on AMF Cloud

AMF Cloud is a virtualized implementation of Allied Telesis Management Framework (AMF) that allows you to install AMF Masters and/or Controllers on a server. Having AMF Masters and Controllers available as virtual machines adds flexibility to the options available for AMF network designs.

AMF Cloud supports a variety of hosting options, now including support for Amazon's AWS (Amazon Web Services) Cloud service.

A step-by-step Installation Guide will be available shortly from our website at alliedtelesis.com/amf.

Traffic control for AR-series firewalls

Available on AR-series firewalls only

Traffic Control (often referred to as Quality of Service or QoS) optimizes the service provided to users when interfaces become oversubscribed. This means creating policies that:

- identify which traffic belongs to which services
- apply different control parameters to the traffic belonging to different services

These control parameters are applied to traffic to optimize the services and can be applied in a variety of combinations:

- prioritization
- bandwidth limiting
- marking
- egress scheduling

Traffic Control replaces the existing feature called Traffic Shaping.

For details, see your device's Command Reference and the Traffic Control Feature Overview and Configuration Guide.

Tunneling of PPP via L2TP

Available on AR-series firewalls only.

Version 5.4.6-0.x enables you to configure the AR-series firewall PPPoE Access concentrator to terminate multiple incoming PPPoE client connections and tunnel their PPP sessions via the L2TP LAC to one or more remote L2TP LNS devices. You can set the device to determine each L2TP tunnel destination by using static configuration or performing RADIUS or DNS lookups, based on the domain information contained within each PPPoE client username.

For details, see your device's Command Reference and the L2TP Feature Overview and Configuration Guide.

Increased number of firewall connections on AR4050S

Available on AR4050S only

Version 5.4.6-0.x increases the number of simultaneous firewall sessions to 300000 on AR4050S NGFWs.

The limit remains 100000 for AR3050S and AR2050V firewalls.

Limiting the number of firewall connections

Available on AR-series firewalls only

Version 5.4.6-0.x enables you to limit the number of firewall sessions associated with a specific entity. The limit will be applied to each host on that entity, and to both IPv4 and IPv6.

Use the following commands to configure and manage firewall connections:

- connection-limit
- clear firewall connections
- show firewall connections
- show firewall connections limits
- show firewall connections limits config-check

For details, see your device's Command Reference.

URL filtering

Available on AR-series firewalls only.

URL Filtering blocks all HTTP access to a list of websites. You can either specify a short list of websites to block (up to 1000 blacklist and 1000 whitelist rules), or subscribe to the blacklist service offered by Kaspersky.

If you subscribe to the Kaspersky service, you can create additional blacklists to block extra URLs or whitelists to allow URLs that the Kaspersky service blocks.

For details, see your device's Command Reference and the URL Filtering Feature Overview and Configuration Guide.

Increased number of bridge instances

Available on AR-series firewalls only

In version 5.4.6-0.x the maximum number of bridges that can be configured on an AR-series firewall has been increased from 16 to 64.

Limited local proxy ARP

Available on all AlliedWare Plus devices

Version 5.4.6-0.x supports limited local proxy ARP, which allows you to stop MAC address resolution for specified hosts. Limited local proxy ARP works by intercepting ARP requests for the specified hosts and responding with your device's own MAC address details instead of the destination host's details. This stops hosts from learning the MAC address of the other hosts through ARP requests.

Limited local proxy ARP ensures that the specified devices cannot send traffic that bypasses Layer 3 routing on your device. This gives you control over which hosts may communicate with one another.

On AR-series firewalls, limited local proxy ARP supports Static NAT configurations in which the NAT configuration's public address is different to the ethernet interface's address.

To configure limited local proxy ARP , use the following new commands.

ip limited-local-proxy-arp

Overview Use this command to enable local proxy ARP, but only for a specified set of IP addresses. This makes the device respond to ARP requests for those IP addresses when the addresses are reachable via the interface you are configuring.

To specify the IP addresses, use the command **local-proxy-arp**.

Use the **no** variant of this command to disable limited local proxy ARP. This stops your device from intercepting and responding to ARP requests for the specified hosts. This allows the hosts to use MAC address resolution to communicate directly with one another.

Syntax

```
ip limited-local-proxy-arp
no ip limited-local-proxy-arp
```

Default Limited local proxy ARP is disabled by default.

Mode Interface Configuration

Usage Limited local proxy ARP supports Static NAT configurations in which the NAT configuration's public address is different to the ethernet interface's address.

On such ethernet interfaces, the device needs to respond to ARP requests for the public address so that it will receive packets targeted at that address.

Limited local proxy ARP makes this possible. It is especially useful when you have a number of 1-1 NAT configurations and each public address falls within the public interface's subnet. If you enable limited local proxy ARP on the public interface and specify suitable addresses, 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 its own MAC address.

