

## Aims

---

The aims of this unit are to:

- Understands the usage of switches and VLANs in network design.
- Configure basic information on a Cisco switch.
- Configure Cisco switches for VLANs.

## Introduction

---

This unit outlines the importance of network switches, especially as they improve network security, and also allow for faster communications than traditional connection devices, such as hubs. A switch enhances the security of a network as it allows for a direct connection between two devices, where no other devices on the switch can *listen* to the connection. They also enhance security as a switch can be programmed to create a virtual LAN (vLAN), where nodes which connect to one vLAN can be isolated from other vLANs. Thus a device may connect to the same network switch, but connect to a different network than other devices which also connect to the same switch. A vLAN can span across one or more switches, which aids the configuration of the network.

## vLANs

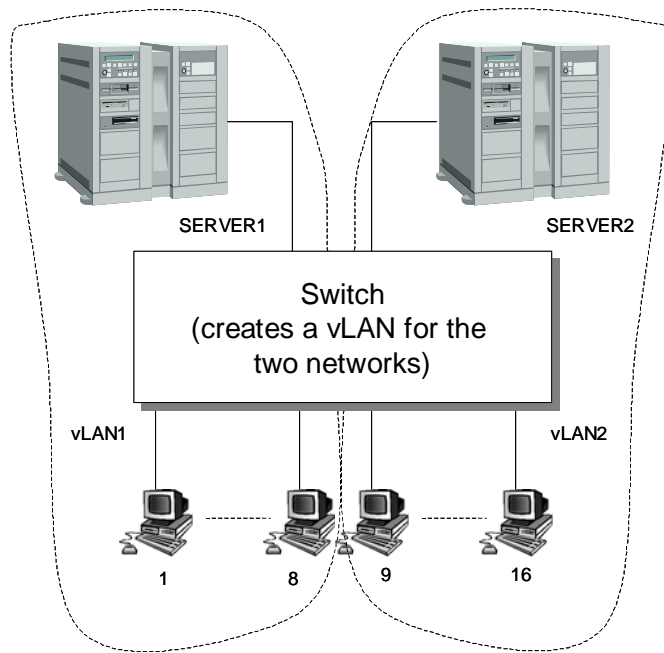
---

vLANs are a new technology, which uses software to define a broadcast domain, rather than any physical connections. In a vLAN a message transmitted by one node is only received by other nodes with a certain criteria to be in the domain. It is made by logically grouping two or more nodes and a vLAN-initialized switching device, such as intelligent switches (which use the MAC address to forward data frames) or routers (which use the network address to route data packets). The important concept with vLANs is that the domain is defined by software, and not by physical connections.

There are two methods that can define the logical grouping of nodes within a vLAN:

- **Implicit tagging.** This uses a special tagging field which is inserted into the data frames or within data packets. It can be based upon the MAC address, a switch port number, protocol, or another parameter by which nodes can be logically grouped. The main problem with implicit tagging is that different vendors create different tags which make vendor interoperability difficult. This is known as frame filtering.
- **Explicit tagging.** This uses an additional field in the data frame or packet header. This can also lead to incompatibility problems, as different vendor equipment may not be able to read or process the additional field. This is known as frame identification.

It is thus difficult to create truly compatible vLANs until standards for implicit and explicit tags are standardized. One example of creating a vLAN is to map ports of a switch to create two or more virtual LANs. For example, a switch could connect to two servers and 16 clients. The switch could be configured so that eight of the clients connected to one server through a vLAN, and the other eight onto the other server. This setup is configured in software, and not by the physical connection of the network. Figure 4 shows a possible implementation where nodes 1 to 8 create a vLAN through the switch with SERVER1, and nodes 9 to 16 create a vLAN with SERVER2. The switch would map ports to create the vLANs, where the two networks are now independent broadcast domains (network segments), and will only receive the broadcasts from each of their virtual LANs. Normally a switch would connect any one of its ports to another port, and allow simultaneous connection. In this case, the switch allows for multiple connections onto a segment. Now, with the vLAN, data frames transmitted on one network segment will stay within that segment and are not transmitted to the other vLAN.



