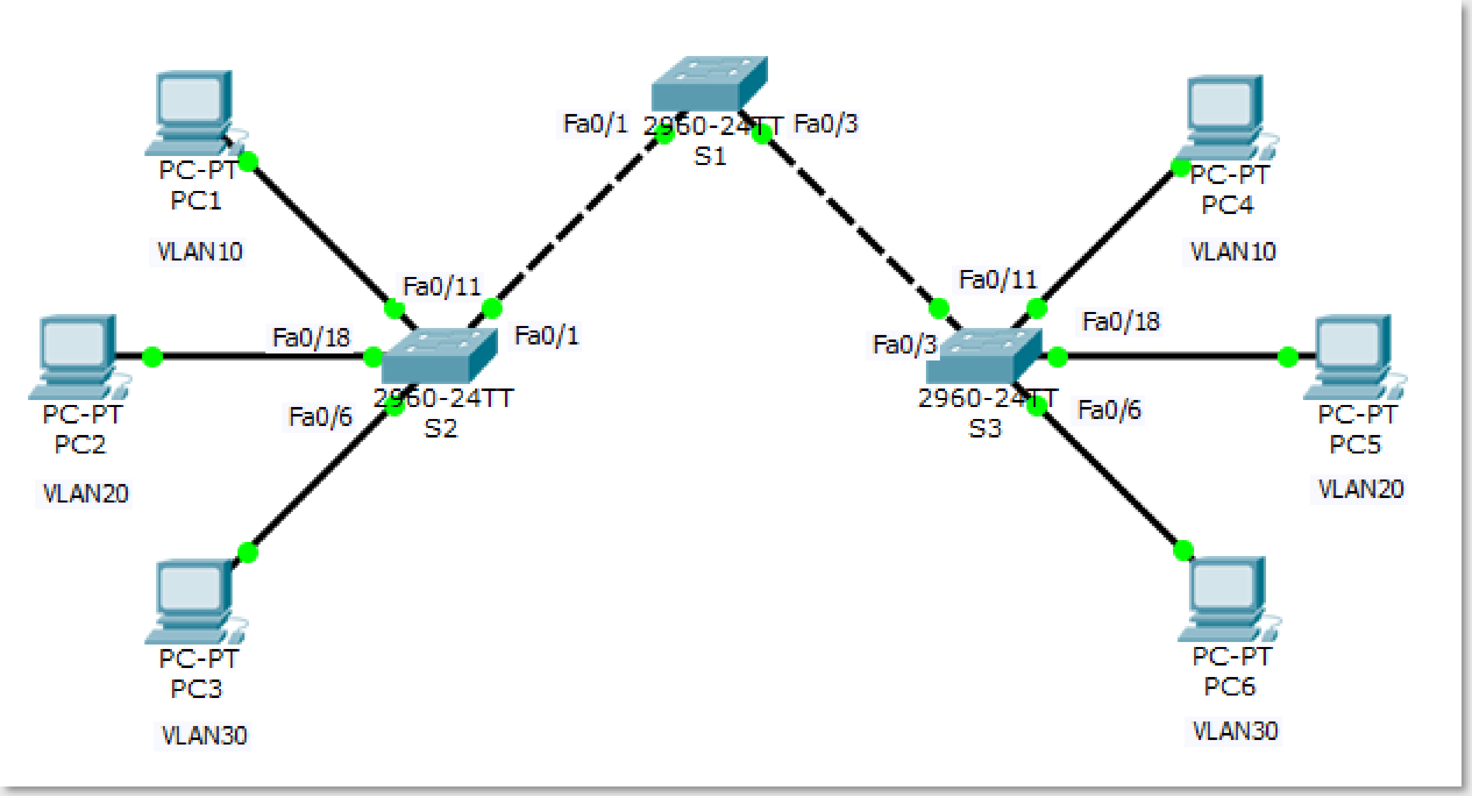
Lab 9

Virtual LANs

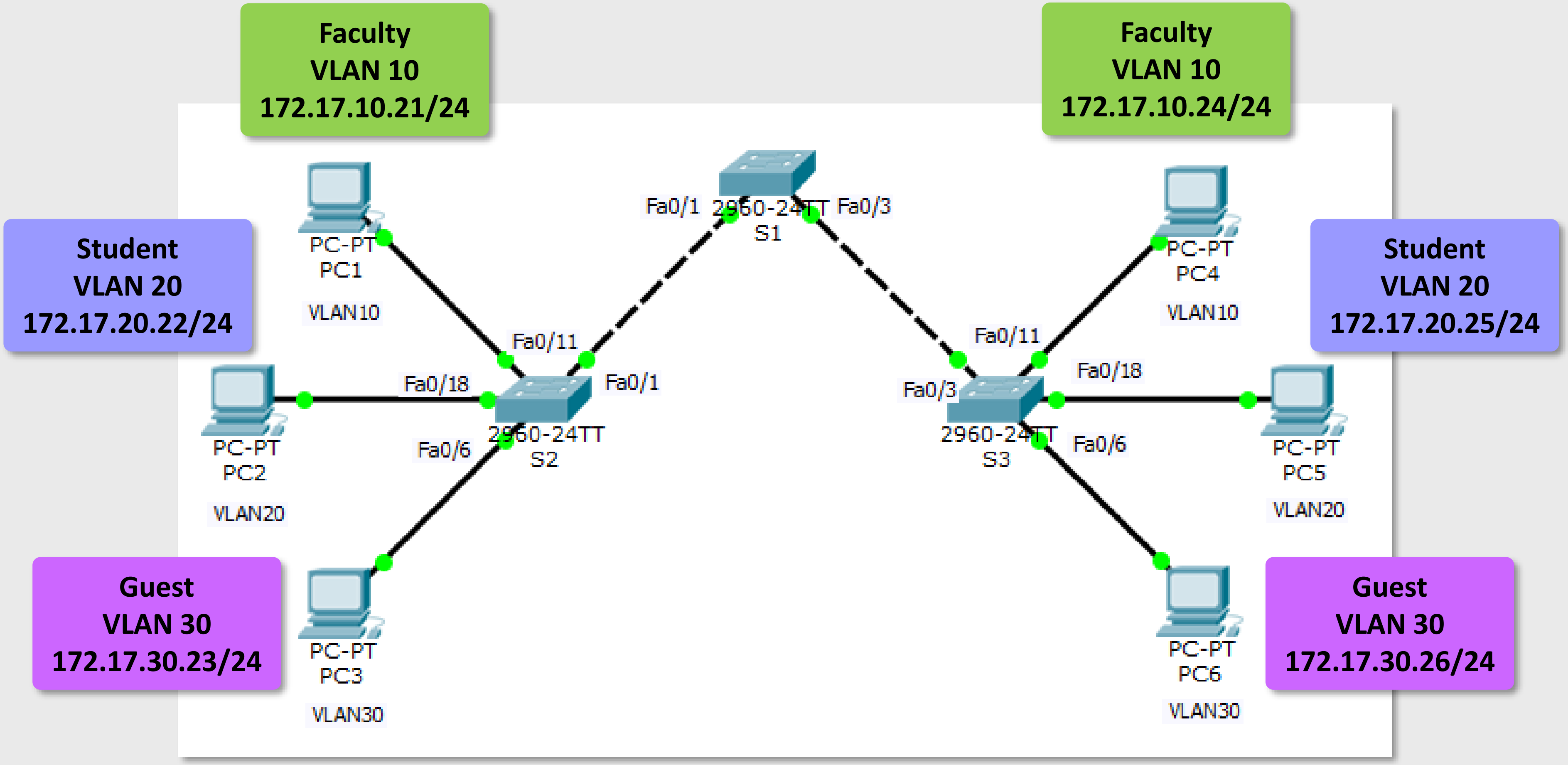
Introduction

- Switched LAN
  - Huge broadcast traffic amount
  - Security issues



Virtual LANs

- One shared physical infrastructure (devices and cabling)
- Multiple logical LANs



