Advanced Computer Network

Virtual Local Area Networks
VLAN

Some drawbacks in a LAN configuration

Lack of traffic isolation.

Although the hierarchy localizes group traffic to within a single switch, broadcast traffic must still traverse the entire institutional network.

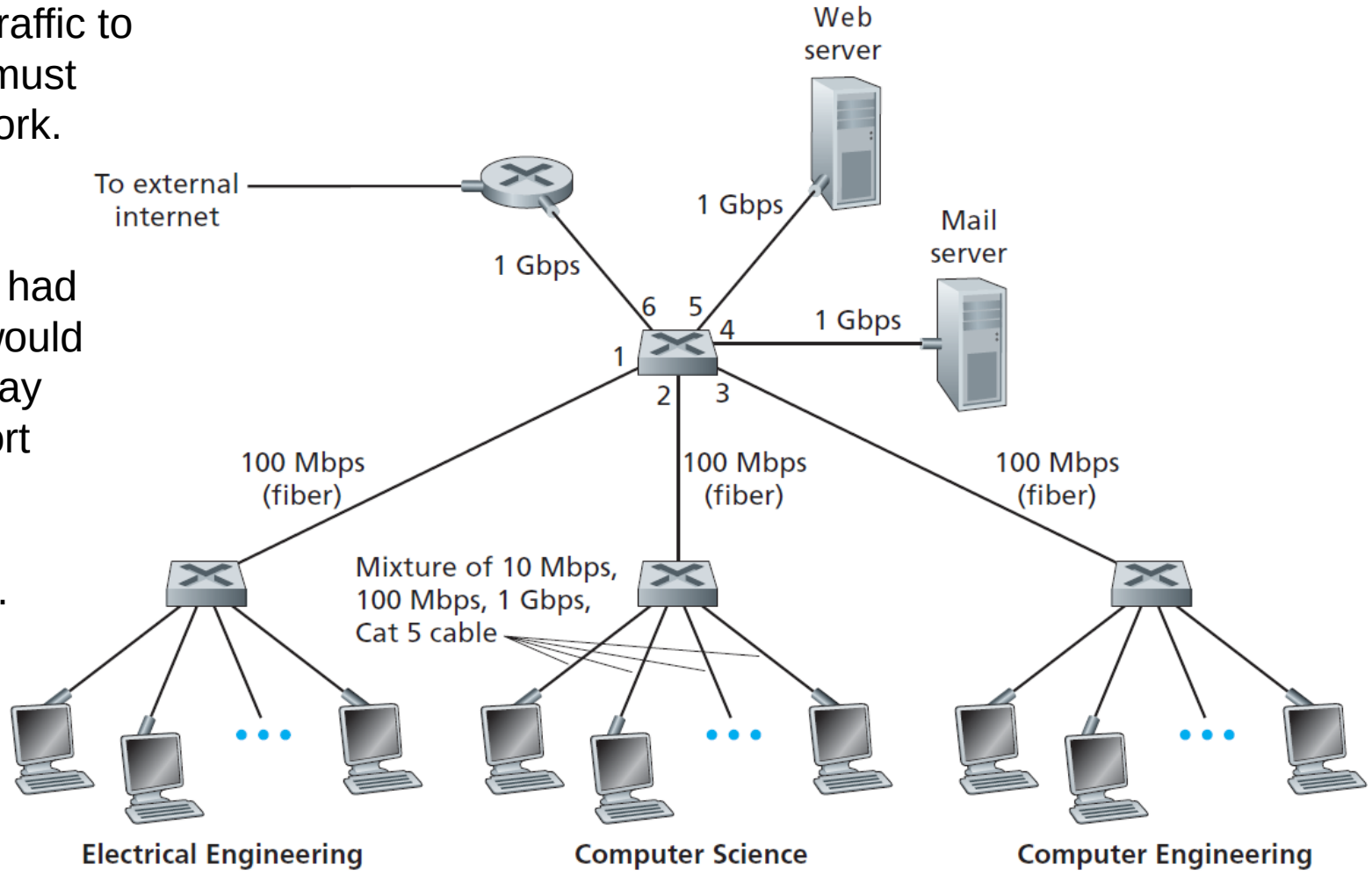
Inefficient use of switches.

