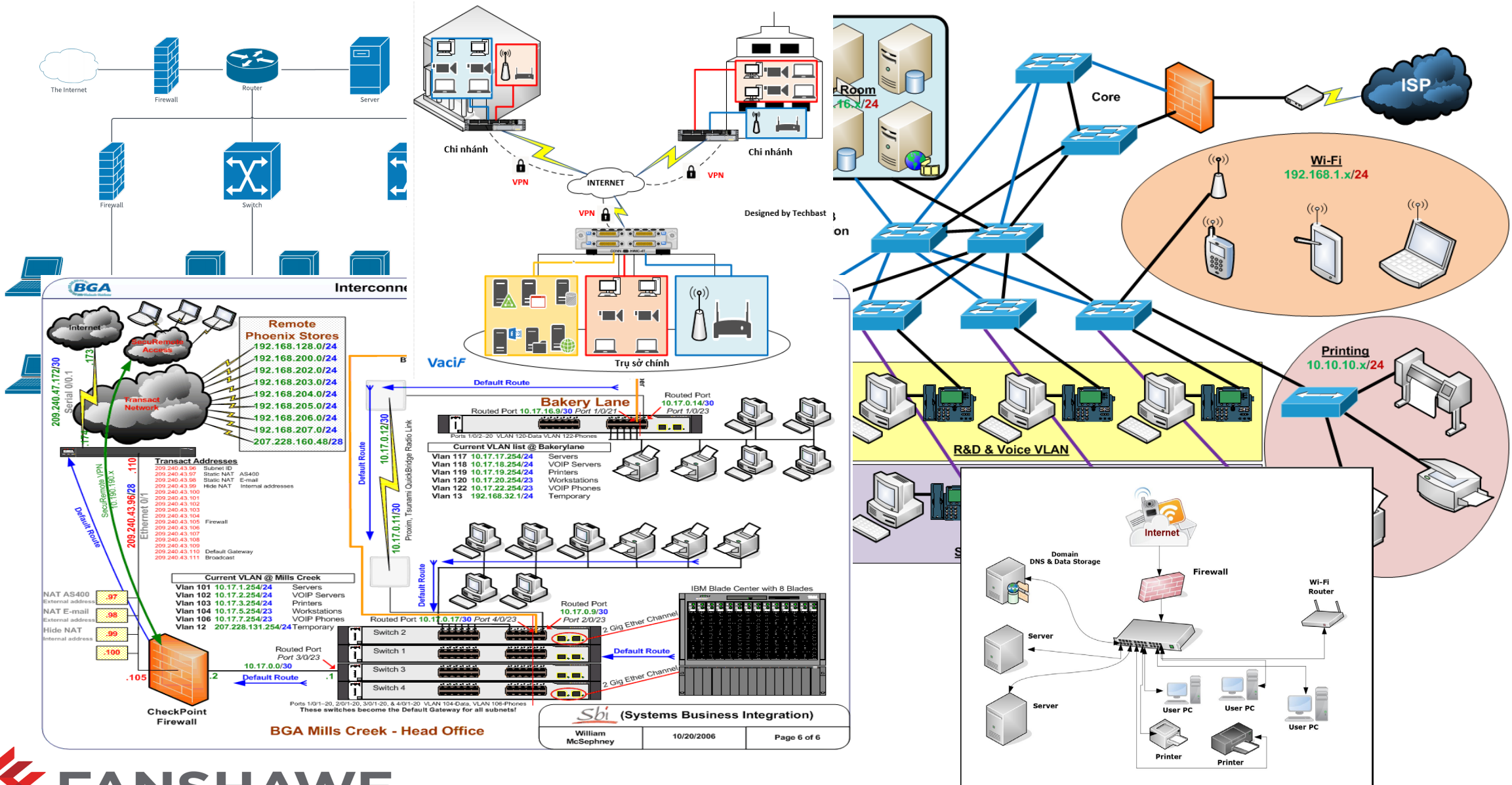


# VLANs



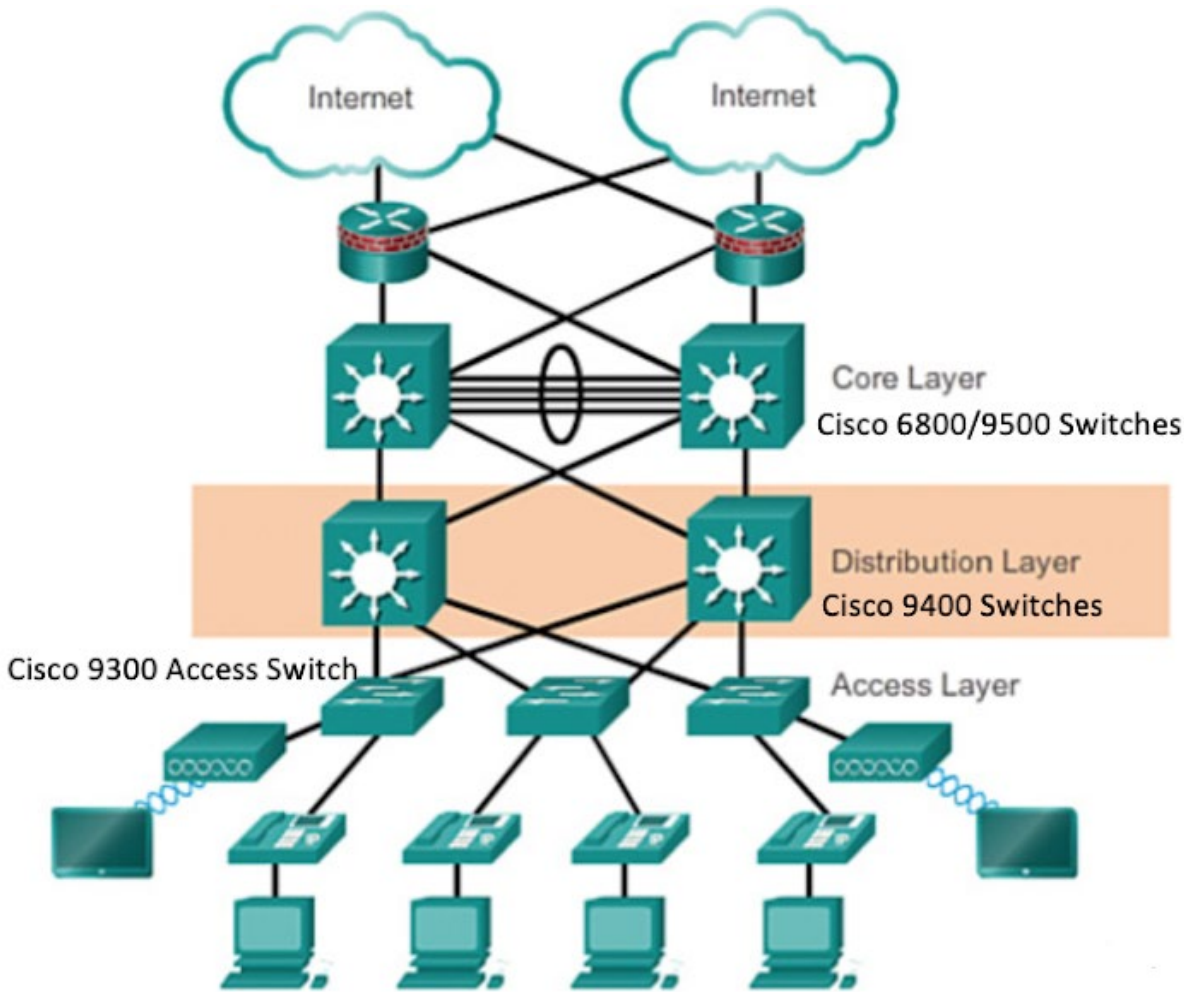
# House Keeping

INFO-6047 Switching and Routing					
ISM1 - Information Security Management (ISM1-ITY-20189) Detailed Weekly Content					
Week	Date of Lecture or Tests, 7:00 – 9:00 PM EST	Lecture/Test	Reading	Lab Time INFO-6047-01 Wednesday 5:00 – 8:00 PM EST INFO-6047-02 Tuesday 5:00 – 8:00 PM EST	Grade
Week 01	Monday, January 02, 2023	College-Wide Orientation			
Week 02	Monday, January 09, 2023	Introduction	N/A	Lab 01 - Basics of PT	3.0%
Week 03	Monday, January 16, 2023	Basics of Routing	Chapter 01 & 02 (Introduction to Networking, Network Media Copper)	Lab 02 - Intro to Routing	3.0%
Week 04	Monday, January 23, 2023	Basics of Switching	Chapter 03 & 04 (Network Media Fiber Network Media Wireless)	Lab 03 - Intro to Switching	3.0%
Week 05	Monday, January 30, 2023	VLANs	Chapter 05 (Data Encoding & Transmision)	Lab 04 - VLANs	3.0%
Week 06	Monday, February 06, 2023	Routing	Chapter 06 (Network OS & Comuncations)	Lab 05 - Routing	3.0%
Week 07	Monday, February 13, 2023	Mid-Term Test		Mid-Term (Test 1)	32.0%
Study Break	Monday, February 20, 2023	Study Break - No Class This Week			
Week 08	Monday, February 27, 2023	Inter-VLAN Routing	Chapter 10 (TCP/IP Fundamentals)	Lab 06 - Inter VLAN Routing	3.0%
Week 09	Monday, March 06, 2023	Static Routing	Chapter 11 (Subnetting)	Lab 07 - Static & Default Routs	3.0%