Example The following configuration snippet shows how to use limited local proxy ARP, if you are using NAT for an HTTP server with an address of 172.22.0.3 connected via eth1, and eth1 has an address of 172.22.0.1:

```
! Create a private zone for the HTTP server with address 172.22.200.3:
zone private
network vlan1
ip subnet 172.22.200.0/24
host http_server
ip address 172.22.200.3
!
! Create a public zone for the HTTP server with address 172.22.0.3:
zone public
network eth1
ip subnet 0.0.0.0/0 interface eth1
host http_server
ip address 172.22.0.3
!
! Create a NAT rule to map from the public to the private zone:
nat
rule 10 portfwd http from public.eth1 to public.eth1.http_server with dst
private.vlan1.http_server
enable
!
! Configure eth1. It has a different public address than the HTTP server:
interface eth1
ip limited local-proxy-arp
ip address 172.22.0.1/24
!
! Configure vlan1:
interface vlan1
ip address 172.22.200.5/24
!
! Tell the device to respond to ARPs for the HTTP server public address:
local-proxy-arp 172.22.0.3/32
```

local-proxy-arp

Overview Use this command to specify an IP subnet for use with limited local proxy ARP. When limited local proxy ARP is enabled with the command **ip limited-local-proxy-arp**, the device will respond to ARP requests for addresses in that subnet. Use the **no** variant of this command to stop specifying a subnet for use with limited local proxy ARP.

Syntax

```
local-proxy-arp [<ip-add/mask>]
no local-proxy-arp [<ip-add/mask>]
```

Parameter	Description
<ip-add/mask>	The IP subnet to use with limited local proxy ARP, in dotted decimal format (A.B.C.D/M). To specify a single IP address, use a 32-bit mask.

Default No subnets are specified for use with limited local proxy ARP.

Mode Global Configuration

Null encryption option for IPsec

Available on AR-series firewalls only

Version 5.4.6-0.x adds the option **null** to the encryption options for IPsec, via the command:

```
awplus(config-ipsec-profile)# transform <1-255> protocol esp
integrity {sha1|sha256|sha512} encryption null
```

This option is not intended for use in a live network. It should only be used for testing purposes.

Flexible RADIUS group selection

Available on SBx8100, SBx908, DC2552XS, x930, x610, x510, IX5, x310 and x230 Series switches and AR-series firewalls. Note that AR-series firewalls do not support 802.1x.

Version 5.4.6 enables you to create user-defined named method lists and apply these lists to authentication and accounting configurations for the three device authentication types: IEEE 802.1x-based, Web-based, and MAC-based authentication.

Previously only the default method list could be configured for device authentication and accounting.

Method lists are configured using the appropriate **aaa authentication** or **aaa accounting** command for the authentication type you wish to configure. They are applied to an interface using the relevant **authentication** or **accounting** command (see below for a list of newly created and updated commands).

Use the **show aaa server group** command to display a device's configured method lists and the **show radius server group** command to display radius server groups.

Commands

The flexible RADIUS group selection feature introduces the following new commands:

Commands	Purpose
dot1x authentication auth-web authentication auth-mac authentication	Applies a named authentication method list to an interface, overriding the default method list, for the specified authentication type.
dot1x accounting auth-web accounting auth-mac accounting	Applies a named accounting method list to an interface, overriding the default method list, for the specified authentication type.
show aaa server group	Shows the AAA users and associated method lists.
show radius server group	Shows the RADIUS server group/s configuration.

These commands have been updated for managing named method lists:

Commands	Purpose
aaa authentication dot1x aaa authentication auth-web aaa authentication auth-mac	Use to configure the **default** or a named authentication method list. Previously only the **default** method list was available.
aaa accounting dot1x aaa accounting auth-web aaa accounting auth-mac	Use to configure the **default** or a named accounting method list. Previously only the **default** method list was available.
show auth supplicant	Updated to show which server and server group are selected for a supplicant (client).

Example In this example we add two radius server groups 'rad_group_vlan10' and 'rad_group_vlan20', create two authentication method lists, which reference these server groups, and then apply these method lists to vlan10 and vlan20.

The example illustrates how to do this for MAC-based device authentication but the process is identical for the other device authentication types (namely 802.1x-based and Web-based authentication) as well as for accounting on all authentication types.

