

# LAN Technology

---

## Virtual LAN Protocol

*Arash Habibi Lashkari*

*PHD of Computer Science - Information Security*

*July 2010*

# *Virtual LAN Protocol*

---

## Outlines:

VLAN: Virtual Local Area Network and the IEEE 802.1Q

IEEE 802.1P: LAN Layer 2 QoS/CoS protocol for Traffic Prioritization

PPTP: Point to Point Tunneling Protocol

L2TP: Level 2 Tunneling Protocol

IPSec: IP Security

GMRP: GARP Multicast Registration Protocol

GARP: Generic Attribute Registration Protocol

GVRP: CARP VLAN Registration Protocol

# *What Is a VLAN?*

---

It is the territory over which a broadcast packet is delivered. (Also known as a broadcast domain)

Can be seen as a group of end hosts, perhaps on multiple physical LAN segments, that are not constrained by their physical location and can communicate as if they were on a common LAN.

VLAN related standards: IEEE 802.1Q and IEEE 802.1p

# *LAN v.s. VLAN*

---

VLAN allows you to have separate LANs among ports on the same switch.

For example, we configure a switch so that ports 1 – 32 are on VLAN A and ports 33 – 64 are on VLAN B.

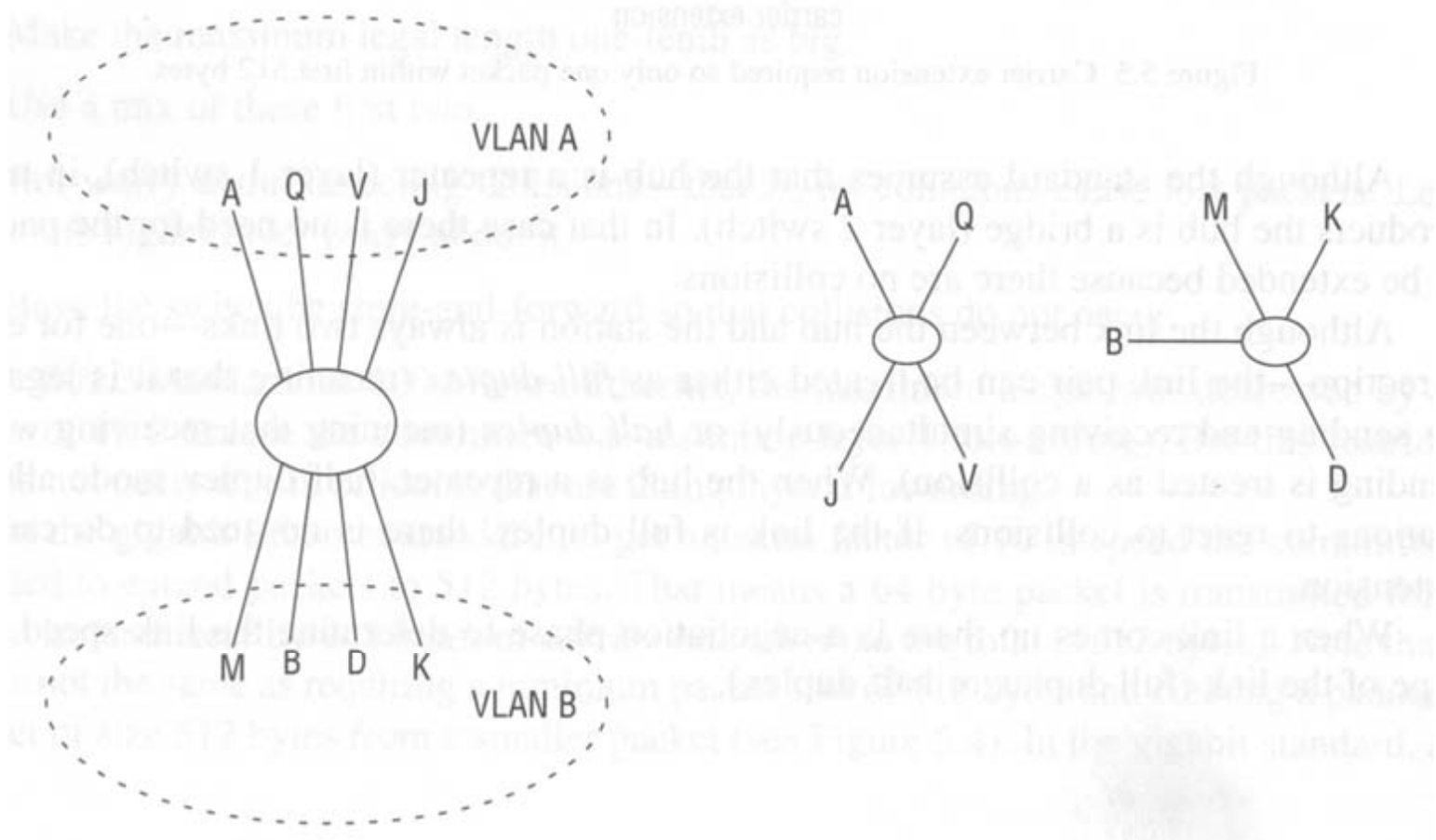
The switch would act as two separate switches.