Faculty
VLAN 10
172.17.10.21/24

Student
VLAN 20
172.17.20.22/24

Guest
VLAN 30
172.17.30.23/24

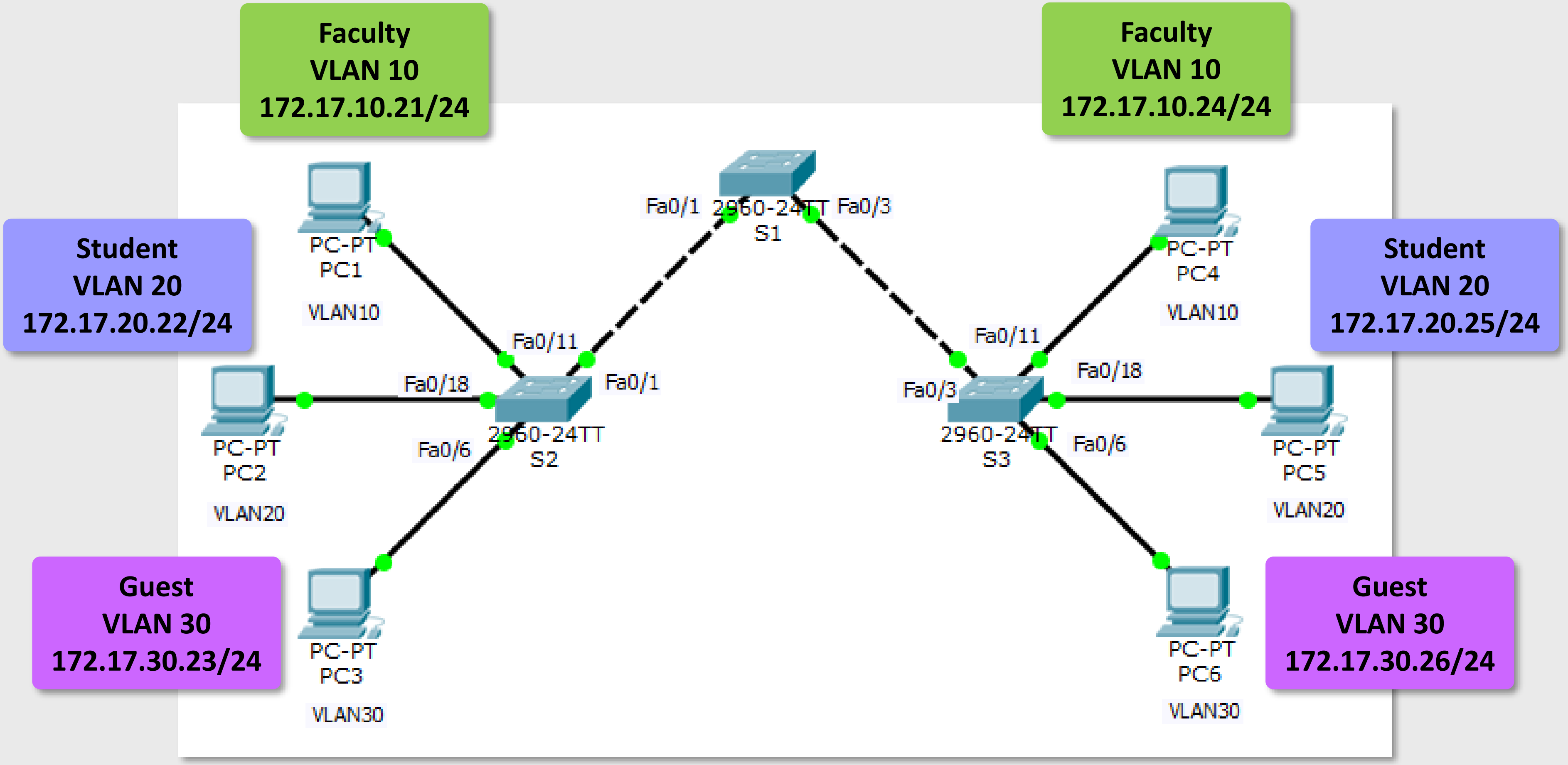
Faculty
VLAN 10
172.17.10.24/24

Student
VLAN 20
172.17.20.25/24

Guest
VLAN 30
172.17.30.26/24

Benefits of VLANs

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



Faculty
VLAN 10
172.17.10.21/24

Student
VLAN 20
172.17.20.22/24

Guest
VLAN 30
172.17.30.23/24

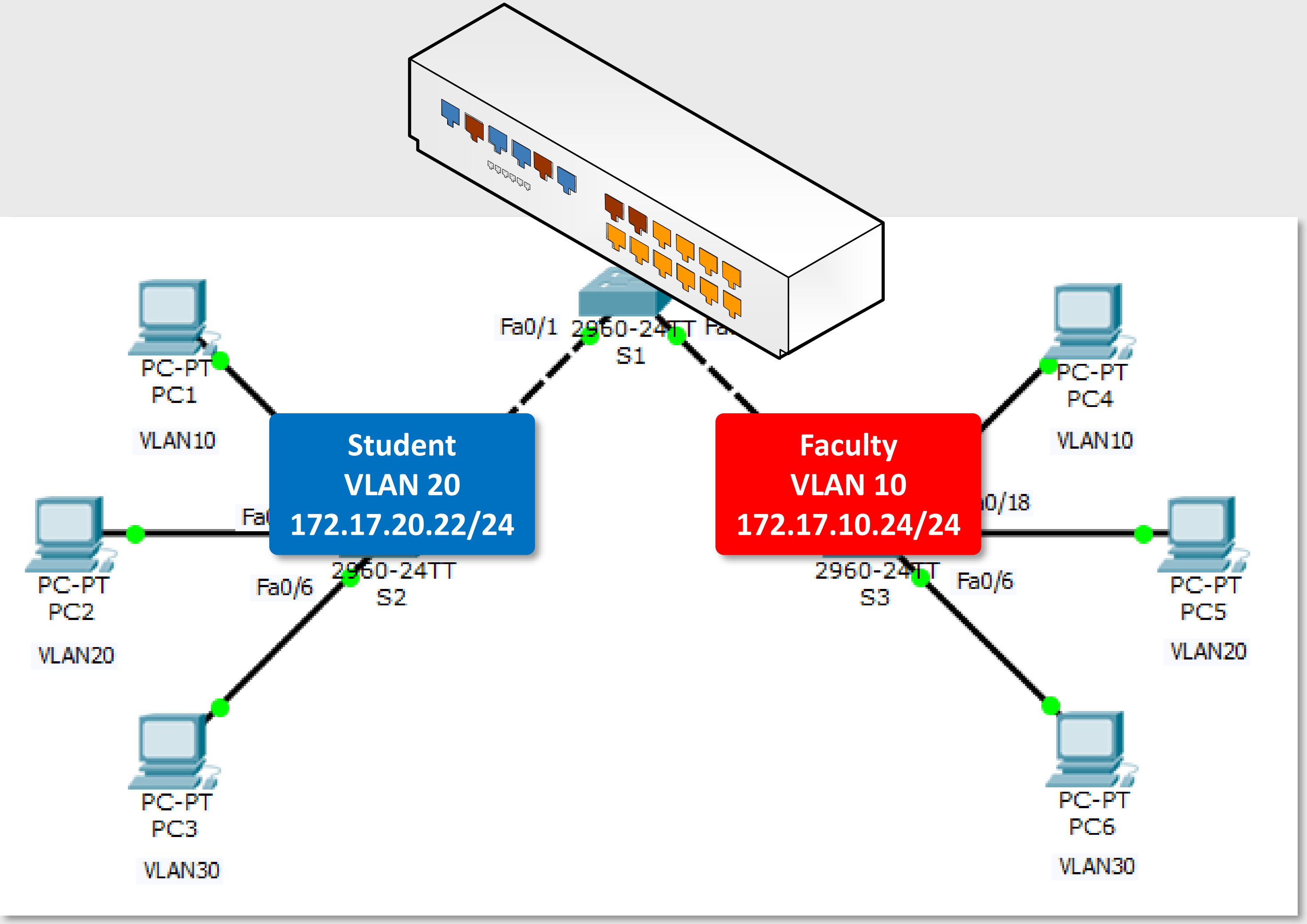
Faculty
VLAN 10
172.17.10.24/24

Student
VLAN 20
172.17.20.25/24

Guest
VLAN 30
172.17.30.26/24

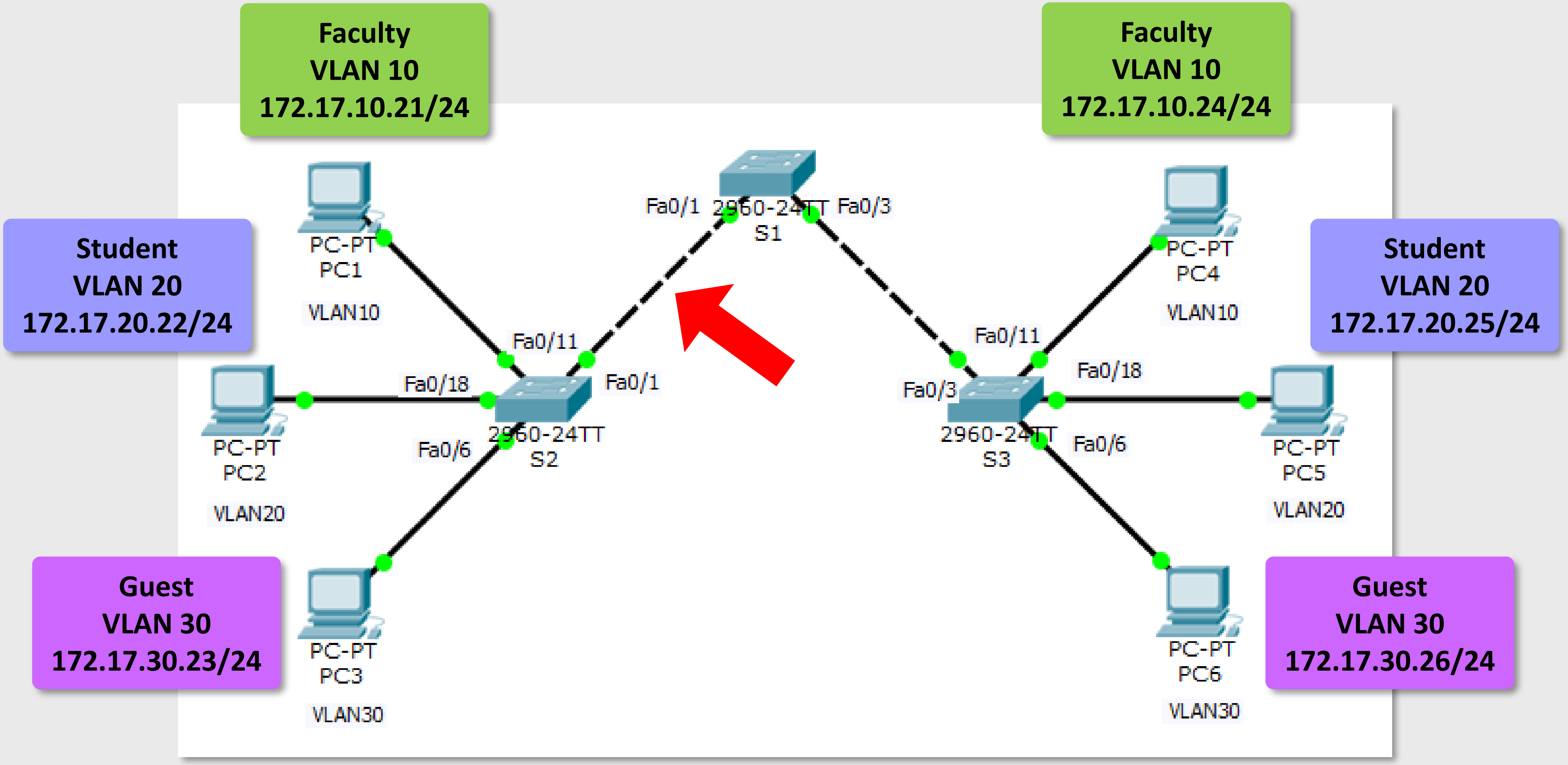
VLAN – intra-switch

- Single main highly reliable switch
- Grouping of ports into distinct *broadcast* domains



