Allied Telesis™

Novice Guide to Networking with AlliedWare Plus™

Feature Overview and Configuration Guide

Introduction

While networking is positioned by some vendors as being a complex topic best left to professionals, leaving customers to feel like it is akin to black magic, the reality is that with a basic understanding of networking and by following a handful of simple rules, a reliable network that performs well can be quickly and simply deployed.

This document aims to provide an overview of considerations when deploying a network in a simple, easy to follow guide. It is important to understand that this is an overview intended for most commonly deployed networks and that your specific requirements may vary from these.

If you'd like further information about deploying networks or are looking for a deeper understanding of the fundamentals of networking, protocols and how to solve problems when things go wrong, Allied Telesis delivers formal certified training for everyone from first time installers to networking professionals.

Contact your local Allied Telesis representative or visit Allied Telesis Training for more information.

AlliedWare Plus™
OPERATING SYSTEM

Contents

Related documents

You also may find the following documents useful:

- Getting Started with the AlliedWare Plus Command Line Interface

- Getting Started with the Device GUI on Switches

- Getting Started with the Device GUI on VPN Routers

- Getting Started with the Device GUI on UTM Firewalls

- LACP Feature Overview and Configuration Guide

- AMF Feature Overview and Configuration Guide

- VLANs Feature Overview and Configuration Guide

- STP Feature Overview and Configuration Guide

- IGMP Feature Overview and Configuration Guide

- IP Feature Overview and Configuration Guide

Products and software version

This guide applies to Allied Telesis networking devices that feature the AlliedWare Plus™ operating system. Usage and output from some commands may vary depending on the hardware platform and software version in use. For further information, please refer to the Command Reference for the specific hardware model and software version that is currently in use.

Example network

Below is a typical network setup that we'll refer to throughout this guide. You can see a pair of x530 Series switches form the network core using Virtual Chassis Stacking (VCStack) to create a single virtual device out of the two physical units. This removes any single point of failure, and uses the full bandwidth of the network. The x230 Series access switches connect user devices to the network.
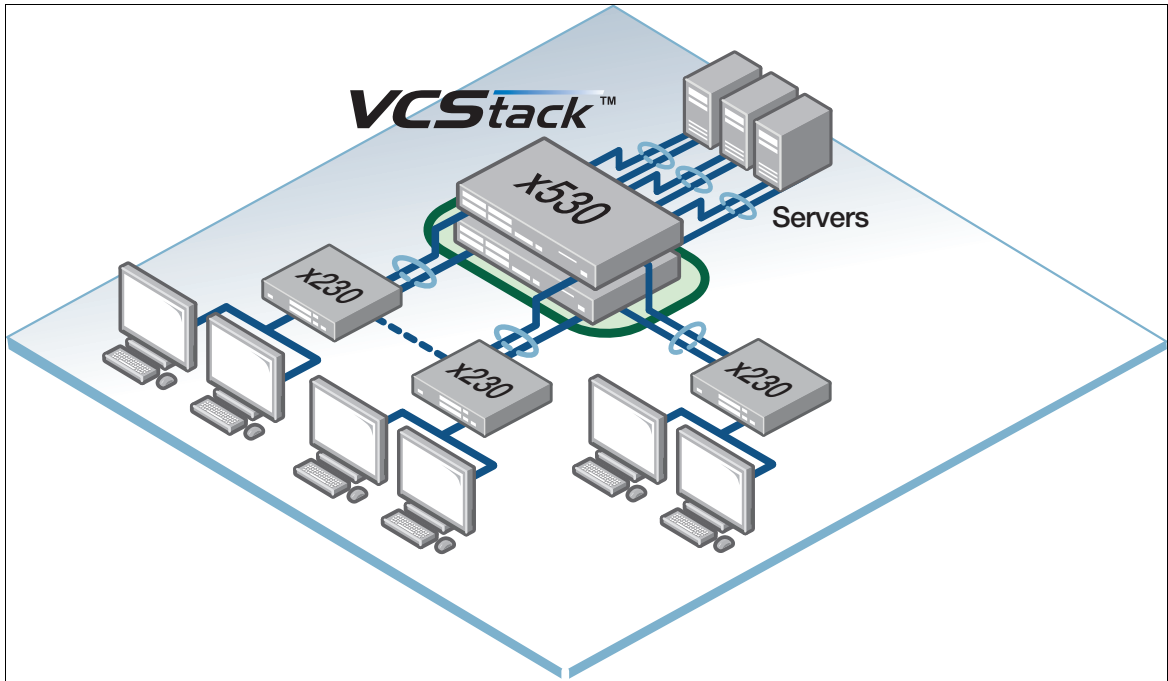
Managing the device