If instead of three groups, the institution had 10 groups, then 10 first-level switches would be required. If each group were small, say less than 10 people, then a single 96-port switch would likely be large enough to accommodate everyone, but this single switch would not provide traffic isolation.

Managing users.

If an employee moves between groups, the physical cabling must be changed to connect the employee to a different switch.

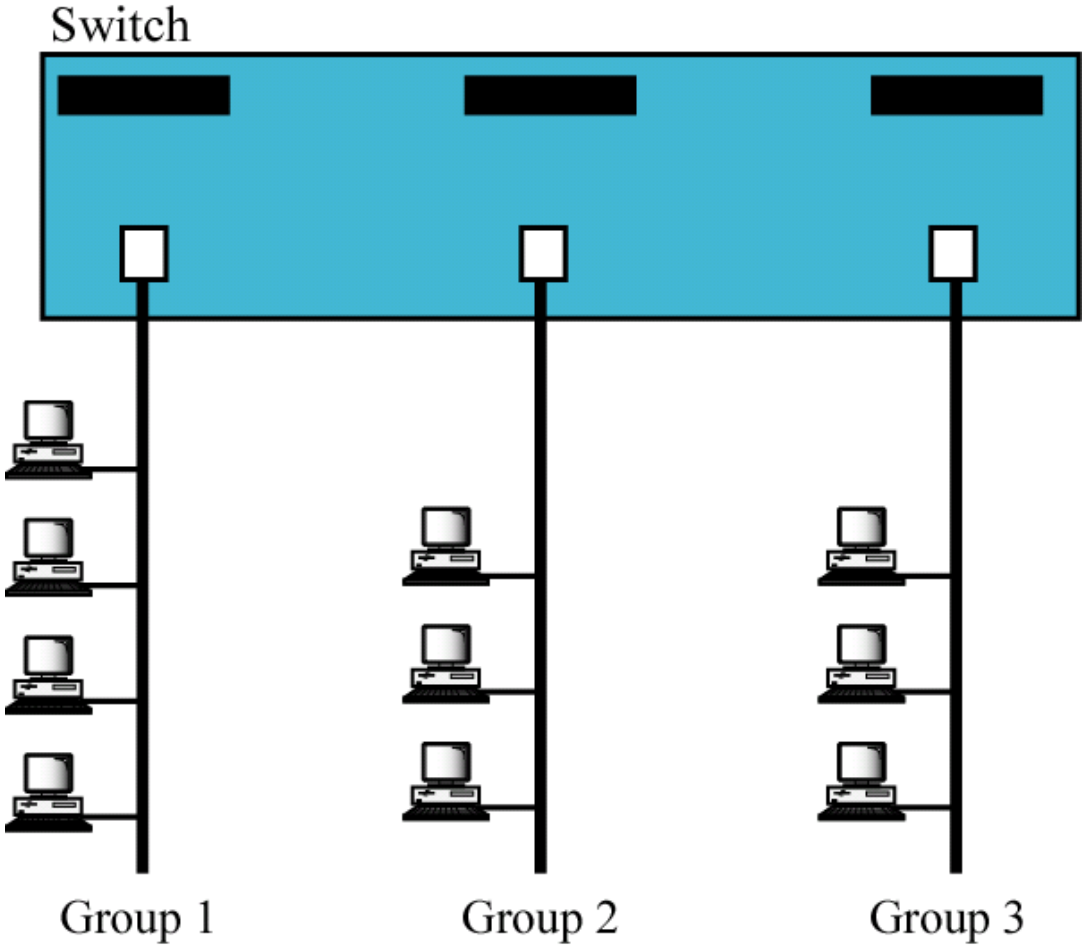
Employees belonging to two groups make the problem even harder.



What is VLAN ?

Virtual Local Area Networks, or **VLANs**, are a very simple concept that has been very poorly defined by the industry.

