VLANS

Lecture 3

SWITCHING BASICS

Mark Cummins – Institute of Technology Blanchardstown

LECTURE OVERVIEW

In this lecture:

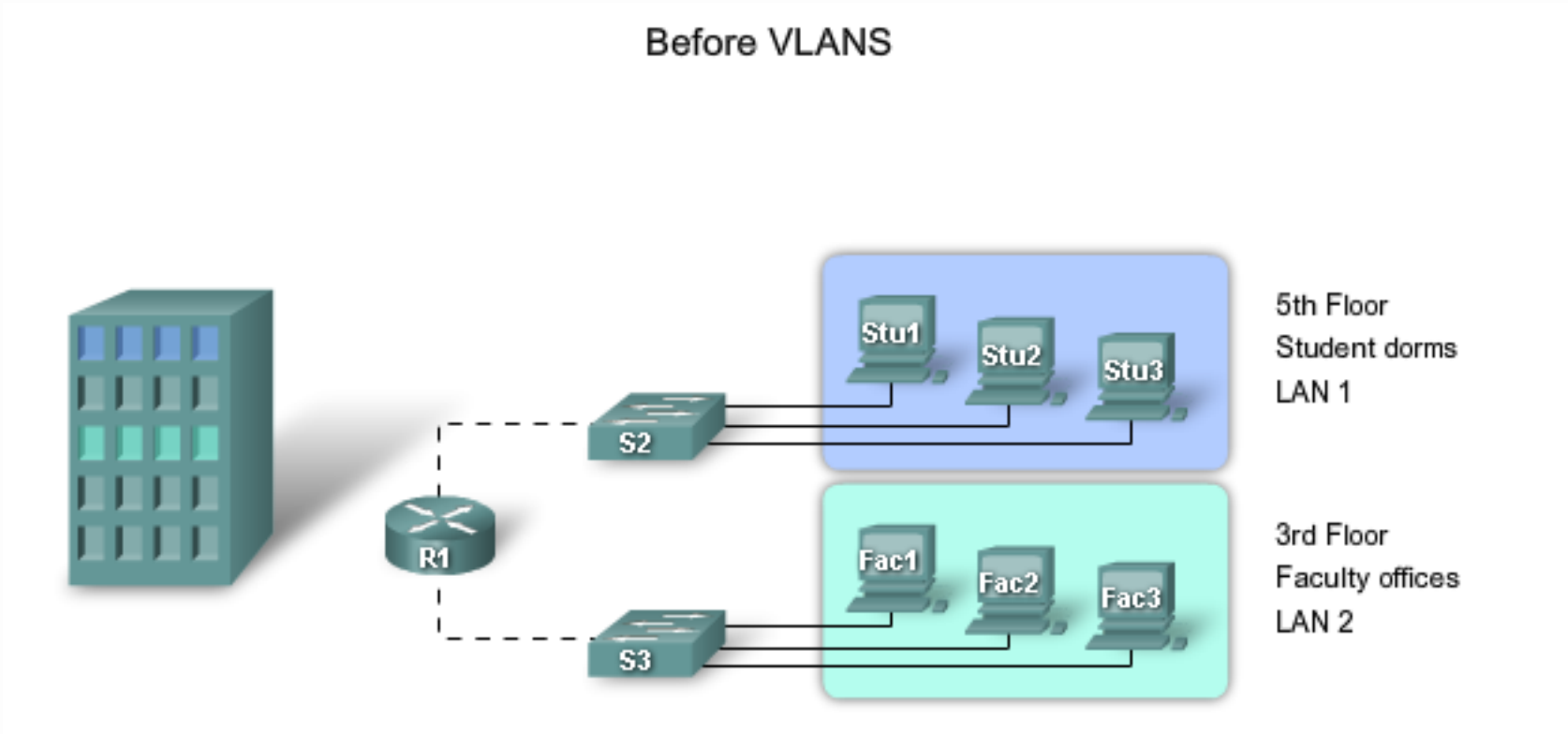
- Explain the role of VLANs in a network.
- Explain the role of trunking VLANs.
- Configure VLANs on the switches.
- Troubleshoot the common software or hardware configuration problems associated with VLANs on.

WHY USE VLANS?