Networking devices such as switches, routers, and firewalls feature a number of different mechanisms for management, which can be broken down into the following groups:

Command Line Interface (CLI):

- Console

- Telnet

- SSH

Graphical User Interface (GUI):

- Web GUI/Interface

This guide provides details of how to manage the device using a **CLI**. Initial configuration of the device must be performed using the CLI, otherwise the device won't be reachable across the network.

You are strongly encouraged to learn how to manage the device using a CLI as this provides a number of benefits including:

- Configuration consistency across devices

- Access to detailed diagnostic information

- Easier remote support

For more information, please see the: Getting Started Feature Overview and Configuration Guide.

Using the GUI to access the CLI

You can also use the Graphical User Interface (GUI) to monitor and manage your device, and access the CLI. Please see the relevant device GUI documents listed here: "Related documents" on page 3

Changing the default username and password

The default username for Allied Telesis devices is **manager** and the default password is **friend**. This should be changed upon initial deployment. To change the password for the default manager account, use the command:

```
awplus(config)# username <manager> password <newpassword>
```

For more information, please see the: Getting Started Feature Overview and Configuration Guide.

Saving the configuration

Any changes made to the configuration take effect immediately on the running configuration of the device, and will affect your live network. You must save the configuration to ensure that these changes become part of the startup configuration that will run if the device is rebooted. This ensures the current configuration will be used after any power outage, software upgrade, or user initiated reboot of the device.

To do this, use the command:

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

For more information, please see the: Getting Started Feature Overview and Configuration Guide.

Device and port numbering

In the AlliedWare Plus Operating System, switch ports are named portx.y.z (e.g. port1.0.1) where:

- x is the stack ID number

- y is the module number

  For ports on the base unit, the module number is 0. For switches with line cards and expansion modules, the module number is the number that is printed on the switch or chassis to indicate the module number.

- z is the port number

For example, the second port on the first x530 unit in the VCStack of the example network on page 4, would be port1.0.2, whereas the fifth port of the second x530 unit in the VCStack would be port 2.0.5.

More about port numbering

In order to simplify the configuration of a number of ports simultaneously, you can specify port ranges. To configure a continuous range of ports at the same time, enter the range in either of the following formats:

```
portx.y.z-portx.y.z
portx.y.z-x.y.z
```

Where the ports are not continuous, you use a comma separated list to specify a number of ports simultaneously:

```
portx.y.z,portx.y.z
```

Continuous and non-continuous port ranges can be mixed by using a combination of the above port numbering conventions. For example:

```
portx.y.z,portx.y.z-portx.y.z
```

For more information, please read the Switching Feature Overview and Configuration Guide.

Links and ports

Link Aggregation Control Protocol (LACP)

LACP is a protocol that enables two or more links to be aggregated or bundled providing greater bandwidth and a level of redundancy in the event of link or interface failure. When used across a stack of switches with VCStack™ enabled, (for example, across the two x530 units as shown in the example network on page 4), or across line cards of a chassis switch, link aggregation also provides redundancy in the event of switch or line card failure.