One for forwarding packets among ports 1 – 32.

The other for forwarding packet between ports 33 – 64.

# VLAN Example

---



# *Why Using VLAN?*

---

Separate broadcast domains: a group of end hosts will not be bothered by the broadcast traffic generated by another group of end hosts.

Achieve higher security: now a host cannot snoop on the traffic of another group of hosts.

Ease management: do not need to change a host's IP address when it moves.

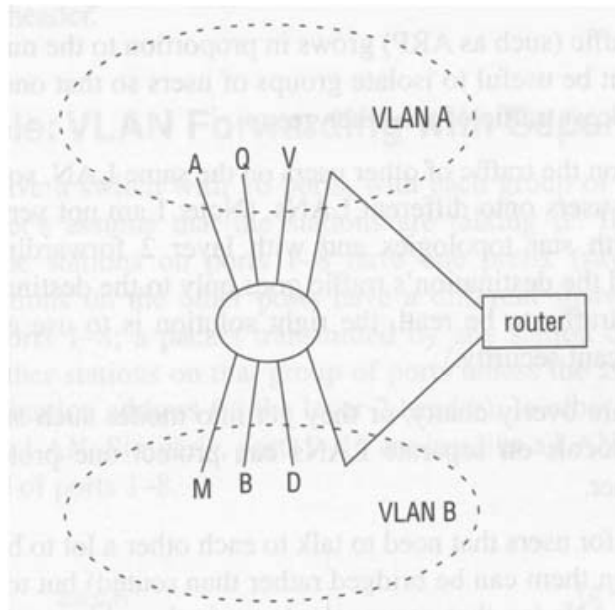
Nowadays most high-end switches and routers all use VLAN.  
(For example, CISOC routers and 3COM switches.)

If you do not know VLAN, you do not know how to configure these routers/switches.

## *Need A Router to Connect Different VLANs*

---

To get from one VLAN to the other, we need a router that connects to a port in each VLAN.



# *VLAN Types*

---

VLAN membership can be defined in several ways:

**Port-based** (e.g., ports 1-8 belong to VLAN A and ports 9-16 belong to VLAN B)

**Protocol-based** (e.g., end hosts (actually, the ports connecting to these hosts) who use IP belong to VLAN A and end hosts who use Appletalk belong to VLAN B)

**MAC-layer grouping** (e.g., 1:1:1:1:1:1 and 2:2:2:2:2:2 belong to VLAN A and 3:3:3:3:3:3 and 4:4:4:4:4:4 belong to VLAN B).

**Network-layer grouping:** (e.g., 140.113.1.1 and 140.113.1.2 belong to VLAN A and 140.113.2.1 and 140.113.2.2 belong to VLAN B).

**Multicast grouping:** (e.g., the hosts who have joined in multicast group A belong to VLAN A and the hosts who have join multicast group B belong to VLAN B.)