A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

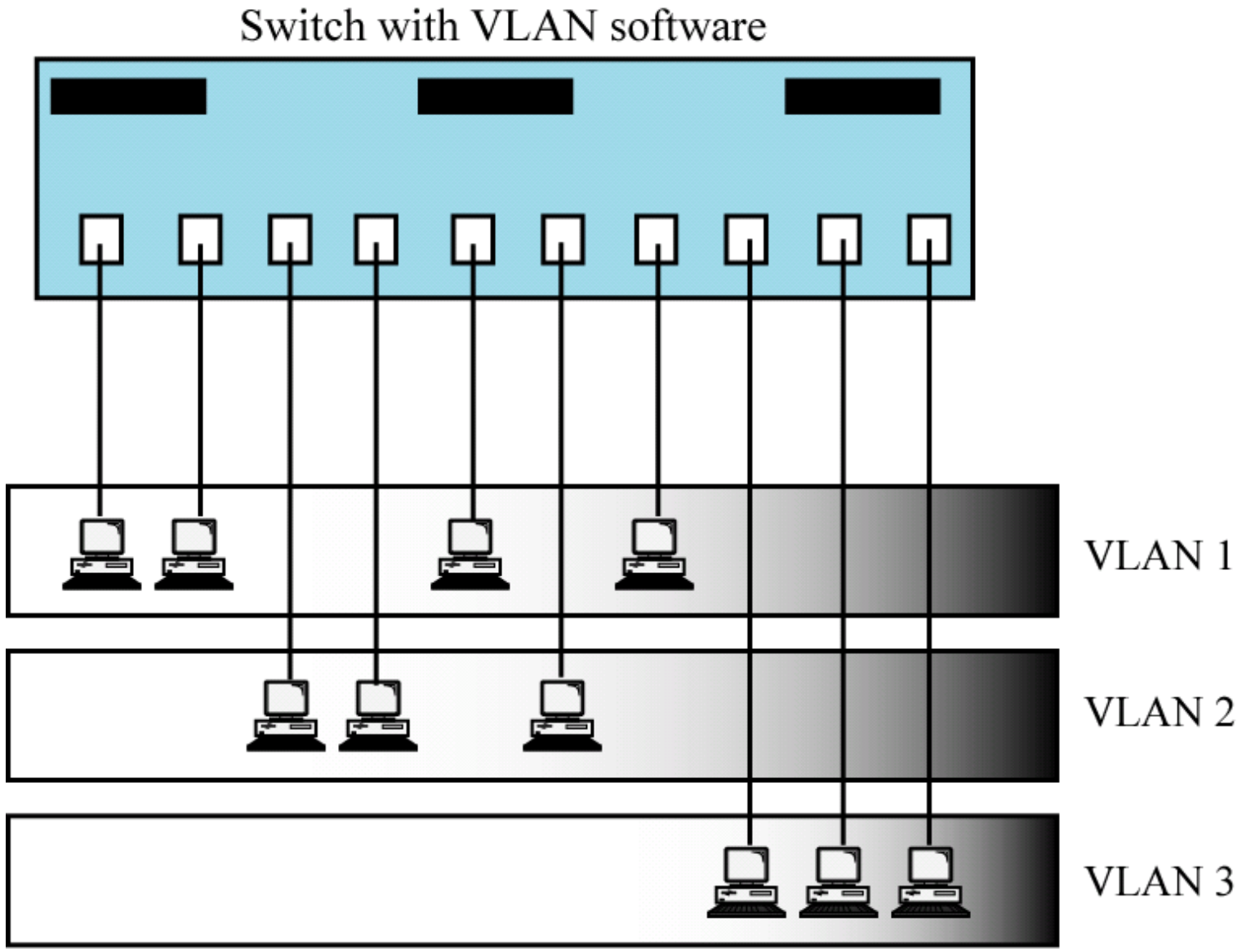


- vendor-specific solution and strategy, so defining it is an issue.
- VLAN's allow a network manager to logically segment a LAN into different broadcast domains.(VLANs define broadcast domains in a Layer 2 network.)
- multiple physical LAN segments independent of physical location and can communicate as if they were on a common LAN

