Traffic Engineering 1: Logical Separation at Layer 2 - the VLAN

In many cases, it will not be possible to physically separate H.323 and campus network traffic, and it will be necessary for all traffic to share the same physical links. In this case there are some methods that can be used to provide some level of protection to H.323 traffic, above that provided to the campus traffic.

This section will look at the concept and practice of providing Virtual LANs or VLANs and then Chapter 6 will look at ‘persuading’ network equipment to queue and forward traffic differently, based on what that traffic is, i.e. providing preferential treatment to H.323 traffic. A VLAN is, in effect, an overlay network that uses the underlying physical network to provide one or more virtual LANs on top of it. At installation, a physical LAN will map to the default VLAN (usually VLAN 1) and so any broadcast traffic sent by any host will be forwarded to all other hosts on the network.

The physical network can then be further split up into a number of VLANs, such that a broadcast will be restricted to be within the VLAN only, and will only be seen by other hosts in the same VLAN, rather than all the hosts on the same physical LAN. A typical use of a VLAN is where a common group of users are topologically spread out, but for whatever reasons need to be in the same broadcast domain. That could be for server requirements or other application needs, but the network administrator does not want their traffic to be seen on the rest of the network, whether that is for load, security or other reasons. Placing all the hosts in the same VLAN will allow hosts spread around the campus network to act as though they are in their own, dedicated LAN. They will receive no broadcast traffic from outside the VLAN and will send no broadcast traffic out of the VLAN.

VLANs can be used to:

- provide extra security
- create logical groups that reflect organisational structure
- cut down on unwanted or unnecessary traffic
- reduce broadcasts
- ease network management.

It should be remembered that VLANs are Layer 2 constructions and any traffic that needs to move outside the VLAN will require a Layer 3 routing decision to be taken – in the same way as if it was a collection of separate physical LANs connected to a router. For this reason VLANs and IP subnets are generally identical in scope.
In the case of H.323 equipment, a VLAN can be used to protect the videoconferencing equipment, and the network links to that equipment, from receiving certain broadcast traffic, thus relieving the equipment’s network link and interface of handling that additional load.

Figure 8 (overleaf) shows the use of a VLAN to link H.323 videoconferencing equipment together.

To configure a VLAN port on a Cisco® 2950 switch:

```
! in Interface Configuration mode
Switch(config)#int fa 0/3
Switch(config-if)#switchport access vlan 323
%Access VLAN does not exist. Creating VLAN 323
Switch(config-if)#int fa0/4
Switch(config-if)#switchport access vlan 323
Switch(config-if)#CTRL-Z
```

As can be seen, if the VLAN does not currently exist the switch will automatically create it as soon a port is put into it.

Showing the running configuration gives:

```
…!
interface FastEthernet0/2
!
interface FastEthernet0/3
switchport access vlan 323
!
interface FastEthernet0/4
switchport access vlan 323
!…
```

Figure 8: Simple VLANs.

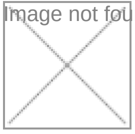


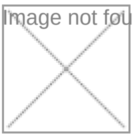
Image not found or type unknown

This will allow the equipment connected to VLAN 323 ports to communicate with each other, and all the other ports in the default VLAN 1 to talk to each other, but at the moment there is no method of sending traffic from one VLAN to the other which of course is essential. In most cases, the core network switch at a campus will be a device that is capable of Layer 3 operation as well as Layer 2 switching. In this case, the routing decision for inter-VLAN traffic can take place within the same switch. See section 5.1 on inter-VLAN routing. The simple example above shows VLANs on a single switch, but in most situations the VLANs will need to span more than a single switch. One way to link two switches together that have VLANs configured is simply to provide two separate physical links between the switches, one for each VLAN, and put those link ports into the appropriate VLANs. However, in general, where there are a number of VLANs in use, providing physical links per VLAN will not be scaleable.

In order to allow VLANs to traverse inter-switch links, VLAN trunks can be established which consist of a single physical link that is capable of supporting as many VLANs as are configured on the switch. It is worth remembering that a single host connected to a port can only be in one VLAN, but inter-switch links can support as many VLANs as required.

There is a standard for providing inter-switch VLAN trunks – however, that does not mean that there are no proprietary options available as well. The standard for VLAN trunking is based on 802.1q – also referred to as simply ‘dot1q’. In theory, and mostly in practice, 802.1q allows different manufacturers’ switches to trunk VLANs successfully between them. Cisco® have an alternative which is known as ISL (Inter-Switch Link). This document will assume 802.1q VLANs will be used.

