KEMENTERIAN PENDIDIKAN MALAYSIA

UTeM
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

FTMK
FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

/ myftmk

Chapter 10

VIRTUAL LOCAL AREA NETWORK (VLAN)

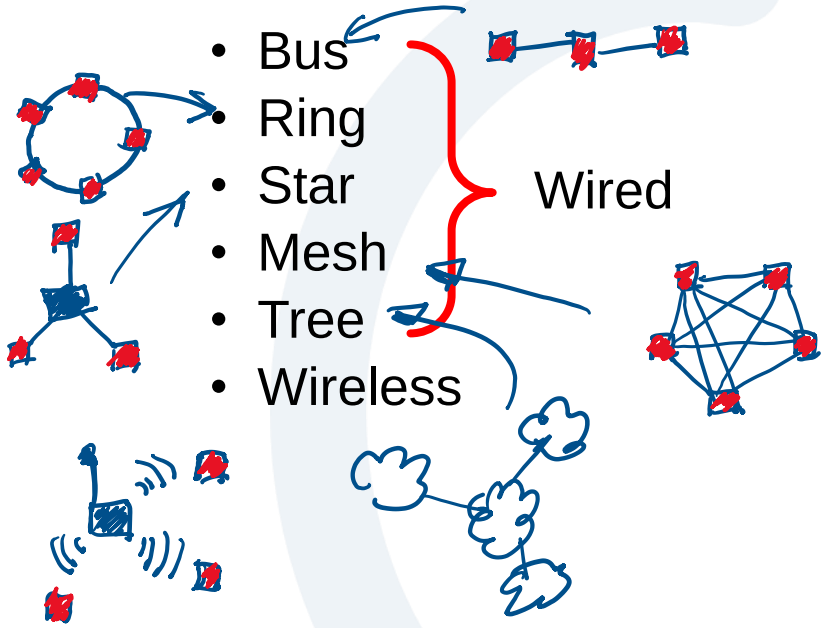
by
Nazrulazhar Bahaman
nazrulazhar@utem.edu.my

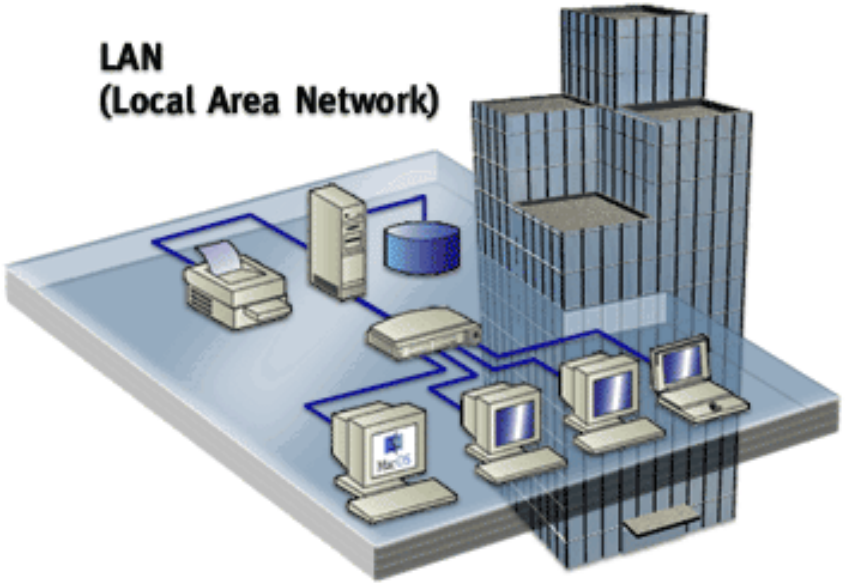
Objectives

- Explain the purpose of VLANs in a switched network.
- Analyze how a switch forwards frames based on VLAN configuration in a multi-switched environment
- Configure a switch port to be assigned to a VLAN based on requirements.
- Configure a trunk port on a LAN switch.

Local Area Network

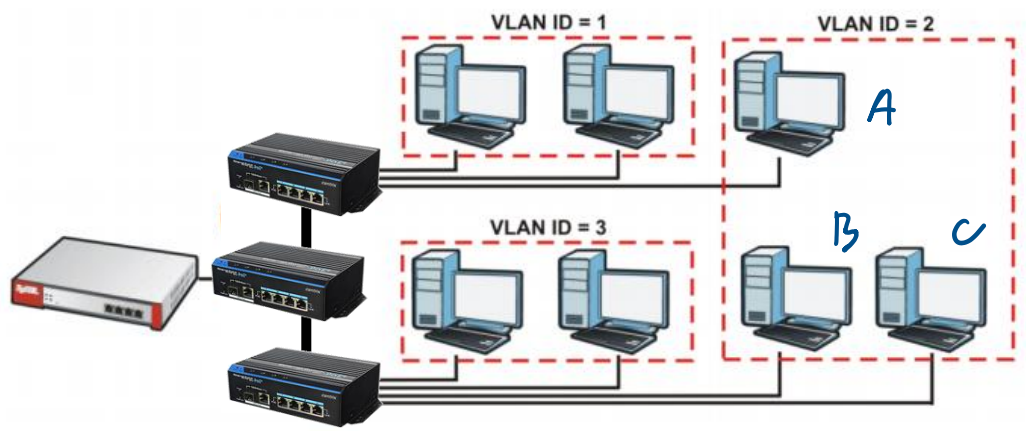
- A local area network supplies networking capability to a group of computers in close proximity to each other, like in an office building, school, or home.
- LANs are usually built to enable the sharing of resources and services like files, printers, games, applications, email, or internet access.
- LAN Topology
  - Bus
  - Ring
  - Star
  - Mesh
  - Tree
  - Wireless





