

# CS 540

# Computer Networks II

Sandy Wang  
sandy.w@svuca.edu

## **2.1 VLAN**

# Topics

1. Overview
2. **LAN Switching**
3. IPv4
4. IPv6
5. Tunnels
6. Routing Protocols -- RIP, RIPng
7. Routing Protocols -- OSPF
8. IS-IS
9. Midterm Exam
10. BGP
11. MPLS
12. Transport Layer -- TCP/UDP
13. Congestion Control & Quality of Service (QoS)
14. Access Control List (ACL)
15. Final Exam

# Reference Books

- **Routing TCP/IP Volume I, 2nd Edition** by Jeff Doyle and Jennifer Carroll  
ISBN: 1-57870-089-2
- **Routing TCP/IP Volume II** by Jeff Doyle and Jennifer DeHaven     ISBN: 1-57870-089-2
- **Cisco CCNA Routing and Switching ICND2 200-101 Official Cert Guide, Academic Edition** by Wendel Odom -- July 10, 2013.     ISBN-13: 978-1587144882
- **The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference** by Charles M. Kozierok – October 1, 2005.     ISBN-13: 978-1593270476
- **CCNA Routing and Switching 200-120 Network Simulator.** By Wendell Odom, Sean Wilkins. Published by Pearson IT Certification.
- <http://class.svuca.edu/~sandy/class/CS540/>

# Network Device Types

- There are 5 general devices:

- layer 2 {
- Repeater
  - Hub receives & broadcast.
  - Bridge smarter, remember the node on which side.
  - Switch multipoint bridge
  - Router

# Network Device - Repeater

- Repeater
  - A Layer 1 device
  - An electronic device to receive a signal on a port and retransmits it at a higher level or higher power
  - Used when you need to go farther distances than the cabling will allow
  - Usually has 2 ports (IN/OUT)

# Network Device - Hub

- Hub
  - A Layer 1 device
  - A device that contains multiple ports
  - Has no logic or “brain”
  - Simply passes data out all other ports
  - In simple terms, it is a multi-port repeater

# Network Device - Bridge

- Bridge
  - A Layer 2 device
  - Connects multiple Layer 2 segments
  - Has logic or “brain”
  - Learns what Layer 2 MAC addresses are associated with each port
  - Receives frames destined for a particular MAC address and only sends the data out the correct port

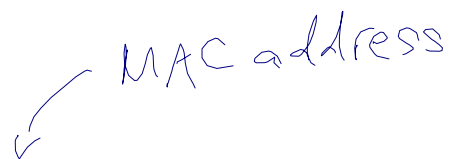


# Network Device - Switch

- Switch

- A layer 2 device
- Basically a multi-port bridge
- Learns MAC Addresses to Port mappings
- Doesn't flood data out every port unless the MAC address hasn't been learned

MAC address



# Network Device - Router

- Router
  - A Layer 3 device
  - Connects multiple Layer 3 networks
  - Uses Layer 3 addressing (IP addressing)
  - Allows communication between different Layer 2 segments
  - Breaks up broadcast domains

# Broadcast Domain?

- A broadcast domain is a network segment in which any network device can transmit data directly to another device without going through a router
- A layer 3 device breaks up a broadcast domain

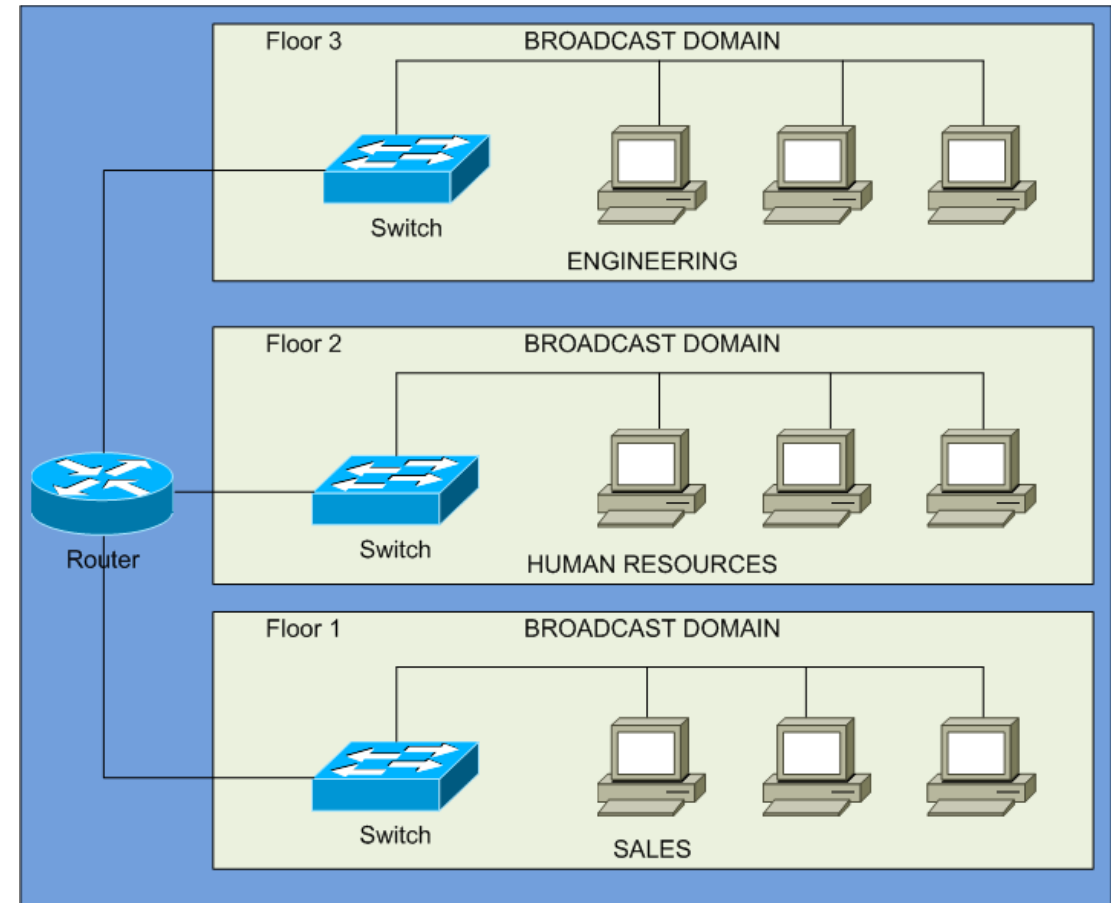
So what is a VLAN?

# What is a VLAN?

- A virtual local area network (VLAN) is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain regardless of their physical location.

