Case Study: The QoS H.323 Network at University of Wales, Aberystwyth

The UWA (University of Wales, Aberystwyth) gatekeeper currently has seven H.323 videoconferencing endpoints in its zone. These consist of:

- four UWA WVN PictureTel 970 CODECs (each with a potential bandwidth of up to 2Mbit/s).
- two Leadtek BVP 8770 H.323 videophones. These have a maximum bandwidth of 640kbit/s.
- a Tandberg® 8000, with a maximum bandwidth of 768kbit/s.

These are distributed around the University as follows:

- ABER-PENGLAIS-HOL (HOL), a 970, is on the main campus.
- ABER-PENGLAIS-WVN (WVN), a 970, is also on the main campus.
- ABER-DILS-125 (DILS), a 970, is on a remote campus, located a mile away from the main campus. The two campuses are linked by a dedicated fibre. As well as University departments, this link also supports the Welsh Institute for Rural Studies (formerly the Welsh Agricultural College).
- ABER-OLDCOL-1LP (1LP), a 970, is situated in the Old College and is linked to the main campus over 100Mbit/s microwave link.
- ABER-PENGLAIS-IS (IS) is a Tandberg® 8000 which is also on the main campus.
- The Leadtek videophones are currently set up to be portable around the college, so are usually only connected temporarily. They can register with the gatekeeper with various IP addresses, depending on their physical location.

There are also two WVN studios on adjacent organisations' networks that are registered with the UWA gatekeeper and whose data is also routed through the UWA Cisco® MCM (Multimedia Conference Manager) H.323 proxy. These are the National Library of Wales (referred to here as NLW) and the second campus of Coleg Ceredigion, the local Further Education College (referred to here as CC).

This example examines how the different studios at UWA have been connected to the gatekeeper, and to the SAR, and what QoS measures have been taken to support the use of these CODECS.

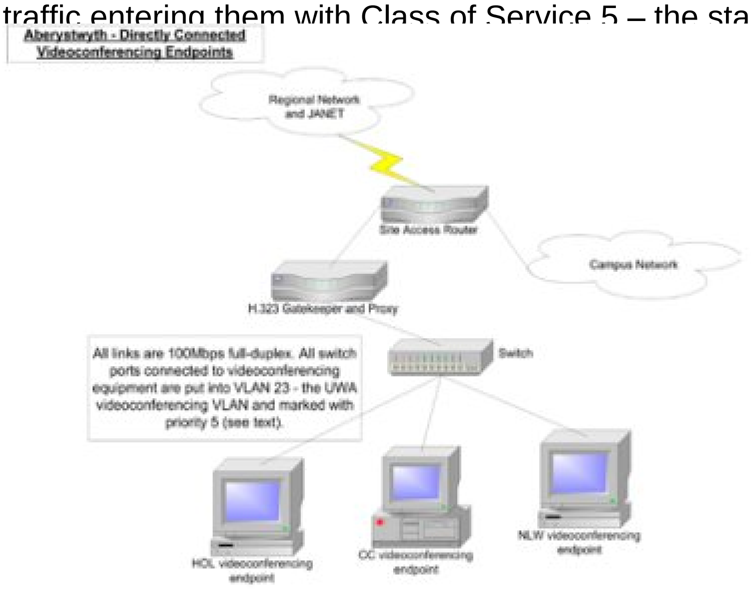
Description

All studios are on the same Class C IP subnet, which has been designated for H.323 endpoints. The HOL, CC and NLW studio CODECs are physically directly connected through patched fibre to ports on a dedicated switch. This is a Cisco® Catalyst® 3524, a 24-port switch. Another port on the switch connects to a Cisco® Catalyst® 3662 router (the MCM router) that is running the H.323 gatekeeper and H.323 proxy based on Cisco® MCM. This is a security measure rather than a QoS one.

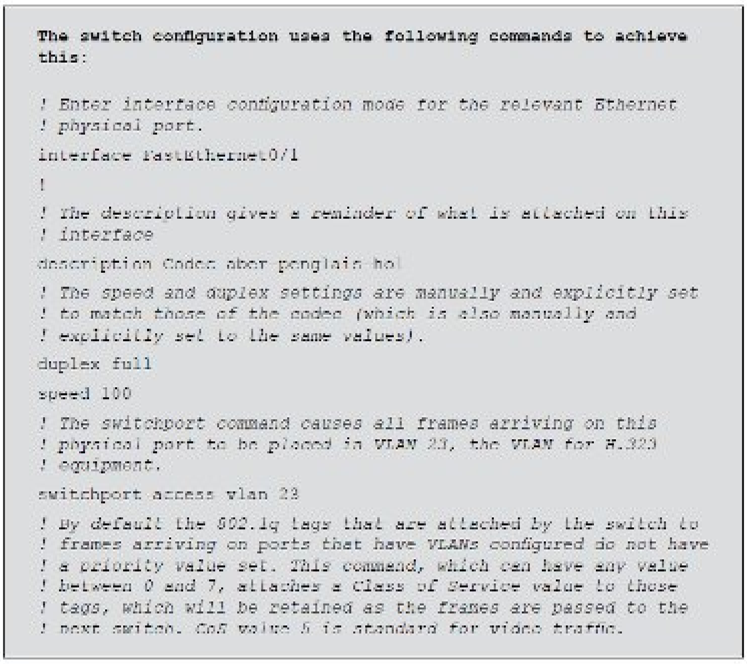
Many of the techniques for offering QoS support to real-time applications described in this report are deployed at UWA. There are directly connected studios and also videoconferencing endpoints that are connected across the campus LAN with VLAN and CoS support, in most cases via trunked VLANs.