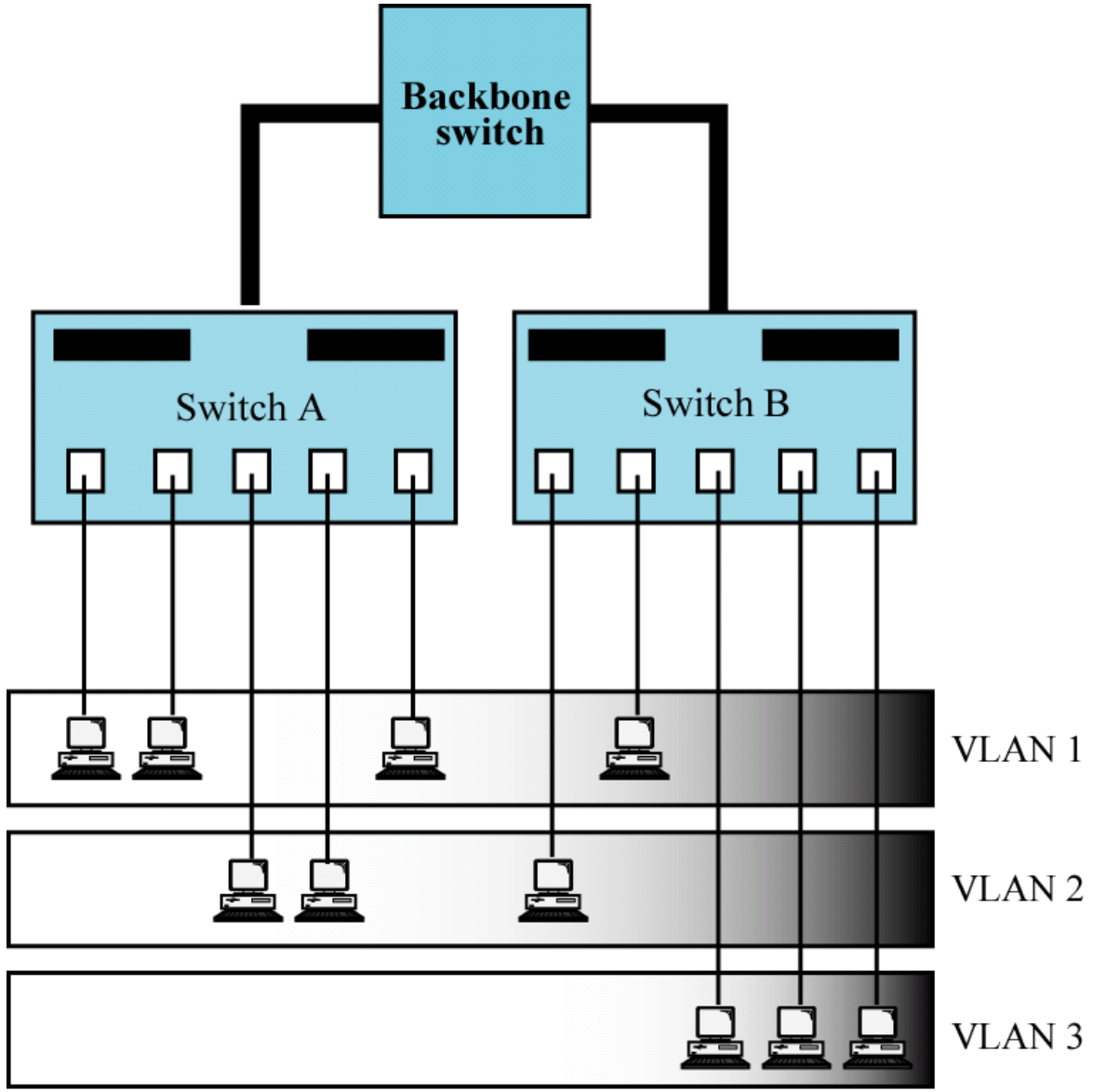
Why use VLAN's?