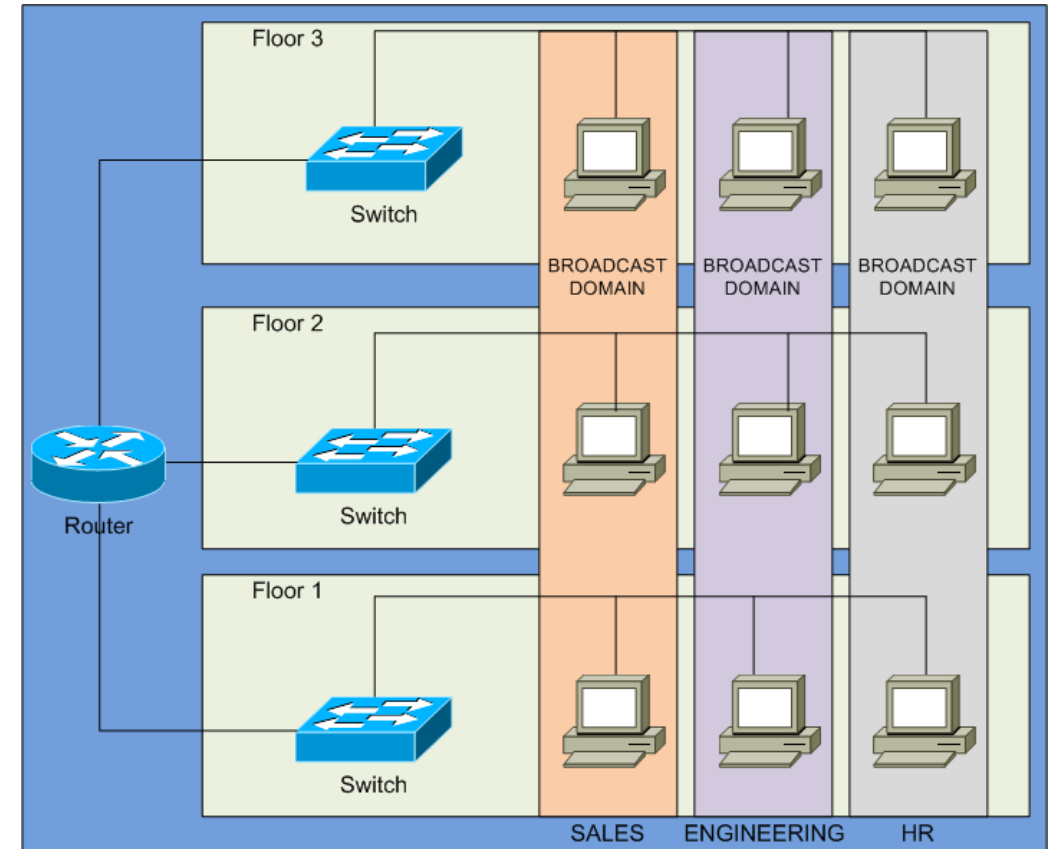
# Traditional LAN

- A traditional LAN would require all users of the same requirements and same IP subnet (broadcast domain) be connected to the same equipment.



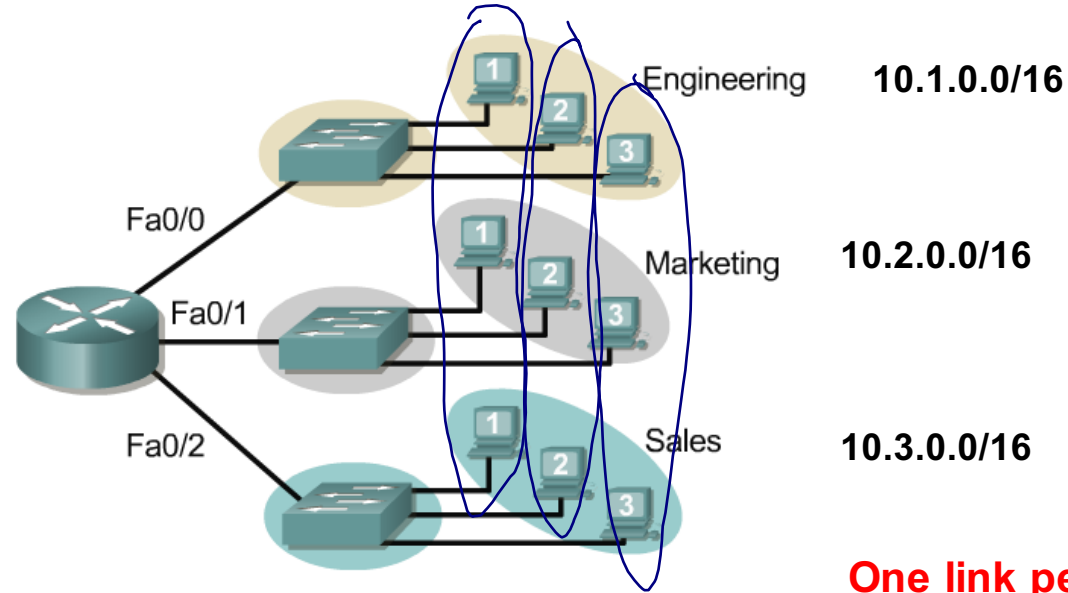
# VLAN-based LAN

- By utilizing VLANs, the same users can be spread out over various geographical locations and still remain in their same IP subnet (broadcast domain).



# Broadcast domains with VLANs and routers

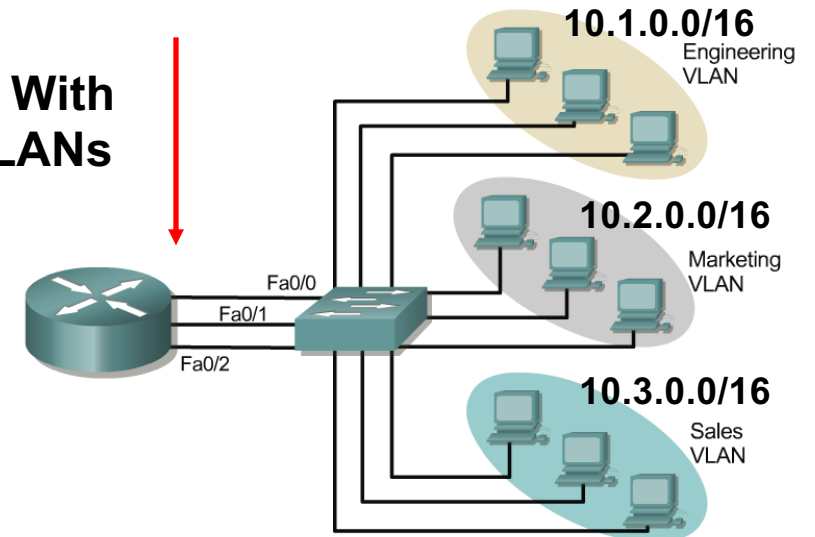
## 1) Without VLANs



- 1) Without VLANs, each group is on a different IP network and on a different switch.
- 2) Using VLANs. Switch is configured with the ports on the appropriate VLAN. Still, each group on a different IP network; however, They are all on the same switch.
- What are the broadcast domains in each?