Step 1: Add the RADIUS servers

```
awplus#configure terminal
awplus(config)#radius-server host 192.168.1.101 key allied
awplus(config)#radius-server host 192.168.1.102 key allied
```

Step 2: Create RADIUS server groups

```
awplus(config)#aaa group server radius rad_group_vlan10
awplus(config-sg)#server 192.168.1.101
awplus(config-sg)#exit
awplus(config)#aaa group server radius rad_group_vlan20
awplus(config-sg)#server 192.168.1.102
awplus(config-sg)#exit
```

Step 3: Create the named authentication method lists

```
awplus(config)#aaa authentication auth-mac default group radius
awplus(config)#aaa authentication auth-mac vlan10_auth group
rad_group_vlan10
awplus(config)#aaa authentication auth-mac vlan20_auth group
rad_group_vlan20
```

Step 4: Enable MAC authentication on the interfaces

```
awplus(config)#int port1.0.10-1.0.19
awplus(config-if)#switchport access vlan 10
awplus(config-if)#auth-mac enable
awplus(config-if)#exit
awplus(config)#int port1.0.20-1.0.29
awplus(config-if)#switchport access vlan 20
awplus(config-if)#auth-mac enable
awplus(config-if)#exit
awplus(config)#int port1.0.30
awplus(config-if)#switchport mode trunk
awplus(config-if)#switchport trunk allowed vlan add 10,20,30
awplus(config-if)#exit
```

Step 5: Apply named method list to the interfaces

```
awplus(config)#int vlan10
awplus(config-if)#auth-mac authentication vlan10_auth
awplus(config-if)#exit
awplus(config)#int vlan20
awplus(config-if)#auth-mac authentication vlan20_auth
awplus(config-if)#exit
```

Packet forwarding to a specified network for unauthorized supplicants

Available on all AlliedWare Plus devices

Version 5.4.6-0.x supports packet forwarding to a network destination for unauthorized clients using Web-based authentication.

The following commands have been updated to accept a masked IP address parameter where previously they only allowed for a single IP host to be supplied:

```
auth-web forward [<ip-address>|<ip-address/mask>] {arp|dhcp|dns|tcp
   <1-65535>|udp <1-65535>}

auth guest-vlan forward {<ip-address>|<ip-address/mask>} [dns|
   tcp <1-65535>|udp <1-65535>]
```

Example To enable packet forwarding of TCP port 137 traffic from the guest vlan to the 10.0.0.0/24 subnet, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(conf-if)# auth guest-vlan forward 10.0.0.0/24 tcp 137
```

Openflow support

Available on DC2552XS/L3, x930, x510, x310 and x230 Series switches

OpenFlow is a protocol that enables Software-defined Networking (SDN). SDN is a network architecture that allows network administrators to control traffic from a centralized SDN controller without managing individual switches. SDN is materialized by decoupling the network control function (control plane) and forwarding function (data plane). OpenFlow is a protocol for the control plane to communicate with the data plane in SDN.

Openflow support is available with a feature licence. To purchase a licence, contact your local authorized Allied Telesis sales center.

For details, see your device's Command Reference.

Support for new features on x230 series switches

Available on x230 Series switches

Version 5.4.6-0.x adds support for the following features on x230 Series switches:

- RIP and static routing
- Q-in-Q (VLAN double tagging)
- DHCP relay

These features are available with a feature licence. To purchase a licence, contact your local authorized Allied Telesis sales center.

Support for new features on DC2552XS/L3 switches

Available on DC2552XS/L3 switches

Version 5.4.6-0.x adds support for the following features on DC2552XS/L3 switches:

- IPv6 ACLs
- Management ACL (the commands **vty ipv6 access-class** and **vty access-class**).

Support for the management ACL on IE200 series switches

Newly available on IE200 Series switches

Version 5.4.6-0.x adds support for the Management ACL, which restricts who is allowed remote access to your device using Telnet or SSH. This Management ACL is a simple security feature that binds an ACL (Access Control List) to the VTY's (Virtual Terminal Lines). This will allow or deny IP addresses included in the ACL to create a connection to your device. The commands are:

- **vty ipv6 access-class** and
- **vty access-class**.

Both commands have a **no** variant.

To check the ACLs' setting run the **show running-config** command.

VLAN translation

Available on IE510, x510, IX5, x310 Series switches

Version 5.4.6-0.x supports VLAN translation, which translates a VLAN's VLAN-ID to another value for use on the wire.

In Metro networks, it is common for the Network Service Provider to give each customer their own unique VLAN, yet at the customer location, give all the customers the same VLAN-ID for tagged packets to use on the wire. VLAN-ID translation can be used by the Service Provider to change the tagged packet's VLAN-ID at the customer location to the VLAN-ID for tagged packets to use within the NSP's network.

VLAN-ID translation is also useful in Enterprise environments where it can be used to merge two networks together without manually reconfiguring the VLAN numbering scheme. This situation can occur if two companies have merged and the same VLAN-ID is used for two different purposes.

Similarly within a Network Service Provider's network, Layer 2 networks may need to be rearranged, and VLAN translations make such rearrangement more convenient.

To configure VLAN translation, use the following commands.

switchport vlan translation vlan vlan

Use this command to create a VLAN translation entry on an interface. The translation entry translates a packet's VLAN-ID as seen on the wire.

Use the **no** variant to remove all translation entries or a specific entry.

This command can be applied to a switch port or a static channel group, or a dynamic (LACP) channel group. The interface must be in a mode that supports tagged packets.

Syntax