**Figure 1**  
Creating a vLAN by mapping ports of a switch

## Advantages of vLANs

The main advantages of using vLAN are:

- **Creation of virtual networks.** Just as many organizations build open-plan offices which can be changed when required, vLANs can be used to reconfigure the logical connections to a network without actually having to physically move any of the resources. This is especially useful in creating workgroups where users share the same resources, such as databases and disk storage.
- **Ease of administration.** vLANs allow networks to be easily configured, possibly at a distance from the configured networks. In the past reconfiguration has meant recabling and the movement of networked resources. With vLANs the resources can be configured with software to setup the required network connections.
- **Improved bandwidth usage.** Normally users who work in a similar area share resources. This is typically known as a workgroup. If workgroups can be isolated from other workgroups then traffic which stays within each of the workgroups does not affect other workgroups. A vLAN utilizes this concept by grouping users who share information and configuring the networked resources around them. This makes much better usage of bandwidth than workgroup users who span network segments. The amount of broadcast traffic on the whole network is also reduced, as broadcasts can be isolated within each of the workgroups. A typical drain on network bandwidth is when network servers broadcast their services at regular intervals (in Novell NetWare this can be once every minute, and is known as the Service Advertising Protocol). With vLANs these broadcasts would be contained within each of the vLANs that the server is connected to.
- **Microsegmentation.** This involves dividing a network into smaller segments, which will increase the overall bandwidth available to networked devices.
- **Enhanced security.** vLANs help to isolate network traffic so that traffic which stays within a vLAN will not be transmitted outside it. Thus it is difficult for an external

user to 'listen' to any of the data that is transmitted across the vLAN, unless they can get access to one of the ports of the vLAN device. This can be difficult as this would require a physical connection, and increases the chances of the external user being caught 'spying' on the network.

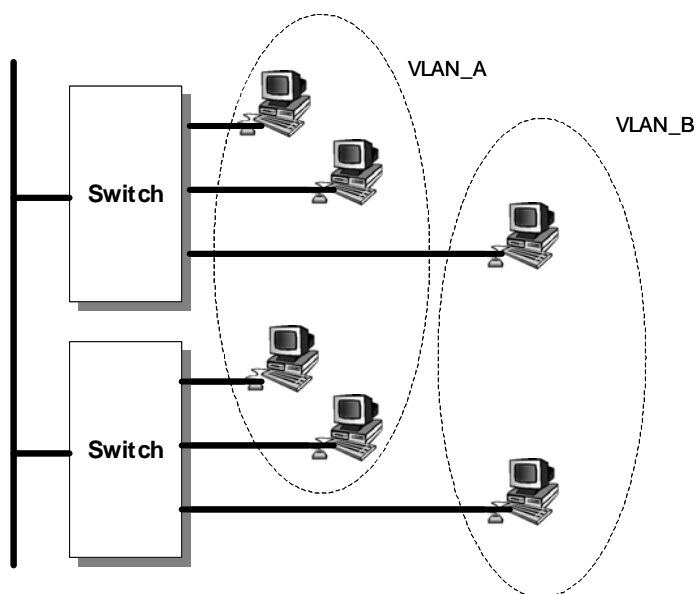
- **Relocate servers into secured locations.** vLANs allows for servers to be put in a physical location in which they cannot be tampered with. This will typically be in a secure room, which is under lock and key. The vLAN can be used to map hosts to servers.
- **Easy creation of IP subnets.** vLANs allow the creation of IP subnets, which are not dependent on the physical location of a node. Users can also remain part of a subnet, even if they move their computer.

## vLAN structure

---

A vLAN can be created by connecting workgroups by a common backbone, where broadcast frames are switched only between ports within the same vLAN. This requires port-mapping to establish the broadcast domain, which is based on a port ID, MAC address, protocol or application. Each frame is tagged with a VLAN ID. Figure 5 illustrates that switches are one of the core components of a VLAN. Each switch is intelligent enough to decide whether to forward data frame, based on VLAN metrics (such as port ID, MAC address or network address), and to communicate this information to other switches and routers within the network. The switching is based on frame filtering or frame identification.

Most early vLANs were based on frame filters, but the IEEE 802.1q vLAN standard is based on frame tagging, as this allows for scalable networks. With frame tagging, each frame has a uniquely assigned user-defined ID. A unique identifier in the header of each frame is forwarded throughout the network backbone (vertical cabling), as illustrated in Figure 5. Each switch then reads the identifier, and if the frame is part of a network which it controls, the switch removes the identifier before the frame is transmitted to the target node (horizontal cabling). As the switching occurs at the data link layer, there is not a great processing time overhead.



**Figure 2**  
vLANs using a  
backbone and  
switches

## VLAN broadcasts

---

vLANs rely on broadcasts to the virtual network, but they are constrained within the virtual network, and thus are not transmitted to other virtual networks. This should reduce the amount of overall network broadcasts (especially from broadcast storms). The broadcast domain can be reduced by limiting the number of switched ports which connect to a specific vLAN. The smaller the grouping, the lower the broadcast effect.