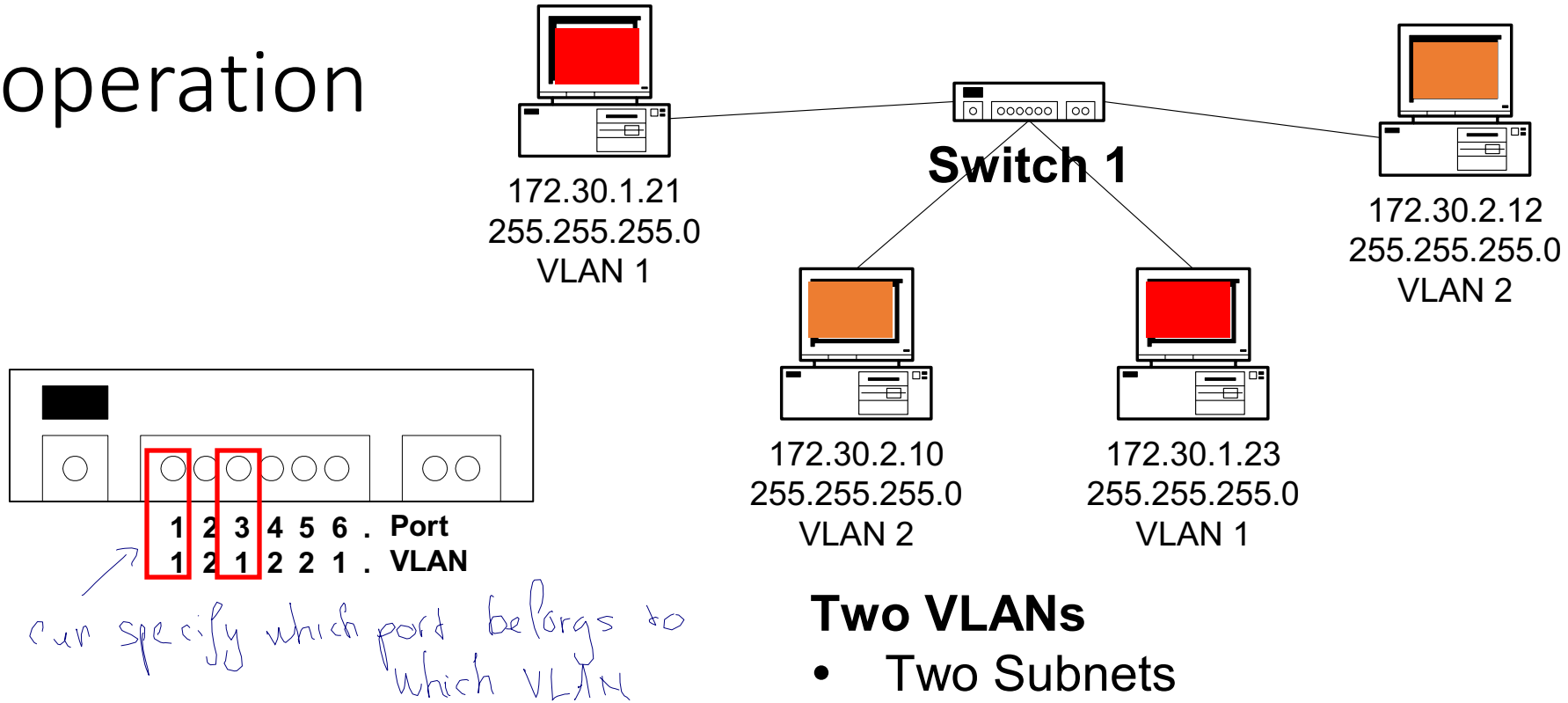
**One link per VLAN or a single VLAN Trunk (later)**

## 2) With VLANs





# VLAN operation

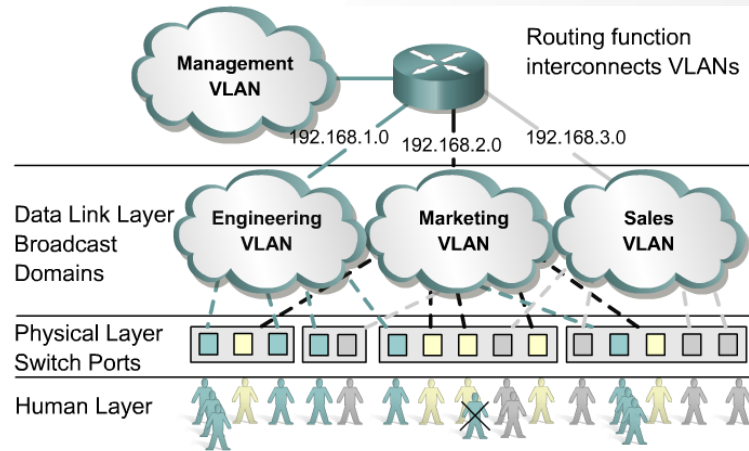


Important notes on VLANs:

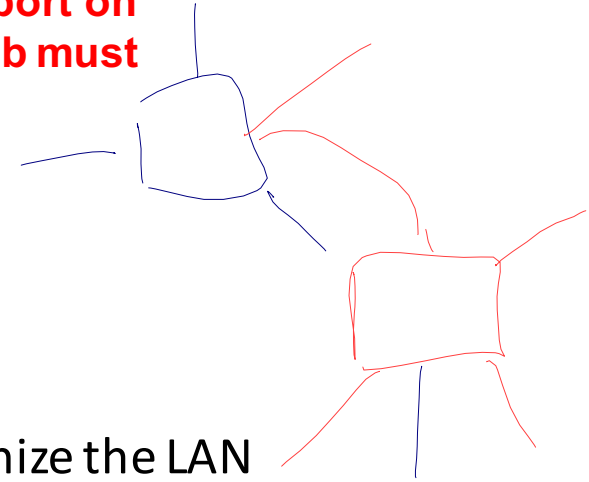
1. VLANs are assigned on the switch port. There is no "VLAN" assignment done on the host (usually).
2. In order for a host to be a part of that VLAN, it must be assigned an IP address that belongs to the proper subnet.  
Remember: VLAN = Subnet
3. Assigning a host to the correct VLAN is a 2-step process:
  1. Connect the host to the correct port on the switch.
  2. Assign to the host the correct IP address depending on the VLAN membership