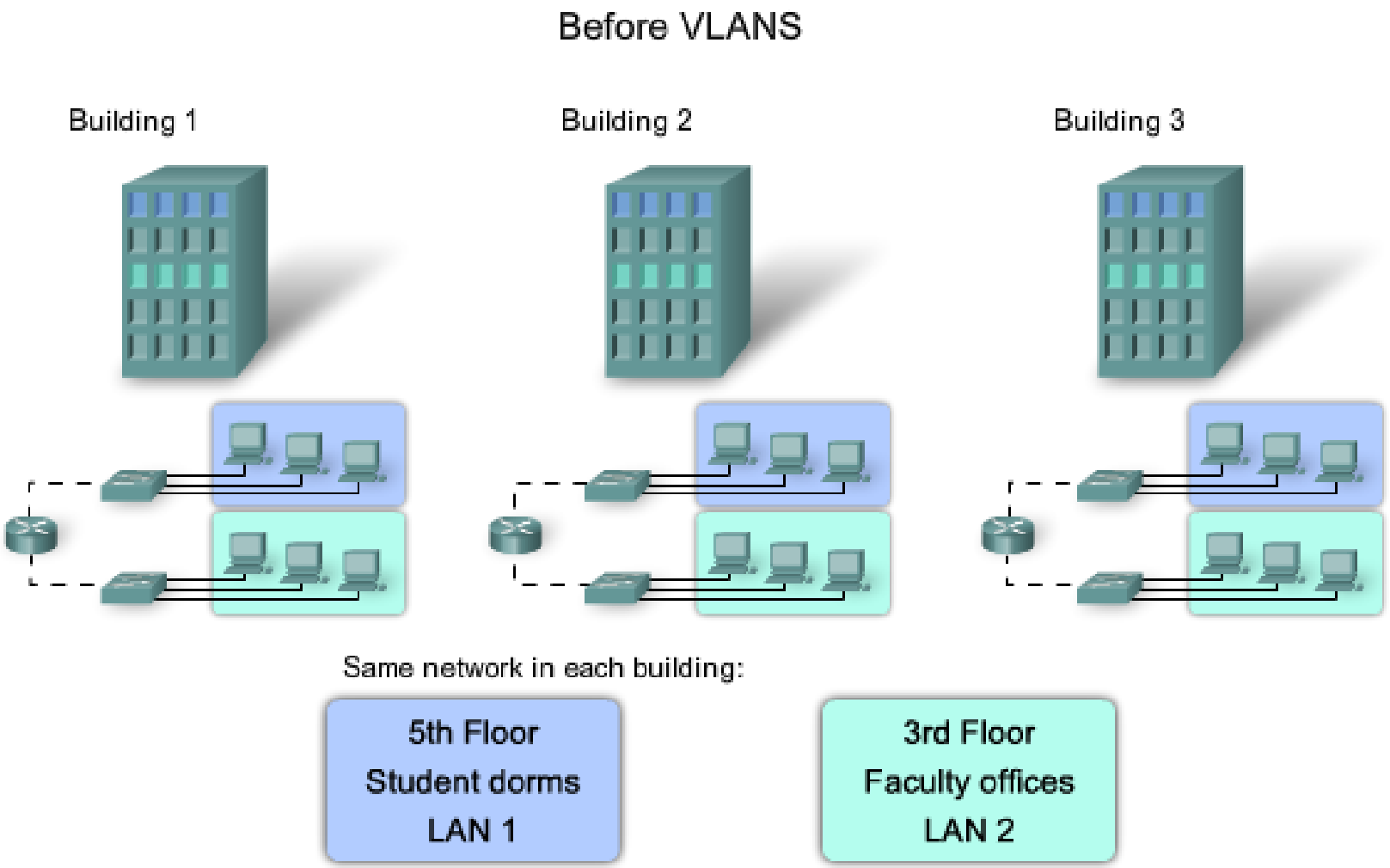
- Network performance can be improved by the separation of large broadcast domains into smaller ones with VLANs.

- Smaller broadcast domains limit the number of devices participating in broadcasts and allow devices to be separated into functional groupings.

BEFORE VLANS



BEFORE VLANS



BEFORE VLANS

- How can the network accommodate the shared needs of the geographically separated departments?
- Do you create a large LAN and wire each department together?