## vLAN's and security

---

vLANs increase security of data as transmitted data is confined to the vLAN in which it is transmitted. These provide natural firewalls, in which external users cannot gain access to the data within a vLAN. This security occurs, as switch ports can be grouped based on the application type and access privileges. Restricted applications and resources can be placed in a secured VLAN group.

The two types of vLANs are:

- **Static vLANs.** These are ports on a switch that are statically assigned to a VLAN. These remain permanently assigned, until they are changed by the administrator. Static vLANs are secure and easy to configure, and are useful where vLANs are fairly well defined.
- **Dynamic VLANs.** These are ports on a switch which automatically determine their VLAN assignments. This is achieved with intelligent management software, using MAC addresses, logical addressing, or the protocol type of the data packets. Initially, where a node connects to the switch, the switch detects its MAC address entry in the VLAN management database and dynamically configures the port with the corresponding VLAN configuration. The advantage of dynamic vLANs is that they require less setup from the administrator (but the database must be initially created).

The broadcast domain in a vLAN is defined by each vLAN, as illustrated in Figure 6. A node broadcasting into the vLAN will only be transmitted to nodes within its vLAN. Nodes not connected to the same vLAN, even although they connect to the same switch as the broadcasting node, will not receive the broadcast. The only way for nodes to intercommunicate across differing vLANs is to be routed through a router (as illustrated in Figure 7).

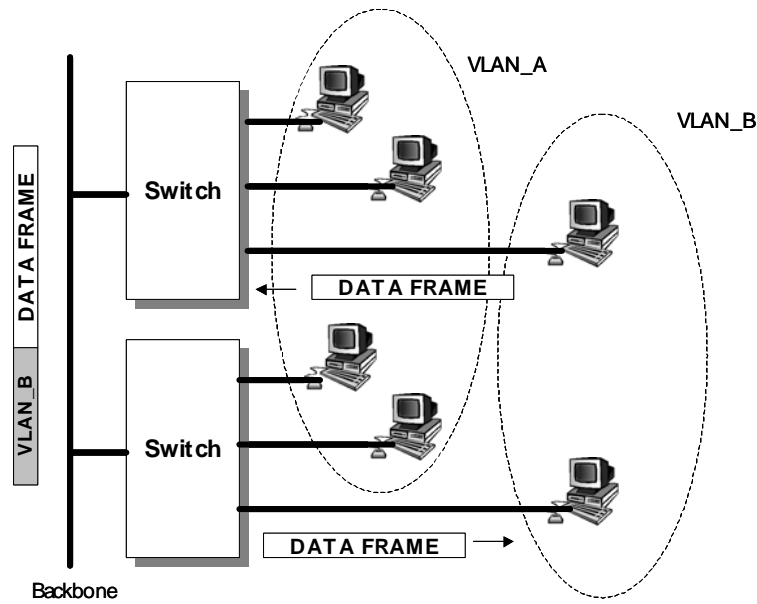


Figure 3 vLANs using frame tagging

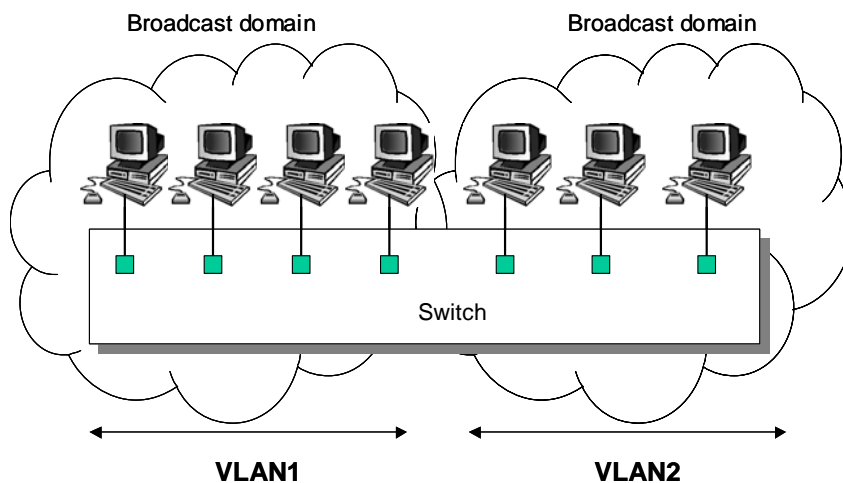


Figure 4 Broadcast domains for vLANs

Note that a broadcast domain extends the full length of the vLAN, and not onto other vLANs. A router does not forward broadcasts, thus the vLAN is isolated from other networks. The router provides intercommunicate between vLANs, and security is enhanced by implement security restrictions on the ports of the router.