# Benefits of VLANs

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



**If a hub is connected to VLAN port on a switch, all devices on that hub must belong to the same VLAN.**

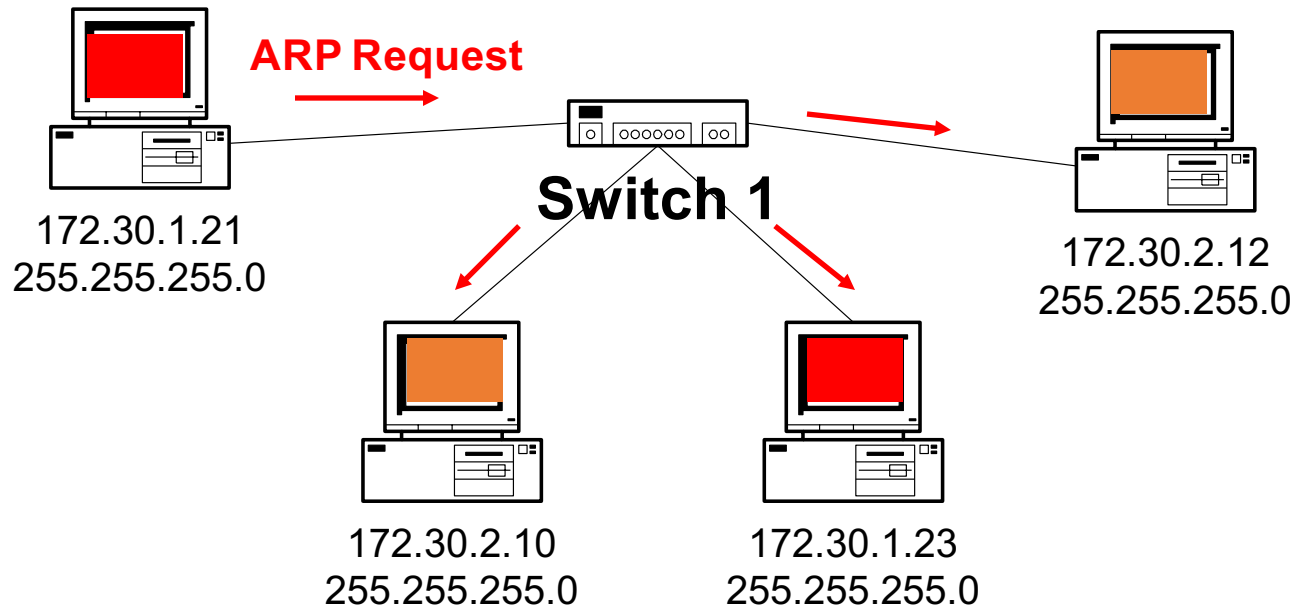


- The key benefit of VLANs is that they permit the network administrator to organize the LAN logically instead of physically.
- This means that an administrator is able to do all of the following:
  - Easily move workstations on the LAN.
  - Easily add workstations to the LAN.
  - Easily change the LAN configuration.
  - Easily control network traffic.
  - Improve security.

benefits

- security
- ease of mgmt.

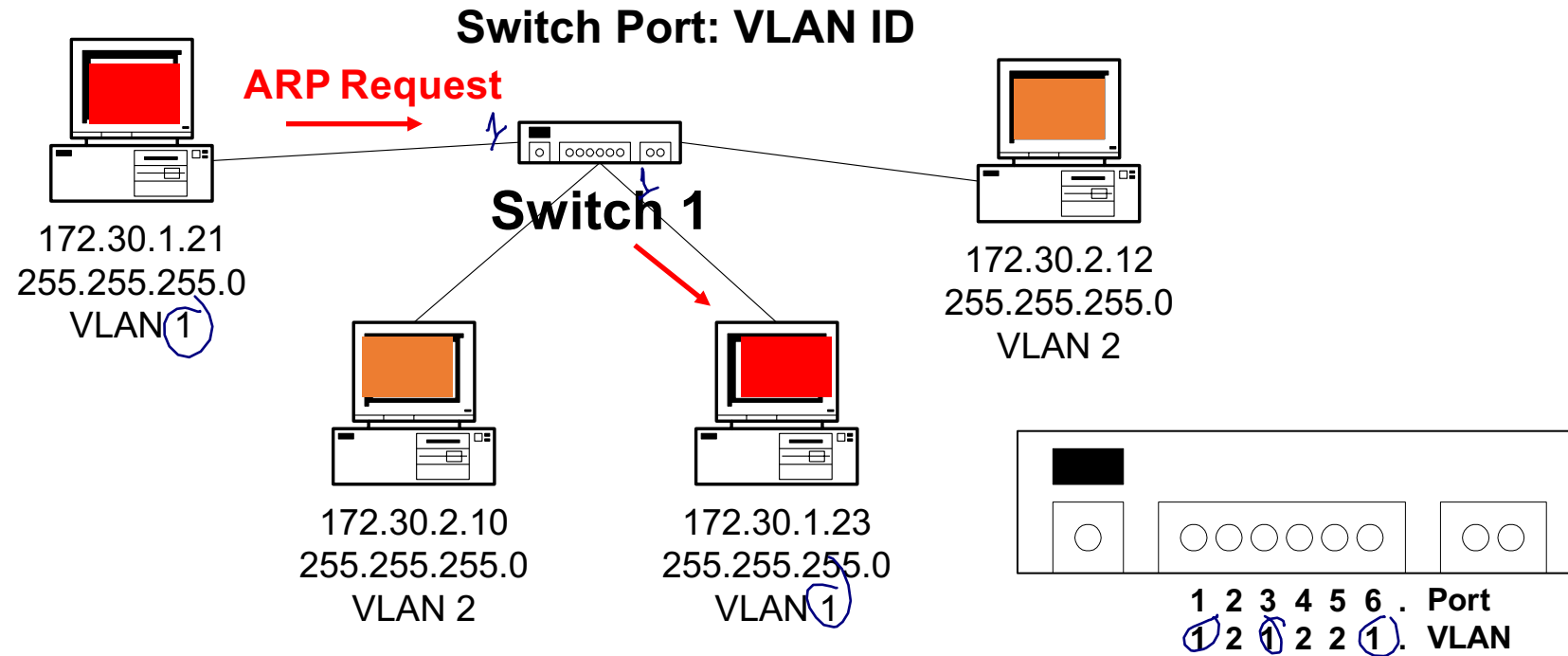
# Without VLANs – No Broadcast Control



## No VLANs

- Same as a single VLAN
  - Two Subnets
- Without VLANs, the ARP Request would be seen by all hosts.
  - Again, consuming unnecessary network bandwidth and host processing cycles.