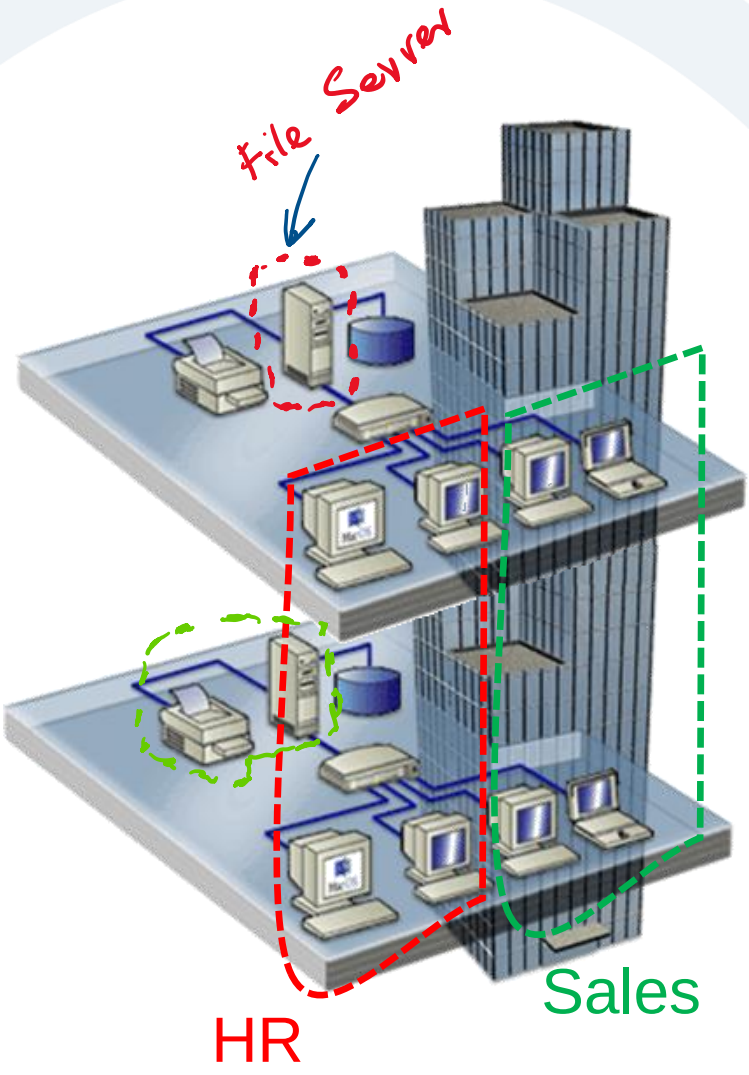
What is VLAN?

- VLANs logically segment physical switched networks based on the functions, project teams or applications of the organization regardless of the physical location or connections to the network.
  - Wired or wireless or both
- All workstations and servers used by a particular workgroup share the same VLAN, regardless of the physical connection or location.

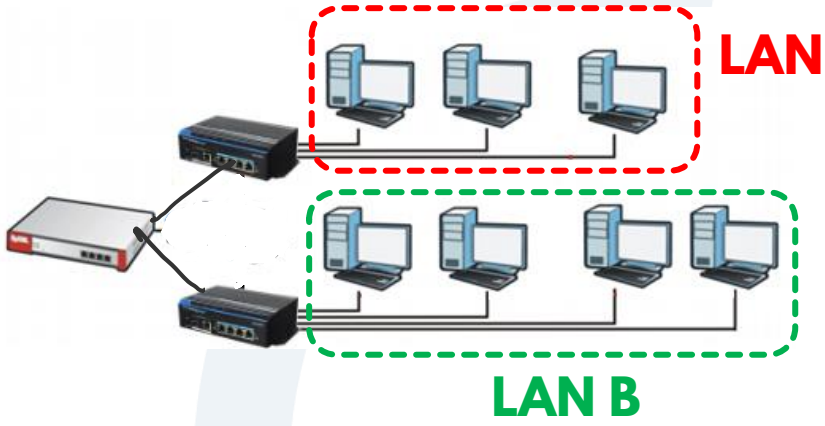


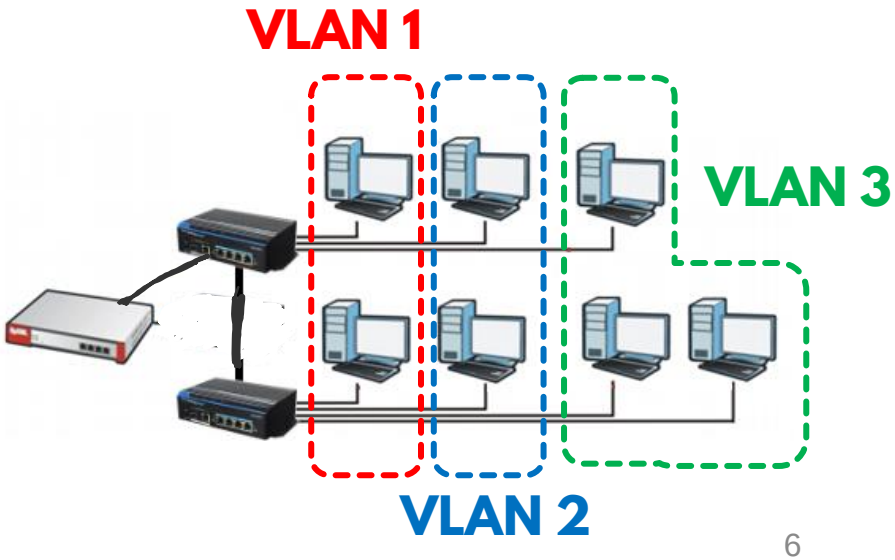
A, B, C share VLAN 2

- A workstation in a VLAN group is restricted to communicating with file servers in the same VLAN group.
  - A group of users in same broadcast domain
  - Can be based on port ID, MAC address protocol or application
  - LAN Switches and network management software provide a mechanism to create VLANs
  - Frame tagged with VLANs

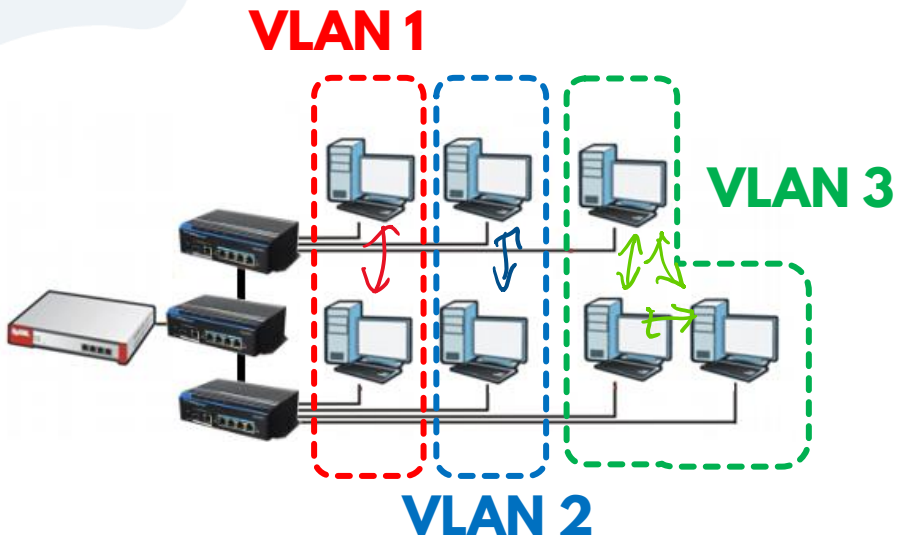


- VLANs function by logically segmenting the network into different broadcast domains so that packets are only switched between ports that are designated for the same VLAN.
- Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management.