VLAN – inter-switch

- Concept extended to all switches in the LAN
- **Problem:** forwarding of frames received over a link interconnecting two switches (trunk)



Faculty
VLAN 10
172.17.10.21/24

Faculty
VLAN 10
172.17.10.24/24

Student
VLAN 20
172.17.20.22/24

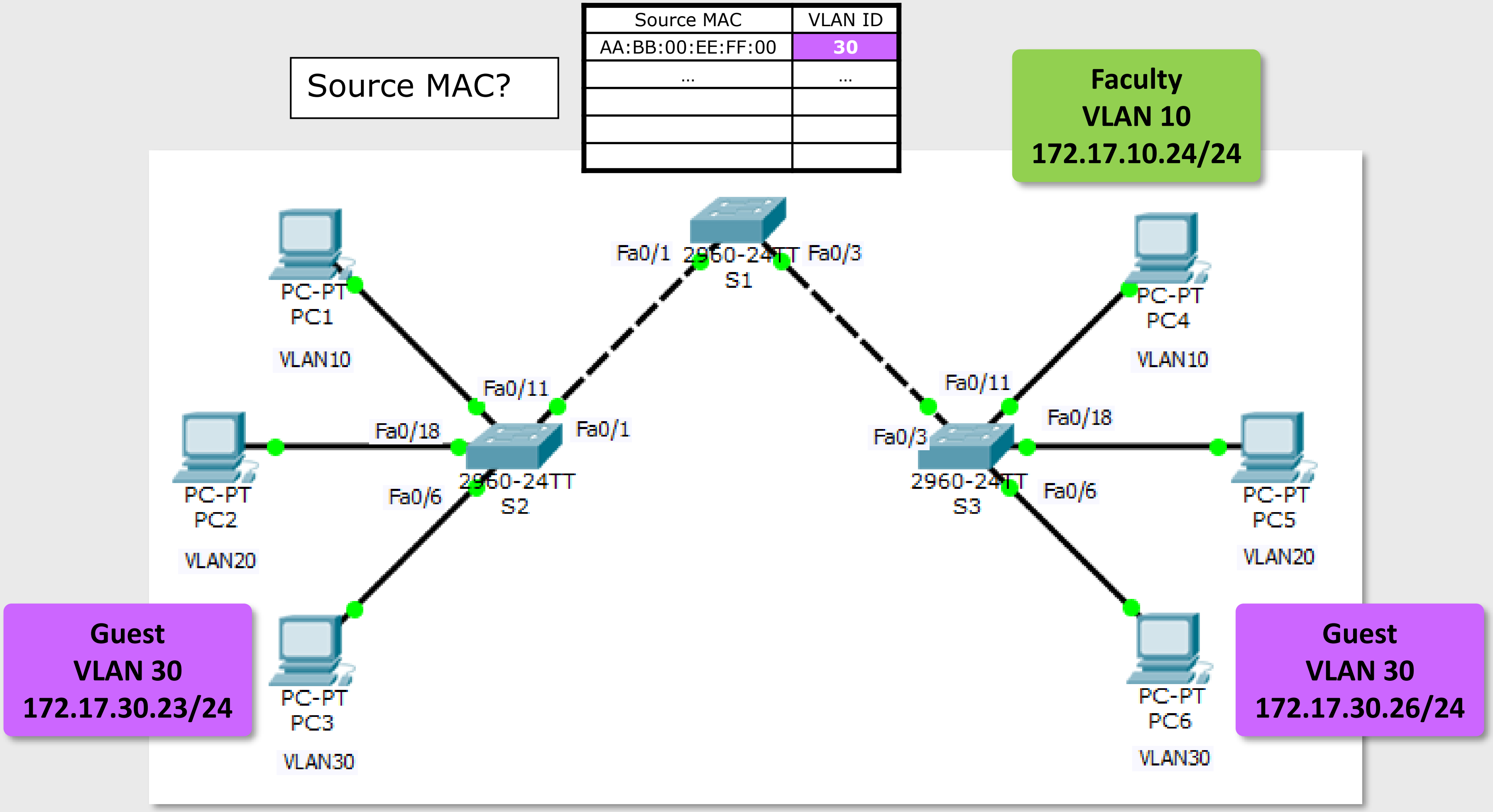
Student
VLAN 20
172.17.20.25/24

Guest
VLAN 30
172.17.30.23/24

Guest
VLAN 30
172.17.30.26/24

VLAN – inter-switch (2)

- Solution 1: ***frame filtering***
- VLAN membership based on the source MAC address



Source MAC?

Source MAC	VLAN ID
AA:BB:00:EE:FF:00	30
…	…

Faculty
VLAN 10
172.17.10.24/24

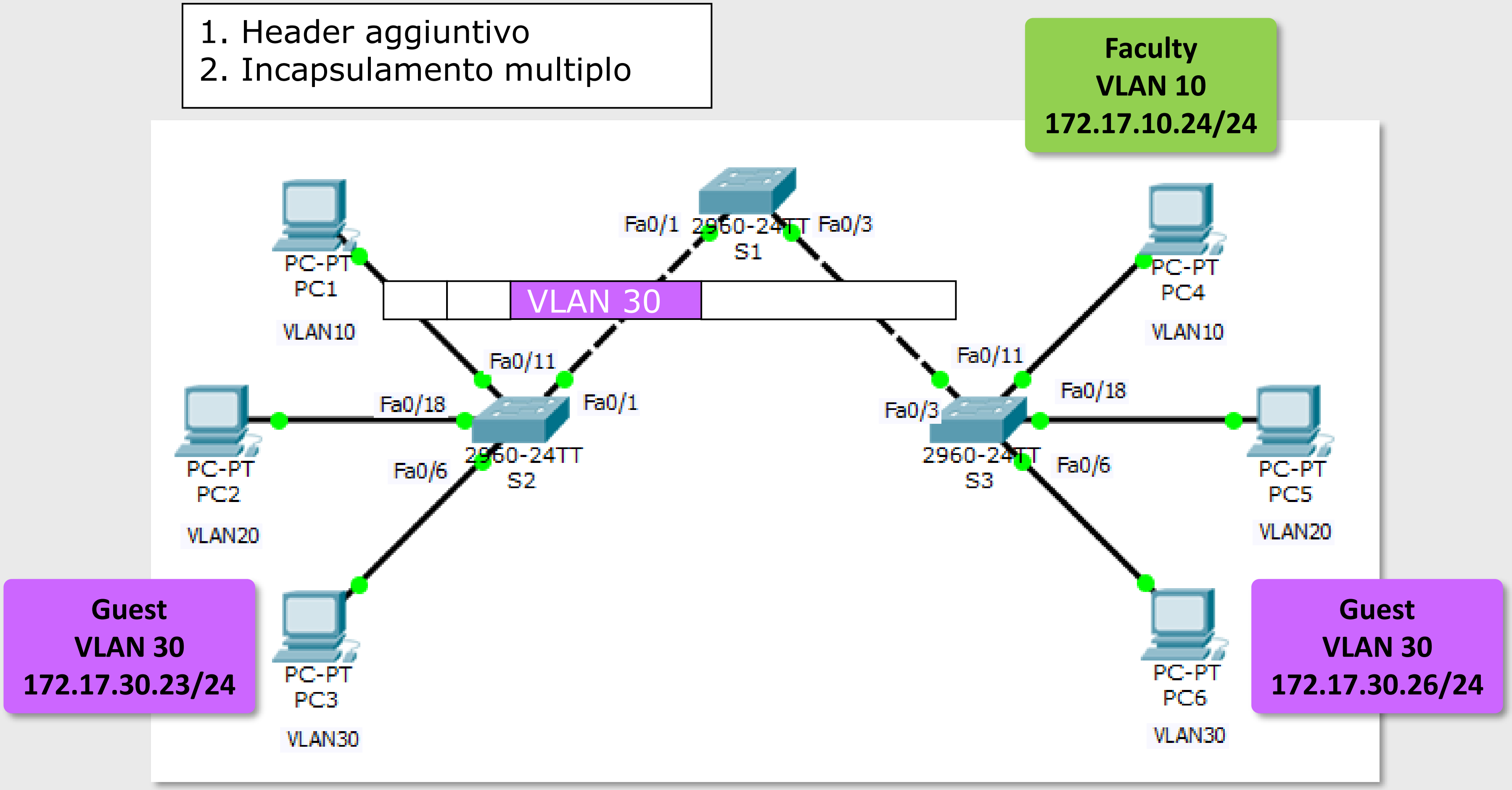
Guest
VLAN 30
172.17.30.23/24

Guest
VLAN 30
172.17.30.26/24

VLAN – inter-switch (3)

- Solution 2: ***frame tagging***
- VLAN membership based on ingress port

1. Header aggiuntivo
2. Incapsulamento multiplo



Frame filtering vs. frame tagging

- Frame filtering
  - Pros
    - Full control – VLAN membership is managed per host
    - Seamless support for host mobility
  - Cons
    - Inefficient forwarding process
    - Low scalability of management

- Frame tagging
  - Pros
    - Scalability of management
    - Scalability of control
  - Cons
    - Need for standard protocols to ensure interoperability
    - No support for host mobility