All links shown in Figure 10 (overleaf) are 100Mbit/s full-duplex – set on both the switch end of the link and on each of the videoconferencing endpoints. The switchports are also set to mark traffic entering them with Class of Service 5 – the standard CoS marking for video traffic.

points at UWA.


Aberystwyth - Directly Connected
Videoconferencing Endpoints
Regional Network and JANET
Site Access Router
Campus Network
H.323 Gatekeeper and Proxy
Switch
All links are 100Mbps full-duplex. All switch ports connected to videoconferencing equipment are put into VLAN 23 - the UWA videoconferencing VLAN and marked with priority 5 (see text).
HOL videoconferencing endpoint
CC videoconferencing endpoint
NLW videoconferencing endpoint

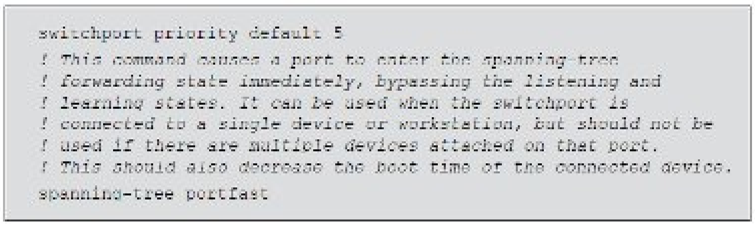
[1]



The switch configuration uses the following commands to achieve this:

```
! Enter interface configuration mode for the relevant Ethernet
! physical port.
interface FastEthernet0/1
!
! The description gives a reminder of what is attached on this
! interface
description Codec aber penglais hol
! The speed and duplex settings are manually and explicitly set
! to match those of the codec (which is also manually and
! explicitly set to the same values).
duplex full
speed 100
! The switchport command causes all frames arriving on this
! physical port to be placed in VLAN 23, the VLAN for H.323
! equipment.
switchport access vlan 23
! By default the 802.1q tags that are attached by the switch to
! frames arriving on ports that have VLANs configured do not have
! a priority value set. This command, which can have any value
! between 0 and 7, attaches a Class of Service value to those
! tags, which will be retained as the frames are passed to the
! next switch. CoS value 5 is standard for video traffic.
```

[2]



```
switchport priority default 5
! This command causes a port to enter the spanning-tree
! forwarding state immediately, bypassing the listening and
! learning states. It can be used when the switchport is
! connected to a single device or workstation, but should not be
! used if there are multiple devices attached on that port.
! This should also decrease the boot time of the connected device.
spanning-tree portfast
```

[3]

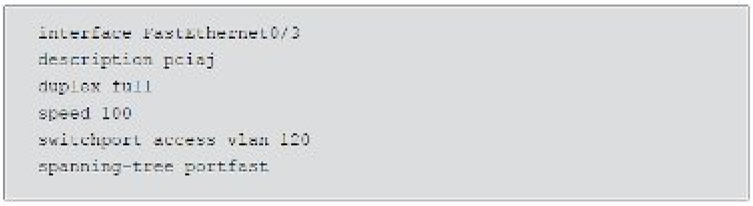
All switches that connect videoconferencing endpoints do so by placing them into a VLAN (with the exception of the videophones, which move around to different locations at the University). All of the switches that are directly connected to videoconferencing endpoints place them in VLAN 23 and assign priority 5 to inbound frames on that port. So the same set of instructions would be used at those locations.

H.323 traffic that is received by the gatekeeper/proxy and forwarded to the videoconferencing endpoints also needs to receive QoS support as far as possible. The gatekeeper and H.323 proxy are also in the same subnet and VLAN as the other H.323 equipment. A similar set of commands is issued to place the gatekeeper in VLAN 23, and to tag frames received on the gatekeeper's port with CoS priority 5 for forwarding to the videoconferencing endpoints.

