SLIIT

Discover Your Future

IT2050 – Computer Networks

Lecture 7

Virtual Local Area Networks (VLAN)

SLIIT FACULTY OF COMPUTING

Sections & Objectives

VLAN Segmentation

- Explain the purpose of VLANs in a switched network.
- Explain how a switch forwards frames based on VLAN configuration in a multi-switch environment.

VLAN Implementations

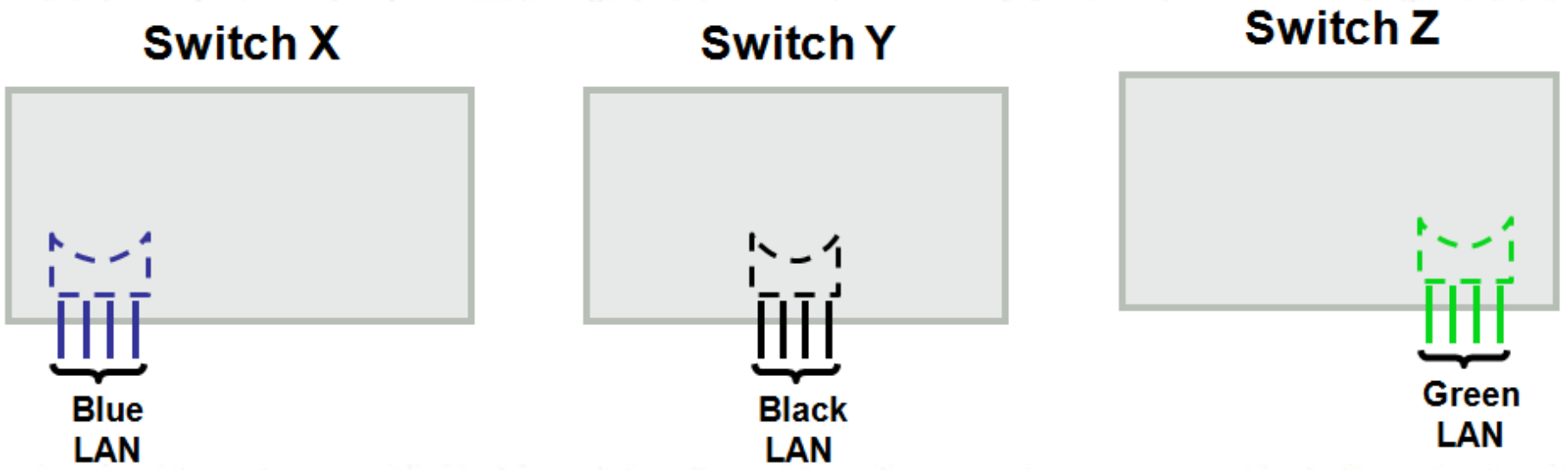
- Configure a switch port to be assigned to a VLAN based on requirements.
- Configure a trunk port on a LAN switch.
- Troubleshoot VLAN and trunk configurations in a switched network.

Inter-VLAN Routing Using Routers

- Describe the two options for configuring Inter-VLAN routing.
- Configure Router-on-a-Stick Inter-VLAN Routing

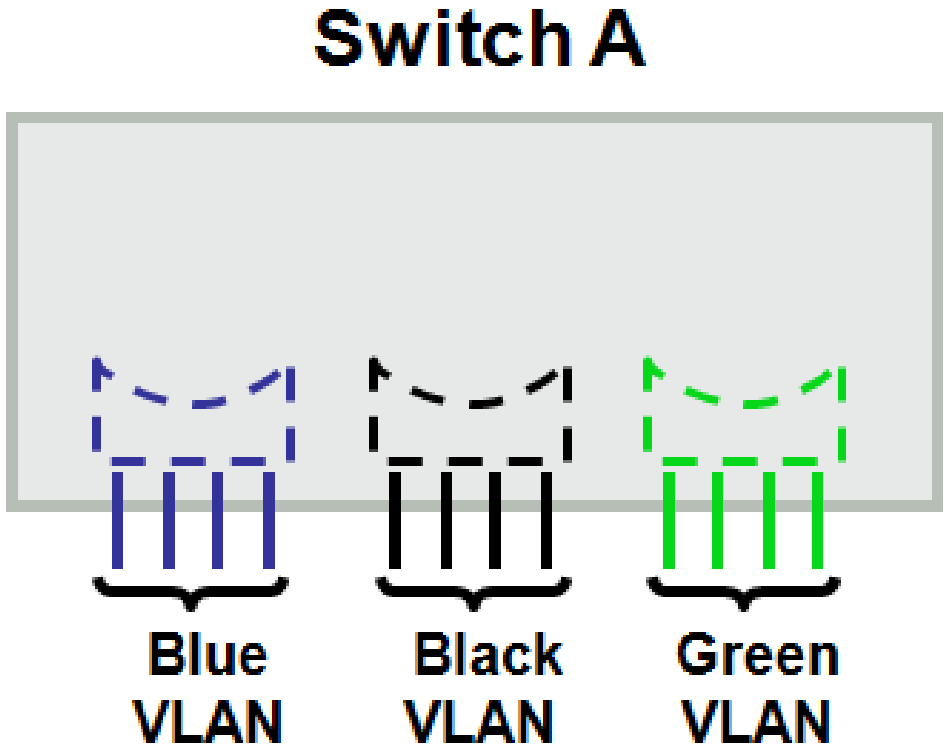
VLAN Segmentation

Broadcast Domains



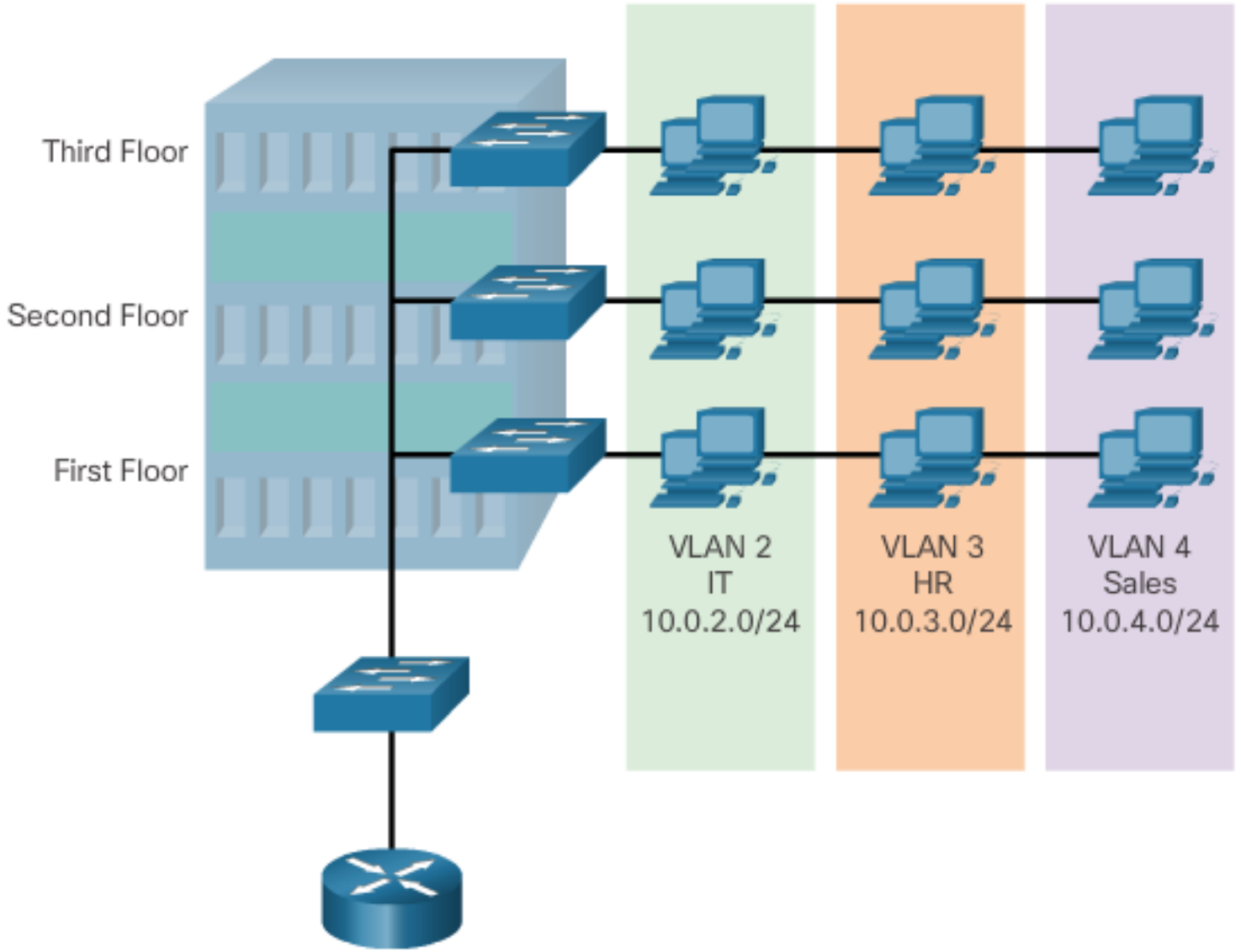
- Three separate broadcast domains
- Requires three switches

VLAN cont.