```
switchport vlan translation vlan <wire-vid> vlan <vid>
no switchport vlan translation [all|vlan <wire-vid>]
```

Parameter	Description
`vlan <wire-vid>`	VLAN-ID of the packet as you want it to be seen on the wire.
`vlan <vid>`	VLAN-ID of the VLAN as it was assignedwhen the VLAN was created.
`all`	Delete all translation entries.

Default None (by default, no translation entries exist)

Mode Interface Configuration for a switch port or a static channel group, or a dynamic (LACP) channel group. The interface must be in a mode that supports tagged packets.

Example To translate VLAN100 to VLAN200 on port 1.0.1, use the commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.1
awplus(config-if)#switchport vlan translation vlan 200 vlan 100
```

switchport vlan translation default drop

Use this command to configure a default behavior of dropping inbound tagged packets that have a VLAN-ID that does not match any entries in the VLAN translation table for an interface.

Use the **no** variant to stop dropping non-matching inbound packets and let them be accepted as is for further processing.

Syntax

```
switchport vlan translation default drop
no switchport vlan translation default drop
```

Default Do not drop packets

Mode Interface Configuration for a switch port or a static channel group, or a dynamic (LACP) channel group. The interface must be in a mode that supports tagged packets.

Example To drop inbound tagged packets if they do not match a VLAN translation entry, use the commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.1
awplus(config-if)#switchport vlan translation default drop
```

show interface switchport vlan translation

Use this command to display VLAN translation information for some or all interfaces.

Syntax

```
show interface switchport vlan translation [<interface-list>]
```

Mode Privileged Exec / User Exec

Example To display VLAN translation information for port1.0.1 and port1.0.2, use the command:

```
awplus#show interface switchport vlan translation port1.0.1-
port1.0.2
```

Output

```
awplus#show interface switchport vlan translation port1.0.1-
port1.0.2
Interface: port1.0.1
VLAN on Wire    VLAN
-------------   ---------------
  1649          100
  default       drop

Interface: port1.0.2
VLAN on Wire    VLAN
-------------   ---------------
  1650          100
  default       accept
```

Logging enhancements

Available on all AlliedWare Plus devices

Logging facilities

Version 5.4.6-0.x enables you to configure an outgoing syslog facility. This determines where the syslog server will store the log messages.

The syntax of the new command is:

```
log facility {kern|user|mail|daemon|auth|syslog|lpr|news|uucp|
cron|authpriv|ftp|local0|local1|local2|local3|local4|local5|
local6|local7}
```

The facility is displayed in the output of the **show log config** command.

Specifying a source interface or IP address for syslog messages

Version 5.4.6-0.x enables you to specify a source interface or IP address for the device to send syslog messages from. You can specify any one of an interface name, an IPv4 address or an IPv6 address.

This is useful if the device can reach the syslog server via multiple interfaces or addresses and you want to control which interface/address the device uses.

The syntax of the new command is:

```
log host source {<interface-name>|<ipv4-addr>|<ipv6-addr>}
```

The source interface/address is displayed in the output of the **show log config** command.

Filtering out categories of log messages

Version 5.4.6-0.x adds a new parameter to logging filter commands, which enables the device to drop unwanted log messages.

The new option is intended to drop low-priority log messages if they are over-filling the log files. Use it with caution, to avoid dropping important messages.

To configure the device to drop logs, specify the level, program, facility or message text you want to drop, and then use the new **exclude** parameter to specify to drop them.

The option is available for the following log commands:

- log buffered
- log console
- log email
- log host
- log monitor
- log permanent

For example, the syntax for the **log buffered** command is:

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

Support for services like Microsoft Network Load Balancing (MS-NLB)

Newly supported on x930, IE510, x510, IX5, x310 and x230 Series switches. Already supported on SBx908 and SBx8100 Series switches in earlier software versions.

Version 5.4.6-0.x enables the switch to support services like Microsoft Network Load Balancing (MS-NLB).

Such services use ARP with disparate MAC addresses to ensure that packets destined for a server cluster virtual address are sent to all servers in the cluster. Disparate MAC addresses mean that the MAC address in the "sender hardware address" field of an ARP reply is different to the MAC address in the "Source MAC address" field of the Ethernet header that the ARP packet is encapsulated in.

To configure support for such services, use the following commands.

arp-mac-disparity

Syntax