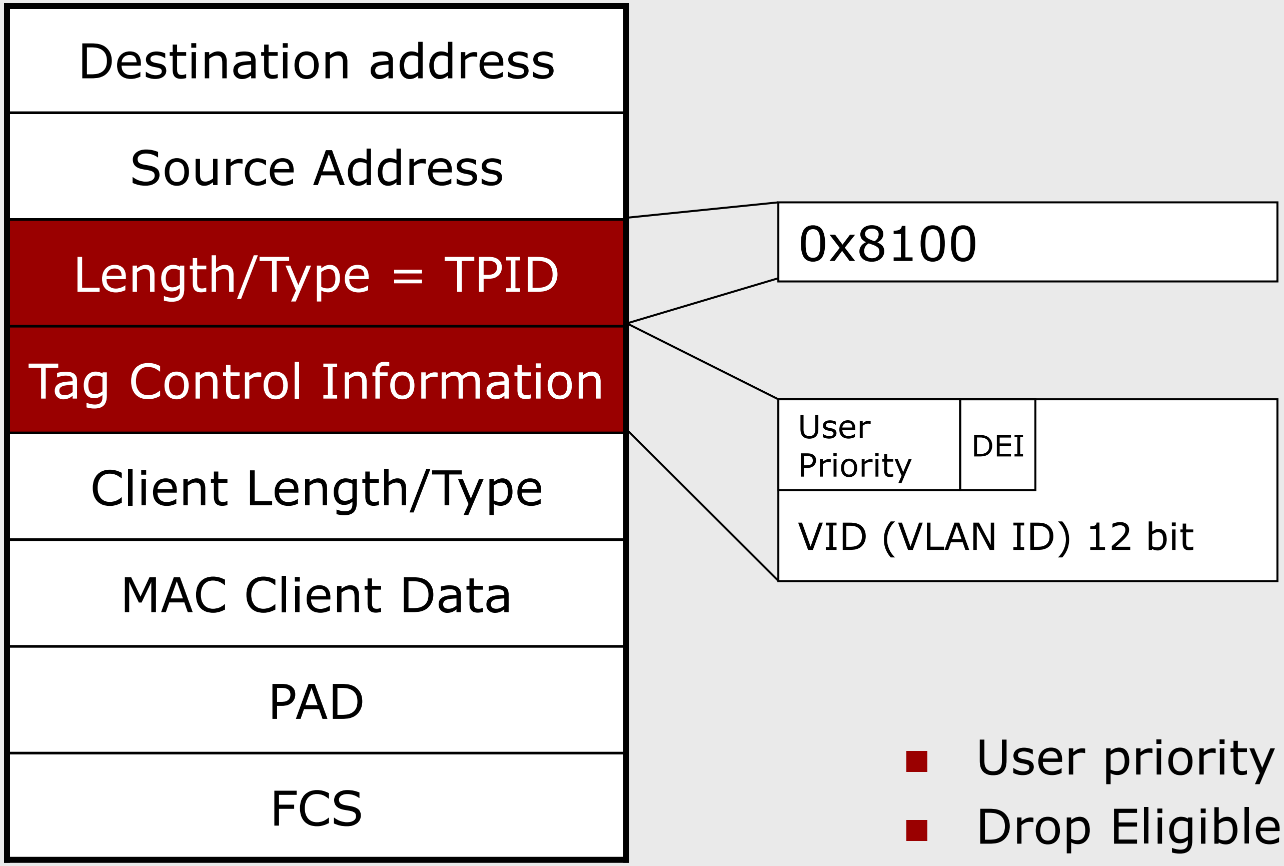
VLAN standards – 802.1Q

- IEEE 802.1Q – *Virtual Bridged Local Area Networks*
  - Port-based VLAN membership
  - Specification of the *tagging* procedure
  - Specification of VLAN-based forwarding process

- IEEE 802.3ac – *Frame extensions for Virtual Bridged Local Area Network (VLAN) tagging on 802.3 networks*

- IEEE 802.1p – *Traffic Class Expediting and Dynamic Multicast Filtering* (in 802.1D-1998)
  - Support for priority classes

802.1Q - Formato dei pacchetti *tagged*



- User priority – range 0-7
- Drop Eligible Indicator
- VLAN ID – range 2-4094
  - 0: null
  - 1: default VLAN
  - 4095: reserved

802.1Q – Device type

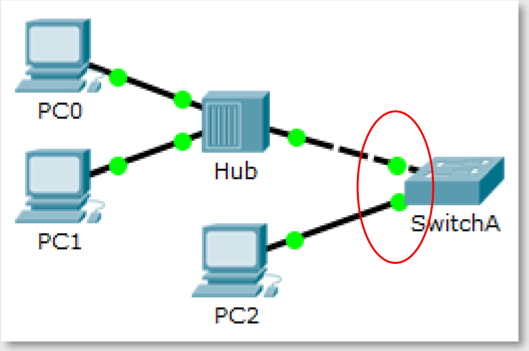
- Two types of device
  - ***VLAN-aware***, manages both tagged and untagged frames
  - ***VLAN-unaware***, manages untagged frames only
    - Legacy switches
    - Low-end switches

- Devices compliant with the 801.1Q standard (as declared by manufacturer specifications) are *VLAN-aware*

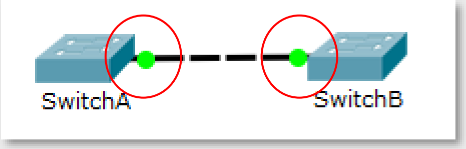
- Classification applies also to NICs
  - *A host NIC can be configured as a trunk. Example of use?*

802.1Q – Port and link types

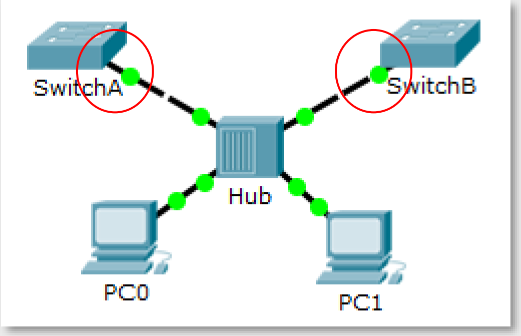
- **Access port – Access link**
  - Tx/Rx untagged frames



- **Trunk port – trunk link**
  - Tx/Rx tagged frames



- **Hybrid port – hybrid link**
  - Tx/Rx both tagged and untagged frames
  - Untagged frames are forwarded to a configured link *native VLAN*



Cisco IOS – VLAN id ranges

- **Normal Range VLANs**
  - Used in small- and medium-sized business and enterprise networks
  - Identified by a VLAN ID between 1 and 1005
    - IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs
  - IDs 1 and 1002 to 1005 are automatically created and cannot be removed
  - Configurations are stored within a VLAN database file, called **`vlan.dat`**, located in the flash memory of the switch
- **Extended Range VLANs**
  - Enable service providers to extend their infrastructure to a greater number of customers
  - Are identified by a VLAN ID between 1006 and 4094
  - Support fewer VLAN features than normal range VLANs
  - Are saved in the running configuration file
- Constraints
  - Cisco Catalyst 2960 switch can support up to **255** normal range and extended range VLANs overall

Cisco IOS – special VLAN types

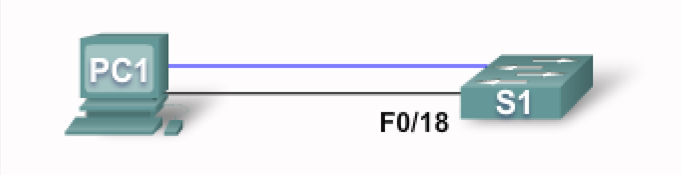
- **Default VLAN**
  - Pre-configured VLAN for Cisco switches (VLAN ID 1)
    - Cannot be renamed nor deleted
  - All switch ports are members of this VLAN after boot-up

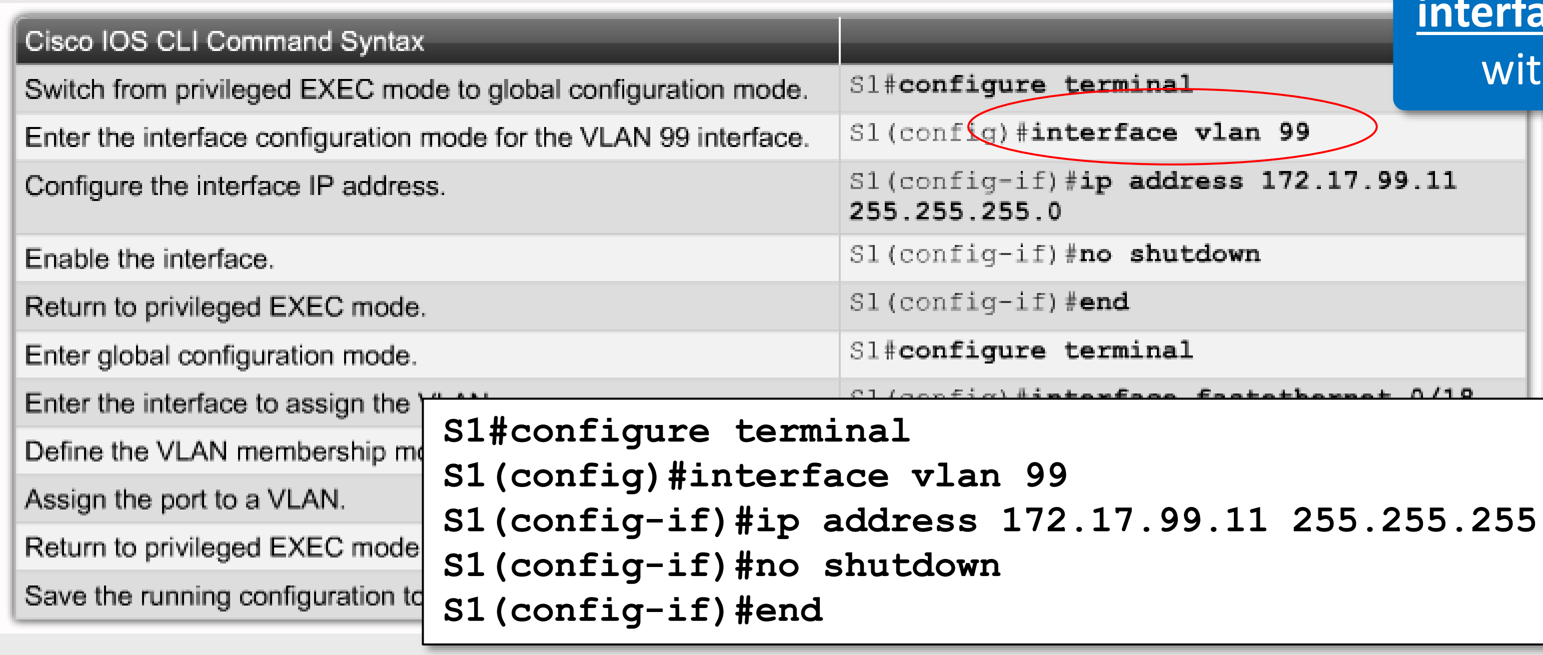
- **Native VLAN**
  - Untagged traffic on hybrid ports (trunk ports are hybrid by default on Cisco switches) is placed on the native VLAN (1 by default)
  - Security best practice: unused VLAN other than VLAN 1 and other VLANs