**Policy grouping** (primarily for network and information security control.)



# MAC-layer grouping

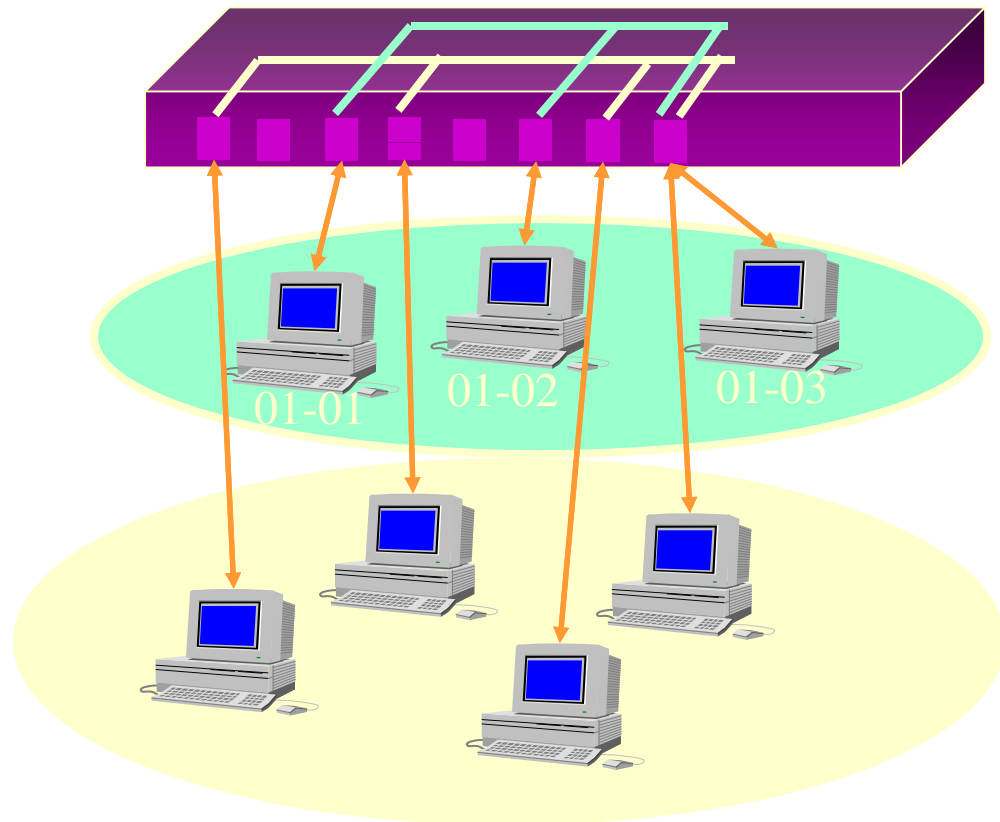
---

## VLAN A

00-00-00-00-01-01  
00-00-00-00-01-02  
00-00-00-00-01-03

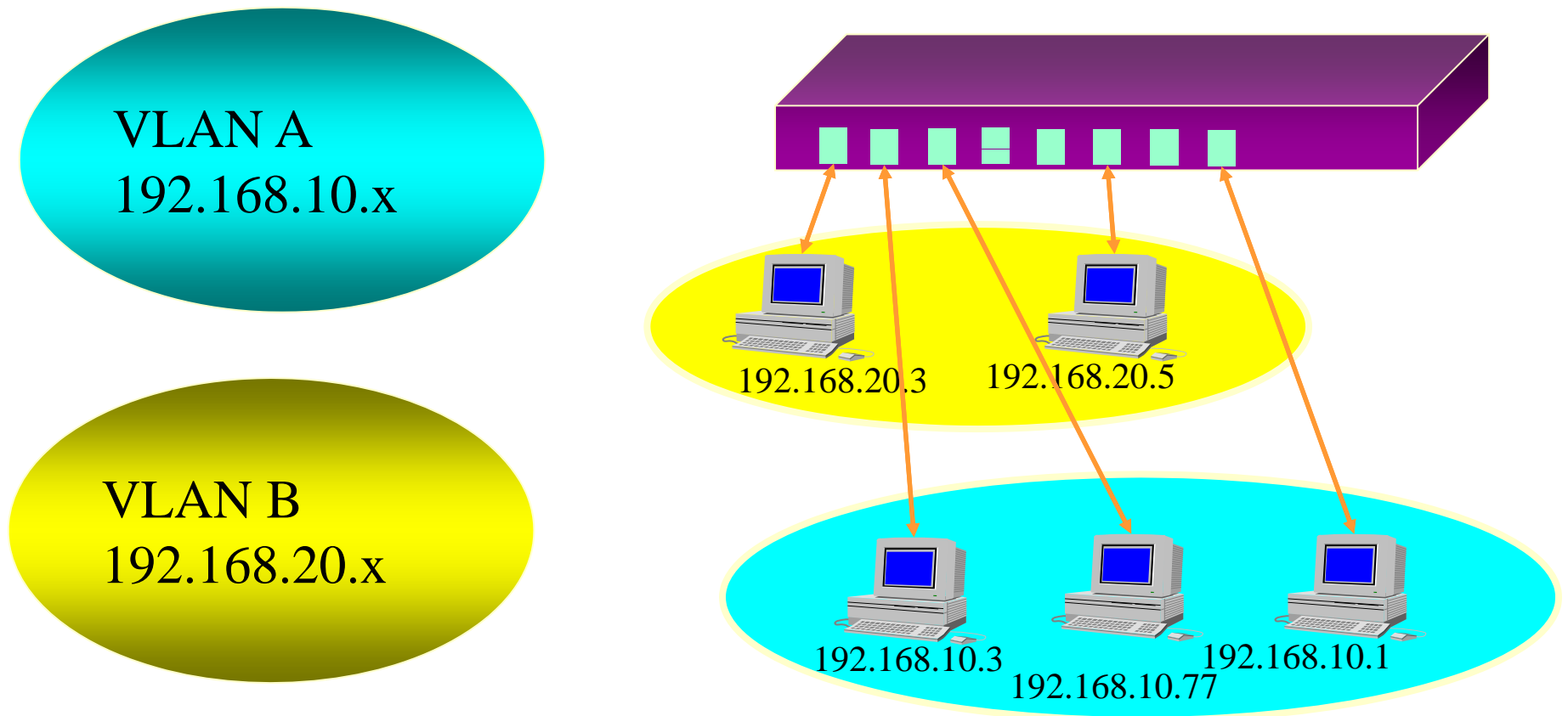