- Each logical VLAN is like a separate physical switch
  - Each VLAN is a separate broadcast domain (3 broadcast domains)
  - Each VLAN contains a separate MAC address table
  - Computer in Blue VLAN will not be able to send a frame to Black VLAN or Green VLAN

Defining VLAN Groups



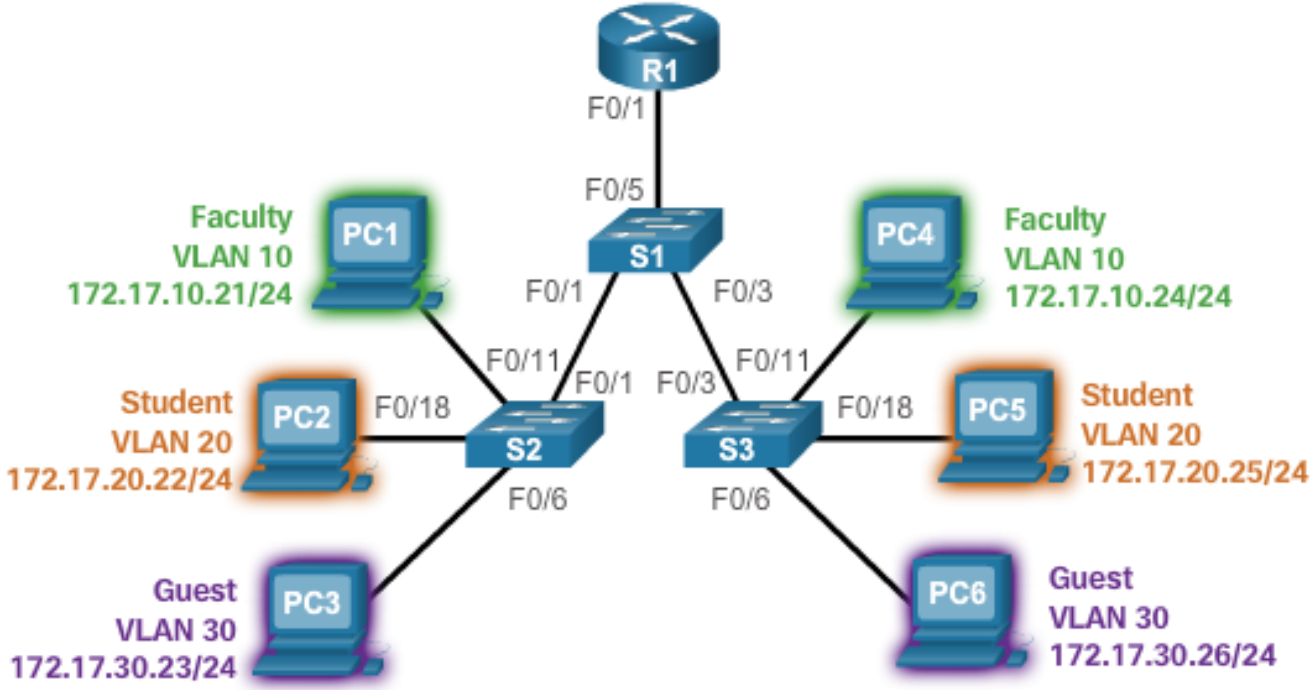
VLAN Definitions (cont.)

- **VLANs allow an administrator to segment networks based on factors such as function, project team, or application, without regard for the physical location of the user or device.**
- **VLANs enable the implementation of access and security policies according to specific groupings of users.**
- **A VLAN is a logical partition of a Layer 2 network.**
- **Multiple partitions can be created, allowing for multiple VLANs to co-exist.**

VLAN Definitions (cont.)

- **Each VLAN is a broadcast domain, usually with its own IP network.**
- **VLANs are mutually isolated, and packets can only pass between them via a router.**
- **The partitioning of the Layer 2 network takes place inside a Layer 2 device, usually via a switch.**
- **The hosts grouped within a VLAN are unaware of the VLAN's existence.**

Benefits of VLANs



- Improved Security
- Reduced Cost
- Better Performance
- Smaller Broadcast Domains
- IT Efficiency
- Management Efficiency
- Simpler Project and Application Management

Types of VLANs

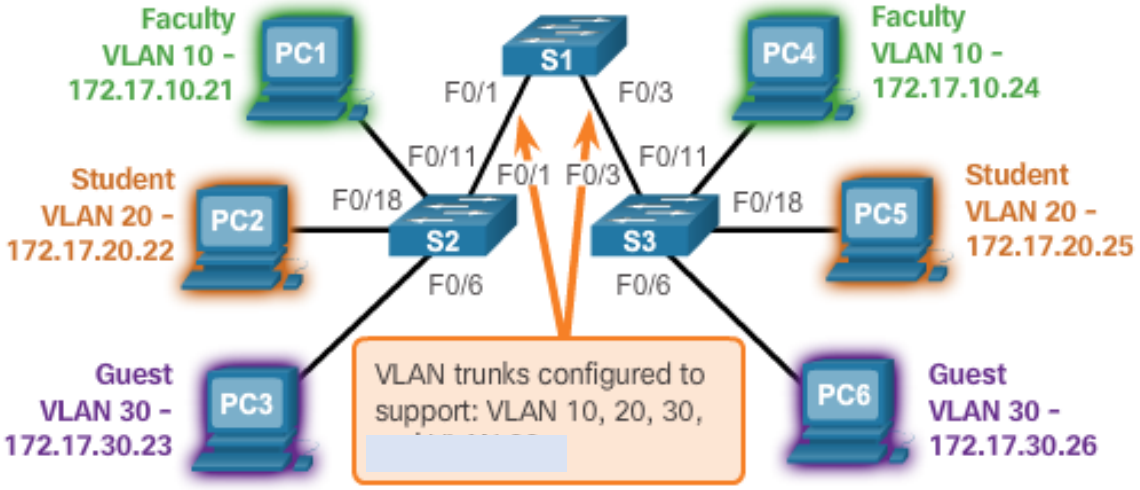
- **Data VLAN** – user generated traffic
- **Default VLAN** – all switch ports become part of this VLAN until switch is configured,
- **Management VLAN** – used to access management capabilities

VLAN Trunks

VLAN 10 Faculty/Staff - 172.17.10.0/24
VLAN 20 Students - 172.17.20.0/24
VLAN 30 Guest - 172.17.30.0/24

F0/1-5 are 802.1Q trunk interfaces

F0/11-17 are in VLAN 10.
F0/18-24 are in VLAN 20.
F0/6-10 are in VLAN 30.

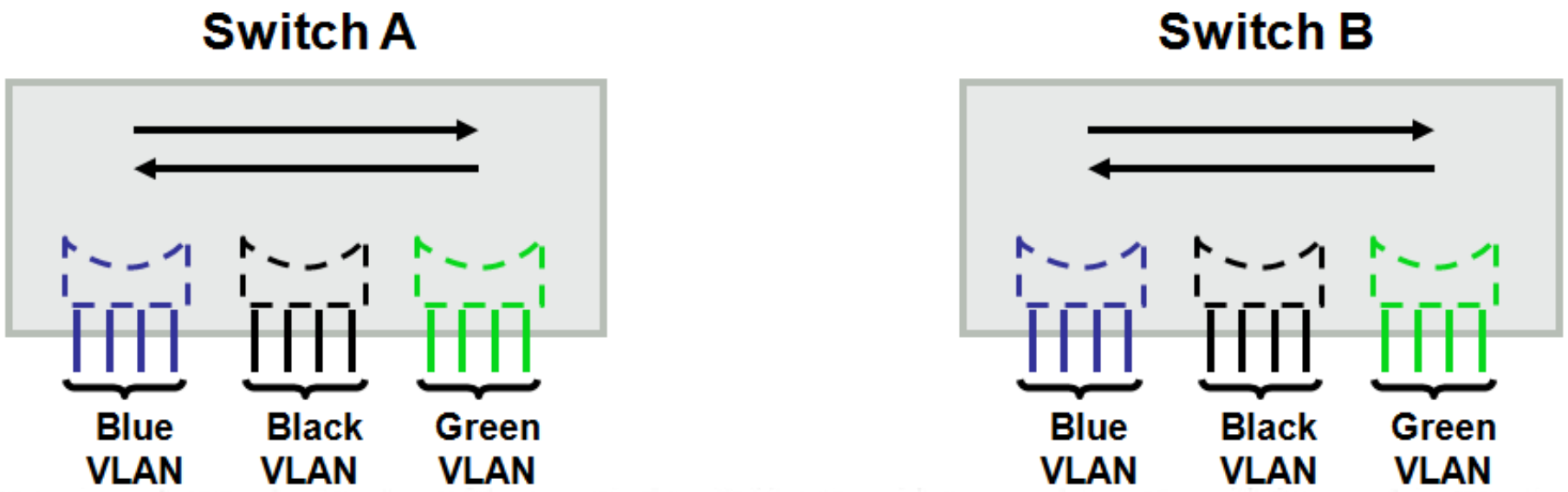


The links between switches S1 and S2, and S1 and S3 are configured to transmit traffic coming from VLANs 10, 20, 30 the network. This network could not function without VLAN trunks.

VLAN Trunks (cont.)