- **Management VLAN**
  - Any VLAN configured to access the management capabilities of a switch
    - The switch virtual interface (SVI) of that VLAN is assigned an IP address and subnet mask
  - Security best practice: use a VLAN other than VLAN 1 as management VLAN

Cisco IOS – Management VLAN

- Enable remote configuration using TCP/IP
  - Assign the switch an IP address (associated to the *management* VLAN)





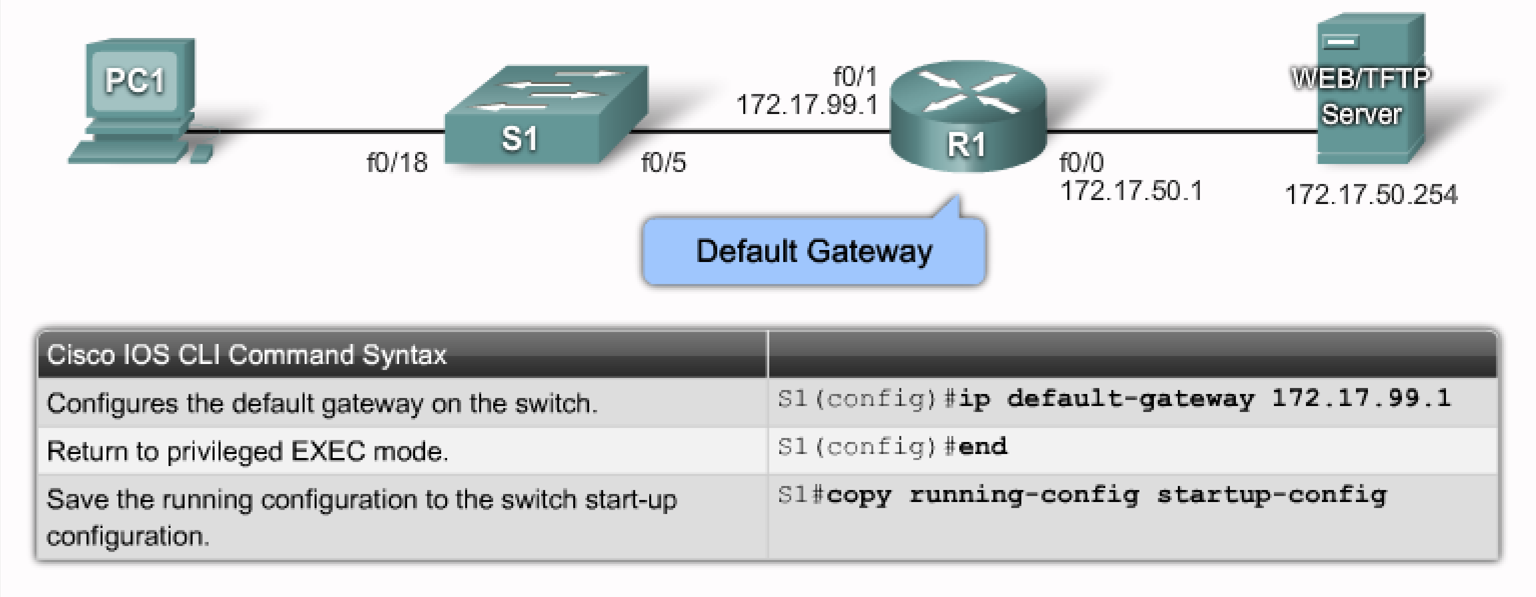
Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	S1#**configure terminal**
Enter the interface configuration mode for the VLAN 99 interface.	S1(config)#**interface vlan 99**
Configure the interface IP address.	S1(config-if)#**ip address 172.17.99.11 255.255.255.0**
Enable the interface.	S1(config-if)#**no shutdown**
Return to privileged EXEC mode.	S1(config-if)#**end**
Enter global configuration mode.	S1#**configure terminal**
Enter the interface to assign the	S1(config)#**interface fastethernet 0/18**
Define the VLAN membership m	
Assign the port to a VLAN.	
Return to privileged EXEC mode	
Save the running configuration to	

virtual **Layer 3 interface** associated with VLAN 99

```
S1#configure terminal
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end
```

Basic configuration

- Enable remote configuration using TCP/IP
  - Configure a default gateway

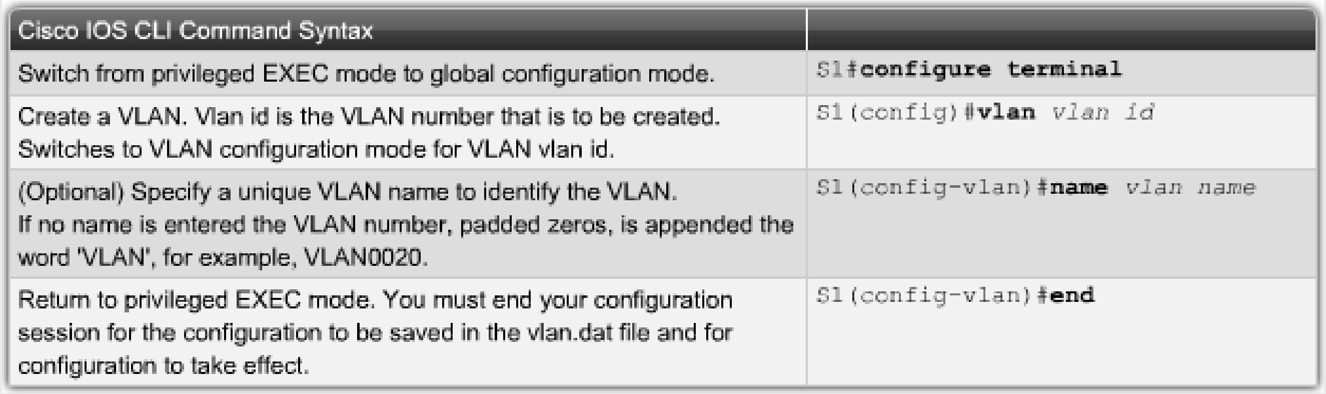


Cisco IOS CLI Command Syntax	
Configures the default gateway on the switch.	`S1(config)#`**`ip default-gateway 172.17.99.1`**
Return to privileged EXEC mode.	`S1(config)#`**`end`**
Save the running configuration to the switch start-up configuration.	`S1#`**`copy running-config startup-config`**

- Verify configuration
  - **`show running-config`**
  - **`show ip interface brief`**

Cisco IOS – managing VLANs

- Adding a VLAN



Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	S1#**configure terminal**
Create a VLAN. Vlan id is the VLAN number that is to be created. Switches to VLAN configuration mode for VLAN vlan id.	S1(config)#**vlan** *vlan id*
(Optional) Specify a unique VLAN name to identify the VLAN. If no name is entered the VLAN number, padded zeros, is appended the word 'VLAN', for example, VLAN0020.	S1(config-vlan)#**name** *vlan name*
Return to privileged EXEC mode. You must end your configuration session for the configuration to be saved in the vlan.dat file and for configuration to take effect.	S1(config-vlan)#**end**

- Deleting a VLAN
  - Command: **`no vlan`** ***`vlan-id`***
    - Ports assigned to the VLAN are not able to communicate until they are reassigned to a different VLAN
  - Command: **`delete flash:vlan.dat`**

Cisco IOS – managing VLANs

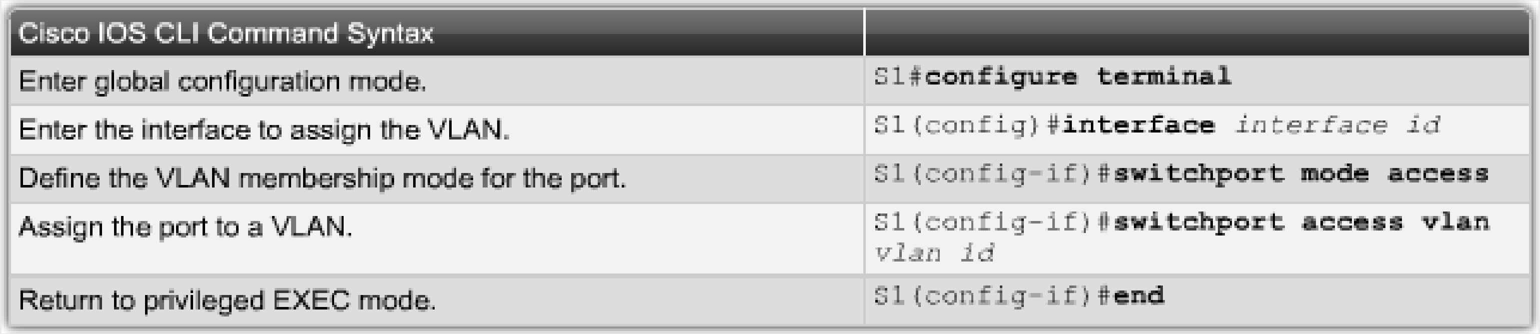
- Example

```
Sw0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw0(config)#vlan 20
Sw0(config-vlan)#name Administration
Sw0(config-vlan)#end

%SYS-5-CONFIG_I: Configured from console by console
Sw0#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
                                                Gig1/1, Gig1/2
20   Administration                   active    
1002 fddi-default                     active    
1003 token-ring-default               active    
1004 fddinet-default                  active    
1005 trnet-default                    active    
Sw0#
```