```
arp-mac-disparity {multicast|multicast-igmp|unicast}
no arp-mac-disparity {multicast|multicast-igmp|unicast}
```

Parameter	Description
`multicast`	Enables support of server clusters operating in multicast mode. Packets destined for the server cluster are flooded to all ports in the VLAN.
`multicast-igmp`	Enables support of server clusters operating in multicast/IGMP mode. In multicast/IGMP mode, the MS-NLB server cluster uses IGMP reports to forward server traffic to a limited set of ports.
`unicast`	Enables support of server clusters operating in unicast mode. Packets destined for the server cluster are flooded to all ports in the VLAN.

Default ARP-MAC disparity support is disabled and:

- If the disparate ARP has a multicast MAC address in the ARP reply, the switch drops the ARP reply and does not learn any associated addresses
- If the disparate ARP has a unicast MAC address in the ARP reply, the switch learns the address in the ARP reply. The learned ARP entry points to the single port that the ARP reply arrived on. Matching traffic will go out this port.

Mode Interface Configuration for a VLAN interface.

Usage When you are using **multicast** mode, you can limit the number of ports that packets are flooded to, instead of flooding to all ports in the VLAN. To do this, specify the list of ports when creating the ARP entry.

For example, to flood only port1.0.1 to port1.0.3, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# arp 10.10.1.100 010e.11ff.2222 port1.0.1-port1.0.3
```

Example To enable support for MS-NLB in unicast mode on interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# arp-mac-disparity unicast
```

Rate limiting ICMP error messages

Available on SBx8100, SBx908, DC2552XS, x930, x610, x510, IE510, IX5, x310 and x230 Series switches and AR-series firewalls.

Version 5.4.6-0.x enables you to rate limit ICMP error messages in both IPv4 and IPv6.

Rate limiting ICMP messages may protect your network from some DoS attacks. Some DoS attacks send a flood of traffic to devices that do not exist, causing an intervening router to reply with an ICMP unreachable message for each unknown destination. ICMP rate limiting prevents the router from generating an overwhelming number of ICMP error messages in such attacks.

To configure ICMP rate limiting, configure the interval between error messages with the following new commands:

Syntax

```
ip icmp error-interval <0-2147483647>
ipv6 icmp error-interval <0-2147483647>
```

where <0-2147483647> is the interval between replies, in milliseconds.

Default The default interval is 1000ms (1 second).

Mode Global configuration

Example To reply to IPv4 ICMP messages only once every 5 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip icmp error-interval 5000
```

Per-interface ICMP redirect setting

Newly supported on DC2552XS/L3, x930, IE510, x510, IX5, x310 and x230 Series switches. Already supported on SBx908 and SBx8100 Series switches in earlier software versions.

The **ip redirects** command enables the device to send ICMP redirect messages. These messages are used to notify hosts that a better route is available to a destination.

With version 5.4.6-0.x, this functionality can be turned on and off individual interfaces, on SBx8100, SBx908, DC2552XS/L3, x930, IE510, x510, IX5, x310 and x230 Series switches.

Note that this functionality can be enabled globally on x610 Series switches and AR-series firewalls.

Disable ICMP type 3, destination unreachable, messages

Available on all AlliedWare Plus devices

Version 5.4.6 supports the disabling of ICMP type 3, destination unreachable, messages for IPv4 and IPv6. 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.

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
```

Processing of ARP replies with a broadcast destination MAC

Available on all AlliedWare Plus devices

Version 5.4.6 supports processing of ARP replies that arrive with a broadcast destination MAC (ffff.ffff.ffff). This makes neighbors reachable if they send ARP replies that contain a broadcast destination MAC.

To enable this feature, use the command:

```
awplus(config-if)# arp-reply-bc-dmac
```

Example To allow processing of ARP replies that arrive on VLAN2 with a broadcast destination MAC, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)#  arp-reply-bc-dmac
```

Logging of changes to the MAC address table

Available on SBx908, x930, x610, x510, IX5, x310, IE200 and x230 Series switches.

Version 5.4.6-0.x adds the option of creating log entries when the content of the FDB (forwarding database) changes. Log messages are produced when a MAC address is added to or removed from the FDB.

caution: MAC address table logging may impact the performance of the switch. Only enable it when necessary as a debug tool.

Use the **no** variant of this command to stop creating log entries when the content of the FDB changes.

To enable logging, use the following new command.

mac address-table logging

Syntax

```
mac address-table logging
no mac address-table logging
```

Default MAC address table logging is disabled by default.

Mode User Exec/Privileged Exec

Usage When MAC address table logging is enabled, the switch produces the following messages on SBx908 switches:

Change	Message format	Example
MAC added	MAC add <*mac*> <*port*> <*vlan*>	MAC add eccd.6db5.68a7 port1.1.1 vlan2
MAC deleted	MAC delete <*mac*> <*port*> <*vlan*>	MAC delete eccd.6db5.68a7 port1.1.1 vlan2
MAC aged out	MAC age-out <*mac*> <*port*> <*vlan*>	MAC age-out eccd.6db5.68a7 port1.1.1 vlan2

When MAC address table logging is enabled, the switch produces the following messages on x930, x610, x510, IX5, x310, IE200 and x230 Series switches:

Change	Message format	Example
MAC added	MAC add <*mac*> <*port*> <*vlan*>	MAC add eccd.6db5.68a7 port1.0.1 vlan2
MAC removed	MAC remove <*mac*> <*port*> <*vlan*>	MAC remove eccd.6db5.68a7 port1.0.1 vlan2

On x930, x610, x510, IX5, x310, IE200 and x230 Series switches, rapid changes may not be logged. For example, if an entry is added and then removed within a few seconds, those actions may not be logged.