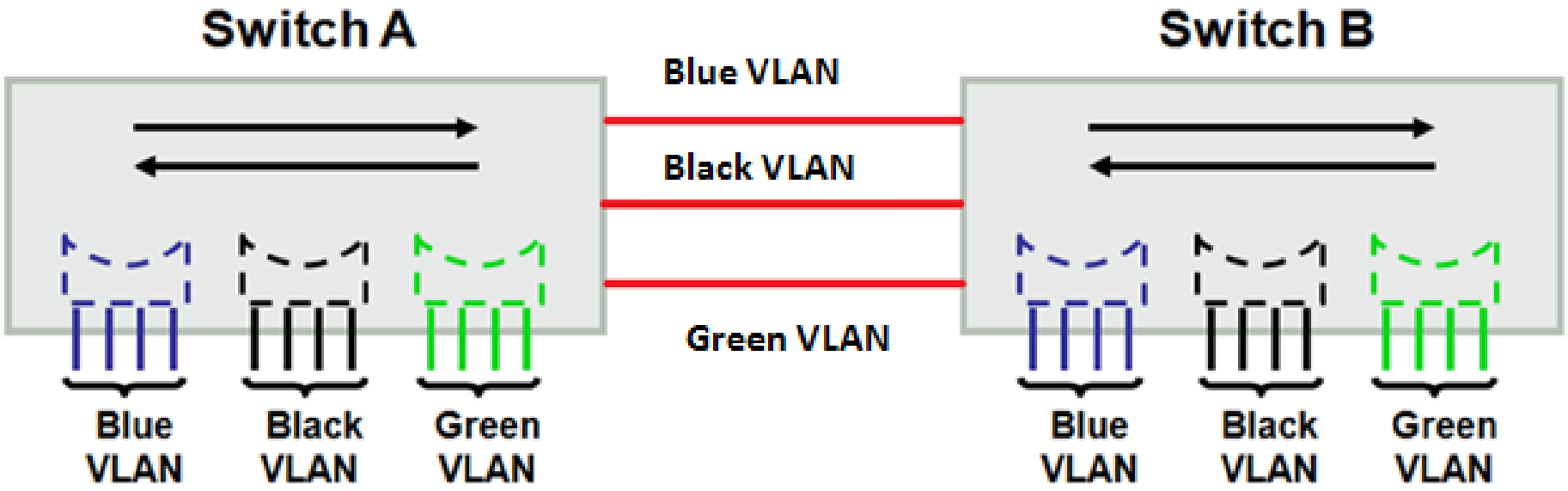
- A VLAN trunk is a point-to-point link that carries more than one VLAN.
- A VLAN trunk is usually established between switches so same-VLAN devices can communicate, even if physically connected to different switches.
- A VLAN trunk is not associated to any VLANs; neither is the trunk ports used to establish the trunk link.
- Cisco IOS supports IEEE802.1q, a popular VLAN trunk protocol.

VLAN cont.

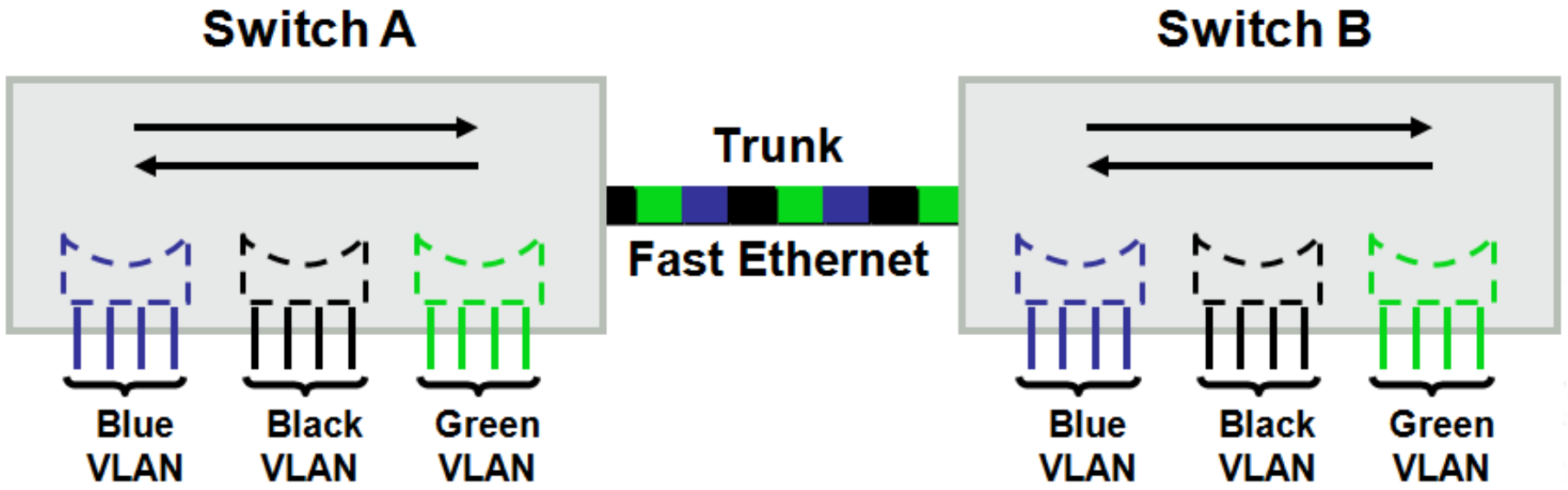


- VLANs can span across multiple switches

VLAN cont.

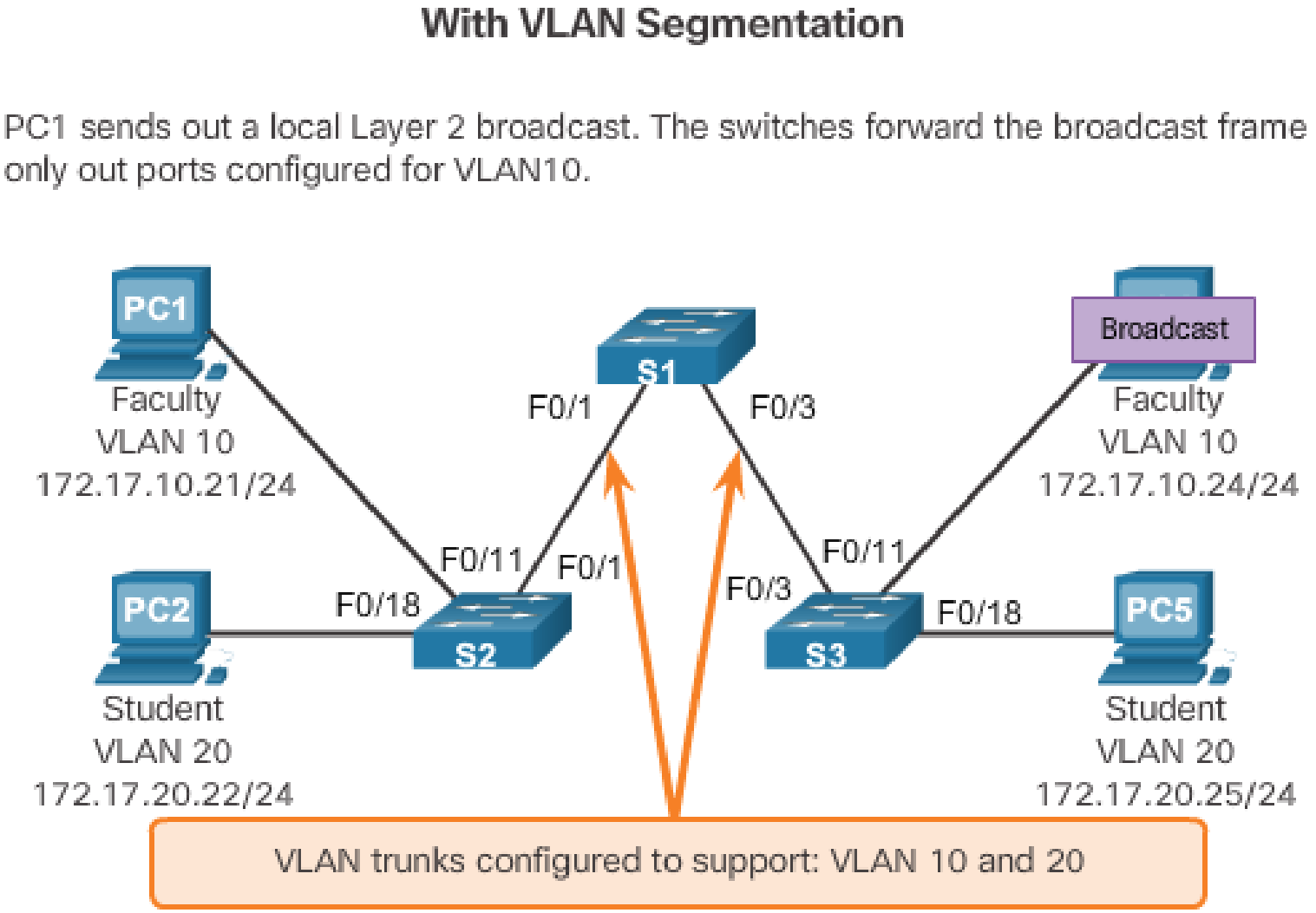

Switch A
Switch B
Blue VLAN
Black VLAN
Green VLAN
Blue VLAN
Black VLAN
Green VLAN
Blue VLAN
Black VLAN
Green VLAN

VLAN tagging for source identification



- The process of adding an additional header to a LAN frame
- Used to identify the VLAN to which the frame belongs
- Cisco refers to this as ***TRUNKING***
- Trunks carry traffic for multiple VLANs

Controlling Broadcast Domains with VLANs



Controlling Broadcast Domains with VLANs

- VLANs can be used to limit the reach of broadcast frames.
- A VLAN is a broadcast domain of its own.
- A broadcast frame sent by a device in a specific VLAN is forwarded within that VLAN only.
- VLANs help control the reach of broadcast frames and their impact in the network.
- Unicast and multicast frames are forwarded within the originating VLAN.