For example, to configure ports in an LACP bundle, use the following commands:

```
awplus(config)# interface port1.0.5-1.0.6
awplus(config-if)# channel-group 1 mode active
```

To view LACP configuration for the switch, use the **show etherchannel** command:

```
awplus#show etherchannel
LAG Maximum        : 128
LAG Static  Maximum: 96
LAG Dynamic Maximum: 32
LAG Static   Count  : 0
LAG Dynamic Count  : 1
LAG Total    Count  : 1
Lacp Aggregator: po1
Member:
 port1.0.1
 port1.0.2
```

To view the LACP state of a specific LACP bundle and if it is currently active (synchronized):

```
awplus# show etherchannel 1
Aggregator po1 (IfIndex: 4601)
 Mac address: ec:cd:6d:ef:d7:5c
 Admin Key: 0001 - Oper Key 0001
 Receive link count: 2 - Transmit link count: 2
 Individual: 0 - Ready: 1
 Partner LAG: 0x8000,00-00-cd-2a-f6-0d,0x0002
  Link: port1.0.1 (IfIndex: 5001) synchronized
  Link: port1.0.2 (IfIndex: 5002) synchronized
```

When ports are configured for link aggregation and the Spanning Tree Protocol (STP) is enabled, the ports are removed from any Spanning Tree instance.

When VLANs are being configured, the VLAN configuration must be consistent across all ports that are a member of an LACP bundle. For this reason, the VLAN configuration must be applied to the LACP bundle instead of the individual ports.

While static link aggregation can be configured, this should be avoided as it is possible for a link to be inactive and the switches will continue to send traffic across the LACP bundle. For more information, please read the LACP Feature Overview Guide.

Power over Ethernet (PoE)

PoE is a technology that supplies power to network devices by utilizing the same cabling used to carry network traffic. PoE is appropriate for devices that have low power consumption—PDs (Powered Devices) such as wireless access points, IP telephones, Webcams, and even other Ethernet switches.

PoE is defined by the 802.3af, 802.3at and 802.3bt (PoE++) standards. The 802.3af standard supplies a maximum of 15.4W from the switch, 802.3at supplies a maximum of 30W and 802.3bt supplies a maximum of around 90W. See this article, provided by STH for more information on the differences between the PoE standards. For more information about PoE and AlliedWare Plus, see the Power over Ethernet Feature Overview Guide.

Power is allocated to PD's based on the class they are identified as and the switch must allocate this power regardless of how much power is actually required or used. For example, an IP camera may identify itself as a Class 0 device which means the switch must allocate 15.4W even though it may only use a maximum of 4W. When a device is connected that requires power that exceeds the switches overall power capacity, power to that device will be denied which will result in the device not functioning.

To overcome this limitation, the power assigned for each port can be defined statically to ensure that the switch can supply power to the maximum number of devices possible. To view the devices that are powered using POE, their power class or actual power consumption, use the **show power-inline** command:

```
awplus#sho power-inline
PoE Status:

 Stack member 1
 Nominal Power: 370W
 Power Allocated: 14W
 Actual Power Consumption: 3W
 Operational Status: On
 Power Usage Threshold: 80% (296W)
 Detection of legacy devices is enabled
 RPS Boost Mode: Disabled
 High Availability Network Power: Disabled
PoE Interface:
Interface    Admin    Pri  Oper     Power Device        Class Max
                                    (mW)                       (mW)
port1.0.1    Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.2    Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.3    Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.4    Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.5    Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.6    Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.7    Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.8    Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.9    Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.10   Enabled  Low  Powered  1622 n/a              2  7000 [C]
port1.0.11   Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.12   Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.13   Enabled  Low  Powered  1790 n/a              2  7000 [C]
port1.0.14   Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.15   Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.16   Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.17   Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.18   Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.19   Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.20   Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.21   Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.22   Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.23   Enabled  Low  Off         0 n/a            n/a   n/a
port1.0.24   Enabled  Low  Off         0 n/a            n/a   n/a
```

In the output above, you can see that the devices that are powered are identified as Class 2 devices which results in the switch allocating 7000mW, even though they are actually drawing less than 4000mW.