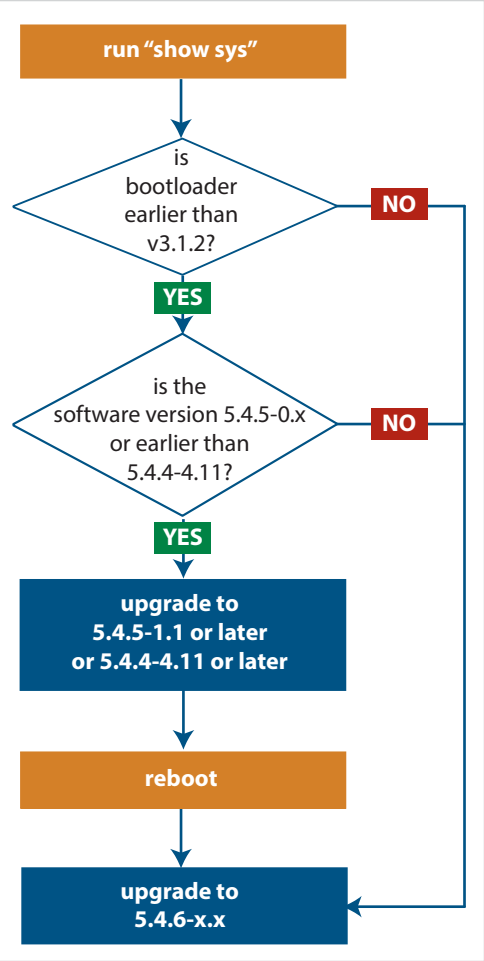
Example To create log messages when the content of the FDB changes, use the command:

```
awplus# mac address-table logging
```

Important Considerations Before Upgrading

Bootloader compatibility for SBx81CFC960

On the AT-SBx81CFC960, please check your bootloader and current software version before you upgrade to AlliedWare Plus software version 5.4.6.



If your bootloader is older than 3.1.2, you can only upgrade to 5.4.6 from the following software versions:

- 5.4.5-1.1 or higher (including 5.4.5-2.x and 5.4.5-3.x)
- 5.4.4-4.11 or higher

If your bootloader is older than 3.1.2, your switch must be running one of the above versions when you upgrade to 5.4.6.

Note that you cannot upgrade to 5.4.6 directly from 5.4.5-0.x.

To see your bootloader and current software version, check the "Bootloader version" and "Software version" fields in the command:

```
awplus# show system
```

If you experience issues when upgrading, please contact your Allied Telesis support team. See our website at alliedtelesis.com/support.

Licensing

From software version 5.4.4-0.4 onwards, AlliedWare Plus software releases need to be licensed for SBx908 and SBx8100 switches.

If you are upgrading to 5.4.6-0.x on your SBx908 or SBx8100 switch, please ensure you have a 5.4.6 license on your switch. To obtain a license, contact your authorized Allied Telesis support center. You will need to provide the MAC addresses of the switches you want to license. For details, see:

- "Licensing this Software Version on an SBx908 Switch" on page 67 and
- "Licensing this Software Version on a Control Card for an SBx8100 Series Switch" on page 69.

Upgrading a VCStack

This version supports VCStack "reboot rolling" upgrades. With the **reboot rolling** command, you can reduce downtime when upgrading a VCStack.

You can use the **reboot rolling** command to upgrade to any 5.4.6-0.x version from:

- 5.4.5-x.x, or
- 5.4.4-1.x or later.

You cannot use rolling reboot to upgrade directly to 5.4.6-0.x from 5.4.4-0.x or earlier versions. If you wish to use rolling reboot, follow these steps:

- For releases 5.4.3-x.x or earlier, first upgrade to 5.4.4-0.x
- Next, upgrade from 5.4.4-0.x to any 5.4.5-x.x version
- Finally, upgrade from 5.4.5-x.x to 5.4.6-0.x.

Forming or extending a VCStack

If you create a VCStack from switches that are running different software versions, auto-synchronization ensures that all members will run the same software version when they boot up.

Auto-synchronization is supported between 5.4.6-0.x and:

- 5.4.5-x.x, and
- 5.4.4-2.x or later.

Autosynchronisation is not supported between 5.4.6-0.x and 5.4.4-1.x or 5.4.4-0.x.

Before you add a new switch to a stack, make sure the new switch's software version is compatible with the stack's version. If the new switch is running an incompatible version, it cannot join the stack until you have manually upgraded it.

AMF software version compatibility

We strongly recommend that all nodes in an AMF network run the same software release.

