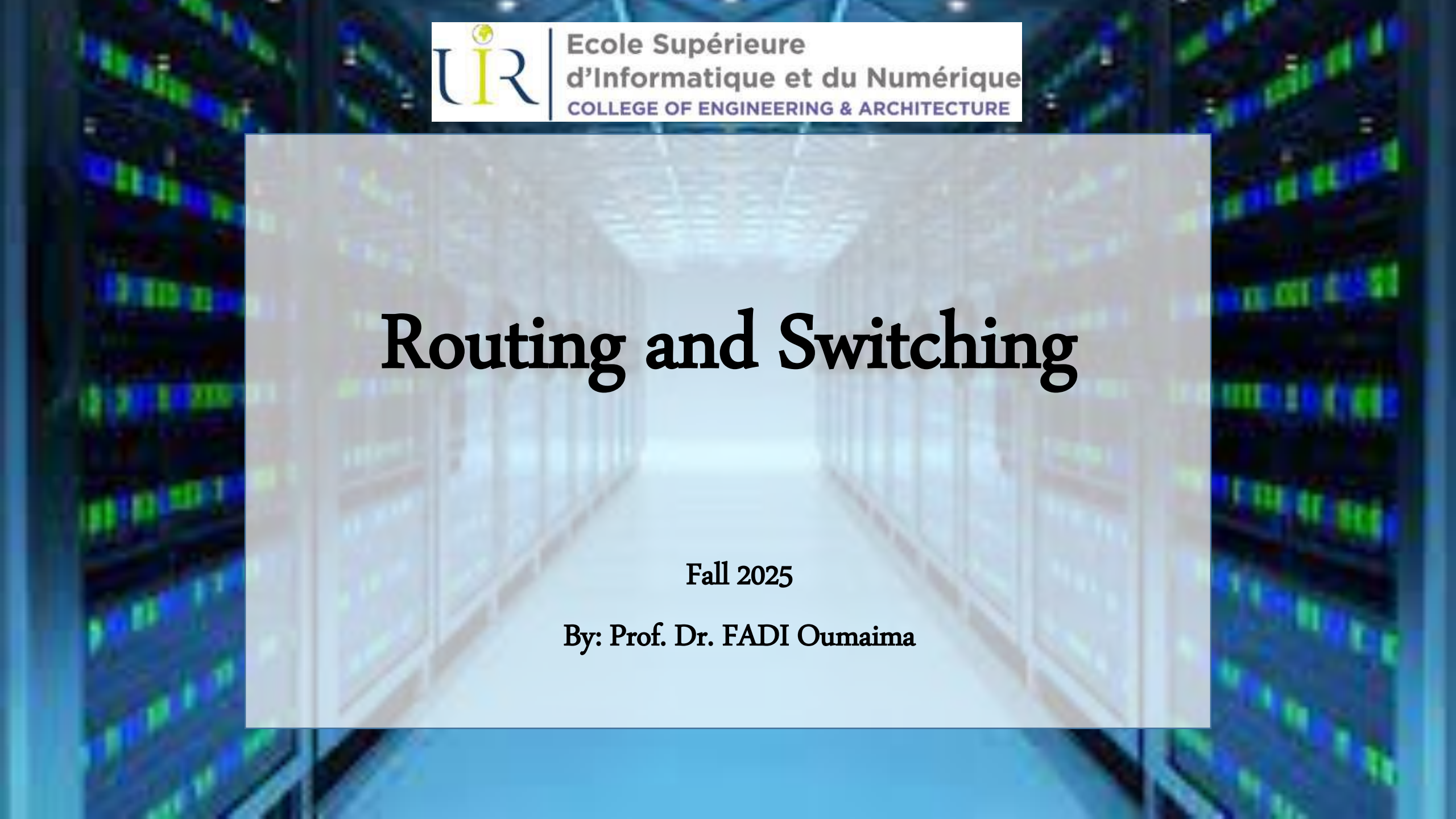


Routing and Switching

Fall 2025

By: Prof. Dr. FADI Oumaima

Evaluation

Lab Report+ Quiz:**10%**

CC: **20%**

CF: **50%**

HCIA-certification: **20%**

Chapter3 : VLSM & VLAN

Topics:

- Subnetting techniques & VLSM (Variable Length Subnet Masking)
- VLSM addressing/ Subnet ip@
- VLAN: Definition and why?
- VLAN types
- VLAN Tag
- VLAN Trunk
- Static vs Dynamic Trunking

IPv4: Special Addresses

These addresses are not operating in the internet:

- **10.0.0.0 à 10.255.255.255**
- **172.16.0.0 à 172.31.255.255**
- **192.168.0.0 à 192.168.255.255**

VLSM: Variable Length Subnet Mask

1. Splits a subnet into smaller subnets

Instead of one large subnet, we divide it into several smaller ones.

Example: /24 network can be split into /25, /26, /27 … depending on needs.

2. “Sub-subnetting”

VLSM is like subnetting a subnet.

You can keep breaking down networks until you get the right size for each group.

3. Flexible subnet sizes

Each subnet can have a different number of hosts.

You assign a **larger subnet** for departments with many devices, and a **smaller subnet** for areas with fewer devices.

VLSM: Variable Length Subnet Mask

Address given:
Network: 192.168.0.0/16
Meaning:
Network portion = first 16 bits (192.168)
Host portion = last 16 bits
So the network covers **192.168.0.0 → 192.168.255.255**

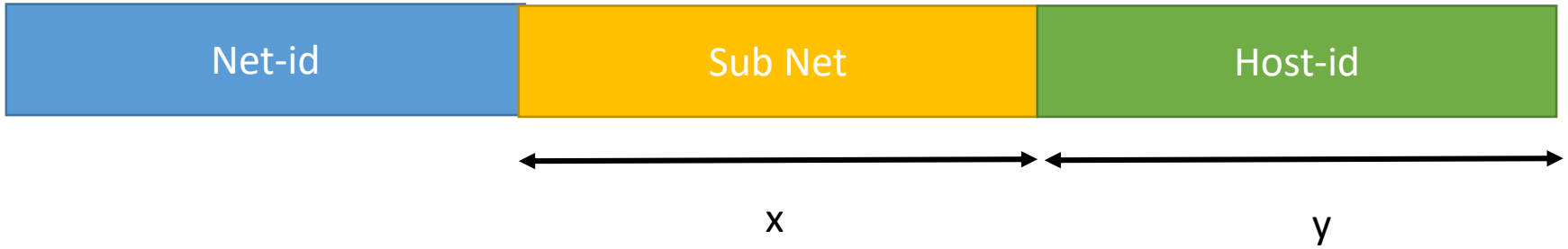
What is the broadcat address for: 192.168.0.0/16? **192.168.255.255**

What about 192.168.3.255 ?