Cisco IOS – managing access ports

- An access port can belong to only one VLAN at a time

- Assign access port(s) to a VLAN



Cisco IOS CLI Command Syntax	
Enter global configuration mode.	`S1#`**`configure terminal`**
Enter the interface to assign the VLAN.	`S1(config)#`**`interface`** *`interface id`*
Define the VLAN membership mode for the port.	`S1(config-if)#`**`switchport mode access`**
Assign the port to a VLAN.	`S1(config-if)#`**`switchport access vlan`** *`vlan id`*
Return to privileged EXEC mode.	`S1(config-if)#`**`end`**

- Managing VLAN membership
  - Resetting port membership to default VLAN 1

```
Switch(config-if)#no switchport access vlan
```

  - Reassigning a port to a different VLAN
    - When you reassign an access port to an existing VLAN, the port is automatically removed from the previous VLAN

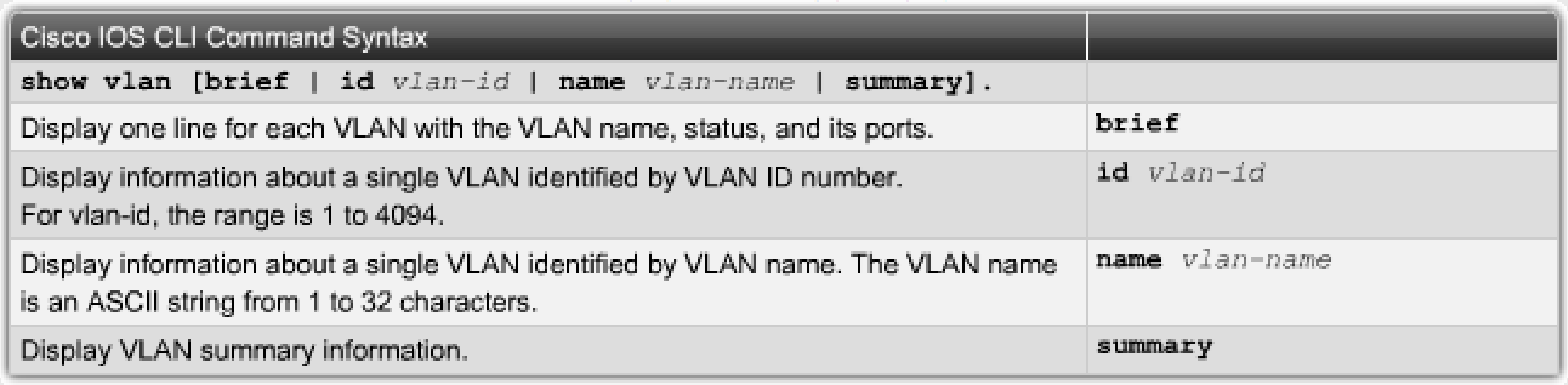
Cisco IOS – managing access ports

- Example

```
Sw0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw0(config)#interface range Fa0/18-24
Sw0(config-if-range)#switchport mode access
Sw0(config-if-range)#switchport access vlan 20
Sw0(config-if-range)#end

%SYS-5-CONFIG_I: Configured from console by console
Sw0#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, Gig1/1, Gig1/2
20   Administration                   active    Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Sw0#
```

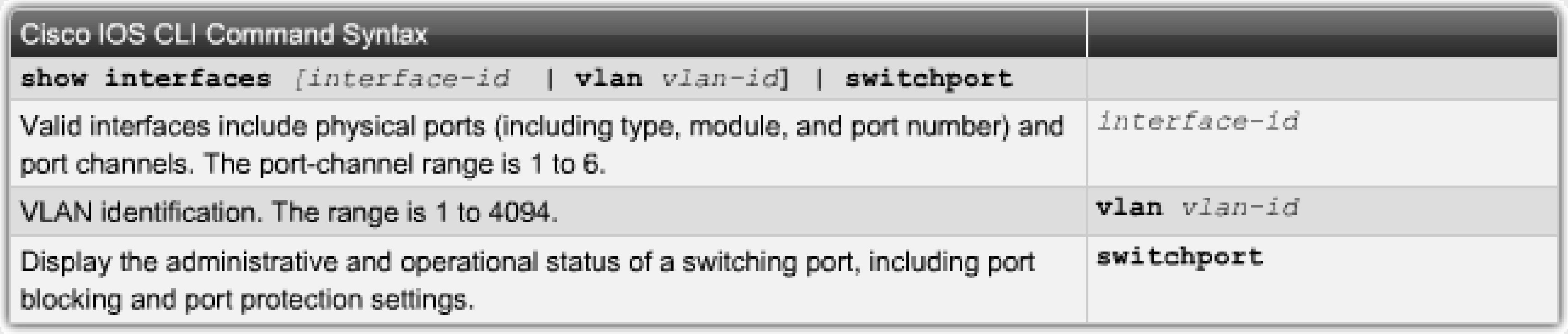
Cisco IOS – verify VLAN configuration

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**

Show Interfaces Command



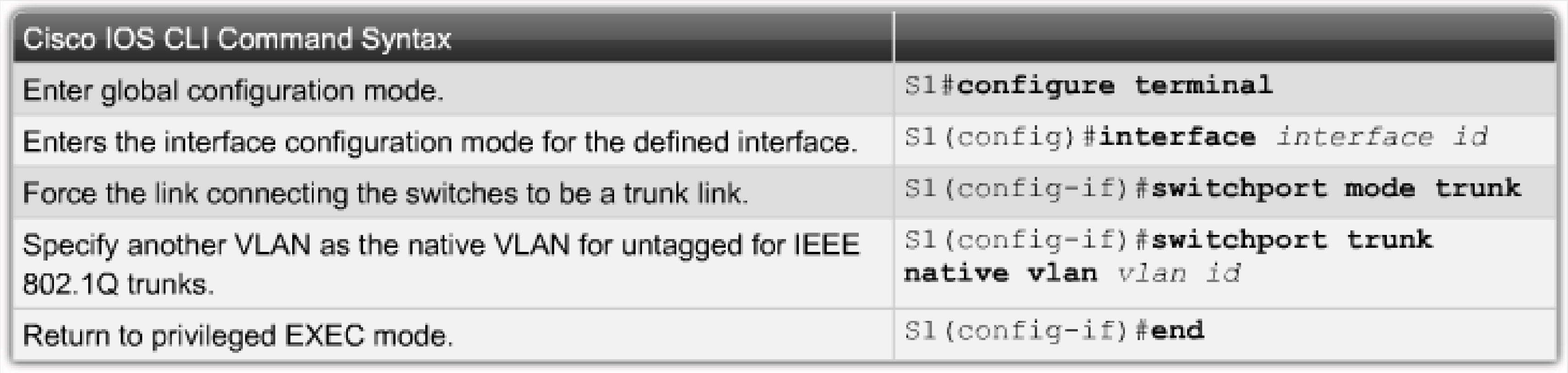
Cisco IOS CLI Command Syntax	
show interfaces *[interface-id* **| vlan** *vlan-id*] **| switchport**	
Valid interfaces include physical ports (including type, module, and port number) and port channels. The port-channel range is 1 to 6.	*interface-id*
VLAN identification. The range is 1 to 4094.	**vlan** *vlan-id*
Display the administrative and operational status of a switching port, including port blocking and port protection settings.	**switchport**

Cisco IOS – verify VLAN configuration

```
Sw0#show vlan name Administration

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
20   Administration                   active    Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0

Sw0#show interfaces Fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 20 (Administration)
Trunking Native Mode VLAN: 1 (default)
...
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
Sw0#
```

Cisco IOS – managing trunks

- Configure a trunk on a switch port



Cisco IOS CLI Command Syntax	
Enter global configuration mode.	`S1#`**`configure terminal`**
Enters the interface configuration mode for the defined interface.	`S1(config)#`**`interface`** *`interface id`*
Force the link connecting the switches to be a trunk link.	`S1(config-if)#`**`switchport mode trunk`**
Specify another VLAN as the native VLAN for untagged for IEEE 802.1Q trunks.	`S1(config-if)#`**`switchport trunk native vlan`** *`vlan id`*
Return to privileged EXEC mode.	`S1(config-if)#`**`end`**

- Trunk ports support both tagged and untagged traffic
  - Incoming untagged frames (or tagged frames with a null VLAN ID) are considered as tagged with the native VLAN ID
  - Outgoing tagged frames with a VLAN ID equal to the native VLAN ID are sent untagged
  - All other traffic is sent with a VLAN tag

Cisco IOS – managing trunks

- Example

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
Switch#
```

Cisco IOS – managing trunks

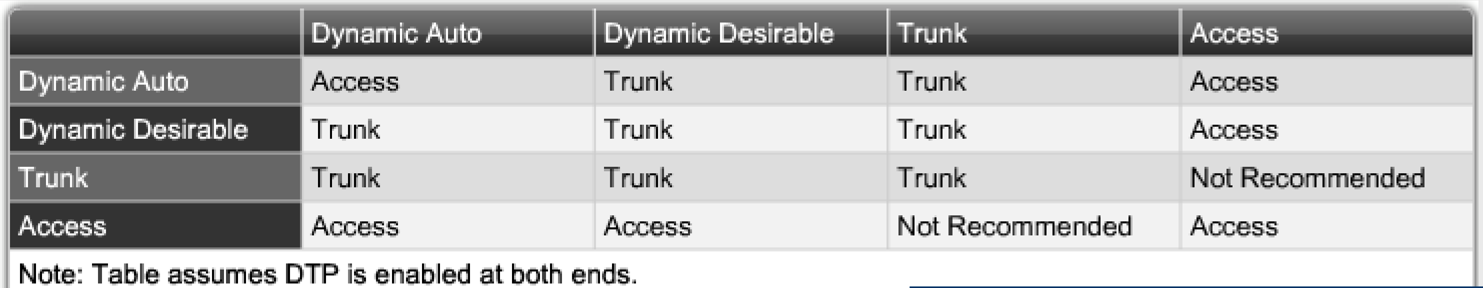
- Configuring allowed VLANs

```
switchport trunk allowed vlan {add | except | none | remove} vlan-id[,vlan-id,...]
switchport trunk allowed vlan all
```