## VLAN B

00-00-00-00-02-01  
00-00-00-00-02-03  
00-00-00-00-02-04

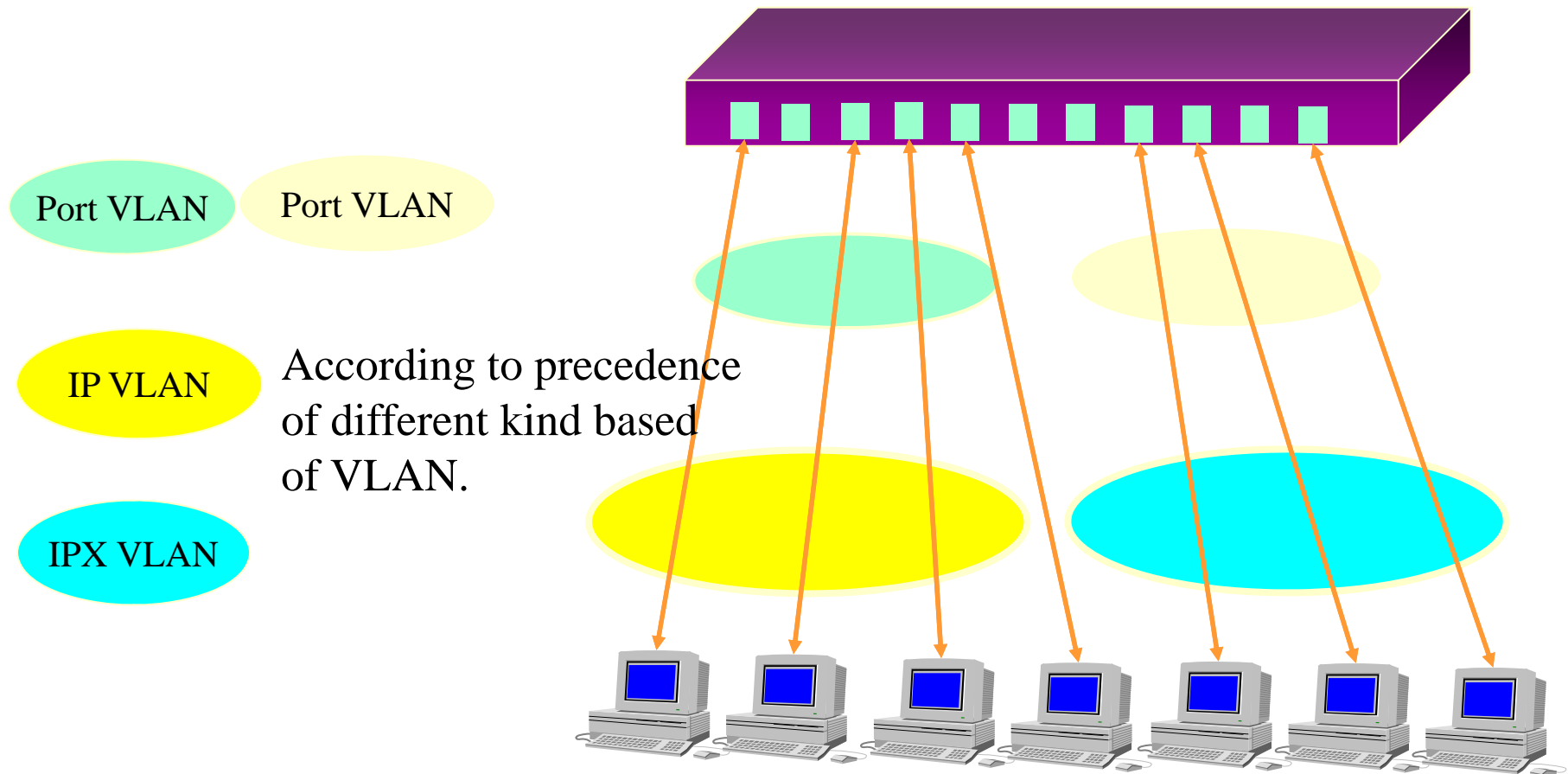


# Network-layer grouping

---



# Policy grouping



# *VLAN Aims and Benefits*

---

VLANs are supported over all **IEEE 802 