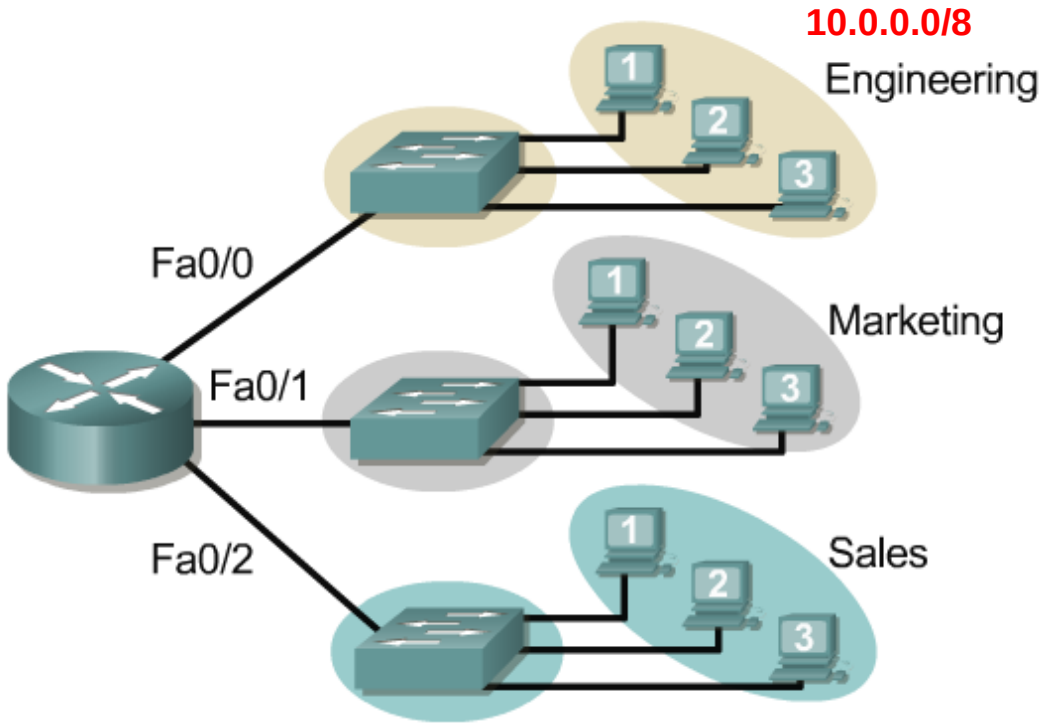
- Performance
- Formation of Virtual Workgroups
- Simplified Administration
- Reduced Cost
- Security

A switch using VLAN software



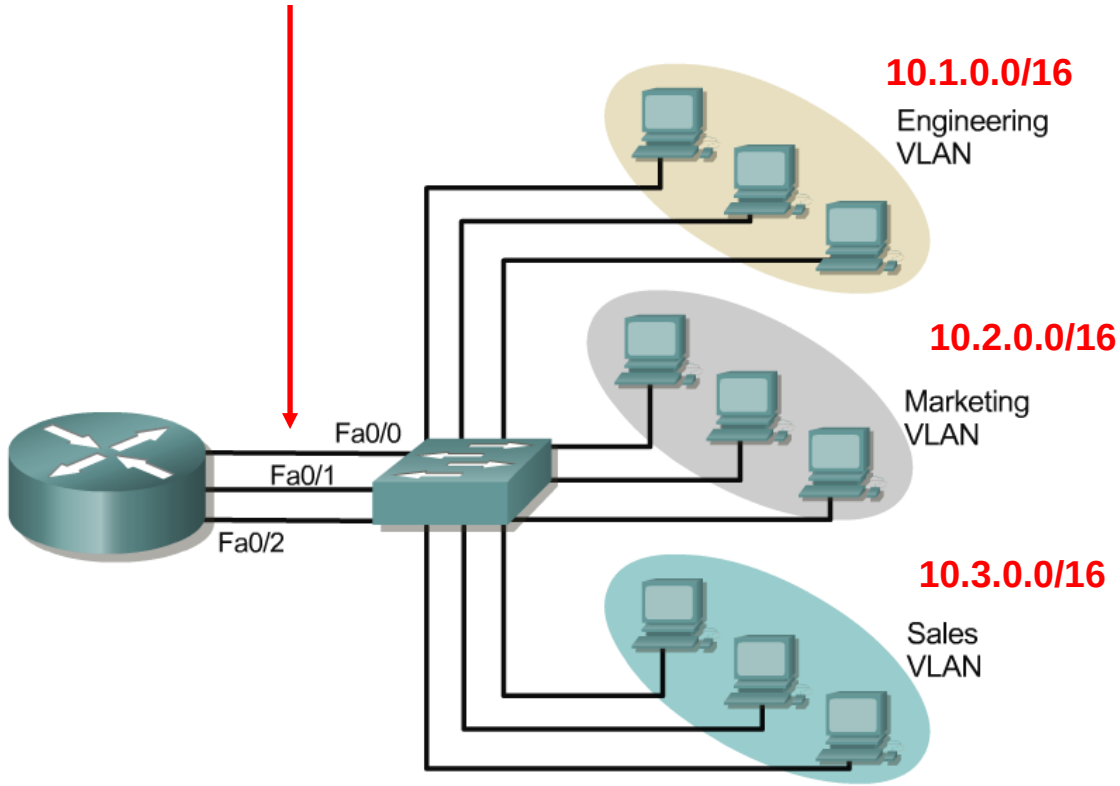
Two switches in a backbone using VLAN software