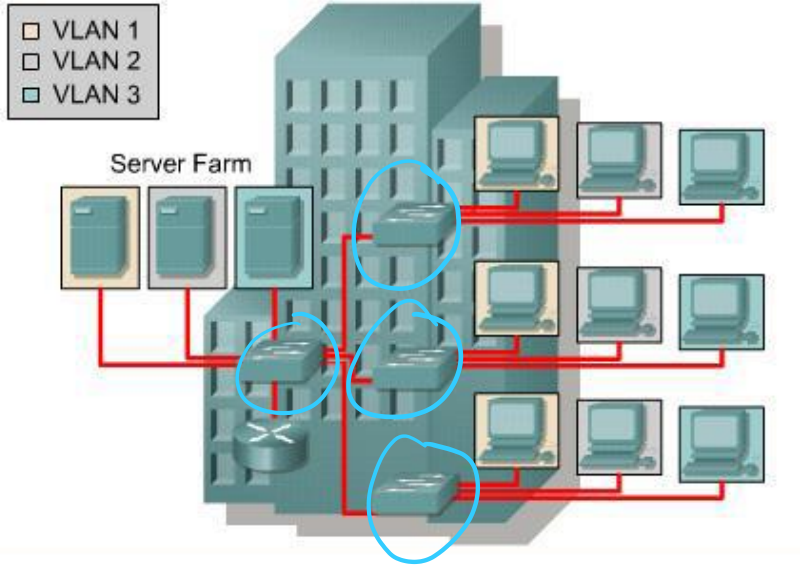


- VLANs address scalability, security, and network management.
- Switches may not bridge any traffic between VLANs, as this would violate the integrity of the VLAN broadcast domain.
- Traffic should only be routed between VLANs.



Broadcast Domain

- A VLAN is a broadcast domain created by one or more switches.
  - A switch creates a broadcast domain
  - VLANs help manage broadcast domains
  - VLANs can be defined on port groups, users or protocols
  - LAN switches and network management software provide a mechanism to create VLANs



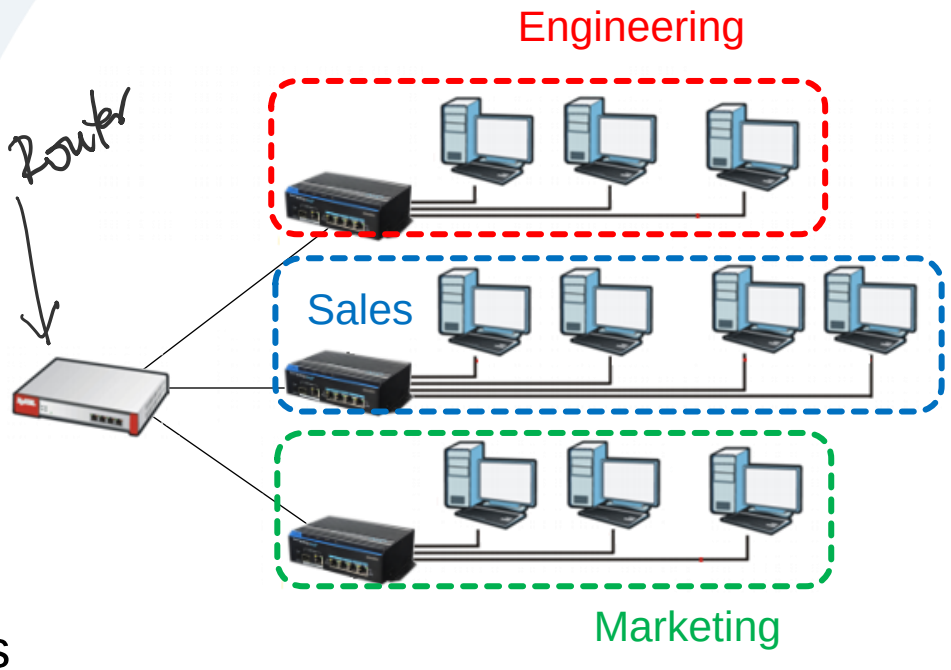
Broadcast Domain Physically

- Layer 3 routing allows the router to send packets to the three different broadcast domains.

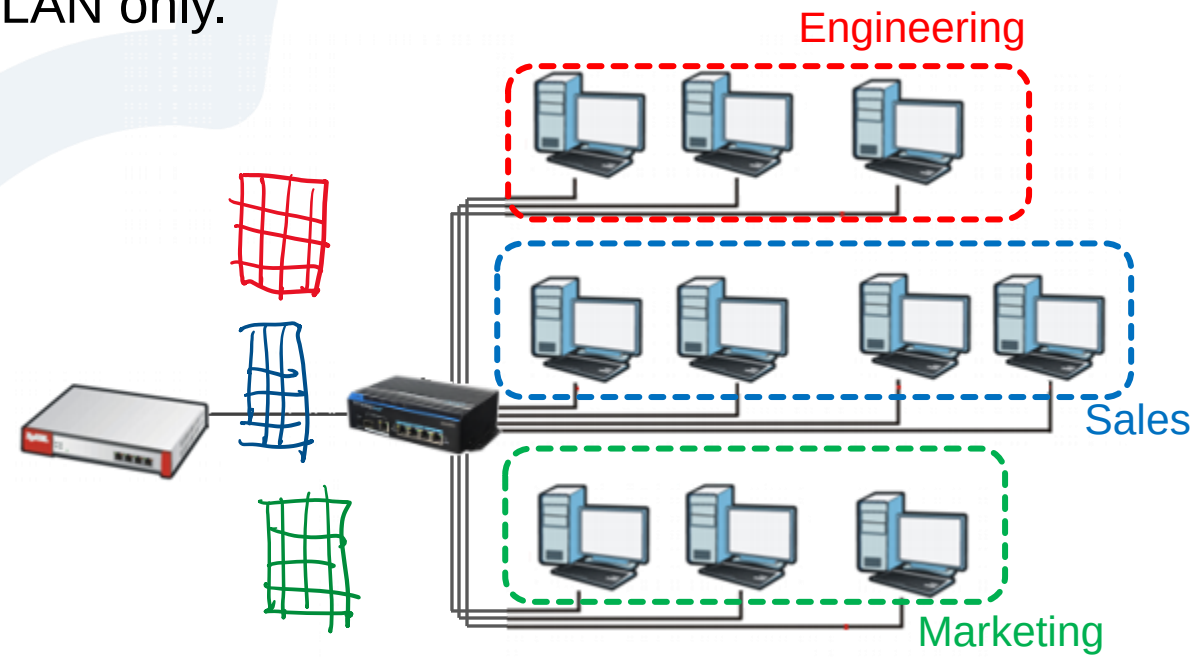
- Three switches and 1 router
  - Switch for Engineering
  - Switch for Marketing
  - Switch for Sales