If we have /16, then
192.168.3.255 is NOT the broadcast address,

/24 → network = 192.168.3.0/24 → broadcast = 192.168.3.255

VLSM: Variable Length Subnet Mask



Number of subnets = 2^x

Number of hosts per network = 2^y – 2

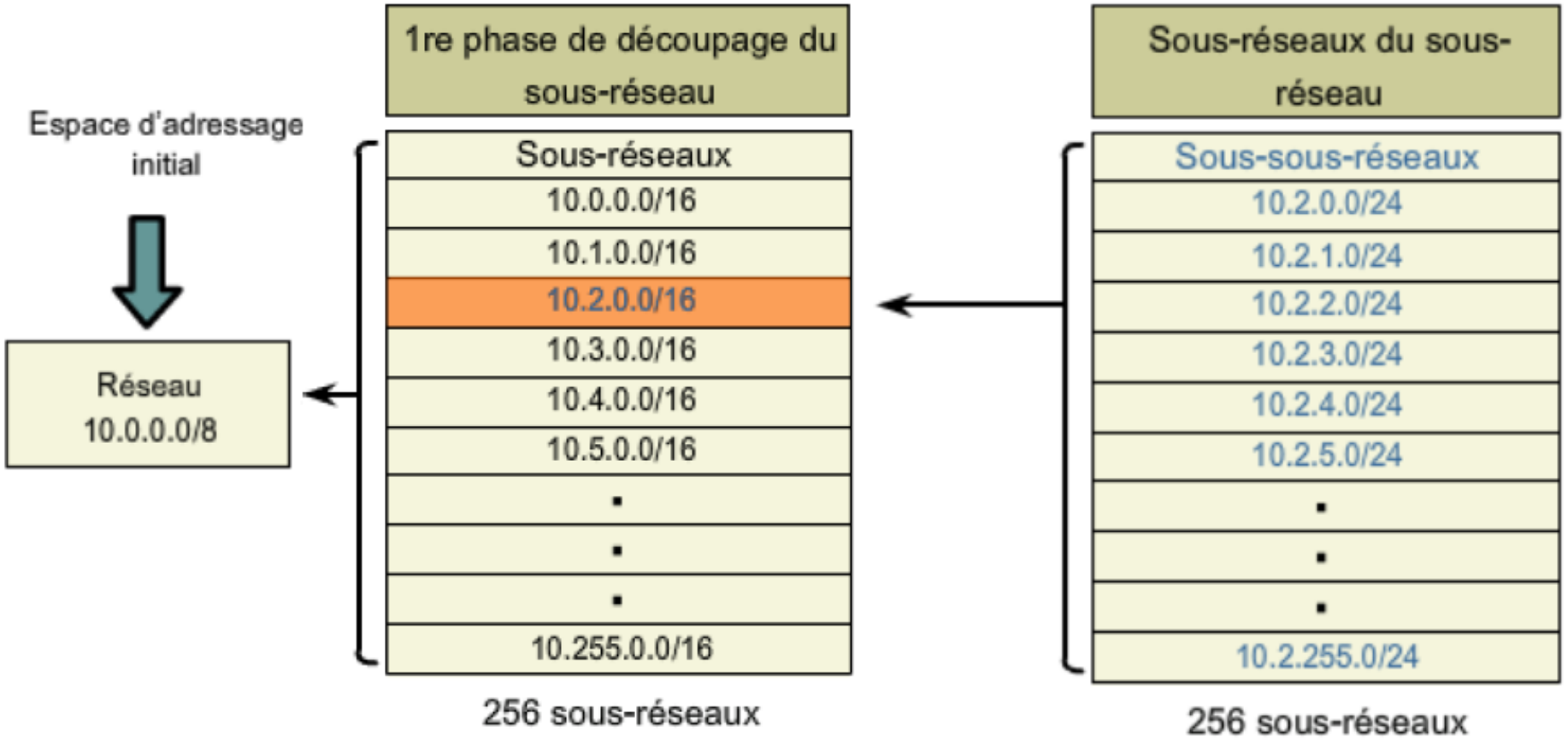
Example

Given a Class B address with a mask of **255.255.255.128**

Number of subnets = 2^9 = 512

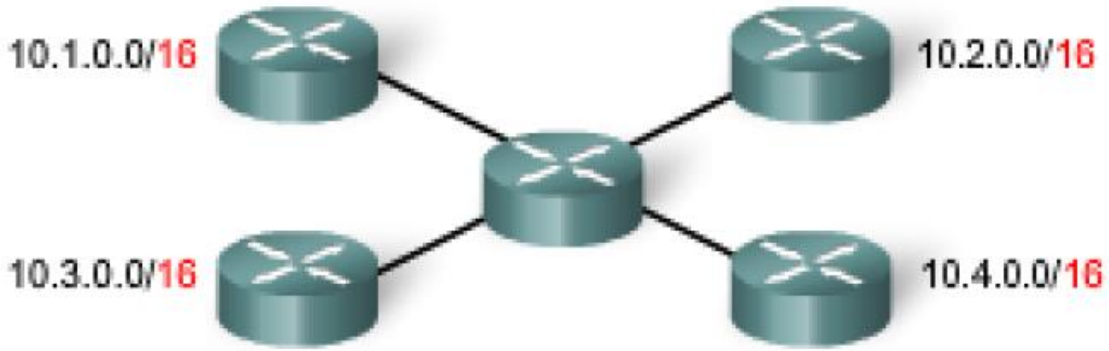
Number of hosts per network = 2^7 – 2 = 126

VLSM: Variable Length Subnet Mask



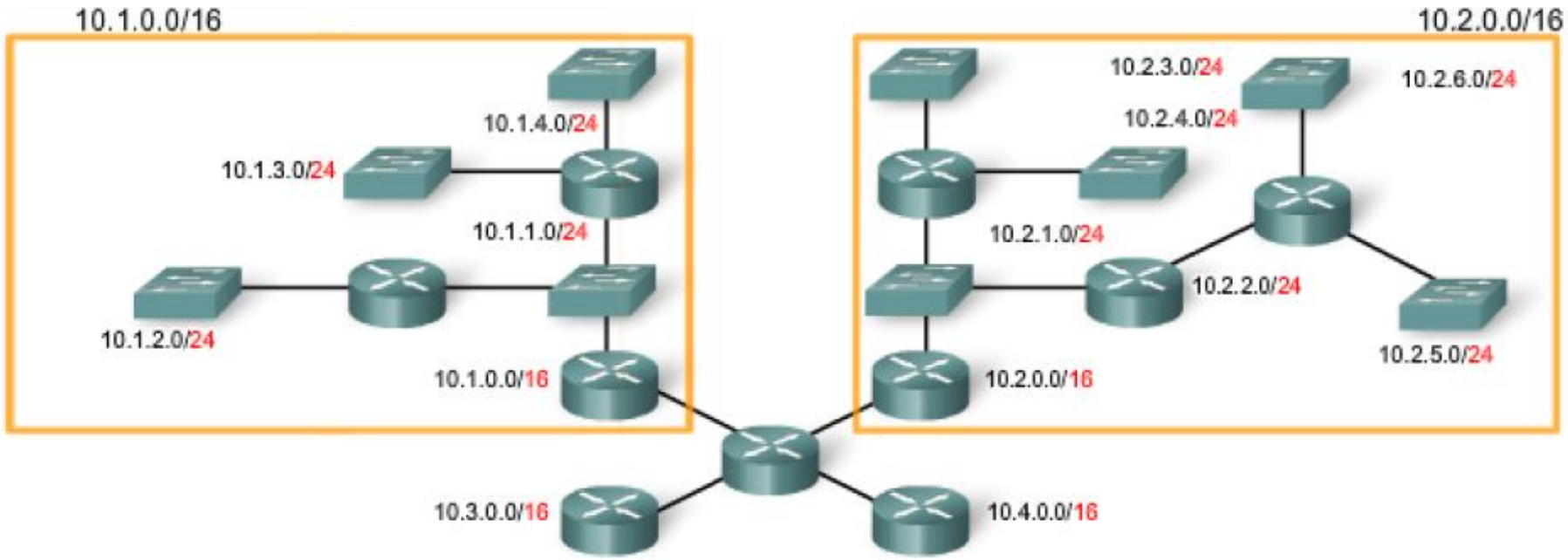
VLSM: Variable Length Subnet Mask

The figure illustrates the **10.0.0.0/8** network, which has been subdivided using the **/16 subnet mask**, resulting in **256 subnets**.