Tagging Ethernet Frames for VLAN Identification

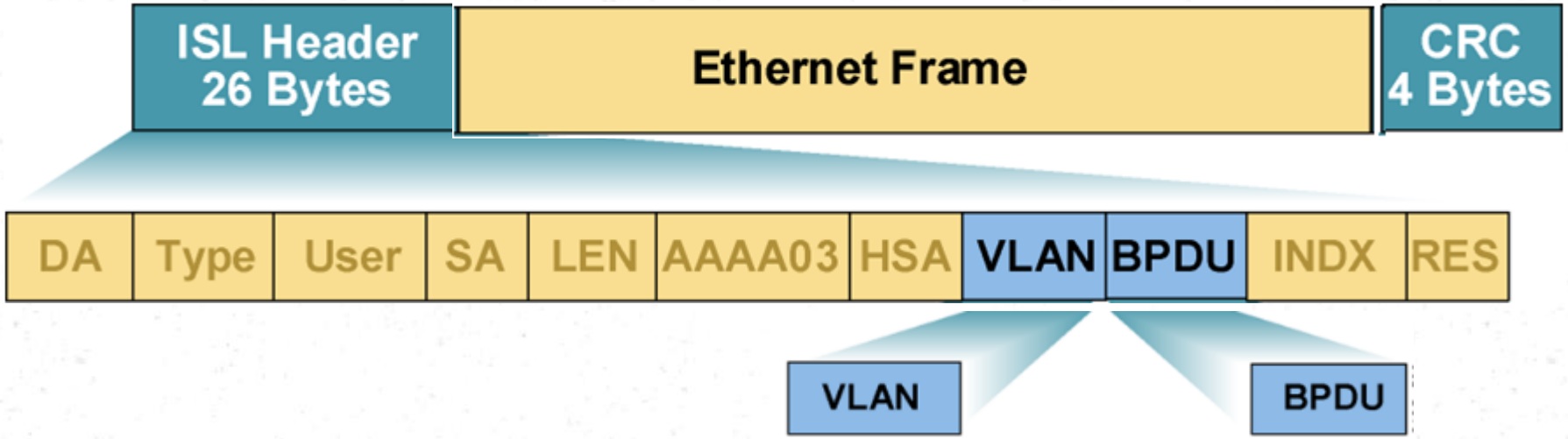
- Frame tagging is the process of adding a VLAN identification header to the frame.
- It is used to properly transmit multiple VLAN frames through a trunk link.
- Switches tag frames to identify the VLAN to which they belong.
- Different tagging protocols exist; ISL , IEEE 802.1Q.
- The protocol defines the structure of the tagging header added to the frame.
- Switches add VLAN tags to the frames before placing them into trunk links and remove the tags before forwarding frames through non-trunk ports.
- When properly tagged, the frames can transverse any number of switches via trunk links and still be forwarded within the correct VLAN at the destination.

Trunking

Tagging	Method	Media	Description
Inter-Switch Link (ISL)	Fast Ethernet	ISL header encapsulates the LAN frame and there is a VLAN ID field in the ISL header	Frame is lengthened.
802.IQ	Fast Ethernet	IEEE defined Ethernet VLAN protocol	Header is modified.

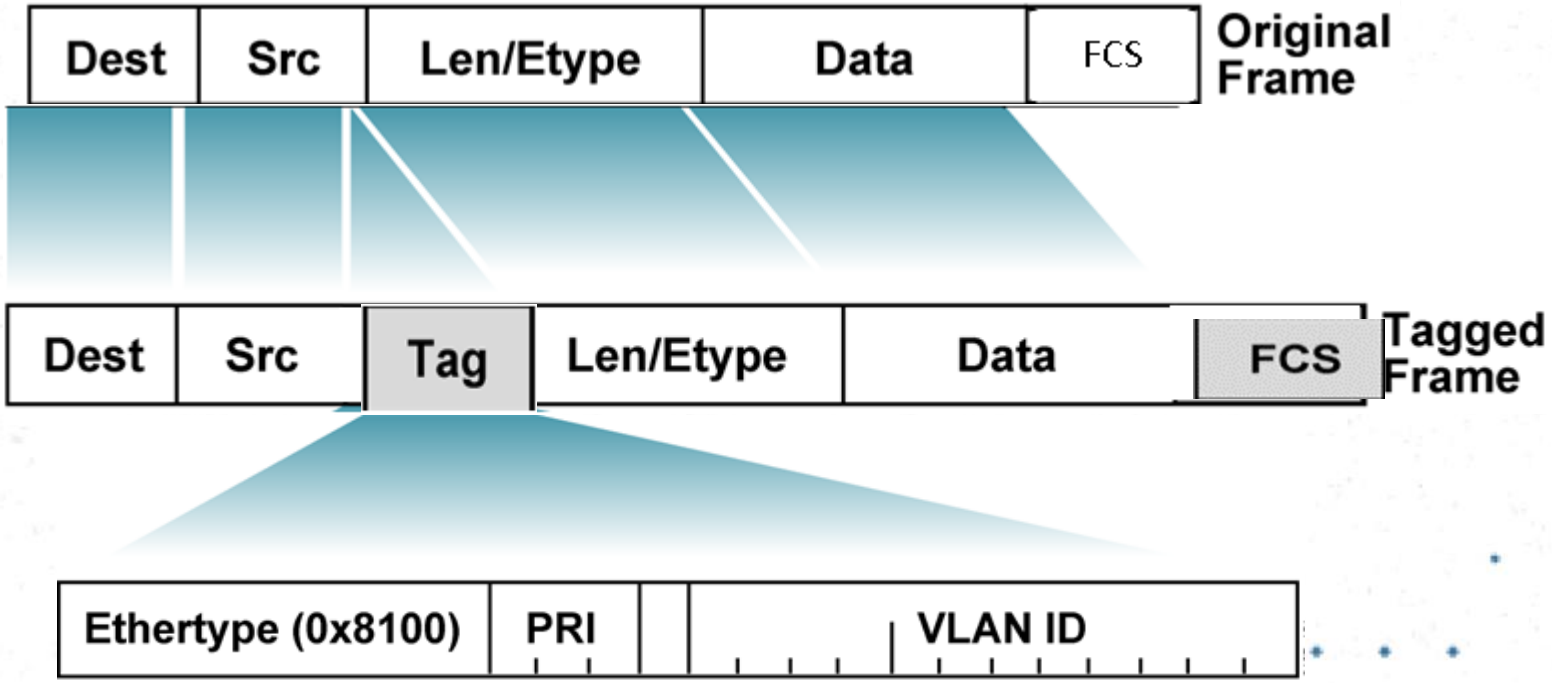
- There are two types of VLAN Trunking:
  - ISL (Inter-Switch Link) – Cisco Proprietary
  - IEEE 802.1Q

ISL (Inter-Switch Link)