Week 10	Monday, March 13, 2023	Dynamic Routing - RIP	Chapter 12 (Additional Transmission Modalities)	Lab 08 - RIP Protocol	3.0%
Week 11	Monday, March 20, 2023	Dynamic Routing - OSPF	Chapter 14 (RA & LD Communications)	Lab 09 - OSPF Protocol	3.0%
Week 12	Monday, March 27, 2023	Access Control Lists	Chapter 15 (Network Security)	Lab 10 - ACLs	3.0%
Week 13	Monday, April 03, 2023	DHCP	Chapter 16 Maintaining the Network)	Lab 11 - DHCP	3.0%
Week 14	Monday, April 10, 2023	NAT	Chapter 17 (Troubleshooting Fundamentals of a Network)	Lab 12 - NAT	3.0%
Week 15	Monday, April 17, 2023	Final Test		Final Test (Test 2)	32%

Labs and quizzes will open Monday at 00:01 AM EST and the quiz will close Sunday at 23:59 PM EST.  
Tuesday Section-02 from 5:00 – 8:00 PM EST and Wednesday Section-01 from 5:00 – 8:00 PM EST

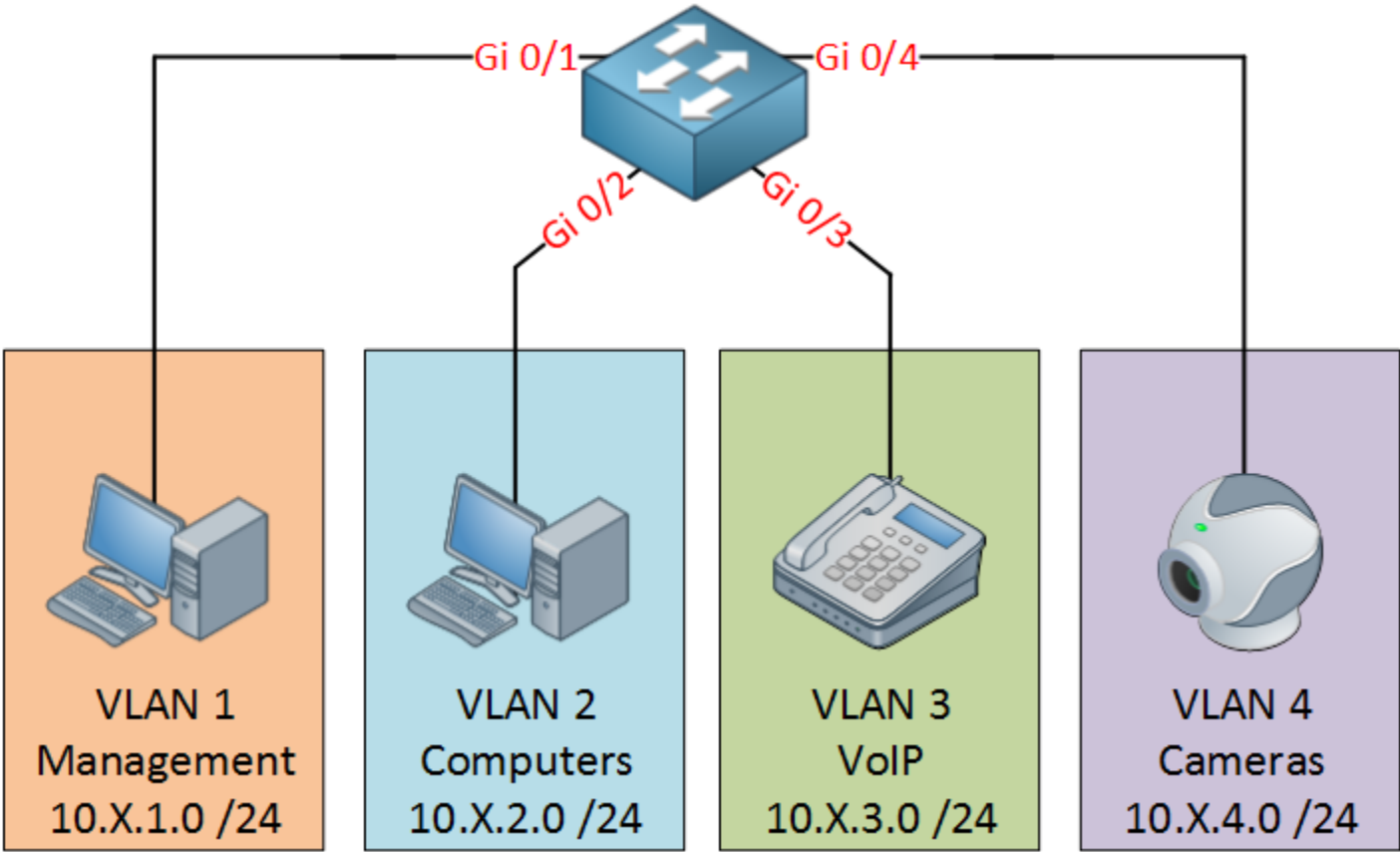
# Review - Lecture 03 – Basics of Switching

- Form Factor
- Ethernet Switches
  - Data Link Layer
  - Broadcast / Unicast
  - MAC Address Table
  - Switch Forwarding Methods
    - Cut-Through
    - Store & Forward
- Network Latency
  - Network Congestion
  - Alleviating Network Congestion
- Switching - Layer 2 / 3
- Switch Database Management (SDM)
- Basic commands



# Summary - VLANs

- Local Area Network (LAN)
- Solution using Routers
- Solution using VLANs
- VLANs
- Trunks
- Native VLAN
- Configure Trunk Port
- Configuring VLANs/Trunks
- DTP
- VLAN Security
- VLAN Design Guidelines
- LAB
- Quiz