Broadcast domains

## VLAN broadcast domains

As previously mentioned the broadcast domain is important, as nodes use it to determine the MAC addresses of nodes within their vLAN. In Figure 8, a node on VLAN1 could only communicate with a node on VLAN2 if would use the network address of the node on VLAN2. For example if Node A communicates with Node B, it would broadcast an ARP request into its vLAN for the MAC address of Node B, which would return it back

to the vLAN. Node A can then communicate with Node B, as it uses the MAC address of Node B, and its network layer address. If Node A wishes to communicate with Node C, it will send out an ARP request to the port on the router to which it connects to (its gateway). This port will respond back with its MAC address. Node A will then send out a data frame with the MAC address of the gateway, and the destination address of Node C. The router will then forward it onto the port which has Node C connected to it, and changes the destination MAC address to the MAC address of Node C (if it already knows it, else it would initially send out an ARP request for it). The router will generally test the incoming data frame for security purposes, and will only forward it if Node A is allowed to communicate with Node C (allowing for certain conditions).

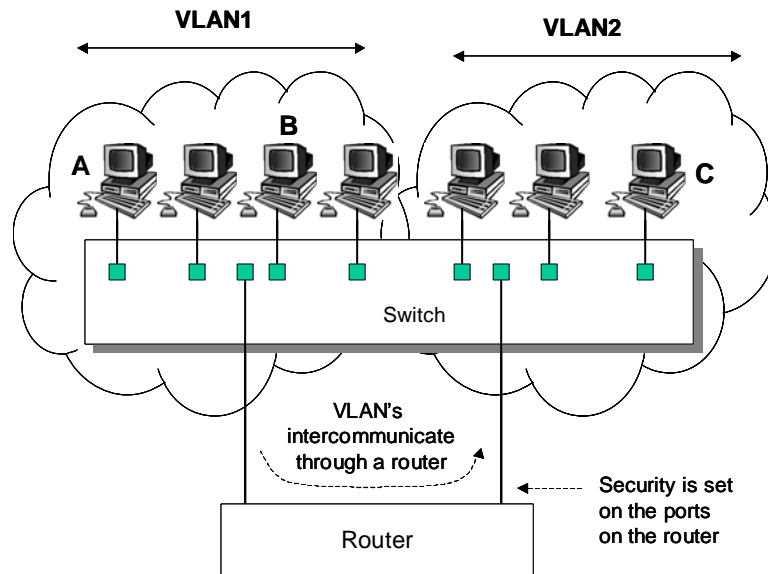
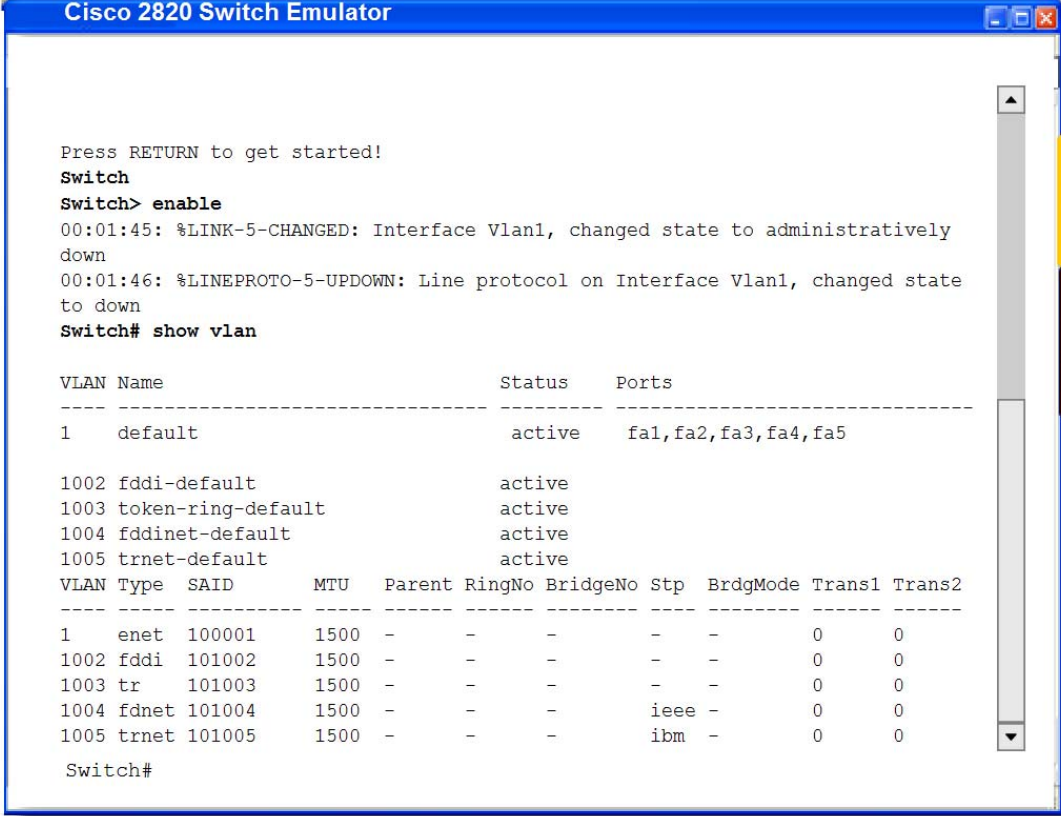