Figure 9 shows the topology with trunked VLANs between the switches. At this stage this will allow the dotted and dashed links to communicate between the switches – now, there are truly two virtual LANs, and at this stage it should be remembered that there is no provision for inter-VLAN traffic as Layer 3 routes between the VLANs have not been configured.



It is of course possible to place an entire switch, and all its connected hosts and downstream switches, into a VLAN by simply configuring a VLAN on the port on the upstream switch to which it connects. The alternative would be specifically to place all the ports in the switch, andthe link ports, into the VLAN.

To configure a VLAN port on a 3Com® 4400 switch

Firstly, the VLAN must be explicitly created

Select Menu Option: bridge vlan create 323 VIDEO-VLAN

Here 323 is the VLAN ID and VIDEO-VLAN is the text name of the VLAN

Select Menu Option: Bridge vlan modify addport 323 1:2 untagged

This adds VLAN 323 to port 1:2 (unit 1: port 2). The untagged keyword tells the switch that a host will be connected to this port and it is not a VLAN trunk.

You will see that for Switch 1, the Cisco® 3524, the VLAN trunk encapsulation has been explicitly set to 802.1q. By default the 3524 uses Cisco® ISL rather than 802.1q encapsulation for VLAN trunks.

However, Switch 2, the Cisco® 2950, has no support for ISL and so uses 802.1q by default – hence there is no encapsulation command for Switch 2.

Figure 9: Trunked VLANs.

To configure a VLAN trunk for all VLANs between two Cisco® switches:

```
Switch 1 (Cisco® 3524)
! Port 0/24 is the link to the second switch
Int fa0/24
switchport trunk encapsulation 802.1q
switchport mode trunk
Switch 2 (Cisco® 2950)
!
Int fa0/24
switchport mode trunk
!
```

Inter-VLAN Routing

Provisioning VLANs can provide a solution which will allow a LAN to expand beyond what was possible before, and allow better management and control of the network. Most of the large, flat networks that were previously deployed at some campuses are gradually being replaced by VLANed and subnetted networks, to allow better segmentation and control of broadcast and other traffic.

Remember, though, that VLANs exist at Layer 2 only. To allow traffic to move between VLANs, a Layer 3 routing decision must be taken.

Our example network has a Cisco® 6500 switch at the core of the network, so VLANs are provisioned from the core 6500 out towards the edges, and the 6500 router blade provides the Layer 3 inter-VLAN routing capability.

To configure a VLAN trunk for all VLANs between two 3Com® 4400 switches:

On each switch, create the VLANs as described above and then use the command:

```
Select Menu Option: bridge vlan modify addport 323 1:24 tagged
```

This will add VLAN 323 to port 1:24 which is the link port to the other switch. The tagged keyword tells the switch that this is a VLAN trunk as opposed to a single host connection.

To configure a VLAN trunk for all VLANs between a 3Com® 4400 and a Cisco® 2950 switch:

The configuration is the same as the configuration detailed above.

As the trunk is based on the 802.1q standard it will work between different manufacturers’ equipment.

Cisco® 6509 Layer 2 Switch VLAN commands

To set a VLAN’s name

```
set vlan 323 name Video_Conference_Suite
```

To disable Spanning Tree on VLANs

```
set spantree disable 323
```

To place switchports into VLAN 323

```
#module 2 : 8-port 1000BaseX Ethernet
set module name 2
set vlan 323 2/5
```

To configure a port as a 802.1q VLAN trunk

```
set trunk 2/2 on 802.1q
```

As inter-VLAN traffic is a Layer 3 decision, stopping traffic moving between VLANs needs to be done either by not routing traffic, or by controlling traffic by means of a firewall or accesslist restrictions. This is especially true of IP directed-broadcast or Layer 3 broadcast traffic, e.g. to x.255.255.255, which you would normally not want to allow inter-VLAN.

It must be noted that whilst the provisioning of VLANs is relatively simple, provisioning very strict Layer 3 filters on inter-VLAN traffic in an environment where there may be Microsoft®, Novell® or other complex client-server systems in place can be complex and demanding. A full understanding of the protocols, ports and traffic between clients and servers is needed.

Source URL: https://community-stg.jisc.ac.uk/library/videoconferencing-booking-service/traffic-engineering-1-logical-separation-layer-2-vlan