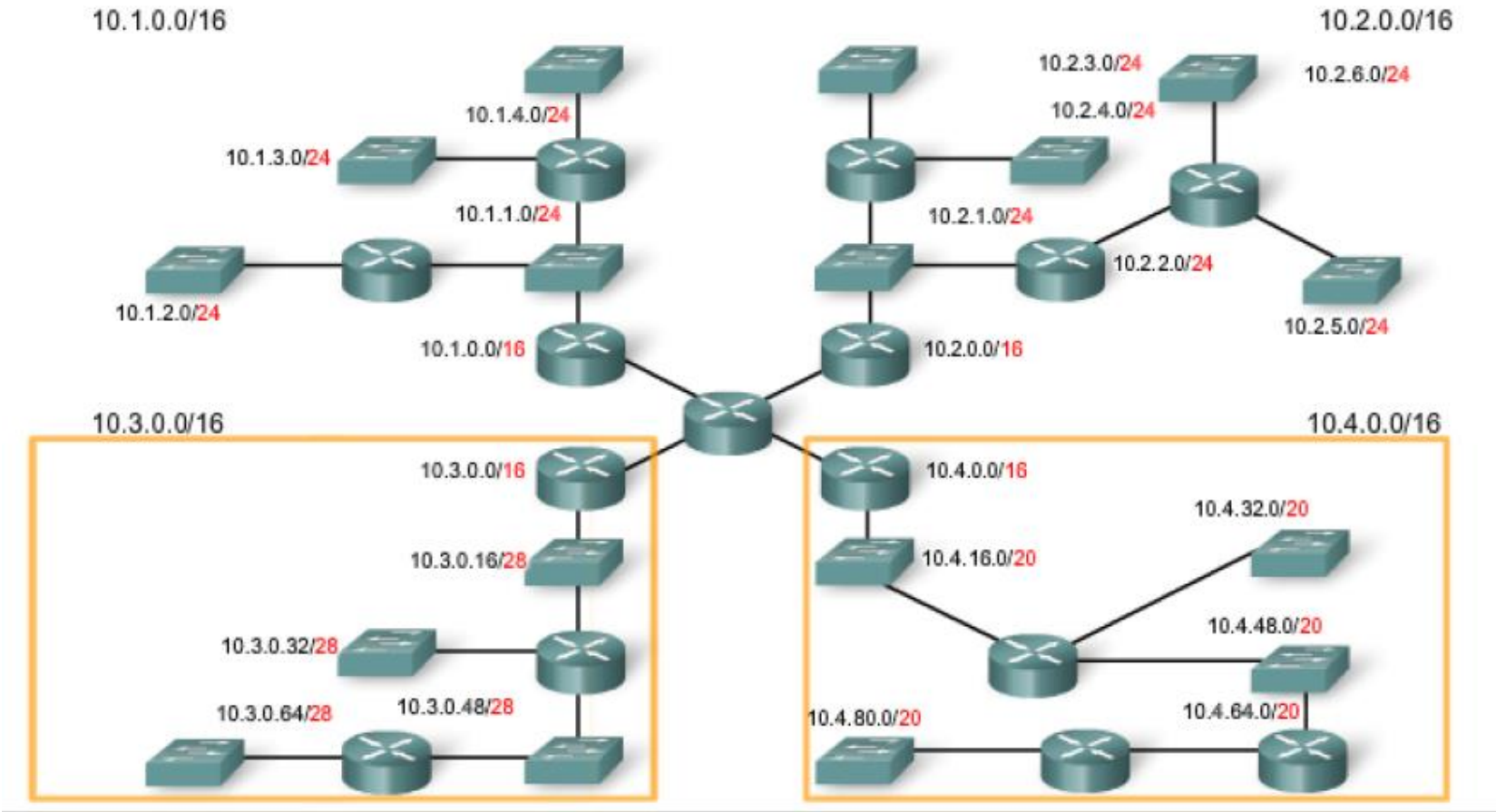
VLSM: Variable Length Subnet Mask

The subnets **10.1.0.0/16** and **10.2.0.0/16** are further subdivided using the **/24 mask**.



VLSM: Variable Length Subnet Mask

Similarly, the subnets **10.3.0.0/16** and **10.4.0.0/16** are respectively divided into subnets using the **/28** and **/20** masks.



VLSM: Variable Length Subnet Mask

My IP address: 192.168.25.132

Translated into binary:

11000000.10101000.00011001.10000100

My network mask: 255.255.255.128

Translated into binary:

11111111.11111111.11111111.10000000

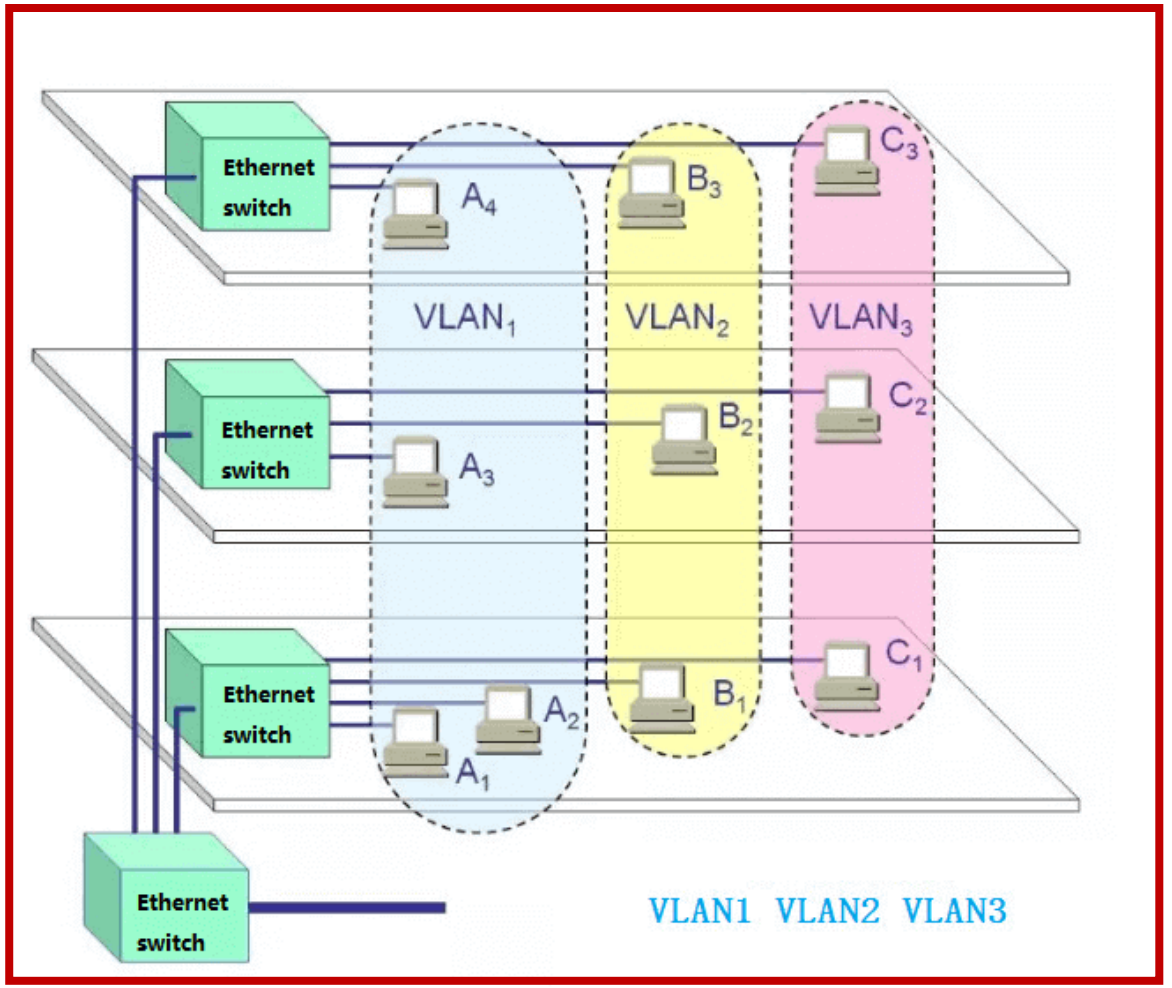
Network address:

11000000.10101000.00011001.10000000

That is: 192.168.25.128

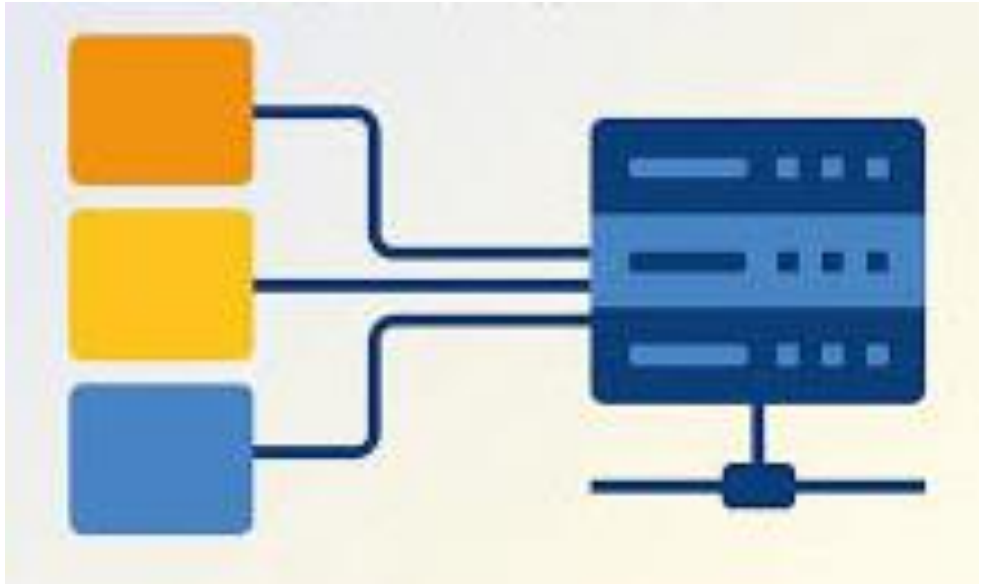
Conclusion: We can assume that the machines on my local network have addresses from **129 to 254**.


WAN
Wide Area Network
MAN
Metropolitan
Area Network
LAN
Local Area Network

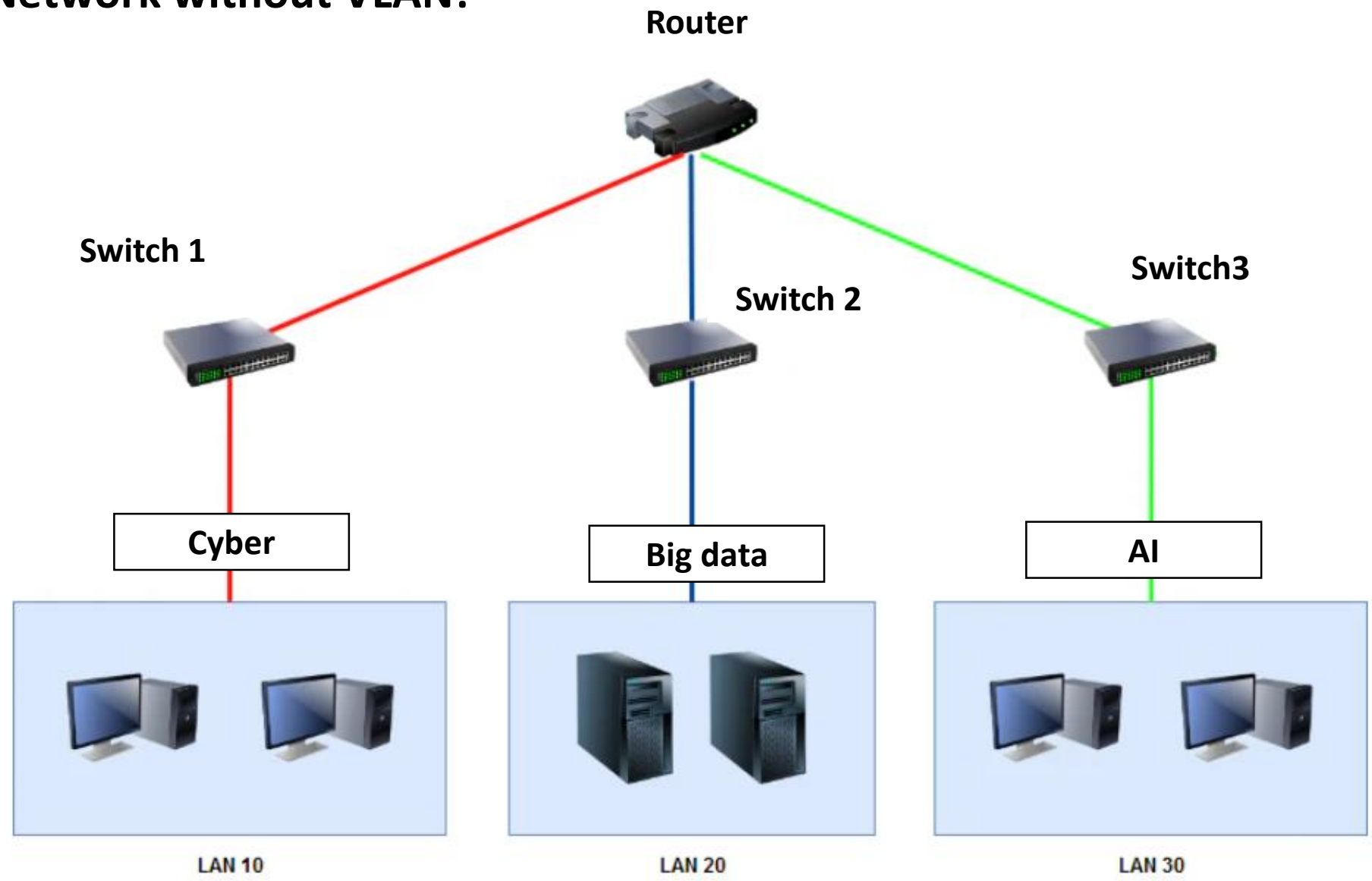

Ethernet switch
Ethernet switch
Ethernet switch
Ethernet switch
A4
A3
A2
A1
B3
B2
B1
C3
C2
C1
VLAN1
VLAN2
VLAN3
VLAN1 VLAN2 VLAN3

Why we need VLANs?

1. Virtual local area networks provide connectivity and security, while countering broadcasts and failing domains.
2. Virtual local area networks logically segment networks and contain broadcasts in order to improve network security and performance.
3. Switches on which aggregation is enabled allow virtual local area networks to extend across many geographical sites.
4. The VTP (VLAN Trunking Protocol) is used to simplify the configuration and management of virtual local area networks within a complex switched enterprise network.