# Local Area Network (LAN)

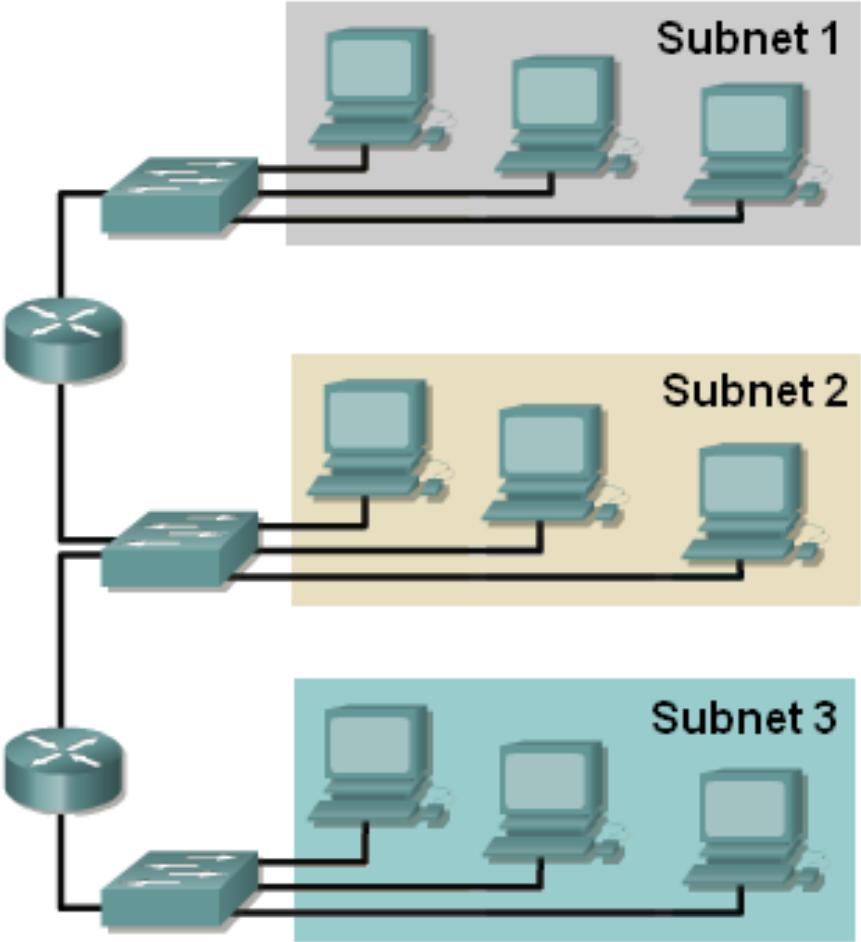
- For “Ethernet” some number of **addresses** are defined by a **MASK or CIDR**  
 $192.168.1.0/30 = 4 \text{ addresses (2 usable)}$   
 $192.168.1.16/28 = 16 \text{ addresses (14 usable)}$   
 $192.168.1.64/26 = 64 \text{ addresses (62 usable)}$   
 $192.168.1.0/24 = 256 \text{ addresses (254 usable)}$
- Split up broadcast domains to make better use of the bandwidth
- Groups users in the same department together for access to servers
- Security - restrict access by certain users to some areas of the LAN
- Provide a way for different areas of the LAN to communicate with each other

# Solution Using Routers

- Divide the LAN into subnets
- Use routers to link the subnets

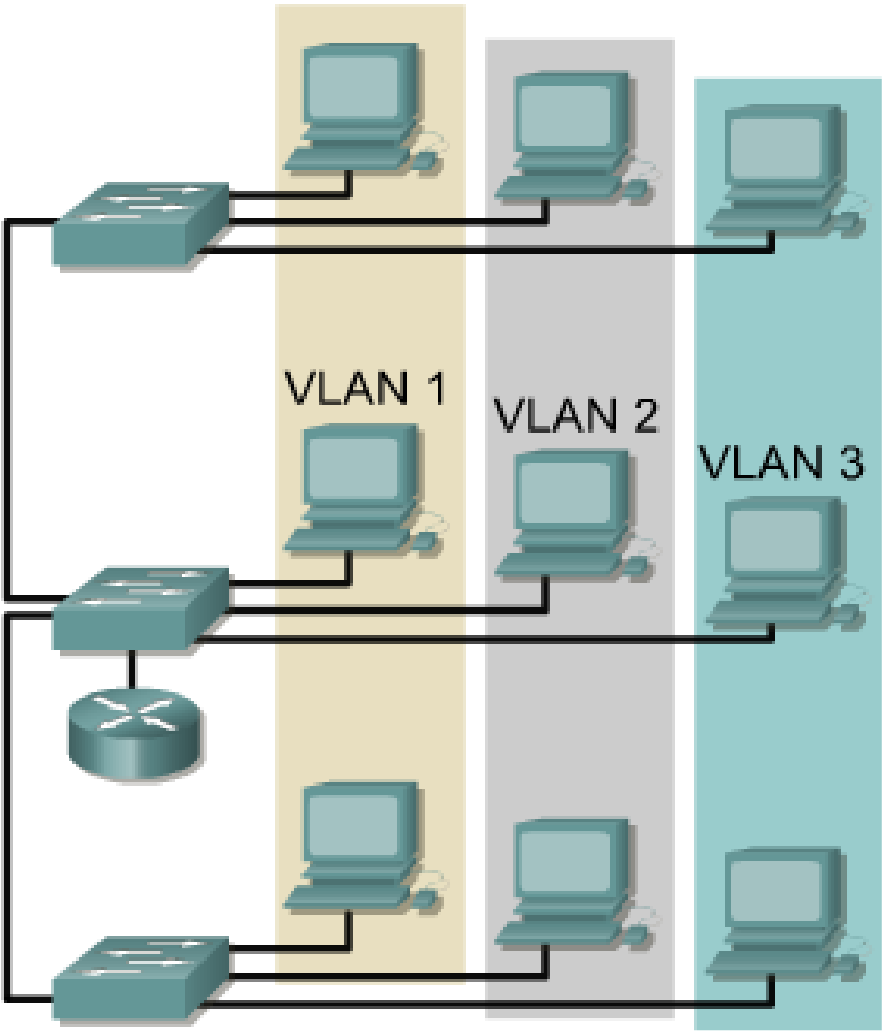
## BUT

- Routers are expensive
- Routers are slower than switches
- Subnets are restricted to limited physical areas
- Subnets are inflexible



# Solution Using VLANs

- Membership can be by function and not by location
- Managed by switches
- Router needed for communication between VLANs





# VLANs

- What is a VLAN
  - a logical partition of a Layer 2 network
  - a logically separate IP sub-network
- VLANs allow multiple IP networks and subnets to exist on the same switched network
- **For computers to communicate on the same VLAN, each must have an IP address and a subnet mask that is consistent for that VLAN**
- Each VLAN
  - is its own broadcast domain  
(packets can only be **routed** between different VLANs)



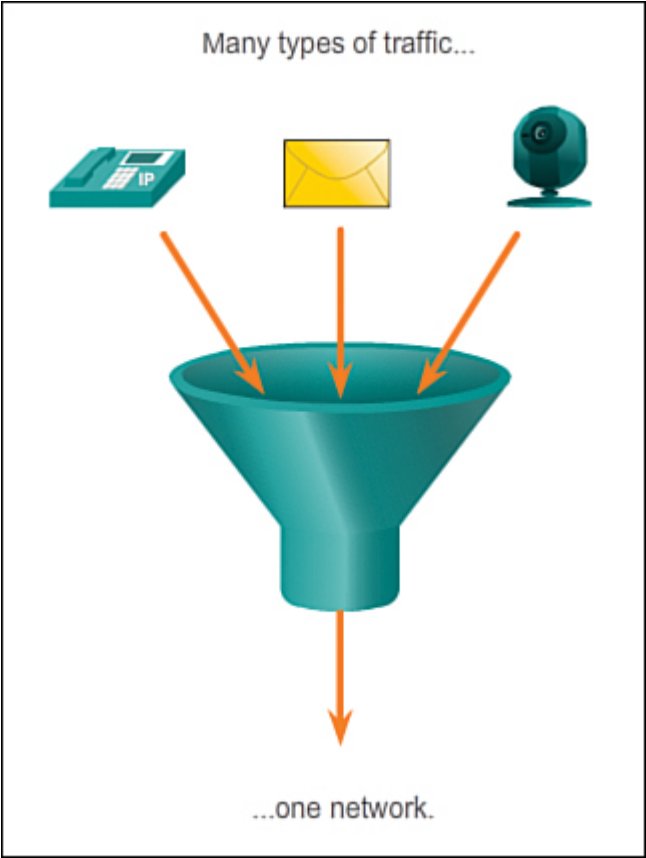
## VLAN Numbers

- VLANs are split into two categories:
  - **Normal range VLANs**
    - VLAN numbers from 1 to 1,005
    - VLAN 1: default Ethernet VLAN, all ports start in this VLAN
    - VLANs 1002 – 1005 automatically created for Token Ring and FDDI
  - **Extended Range VLANs**
    - VLAN numbers from 1,006 to 4,096
- Catalyst 2960 switch can have up to 255 VLANs
  - VLAN information is stored in the VLAN database, **vlan.dat** in the NVRAM memory of the switch

**NOTE:** Configuring Cisco devices, VLANs are **NOT** cleared with the **erase startup-config** command because all VLAN information is saved in the **vlan.dat** file. So, you will also need the **delete vlan.dat** command to set the system back to default values.

