AlliedWare Plus™ OS

How To | Configure a VoIP Phone System with PoE/PoE+

Introduction

IP phones use Voice over IP (VoIP) technologies that allow telephone calls to be made over an IP network such as the Internet instead of the ordinary PSTN system. Calls can traverse the Internet, or a private IP Network such as that of a company.

This How To demonstrates how to configure a number of the key features to allow AlliedWare Plus™ switches to control a VoIP network using phones from different manufacturers.

The switches will make use of the following features:

- Power over Ethernet (PoE)
- 802.1x port authentication
- RADIUS server
- LLDP-MED
- DHCP server
- QoS in conjunction with LLDP-MED
- SNMP

This combination of features provides a secure, flexible, solution to enable almost plug-and-play network connectivity for VoIP phones and workstations.

Additional reading about PoE (IEEE 802.3af) and PoE+(IEEE 802.3at) standards is included at the end of this document, see "About Power over Ethernet (PoE and PoE+)" on page 37.

List of terms:

LLDP-MED

Link **L**ayer **D**iscovery **P**rotocol **M**edia **E**ndpoint **D**iscovery is an enhancement to IEEE's 802.1AB LLDP, adding media- and IP telephony-specific messages that can be exchanged between the network and endpoint devices.

802.1x

IEEE 802.1x is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN, either establishing a point-to-point connection or preventing it if authentication fails. It is used for securing wireless 802.11 access points and is based on the Extensible Authentication Protocol (EAP).

What information will you find in this document?

This How To Note begins with the following information:

- "Related How To Notes" on page 2
- "Which products and software version does it apply to?" on page 2

This document describes the phone connection sequence and the setup process for the AT-x600-24Ts-POE/ AT-x600-24Ts-POE+, AT-x900-24XT RADIUS and DHCP Server, and AT-8000GS/24POE. This is followed with a section on verifying the setup. Full configuration files are supplied in the Appendix. See the full Table of Contents on page 3.

Related How To Notes

You also may find the following How To Notes useful:

- How To Configure QoS to prioritize SSH, Multicast, and VoIP Traffic
  http://www.alliedtelesis.com/media/datasheets/howto/aw_qos_ssh_mult_voip.pdf
- How to Use 802.1x Security with AT-WA7400 APs, AT-8624PoE Switches, and Linux's freeRADIUS and Xsupplicant
  http://www.alliedtelesis.com/media/datasheets/howto/use8021x-sec_sd_a.pdf

Which products and software version does it apply to?

This How To Note applies to the following Allied Telesis managed Layer 2 and Layer 3 switches:

- SwitchBlade x8100
- SwitchBlade x908
- x600 and x610 series switches (L3)
- x900 series switches (L3)
- x510 series switches
- AT-8000GS/24POE switches (L2)

It requires AlliedWare Plus™ software version **5.3.3** or later.

Contents

Phone connection sequence

When a PoE powered IP phone is connected to an Ethernet switch, a number of different protocols have to operate in a particular sequence in order to enable secure network access for the phone, and to dynamically configure the phone and the switch to interoperate correctly.

How it all fits together

To illustrate how features fit together to create a VoIP solution, let's work through the sequence of events when a VoIP phone is connected to a PoE port.

The following steps are performed:

1. The **switch detects the presence of the phone** and supplies the correct amount of power to allow it to start up. No configuration is required as PoE is enabled by default.
2. The **phone is authenticated** using 802.1x port authentication. The switch blocks all access to the network through the connected port until this process is completed.
   - The authentication process requires that a **username** and **password** be configured on the phone and that there is a matching user entry in the RADIUS server.
   - The phone sends an **authentication request** to the switch, which then sends the request to its configured RADIUS server.
   - The RADIUS server looks up the username and password in its user database and returns an **authentication success** message.
   - The RADIUS authentication success message will also inform the switch which **VLAN** the phone is to use. The VLAN and its tagging state are configured as user attributes in the RADIUS server. The switch will then set up this VLAN as the Voice VLAN on the port.
3. Based on the VLAN information sent to the switch by the RADIUS server, the switch will then, using LLDP-MED, inform the phone of the VLAN ID that the phone needs to **tag** its packets with. The LLDP-MED frames sent by the switch also inform the phone which values it should put in the **QoS fields** of its packets (802.1p and DSCP fields).

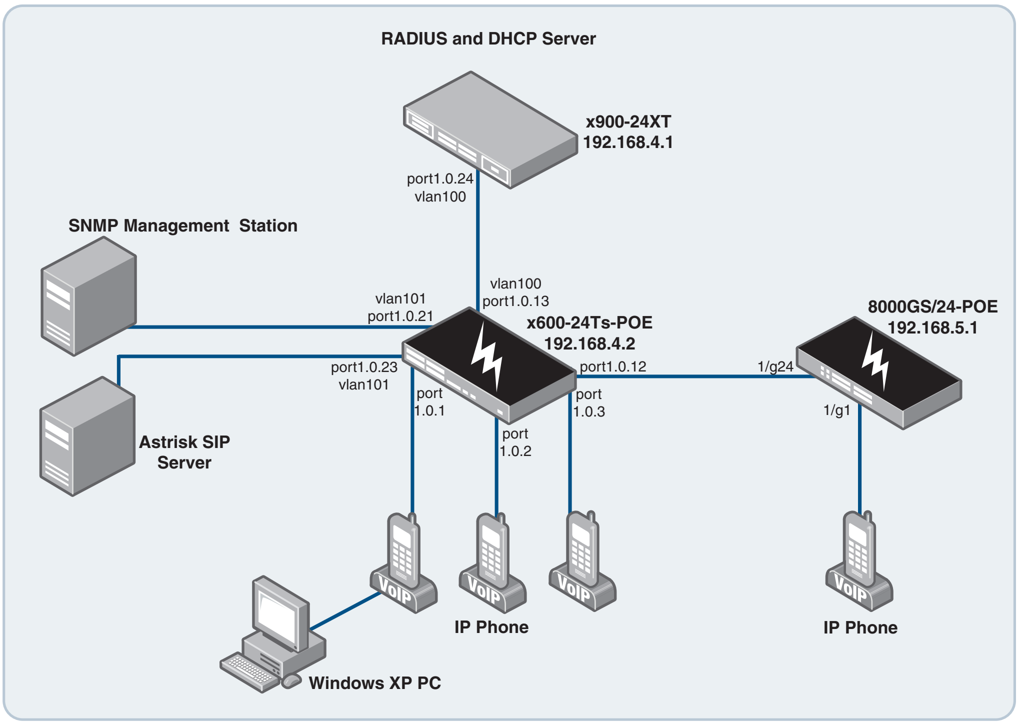
   It is often desirable to treat the voice and data traffic separately so that appropriate Quality of Service (QoS) policies can be applied to each.
4. The **phone requests an IP address**, and other information, from a DHCP server.
   - The DHCP server can assign different options to the phone depending on the phone’s capabilities. For example, the Cisco 7941 can accept TFTP server location and boot file DHCP options from the server, which it then uses to load its configuration.

The phone is now in a state where it can communicate with other devices on the network. At this point it needs to **register** with a **SIP server** and the address of this can also be assigned by the DHCP server using a specific DHCP Option.

Note: The configuration of the SIP server is outside the scope of this document.

5. All traffic sent from the phones will be sent with a specified **Diffserv** value, as described in step 3. The switches will be configured to prioritise this traffic to ensure the voice traffic is always forwarded and with a low latency.
6. The presence of a new phone will then be announced to the SNMP server using SNMP Traps sent by the PoE switch.

Steps 2 and 4 will be repeated for any PCs connected via the PC port on the phones.



AT-x600-24Ts-POE setup

Let us now look in more detail at how to configure the various features on the switch that are involved in the VoIP solution.

Tip When using the AlliedWare Plus command line, typing **Ctrl-D** exits the current mode, and returns the prompt to the previous level. This is equal to the **exit** command.

PoE

Power over Ethernet (PoE) is a mechanism for supplying power to network devices, called Powered Devices (PDs), over the same cabling used to carry the network traffic.

No special configuration is required to enable the PoE feature as this is enabled on all ports by default. This can be disabled using the **no power-inline enable** command on a per port basis.

For example:

```
awplus# conf t
awplus(config)# int port1.0.5
awplus(config-if)# no power-inline enable
```

Note: The maximum possible power requirement on the AT-x600-24Ts-POE (24 ports * 15.4W ~ 370 watts) is below the maximum amount of power available (400 watts). This means that you can connect powered devices to all the ports on the switch without having to be concerned about exceeding the available power.***Reference the updated command for 'enhanced POE power' levels which has been added to 534-04 updated release note for the existing AT-x600-24Ts-POE. ***

802.1x port authentication

The IEEE Standard 802.1x provides a method of restricting access to networks based on authentication information. This functionality allows a network controller to restrict external devices from gaining access to the network behind an 802.1x controlled port. External devices that wish to access services via a port under 802.1x control must first authenticate themselves and gain authorisation before any packets originating from, or destined for, the external device are allowed to pass through the 802.1x controlled port.