BEFORE VLANS

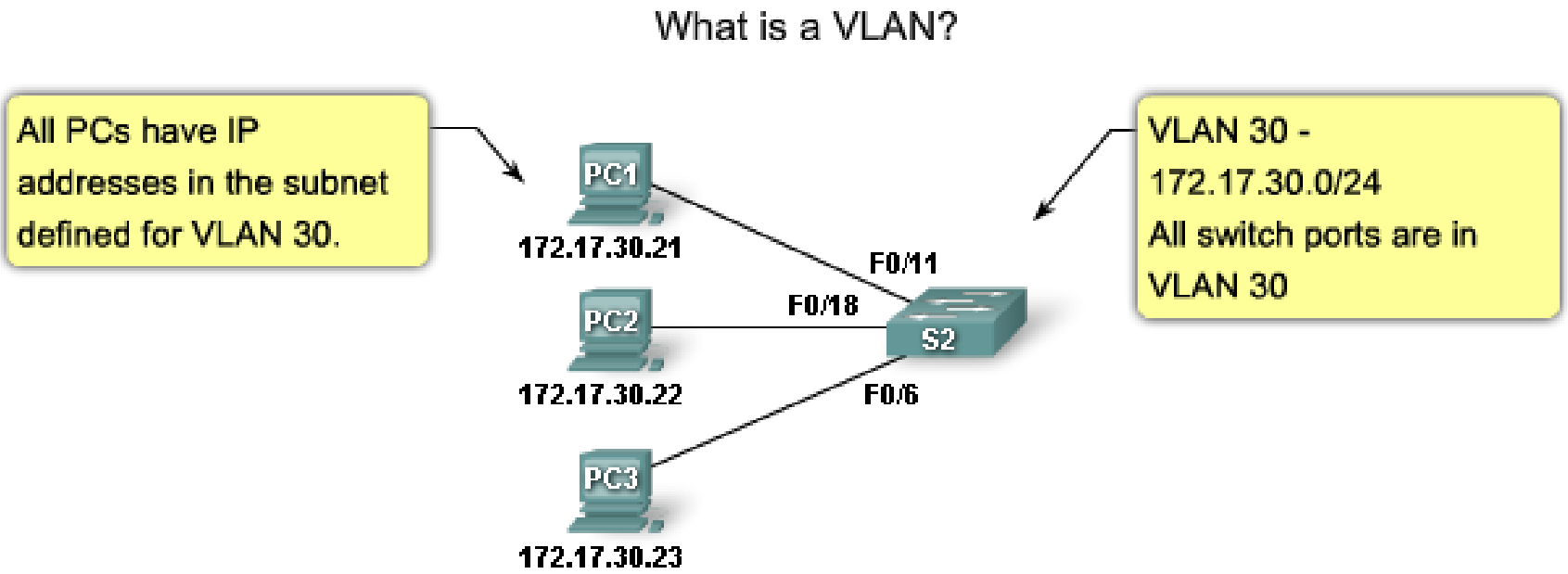
- How easy would it be to make changes to that network?

- It would be great to group the people with the resources they use regardless of their geographic location, and it would make it easier to manage their specific security and bandwidth needs.

THE SOLUTION

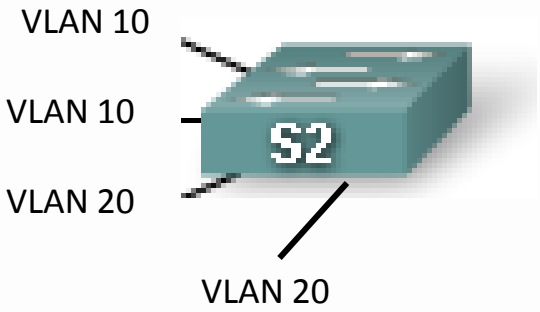
- The solution is to use a networking technology called a virtual LAN (VLAN).
- A VLAN allows a network administrator to create groups of logically networked devices that act as if they are on their own independent network.
- When you configure a VLAN, you can name it to describe the primary role of the users for that VLAN.

WHAT IS A VLAN?