### VLAN Types

- Default VLAN
- Data or user VLAN
- Voice VLAN
- Management VLAN
- Native VLAN



## Default VLAN

- On Cisco devices, VLAN 1 is there by default
- Initially **all ports** are in VLAN 1
- Do not use VLAN 1 for data, voice, or management traffic for security reasons  
(you can only disable / shutdown VLAN 1. **You can not delete or rename it**)

VLAN 1

Default configuration, all interfaces in VLAN 1

A few predefined VLANs not normally used these days

```
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 to forward data by default.
- Native VLAN is VLAN 1 by default.
- Management VLAN is VLAN 1 by default.
- VLAN 1 cannot be renamed or deleted.

## Data VLAN

- Carry files, e-mails, shared application traffic, most user generated traffic
- Separate VLAN for each group of users is possible (segmentation)

## Port Based – Static (Port Centric)

- Each switch port intended for an end device is configured to belong to a VLAN
- Any device connecting to that port belongs to the port's VLAN
- There are other ways of assigning VLANs but this is the usual way
- These are called access ports

Port Based – Static (Port Centric) (continued)


```
S3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#interface fastEthernet0/18
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 20
S3(config-if)#end
```

- If VLAN 20 did not exist before –then it does now

Switch#sho vlan

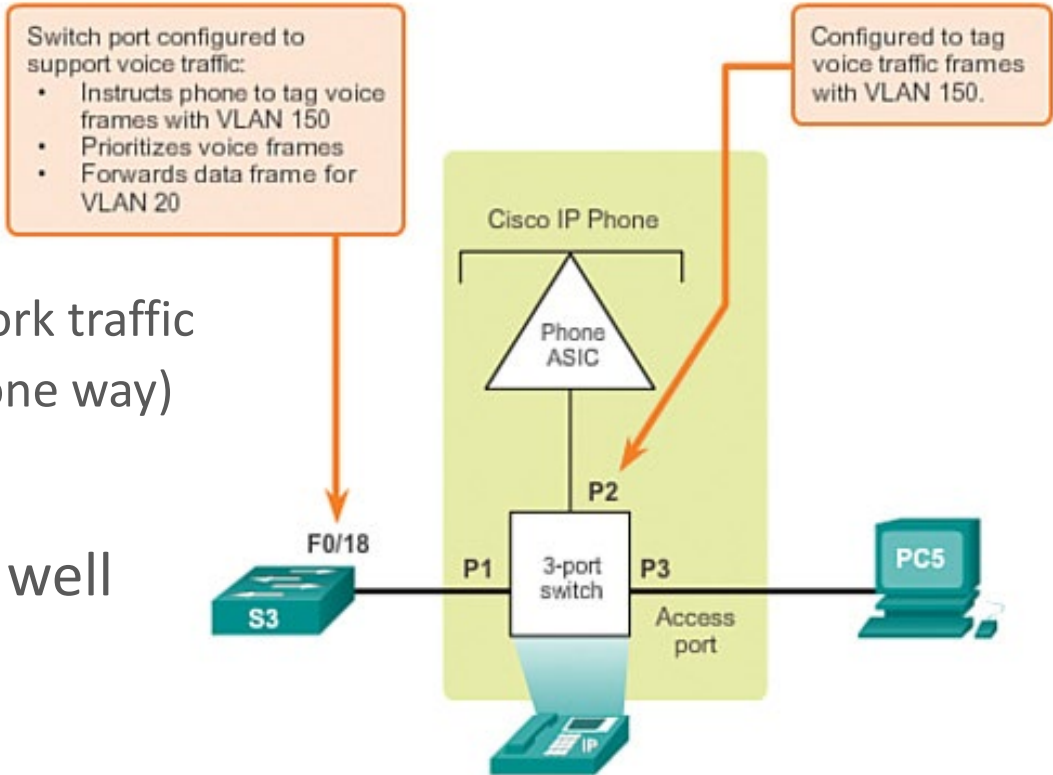
VLAN Name		Status	Ports
-----			-----
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
20	VLAN0020	active	Fa0/18
-----			-----

Default name



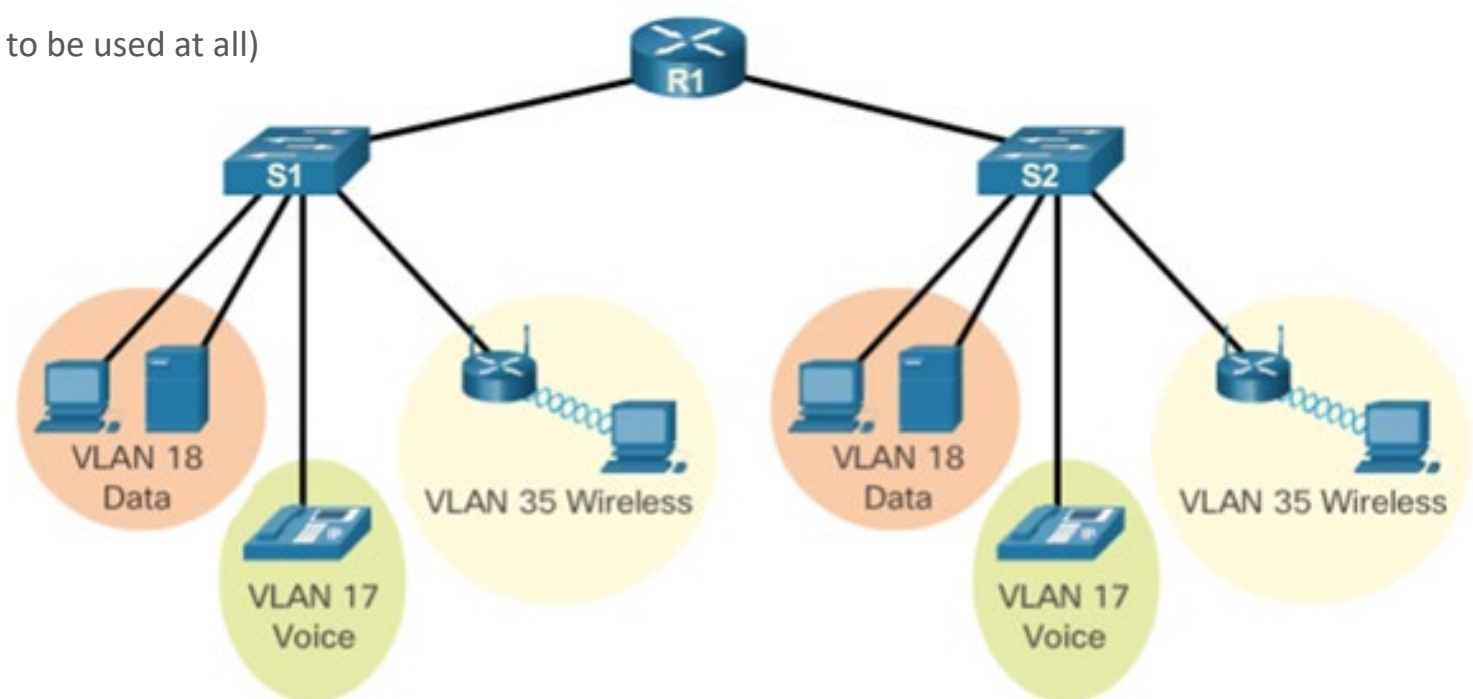
Voice VLAN

- VoIP traffic is time-sensitive and requires:
  - Ensured bandwidth to ensure voice quality
  - Transmission priority over other types of network traffic
  - Delay of less than 150ms across the network (one way)
- Use with IP phone
- Most but not all phones acts as a switch as well  
(3 port switch, one port to the switch (S3) one port to the PC (PC5)  
one internal port for the phone communication)
- Voice traffic is tagged, given priority
- Data not tagged, no or lower priority



Management VLAN

- Assign IP address
- Used for telnet/SSH or web access for management purposes
- By default, VLAN1 - for security reasons is best not to be used as management VLAN (best not to be used at all)





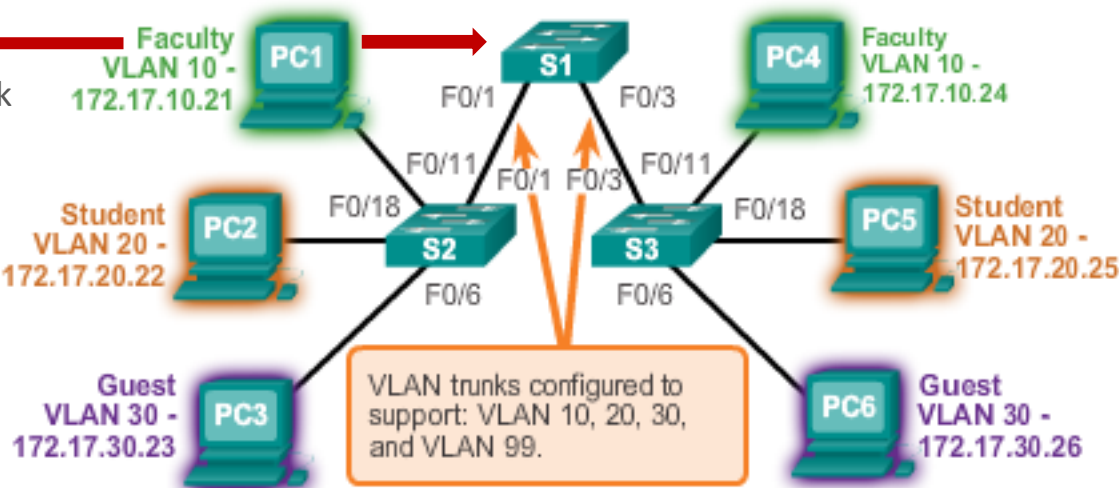
# Trunks

- Carries traffic for more than one VLAN on one cable
- Does not belong to a specific VLAN (but can)
- Uses a tag to identify the VLAN