The steps you need to configure for 802.1x port authentication are:

1. Specify the address of the RADIUS server along with the shared secret key.

```
awplus# conf t
awplus(config)# radius-server host 192.168.4.1 key testing
```

Note: The shared secret key must be the same as the key specified on the RADIUS server.

2. Enable 802.1x globally and define the authentication method.

```
awplus(config)# aaa authentication dot1x default group radius
```

3. Configure 802.1x on the switch ports that require authentication.

```
awplus(config)#int port1.0.1
awplus(config-if)#dot1x port-control auto
```

Note: This will also add the command **dot1x control-direction both** into the running configuration.

4. Enable portfast, as these ports are not intended to be connected to other switches.

```
awplus(config-if)# spanning-tree portfast
```

5. Enable dynamic VLAN assignment on the ports.

```
awplus(config-if)# auth dynamic-vlan-creation
```

Note: To allow the IP phone to send VLAN tagged traffic, this must be used in conjunction with LLDP-MED, see "LLDP-MED and voice VLAN" on page 7 for more information.

6. Set the authentication host mode to multi-supplicant and the dynamic VLAN creation type to multi. This allows a PC to be connected through the phone using a different VLAN.

   The commands required for this are:

```
awplus(config-if)# auth host-mode multi-supplicant
awplus(config-if)# auth dynamic-vlan-creation type multi
```

LLDP-MED and voice VLAN

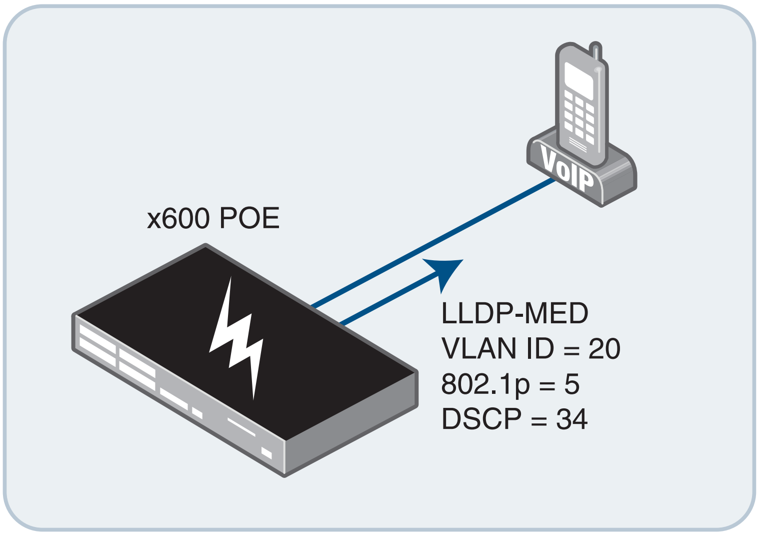
LLDP for Media Endpoint Devices (LLDP-MED) is an extension of LLDP used between LAN network connectivity devices – such as switches – and the media endpoint devices connected to them – such as IP phones.

A powerful feature of LLDP-MED is its ability to carry configuration instructions from the switch to the media devices that are connected to the switch. This configuration information is carried in an LLDP-MED **Network Policy** field. The Network Policy carries information such as the VLAN ID with which the endpoint should tag its packets, and the QoS markers that it should insert into packets.

In AlliedWare Plus, the information that is carried from the switch to the VoIP phones by LLDP-MED is configured as **voice** parameters on the port to which the media device connects. The **voice** parameters that can be configured are:

- the **voice VLAN** configures the VLAN ID and 802.1p values that LLDP-MED will carry in the network Policy. Typically phones use DSCP in preference to VLAN priority.

- the **voice DSCP** configures the DSCP value that LLDP-MED will carry in the network Policy.



The following steps are required for the switch to inform the phones of their VLAN and Diffserv parameters:

1. Enable LLDP.

```
awplus(config)# lldp run
```

2. Enable the voice VLAN feature on authenticating ports (port1.0.1, port1.0.2 and port1.0.3 in this example).

```
awplus(config)# int port1.0.1-1.0.3
awplus(config-if)# switchport voice vlan dynamic
awplus(config-if)# switchport voice vlan priority 5
```

Note: The **dynamic** option on this command specifies that the VLAN ID assigned to the phone will be supplied by the RADIUS server as part of the 802.1x authentication process. Alternatively a VLAN ID can be specified here.

3. Configure the Voice VLAN DSCP value.

```
awplus(config-if)# switchport voice dscp 34
```

Note: This will inform the phone to assign the Diffserv Code point value of 34 to all packets sent. This can then be used later to prioritise traffic using QoS.

Quality of Service (QoS)

To ensure the best quality of voice calls, we want to prioritise voice traffic over all other traffic passing through the switch. The phones will now be sending all traffic with a DSCP value of 34, so the switch will simply place this traffic into a higher queue.

1. Enable QoS.

```
awplus(config)# mls qos enable
```

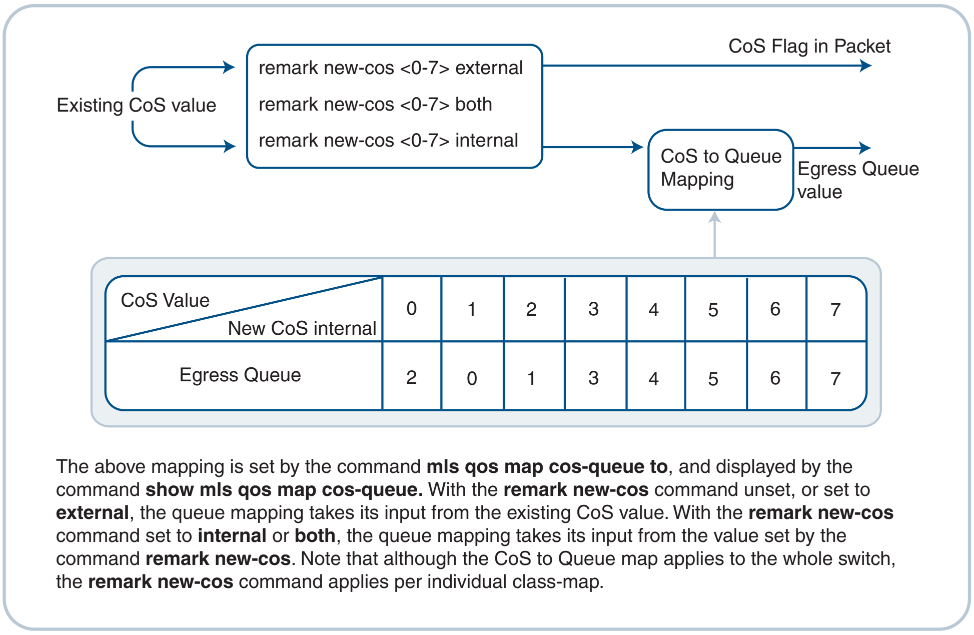
2. Create a class map and set this to match on DSCP value of 34.

```
awplus(config)# class-map voip-cm
awplus(config-cmap)# match dscp 34
```

3. Create a policy map and set all traffic in the class map to be placed in queue 5.

```
awplus(config)# policy-map voip-pm
awplus(config-pmap)# class voip-cm
awplus(config-pmap-c)# remark new-cos 5 internal
```

Note: The **remark** command will change the CoS value of the packet which will then be used to decide which queue to use based on the CoS to queue map.


Existing CoS value
remark new-cos <0-7> external
remark new-cos <0-7> both
remark new-cos <0-7> internal
CoS Flag in Packet
CoS to Queue Mapping
Egress Queue value

CoS Value / New CoS internal	0	1	2	3	4	5	6	7
Egress Queue	2	0	1	3	4	5	6	7

The above mapping is set by the command **mls qos map cos-queue to**, and displayed by the command **show mls qos map cos-queue.** With the **remark new-cos** command unset, or set to **external**, the queue mapping takes its input from the existing CoS value. With the **remark new-cos** command set to **internal** or **both**, the queue mapping takes its input from the value set by the command **remark new-cos**. Note that although the CoS to Queue map applies to the whole switch, the **remark new-cos** command applies per individual class-map.

4. Apply the policy map to all ports which have phones connected.

```
awplus(config)# int port1.0.1-1.0.3
awplus(config-if)# service-policy input voip-pm
```

SNMP

SNMP can be used in conjunction with LLDP-MED to notify a Trap host whenever a new LLDP-MED device is added to the network. The following configuration steps are required for this:

1. Create an access list to allow the SNMP management station to access the switch (optional).

   ```
   awplus(config)# access-list 1 permit 192.168.3.100
   ```

2. Create an SNMP community named **public** with read/write access.

   ```
   awplus(config)# snmp-server community public rw 1
   ```

Note: The last parameter, 1, specifies the access list to use. If no access list is defined this is simply omitted.