# With VLANs – Broadcast Control



## Two VLANs

- Two Subnets

# How VLANs work?

# How VLANs Work?

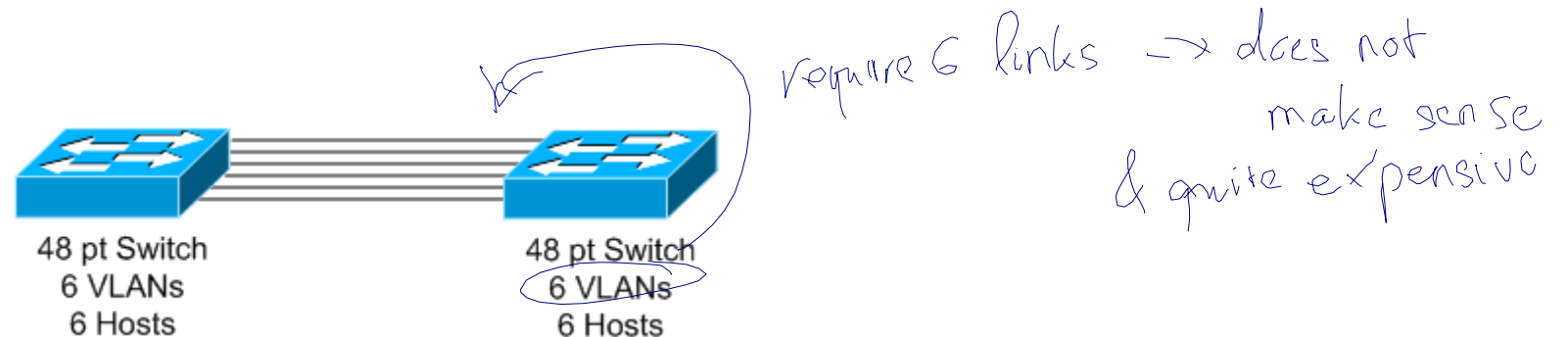
- VLANs are identified by a number (12 bits)
  - Valid ranges 1-4094
- On a VLAN-capable switch, you assign ports with the appropriate VLAN number
- The switch then only allows data to be sent between ports with the same VLAN

# How VLANs Work?

- Since almost every network is larger than a single switch, there needs to be a way to have traffic sent between two different switches
- One way to do it is to assign a port on each switch with a VLAN and run a cable between the switches
  - Not very feasible or cost effective

# How VLANs work?

- For example, if there were 6 hosts on each switch on 6 different vlans, you would need 6 ports on each switch to connect the switches together. This would mean that if you had 24 different vlans you could only have 24 hosts on a 48 port switch





# How VLANs work?

- There was a standard develop to make it so that a single connection between two switches could be used to send traffic for all vlans
- 802.1q – Provides a VLAN tag in front of the Layer 2 frame

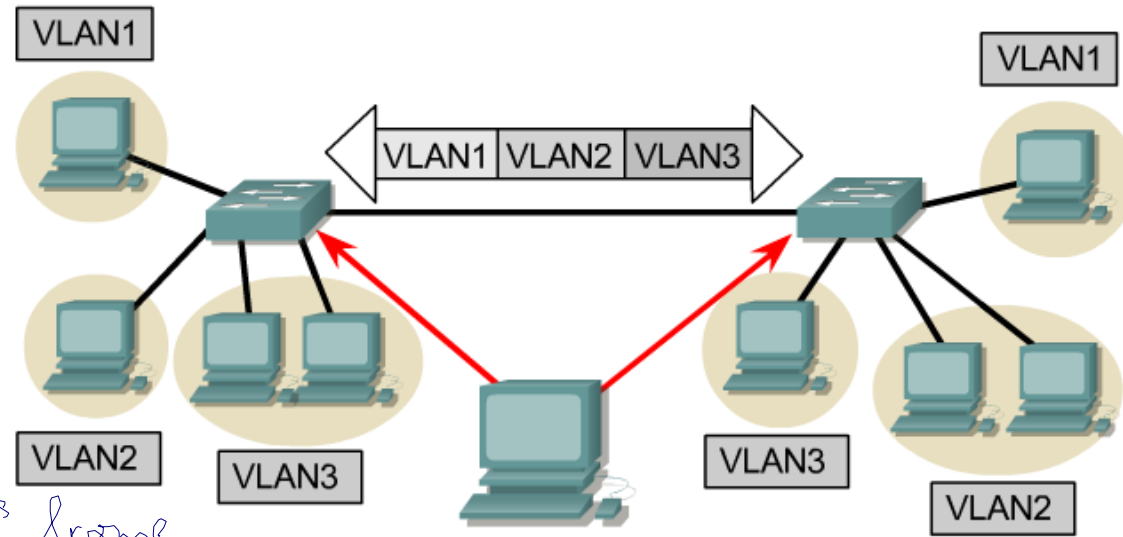
# How VLANs work?

- You enable 802.1q tagging (trunking) on the ports between the switches
- The switch receives the frame with the 802.1q header and strips it off
- It determines what VLAN and sends the data to the appropriate port