To limit the power supplied to these devices, select the port or port ranges the devices are connected to and use the **power-inline max <power>** command to limit the power supplied:

awplus(config)#int port1.0.10,port1.0.13

awplus(config-if)#power-inline max 4000

It is also possible to show the power parameters of individual ports or a range of ports using the **show power-inline int** command:

```
awplus#show power-inline int port1.0.10,port1.0.13
Interface    Admin    Pri  Oper     Power Device        Class Max
                                    (mW)                       (mW)
port1.0.10   Enabled  Low  Powered  1622 n/a              2  4000 [U]
port1.0.13   Enabled  Low  Powered  1622 n/a              2  4000 [U]
```

Data Link Layer

VLANs

A VLAN is technology that enables a physical network to be broken up into one or more logical networks or Virtual LANs. VLANs are typically used where multiple applications are being deployed across a single network infrastructure. For more information on VLANs, please read the: VLANs Feature Overview and Configuration Guide.

Care must be taken to ensure that VLAN configuration is consistent across the entire network. All switches within the network should have the same VLANs and VLAN IDs configured. In order to simplify deployment and trouble-shooting, all uplink ports should be a member of all VLANs. This ensures that traffic leaving a switch is correctly identified as it reaches the switch at the other end of the link. In the example diagram, the uplink ports of the x230 switches should be tagged for all VLANs, so traffic going to the x530 VCStack network core is correctly identified.

A tool for helping with consistency in configuration of VLANs and other features across a network is the Allied Telesis Management Framework (AMF). AMF can be used to simplify the deployment and ongoing management of networks. For more information about AMF, please read the: AMF Feature Overview and Configuration Guide.

By default, all ports are untagged members of VLAN 1. To create a second VLAN, use the following commands:

```
awplus(config)# vlan database
awplus(config-vlan)# vlan 2
```

A name can be associated with a VLAN to improve manageability of the network:

```
awplus(config-vlan)# vlan 2 name voip
```

Once a VLAN has been created, ports can then be associated with the VLAN. A port can either be an untagged member of a single VLAN, in which case no VLAN header will be sent with the Ethernet frame, or it can be a tagged member of one or more VLANs, in which case the Ethernet frames will include a header to identify which VLAN the frame belongs to.

To configure a port as an untagged member of VLAN 2:

```
awplus(config)# int port1.0.3
awplus(config-if)# switchport access vlan 2
```

To configure a port as an untagged member of VLAN 2 and a tagged member of VLAN 3:

```
awplus(config)# int port1.0.4
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk native vlan 2
awplus(config-if)# switchport trunk allowed vlan add 3
```

To view the VLAN and port state of a switch, use the command:

```
awplus# show vlan brief
```

```
awplus#show vlan brief

VLAN ID  Name     Type    State   Member ports
                                  (u)-Untagged, (t)-Tagged
====  =======  ======  ======  ==============================
1     default  STATIC  ACTIVE  po1(u) port1.0.1(u) port1.0.2(u)
                                   port1.0.5(u) port1.0.6(u) port1.0.7(u)
                                port1.0.8(u) port1.0.9(u)
                                port1.0.10(u) port1.0.11(u)
                                port1.0.12(u) port1.0.13(u)
                                port1.0.14(u) port1.0.15(u)
                                port1.0.16(u) port1.0.17(u)
                                port1.0.18(u) port1.0.19(u)
                                port1.0.20(u) port1.0.21(u)
                                port1.0.22(u) port1.0.23(u)
                                port1.0.24(u) port1.0.25(u)
                                port1.0.26(u) port1.0.27(u)
                                port1.0.28(u)
2     voip     STATIC  ACTIVE  port1.0.3(u) port1.0.4(u)
3     security STATIC  ACTIVE  port1.0.4(t)
```

Spanning Tree Protocol

The Spanning Tree Protocol or STP, is a technology that enables redundancy to be delivered throughout a network while also providing a mechanism for ensuring that broadcast storms don't occur when there are multiple links between switches.