Figure 5 Broadcast domains for vLANs

## Activity 5.1: Programming Cisco switches

The following sections relate to the programming a Cisco switch. For this purpose a special emulator has been developed. This is shown in Figure 9.



```
Press RETURN to get started!
Switch
Switch> enable
00:01:45: %LINK-5-CHANGED: Interface Vlan1, changed state to administratively
down
00:01:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
to down
Switch# show vlan

VLAN Name                Status    Ports
-----
1    default                 active    fa1, fa2, fa3, fa4, fa5

1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default        active
1005 trnet-default          active
VLAN Type  SAID      MTU    Parent RingNo BridgeNo  Stp  BrdgMode Trans1 Trans2
-----
1    enet   100001    1500   -     -     -     -     -     0     0
1002 fddi   101002    1500   -     -     -     -     -     0     0
1003 tr    101003    1500   -     -     -     -     -     0     0
1004 fdnet 101004    1500   -     -     -     -     ieee -     0     0
1005 trnet 101005    1500   -     -     -     -     ibm  -     0     0

Switch#
```

Time taken: 0:0:11 Privileged EXEC mode

RE-SIZE  
HELP  
Author: w.buchanan

Figure 9: Cisco 1900/2800 switch emulator

## Showing version of switch

Initially you will be in the user executive (Exec) mode, and the functions that you can perform are limited.

- 1 Use the ? command to view the commands in this mode.
  - What commands are available in Exec mode?
- 2 Use the **show version** command to show the current operating system details.
  - How many Ethernet ports does the switch have?
  - What is the MAC address of the switch?

## Setting host and IP information

Next go into the privileged executive mode:

- 1 Go into the privileged mode by typing `enable`.
  - How does the prompt change?
- 2 Use the `?` command to view the commands in this mode.
  - What commands are available in Privileged Exec mode?
- 3 Configure the device using by typing `config t`.
  - How does the prompt change?
- 4 Set the hostname by typing `hostname myhost`.
- 5 Go back to the user executive mode with the command `exit`.
- 6 Show the IP parameters of the switch with the command `show ip interface`.
  - What are the parameters displayed?
- 7 Go back to configuration mode with `config t`.
- 8 Configure the VLAN with the `interface vlan 1` command.
- 9 Set the IP address and subnet mask with the command `ip address 192.168.0.1 255.255.255.0`.
- 10 Go back to privileged mode with `exit`.
- 11 Show the IP parameters again with `show ip interface`.
  - What are the parameters displayed?
- 12 From the config mode, set the gateway address to 192.168.0.2, the domain-name is mycomp.com, the name-server to 192.168.0.10, using:

```
(config)# ip default-gateway 192.168.0.2
(config)# ip domain-name mycomp.com
(config)# ip name-server 192.168.0.10
```

- 14 Show the main system configuration with `show running-config`.
  - What are the parameters displayed?

## Setting telnet interface

---

It is possible to remotely log into the switch over the network using TELNET. To do this the following is achieved:

- 1 Go to the Executive Privileged mode (that is, with the `#` prompt).
- 2 Go to the configuration mode (that is, with the `(config) #` prompt).
- 3 Use the `line vty 0 15` to create up to 16 possible TELNET sessions.
- 4 Use the `password fred` to define the password as fred
- 5 Exit from the config mode with `end`.
- 6 Show the current running configuration with `show running-config`.
  - Has the configuration been updated?