3. Specify the host that traps will be sent to.

   ```
   awplus(config)# snmp-server host 192.168.3.100 version 2c public
   ```

4. Enable the sending of LLDP traps globally.

   ```
   awplus(config)# snmp-server enable trap lldp
   ```

5. Enable the sending of LLDP-MED traps (per port).

   ```
   awplus(config)# interface port1.0.1-1.0.3
   awplus(config-if)# lldp med-notifications
   ```

LLDP-MED: Location identification TLV

Location information can be configured for each port, and advertised to remote devices, which can then transmit this information in calls; the location associated with voice devices is particularly important for emergency call services. The location information is advertised to the phones in a LLDP TLV (Type, Length, Value) field. All ports may be configured with the location of the switch, or each port may be configured with the location of the remote voice device connected to it.

At the time of writing none of the phones tested supported this feature. So the following is an example of how this would be configured.

The basic steps are:

- You must first configure a **Location Configuration Information** (LCI) of which there are three types: coordinate-based, Emergency Location Identification Number (ELIN), and civic address.
- The LCI's are configured with an identifier which is a number in the range 1 to 4095.
- Each LCI is then added to a port using its identification number.

1. Enable LLDP.

   ```
   awplus(config)# lldp run
   ```

2. Create a LCI (ELIN type).

   ```
   awplus(config)# location elin-location 1234567890 identifier 2
   ```

3. Add the LCI to a port.

   ```
   awplus(config)# interface port1.0.1
   awplus(config-if)# location elin-location-id 2
   ```

AT-x900-24XT RADIUS and DHCP server setup

At this point, we have completed the configuration of the VoIP solution features on the PoE switch that the phones connect to. Now we move on to the other services that are required in the network in order for the solution to work. In particular, the network requires a:

- RADIUS server to handle authentication requests.
- DHCP server to allocate IP addresses to phones and PCs.

Both of these services can be provided by a switch running AlliedWare Plus. In this section, we look at how to configure those services under AlliedWare Plus.

RADIUS server

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service.

This example has three groups: cisco-phone, generic-phone, and PC. These different groups will then be assigned different VLANs using the **egress-vlan-id** option (this uses the RADIUS attribute type 56 Egress-VLAN ID as defined in RFC4675). This will then determine the DHCP parameters the connected devices will receive.

The VLAN assigned for a PC will be untagged as most PC's cannot receive tagged packets.

The steps needed to configure the local RADIUS sever on AlliedWare Plus are:

1. Enter Local RADIUS server configuration mode.

   ```
   awplus(config)# radius-server local
   ```

2. Enable Local RADIUS server.

   ```
   awplus(config-radsrv)# server enable
   ```

3. Add the client device which the RADIUS server will receive authentication requests from. This includes the shared secret key, which must be the same as the key specified on the client.

   ```
   awplus(config-radsrv)# nas 192.168.4.2 key testing
   ```

4. Create user groups.

```
awplus(config-radsrv)# group cisco-phone
awplus(config-radsrv-group)# egress-vlan-id 20 tagged
awplus(config-radsrv-group)# group generic-phone
awplus(config-radsrv-group)# egress-vlan-id 30 tagged
awplus(config-radsrv-group)# group pc
awplus(config-radsrv-group)# egress-vlan-id 40 untagged
```

5. Create users and assign these into groups.

```
awplus(config-radsrv)# user 2440 password 2440 group generic-phone
awplus(config-radsrv)# user CP-7941G-SEP002545951E11 password
   11111 group cisco-phone
awplus(config-radsrv)# user test password test group pc
```

DHCP server

DHCP is widely used to dynamically assign host IP addresses from a centralized server that reduces the overhead of administrating IP addresses. DHCP helps conserve the limited IP address space because IP addresses no longer need to be permanently assigned to hosts.

The DHCP server uses address pools when responding to DHCP client requests. Address pools contain specific IP configuration details that the DHCP server can allocate to a client. You can configure multiple address pools on the device for different networks.

In this network we will have three pools; one for a generic phone, one for a Cisco phone and one for workstations. This corresponds with the three RADIUS user groups described in the previous section.

All pools will have a network, range, and default router configured as follows:

1. Create a DHCP pool and enter the configuration mode for that pool.

```
awplus# conf t
awplus(config)# ip dhcp pool generic-phone
```

2. Set the network that this pool will assign addresses in.

```
awplus(dhcp-config)# network 192.168.30.0 255.255.255.0
```

3. Configure the range of IP addresses to allocate.

```
awplus(dhcp-config)# range 192.168.30.1 192.168.30.100
```

4. Configure the default router to be assigned to clients.

```
awplus(dhcp-config)# default-router 192.168.30.254
```

5. The two other pools will be configured in the same way.

```
awplus(config)# ip dhcp pool cisco-phone
awplus(dhcp-config)# network 192.168.20.0 255.255.255.0
awplus(dhcp-config)# range 192.168.20.1 192.168.20.100
awplus(dhcp-config)# default-router 192.168.20.254
awplus(config)# ip dhcp pool pc
awplus(dhcp-config)# network 192.168.40.0 255.255.255.0
awplus(dhcp-config)# range 192.168.40.1 192.168.40.100
awplus(dhcp-config)# default-router 192.168.40.254
```

   This is the minimum configuration required by the phones to allow them to connect to the network. The phones will also need to be configured with other network specific parameters and at the very least they will need to be configured with the address of a SIP Server. This could be configured on each phone but it is more desirable to have this type of information configured dynamically. This can be done using **DHCP Options**. Options describe the network configuration, and various services that are available on the network and are configured separately on each pool.

6. Enable the DHCP Server feature

```
awplus(config)# service dhcp-server
```

The DHCP server options for this network are configured as follows:

1. Define the options to use along with a name.

```
awplus# conf t
awplus(config)# ip dhcp option 120 name 120_Sip_Server ip
awplus(config)# ip dhcp option 150 name 150_tftpserver ip
```

Note: In this network we are using a generic phone which will use the SIP server option and a Cisco phone which will load its configuration from the TFTP server.

2. Add the user defined options to the DHCP pool(s).

```
awplus(config)# ip dhcp pool generic-phone
awplus(dhcp-config)# option 120_Sip_Server 192.168.3.1
awplus(config)# ip dhcp pool cisco-phone
awplus(dhcp-config)# option 150_tftpserver 192.168.3.1
```

3. The boot file also needs to be specified for the Cisco phone.

```
awplus(dhcp-config)# bootfile SEP002545951E11.cnf.xml
```

QoS

The x900 also needs a QoS configuration to ensure any voice traffic that passes through this switch is prioritised over other traffic (it is recommended that voice traffic is prioritised on all switches in the network).

This configuration is similar to, but not the same as, the x600 configuration.

1. Enable QoS.

```
awplus(config)# mls qos enable
```

2. Configure a premark-dscp map.

```
awplus(config)# mls qos map premark-dscp 34 to new-queue 5
```

Note: The x900 and x600 series switches have different switching architecture and so the QoS setup is handled differently. This command is used on the x900 series instead of the **remark new-cos** command, as used on the x600 series.

3. Create a class map.

```
awplus(config)# class-map voip-cm
```

4. Create a policy map and set all traffic in the class map to be placed in queue 5.

```
awplus(config)# policy-map voip-pm
awplus(config-pmap)# class voip-cm
awplus(config-pmap-c)# trust dscp
```

Note: The **trust dscp** command is used to enable the premark-dscp map to replace the bandwidth-class, CoS, DSCP, and queue of classified traffic based on a lookup of the DSCP value.

5. Apply the policy map to all ports which may receive voice traffic.

```
awplus(config)# int port1.0.1-1.0.24
awplus(config-if)# service-policy input voip-pm
```

AT-8000GS/24POE setup

The features available on this device do not allow the same level of dynamic behaviour as can be achieved with the AT-x600-24TS-POE.

The AT-8000GS/24POE can be configured to provide either (but not both) of the following functions:

- Dynamic VLAN assignment from the RADIUS sever (via 802.1x), but this is limited to untagged VLANs only. This means it is not possible to have the PC connected through the phone using a different VLAN. This requires several changes to the RADIUS and DHCP server configuration.

- LLDP-MED providing VLAN and DSCP values to the phone. This requires a static VLAN configuration on the port with both a tagged VLAN (for the phone) and an untagged VLAN (for the PC). This requires no changes to the RADIUS and DHCP server configuration.