In the example network, if the dotted link between two of the x230 switches was connected, there would be a loop between these two switches and the x530 VCStack core. Ethernet frames could circle this loop indefinitely creating a broadcast storm, and greatly affecting network performance. In a network design with potential loops, STP disables one link to remove the possibility of broadcast storms, and only enables the link again if the loop is removed through reconfiguration, or the failure of an active device or link.

STP includes a number of variations including Rapid Spanning Tree Protocol or RSTP that converges quickly and Multi-instance Spanning Tree Protocol or MSTP which allows multiple Spanning Tree instances to be configured throughout a network.

It is important that the entire network uses a consistent approach to Spanning Tree with Spanning Tree either being disabled throughout the entire network or being enabled across the entire network. Where Spanning Tree is enabled, the following points should be used as an initial configuration:

Ensure that:

■ STP is enabled on all devices

■ STP mode is set to RSTP

■ the core network switch(es) have their Bridge Priority set

■ consistent VLAN configuration is used across all uplink ports
(see the section on "VLANs" on page 10).

■ all non-uplink ports have **autoedge** enabled

By default, all switches running AlliedWare Plus have Spanning Tree enabled and the Spanning Tree mode is set to RSTP. The current Spanning Tree status can be viewed by entering the command:

```
awplus# show span brief
```

```
awplus#show span brief
Default: Bridge up - Spanning Tree Enabled
Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
Default: Root Id 8000:eccd6defd75c
Default: Bridge Id 8000:eccd6defd75c

Port            Designated Bridge    Port Id  Role            State
po1              8000:eccd6defd75c    81f9     Designated      Forwarding
port1.0.3        8000:eccd6defd75c    838b     Disabled        Discarding
port1.0.4        8000:eccd6defd75c    838c     Disabled        Discarding
port1.0.5        8000:eccd6defd75c    838d     Disabled        Discarding
port1.0.6        8000:eccd6defd75c    838e     Disabled        Discarding
port1.0.7        8000:eccd6defd75c    838f     Disabled        Discarding
port1.0.8        8000:eccd6defd75c    8390     Disabled        Discarding
port1.0.9        8000:eccd6defd75c    8391     Disabled        Discarding
port1.0.10       8000:eccd6defd75c    8392     Disabled        Discarding
port1.0.11       8000:eccd6defd75c    8393     Disabled        Discarding
port1.0.12       8000:eccd6defd75c    8394     Disabled        Discarding
port1.0.13       8000:eccd6defd75c    8395     Disabled        Discarding
port1.0.14       8000:eccd6defd75c    8396     Disabled        Discarding
port1.0.15       8000:eccd6defd75c    8397     Disabled        Discarding
port1.0.16       8000:eccd6defd75c    8398     Disabled        Discarding
port1.0.17       8000:eccd6defd75c    8399     Disabled        Discarding
port1.0.18       8000:eccd6defd75c    839a     Disabled        Discarding
port1.0.19       8000:eccd6defd75c    839b     Disabled        Discarding
port1.0.20       8000:eccd6defd75c    839c     Disabled        Discarding
port1.0.21       8000:eccd6defd75c    839d     Disabled        Discarding
port1.0.22       8000:eccd6defd75c    839e     Disabled        Discarding
port1.0.23       8000:eccd6defd75c    839f     Disabled        Discarding
port1.0.24       8000:eccd6defd75c    83a0     Disabled        Discarding
port1.0.25       8000:eccd6defd75c    83a1     Disabled        Discarding
port1.0.26       8000:eccd6defd75c    83a2     Disabled        Discarding
port1.0.27       8000:eccd6defd75c    83a3     Disabled        Discarding
port1.0.28       8000:eccd6defd75c    83a4     Disabled        Discarding
```

The default Spanning Tree **Bridge Priority** is '32768'. Spanning Tree uses the Bridge Priority to determine where the Spanning Tree calculation begins from, the device with the lowest value for Bridge Priority is the root bridge. Where the Bridge Priority is the same for all devices, the device with the smallest MAC address is elected as the root bridge.