LAN MAC protocols**, and over shared media LANs as well as point-to-point LANs.

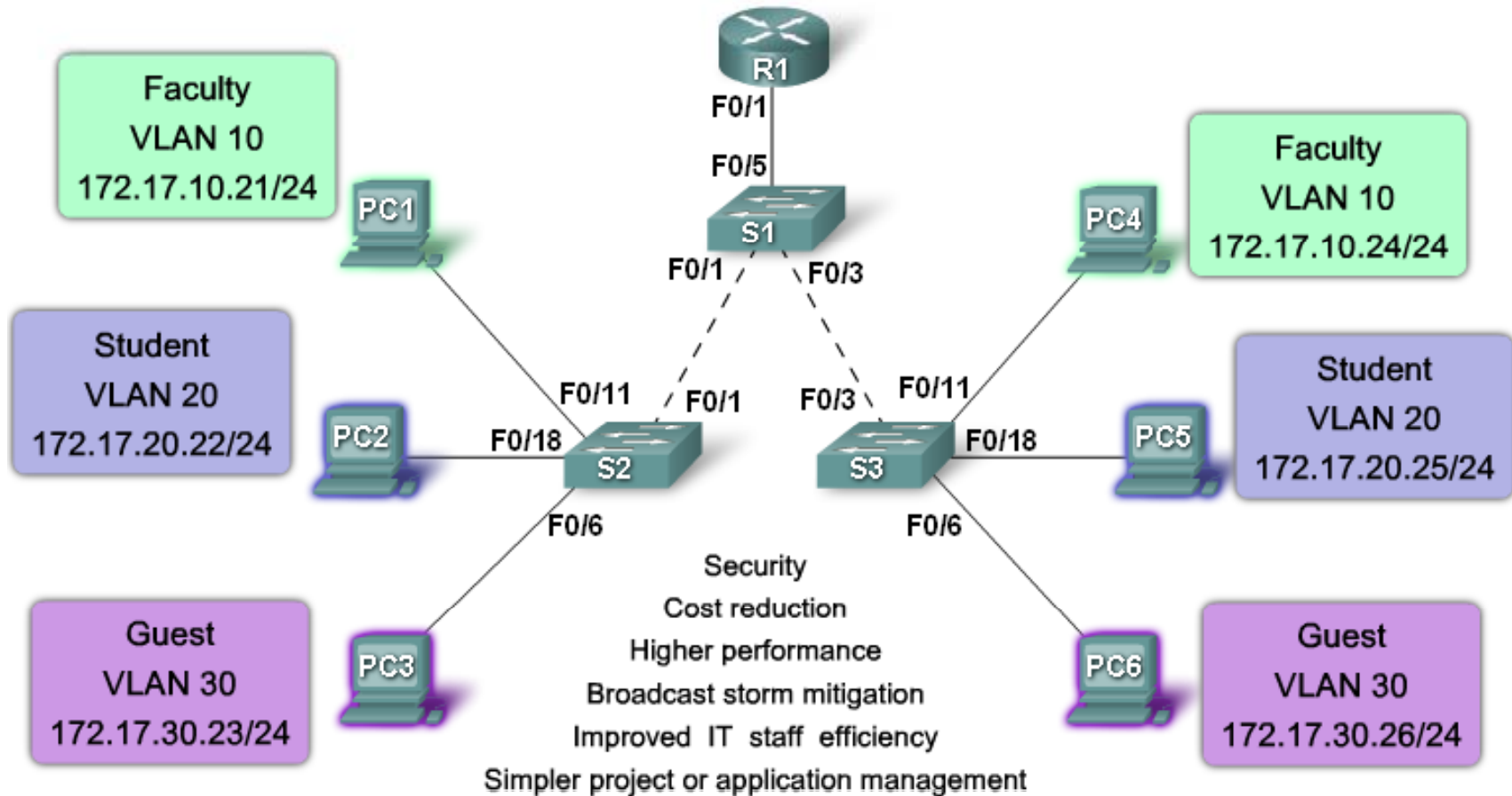
VLANs facilitate **easy administration of logical groups** of stations that can communicate as if they were on the same LAN.