Dynamic VLAN assignment

802.1x port authentication

The steps you need to configure for 802.1x with Dynamic VLAN assignment are:

1. Specify the address of the RADIUS server along with the shared secret key.

```
console# configure
console(config)# radius-server host 192.168.4.1 key testing
```

Note: The shared secret key must be the same as the key specified on the RADIUS server.

2. Enable 802.1x globally and define the authentication method.

```
console(config)# aaa authentication dot1x default group radius
```

3. Configure 802.1x on the switch ports that require authentication and enable dynamic VLAN assignment on the ports.

```
console(config)# interface ethernet 1/g1
console(config-if)# dot1x radius-attributes vlan
console(config-if)# dot1x port-control auto
```

Note: The commands must be entered in this order.

4. As these ports are not intended to be connected to other switches, portfast should also be enabled using **spanning-tree portfast**. This will ensure the interface will come up quickly and spanning tree topology change messages will not be sent when this port changes state.

RADIUS server configuration

The AT-8000GS/24POE does not support the RADIUS attribute type 56, Egress-VLANID as defined in RFC4675; instead it supports type 81, Tunnel-Private-Group-ID as defined in RFC2868. The differences are:

- Type 56, Egress-VLANID allows the setting of a VLAN ID along with specifying if the VLAN is tagged or untagged.
- Type 81, Tunnel-Private-Group-ID simply allows the setting of a VLAN ID which will be untagged. This must also be used with the types: 64, Tunnel-Type, which is set to 13 to indicate the type is a VLAN and 65, Tunnel-Medium-Type which is set to 6 to specify 802 or Ethernet.

To support the dynamic allocation of VLAN IDs to the AT-8000GS/24POE switch, it is necessary to create groups on the x900 RADIUS server that are specifically configured for supplicants connecting via the AT-8000GS/24POE.

1. Enter Local RADIUS server configuration mode.

   ```
   awplus(config)# radius-server local
   ```

2. Add the client device which the RADIUS server will receive authentication requests from. This includes the shared secret key which must be the same as the key specified on the client.

   ```
   awplus(config-radsrv)# nas 192.168.5.1 key testing
   ```

3. Create User Group and specify VLAN.

   ```
   awplus(config-radsrv)# group 8000GS-phones
   awplus(config-radsrv-group)# vlan 50
   ```

Note: The **vlan** command for the group specifies the VLAN ID and also sets the Tunnel-Type and Tunnel-Medium-Type to the correct values.

4. Create users and assign these into groups.

   ```
   awplus(config-radsrv)# user <username> password <password> group
      8000GS-phones
   ```

Note: This is the same as for the phones connected to the x600.

LLDP-MED

Static VLAN configuration

As with the x600, the AT-8000GS/24POE can pass the voice VLAN and voice DSCP (or Diffserv) information to the phone using LLDP-MED. However, this cannot be used in conjunction with Dynamic VLAN assignment so this needs to be removed from the configuration.

To remove the Dynamic VLAN assignment from the port enter the following:

```
console(config)# interface ethernet 1/g1
console(config-if)# dot1x port-control force-authorized
console(config-if)# no dot1x radius-attributes vlan
console(config-if)# dot1x port-control auto
```

Note: This series of commands disables 802.1x on the port, then removes the Dynamic VLAN assignment feature and then re-enables 802.1x again.

As Dynamic VLAN assignment has been disabled on this port the VLANs now need to be configured manually. In the x600 configuration we used VLAN 30 for Cisco phones. These are configured as follows (the VLANs have already been created).

```
console(config)# interface ethernet 1/g1
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk native vlan 2
console(config-if)# switchport trunk allowed vlan add 30
```

Notes: VLAN 2 is used for 802.1x authentication messages and will also be used by a PC connected through the phone.

This configuration is still using 802.1x Port Authentication. The configuration on the RADIUS server does not need to change when moving phones between the x600 and the AT-8000GS/24POE. Any VLAN information returned in the RADIUS accept message will be ignored.

LLDP-MED configuration

The following steps are required for the switch to inform the phones of their VLAN and Diffserv parameters:

1. Create a Network Policy for the voice traffic.

```
console(config)# lldp med network-policy 1 voice vlan 30 vlan-
   type tagged dscp 34
```

2. Create a Network Policy for the voice signalling traffic

```
console(config)# lldp med network-policy 2 voice-signaling vlan
   30 vlan-type tagged dscp 34
```

3. Enable LLDP-MED network policy on the port

```
console(config)# interface ethernet 1/g1
console(config-if)# lldp med enable network-policy
```

4. Add the LLDP-MED policies to the port.

```
console(config-if)# lldp med network-policy add 1
console(config-if)# lldp med network-policy add 2
```

Verifying the setup

PoE

The PoE status for the x600 can be displayed using the command **show power-inline**:

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

Stack Member 1
 Nominal Power: 370W
 Power Allocated: 15W
 Actual Power Consumption: 7W
 Operational Status: On
 Power Usage Threshold: 80% (296W)

PoE Interface:
Interface   Admin     Pri   Oper      Power  Device              Class  Max
                                       (mW)                             (mW)
port1.0.1   Enabled   Low   Powered   3846  n/a                    2   7295 [C]
port1.0.2   Enabled   Low   Powered   2719  n/a                    2   7295 [C]
port1.0.3   Enabled   Low   Off          0  n/a                  n/a  15400 [C]
port1.0.4   Enabled   Low   Off          0  n/a                  n/a  15400 [C]
port1.0.5   Disabled  Low   Disabled     0  n/a                  n/a  15400 [C]
port1.0.6   Enabled   Low   Off          0  n/a                  n/a  15400 [C]
port1.0.7   Enabled   Low   Off          0  n/a                  n/a  15400 [C]
port1.0.8   Enabled   Low   Off          0  n/a                  n/a  15400 [C]
port1.0.9   Enabled   Low   Off          0  n/a                  n/a  15400 [C]
port1.0.10  Enabled   Low   Off          0  n/a                  n/a  15400 [C]
port1.0.11  Enabled   Low   Off          0  n/a                  n/a  15400 [C]
port1.0.12  Enabled   Low   Off          0  n/a                  n/a  15400 [C]
```

In this example power is being delivered from ports 1.0.1 and 1.0.2.

802.1x port authentication

Check the RADIUS server status

The RADIUS client switch's view of the communication with the RADIUS server.

The first step in verifying the setup of 802.1x is to make sure that the authenticating switch (x600 in this case) is communicating with the RADIUS server.

The command **show radius** is used for this. This will show the configuration parameters and the status of any RADIUS servers that are reachable. In particular check that the Auth Status for the RADIUS server is **alive**.

```
awplus#show radius
RADIUS Global Configuration
  Source Interface    : not configured
  Secret Key          :
  Timeout             : 5 sec
  Retransmit Count    : 3
  Deadtime            : 0 min

Server Host : 192.168.4.1
  Authentication Port : 1812
  Accounting Port     : 1813
  Secret Key          : testing

Server Host/    Auth  Acct  Auth           Acct
IP Address      Port  Port  Status         Status
------------------------------------------------------------
192.168.4.1     1812  1813  Alive          Unknown
```

The command **show radius statistics** can be used to check for errors.

```
awplus#show radius statistics
RADIUS statistics for Server: 192.168.4.1
  Access-Request Tx     : 21 - Retransmit       : 1
  Access-Accept Rx      : 10 - Access-Reject Rx : 0
  Access-Challenge Rx   : 10
  Unknown Type          : 0 - Bad Authenticator: 0
  Malformed Access-Resp : 0 - Wrong Identifier : 0
  Bad Attribute         : 0 - Packet Dropped   : 0
  TimeOut               : 1 - Dead count       : 0
  Pending Request       : 0
```

The RADIUS server's view of the communication with the clients

The command **show radius local-server statistics** can be used on the x900 to verify communication. In the example below, we can see that the NAS 192.168.4.2 has had one successful authentication for each of two phones.

```
Radius#show radius local-server statistics
Server status  : Run (administrative status is enable)
Enabled methods: MAC EAP-MD5 EAP-TLS EAP-PEAP

Successes              :2              Unknown NAS            :0
Unknown username       :0              Invalid passwords      :0
Invalid packet from NAS:0              Internal Error         :0
Unknown Error          :0

NAS : 127.0.0.1
Successes              :0              Shared key mismatch    :0
Unknown username       :0              Invalid passwords      :0
Unknown RADIUS message :0              Unknown EAP message    :0
Unknown EAP auth type  :0              Corrupted packet       :0

NAS : 192.168.4.2
Successes              :2              Shared key mismatch    :0
Unknown username       :0              Invalid passwords      :0
Unknown RADIUS message :0              Unknown EAP message    :0
Unknown EAP auth type  :0              Corrupted packet       :0

Username                     Successes  Failures
2440                                 1         0
CP-7941G-SEP002545951E11             1         0
test-pc                              0         0
```

Check 802.1x status

Check port status:

The command **show dot1x interface** will show if the port is authorized or not along with the status of the dot1x port specific settings.