- Cisco uses two types of trunking
  - 802.1q (International standard)
  - Cisco ISL (InterSwitch Link, Cisco proprietary)

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  
VLAN 99 Management and Native - 172.17.99.0/24

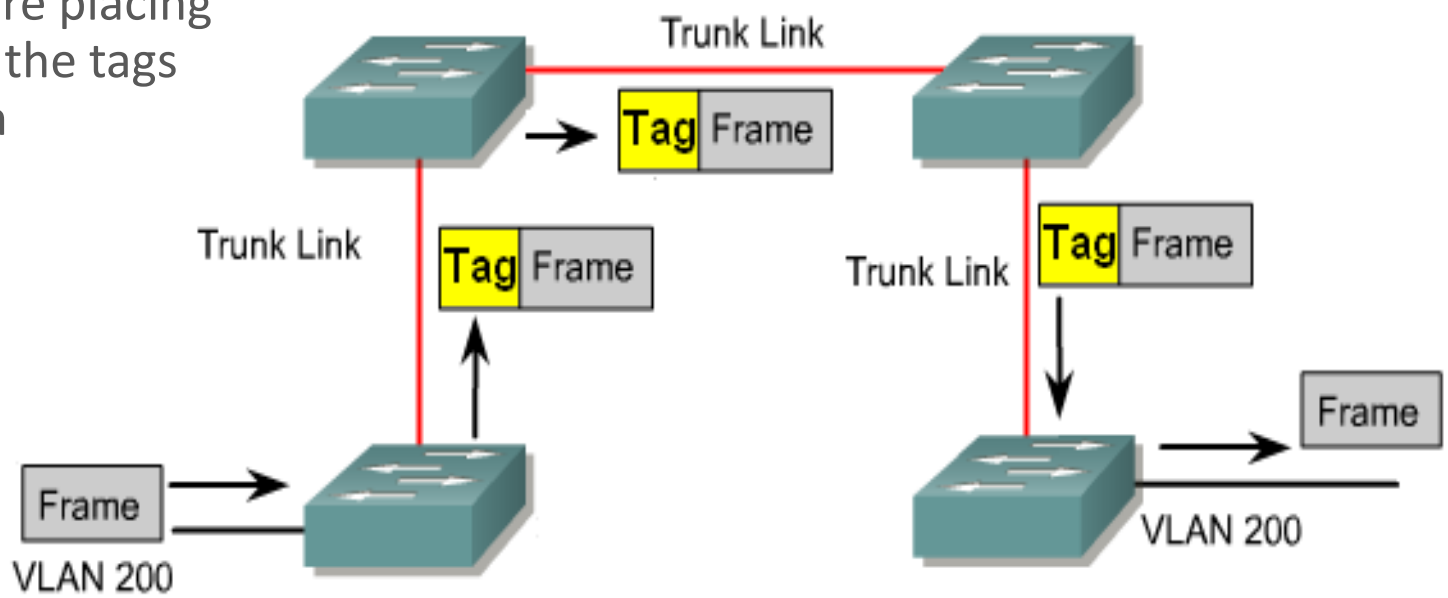
F0/1-5 are 802.1Q trunk interfaces with native VLAN 99.  
F0/11-17 are in VLAN 10.  
F0/18-24 are in VLAN 20.  
F0/6-10 are in VLAN 30.

All VLANs must be created on S1, even if not assigned to ports, this is needed for the trunks to work



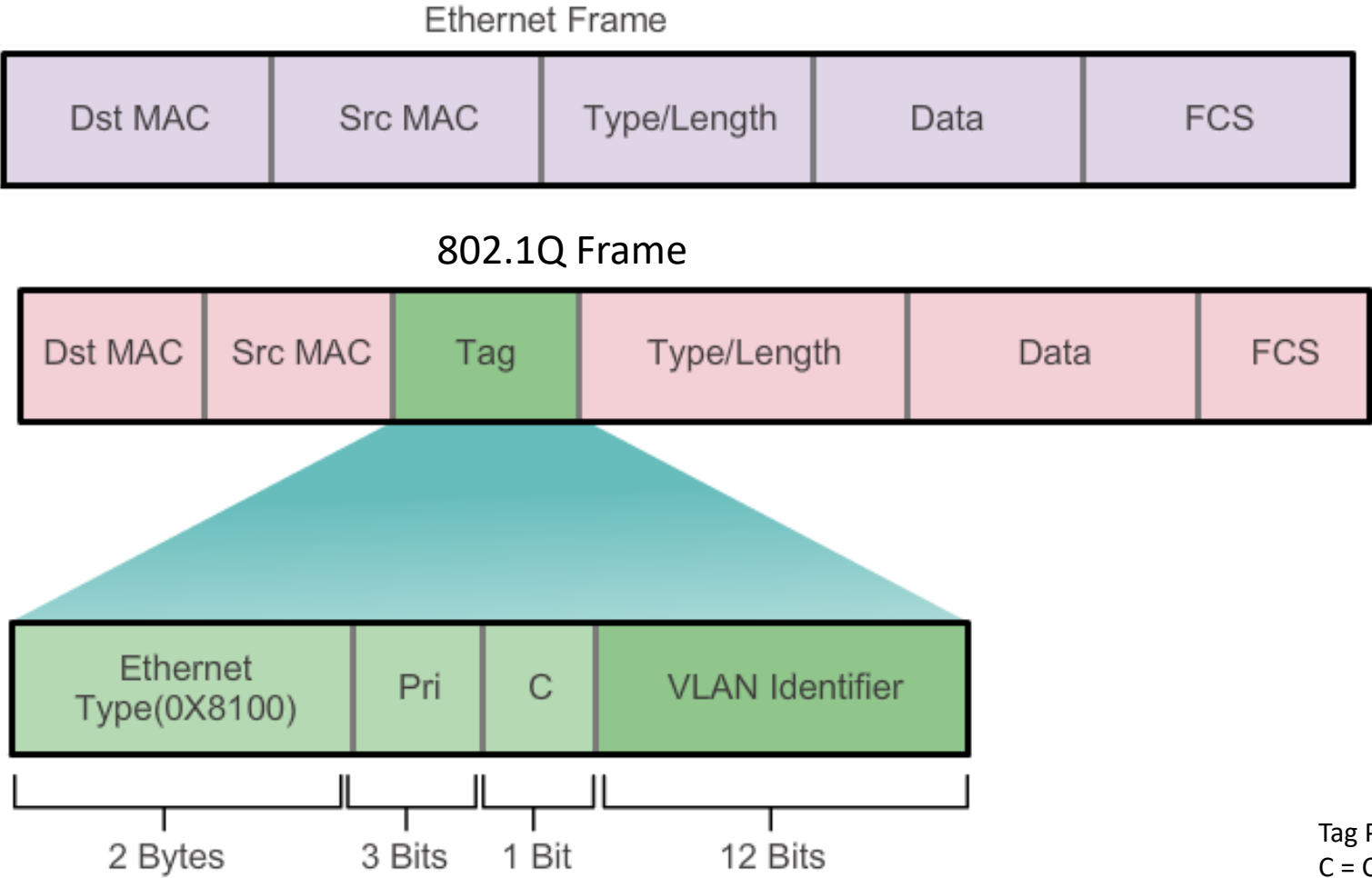
## Tag to Identify VLAN

- **Frame tagging** is the process of adding a VLAN identification header to the Ethernet frame
- Used to transmit multiple VLAN frames through a trunk link
- Switches will tag frames to identify which VLAN that traffic belong to
  - Different tagging protocols exist; IEEE 802.1Q , Cisco ISL
  - The protocol defines the structure of the tagging header added to the frame
- Add VLAN tags to the frames before placing them into trunk links and remove the tags before forwarding frames through nontrunk (access) ports
- Added to the frame when it goes on to the trunk
- Removed when frame leaves the trunk



# Trunks (continued)

## Frame Tagging IEEE 802.1Q



Tag Protocol Identifier  
C = Canonical Format Indicator  
Pri = Priority  
VLAN identifier

# Native VLAN

- Frames that belong to the native VLAN are not tagged
- Untagged frames received on a trunk port are forwarded on to the native VLAN
- In Cisco switches, the native VLAN is VLAN 1, by default
- Switch will drop tagged frames received from the native VLAN
  - This can happen if non-Cisco devices are connected

## Configure Trunk Port

- Configure a trunk port and tell it which VLAN is the native VLAN (if not VLAN 1)
  - **SW-1(config)# int fa0/1**
  - **SW-1(config-if)# switchport mode trunk**
  - **SW-1(config-if)# switchport trunk native vlan 99**
- By default, native VLAN is VLAN 1  
(you should be able to see this in the labs we do)
- Different switches have ports in different default configurations, this means you may have to use a different set of commands to hard code a port as a trunk  
(our L2 and L3 switches, in our labs, use different sets of commands to hard coded trunks)

# Configuring VLAN/Trunks

## Create a VLAN

- Assign switchports to VLANs statically
- Verify VLAN configuration
  1. Does it have a name?
  2. Assigned to ports?
  3. Is the interface up?
- Enable trunking on inter-switch/router connections
- Verify trunk configuration

## Creating a VLAN (continued)