- Each switch treats all port as members of one broadcast domain

- Router is used to route packets among the three broadcast domains



- Implementing VLANs on a switch causes the following to occur:
  - The switch maintains a separate bridging table for each VLAN.
  - If the frame comes in on a port in VLAN 1, the switch searches the bridging table for VLAN 1.
  - When the frame is received, the switch adds the source address to the bridging table if it is currently unknown.
  - The destination is checked so a forwarding decision can be made.
  - For learning and forwarding the search is made against the address table for that VLAN only.



VLAN Operation

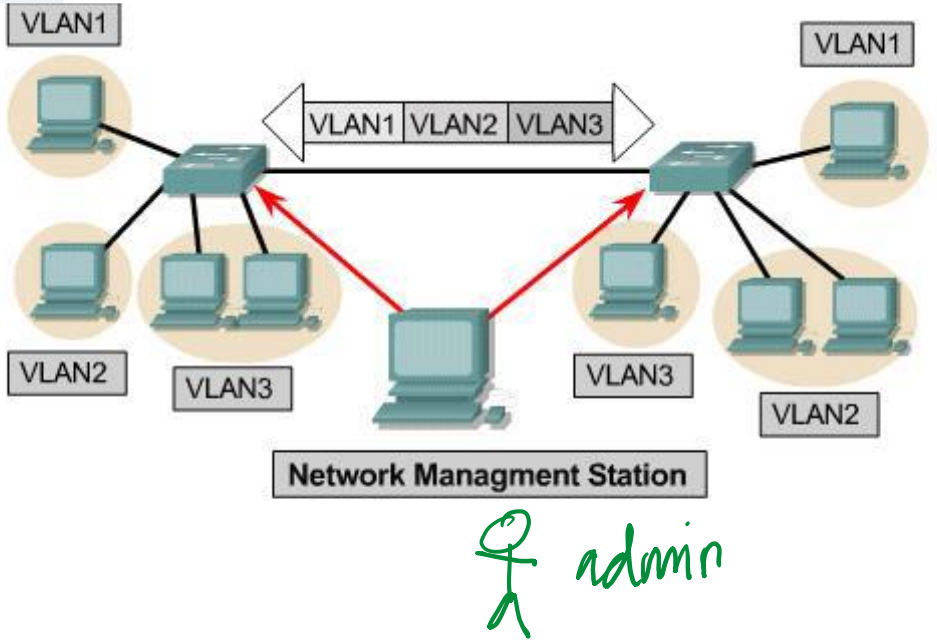
- Static VLAN
- Dynamic VLANs

VLAN Operation

Static VLAN

- Each switch port could be assigned to a different VLAN.
- Ports assigned to the same VLAN share broadcasts.
- Ports that do not belong to that VLAN do not share these broadcasts.

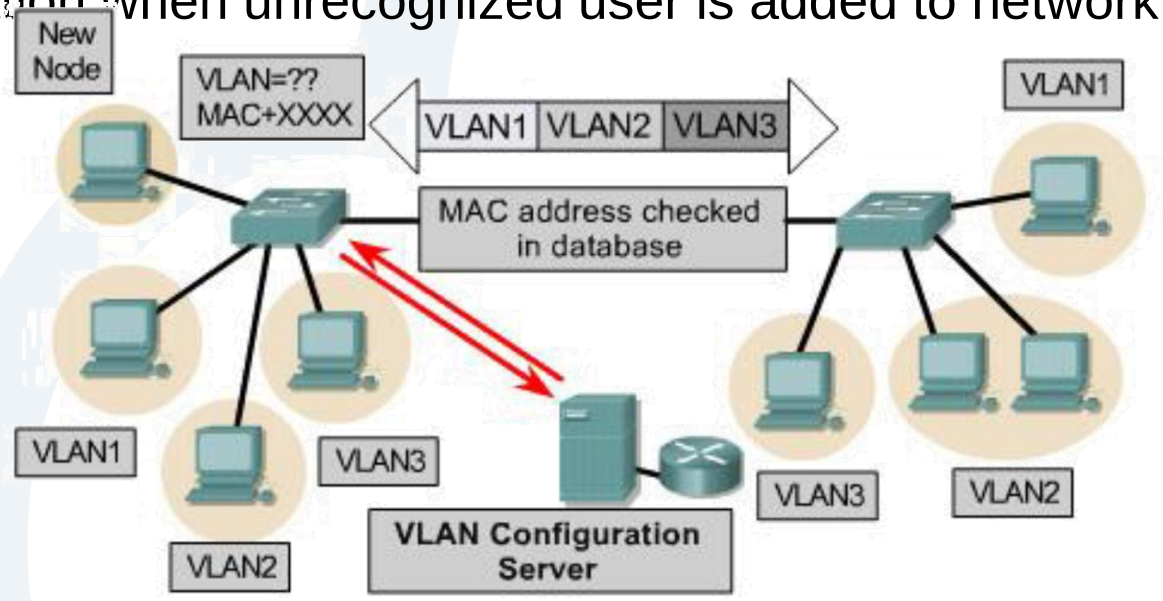
- Secure, easy to configure and monitor



VLAN Operation

Dynamic VLANs

- VLANs assigned using centralized VLAN management application
- VLANs based on MAC address, logical address or protocol type
- Less administration in wiring closet
- Notification when unrecognized user is added to network