# VLAN Tagging

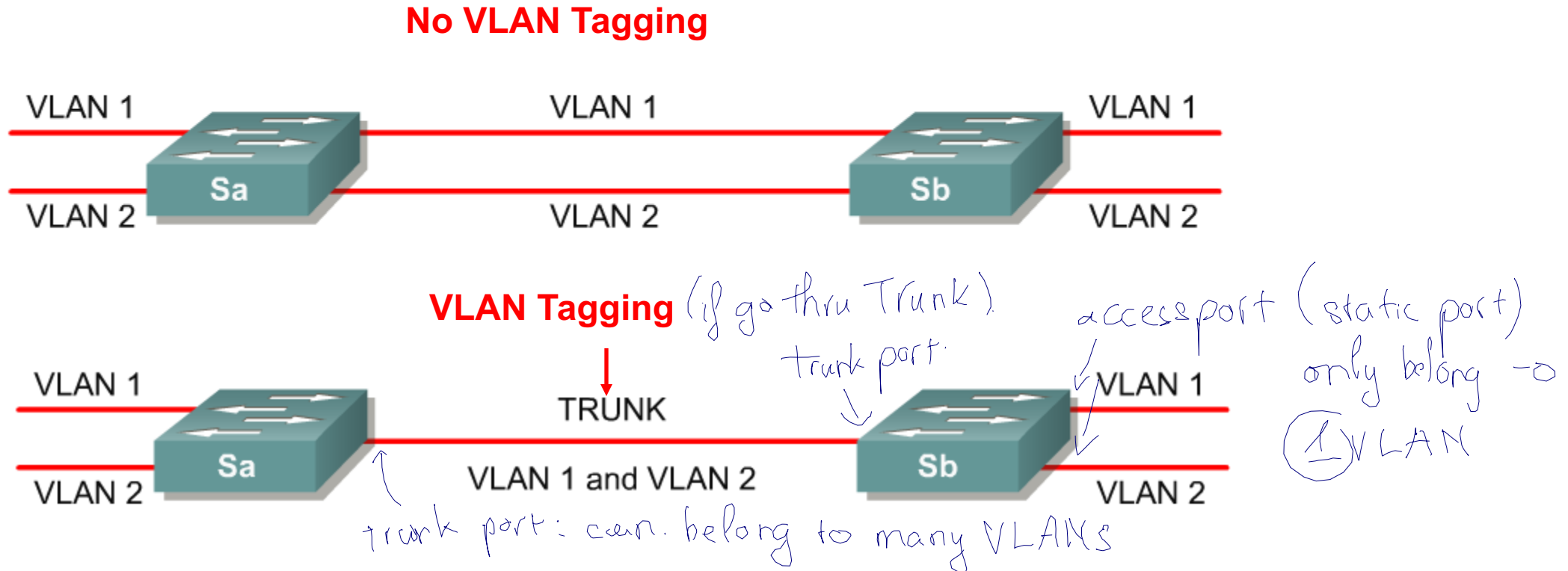
# VLAN Tagging

on the recipient if on the same port receives data from multiple VLANs it does not know which VLAN it comes from



- **VLAN Tagging is used when a link needs to carry traffic for more than one VLAN.**
  - This link As packets are received by the switch from any attached end-station device, a unique packet identifier is added within each header.
- This header information designates the VLAN membership of each packet.
- The packet is then forwarded to the appropriate switches or routers based on the VLAN identifier and MAC address.
- Upon reaching the destination node (Switch) the VLAN ID is removed from the packet by the adjacent switch and forwarded to the attached device.
- Packet tagging provides a mechanism for controlling the flow of broadcasts and applications while not interfering with the network and applications.
- This is known as a trunk link or VLAN trunking.

# VLAN Tagging



- VLAN Tagging is used when a link needs to carry traffic for more than one VLAN.
- Tagging is used so the receiving switch knows which ports it should flood broadcast and unknown unicast traffic (only those ports belonging to the same VLAN).

# A Closer look at VLAN Tagging

**ISL** *Cisco*

|            |           |           |            |            |              |            |            |              |            |            |   |              |
|------------|-----------|-----------|------------|------------|--------------|------------|------------|--------------|------------|------------|---|--------------|
| 40<br>bits | 4<br>bits | 4<br>bits | 48<br>bits | 16<br>bits | 24<br>bits   | 24<br>bits | 15<br>bits | 1<br>bits    | 16<br>bits | 16<br>bits | <b>Ethernet Frame</b><br>1500 bytes plus 18 byte header<br>(1518 bytes) | 32<br>bits   |
| DA         | TYPE      | USER      | SA         | LEN        | SNAP/<br>LLC | HSA        | VLAN<br>ID | BPDU/<br>CDP | INDX       | Reserved   |   | FCS<br>(CRC) |

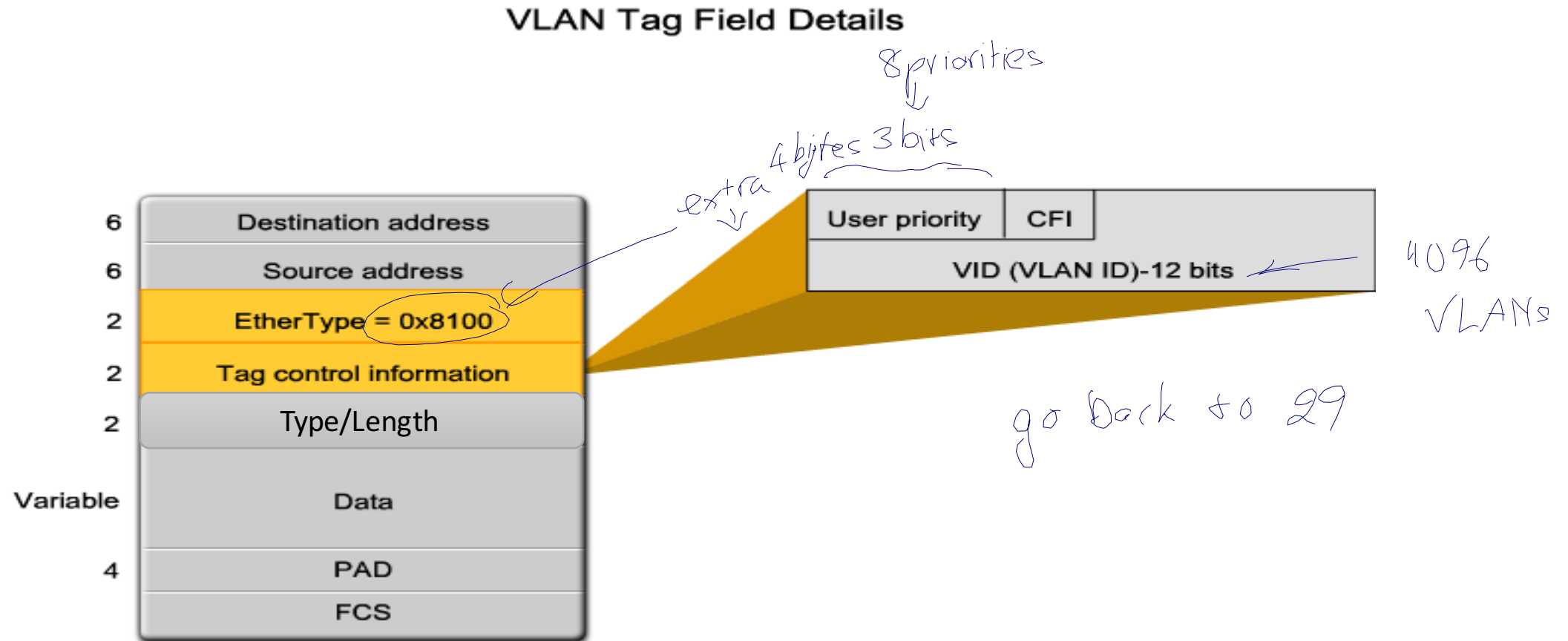
**IEEE 802.1Q** *std*

*only purpose: tells which VLAN it comes from*

|                   |                       |                      |                          |                    |
|-------------------|-----------------------|----------------------|--------------------------|--------------------|
| SA and DA<br>MACs | <b>802.1q<br/>Tag</b> | Type/Length<br>Field | Data (max 1500<br>bytes) | <b>New<br/>CRC</b> |
|-------------------|-----------------------|----------------------|--------------------------|--------------------|

- There are two types of VLAN Tagging:
  - ISL (Inter-Switch Link) – Cisco Proprietary
  - IEEE 802.1Q
- 802.1Q is recommended by Cisco and is used with multi-vendor switches.