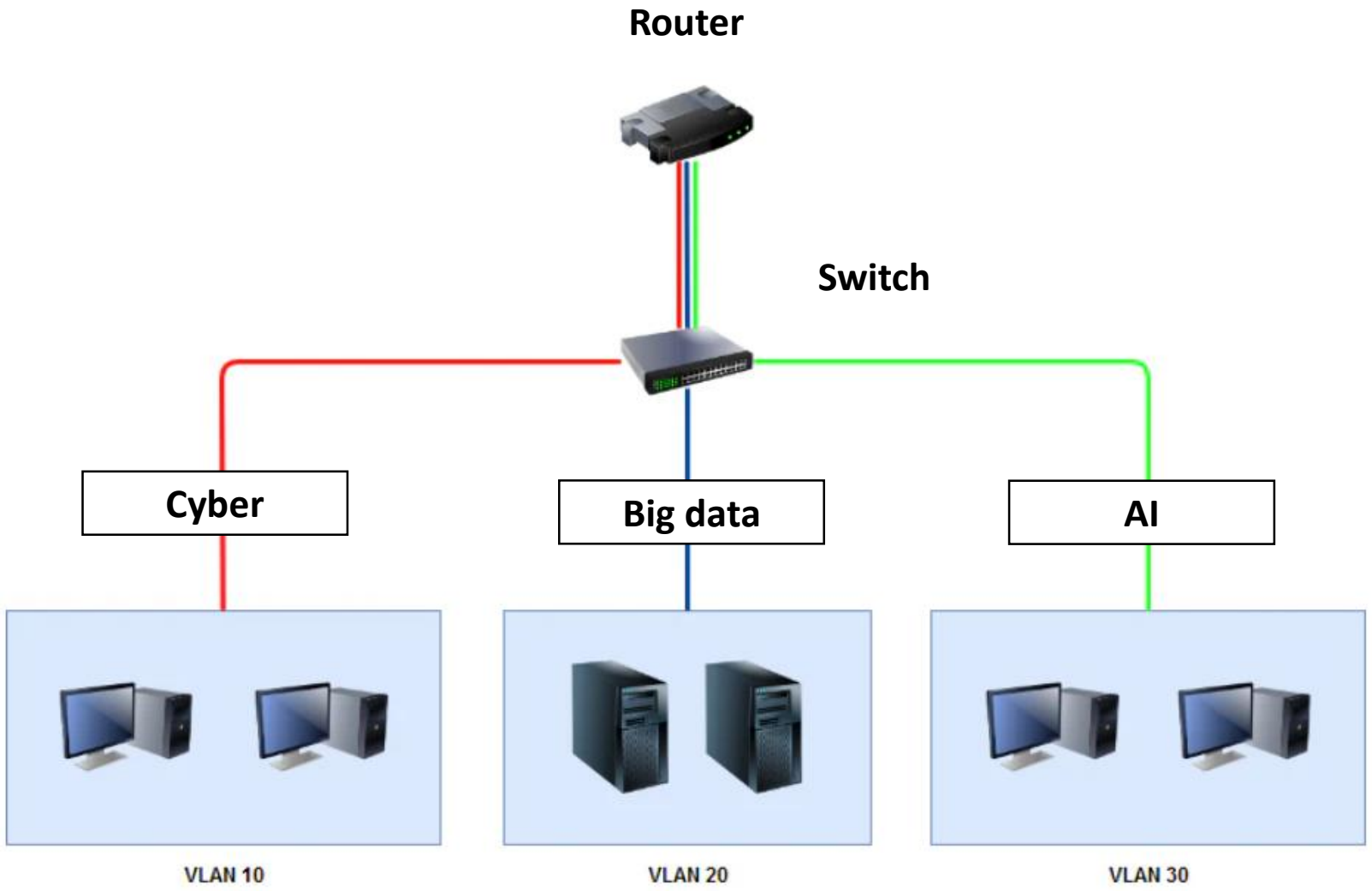
Network without VLAN!



⇒ Each network can be set to a different subnet on the router

⇒ Each switch considers all the ports a domain of broadcast

Network with VLAN!



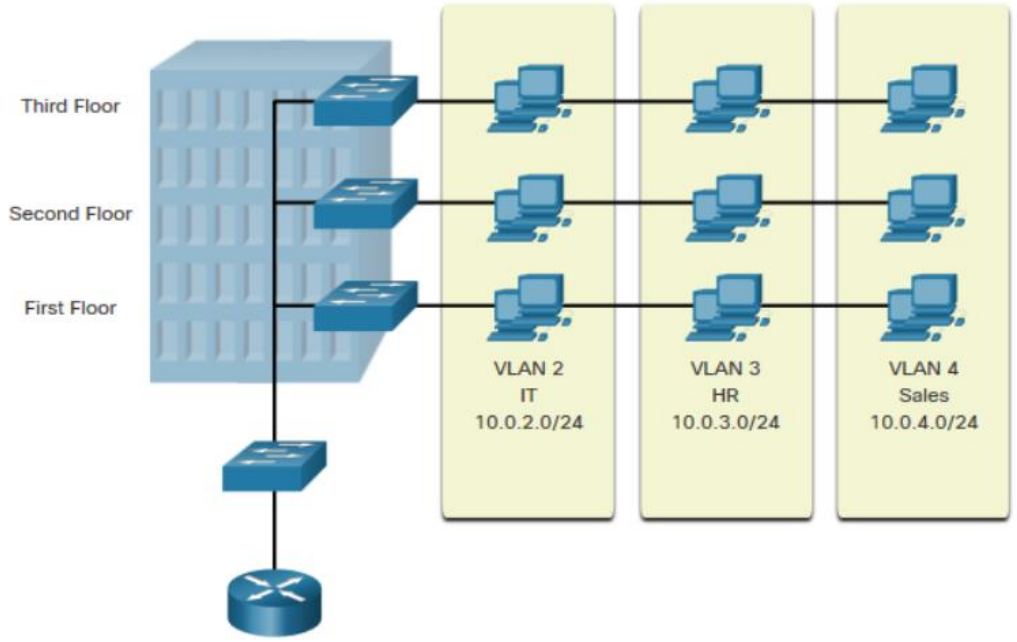
=> Different VLANs are established on the switch ports!

Network with VLAN!

VLANs are logical connections with other similar devices.

Placing devices into various VLANs have the following characteristics:

- Provides segmentation of the various groups of devices on the same switches
- Provide organization that is more manageable
  - Broadcasts, multicasts and unicasts are isolated in the individual VLAN
  - Each VLAN will have its own unique range of IP addressing



VLAN (Virtual Local Area Network)

A VLAN is a virtual local area network

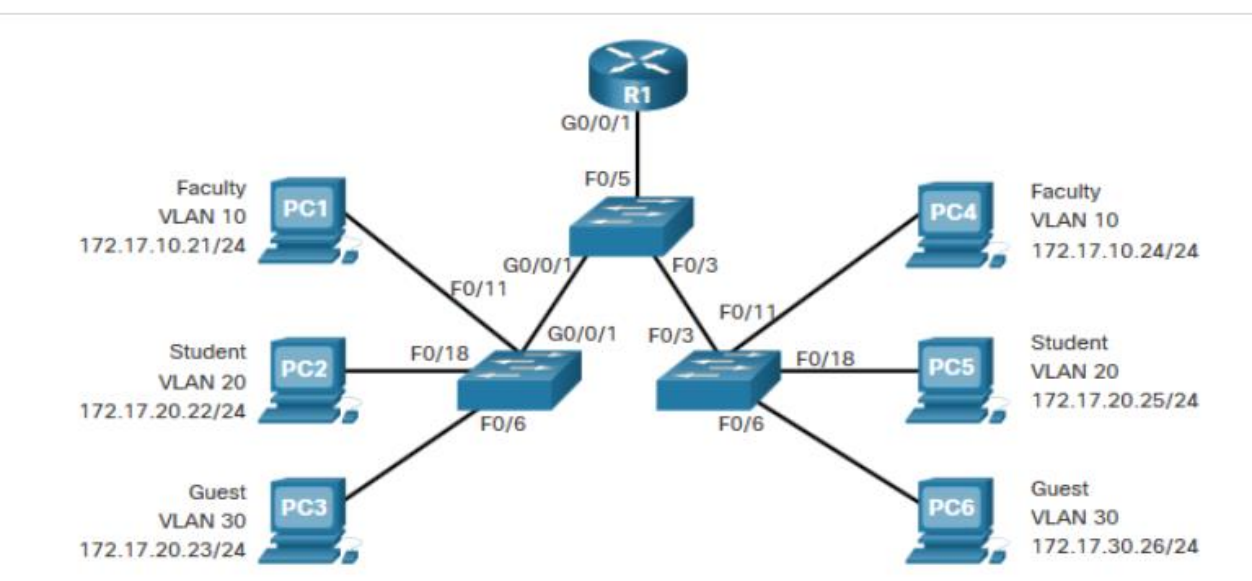
The geographical location of the elements of the VLAN can be arbitrary, which implies emulating a local network, even if all of the clients are geographically distributed over several switches