**Traffic between VLANs is restricted** (Broadcast Domain).

VLANs **maintain compatibility with existing bridges** and end-stations.

If all Bridge Ports are configured to transmit and receive Untagged Frames, **bridges will work in plug-and-play mode**.

# Benefits of VLAN in a picture



# *VLAN Standard*

---

## IEEE 802.1P

Traffic Class Expediting (Prioritization).

Dynamic Multicast Filtering (GARP/GMRP).

## IEEE 802.1Q

Tagging

Ingress Rule, Forwarding Rule, Egress Rule (Frame Processing).

Port-based VLAN.

IVL/SVL, Asymmetric VLAN

VLAN Membership Maintain (GARP/GVRP).

## GVRP and Spanning Tree

# *IEEE 802.1P and 802.1Q*

---

802.1p basically an extension to 802.1D that defines enhancements to MAC bridges:

- Traffic Classes in bridges

- Dynamic Multicast Filtering including Registration and Management Services.

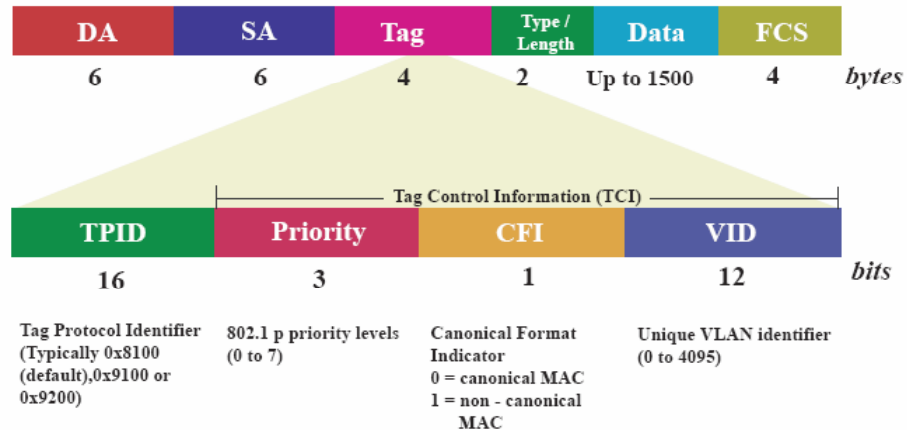
802.1Q is a standard for VLANs:

- Architecture of VLANs.

- Service provide in VLANs.

- Protocols and algorithms need to provide services.

# Virtual Local Area Network and the IEEE 802.1Q Structure



**TPID**- defined value of 8100 in hex. When a frame has the EtherType equal to 8100, this frame carries the tag IEEE 802.1Q / 802.1P.

**TCI** - Tag Control Information field including user priority, Canonical format indicator and VLAN ID.

**User Priority**- Defines user priority, giving eight ( $2^3$ ) priority levels. IEEE 802.1P defines the operation for these 3 user priority bits.

**CFI**- Canonical Format Indicator is always set to zero for Ethernet switches. CFI is used for compatibility reason between Ethernet type network and Token Ring type network. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port.

**VID**- VLAN ID is the identification of the VLAN, which is basically used by the standard 802.1Q. It has 12 bits and allow the identification of 4096 ( $2^{12}$ ) VLANs. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.



# *LAB*

---

Follow Lab 5 by Packet Tracer

# *Questions*

---