You should set the core switch with a lower Bridge Priority than other switches.

To set the Bridge Priority:

```
awplus(config)# span priority
awplus(config)# span priority 8192
```

By default, all ports are configured as standard Spanning Tree ports. Those ports that have edge devices such as workstations, access points, or telephones connected, should be configured as **autoedge ports** to minimize the time for the port to become operational and to ensure the port going down or up does not generate a TCN (Topology Change Notification). TCNs within a network cause all switches to flush their internal tables which will result in network disruption.

To set ports to autoedge:

```
awplus(config)#int port1.0.1-port1.0.24
awplus(config-if)#span autoedge
% Port port1.0.1 is not under spanning tree control
% port is either in a channel group or within an EPSR vlan
% Port port1.0.2 is not under spanning tree control
% port is either in a channel group or within an EPSR vlan
```

Note that as ports 1 and 2 are a member of an LACP bundle, Spanning Tree could not be configured.

For more information about the Spanning Tree Protocol, please read the: STP Feature Overview and Configuration Guide.

Multicasting

Many applications such as hospitality entertainment systems and IP CCTV systems require multicasting to be configured to support the system. Multicasting saves network bandwidth by managing traffic for application like streaming video, so that the traffic is only sent where it is required. The intelligent forwarding of multicast traffic keeps networks running at optimal levels.

Multicast applications require at least one multicast or IGMP querier to be configured on the network and all devices to support multicast or IGMP Snooping. By default, AlliedWare Plus devices have multicast of IGMP Snooping enabled by default. At a minimum, the core switch must be configured for IGMP querying.

To correctly configure IGMP, IGMP querying should be enabled on each VLAN:

```
awplus(config)# int vlan1
awplus(config-if)# ip igmp
awplus(config)# int vlan2
awplus(config-if)# ip igmp
awplus(config)# int vlan3
awplus(config-if)# ip igmp
```

To view the IGMP Snooping tables on a device:

```
awplus#show ip igmp snoop statistics int vlan1
IGMP Snooping statistics for vlan1
Interface:      vlan1
Group:          224.0.5.128
Flags:
Uptime:         00:01:57
Group mode:     Exclude (Expires: 00:02:55)
Last reporter:  192.168.1.73
Source list is empty

Port member list:
port1.0.33 - 175 secs (if)

Interface:      vlan1
Group:          239.255.255.250
Flags:
Uptime:         00:02:01
Group mode:     Exclude (Expires: 00:02:57)
Last reporter:  192.168.1.201
Source list is empty

Port member list:
port1.0.33 - 178 secs (if)
```

To view the IGMP querying information on a device:

```
awplus#show ip igmp group
IGMP Connected Group Membership
Group Address    Interface          Uptime   Expires  Last Reporter
224.0.5.128      vlan1              00:03:39 00:03:18 192.168.1.73
239.255.255.250  vlan1              00:03:43 00:03:22 192.168.1.186
```

For more information, please read the IGMP Feature Overview and Configuration Guide.

Network Layer

IP addressing

Managed Layer 2 and Layer 3 switches enable IP addresses to be assigned to interfaces (VLANs) for management. Layer 3 switches also support the routing or forwarding of traffic from one interface (VLAN) to another. It is important for a consistent approach to VLANs and IP addressing be taken across an entire network.