# VLAN Trunk - 802.1Q Frame tagging (3)



# VLAN Trunk - 802.1Q Frame tagging (1)

- The VLAN tag field consists of an EtherType field, a tag control information field, and the FCS field.
- EtherType field
  - Set to the hexadecimal value of 0x8100.
  - This value is called the tag protocol ID (TPID) value.
  - With the EtherType field set to the TPID value, the switch receiving the frame knows to look for information in the tag control information field.

indication of VLAN + tag



# VLAN Trunk - 802.1Q Frame tagging (2)

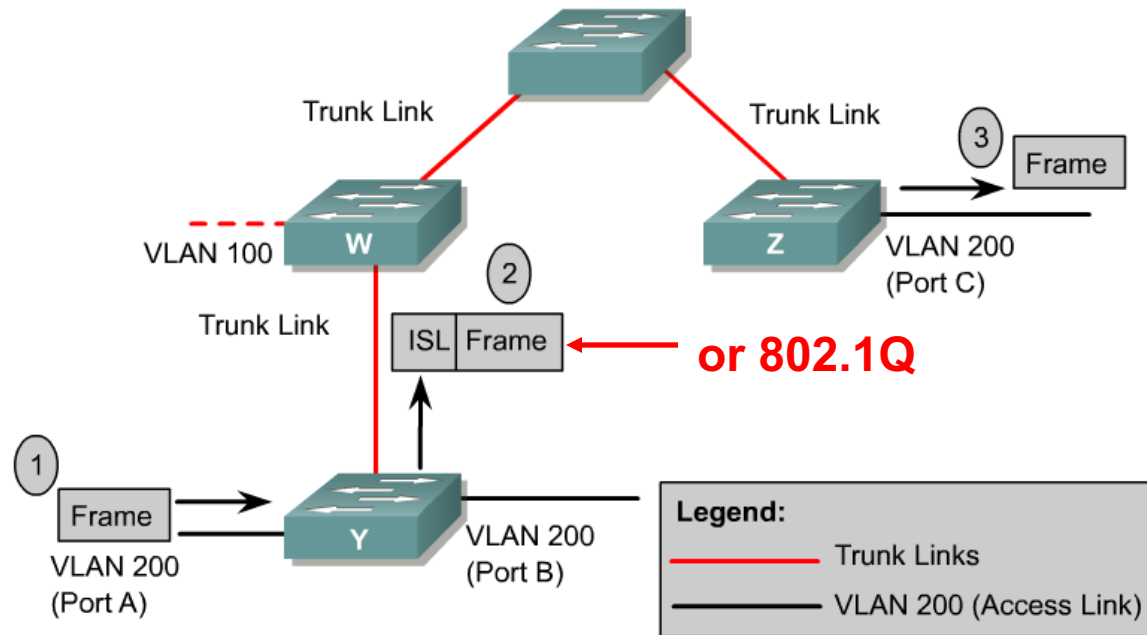
- Tag control information field

- 3 bits of user priority - Used by the 802.1p standard, which specifies how to provide expedited transmission of Layer 2 frames.
- 1 bit of Canonical Format Identifier (CFI) - Enables Token Ring frames to be carried across Ethernet links easily.
- 12 bits of VLAN ID (VID) - VLAN identification numbers; supports up to 4096 VLAN IDs.

- FCS field

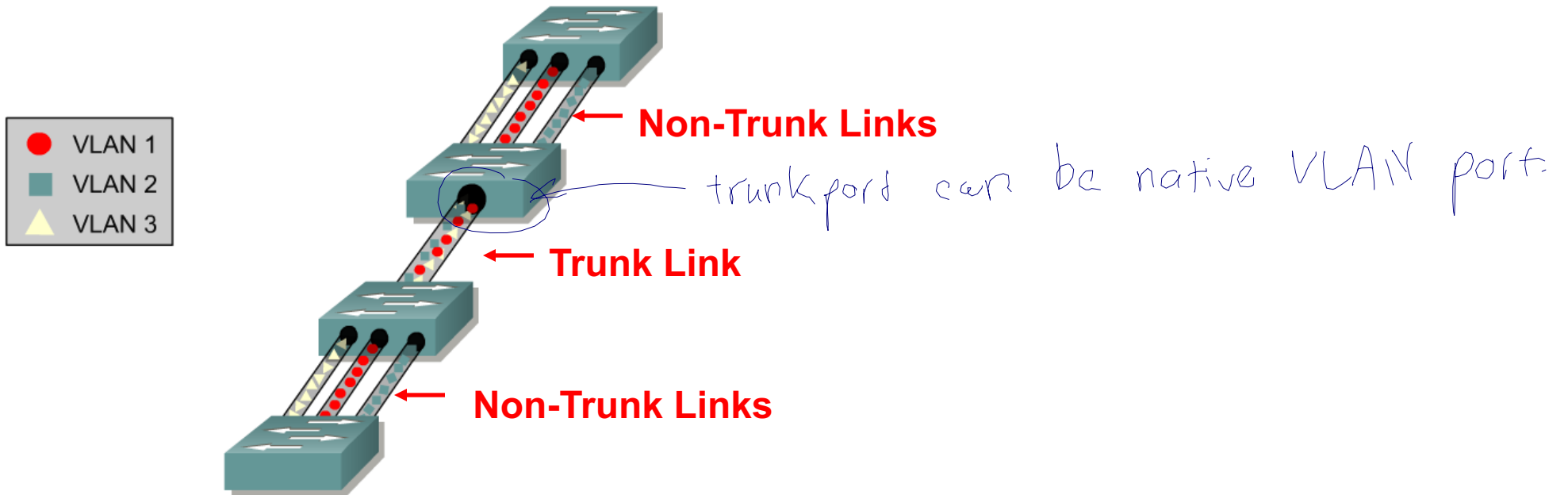
- After the switch inserts the EtherType and tag control information fields, it recalculates the FCS values and inserts it into the frame.