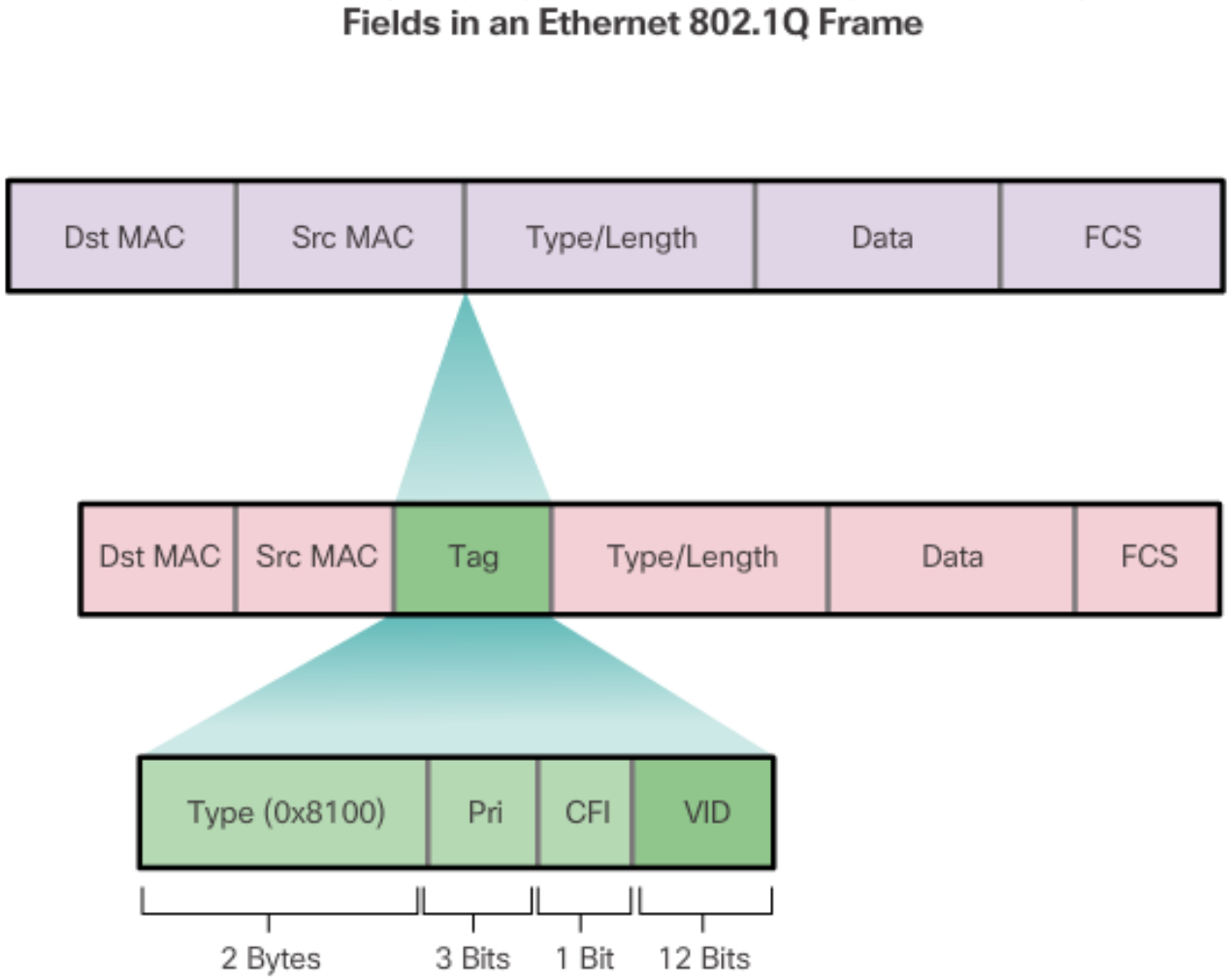
- Full Ethernet frame is encapsulated with a ISL
- Indicate the VLAN ID (12 bit) to identify the VLAN
- CISCO proprietary

IEEE 802.1Q



- The IEEE 802.1Q tag is inserted by the switch before sending the frame across the trunk
  - Indicate the VLAN ID (12 bit) to identify the VLAN

802.1Q Tagging



Configuring IEEE 802.1q Trunk Links

Trunk Configuration

```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)#
S1(config-if)# switchport trunk allowed vlan 10,20,30,99
S1(config-if)# end
```

Resetting the Trunk to Default State

Resetting Configured Values on Trunk Links

Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface interface_id`
Set trunk to allow all VLANs.	`S1(config-if)# no switchport trunk allowed vlan`
Reset native VLAN to default.	`S1(config-if)# no switchport trunk native vlan`
Return to the privileged EXEC mode.	`S1(config-if)# end`

Troubleshoot VLANs and Trunks

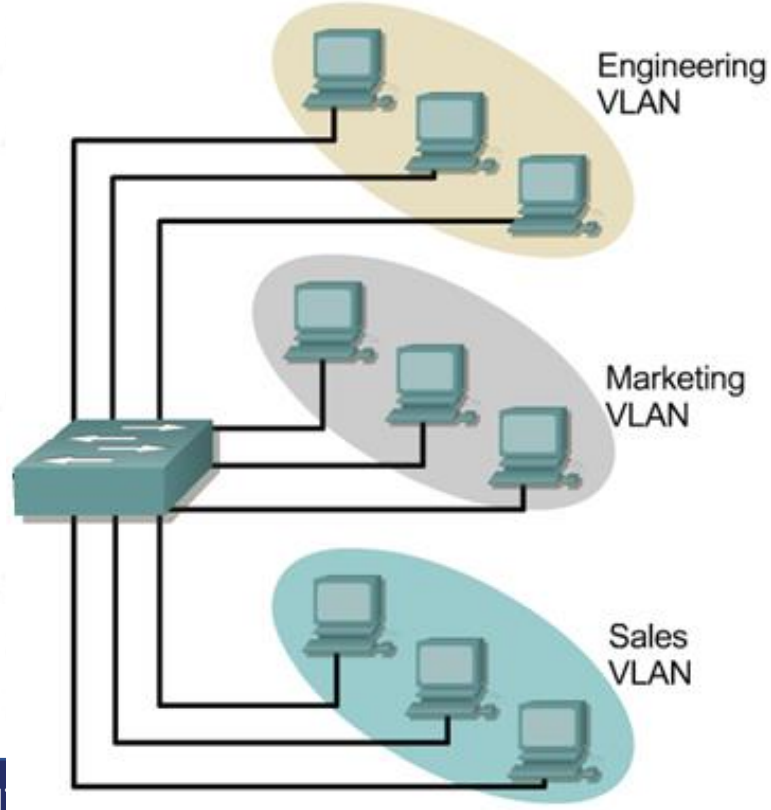
- VLANs must be allowed in the trunk before their frames can be transmitted across the link.
- Use the **switchport trunk allowed vlan** command to specify which VLANs are allowed in a trunk link.
- Use the **show interfaces trunk** command to ensure the correct VLANs are permitted in a trunk.

Inter-VLAN Routing Using Routers

Passing traffic between VLANs

- Each VLAN will have different IP subnets
- VLANs don’t send data frames to other VLAN

  (Separate MAC address table for each VLAN)



Inter-VLAN Routing

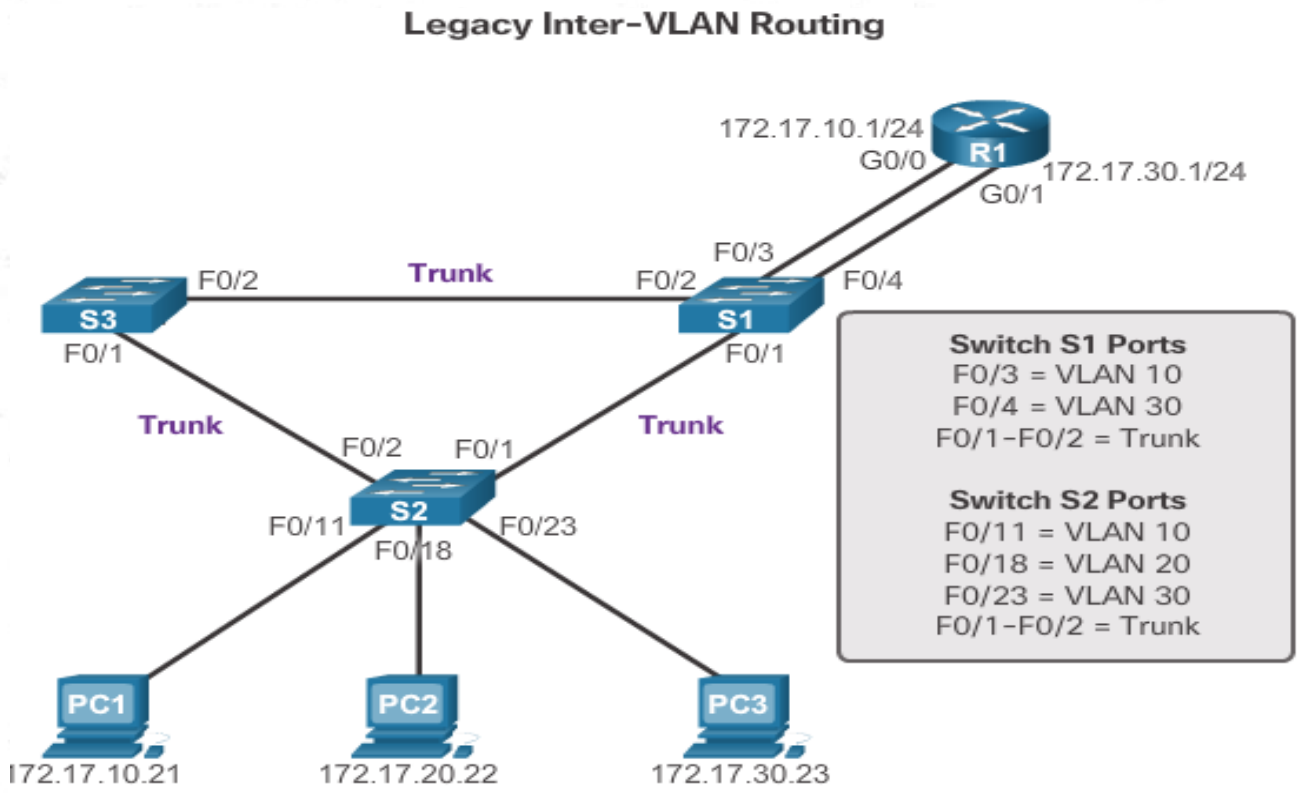
- **Layer 2 switches cannot forward traffic between VLANs without the assistance of a router.**
- **Inter-VLAN routing is a process for forwarding network traffic from one VLAN to another, using a router.**

Legacy Inter-VLAN Routing

In the past:

- Actual routers were used to route between VLANs.
- Each VLAN was connected to a different physical router interface.
- Packets would arrive on the router through one interface, be routed and leave through another.
- Because the router interfaces were connected to VLANs and had IP addresses from that specific VLAN, routing between VLANs was achieved.
- Large networks with large number of VLANs required many router interfaces.