```
SW-1(config)# vlan 20
SW-1(config-vlan)# name student
-----
SW-1(config)# interface fastethernet 0/18
SW-1(config-if)# switchport mode access
SW-1(config-if)# switchport access vlan 20
-----
SW-1(config)# interface vlan 20
SW-1(config-if)# ip address x.x.x.x m.m.m.m
SW-1(config-if)# no shutdown
```

Step 1. Start by giving the VLAN a name.

Step 2. Assign the VLAN to one or more ports.

Step 3. Make sure the VLAN is up and running, this is where you can also assign an IP address if you need to.  
x.x.x.x = IP address  
m.m.m.m = Mask

- VLAN will be saved in the VLAN database (vlan.dat) rather than running-config or startup-config files.
- If you do not give the VLAN a name, (step one above) then the name will be auto created as “VLAN0020” in this case for VLAN 20.



# Configuring VLAN/Trunks (continued)

## Creating a VALN (continued)

Creating VLAN 20 and assigning it to port fa0/18

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#no vlan 20
S1(config)#no vlan 18
S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

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, Fa0/11, Fa0/12
                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                   Fa0/17, Fa0/19, Fa0/20, Fa0/21
                                   Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                   Gig0/2

1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default        active
1005 trnet-default          active
S1#
```

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#inter f 0/18
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
sh vlan br

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, Fa0/19, Fa0/20, Fa0/21
                                   Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                   Gig0/2

18   VLAN0018              active
20   VLAN0020              active    Fa0/18
1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default        active
1005 trnet-default          active
S1#
```

gone

Deleting VLAN 18 and 20

Where did port fa0/18 go?

# Configuring VLAN/Trunks (continued)

## Verifying VLAN Information

show interface fa0/18 switchport

show VLAN name student

show interface VLAN 20

```
S1#show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
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 Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
```

```
S1# show interfaces vlan 20
vlan20 is up, line protocol is down
Hardware is Ethernet, address is 001c.57ec.0641
001c.57ec.0641)
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/2
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes);
drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicast)
0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
```

```
S1# show vlan name student

VLAN Name
-----
20      student

VLAN Type SAID MTU Parent RingNo
-----
20      enet 100020 1500 -      -

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#
```

Show VLAN brief

```
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, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/19, Fa0/20, Fa0/21
Fa0/22, Fa0/23, Fa0/24, Gig0/1
Gig0/2
1002 fddi-default      active
1003 token-ring-default      active
1004 fddinet-default      active
1005 trnet-default      active
S1#
```



## Deleting VLAN Database

**Sw-1# erase startup-config** does not get rid of any VLAN information that has been saved.

```
sw-1#dir
Directory of flash:/

 1  -rw-     4414921      <no date>  c2960-lanbase-mz.122-25.FX.bin
 3  -rw-         3076      <no date>  config.text
 2  -rw-          796      <no date>  vlan.dat

64016384 bytes total (59597591 bytes free)
```

Saved configuration  
Saved VLAN configuration

## Sw-1# delete vlan.dat

Delete filename [vlan.dat]? **↵Enter**  
Delete flash:/vlan.dat? [confirm] **↵Enter**  
(%Error deleting flash:/vlan.dat (No such file or directory)) **↵** may get this if there is no “vlan.dat” file  
After the **reload** command (and following the on-screen instructions)

- Switch goes back to the default with all ports in VLAN 1
- You cannot delete VLAN 1

## Configuring a Trunk

- Configuring IEEE 802.1q Trunk

Layer 2 switch trunk configuration

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# <b>configure terminal</b>
Enter interface configuration mode.	S1 (config)# <b>interface interface_id</b>
Force the link to be a trunk link.	S1 (config-if)# <b>switchport mode trunk</b>
Specify a native VLAN for untagged 802.1Q trunks.	S1 (config-if)# <b>switchport trunk native vlan vlan_id</b>
Specify the list of VLANs to be allowed on the trunk link.	S1 (config-if)# <b>switchport trunk allowed vlan vlan-list</b>
Return to the privileged EXEC mode.	S1 (config-if)# <b>end</b>

Layer 3 switch trunk configuration adds this one line

**switchport trunk encapsulation dot1q**

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



# Configuring VLAN/Trunks (continued)

## 802.1Q Trunk Verification

show interface f0/1 switchport

show interface trunk

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 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)
Administrative Native VLAN tagging: enabled
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 Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