Without VLAN

One link per VLAN or single VLAN Trunk



With VLAN

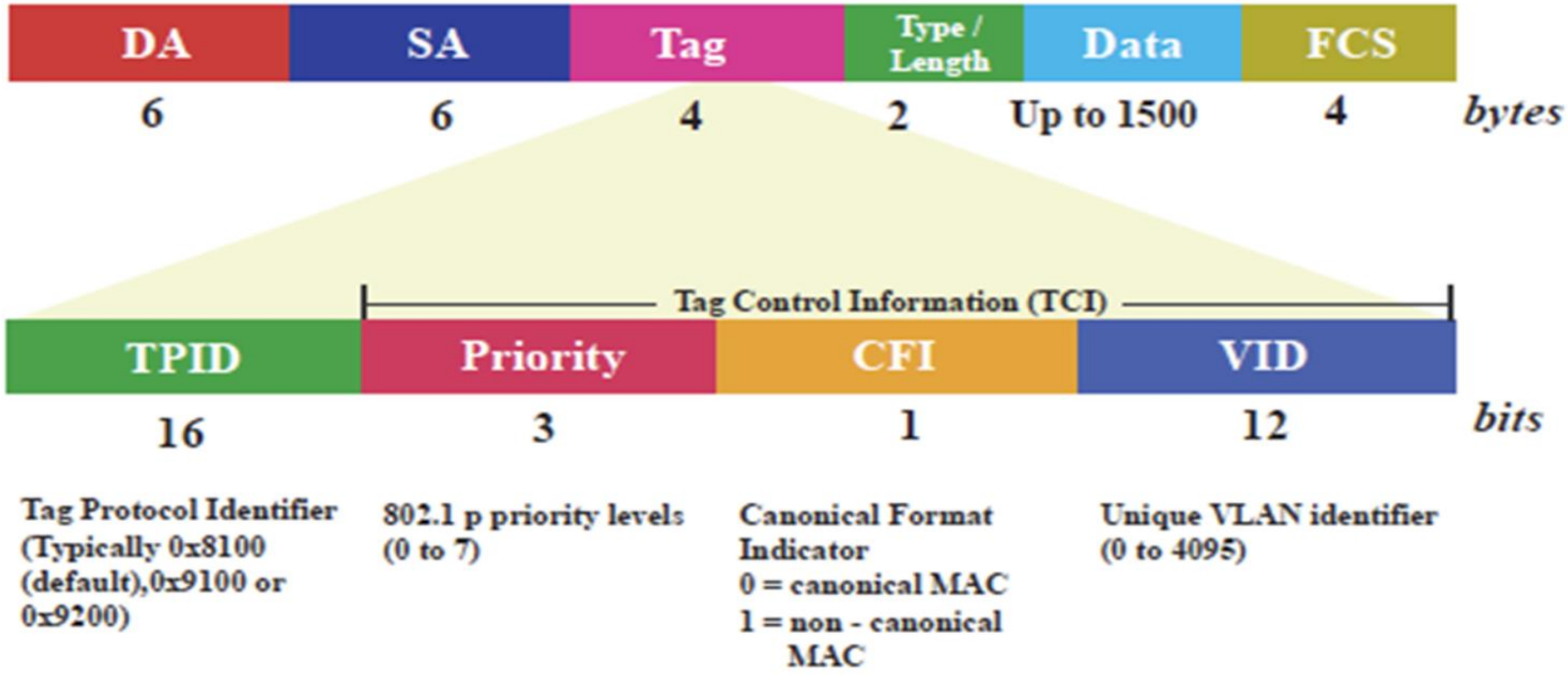
The switch is configured where each port can be specified as a VLAN.