Videoconferencing Endpoints Connected over Trunked VLANs

The situation is a little different where a switch is receiving frames from videoconferencing endpoints and also from other equipment, such as workstations etc. Care then has to be taken to apply the correct VLANs and priorities to the different ports.

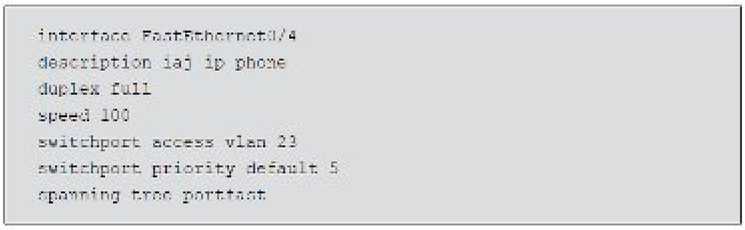
In the next command extract, a workstation is attached on an interface and is placed in VLAN 120 – the default VLAN for staff workstations



```
interface FastEthernet0/3
description pciaj
duplex full
speed 100
switchport access vlan 120
spanning-tree portfast
```

[4]

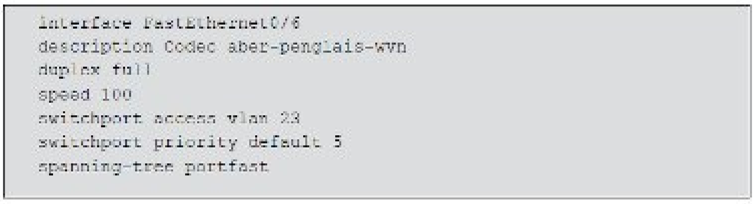
The next extract configures an IP phone. Currently there are a few IP telephones deployed at UWA and these are placed in the same VLAN, as they are also H.323 equipment. It should be noted, however, that the QoS settings for a discrete VoIP deployment would differ from those deployed for a videoconferencing network. In these cases manufacturers recommend different parameters and – in some cases – have developed specific commands and architectures for supporting VoIP/IP telephony in the LAN, which are beyond the scope of this report.



```
interface FastEthernet0/4
description iaj ip phone
duplex full
speed 100
switchport access vlan 23
switchport priority default 5
spanning-tree portfast
```

[5]

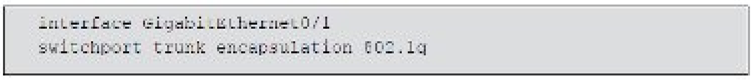
The switchport that is connected to the H.323 videoconferencing endpoints is configured in the same way as the directly connected example:



```
interface FastEthernet0/6
description Codec aber-penglais-wvn
duplex full
speed 100
switchport access vlan 23
switchport priority default 5
spanning-tree portfast
```

[6]

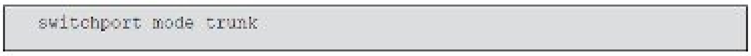
Many irrelevant commands that are in the Cisco® running configuration of this switch are omitted here. The next commands that are of interest are those that trunk the various VLANs:



```
interface GigabitEthernet0/1
switchport trunk encapsulation 802.1q
```

[7]

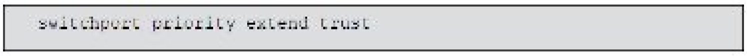
Trunking is a way of carrying traffic from several VLANs over a point-to-point link between two devices. The trunk combines a number of VLANs over a particular link. There have to be corresponding instructions at the other end of the link – in other words, the VLAN trunk link needs to be set up explicitly at both ends of each link. The command line at the other end of the trunk link will be identical. Because there are standard and proprietary methods of configuring VLAN trunks (i.e. there are proprietary alternatives to 802.1q), the command above is used to specify the mode of trunk signalling to be used. In this case the mode is 802.1q, and is the open standard method and not a proprietary one.



```
switchport mode trunk
```

[8]

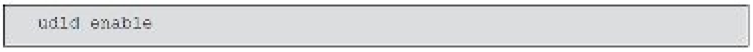
There are various arguments to the switchport mode command – in this case the argument trunk has the effect of forcing the interface to become a VLAN trunk irrespective of the configuration of the device at the other end of the link.



```
switchport priority extend trust
```

[9]

This command tells the switch to trust, act on and pass on the priority or CoS levels found on the 802.1q tagged frames (i.e. those in VLANs) arriving on this physical port. This command can also be used when a H.323 terminal (phone or video videoconferencing endpoint) is the only device attached on a particular port, and the terminal has configurable QoS/CoS parameters.