## Saving the configuration

---

The changes that are made are made only to the running configuration (running-configuration). Once the user has verified that the new changes are okay, they should copy the running configuration into the startup configuration (startup-configuration). Once this is done, the switch will startup with the updated changes. To do this the copy running-config startup-config command is used.

- 1 Go to the configuration model (that is, with the `(config) #` prompt).

- 2 Use the `copy running-config startup-config` command.

Other methods include:

`copy running-config tftp` which copies the running config to the TFTP server.  
`copy tftp running-config` which copies from the TFTP server to the current running config.

## Showing the commands

---

The switch stores all the previous commands, which can be recalled with the `show history` command.

- 1 Use the `show history` to display the previous commands.

## Scrolling through commands

---

The UP and DOWN arrow keys can be used to scroll through the previous command, of which the user can select any of them, as required.

- 1 Use the UP and DOWN arrows to scroll through the command.

## Setting up a VLAN

---

One of the great advantages of switches is that it is possible to create a VLAN, which allows the actual topology of the network to be defined by software rather than actual physical connections. In the following the VLAN is given a name, and then ports are assigned to it.

- 1 Go to the privileged executive mode (that is, with the # prompt).
- 2 Use the `show vlan` command to view the currently assigned VLANs.
  - What are the names of the currently assigned VLANs?
- 3 Use the `vlan database` command to go into the vlan configuration mode.
  - How does the prompt change?
- 4 Use the ? command to view the commands in this mode.
- 5 Use the `show` command to view the currently assigned VLANs.
  - What VLANs are currently present?
- 6 Use the `vlan 2 name fred` to change the name of VLAN number 2 to fred.
  - What message is displayed?
- 7 Use the `show` command to view the currently assigned VLANs.
  - Has the VLAN been added?
- 8 Exit from vlan and configuration modes, and run `show vlan` again.
  - How have the names of the VLANs changed?

## Programming interfaces and assigning to VLANs

---

- 1 Configure the interface by typing interface.
  - How does the prompt change?

- 2 Determine the commands that can be used in the interface menu with ?. List a few of these command.
  - What commands are available in Interface Configuration mode?
- 3 Program the first Ethernet port on the switch (which is 0/1, where the first digit identifies the Ethernet port and the second digit identifies the port number). Do this by entering the **Ethernet 0/1** command.
- 4 Define the this port is assigned to VLAN 2 with the **switchport access vlan 2** command.
- 5 Program the second Ethernet port on the switch (which is 0/2). Do this by entering the **Ethernet 0/2** command.
- 6 Define the this port is assigned to VLAN 2 with the **switchport access vlan 2** command.
- 7 Go back to the Privileged Exec mode, and use the **show vlan** command to show the assigned VLANs against ports.

This is shown next:

```

Cisco 2820 Switch Emulator
Switch> enable
Switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface e0/1
Configuring: 0 Port: 1
Switch(config-if)# switchport access vlan 2
Switch(config-if)# exit
Switch(config)# interface e0/2
Configuring: 0 Port: 2
Switch(config-if)# switchport access vlan 2
Switch(config-if)# exit
Switch(config)# exit
Switch# show vlan

VLAN Name                Status    Ports
-----
1    default                 active    fa1, fa2, fa3, fa4, fa5
2    default                 active    fa1, fa2

1002 fddi-default          active
1003 token-ring-default   active
1004 fddinet-default       active
1005 trnet-default         active
VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp    BrdgMode Trans1 Trans2
-----
Switch#
  
```

Time taken: 0:3:40 Privileged EXEC mode

## Resetting the switch

The two commands to reset the switch are **delete nvram** and **delete vtp**, which can be entered from the config mode.

- 1 Go to the user exec mode (that is, with the # prompt).
- 2 Use the **erase nvram** command.
- 2 Use the **erase vtp** command.

## Reducing commands

---

Many commands can be truncated to a shorter form, such as: sh (show), conf (configuration), e (ethernet), fa (fastethernet), and so on.

## Setting other parameters on the port

---

Apart from defining shutdown, no shutdown and description on the ports, it is possible to set the speed with the speed command (10 - 10 Mbps, 100 - 100 Mbps or auto - autospeed), and with duplex whether the port supports full-duplex (full), half-duplex (half) or auto.

- 1 Go to the privileged interface mode (that is, with the (config) # prompt). Next configure the third Ethernet port with the command `int e0/1` (which is the short form of interface ethernet 0/1)
- 2 Use the `speed 10` command to set the speed to 10Mbps.
- 3 Use the `duplex half` command for half-duplex.
- 4 Go back to the Privileged mode (#) and run `show running-config`, and check that the parameters have been set.