Frame Processing in VLAN environment

Role of Bridges

- bridge on receiving data determines to which VLAN the data belongs either by implicit or explicit tagging [802.1Q].
- The bridge also keeps track of VLAN members in a filtering database which it uses to determine where the data is to be sent
- all the bridges in the VLAN should contain the same information in their respective filtering databases

Frame format

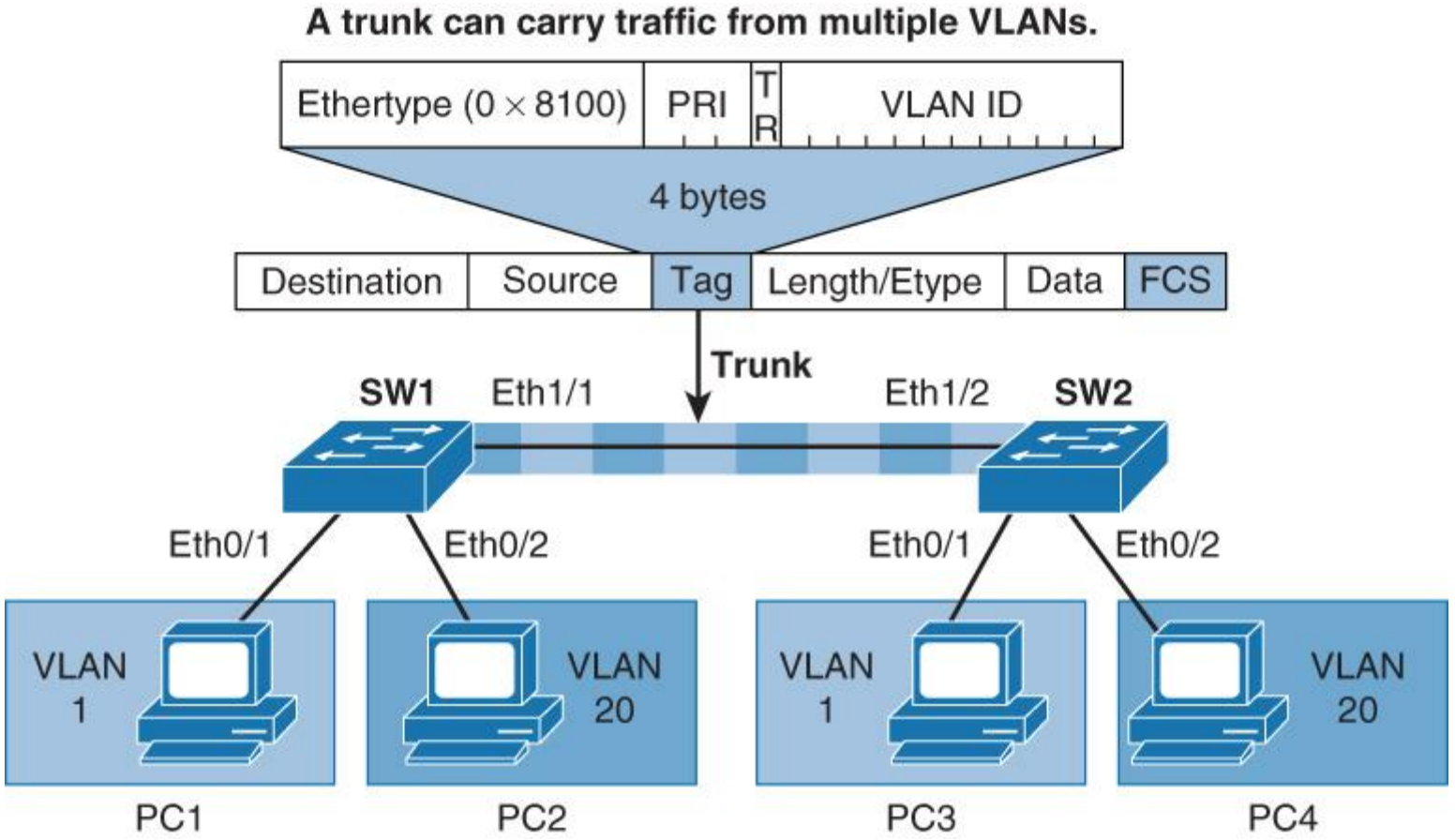


Original Ethernet frame (top), 802.1Q-tagged Ethernet VLAN frame

Tag: Inserted 802.1Q tag (4 bytes, detailed here)