```
awplus#show dot1x interface port1.0.1
Authentication Info for interface port1.0.1
  portEnabled: true - portControl: Auto
  portStatus: Authorized
  reAuthenticate: disabled
  reAuthPeriod: 3600
  PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: in
  KT: keyTxEnabled: false
  critical: disabled
  guestVlan: disabled
  dynamicVlanCreation: multiple-dynamic-VLAN
  hostMode: multi-supplicant
    maxSupplicant: 1024
  dot1x: enabled
    protocolVersion: 1
  authMac: disabled
  authWeb: disabled
  supplicantMac: none
```

Check a port's session statistics

The command **show dot1x sessionstatistics** will show session up times and the authentication methods for 802.1x authorized users.

```
awplus#show dot1x sessionstatistics
Authentication Session Statistics for interface port1.0.1
  session user name: Winxp-pc
    session authentication method: Remote server
    session time: 3352 secs
    session terminate cause: Not terminated yet
  session user name: CP-7941G-SEP002545951E11
    session authentication method: Remote server
    session time: 248381 secs
    session terminate cause: Not terminated yet
Authentication Session Statistics for interface port1.0.2
  session user name: 2101
    session authentication method: Remote server
    session time: 3707 secs
    session terminate cause: Not terminated yet
Authentication Session Statistics for interface port1.0.3
  session user name: 2440
    session authentication method: Remote server
    session time: 245992 secs
    session terminate cause: Not terminated yet
```

Check 802.1x port counters

The command **show dot1x statistics** shows counters for various 802.1x frame types, including any error frames.

```
awplus#show dot1x statistics
Authentication Statistics for interface port1.0.1
  EAPOL Frames Rx: 21 - EAPOL Frames Tx: 21
  EAPOL Start Frames Rx: 9 - EAPOL Logoff Frames Rx: 0
  EAP Rsp/Id Frames Rx: 6 - EAP Response Frames Rx: 4
  EAP Req/Id Frames Tx: 11 - EAP Request Frames Tx: 4
  Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
  EAPOL Last Frame Version Rx: 1 - EAPOL Last Frame Src: 0040.f4dc.faf6
Authentication Statistics for interface port1.0.2
  EAPOL Frames Rx: 98 - EAPOL Frames Tx: 179
  EAPOL Start Frames Rx: 34 - EAPOL Logoff Frames Rx: 0
  EAP Rsp/Id Frames Rx: 34 - EAP Response Frames Rx: 30
  EAP Req/Id Frames Tx: 96 - EAP Request Frames Tx: 30
  Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
  EAPOL Last Frame Version Rx: 1 - EAPOL Last Frame Src: 0008.5d21.0187
Authentication Statistics for interface port1.0.3
  EAPOL Frames Rx: 3 - EAPOL Frames Tx: 3
  EAPOL Start Frames Rx: 1 - EAPOL Logoff Frames Rx: 0
  EAP Rsp/Id Frames Rx: 1 - EAP Response Frames Rx: 1
  EAP Req/Id Frames Tx: 1 - EAP Request Frames Tx: 1
  Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
  EAPOL Last Frame Version Rx: 1 - EAPOL Last Frame Src: 0800.0f37.b9b9
```

Check authorized devices

The command **show dot1x supplicant** will show all of the supplicants currently authorised on the switch. The output below shows three phones on ports 1.0.1, 1.0.2 and 1.0.3. It also shows a PC connected through the phone on port 1.0.1.

```
awplus#show dot1x supplicant
Interface port1.0.1
  authenticationMethod: dot1x
  totalSupplicantNum: 2
  authorizedSupplicantNum: 2
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 2
    webBasedAuthenticationSupplicantNum: 0
    otherAuthenticationSupplicantNum: 0
  Supplicant name: Winxp-pc
  Supplicant address: 0040.f4dc.faf6
    authenticationMethod: 802.1X
    portStatus: Authorized - currentId: 3
    abort:F fail:F start:F timeout:F success:T
    PAE: state: Authenticated - portMode: Auto
    PAE: reAuthCount: 0 - rxRespId: 0
    PAE: quietPeriod: 60 - maxReauthReq: 2
    BE: state: Idle - reqCount: 0 - idFromServer: 2
    CD: adminControlledDirections: in - operControlledDirections: in
    CD: bridgeDetected: false
Cont...
```

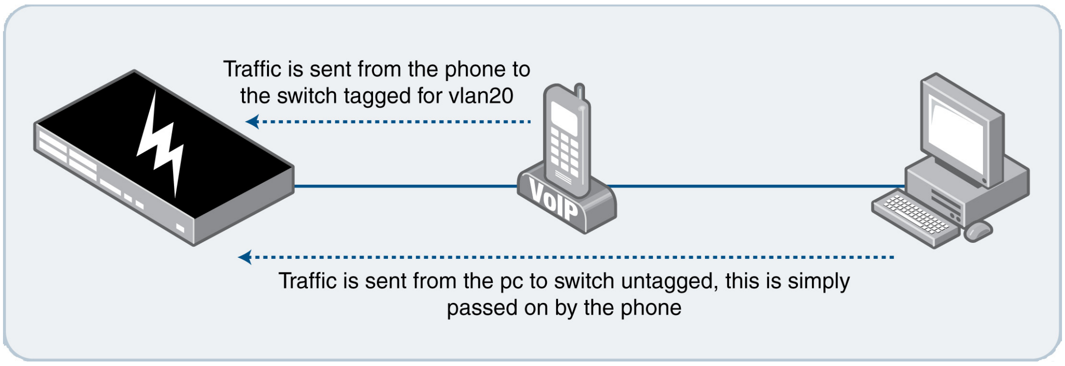
```
    KR: rxKey: false
    KT: keyAvailable: false - keyTxEnabled: false
    dynamicVlanId: 40
    dynamicTaggedVlanId: 0
  Supplicant name: CP-7941G-SEP002545951E11
  Supplicant address: 0025.4595.1e11
    authenticationMethod: 802.1X
    portStatus: Authorized - currentId: 3
    abort:F fail:F start:F timeout:F success:T
    PAE: state: Authenticated - portMode: Auto
    PAE: reAuthCount: 0 - rxRespId: 0
    PAE: quietPeriod: 60 - maxReauthReq: 2
    BE: state: Idle - reqCount: 0 - idFromServer: 2
    CD: adminControlledDirections: in - operControlledDirections: in
    CD: bridgeDetected: false
    KR: rxKey: false
    KT: keyAvailable: false - keyTxEnabled: false
    dynamicVlanId: 0
    dynamicTaggedVlanId: 20

Interface port1.0.2
  authenticationMethod: dot1x
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 1
    webBasedAuthenticationSupplicantNum: 0
    otherAuthenticationSupplicantNum: 0
  Supplicant name: 2101
  Supplicant address: 0008.5d21.0187
    authenticationMethod: 802.1X
    portStatus: Authorized - currentId: 3
    abort:F fail:F start:F timeout:F success:T
    PAE: state: Authenticated - portMode: Auto
    PAE: reAuthCount: 0 - rxRespId: 0
    PAE: quietPeriod: 60 - maxReauthReq: 2
    BE: state: Idle - reqCount: 0 - idFromServer: 2
    CD: adminControlledDirections: in - operControlledDirections: in
    CD: bridgeDetected: false
    KR: rxKey: false
    KT: keyAvailable: false - keyTxEnabled: false
    dynamicVlanId: 0
    dynamicTaggedVlanId: 30
  Interface port1.0.3
  authenticationMethod: dot1x
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 1
    webBasedAuthenticationSupplicantNum: 0
    otherAuthenticationSupplicantNum: 0
  Supplicant name: 2440
  Supplicant address: 0800.0f37.b9b9
    authenticationMethod: 802.1X
    portStatus: Authorized - currentId: 3
  Cont...
```

```
abort:F fail:F start:F timeout:F success:T
   PAE: state: Authenticated - portMode: Auto
   PAE: reAuthCount: 0 - rxRespId: 0
   PAE: quietPeriod: 60 - maxReauthReq: 2
   BE: state: Idle - reqCount: 0 - idFromServer: 2
   CD: adminControlledDirections: in - operControlledDirections: in
   CD: bridgeDetected: false
   KR: rxKey: false
   KT: keyAvailable: false - keyTxEnabled: false
   dynamicVlanId: 0
   dynamicTaggedVlanId: 30
```

Verify PC connection through the phone

As the diagram below shows, a PC can be connected to the switch via the IP phone. In this example both the phone and PC will be authorized on the port using 802.1x. The phone is assigned into VLAN 20 tagged and the PC is assigned into VLAN 40 untagged.


Traffic is sent from the phone to the switch tagged for vlan20
VoIP
Traffic is sent from the pc to switch untagged, this is simply passed on by the phone

The command **show dot1x supplicant** shows that the port has 2 supplicants; the phone, named CP-7941G-SEP002545951E11, has been authenticated; the dynamic tagged VLAN 20 has been assigned for the phone; the PC, named Winxp-pc, has been authenticated and the dynamic (untagged) VLAN 20 has been assigned for the PC.