A VLAN has mechanisms ensuring the selective broadcasting of information (Standard 802.1q)

Basic notions:

- Default VLAN always present (VLAN1)
- Technology standardized on current switches
- Configuration at the equipment level

VLAN benefits



Benefits	Description
Smaller Broadcast Domains	Dividing the LAN reduces the number of broadcast domains
Improved Security	Only users in the same VLAN can communicate together
Improved IT Efficiency	VLANs can group devices with similar requirements, e.g. faculty vs. students
Reduced Cost	One switch can support multiple groups or VLANs
Better Performance	Small broadcast domains reduce traffic, improving bandwidth
Simpler Management	Similar groups will need similar applications and other network resources

Static VLAN

- In a virtual local area network, a machine's membership in a VLAN can be assigned **statically (VLAN N1)** or **dynamically (VLAN N2)**.
- **Static membership** requires an administrator to manually assign each switch port to a specific VLAN.
- This type of membership is the simplest to configure and the most widespread, but it is the most demanding in terms of administration for managing additions, moves, and changes

Dynamic VLAN

- Dynamic VLAN membership requires a **VLAN Management Policy Server (VMPS)**. The VMPS contains a database that associates MAC addresses with VLAN assignments.
- In a dynamic VLAN network, moves, additions, and changes are automated and do not require any administrator intervention.

VLAN types

1. Data VLAN

Carries regular user data traffic

Example: Employees' PCs, printers

2. Voice VLAN

Dedicated to VoIP traffic from IP phones

Ensures priority and low latency for calls

3. Management VLAN

Used for switch management traffic

Example: Accessing the switch via SSH or web interface

4. Default VLAN

Preconfigured VLAN on all switches (usually VLAN 1)

All ports belong to it by default

5. Native VLAN

The VLAN used for untagged frames on a trunk port

Usually configured on trunk links for compatibility

VLAN types

Default VLAN

VLAN 1 is the following:

- The default VLAN
- The default Native VLAN
- The default Management VLAN
- Cannot be deleted or renamed

Note: While we cannot delete VLAN1 Cisco will recommend that we assign these default features to other 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 types

Voice VLAN

• A separate VLAN is required because Voice traffic requires:

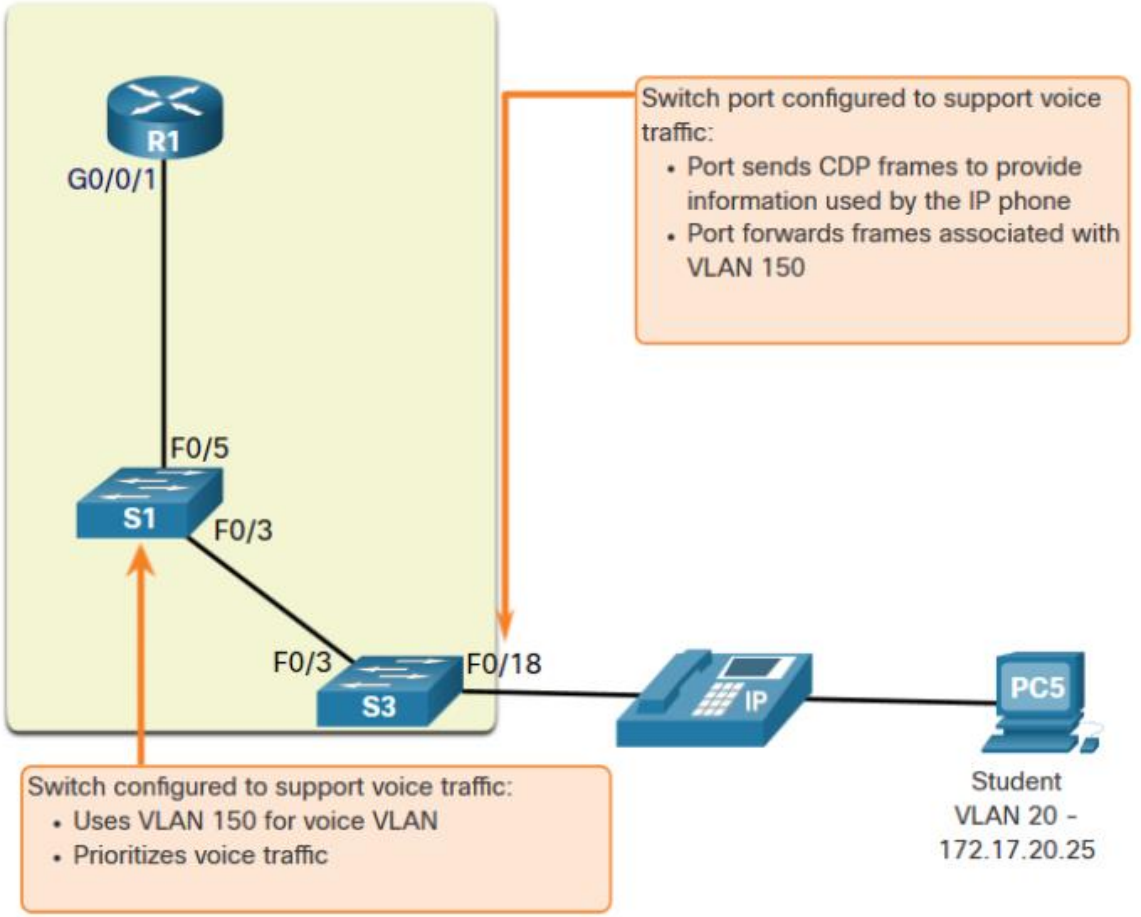
• Assured bandwidth

• High QoS priority

• Ability to avoid congestion

• Delay less that 150 ms from source to destination

• The entire network must be designed to support voice.