```
Switch#show interfaces trunk
Port         Mode         Encapsulation  Status        Native vlan
Fa0/1        on           802.1q         trunking      99

Port         Vlans allowed on trunk
Fa0/1        1-1005

Port         Vlans allowed and active in management domain
Fa0/1        1,20,99


...
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fa0/1
Switch(config-if)#switchport trunk allowed vlan except 20
Switch(config-if)#end
Switch#show interfaces trunk
Port         Mode         Encapsulation  Status        Native vlan
Fa0/1        on           802.1q         trunking      99

Port         Vlans allowed on trunk
Fa0/1        1-19,21-1005

Port         Vlans allowed and active in management domain
Fa0/1        1,99
...
```

Cisco IOS – managing trunks

- Cisco Dynamic Trunking Protocol (DTP)
  - Manages trunk negotiation to setup a trunk link
- Trunking modes (**`switchport mode`** *`mode`*)
  - **`access`**
  - **`trunk`**
  - **`dynamic auto`** (default on 2960)
    - Able to trunk, but do not request the remote port to go to trunking state
  - **`dynamic desirable`**
    - Able to trunk, and asks the remote port to go to trunking state

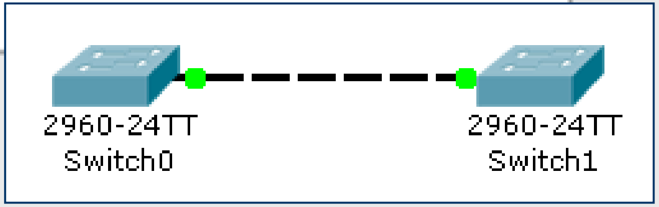


	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Not Recommended
Access	Access	Access	Not Recommended	Access

Note: Table assumes DTP is enabled at both ends.

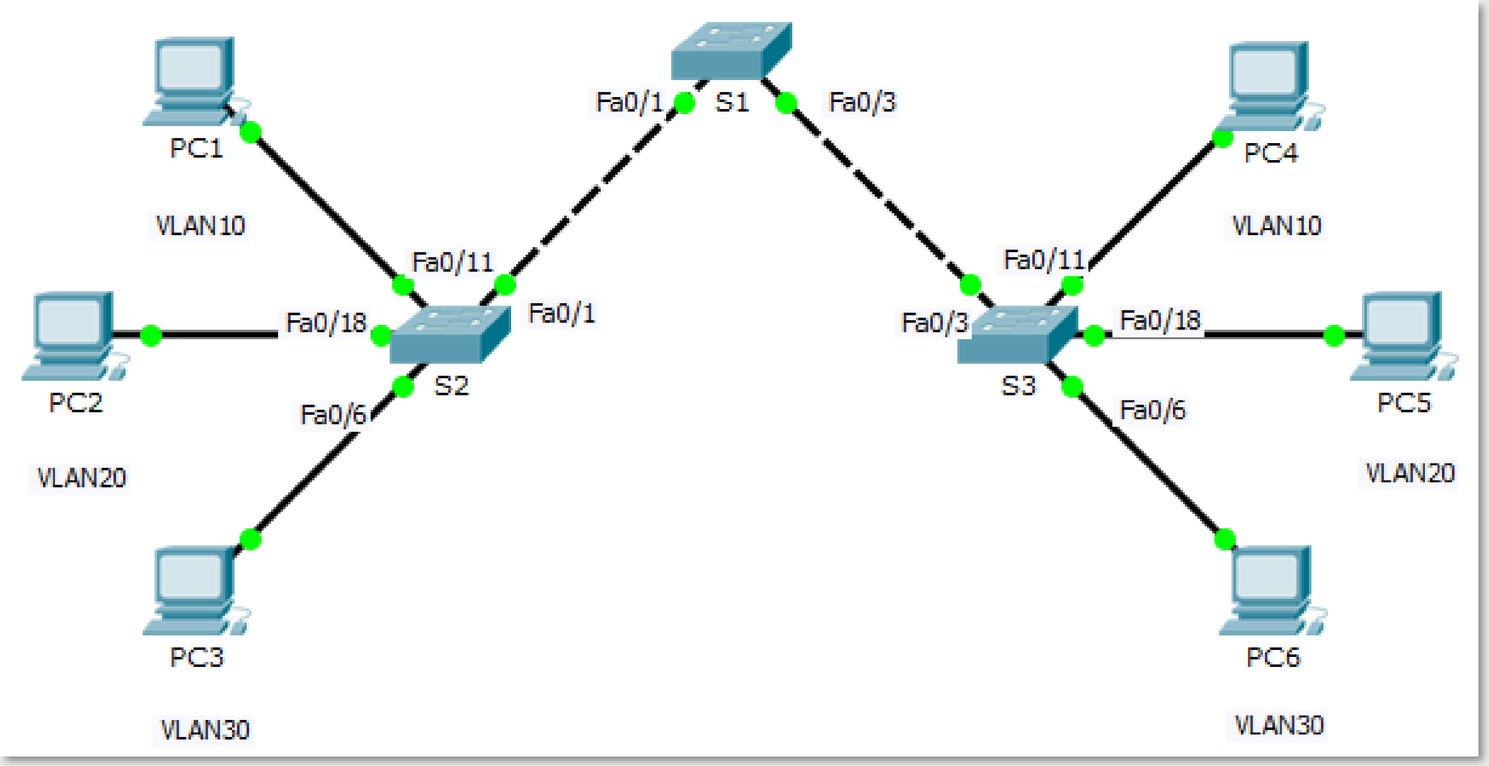
* `show dtp interface` - to determine current settings