If this is not possible, nodes running version 5.4.6-0.x are compatible with nodes running:

- 5.4.5-x.x
- 5.4.4-x.x, and
- 5.4.3-2.6 or later.

However, if you are using Vista Manager and any AMF members are running 5.4.6-x.x, the AMF Master or Controller must also run 5.4.6-x.x. Otherwise Vista Manager will not operate correctly.

Upgrading all switches in an AMF network

This version supports upgrades across AMF networks. There are two methods for upgrading firmware on an AMF network:

- Reboot-rolling, which upgrades and reboots each node in turn
- Distribute firmware, which upgrades each node, but does not reboot them. This lets you reboot the nodes at a minimally-disruptive time.

You can use either of these methods to upgrade to this software version.

You can use these methods to upgrade to this version from 5.4.3-2.6 and later.

In summary, the process for upgrading firmware on an AMF network is:

1. Copy the release .rel files for each product family to the media location you intend to upgrade from (Flash memory, SD card, USB stick etc).

2. Decide which AMF upgrade method is most suitable.

3. Initiate the AMF network upgrade using the selected method. To do this:

    a. create a working-set of the nodes you want to upgrade

    b. enter the command **atmf reboot-rolling <*location*>** or **atmf distribute-firmware <*location*>** where **<*location*>** is the location of the .rel files.

    c. Check the console messages to make sure that all nodes are “release ready”. If they are, follow the prompts to perform the upgrade.

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.

You cannot use ISSU to upgrade to 5.4.6-0.1 from any previous software version.

Licensing this Software Version on an SBx908 Switch

Release licenses are applied with the **license certificate** command, then validated with the **show license** or **show license brief** commands. Follow these steps:

- Obtain the MAC address for a switch
- Obtain a release license for a switch
- Apply a release license on a switch
- Confirm release license application

Step 1: Obtain the MAC address for a switch

A release license is tied to the MAC address of the switch.

Switches may have several MAC addresses. Use the **show system mac license** command to show the switch MAC address for release licensing:

```
awplus# show system mac license

MAC address for licensing:

eccd.6d9d.4eed
```

Step 2: Obtain a release license for a switch

Contact your authorized Allied Telesis support center to obtain a release license.

Step 3: Apply a release license on a switch

Use the **license certificate** command to apply a release license to your switch.

Note the license certificate file can be stored on internal flash memory, or an external SD card, or on a server accessible by the TFTP, SCP or HTTP protocols.

Entering a valid release license changes the console message displayed about licensing:

```
11:04:56 awplus IMI[1696]: SFL: The current software is not licensed.
awplus#license certificate demo1.csv
A restart of affected modules may be required.
Would you like to continue? (y/n): y
11:58:14 awplus IMI[1696]: SFL: The current software is licensed. Exiting
unlicensed mode.

Stack member 1 installed 1 license

1 license installed.
```

Step 4: Confirm release license application

On a stand-alone switch, use the commands **show license** or **show license brief** to confirm release license application.

On a stacked switch, use the command **show license member** or **show license brief member** to confirm release license application.

The **show license** command displays the base feature license and any other feature and release licenses installed on AlliedWare Plus switches:

```
awplus# show license
OEM Territory : ATI USA
Software Licenses
------------------------------------------------------------------------
Index                          : 1
License name                   : Base License
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 20-Mar-2016
License expiry date            : N/A
Features included              : EPSR-MASTER, IPv6Basic, MLDSnoop, OSPF-64,
                                 RADIUS-100, RIP, VRRP

Index                          : 2
License name                   : 5.4.6-rl
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 20-Mar-2016
License expiry date            : N/A
Release                        : 5.4.6
```

Licensing this Software Version on a Control Card for an SBx8100 Series Switch

Release licenses are applied with the **license certificate** command, then validated with the **show license** or **show license brief** commands. Follow these steps:

- Obtain the MAC address for a control card
- Obtain a release license for a control card
- Apply a release license on a control card
- Confirm release license application

If your control card is in a stacked chassis, you do not need to perform these steps on each chassis in the stack, only on the stack master.

If your license certificate contains release licenses for each control card present in a stacked chassis, entering the **license certificate** command on the stack master will automatically apply the release licenses to all the control cards within the stack.

Step 1: Obtain the MAC address for a control card

A release license is tied to the control card MAC address in a chassis.

Chassis may have several MAC addresses. Use the **show system mac license** command to show the control card MAC address for release licensing. Note the MAC addresses for each control card in the chassis. The chassis MAC address is not used for release licensing. Use the card MAC address for release licensing.

```
awplus#show system mac license

MAC address for licensing:


Card                MAC Address
-----------------------------------
1.5                 eccd.6d9e.3312
1.6                 eccd.6db3.58e7

Chassis MAC Address eccd.6d7b.3bc2
```

Step 2: Obtain a release license for a control card

Contact your authorized Allied Telesis support center to obtain a release license.