VLAN types

CDP = Cisco Discovery Protocol

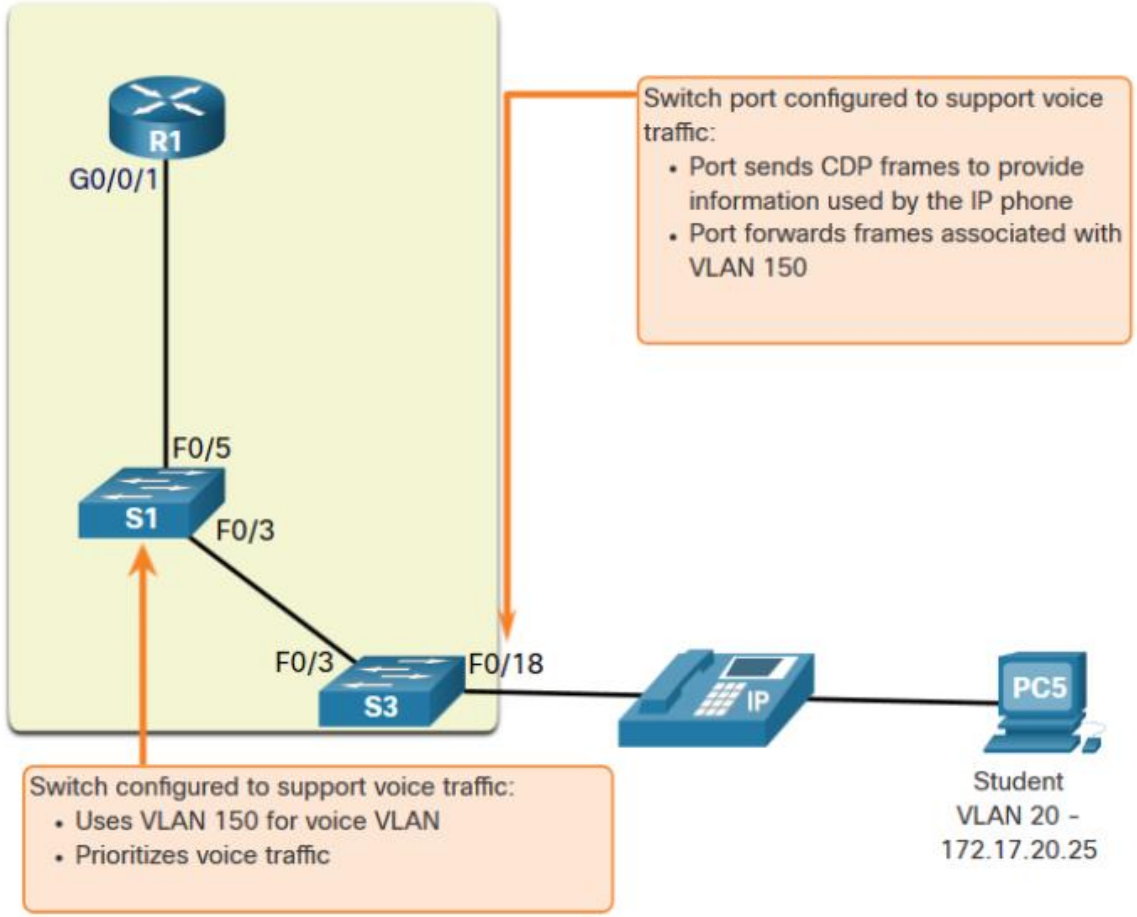
- It's a Layer 2 protocol (Cisco proprietary).

Switches and Cisco IP Phones use CDP to **exchange information about themselves** (device type, IP, port ID, etc.).

- In the context of **Voice VLAN**:

When you plug in a Cisco IP Phone, the **switch port sends CDP messages** telling the phone which **Voice VLAN ID** to use.

The phone then places its traffic in the tagged Voice VLAN and the PC traffic in the untagged Data VLAN.



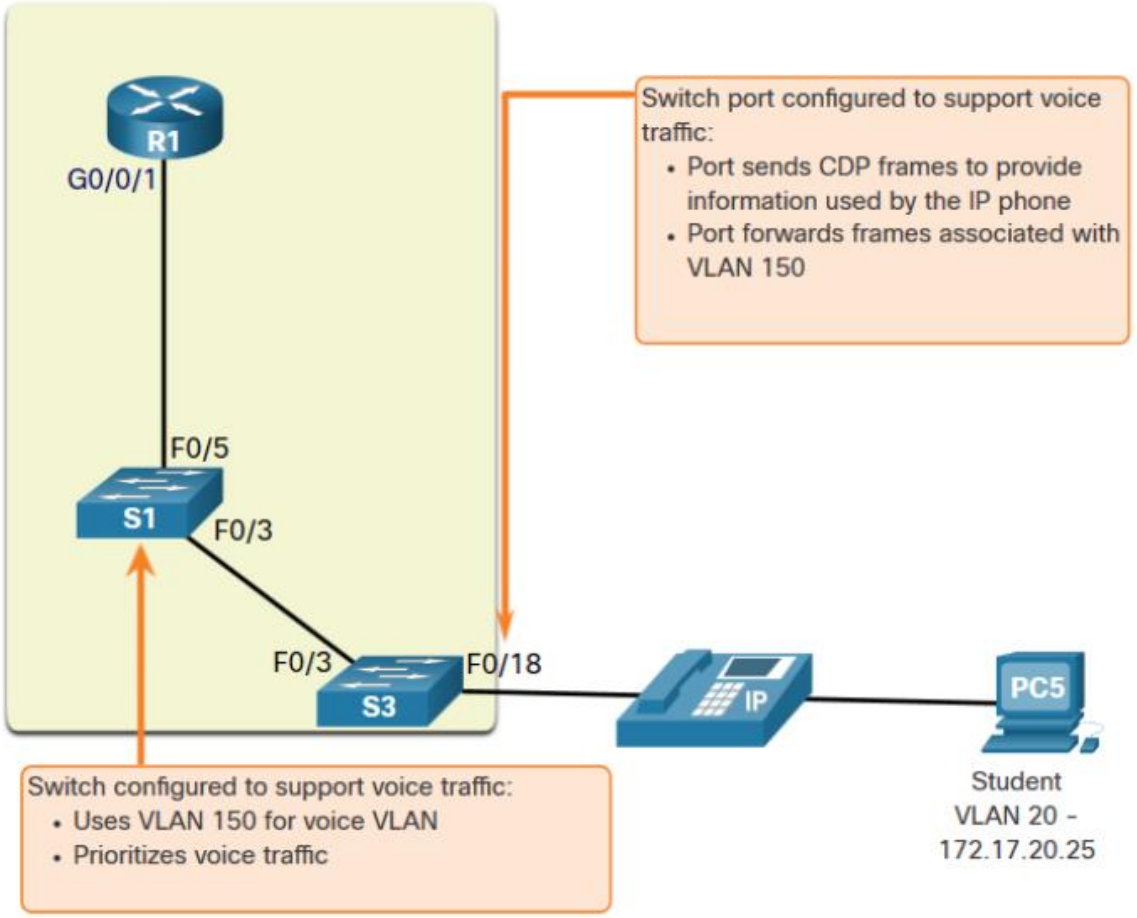
Why use CDP in Voice VLAN?

Automatic VLAN assignment – The phone doesn't need manual VLAN configuration.

Zero-touch provisioning – Just plug the phone in, and it learns its VLAN from CDP.

Traffic separation – Ensures voice and data don't interfere.