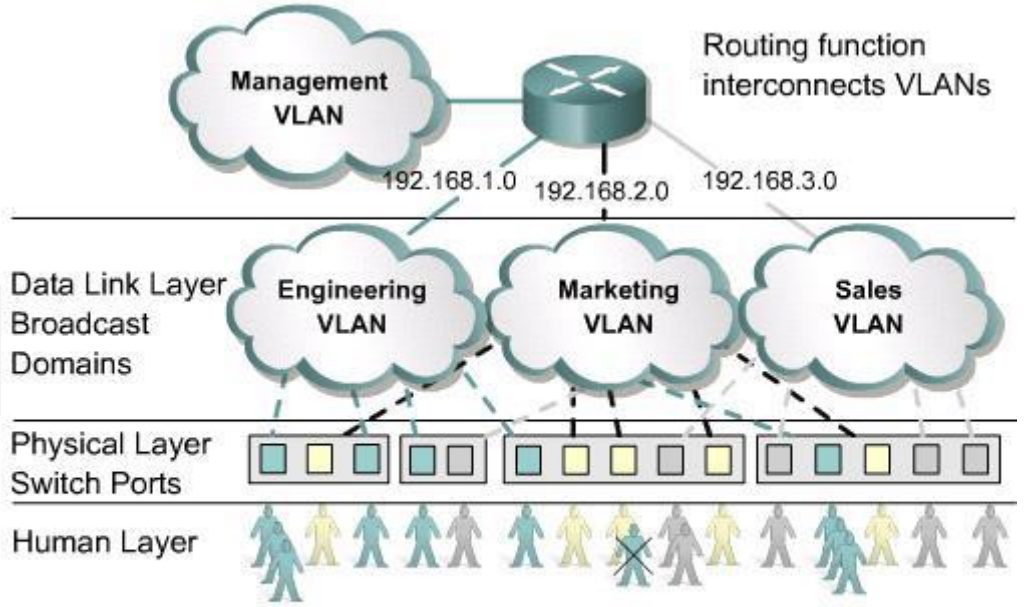
VLAN Operation

- Network administrators are responsible for configuring VLANs both manually and statically.

Configuring VLANs	Description
Statically	Network administrators configure port-by-port. Each Port is associated with a specific VLAN. The network administrator is responsible for keying in the mappings between the ports and VLANs.
Dynamically	The ports are able to dynamically work out their VLAN configuration. Uses a software database of MAC address to VLAN mappings (which the network administrator must set up first).

Benefits of VLANs

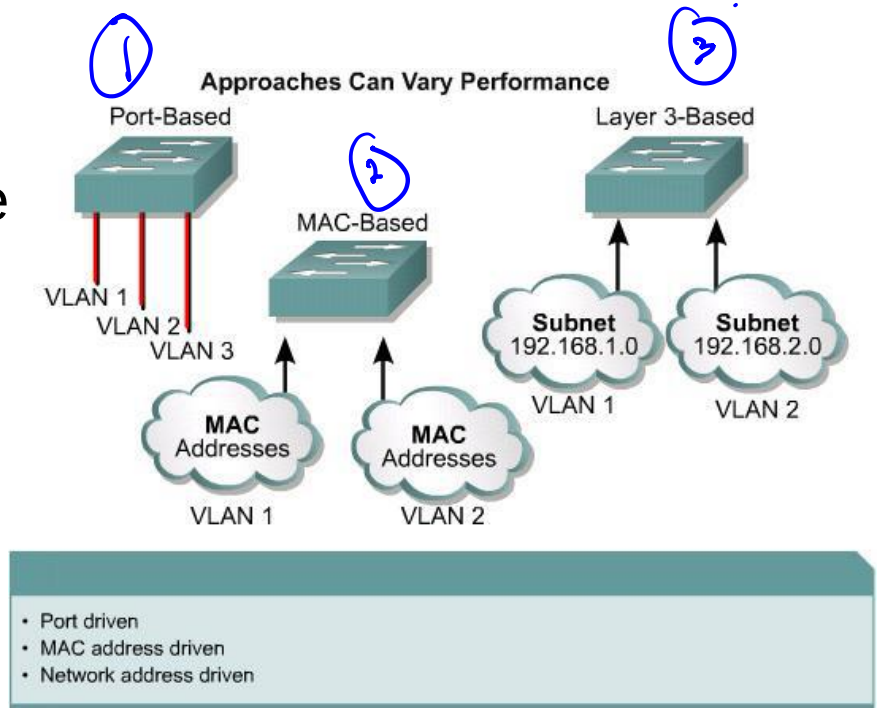
- The key benefit of VLANs is that they permit the network administrator to organize the LAN logically instead of physically.



All users attached to the same switch port must be in the same VLAN.

VLAN Types

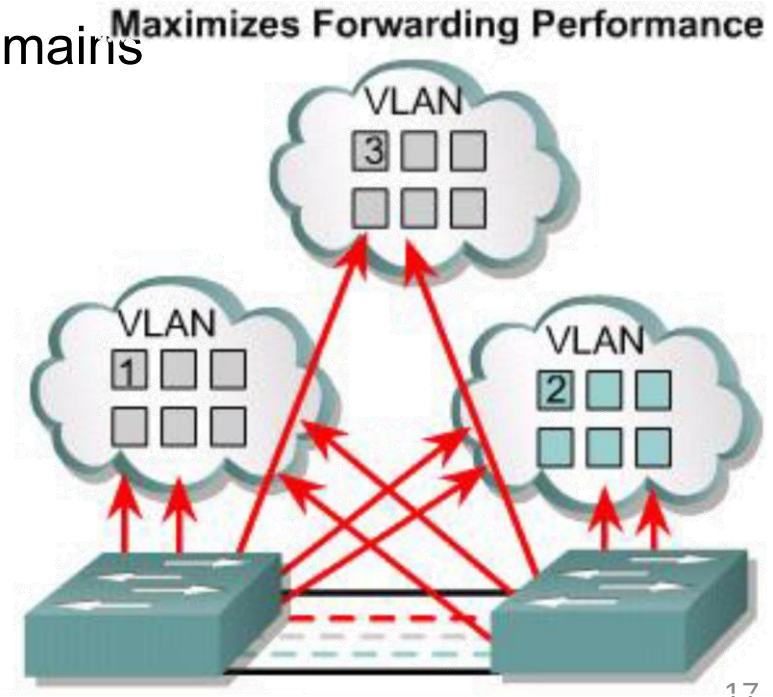
- The frame headers are encapsulated or modified to reflect a VLAN ID before the frame is sent over the link between switches.
- Before forwarding to the destination device, the frame header is changed back to the original format.
- There are three basic VLAN memberships for determining and controlling how a packet gets assigned: -
  - Port-based VLANs
  - MAC address based
  - Protocol based VLANs