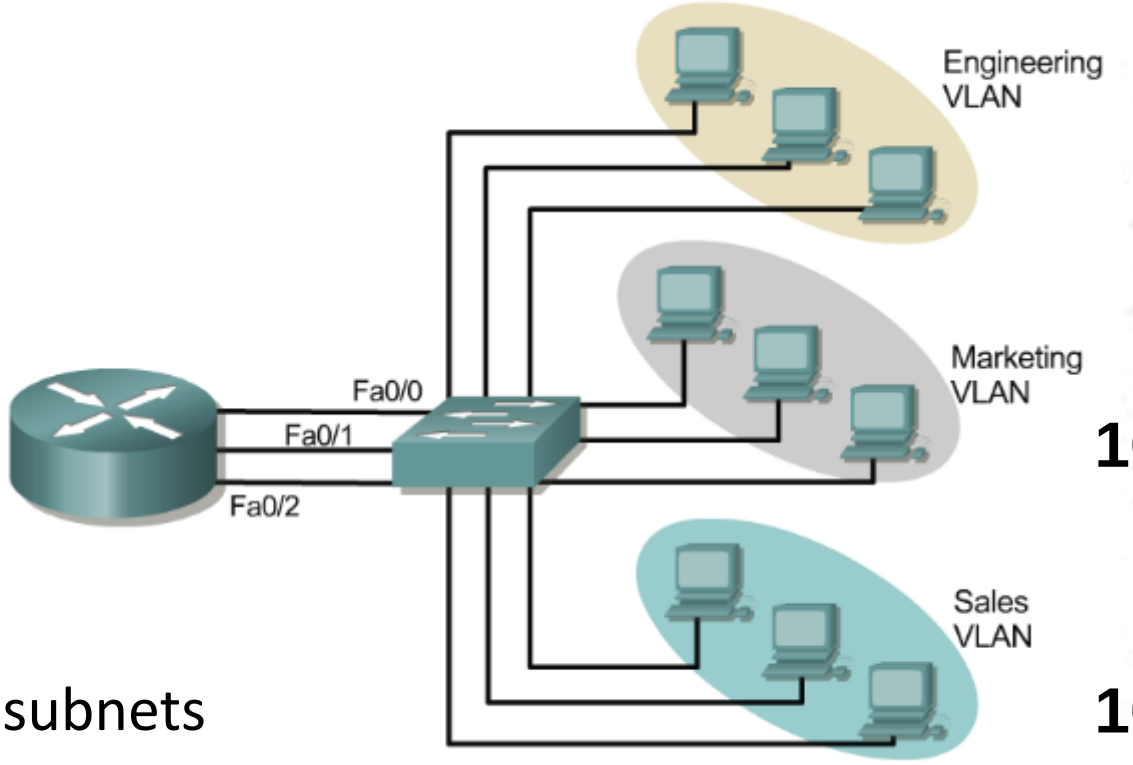
Legacy Inter-VLAN Routing



In this example, the router was configured with two separate physical interfaces to interact with the different VLANs and perform the routing.

Passing traffic between VLANs cont.

- 3 VLANs in 1 switch



10.1.0.0/16

10.2.0.0/16

10.3.0.0/16

- Three IP subnets
- Router with 3 LAN ports
- Waste of resources

Router-on-a-Stick Inter-VLAN Routing

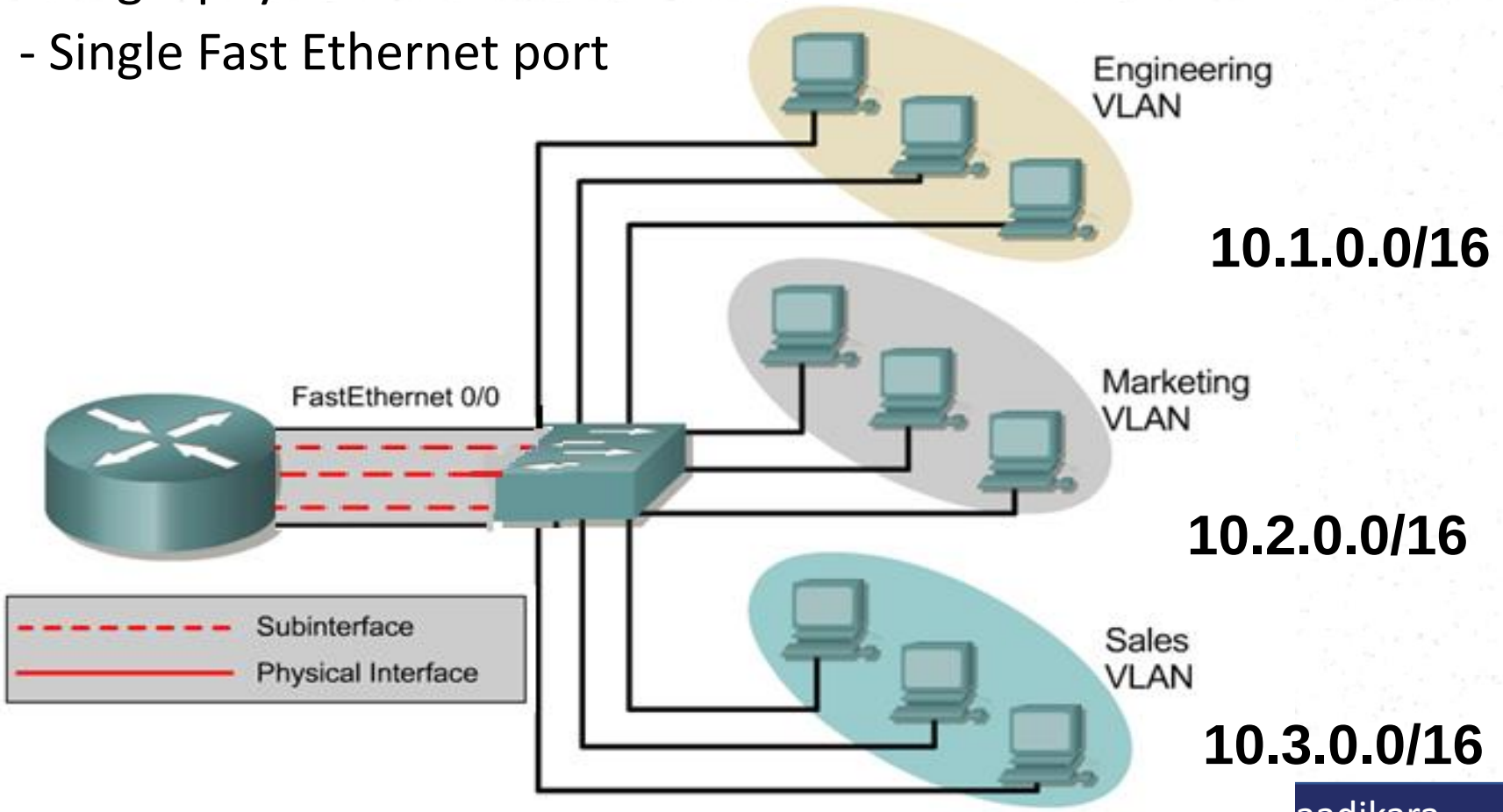
- The router-on-a-stick approach uses only one of the router's physical interface.
- One of the router's physical interfaces is configured as a 802.1Q trunk port so it can understand VLAN tags.
- Logical sub-interfaces are created; one sub-interface per VLAN.
- Each sub-interface is configured with an IP address from the VLAN it represents.
- **VLAN members (hosts) are configured to use the sub-interface address as a default gateway.**

Passing traffic between VLANs cont.