```
Switch(config-if)#do sh inter trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     on        802.1q         trunking    99

Port      Vlans allowed on trunk
Fa0/1     10,20,30

Port      Vlans allowed and active in management domain
Fa0/1     10,20,30

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     10,20,30

Switch(config-if)#
```

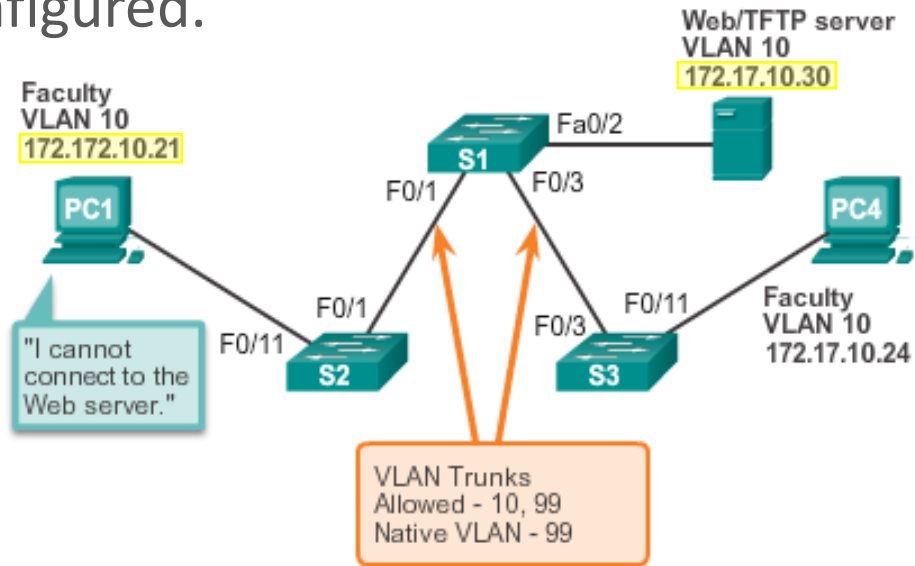
- Only interface that have a “Status – UP” and “Protocol – UP” will be seen in the output of the **show interface trunk**
- Shows the Encapsulation mode
- Shows the VLANs attached to the trunk

(see the **show ip interface brief** command)

# Configuring VLAN/Trunks (continued)

## IP Addressing issues with VLANs

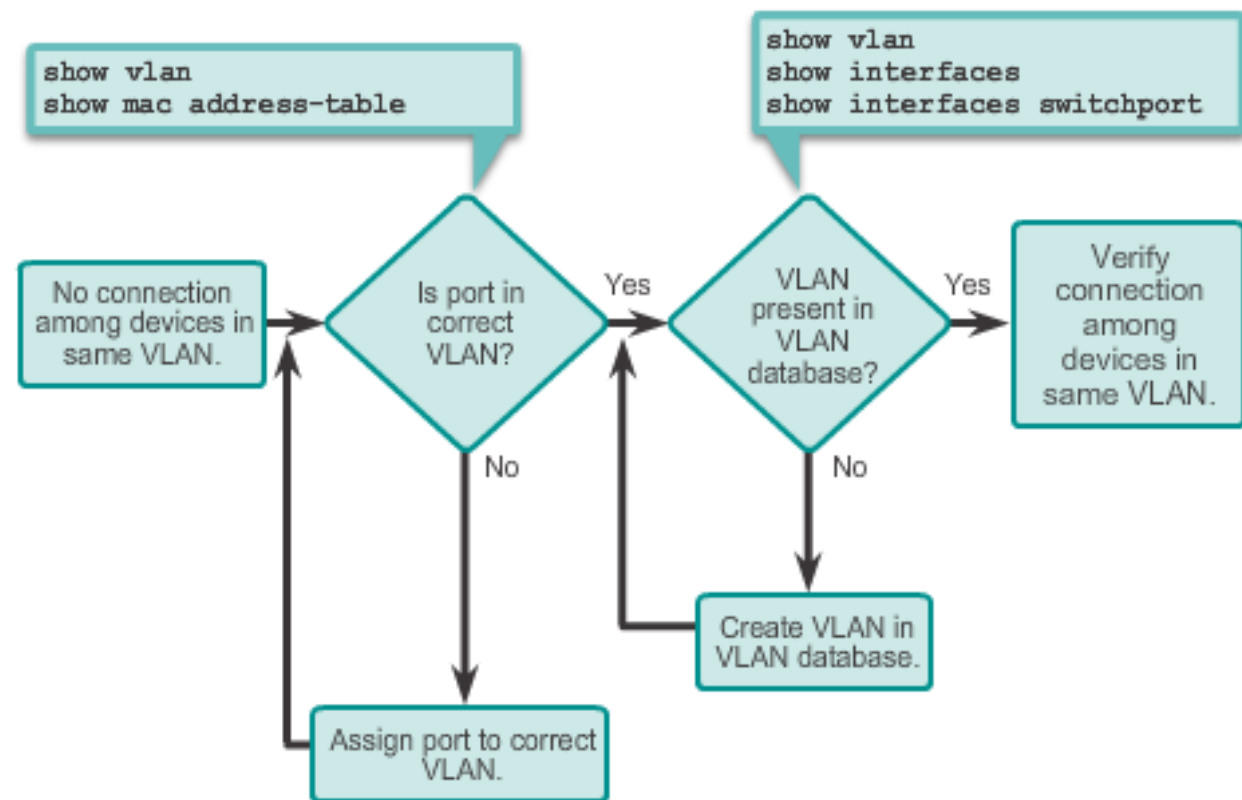
- It is a common practice to associate a VLAN with an IP network.
- Because different IP networks only communicate through a router, all devices within a VLAN must be part of the same IP network to communicate.
- The figure displays that PC1 cannot communicate to the server because it has a wrong IP address configured.



# Configuring VLAN/Trunks (continued)

## Missing VLANs

- If all of the IP address mismatches have been solved, but the device still cannot connect check if the VLAN exists in the switch.





# Dynamic Trunking Protocol (DTP)

## Introduction to Dynamic Trunking Protocol (DTP)

- Switch ports can be manually configured to form trunks
- Switch ports can also be configured to negotiate and establish a trunk link with a connected peer
- The **Dynamic Trunking Protocol (DTP)** manages trunk negotiation
- If the port on the neighbor switch is configured in trunk mode that supports DTP, it manages the negotiation
- DTP is a Cisco proprietary protocol, and it is enabled by default

## Negotiated Interface Modes

- Cisco Catalyst 2960 & 3560 support the following trunk modes:
  - switchport mode dynamic auto
  - switchport mode dynamic desirable
  - switchport mode trunk
  - switchport nonegotiate
- The default DTP configuration for Cisco Catalyst 2960 and 3560 switches is **dynamic auto**
  - **This can cause problems**

Negotiated Interface Modes <sub>(Continued)</sub>

- Two switches set to dynamic auto will not form a trunk
- Best to set trunk manually (at lest one end)
  - Sw-1(config-if)# switchport trunk encapsulation dot1q (needed on a Multilayer (L3) Switch)
  - Sw-1(config-if)# switchport mode trunk

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited connectivity
Access	Access	Access	Limited connectivity	Access

## Trunk Mode Mismatches

- If a port on a trunk link is configured with a trunk mode that is incompatible with the neighbouring trunk port, a trunk link fails to form between the two switches
- Use the **show interfaces trunk** command to check the status of the trunk ports on the switches
- To fix the problem, configure the interfaces with proper trunk modes
  - `Switch(config-if)# switchport trunk encapsulation dot1q` (needed on a Multilayer (L3) Switch)
  - `Switch(config-if)# switchport mode trunk`

## Common Problems with Trunks

- Trunking issues are usually associated with incorrect configurations
- The most common type of trunk configuration errors are:
  1. Native VLAN mismatches - both ends must have the same native VLAN
  2. Trunk mode mismatches - both ends must be configured with trunking on or use DTP to negotiate a trunk with the other end
  3. Allowed VLANs on trunks - the same VLANs must be allowed on the trunk at both ends