VLAN Types

Port-based

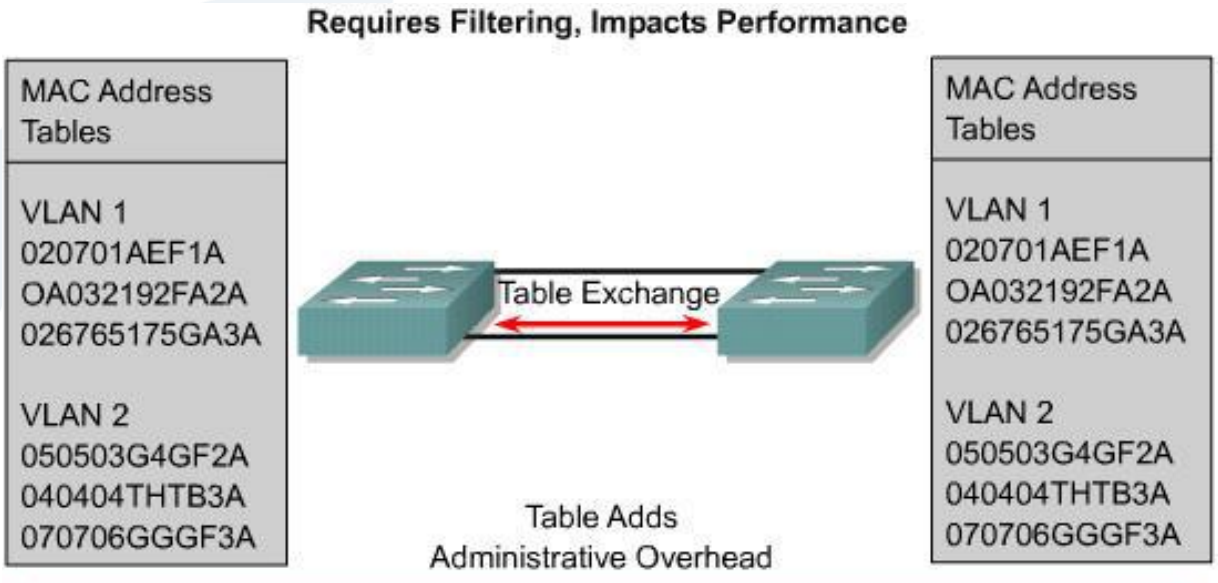
- Most common configuration method
- Port assigned individually, in group across 2 or more switched
- Easily administered via GUIs
- Maximized security between VLANs
- Packets do not “leak” into other domains
- Easily controlled across network



VLAN Types

MAC-Address Based

- Rarely implemented today
- User assigned on MAC addresses
- Offers flexibility, yet adds overhead
- Impacts performance, scalability and administration



VLAN Types

Protocol Based

- Configure like MAC addresses but instead uses a logical or IP address
- No longer common because of DHCP

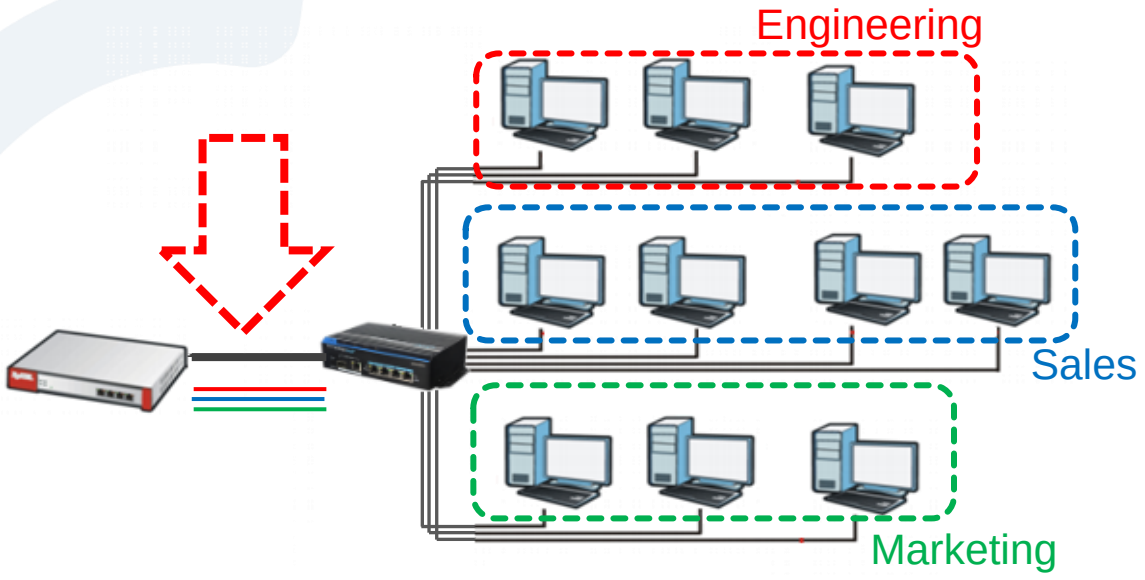
VLAN Types

- The number of VLANs in a switch vary depending on several factors:
  - Traffic patterns
  - Types of applications
  - Network management needs
  - Group commonality

VLAN Types

Frame Tagging / Trunk link

- A trunk is a point-to-point link between the device and another networking device.
- Trunks carry the traffic of multiple VLANs over a single link and allow you to extend VLANs across an entire network
- There are two major methods of frame tagging, Inter-Switch Link (ISL) and 802.1Q.
- ISL used to be the most common, but is now being replaced by 802.1Q frame tagging.