## Enabling spanning-tree

---

Spanning-tree is used to allow the switch to discover the layout of interconnected networks.

- 1 Go to the privileged interface mode (that is, with the (config) # prompt).
- 2 Use the `spanning-tree vlan 1` command to enable it.
- 3 Use the `show spanning` to show the spanning-tree topology.

## Setting line-console password

---

The console password is set by using the line con 0 command from the Privileged Exec mode, and then using the password command.

- 1 Go to the privileged interface mode (that is, with the (config) # prompt). Next configure the third Ethernet port with the `line con 0` (which is the short form of line console 0)
- 2 Use the `password fred` command to set the password to fred.
- 3 Go back to the Privileged mode (#) and run `show running-config`, and check that the parameters have been set.

## Restarting the switch

---

Often the administrator must restart the switch (possibly to be able to reapply settings). To do this the reload command is used:

- 1 Go to Privileged Exec mode.
- 2 Use the `reload` command to reboot the switch.

- What are the messages shown?

## Enabling SNMP

---

SNMP is an excellent protocol which allows remote devices to interrogate network parameters on the local device. As SNMP could cause a security breach if it is not setup correctly, it is off by default. To turn it on:

- 1 Go to Config mode.
- 2 Use the `snmp enable traps` command to initialise snmp.
- 3 Use the `show running-config` to view the snmp setup.
- 4 Use the `show snmp` to view the results from the SNMP agent.

## Showing help

---

Many commands contain a help version. For this type in the command and a '?'. For example:

- 1 `show ?`
- 2 `show ip ?`

## Showing contents of Flash memory

---

The Flash memory contains the OS, HTML pages, and so on. It can be viewed using the following command:

- 1 `show flash`
  - What files and directories are shown?

## Changing and listing directories

---

The file structure can be listed using the DIR command and the directory can be changed with CD (as with DOS).

- 1 Go into the html folder using the `cd html` command, and then uses the `dir` command to list its contents.
  - What files are shown?
- 2 Go back to the top level folder using the `cd ..` command, and then uses the `dir` command to list its contents.

Other command:

<code>show interface e0/1</code>	Show the interface parameters for port 1.
<code>show users</code>	Show connected users.
<code>show snmp</code>	Show SNMP statistics.
<code>show hosts</code>	Show host parameters (domain name, name server, and so on).
<code>show alias</code>	Show host parameters (domain name, name server, and so on).

on).

<b>show boot</b>	Show boot parameters.
<b>show post</b>	Show the results of the post test.
<b>show dot1x</b>	Show details of IEEE 802.1x.

The outline of the commands is:

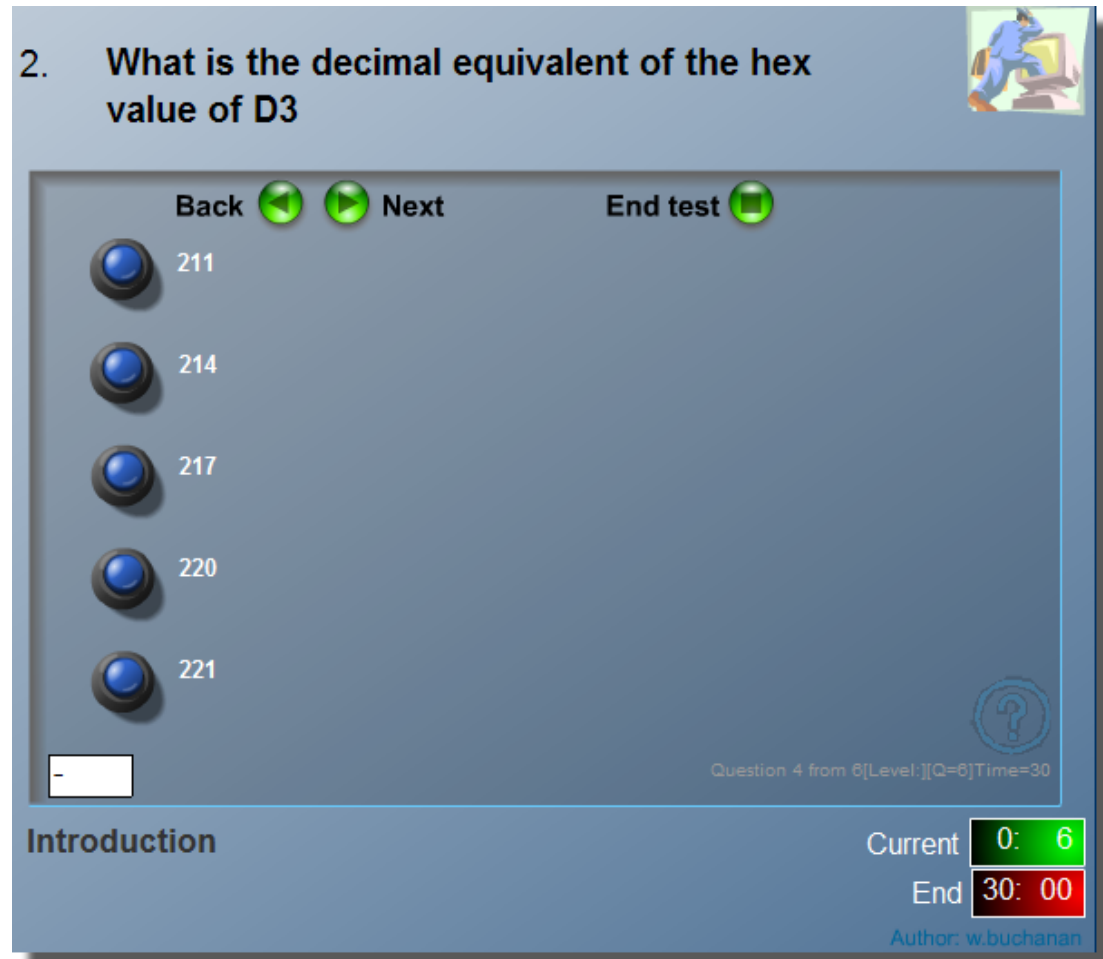
```
Switch> show version
Switch> enable
Switch# config t
myhost(config)# hostname myhost
myhost(config)# exit
myhost# show ip interface
myhost# config t
myhost(config)# interface vlan 1
myhost(config-if)# ip address 192.168.0.1 255.255.255.0
myhost(config-if)# no shutdown
myhost(config-if)# exit
myhost(config)# exit
myhost# show ip interface
myhost# config t
myhost(config)# ip default-gateway 192.168.0.2
myhost(config)# ip domain-name mycomp.com
myhost(config)# ip name-server 192.168.0.10
myhost(config)# exit
myhost# show running-conf
myhost# config t
myhost(config)# line con 0
myhost(config-line)# password fred
myhost(config-line)# exit
myhost(config)# line vty 0 15
myhost(config-line)# password fred
myhost(config-line)# exit
myhost(config)# exit
myhost# copy running-config startup-conf
myhost# show history
myhost# show vlan
myhost# vlan database
myhost(vlan)# vlan 2 name fred
myhost(vlan)# exit
myhost# show vlan
myhost# config t
myhost(config)# interface e0/1
myhost(config-if)# switchport access vlan 2
myhost(config-if)# exit
myhost(config)# interface e0/2
myhost(config-if)# switchport access vlan 2
myhost(config-if)# exit
myhost(config)# exit
myhost# show vlan
myhost# delete nvram
myhost# delete vtp
myhost# config t
myhost(config)# interface e0/1
myhost(config-if)# speed 10
myhost(config-if)# duplex half
myhost(config-if)# exit
myhost(config)# exit
myhost# show running-config
myhost# show snmp
myhost# show flash
myhost# cd html
myhost# dir
myhost# cd ..
myhost# dir
```

```
myhost# config t
myhost(config)# interface e0/1
myhost(config-if)# no cdp enable
myhost(config-if)# exit
myhost(config)# exit
myhost# show cdp
myhost# show cdp traffic
myhost# show cdp neighbors
myhost# config t
myhost(config)# cdp holdtime 20
myhost(config)# cdp timer 30
myhost(config)# exit
myhost# show running
myhost# config t
myhost(config)# ip http server
myhost(config)# exit
myhost# show running
```




## Activity 5.2: Test

---

The end of unit test contains questions on the material in this unit.



2. What is the decimal equivalent of the hex value of D3

Back   Next End test 

211

214

217

220

221

Question 4 from 8[Level: ][Q=6]Time=30

Introduction

Current **0: 6**

End **30: 00**

Author: w.buchanan

## Details

---

**Author:** Dr WJ Buchanan

**Date:** 23 Aug 2003

**WWW:** <http://www.dcs.napier.ac.uk/~bill/cnds.html>  
<http://buchananweb.co.uk/cnds.html>

**Web CT:** <http://neo.napier.ac.uk>

**Associated:** Switch emulator