```
awplus#show dot1x supplicant interface port1.0.1
Interface port1.0.1
  authenticationMethod: dot1x
  totalSupplicantNum: 2
  authorizedSupplicantNum: 2
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 2
    webBasedAuthenticationSupplicantNum: 0
    otherAuthenticationSupplicantNum: 0

Cont...
```

```
Supplicant name: Winxp-pc
  Supplicant address: 0040.f4dc.faf6
    authenticationMethod: 802.1X
    portStatus: Authorized - currentId: 3
    abort:F fail:F start:F timeout:F success:T
    PAE: state: Authenticated - portMode: Auto
    PAE: reAuthCount: 0 - rxRespId: 0
    PAE: quietPeriod: 60 - maxReauthReq: 2
    BE: state: Idle - reqCount: 0 - idFromServer: 2
    CD: adminControlledDirections: in - operControlledDirections: in
    CD: bridgeDetected: false
    KR: rxKey: false
    KT: keyAvailable: false - keyTxEnabled: false
    dynamicVlanId: 40
    dynamicTaggedVlanId: 0
  Supplicant name: CP-7941G-SEP002545951E11
  Supplicant address: 0025.4595.1e11
    authenticationMethod: 802.1X
    portStatus: Authorized - currentId: 3
    abort:F fail:F start:F timeout:F success:T
    PAE: state: Authenticated - portMode: Auto
    PAE: reAuthCount: 0 - rxRespId: 0
    PAE: quietPeriod: 60 - maxReauthReq: 2
    BE: state: Idle - reqCount: 0 - idFromServer: 2
    CD: adminControlledDirections: in - operControlledDirections: in
    CD: bridgeDetected: false
    KR: rxKey: false
    KT: keyAvailable: false - keyTxEnabled: false
    dynamicVlanId: 0
    dynamicTaggedVlanId: 20
```

The VLAN membership can also be verified using the command **show vlan brief**.

```
awplus#show vlan brief

VLAN ID  Name             Type    State   Member ports
                                          (u)-Untagged, (t)-Tagged
======= ================ ======= ======= ================================
1       default          STATIC  ACTIVE  port1.0.1(u) port1.0.2(u) port1.0.3(u)
                                          port1.0.4(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) port1.0.14(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)
                                          port1.0.22(u)
20      cisco-ph         STATIC  ACTIVE  port1.0.1(t)
30      generic-ph       STATIC  ACTIVE  port1.0.2(t) port1.0.3(t)
40      pc               STATIC  ACTIVE  port1.0.1(u)
100     Radius/DHCP      STATIC  ACTIVE  port1.0.13(u)
101     sip-server       STATIC  ACTIVE  port1.0.21(u) port1.0.23(u)
```

LLDP

View LLDP neighbors

The command **show lldp neighbors** will display a summary of connected devices and their capabilities. In the example below, you can see a phone connected to each of ports 1.0.1 - 1.0.3.

```
awplus#show lldp neighbors
LLDP Neighbor Information:

Total number of neighbors on these ports .... 3

 System Capability Codes:
   O = Other   P = Repeater   B = Bridge               W = WLAN Access Point
   R = Router  T = Telephone  C = DOCSIS Cable Device  S = Station Only
 LLDP-MED Device Type and Power Source Codes:
   1 = Class I   3 = Class III    PSE  = PoE    Both = PoE&Local  Prim = Primary
   2 = Class II  N = Network Con. Locl = Local  Unkn = Unknown    Back = Backup

Local    Neighbor        Neighbor        Neighbor                System   MED
Port     Chassis ID      Port ID         Sys Name                Cap.     Ty Pwr
--------------------------------------------------------------------------------
1.0.1    192.168.20.100  002545951E11:P1 SEP002545951E11         --B--T-- 3 Unkn
1.0.2    192.168.30.99   0008.5d21.0187  Aastra IP Phone         --B--T-- 3 Unkn
1.0.3    192.168.30.100  0800.0f37.b9b9  URL 2440@192.168.3.1... --B--T-- 3 Unkn
```

The command **show lldp neighbors detail** will show all of the LLDP information advertised by connected neighbours.

```
awplus#show lldp neighbors detail interface port1.0.2
LLDP Detailed Neighbor Information:

Local port1.0.2:
  Neighbors table last updated 21 hrs 43 mins 2 secs ago

  Chassis ID Type .................. Network address
  Chassis ID ....................... 192.168.30.99
  Port ID Type ..................... MAC address
  Port ID .......................... 0008.5d21.0187
  TTL .............................. 120 (secs)
  Port Description ................. port 0
  System Name ...................... Aastra IP Phone
  System Description ............... Aastra IP Phone
  System Capabilities - Supported .. Bridge, Telephone
                      - Enabled .... Bridge, Telephone
  Management Addresses ............. 192.168.30.99

Cont...
```

```
 Port VLAN ID (PVID) .............. [not advertised]
  Port & Protocol VLAN ............. [not advertised]
  VLAN Names ....................... [not advertised]
  Protocol IDs ..................... [not advertised]
  MAC/PHY Auto-negotiation ......... Supported, Enabled
       Advertised Capability ....... 100BaseTXFD, 100BaseTX, 10BaseTFD,
 10BaseT
       Operational MAU Type ........ 100BaseTXFD (16)
  Power Via MDI (PoE) .............. Not Supported
       Port Class .................. PD
       Pair Control Ability ........ Disabled
       Power Class ................. Class 1
  Link Aggregation ................. [not advertised]
  Maximum Frame Size ............... 1500 (Octets)
  LLDP-MED Device Type ............. Endpoint Class III
  LLDP-MED Capabilities ............ LLDP-MED Capabilities, Network
 Policy,
                                     Extended Power - PD, Inventory
  Network Policy ................... Voice [Unknown]
  Location Identification .......... [not advertised]
  Extended Power Via MDI (PoE) ..... PD
       Power Source ................ Unknown Type 0
       Power Priority .............. High
       Power Value ................. 15.0 Watts
  Inventory Management:
       Hardware Revision ........... 6731i Revision 0
       Firmware Revision ........... 2.5.2.30
       Software Revision ........... [not advertised]
       Serial Number ............... [not advertised]
       Manufacturer Name ...........
 Aastra\x00\x03\x80m6\x80\x80@qt\x00\x00\x00
                                \x00\x00\x00\x00\x00\x80@{\x08\x80@z\xe8
       Model Name .................. 6731i
       Asset ID .................... [not advertised]
```

View LLDP information advertised by the switch

The command **show lldp local-info** will display the information advertised by the switch on a per port basis:

```
awplus#show lldp local-info interface port1.0.2
LLDP Local Information:

Local port1.0.2:
  Chassis ID Type .................. MAC address
  Chassis ID ....................... 0015.77e8.a87c
  Port ID Type ..................... Interface alias
  Port ID .......................... port1.0.2
  TTL .............................. 120
  Port Description ................. [not configured]
  System Name ...................... awplus
  System Description ............... Allied Telesis router/switch, AW+
                                     v5.3.3-0.3
 Cont...
```

```
System Capabilities - Supported .. Bridge, Router
                      - Enabled .... Bridge, Router
  Management Address .............. 192.168.30.254
  Port VLAN ID (PVID) ............. 1
  Port & Protocol VLAN - Supported . Yes
                       - Enabled ... No
                       - VIDs ...... 0
  VLAN Names ...................... default, generic-ph
  Protocol IDs .................... 9000, 0026424203000000,
  0027424203000002,
                              0069424203000003, 888e01, aaaa0300e02b00bb,
                                 88090101, 00540000e302, 0800, 0806, 86dd
  MAC/PHY Auto-negotiation ........ Supported, Enabled
      Advertised Capability ....... 1000BaseTFD, 100BaseTXFD, 100BaseTX,
                                    10BaseTFD, 10BaseT
       Operational MAU Type ........ 100BaseTXFD (16)
  Power Via MDI (PoE) ............. Supported, Enabled
       Port Class .................. PSE
       Pair Control Ability ........ Disabled
       Power Class ................. Class 1
  Link Aggregation ................ Supported, Disabled
  Maximum Frame Size .............. 1522
  LLDP-MED Device Type ............ Network Connectivity
  LLDP-MED Capabilities ........... LLDP-MED Capabilities, Network
  Policy,
                                    Location Identification,
                                    Extended Power - PSE, Inventory
  Network Policy .................. Voice
       VLAN ID ..................... 30
       Tagged Flag ................. Tagged
       Layer-2 Priority ............ 5
       DSCP Value .................. 34
  Location Identification ......... [not configured]
  Extended Power Via MDI (PoE) ..... PSE
       Power Source ................ Primary Power
       Power Priority .............. Low
       Power Value ................. 13.0 Watts
  Inventory Management:
       Hardware Revision ........... X4-0
       Firmware Revision ........... 1.1.1
       Software Revision ........... 5.3.3-0.3
       Serial Number ............... A04264H092800011
       Manufacturer Name ........... Allied Telesis Inc.
       Model Name .................. x600-24Ts-POE
       Asset ID .................... [zero length]
```

View LLDP statistics

The command **show lldp statistics** will show Frame, TLV, and Neighbor counters.

The command displays these statistics **globally** as follows:

```
awplus#show lldp statistics

Global LLDP Packet and Event Counters:

  Frames:    Out ................... 15884
             In .................... 6516
             In Errored ............ 0
             In Dropped ............ 0
  TLVs:      Unrecognized .......... 0
             Discarded ............. 0
  Neighbors: New Entries ........... 14
             Deleted Entries ....... 11
             Dropped Entries ....... 0
             Entry Age-outs ........ 7
```

The command displays these statistics **per interface** as follows:

```
awplus#show lldp statistics interface port1.0.1

LLDP Packet and Event Counters:

port1.0.1
  Frames:    Out ................... 2620
             In .................... 1310
             In Errored ............ 0
             In Dropped ............ 0
  TLVs:      Unrecognized .......... 0
             Discarded ............. 0
  Neighbors: New Entries ........... 2
             Deleted Entries ....... 1
             Dropped Entries ....... 0
             Entry Age-outs ........ 1
```

Appendix - Full configuration files

AT-x600-24Ts-POE

```
!
service password-encryption
!
no banner motd
!
username manager privilege 15 password 8
  $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
access-list 1 permit 192.168.3.100
!
no service ssh
!
service telnet
no service telnet ipv6
!
service http
!
no clock timezone
!
no snmp-server ipv6
snmp-server enable trap lldp
snmp-server community public rw 1
snmp-server host 192.168.3.100 version 2c public
!
exception coredump size unlimited
!
radius-server host 192.168.4.1 key testing
!
aaa authentication dot1x default group radius
!
!
stack virtual-chassis-id 533
!
ip domain-lookup
!
no service dhcp-server
!
no ip multicast-routing
!
lldp run
!
spanning-tree mode rstp
!
no ipv6 mld snooping
!
mls qos enable

!
[Cont...]
```

```
class-map voip-cm
 match dscp 34
!
policy-map voip-pm
 class default
 class voip-cm
  remark new-cos 5 internal
vlan database
 vlan 20 name cisco-ph
 vlan 30 name generic-ph
 vlan 40 name pc
 vlan 100 name Radius/DHCP
 vlan 101 name sip-server
 vlan 2,20,30,40,100-101 state enable
!
interface port1.0.1-1.0.3
 switchport
 switchport mode access
 service-policy input voip-pm
 dot1x port-control auto
 dot1x control-direction in
 auth host-mode multi-supplicant
 auth dynamic-vlan-creation type multi
 spanning-tree portfast
 lldp med-notifications
 switchport voice vlan dynamic
 switchport voice dscp 34
!
interface port1.0.4-1.0.11
 switchport
 switchport mode access
!
  interface port1.0.12
 switchport
 switchport mode access
 switchport access vlan 2
  !
interface port1.0.13
 switchport
 switchport mode access
 switchport access vlan 100
!
interface port1.0.14-1.0.19
 switchport
 switchport mode access
!
interface port1.0.20
 switchport
 switchport mode access
!
interface port1.0.21
 switchport
 switchport mode access
 switchport access vlan 101
!
interface port1.0.22
 switchport
 switchport mode access
[Cont...]
```

```
!
interface port1.0.23
 switchport
 switchport mode access
 switchport access vlan 101
!
interface port1.0.24
 switchport
 switchport mode access
!
  interface vlan2
  ip address 192.168.5.2/24
ip dhcp-relay server-address 192.168.4.1
  !
interface vlan20
 ip address 192.168.20.254/24
 ip dhcp-relay server-address 192.168.4.1
!
interface vlan30
 ip address 192.168.30.254/24
 ip dhcp-relay server-address 192.168.4.1
!
interface vlan40
 ip address 192.168.40.254/24
 ip dhcp-relay server-address 192.168.4.1
!
interface vlan100
 ip address 192.168.4.2/24
!
interface vlan101
 ip address 192.168.3.2/24
!
line con 0
line vty 0 4
!
end
```

AT-8000GS/24POE with dynamic VLANs

Full configuration for example just using 802.1x with Dynamic VLAN Assignment:

```
interface ethernet 1/g1
spanning-tree portfast
exit
interface ethernet 1/g24
switchport mode trunk
exit
  switchport trunk native vlan 2
vlan database
vlan 2,10,20,30,40,50
exit
interface ethernet 1/g24
switchport trunk allowed vlan add 20
exit
interface ethernet 1/g24
switchport trunk allowed vlan add 30
exit
interface ethernet 1/g24
switchport trunk allowed vlan add 40
exit
interface ethernet 1/g24
switchport trunk allowed vlan add 50
exit
  dot1x system-auth-control
interface ethernet 1/g1
dot1x radius-attributes vlan
exit
interface ethernet 1/g1
dot1x port-control auto
exit
interface vlan 2
ip address 192.168.5.1 255.255.255.0
exit
ip default-gateway 192.168.5.2
radius-server host 192.168.4.1 key testing
aaa authentication dot1x default radius
```

AT-8000GS/24POE with static VLANs

Full configuration for example using LLDP-MED with Static VLANs:

```
interface ethernet 1/g1
spanning-tree portfast
exit
interface range ethernet 1/g(1,24)
switchport mode trunk
exit
vlan database
vlan 2,10,20,30,40
exit
interface range ethernet 1/g(1,24)
switchport trunk native vlan 2
exit
interface ethernet 1/g24
switchport trunk allowed vlan add 20
exit
interface range ethernet 1/g(1,24)
switchport trunk allowed vlan add 30
exit
interface ethernet 1/g24
switchport trunk allowed vlan add 40
exit
dot1x system-auth-control
interface ethernet 1/g1
dot1x port-control auto
exit
interface ethernet 1/g1
lldp med enable network-policy
exit
lldp med network-policy 1 voice vlan 30 vlan-type tagged dscp 34
lldp med network-policy 2 voice-signaling vlan 30 vlan-type tagged dscp 34
interface ethernet 1/g1
lldp med network-policy add 1
exit
interface ethernet 1/g1
lldp med network-policy add 2
exit
interface vlan 2
ip address 192.168.5.1 255.255.255.0
exit
ip default-gateway 192.168.5.2
radius-server host 192.168.4.1 key testing
aaa authentication dot1x default radius
```

AT-x900-24XT RADIUS & DHCP server

```
service password-encryption
!
hostname Radius
!
no banner motd
!
username manager privilege 15 password 8
  $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
no service ssh
!
service telnet
!
service http
!
no clock timezone
!
snmp-server
!
exception coredump size large
!
crypto pki trustpoint local
!
crypto pki enroll local
radius-server local
 server enable
 nas 127.0.0.1 key awplus-local-radius-server
 nas 192.168.4.2 key testing
 group cisco-phone
  egress-vlan-id 20 tagged
 group generic-phone
  egress-vlan-id 30 tagged
 group pc
  egress-vlan-id 40 untagged
 user 2101 encrypted password
  IfAWPL3oVNGoJL8ut8aObZz6H0dimjezGsjitvTEf4Y= group generic-phone
 user 2440 encrypted password C42MV+stX/4/
  EuqJXLIKqd2kV1cDvgQxies133iC5Fs= group generic-phone
 user CP-7941G-SEP002545951E11 encrypted password
  r2I8JGfWLgMSR9Ui9tIlgCrRUE1sdzYCpjQEKqhBI7w= group cisco-phone user
  Winxp-pc encrypted password Y4GDytbLNcavpWHT0BRzEvmlnOjJO+PmUMx95Nw1EQ=
  group pc
!
ip domain-lookup
!
ip dhcp option 28 name 28_broadcast ip
ip dhcp option 66 name 66_tftpserver ip
ip dhcp option 120 name 120_Sip_Server ip
ip dhcp option 129 name 129_call_server ip
ip dhcp option 150 name 150_tftpserver ip
ip dhcp option 159 name 159_unassigned_private_mitel ip
ip dhcp option 160 name 160_unassigned_private_mitel ip
  ![cont...]
```