Benefits of VLANs

- Easily move workstations on the LAN
- Easily add workstations to the LAN
- Easily change the LAN configuration
- Easily control network traffic
- Improve security

Configuring VLANs and Trunks

- Configure and verify VLANs and trunks on switched network
  - Create the VLANs
  - Assign switch ports to VLANs statically
  - Verify VLAN operation
  - Enable trunking on the inter-switch connection
  - Verify trunk configuration

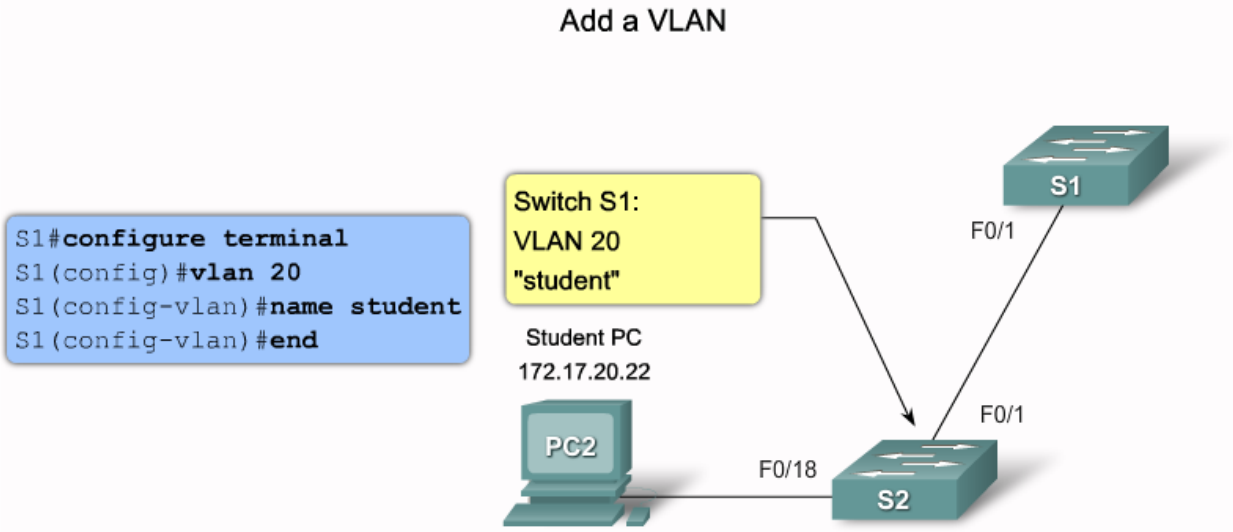
Configuring VLANs

```
#configure terminal
(config)#vlan vlan id

(config-vlan)#name vlan name


(config-vlan)#end
```

Add a VLAN



Configuring VLANs

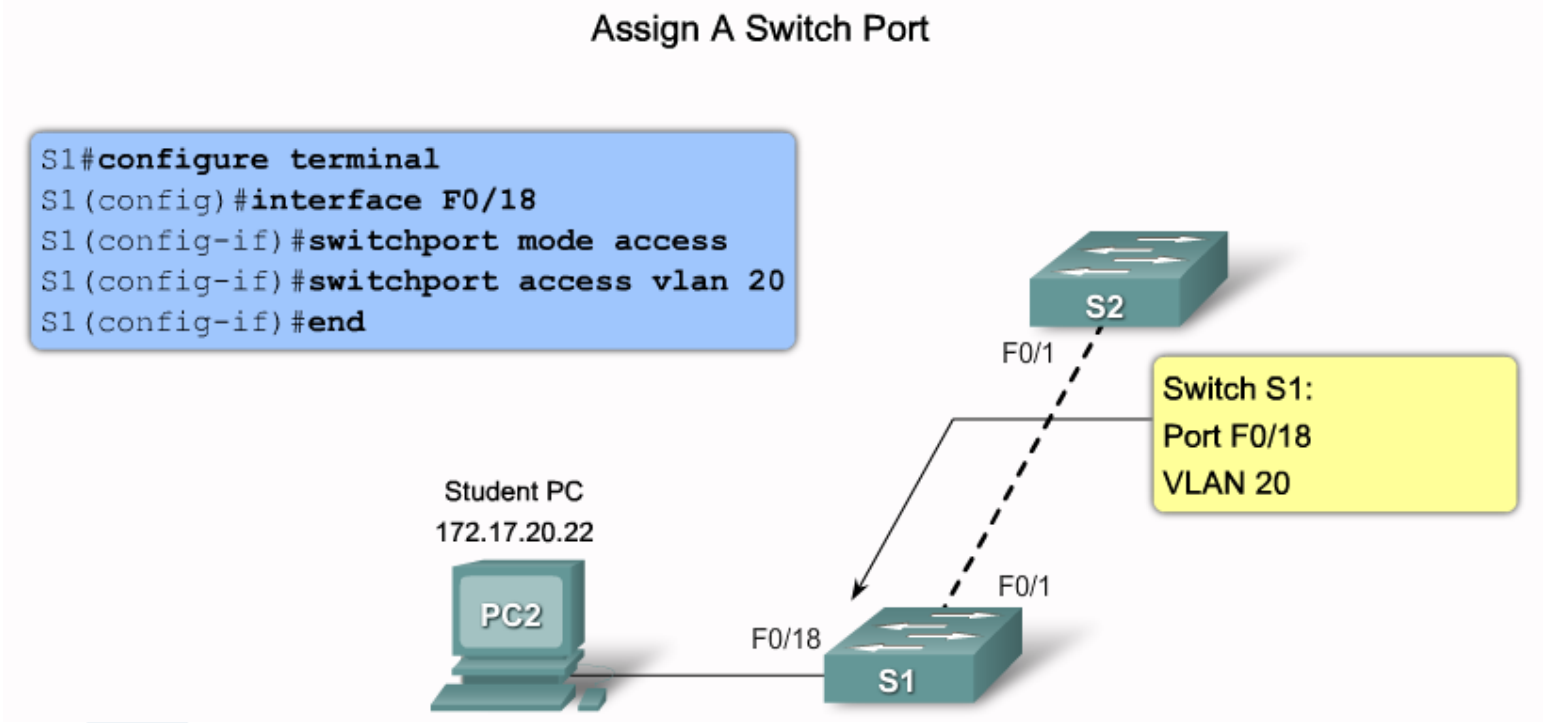
Add a VLAN

```
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
20   student                           active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Configuring VLANs

```
#configure terminal
(config)#interface interface id
(config-if)#switchport mode access
(config-if)#switchport access vlan
vlan id
(config-if)#end
```



Configuring VLANs

Assign A Switch Port

```
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
20   student                          active    Fa0/18
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
S1#
```

Verifying VLAN

Verify VLANs and Port Memberships

```
S1#show vlan name student

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
20   student                          active    Fa0/18

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

```
S1#show vlan summary
Number of existing VLANs            : 6
 Number of existing VTP VLANs       : 6
 Number of existing extended VLANs  : 0
```