# VLAN Security

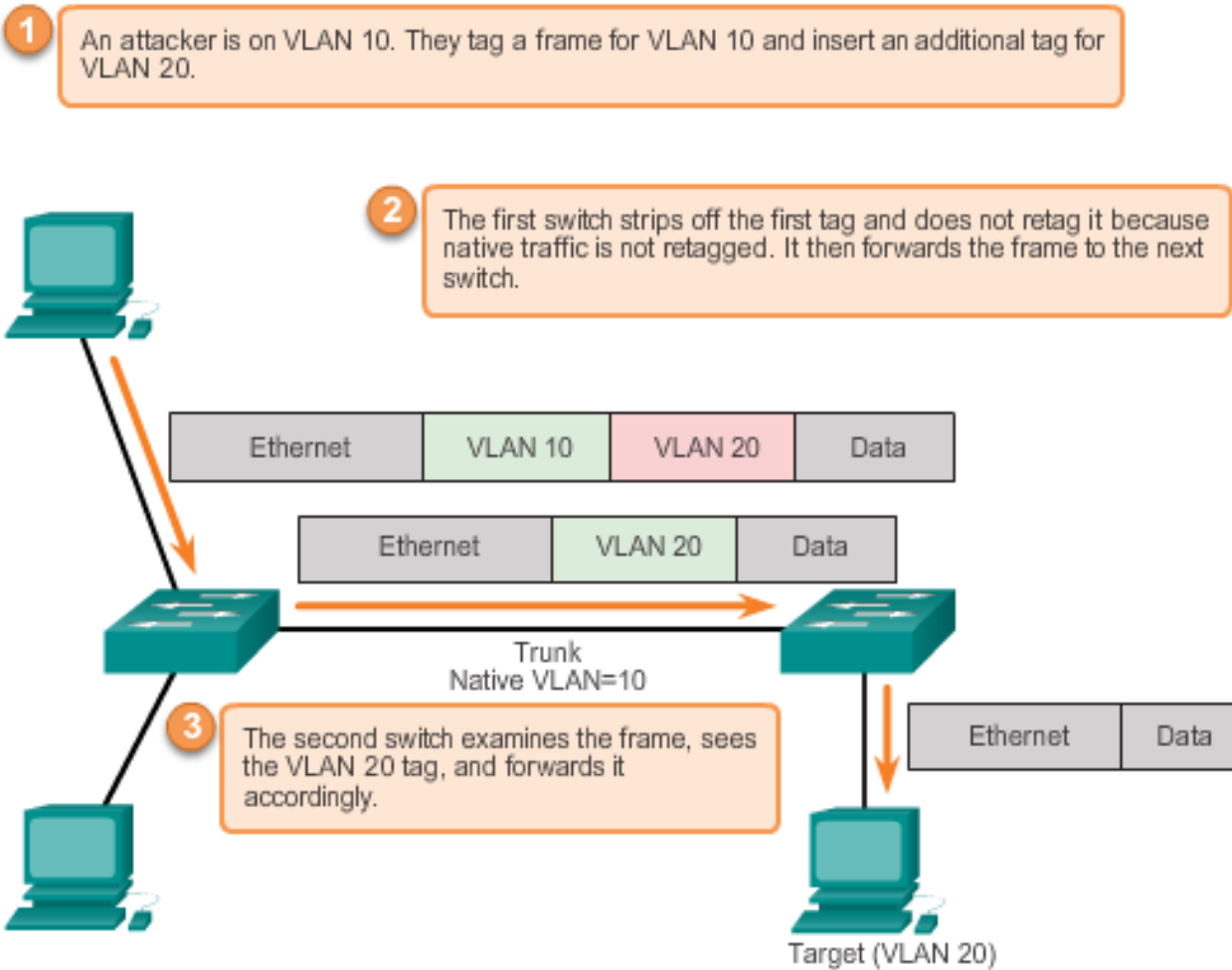
## Switch Spoofing Attack

- There are several different types of VLAN attacks
- Default configuration of the switch port is dynamic auto
- Configuring a host to act as a switch and form a trunk - attacker could gain access to any VLAN in the network
- Attacker is now able to access other VLANs - called a VLAN hopping attack
- Turn off trunking on all ports, except the ones that specifically require trunking

## Double-Tagging Attack

- Double-tagging attack takes advantage of the way that most switches de-encapsulate 802.1Q tags
- Most switches perform only one level of 802.1Q de-encapsulation, allowing an attacker to embed a second, unauthorized attack header in the frame
- After removing the first and legitimate 802.1Q header, the switch forwards the frame to the VLAN specified in the unauthorized 802.1Q header
- To mitigating double-tagging attacks ensure that the native VLAN of the trunk port is different from the VLAN of any user ports

## Double-Tagging Attack (continued)



## VLAN Design Guidelines

- Move all ports from VLAN 1 and assign them to appropriate VLAN
- Shut down all unused switch ports
- Separate management and user data traffic
- Change the management VLAN to a VLAN other than VLAN 1 (preference is VLAN 99) and same for the native VLAN
- Ensure that only devices in the management VLAN can connect to the switches
- The switch should only accept SSH connections
- Disable auto negotiation on trunk ports
- Do not use the auto or desirable switch port modes



- Read the LAB **from start to finish!**

- **Note:** I'm not repeating things from the last few weeks anymore, the labs will say do the Basic system setup, this week is about VLANs, and it will have detailed instruction, but in future labs the instructions will just say create VLANs x, y, and z

- Do the steps of the lab **in order!**

- Optional - Fill in the PowerPoint slides, in order and during the lab, at the appropriate point in time where indicated in the labs!

- Yes, this requires you to download all the stuff from FOL

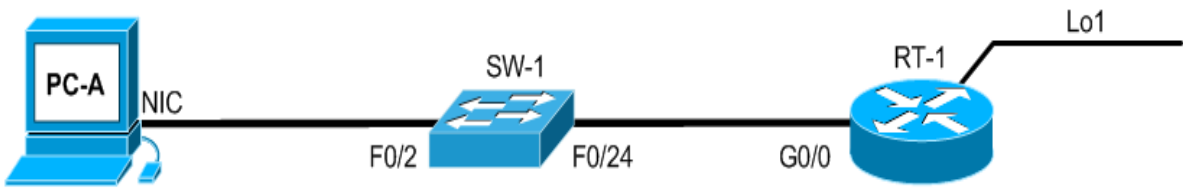
- The lab
  - Optional - The PowerPoint template
  - Any scripts in the "Lab" section
  - ect....

You should download each week's content in FOL to a separate folder on your computer. This becomes part of your study guide when exam time comes around.

# LAB (continued)

## This weeks Lab

- Is about **VLANs**... (a property usually found in a switch)
  - But look at all the router configuration....
  - Checkout the Lab section of FOL for this week. See that there is a file “RT-1.txt”.
  - Open the text file in a text only tool, highlight and copy the content, then paste it into the router in your PT file that was also supplied in FOL this week.
  - I will do this from time to time so that you can focus on the subject for this week.



Device	interface	IP Address	Subnet Mask	Default Gateway	Ports	Vlan name
RT-1	G0/0	no address				
	G0/0.10	192.168.10.254	/24			
	G0/0.20	192.168.20.254	/24			
	G0/0.30	192.168.30.254	/24			
	G0/0.99	192.168.1.254	/24			
	Lo1	10.10.10.10	/32			
SW-1	Vlan 10				1 - 6	Student
	Vlan 20				7 - 12	Faculty
	Vlan 30				13 - 18	Server
	Vlan 99	192.168.1.253	/24	192.168.1.254	19 - 23	Mgmt
	Trunk				24	
PC-A	NIC	DHCP	DHCP	DHCP		

# Quiz

## This weeks quiz

- Contains questions on the lecture, lab, and chapter 05.

# QUESTIONS