- Solution

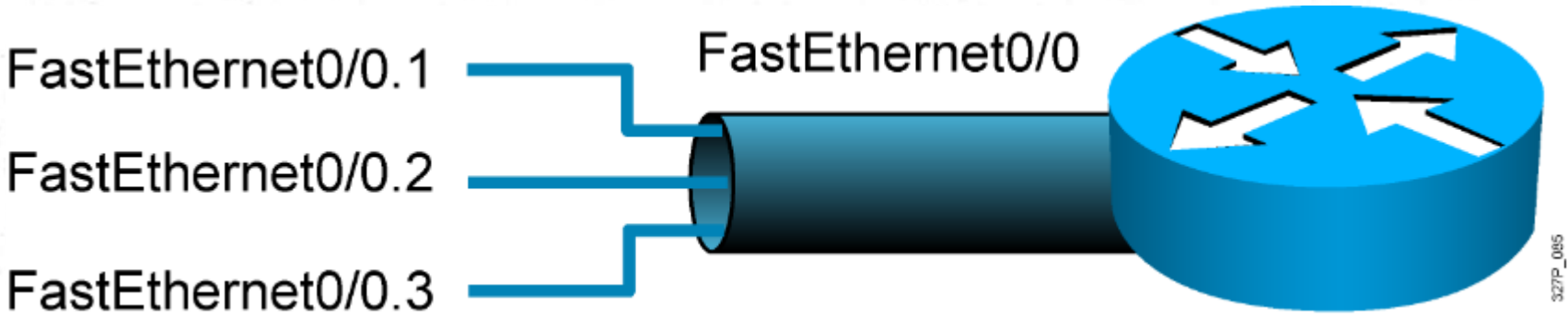
  Router supports trunking (Inter VLAN routing)

  - Single physical connection
  - Single Fast Ethernet port

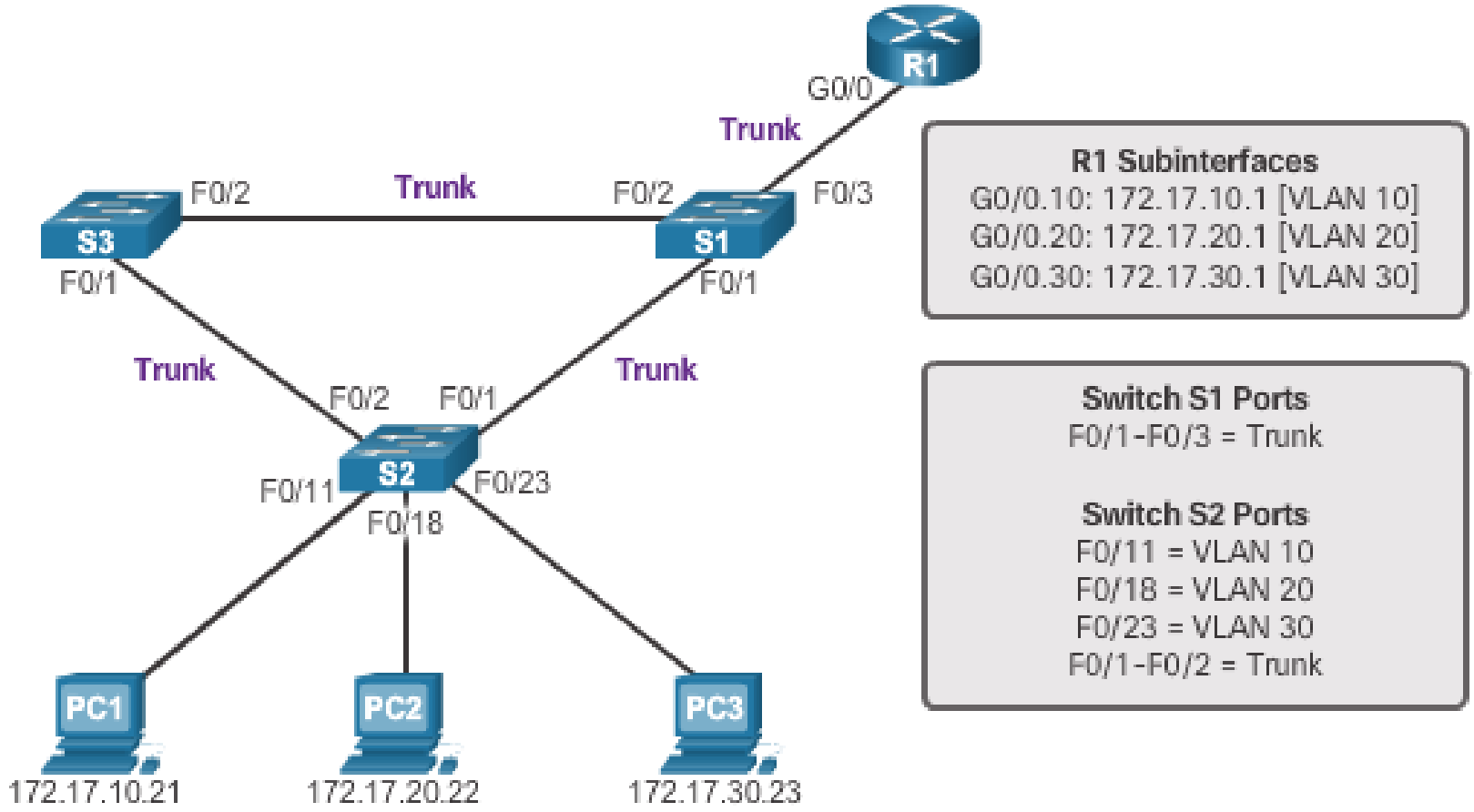


Inter VLAN routing

- Sub interfaces on a router can be used to divide a single physical interface into multiple logical interfaces
- Each physical interface can have up to 65,535 logical interfaces

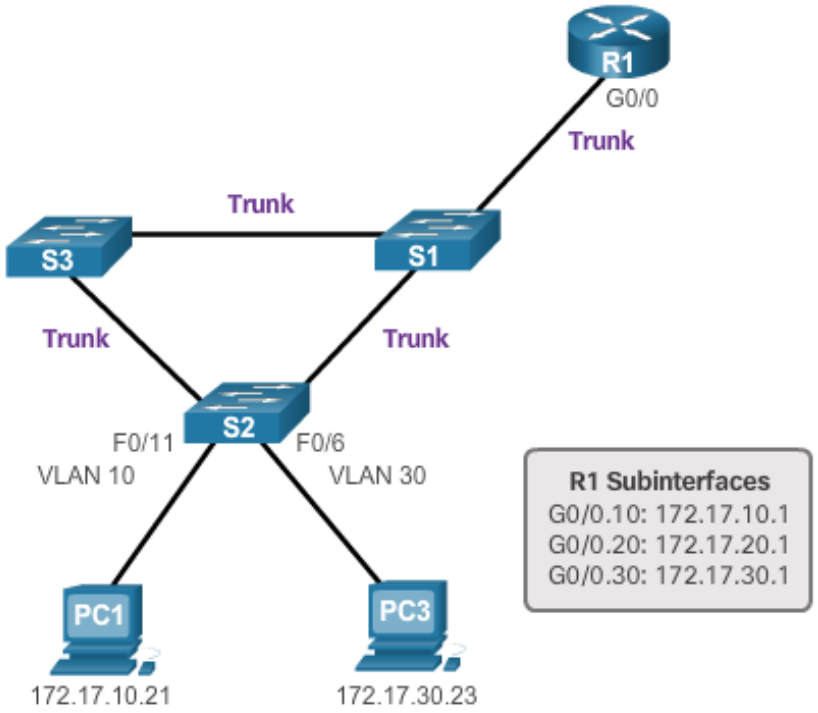


Router-on-a-Stick Inter-VLAN Routing

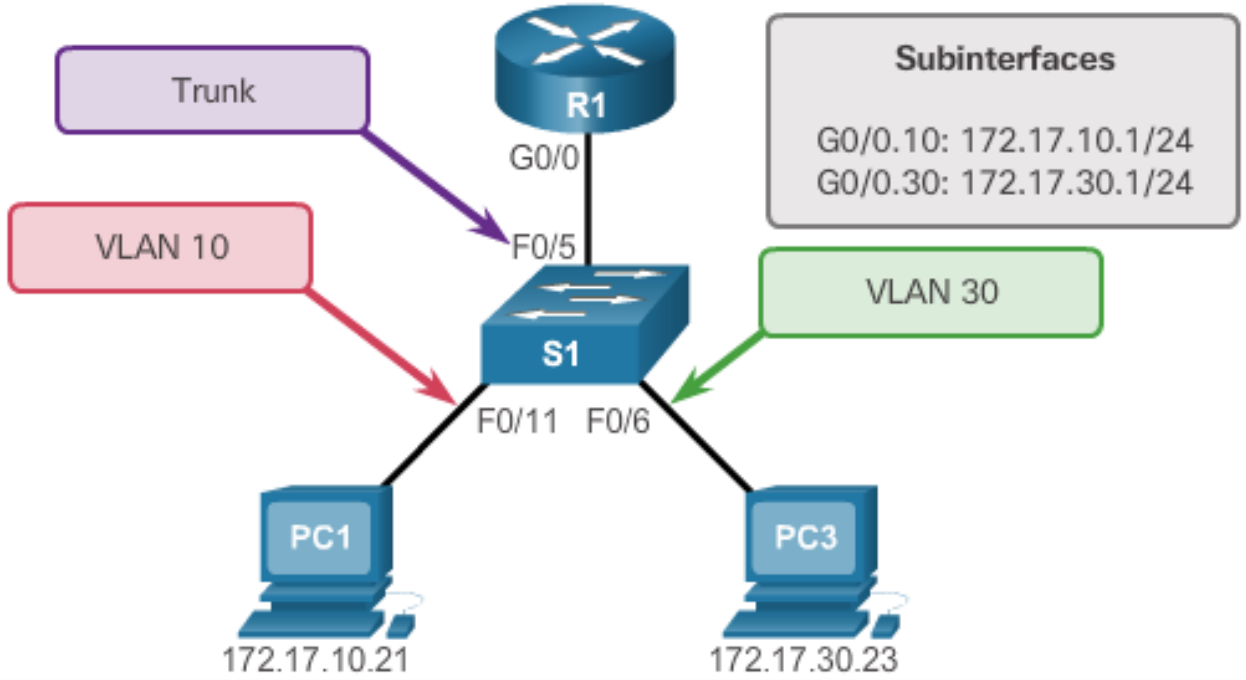


Configure Router-on-a Stick:

- VLAN trunking allows a single physical router interface to route traffic for multiple VLANs.
- The physical interface of the router must be connected to a trunk link on the adjacent switch.
- On the router, sub-interfaces are created for each unique VLAN.
- Each sub-interface is assigned an IP address specific to its subnet or VLAN and is also configured to tag frames for that VLAN.