Verifying VLAN

Verify VLANs and Port Memberships

```
S1#show interfaces vlan 20
Vlan20 is up, line protocol is down
  Hardware is EtherSVI, address is 001c.57ec.0641 (bia 001c.57ec.0641)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
```

Verifying VLAN

Verify VLANs and Port Memberships

```
S1#show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
```

Managing Port

Manage Port Memberships

```
S1(config)#interface fa0/18
S1(config-if)#no switchport access vlan
S1(config-if)#end
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3
                                                Fa0/5, Fa0/6, Fa0/7
                                                Fa0/9, Fa0/10, Fa0/
                                                Fa0/13, Fa0/14, Fa0
                                                Fa0/17, Fa0/18, Fa0
                                                Fa0/21, Fa0/22, Fa0
                                                Gi0/1, Gi0/2
20   student                          active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
```

Managing Port

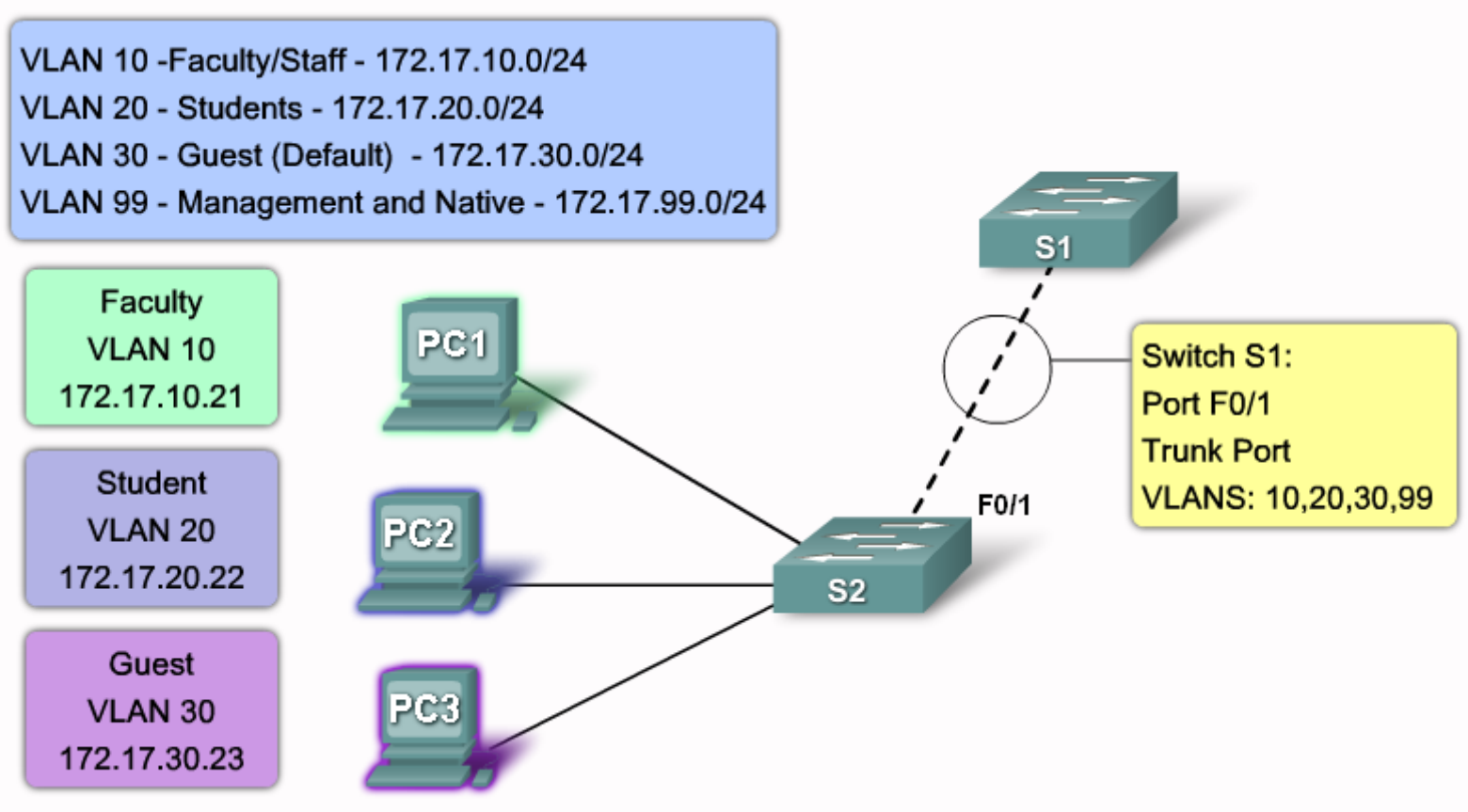
- Delete VLANs
- Alternatively, the entire vlan.dat file can be deleted using the command delete flash:vlan.datfrom privileged EXEC mode.
- After the switch is reloaded, the previously configured VLANs will no longer be present.
- This effectively places the switch into is "factory default" concerning VLAN configurations.

Configure a Trunk

#configure terminal
(config)#interface *interface id*
(config-if)#switchport mode trunk
(config)#switchport trunk native vlan *vlan-id*
(config-if)#switchport trunk allowed vlan add *vlan-list*
(config-if)#end

```
S1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#switchport trunk allowed vlan add 10,20,30
S1(config-if)#end
```

Configure a Trunk



Verify a Trunk

```
S1#show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (management)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
```

Managing a Trunk

```
(config-if)#no switchport trunk allowed
vlan
(config)#no switchport trunk native vlan
(config-if)#switchport mode access
```

```
S1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)#no switchport trunk allowed vlan
S1(config-if)#no switchport trunk native vlan
S1(config-if)#end
S1#show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
...
Trunking VLANs Enabled: ALL
```

Common problems with trunks

Problem	Result	Example
Native VLAN mismatches	Pose a security risks and create unintended results	For example one port has defined as VLAN 99, the other defined as VLAN 100
Trunk mode mismatches	Causes loss of network connectivity	For example on port configured as trunk mode "off" and the other as trunk mode "on".
VLANs and IP Subnets	Causes loss of network connectivity	For example user computers may have been configured with the incorrect IP addresses.
Allowed VLANs on Trunks	Causes unexpected traffic or no traffic is being sent over the trunk	The list of allowed VLANs does not support current VLAN trunking requirements.

THE END