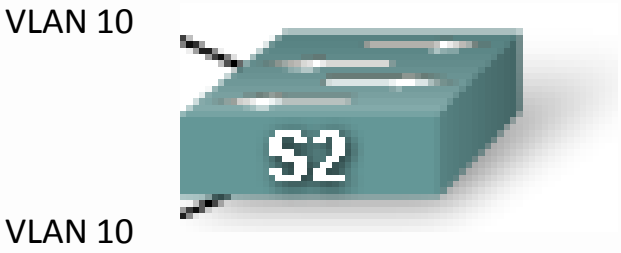


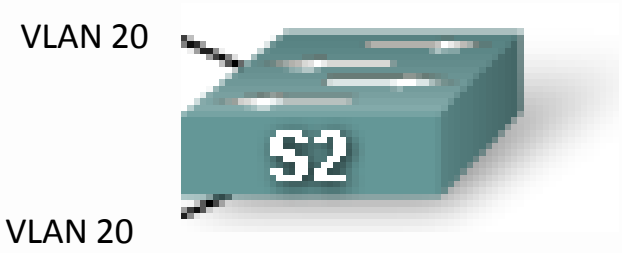
- A VLAN = Subnet (in modern switched LANs)
- On the switch
  - Configure the VLAN
  - Assign the port to the VLAN
- On the PC assign an IP address in the VLAN subnet

WHAT IS A VLAN?



When VLANs are created on a switch, they each act independently of each other. As if each VLAN was a separate Switch . Each with its own MAC Address Table





THE BENEFITS

The primary benefits of using VLANs are as follows:

- Security
- Cost reduction
- Higher performance
- Broadcast storm mitigation
- Improved IT staff efficiency
- Simpler project management

VLAN CHARACTERISTICS

- VLAN ID
  - Normal-range IDs
    - 1 – 1005
    - 1002 -1005 reserved for Token Ring and FDDI VLANs
    - 1 and 1002 to 1005 are automatically created and cannot be removed
    - Stored in the vlan.dat file in flash memory
  - Extended-range IDs
    - 1006 – 4094
    - Designed for service providers
    - Have fewer options than normal range VLANs
    - Stored in the running configuration file
- A Cisco Catalyst 2960 switch supports 255 normal and extended range VLANs

TYPES OF VLAN

There are different types of VLAN:

- Data:

Carries user generated data

- Voice:

Voice-based traffic

- Management:

Traffic used to manage the switch

DEFAULT VLAN

- All switch ports become a member of the default VLAN after the initial boot up of the switch.
- The default VLAN for Cisco switches is VLAN 1.
- VLAN 1 has all the features of any VLAN, except that you cannot rename it and you can not delete it.

DEFAULT VLAN

- By default, Layer 2 control traffic, such as CDP and spanning tree protocol traffic, are associated with VLAN 1.

- It is a security best practice to change the default VLAN to a VLAN other than VLAN 1.

NATIVE VLAN

- A native VLAN is assigned to an 802.1Q trunk port.
- The 802.1Q trunk port places untagged traffic on the native VLAN.
- Untagged traffic is generated by a computer attached to a switch port that is configured with the native VLAN.
- It is a best practice to use a VLAN other than VLAN 1 as the native VLAN.

MANAGEMENT VLAN

- A management VLAN is any VLAN you configure to access the management capabilities of a switch.
- VLAN 1 is the default management VLAN.
- You assign the management VLAN an IP address and subnet mask.
- A switch can be managed via HTTP, Telnet, SSH, or SNMP.

SUMMARY OF VLAN TYPES

- Data
- Voice
- Management
- Default
- Native

SUMMARY OF CHANGES TO DEFAULTS

- All Ports are members of default VLAN
  - Create a new default VLAN
  - Assign all ports to new default VLAN
  - Disable all Ports
  - Don't use this VLAN.
  - Assign Ports from this pool to other VLAN as we need them.