```
Sw0(config-if)#switchport nonegotiate
```



Lab activity

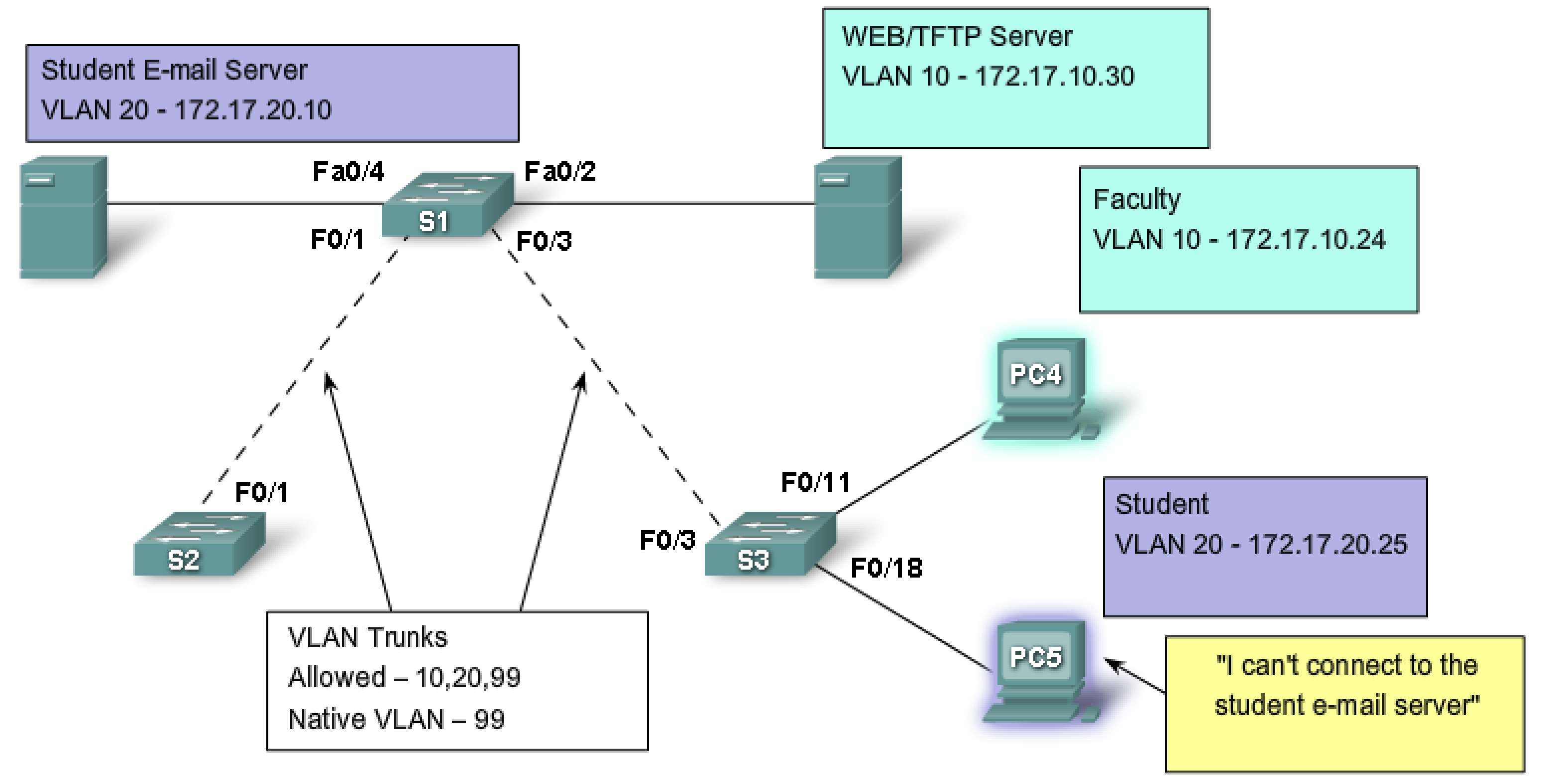
- Configuring VLANs



L

Troubleshooting

- Common problems
  - VLAN and IP subnets configuration
  - Native VLAN mismatches
  - Trunk mode mismatches
  - Allowed VLANs



Student E-mail Server
VLAN 20 - 172.17.20.10

WEB/TFTP Server
VLAN 10 - 172.17.10.30

Faculty
VLAN 10 - 172.17.10.24

Student
VLAN 20 - 172.17.20.25

VLAN Trunks
Allowed – 10,20,99
Native VLAN – 99

"I can't connect to the student e-mail server"

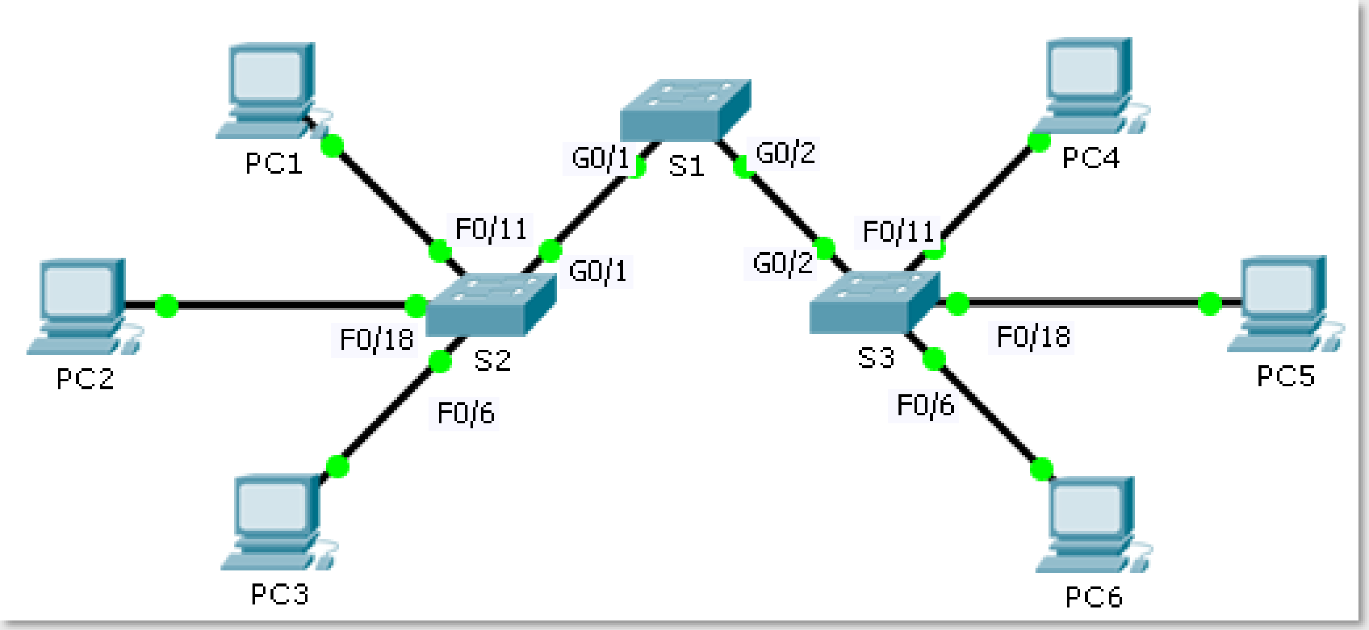
Multiple VLAN Registration Protocol

- Trunk configuration and management
  - **Static**. Allowed VLANs are statically configured per trunk port
  - **Dinamic**. Allowed VLANs are automatically determined by switches and communicated with each other over trunk links

- Dynamic configuration requires an inter-switch communication protocol
  - Proprietary: Cisco *Virtual Trunking Protocol (VTP)*
  - Standard: IEEE 802.1Q *Multiple VLAN Registration Protocol* (*MVRP*)

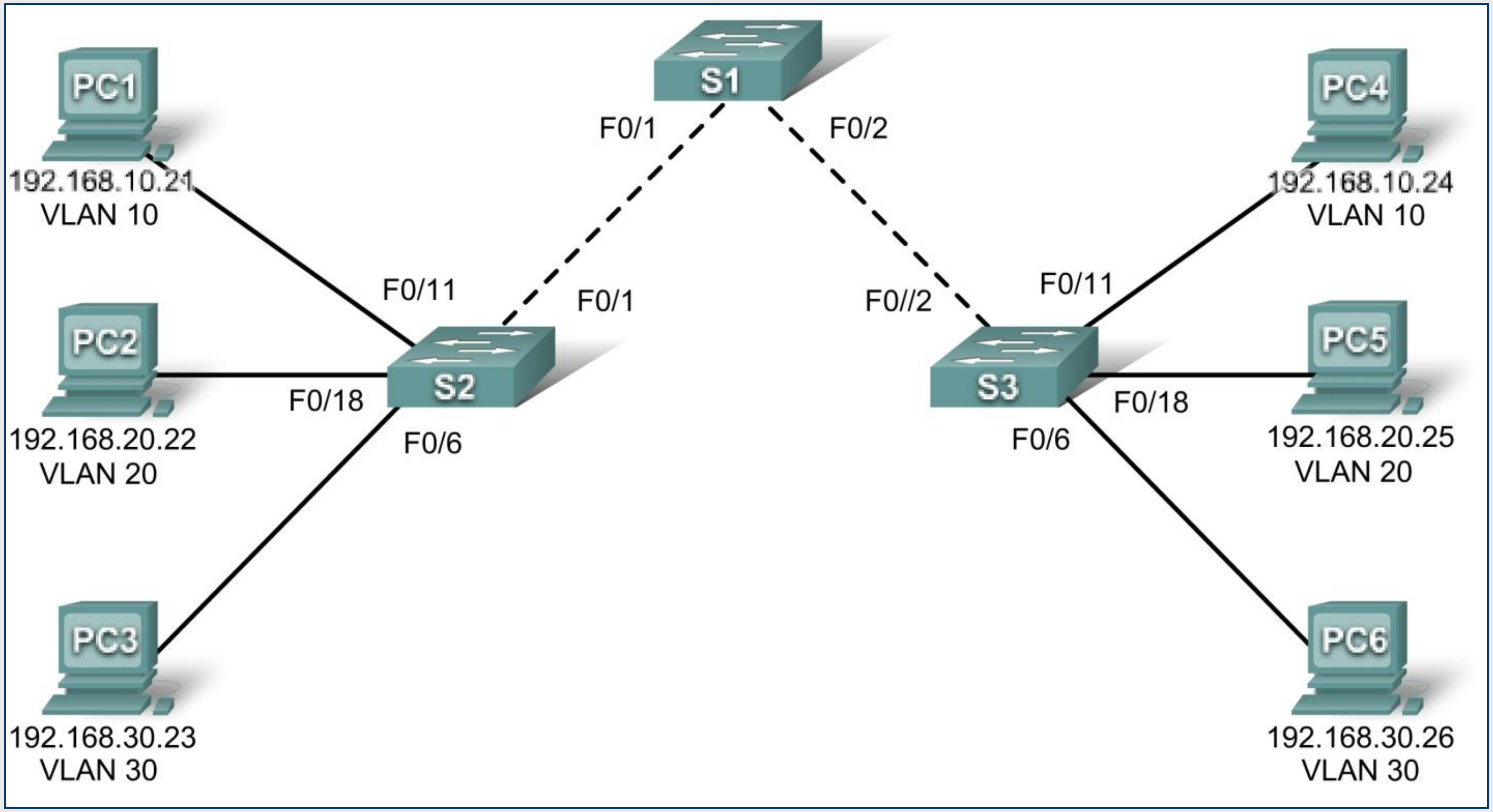
Lab activity

- Troubleshooting (1)



L

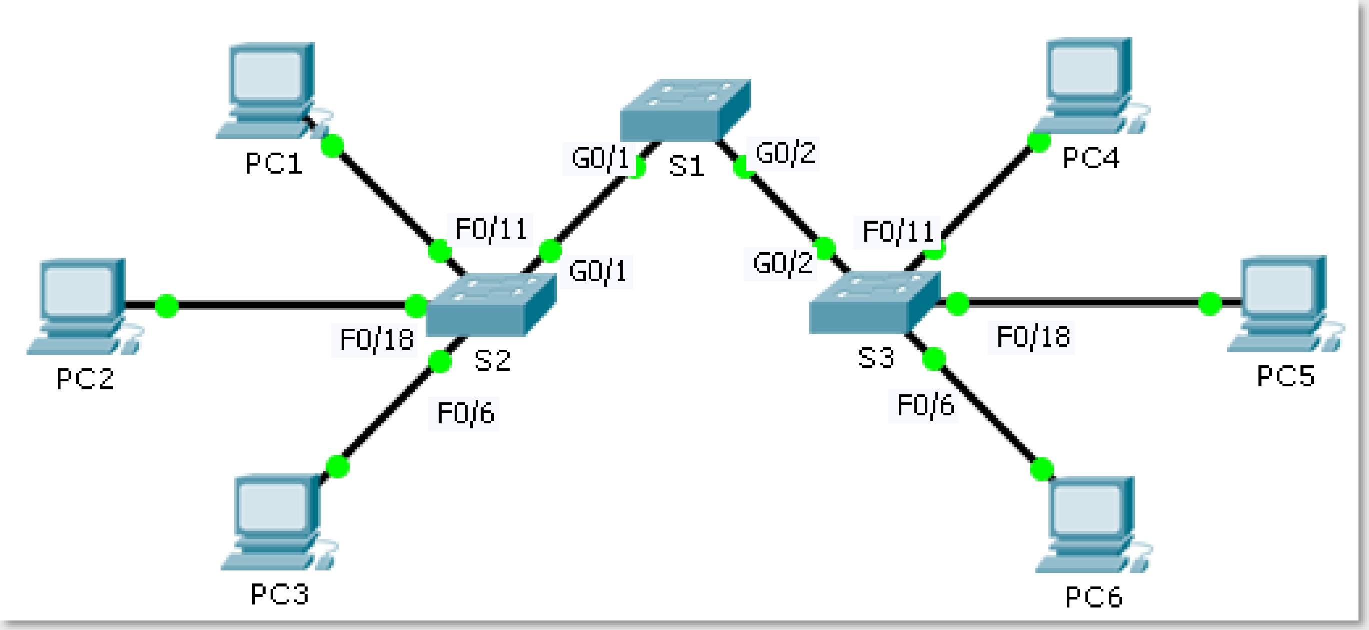
Lab activity



L

Lab activity

- Troubleshooting (2)



L