```
ip dhcp pool generic-phone
 network 192.168.30.0 255.255.255.0
 range 192.168.30.1 192.168.30.100
 default-router 192.168.30.254
 option 129_call_server 192.168.3.1
 option 120_Sip_Server 192.168.3.1
!
ip dhcp pool cisco-phone
 network 192.168.20.0 255.255.255.0
 range 192.168.20.1 192.168.20.100
 default-router 192.168.20.254
 option 150_tftpserver 192.168.3.1
 bootfile SEP002545951E11.cnf.xml
!
ip dhcp pool pc
 network 192.168.40.0 255.255.255.0
 range 192.168.40.1 192.168.40.100
!
service dhcp-server
!
no ip multicast-routing
!
spanning-tree mode rstp
!
mls qos enable
mls qos map premark-dscp 34 to new-queue 5
!
class-map voip-cm
!
policy-map voip-pm
 class default
 class voip-cm
  trust dscp
!
vlan database
 vlan 100 name radius
 vlan 100 state enable
!
interface port1.0.1-1.0.20
 switchport
 switchport mode access
 service-policy input voip-pm
!
interface port1.0.21-1.0.24
 switchport
 switchport mode access
 switchport access VLAN 100
 service-policy input voip-pm
!
interface vlan100
 ip address 192.168.4.1/24
!
ip route 192.168.20.0/24 192.168.4.2
ip route 192.168.30.0/24 192.168.4.2
ip route 192.168.40.0/24 192.168.4.2
!
line con 0
  line vty 0 4
!
end
```

About Power over Ethernet (PoE and PoE+)

PoE is a mechanism for supplying power to network devices over the same cabling used to carry network traffic. PoE supplies power to network devices called Powered Devices (PDs). Note that two PoE standards are now supported in this release, IEEE 802.3af and IEEE 802.3at.

The Institute of Electrical and Electronics Engineers (IEEE) 802.3af, Power over Ethernet (PoE), standard specifies how power should be distributed over Ethernet LAN cables to networked devices. The IEEE 802.3af standard was approved in June 2003.

The IEEE 802.3at standard, Power over Ethernet Plus (PoE+), specifies how higher power levels should be distributed over Ethernet LAN cables to networked devices. The IEEE 802.3at standard was approved in September 2009.

PoE (IEEE 802.3af) & PoE+ (IEEE 802.3at) standards

The IEEE 802.3af-2003 Power Ethernet standard, also known as PoE, was formally approved by the IEEE Standards Board in June 2003 and is an amendment to the existing IEEE 802.3 Ethernet standards, and provides up to 12.95W of DC power at each PD. The Power Sourcing Equipment (PSE) supplies up to 15.4W, but 12.95W is available at the PD because some power is dissipated in the cable.

The IEEE802.3at-2009 Power Ethernet standard, also known as PoE+, was formally approved in September 2009, and provides up 25.5W of DC power at each PD. The PoE+ PSE supplies up to 30W, but 25.5W is available at the PD because some power is dissipated in the cable.

The PoE PSE can supply up to 15.4 watts of power (at 48 VDC) to the PoE device, while at the same time providing standard Ethernet network functionality. The PoE+ PSE can supply up to 30 watts of power (at 56 VDC) to the PoE+ device, while at the same time providing standard Ethernet functionality.

PoE and PoE+ require little configuration or management. The PSE automatically determines whether a device connected to a port is a powered device or not, and can determine the power class of the device.

PoE (IEEE 802.3af)

The IEEE 802.3af-2003 standard specifies how power is distributed along with data on standard Ethernet LAN cables. The IEEE 802.3af standard eliminates the need to have separate Ethernet LAN cables for data and electrical outlets for power. Instead both data and power are distributed over the Ethernet cabling.

Power is injected on the Ethernet cabling along with data by Power Sourcing Equipment, like an Ethernet LAN switch or router. Powered Devices, like Wireless Access Points or an IP Phones, receive power and data over the Ethernet cabling. The PSE employs a power classification method for detecting compatible PDs from non-compatible devices and will only provide the maximum power limit to compatible PDs, based on the PoE device class. The PSE continuously monitors the PDs and stops providing power when it is no longer requested or it detects an overload or short circuit condition on the port.

The IEEE 802.3af, Power over Ethernet specification can provide up to 15.4 watts of power at the PSE. A PD under the IEEE 802.3af specification can use no more than 12.95 watts. The difference in maximum power levels provided by the PSE and available at the PD is in accounting for worst case power loss in the cabling between the PSE and PD, which can be influenced by cable length, quality, and other factors. This amount of wattage is sufficient to power the majority of current generation PoE Devices. The IEEE 802.3af physical layer classification is a static power allocation based on power bands for power management.

The benefits of PoE are more lower installation costs, greater installation flexibility, and remote device management. For example, deploying IP Video Security cameras on ceilings and building perimeters can be expensive if separate Ethernet cabling and power outlets are both required.

PoE+ (IEEE 802.3at)

PoE+ supplies the higher power required from a new generation of network attached devices. These new devices, such as, multiple radio IEEE 802.11n wireless access points, powered pan tilt and zoom IP security cameras, thin clients, door locks, touch screen displays, and video phones frequently require more than the 12.95 watts available with IEEE 802.3af.

The IEEE 802.3at specification can provide up to 30 watts of power at the PSE. A PD under the IEEE 802.3at specification can draw up to 25.5 watts of power, which is sufficient to power a new generation of higher powered PDs.

The IEEE 802.3at specification requires that Powered Devices support a flexible Layer 2 power classification method using Link Layer Discovery Protocol (LLDP). The use of LLDP for power classification provides PoE power allocation in steps of of 0.1 watt, along with an ability to reallocate power, for improved power allocation and management between the PSE and PD.

The IEEE 802.3at specification is backwards compatible with the IEEE 802.3af specification. Powered Devices complying with IEEE 802.3af are compatible with the IEEE 802.3at Power Sourcing Equipment.

Devices that support the IEEE 802.3at specification are optimized to operate with IEEE 802.3at Power Sourcing Equipment to support dynamic power management. PSEs that support the IEEE 802.3af specification interoperate with IEEE 802.3at compliant PDs, as long as the PD can operate using 12.95 watts of power (but without dynamic power allocation and management).

Differences between PoE and PoE+

There are three major differences between the IEEE 802.3af (PoE) specification and the IEEE 802.3at (PoE+) specification, which allow for the higher wattage needed to power recent PDs:

- The IEEE 802.3af specification provides for a voltage range from a minimum of 44 volts DC provided by the Power Sourcing Equipment. The IEEE 802.3at specification increases the minimum voltage to 50 volts DC provided by the Power Sourcing Equipment. The higher voltage allows PoE+ PSEs to provide more wattage than PoE PSEs
  (the maximum wattage is 30 watts for PoE+ PSEs compared to 15.4 watts for PoE PSEs).
- The IEEE 802.3af specification supports the usage of Category 3 (CAT3) Ethernet LAN cables or higher (i.e. CAT4 through CAT6A). The IEEE 802.3at specification requires the usage of Category 5e (CAT5e) Ethernet LAN cables or higher (i.e. CAT6 or CAT6A). The usage of higher category Ethernet LAN cables reduce the cable resistance, allowing more power or wattage to be provided from the PSE to the PD, when comparing PoE+ to PoE.
- The IEEE 802.3af specification provides up to 350 mA of current. The IEEE 802.3at specification provides up to 600 mA of current. Both provide a minimum of 10 mA.

Increased power available from PoE ports

The x600-24Ts-POE switch, can supply more power to PoE ports (the voltage available is still 48V), as described below:

By default, the switch supplies the maximum power limit for the class of the powered device connected to the port. In most cases the default settings will work well. We recommend configuring the new higher maximum power values only if required for particular powered devices connected to particular PoE ports.

The command line interface allows you to enter a value in the range 4000 to 30000 milliWatts:

```
awplus(config-if)# power-inline max <4000-30000>
```

However, the switch rounds this to the nearest available value, and the console reports the actual maximum power value configured for the port. For the x600-24Ts-POE switch, the maximum value available for an individual PoE port is approximately 20W. Entering a higher power value with this command results in a console message like this:

```
The maximum power for port1.0.2 has been rounded to 20625mW in
   hardware.
```

The new higher power value cannot be supplied to all the PoE ports at the same time, because this would exceed the total power available from the switch (370W). Up to 18 ports can supply the maximum power value at the same time. If you configure ports that have powered devices connected to them for a total of more power than the switch can supply, then the configured maximum power will be allocated or denied to each port according to the priorities configured by the command:

```
    awplus(config-if)# power-inline priority {low|high|critical}
```

and the port numbers—for the same priority values, lower-numbered ports are supplied before higher-numbered ports.

For more information about Power over Ethernet on the switch, including power classes, port prioritisation, and other aspects of PoE configuration, see the *Power over Ethernet Introduction* and *Power Over Ethernet Commands* chapters in the *Software Reference*.

Allied Telesis

the **solution :** the **network**

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

alliedtelesis.com