- **EtherType(TPID):** Set to 0x8100 to specify that the 802.1Q tag follows. (two bytes)
- **PRI**: 3-bit 802.1p priority field. Used for Class of Service (CoS) to prioritize traffic. It supports 8 levels of priority (0 to 7).
- **CFI**: Canonical Format Identifier is always set to 0 for Ethernet switches and to 1 for Token Ring-type networks. (one bit)
- **VLAN ID:** 12-bit VLAN field. Identifies the VLAN to which the frame belongs. The VID can range from 0 to 4095, but VLAN 0 is reserved for priority-tagged frames, and VLAN 4095 (0xFFF) is reserved for implementation use, so valid

VLAN Trunks



› **Inter-Switch Link (ISL):** A Cisco proprietary trunking encapsulation (Ignore…. Legacy)

› **IEEE 802.1Q:** An industry-standard trunking method

› Why the VLAN ID is Checked on a Trunk Link?

1. **VLAN Identification**:
    1. The VLAN ID in the tag identifies which VLAN the frame belongs to.
    2. Switches use this information to forward the frame only to ports that are members of the same VLAN (or to other trunk links that allow that VLAN).
2. **VLAN Filtering**:
    1. Trunk links can be configured to allow or disallow specific VLANs.
    2. The switch checks the VLAN ID to ensure the frame is permitted on the trunk.
3. **Broadcast Domain Separation**:
    1. VLANs separate broadcast domains. The switch uses the VLAN ID to ensure that broadcast, multicast, and unknown unicast traffic are forwarded only within the correct VLAN.
4. **QoS and Priority**:
    1. The Priority Code Point (PCP) field in the VLAN tag can be used for Quality of Service (QoS) to prioritize traffic based on the VLAN ID.

VLAN Adding and Removing

› Step 1: PC-A Sends a Frame to Switch 1

› Step 2: Switch 1 Adds a VLAN Tag 20

› Step 3: Switch 1 Forwards the Frame Over the Trunk Link

› Step 4: Switch 2 Receives the Frame

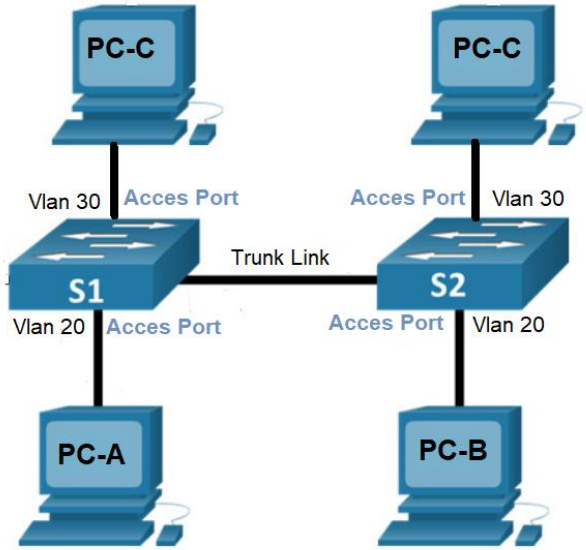
- Switch 2 receives the frame on the trunk link.
- It examines the VLAN tag to determine the VLAN ID (20).
- Switch 2 checks its VLAN database to confirm that VLAN 20 is allowed on the trunk link.

› Step 5: Switch B Processes the Frame

- Since the frame is destined for PC-B (in VLAN 20), Switch 2 forwards it to the appropriate access port.
- Switch 2 removes the VLAN tag (because the frame is being sent out an access port) and forwards the frame to PC-B.

› Step 7: PC-B Receives the Frame

- PC-B receives the untagged frame and processes it.



Field	Value (Hex)	Description
Destination MAC	Host 2's MAC	MAC address of the destination host.
Source MAC	Host 1's MAC	MAC address of the source host.
TPID	`0x8100`	Indicates an 802.1Q-tagged frame.
PCP + DEI + VID	`0x0014`	Priority 0, DEI 0, VLAN ID 20.
EtherType	`0x0800`	Indicates IPv4 payload (for example).
Payload	Data	The actual data being transmitted.
FCS	CRC value	Frame Check Sequence for error detection.