SUMMARY OF CHANGES TO DEFAULTS

- VLAN 1 is the default VLAN
  - Create a new default VLAN
  - VLAN 1 will still exist (we can't delete it)
  - VLAN 1 is used for some background processes (STP, CDP etc.)
- VLAN 1 is also the default Management VLAN
  - Create a new Management VLAN
  - Shutdown the default Interface VLAN 1

SWITCHPORT MEMBERSHIP MODES

- Static VLAN: Each switch port is associated with one or more VLANs

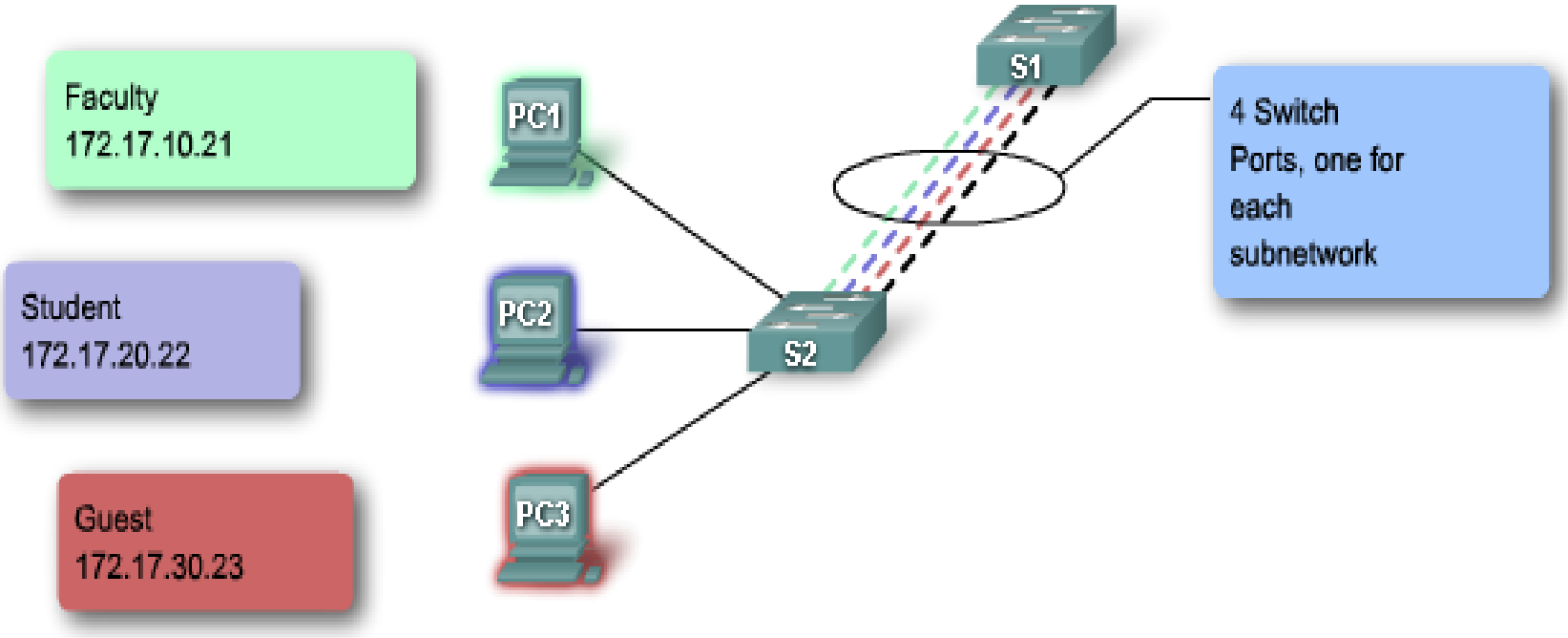
- Dynamic VLAN: you assign switch ports to VLANs dynamically, based on the source MAC address of the device connected to the port. We use a special server called a VLAN Membership Policy Server (VMPS) to do this.

VLAN TRUNKS

- A trunk is a point-to-point link between two network devices that carries more than one VLAN.
- A VLAN trunk allows you to extend the VLANs across an entire network.
- A VLAN trunk does not belong to a specific VLAN, rather it is a conduit for VLANs between switches and routers.

VLAN TRUNKS

Faculty - 172.17.10.0/24
Students - 172.17.20.0/24
Guest - 172.17.30.0/24
Management and Native - 172.17.99.0/24



VLAN TAGGING

- Switches are Layer 2 devices. They only use the frame header info to forward packets.

- The frame header does not contain information about which VLAN the frame should belong to.

VLAN TAGGING

- Subsequently, when Ethernet frames are placed on a trunk they need additional information about the VLANs they belong to.

- This is accomplished by using the 802.1Q encapsulation header. This header adds a tag to the original Ethernet frame specifying the VLAN to which the frame belongs.