Consideration should be given to the IP address ranges that are used and public address ranges should only be used where they have legitimately been supplied. Where organizations have not been provided with legitimate public addressed for use, address ranges outlined in RFC1918 must be used.

These address ranges are:

- 10.0.0.0/8   10.0.0.0-10.255.255.255

- 172.16.0.0/12   172.16.0.0-172.31.255.255

- 192.168.0.0/16   192.168.0.0-192.168.255.255

To allocate an IP address to an interface (VLAN):

```
awplus(config)# int vlan1
awplus(config-if)# ip address 192.168.1.1/24
```

To view the currently configured interfaces and IP addresses:

```
awplus#show ip int
Interface          IP-Address        Status          Protocol
lo                 unassigned        admin up        running
vlan1              192.168.1.1/24    admin up        running
vlan2              unassigned        admin up        down
vlan3              unassigned        admin up        down
```

To configure a default route or default gateway for the device:

```
awplus(config)#ip route 0.0.0.0/0 192.168.1.254
```

For more information, please read the IP Feature and Configuration Overview.

When things go wrong (obtaining support)

While this document is intended as a guide for most commonly deployed network scenarios, it is possible that your scenario requires additional functionality not covered in this guide or that things simply don't work as expected.

When things go wrong:

- Review this document and the commands you've entered to ensure that you haven't missed, mis-read, or mis-typed a command.

- Review the Command Reference for the specific hardware model and software version that is currently in use for the functionality you require.

- Log a support request at alliedtelesis.com/support, clearly stating your details, the device and software revision you're using along with a description of the problem you're having.

Show tech-support

When requesting technical support, one of the first items requested will be a copy of **show tech-support** or simply **show tech**. This command generates system and debugging information for the device and saves it to a file. As a large amount of output is generated, the file which is created is saved in a compressed format in the file system of the device with a .gz extension. To generate a tech support file, use the command:

```
awplus# show tech-support
```

Once created, this file can then be copied from the device and provided to Allied Telesis technical support.

Copying files

Allied Telesis devices can store configuration files, debug information and firmware in their file system. It may be necessary to copy files to or from the device in order to perform an upgrade or at the request of Allied Telesis technical support. Copying can be performed to or from the device using a USB device, TFTP, HTTP or SCP.

To copy a file, use the command:

```
awplus# copy <source-name> <destination-name>
```

Examples: To copy the file **newconfig.cfg** to a USB storage device from your device's Flash memory, use the command:

```
awplus# copy flash:/newconfig.cfg usb:/newconfig.cfg
```

To copy a tech-support file to a TFTP server from the devices Flash memory, use the command:

```
awplus# copy flash:/tech-support.txt.gz tftp://10.0.0.1/tech-support.txt.gz
```

For further information about copying files, please refer to the Command Reference for the device and software revision you are using.

Configuring date and time

When experiencing issues in an environment, it is important to be able to accurately correlate activity to identify the correct sequence of events and determine the root cause of the issue. Configuration of accurate date and time settings are critical to achieving this outcome and NTP or Network Time Protocol is essential for synchronizing date and time information across multiple devices.

To configure NTP, set the timezone the device is located in and configure daylight savings timezone offset, use the following commands:

```
awplus(config)# ntp server 192.0.1.23
awplus(config)# clock timezone aest plus 10:00
awplus(config)# clock summer-time AEST recurring 1 Sun Oct 02:00 1 Sun Apr 02:00 60
```

To verify the date and time, use the command:

```
awplus# show clock
```

To display the status of NTP, use the command:

```
awplus# show ntp status
```

Obtaining further support

Allied Telesis encourages the use of the on-line support center for logging and tracking support calls. Should you not receive a satisfactory response or your request is urgent in nature, please contact your local Allied Telesis office and when requesting immediate support, please quote your **Net.Cover** support contract number.

- Allied Telesis support centre can be found at alliedtelesis.com/support.

- Allied Telesis local office contact information can be found at alliedtelesis.com.