# Trunking operation



- Trunking protocols were developed to effectively manage the transfer of frames from different VLANs on a single physical line.
- The trunking protocols establish agreement for the distribution of frames to the associated ports at both ends of the trunk.
- Trunk links may carry traffic for all VLANs or only specific VLANs.

# VLANs and trunking



- It is important to understand that a **trunk link does not belong to a specific VLAN.**
- The responsibility of a trunk link is to act as a conduit for VLANs between switches and routers (or switches and switches).

# VLAN Trunk – Native VLAN (1)

finish

- Tagged Frames on the Native VLAN
- Control traffic sent on the native VLAN should be **untagged**.
- If an 802.1Q trunk port receives a tagged frame on the native VLAN, it **drops** the frame.
  - Consequently, when configuring a switch port on a Cisco switch, you need to identify these devices and configure them so that they do not send tagged frames on the native VLAN.

# VLAN Trunk –Native VLAN (2)

- **Untagged Frames on the Native VLAN**
- When a Cisco switch trunk port receives untagged frames it forwards those frames to the native VLAN.
- The default native VLAN is VLAN 1.
- When you configure an 802.1Q trunk port, a default Port VLAN ID (PVID) is assigned the value of the native VLAN ID.
- All untagged traffic coming in or out of the 802.1Q port is forwarded based on the PVID value.
  - For example, if VLAN 99 is configured as the native VLAN, the PVID is 99 and all untagged traffic is forward to VLAN 99.
  - If the native VLAN has not been reconfigured, the PVID value is set to VLAN 1.

# Benefits of VLANs

# Benefits of VLAN (1)

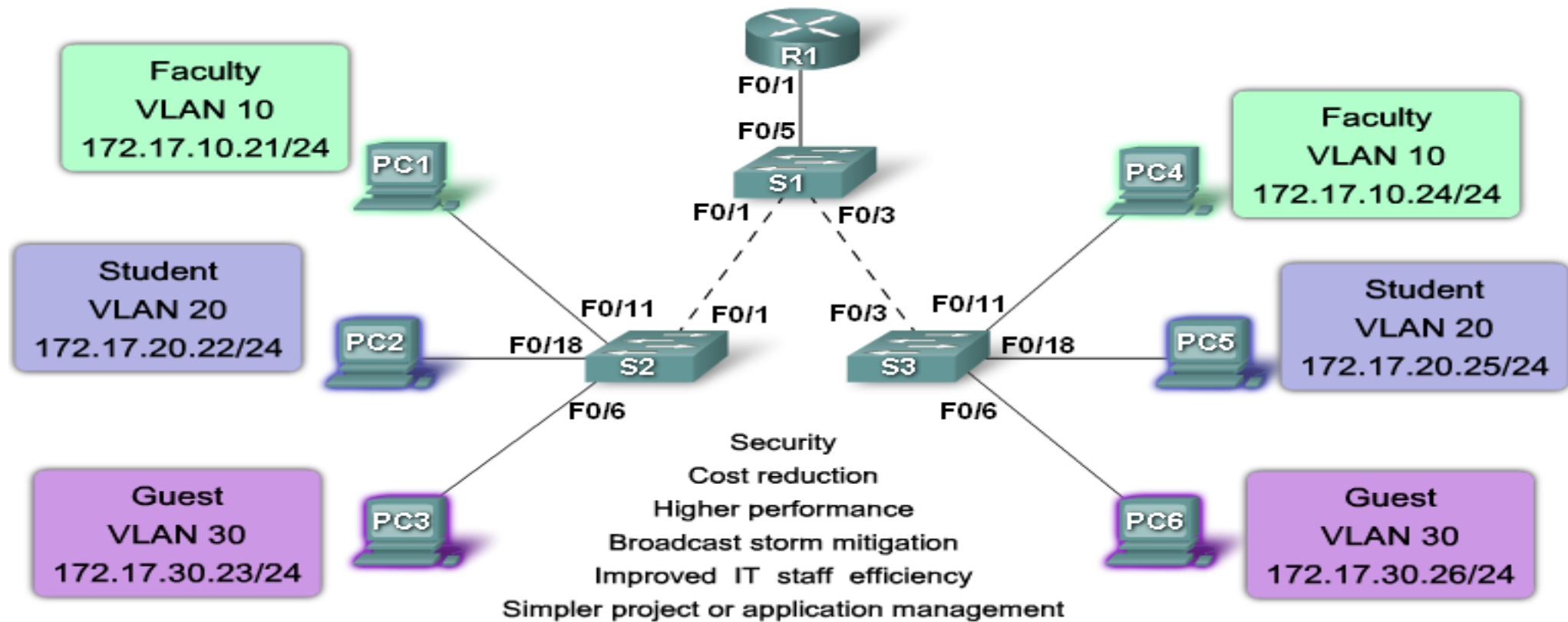
- **Security** - Groups that have sensitive data are separated from the rest of the network, decreasing the chances of confidential information breaches.
  - Faculty computers are on VLAN 10 and completely separated from student and guest data traffic.
- **Cost reduction** - Cost savings result from less need for expensive network upgrades and more efficient use of existing bandwidth and uplinks.

# Benefits of VLAN (2)

- **Higher performance** - Dividing flat Layer 2 networks into multiple logical workgroups (broadcast domains) **reduces unnecessary traffic on the network and boosts performance.**
- **Broadcast storm mitigation** - Dividing a network into VLANs reduces the number of devices that may participate in a broadcast storm.
  - In the figure you can see that although there are six computers on this network, there are only three broadcast domains: Faculty, Student, and Guest.



# Benefits of VLAN (3)



# Benefits of VLAN (4)

- **Improved IT staff efficiency** - VLANs make it easier to manage the network because users with similar network requirements share the same VLAN.
  - When you provision a new switch, all the policies and procedures already configured for the particular VLAN are implemented when the ports are assigned.
  - It is also easy for the IT staff to identify the function of a VLAN by giving it an appropriate name.
  - In the figure, for easy identification VLAN 20 could be named "Student", VLAN 10 could be named "Faculty", and VLAN 30 "Guest."

# Benefits of VLAN (5)

- **Simpler project or application management** - VLANs aggregate users and network devices to support business or geographic requirements.
  - Having separate functions makes managing a project or working with a specialized application easier, for example, an e-learning development platform for faculty.
  - It is also easier to determine the scope of the effects of upgrading network services.

# Benefits of VLAN (6)

- **Simpler project or application management** - VLANs aggregate users and network devices to support business or geographic requirements.
  - Having separate functions makes managing a project or working with a specialized application easier, for example, an e-learning development platform for faculty.
  - It is also easier to determine the scope of the effects of upgrading network services.