Step 3: Apply a release license on a control card

Use the **license certificate** command to apply a release license to each control card installed in your chassis or stack.

Note the license certificate file can be stored on internal flash memory, a USB drive, or on a server accessible by the TFTP, SCP or HTTP protocols.

Entering a valid release license changes the console message displayed about licensing:

```
11:04:56 awplus IMI[1696]: SFL: The current software is not licensed.
awplus# license certificate demo1.csv
A restart of affected modules may be required.
Would you like to continue? (y/n): y
11:58:14 awplus IMI[1696]: SFL: The current software is licensed. Exiting
unlicensed mode.

Stack member 1 installed 1 license

1 license installed.
```

Step 4: Confirm release license application

On a stand-alone chassis, use the commands **show license** or **show license brief** to confirm release license application.

On a stacked chassis, use the command **show license member** or **show license brief member** to confirm release license application.

The **show license** command displays the base feature license and any other feature and release licenses installed on AlliedWare Plus chassis:

```
awplus# show license
OEM Territory : ATI USA
Software Licenses
------------------------------------------------------------------------
Index                          : 1
License name                   : Base License
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 20-Mar-2016
License expiry date            : N/A
Features included              : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100
                                 Virtual-MAC, VRRP

Index                          : 2
License name                   : 5.4.6-rl
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 20-Mar-2016
License expiry date            : N/A
Release                        : 5.4.6
```

Installing this Software Version

Caution: Software versions 5.4.6-x.x require a release license for the SBx908 and SBx8100 switches. Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- "Licensing this Software Version on an SBx908 Switch" on page 67 and
- "Licensing this Software Version on a Control Card for an SBx8100 Series Switch" on page 69.

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

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

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

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

   ```
   awplus# del <filename>
   ```

   You cannot delete the current boot file.

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

   ```
   awplus# copy tftp flash
   ```

   Follow the onscreen prompts to specify the server and file.

4. Move from Privileged Exec mode to Global Configuration mode, using:

   ```
   awplus# configure terminal
   ```

   Then set the switch to reboot with the new software version. For example, for 5.4.6-0.1, use one of the following commands:

Product	Command
x210 series	`awplus(config)# boot system x210-5.4.6-0.1.rel`
x230 series	`awplus(config)# boot system x230-5.4.6-0.1.rel`
IE200 series	`awplus(config)# boot system IE200-5.4.6-0.1.rel`
x310 series	`awplus(config)# boot system x310-5.4.6-0.1.rel`
IX5-28GPX	`awplus(config)# boot system IX5-5.4.6-0.1.rel`
x510 series	`awplus(config)# boot system x510-5.4.6-0.1.rel`
IE510-28GSX	`awplus(config)# boot system IE510-5.4.6-0.1.rel`
x610 series	`awplus(config)# boot system x610-5.4.6-0.1.rel`
SBx908	`awplus(config)# boot system SBx908-5.4.6-0.1.rel`
x930 series	`awplus(config)# boot system SBx930-5.4.6-0.1.rel`
DC2552XS/L3	`awplus(config)# boot system DC2500-5.4.6-0.1.rel`
SBx8100 with CFC400	`awplus(config)# boot system SBx81CFC400-5.4.6-0.1.rel`

Product	Command
SBx8100 with CFC960	`awplus(config)# boot system SBx81CFC960-5.4.6-0.1.rel`
AR2050V	`awplus(config)# boot system AR2050V-5.4.6-0.1.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.4.6-0.1.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.4.6-0.1.rel`

5. Return to Privileged Exec mode and check the boot settings, using:

```
awplus(config)# exit
awplus# show boot
```

6. Reboot using the new software version.

```
awplus# reload
```

Installing the Switch GUI

This section describes how to install and set up the java-based GUI for switches. The GUI enables you to monitor andmanage your AlliedWare Plus switch from your browser.

To install and run the GUI, you need the following system products and setup:

- PC Platform:
  Windows XP SP2 and up / Windows Vista SP1 and up
- Browser: (must support Java Runtime Environment (JRE) version 6)
  Microsoft Internet Explorer 7.0 and up / Mozilla Firefox 2.0 and up

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

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

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

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

   To see the memory usage, use the command:

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

   ```
   awplus# del <filename>
   ```

   You cannot delete the current boot file.

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

   ```
   awplus# configure terminal
   awplus(config)# interface vlan1
   awplus(config-if)#ip address <address>/<prefix-length>
   ```

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

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

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

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

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

6. Copy the GUI file onto your switch from the TFTP server, SD card, or USB storage device.

   TFTP server: Use the command:

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

   SD card: use the command:

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

   USB storage device: use the command:

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

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

7. Ensure the HTTP service is enabled on your switch. Use the commands:

   ```
   awplus# configure terminal
   ```

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

   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 has been disabled then you must enable the HTTP service again.

8. Create a user account for logging into the GUI.

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

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

9. 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.

10. 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.

11. Log into the GUI.

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