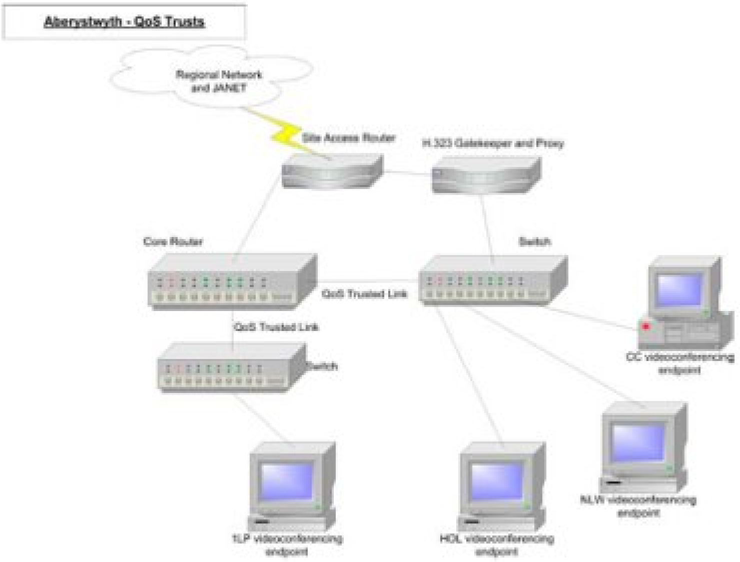
```
udld enable
```

[10]

This command enables the ULDP (Unidirectional Link Detection Protocol) which is necessary whenever STP is running. The ULDP needs to be enabled on both ends of a link to work, but uses information from Layers 1 and 2 to ensure bi-directional physical links are still capable of sending frames in either direction (even though they may be blocked from doing so). If it detects that a link has become unidirectional, it disables the port completely in order to stop possible loop and/or 'black holes'. For more information please see (Cisco, 2003b).

The above commands are run on the switch (and port) that the 1LP CODEC is attached to. This means frames issuing from the 1LP CODEC are prioritised in the switch(es) between it and a central Layer 3 router. The Layer 3 router sends non-H.323 service packets towards the

SAR, but in-service H.323 packets are routed towards the gatekeeper. Because of the network of trust (see Figure 11 below) that has been built, the frame will continue to receive priority treatment as it traverses the switch(es) between it and the gatekeeper/proxy.


Aberystwyth - QoS Trusts
Regional Network and JANET
Site Access Router
H.323 Gatekeeper and Proxy
Core Router
Switch
QoS Trusted Link
QoS Trusted Link
Switch
CC videoconferencing endpoint
NLW videoconferencing endpoint
TLP videoconferencing endpoint
HOL videoconferencing endpoint

[11]

It is worth noting that, depending on the way a videoconference call is dialled from a videoconferencing endpoint, the H.323 traffic can flow in two different ways. H.323 calls set up using E.164 Global Dialling Scheme numbers (Williams, 2002) will use the H.323 proxy and all the H.323 traffic in that call will go through the H.323 proxy. Conversely, if a videoconference call is dialled using an IP address or hostname, the H.323 traffic that is part of that call will not use the H.323 proxy and will follow the normal, default traffic path into and out of the campus. This is due to the different way that E.164 GDS numbers are resolved compared to IP addresses that need no resolution or hostnames that use simple DNS name to IP address mapping. Other non H.323 traffic, such as web page accesses from a PC-based videoconferencing endpoint, will also be routed out to JANET in the normal way.

The inward facing port on the gatekeeper and H.323 proxy is part of the same subnet as the rest of the H.323 equipment on the campus. The outward facing port (i.e. the link to the SAR) has an IP address seen by external internet hosts. The proxy acts as an IP/IP gateway between these two nets, so all GDS dialled set-up, control and media packets are routed through this proxy, and receive (or will receive) QoS support in the LAN, the MAN and the JANET core, based on the parameters of these packets. Out-of-service calls, dialled by IP address, do not use the H.323 proxy and so are routed in a Best Efforts fashion, taking their chances with all of the other Internet packets taking this route.

Source URL: https://community-stg.jisc.ac.uk/library/janet-services-documentation/case-study-qos-h323-network-university-wales-aberystwyth

Links
[1] http://community.ja.net/system/files/h323guide10.jpg
[2] http://community.ja.net/system/files/h323guide-code15.jpg
[3] http://community.ja.net/system/files/h323guide-code16.jpg
[4] http://community.ja.net/system/files/h323guide-code17.jpg
[5] http://community.ja.net/system/files/h323guide-code18.jpg
[6] http://community.ja.net/system/files/h323guide-code19.jpg

[7] http://community.ja.net/system/files/h323guide-code20.jpg

[8] http://community.ja.net/system/files/h323guide-code21.jpg

[9] http://community.ja.net/system/files/h323guide-code22.jpg

[10] http://community.ja.net/system/files/h323guide-code23.jpg

[11] http://community.ja.net/system/files/h323guide11.jpg