Configure Router-on-a Stick: Switch Configuration




```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```

Configure Router-on-a Stick: Router Subinterface Configuration

```
R1(config)# interface g0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# interface g0/0.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0
R1(config)# interface g0/0
R1(config-if)# no shutdown
```

Configure Router-on-a Stick: Verifying Subinterfaces (cont.)

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP,M - mobile,

Gateway of last resort is not set

   172.17.0.0/16 is variably subnetted, 4 subnets, 2 masks
C     172.17.10.0/24 is directly connected, GigabitEthernet0/0.10
L     172.17.10.1/32 is directly connected, GigabitEthernet0/0.10
C     172.17.30.0/24 is directly connected, GigabitEthernet0/0.30
L     172.17.30.1/32 is directly connected, GigabitEthernet0/0.30
```

VLAN Implementations

Types of VLANs (cont.)

VLAN 1

```
Switch# 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
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

- All ports assigned to VLAN 1 by default.
- Native VLAN is VLAN 1 by default.
- Management VLAN is VLAN 1 by default.

VLAN Ranges on Catalyst Switches

- Cisco Catalyst 2960 and 3560 Series switches support over 4,000 VLANs.
- VLANs are split into two categories:
  - Normal range VLANs
    - VLAN numbers from 1 to 1,005
    - Configurations stored in the vlan.dat (in the flash memory)
    - IDs 1002 through 1005 are reserved for Token Ring and Fiber Distributed Data Interface (FDDI) VLANs, automatically created and cannot be removed
  - Extended Range VLANs
    - VLAN numbers from 1,006 to 4,096
    - Configurations stored in the running configuration (NVRAM)
    - VLAN Trunking Protocol (VTP) does not learn extended VLANs

VLAN Ranges on Catalyst Switches

- Normal Range VLANs

```
Switch# 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
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

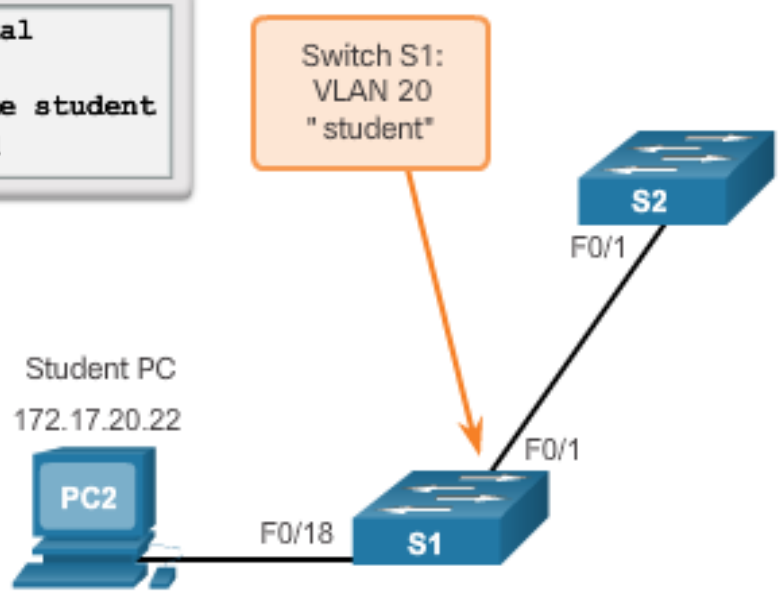
VLAN Assignment

Creating a VLAN

Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Create a VLAN with a valid id number.	`S1(config)# vlan vlan-id`
a unique name to identify the	`S1(config-vlan)# name vlan-name`
to the privileged EXEC mode.	`S1(config-vlan)# end`

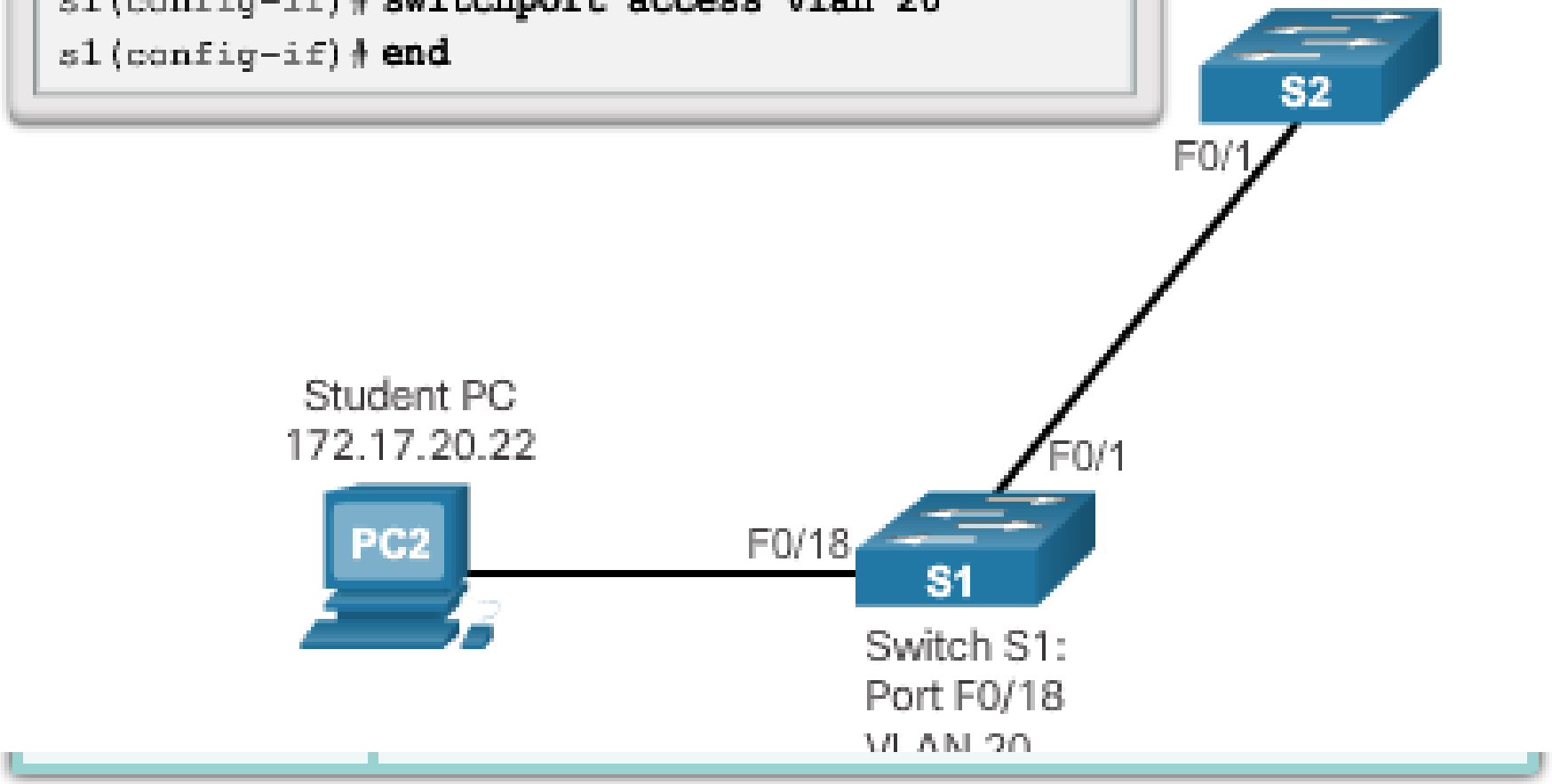
Sample Configuration

```
S1# configure terminal
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# end
```



Assigning Ports to VLANs

```
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```



Changing VLAN Port Membership

- Remove VLAN Assignme

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# **configure terminal**
Remove the VLAN assignment from the port.	S1(config-if)# **no switchport access vlan**
Return to the privileged EXEC mode.	S1(config-if)# **end**

- Interface F0/18 was previously assigned to VLAN 20 which is still active, F0/18 reset to VLAN1

```
S1(config)# int F0/18
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, Fa0/4
                                 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
S1#
```

Changing VLAN Port Membership (cont.)

Verification

```
S1# sh interfaces F0/18 switchport
Name: F0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

Deleting VLANs

```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh 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, Fa0/12, 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
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
S1#
```

Verifying VLAN Information

`show vlan` Command

Cisco IOS CLI Command Syntax	
show vlan [**brief** | **id** *vlan-id* | **name** *vlan-name* | **summary**]	
Display one line for each VLAN with the VLAN name, status, and its ports.	**brief**
Display information about a single VLAN identified by VLAN ID number. For vlan-id, the range is 1 to 4094.	**id** *vlan-id*
Display information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.	**name** *vlan-name*
Display VLAN summary information.	**summary**

Verifying VLAN Information

```
S1# show vlan name student

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------
20   student                           active    Fa0/11, 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            : 7
Number of existing VTP VLANs        : 7
Number of existing extended VLANS   : 0

S1#
```