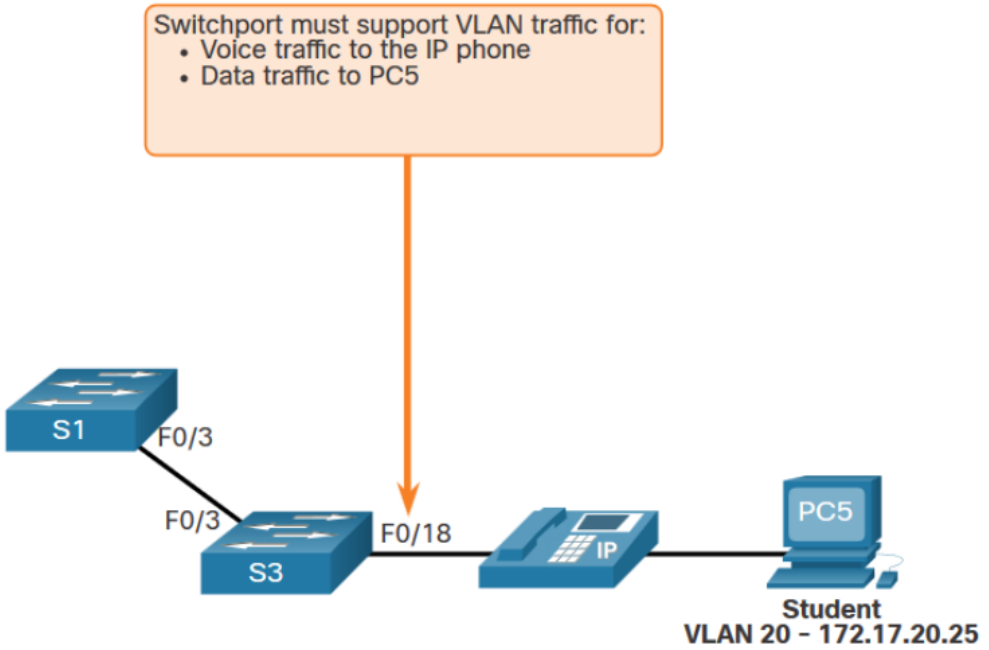
QoS support – Switch can prioritize Voice VLAN traffic for better call quality.



Data and Voice VLANs

An access port may only be assigned to **one data VLAN**.

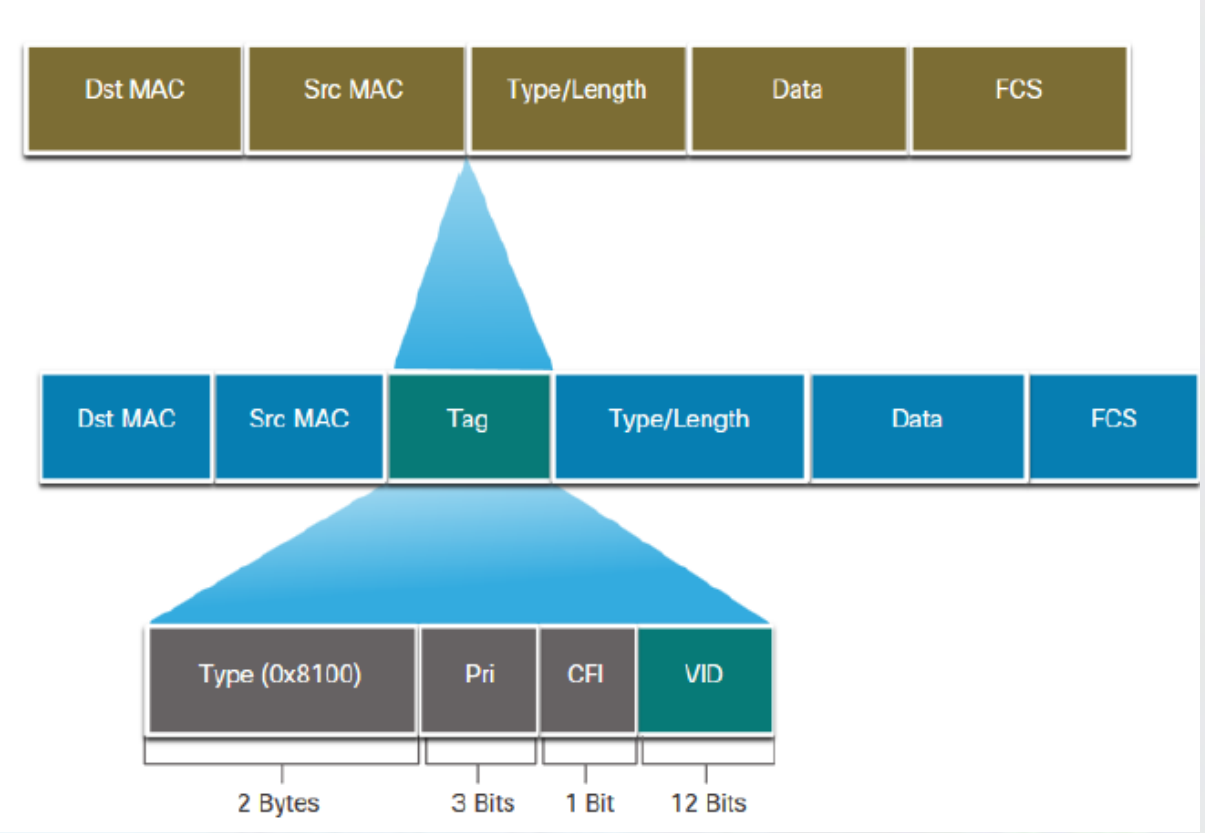
However it may also be assigned to one Voice VLAN for when a phone and an end device are off of the same switchport.



VLAN identification with tag

The IEEE 802.1Q header is 4 Bytes

- When the tag is created the FCS must be recalculated.
- When sent to end devices, this tag must be removed and the FCS recalculated back to its original number



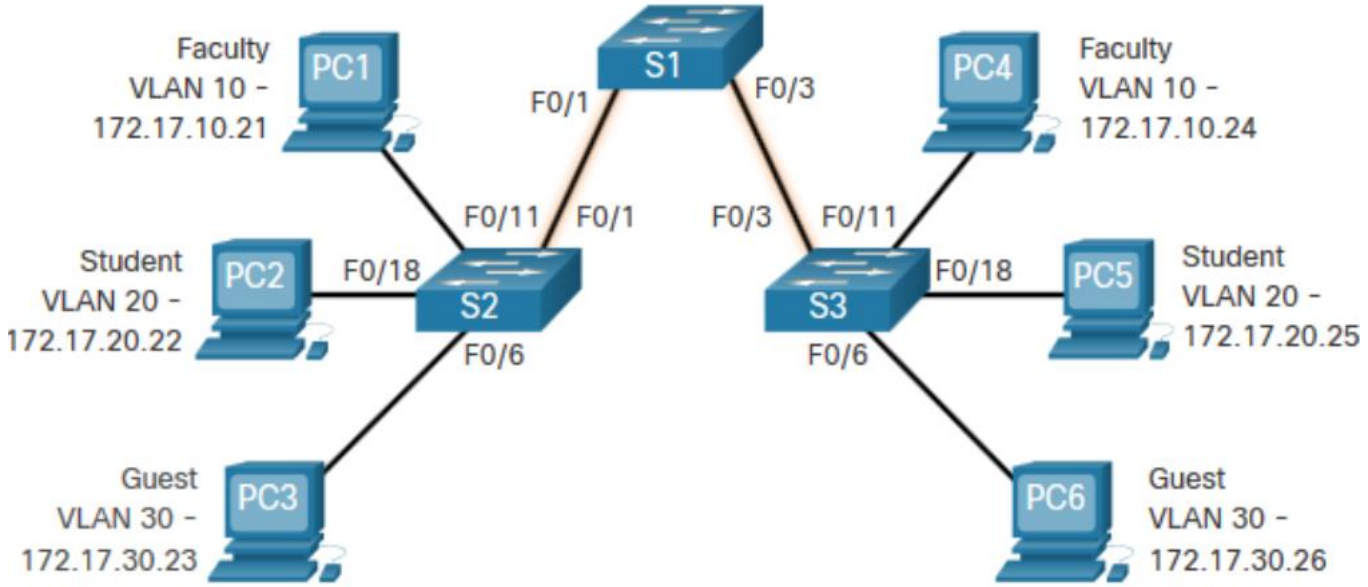
802.1Q VLAN Tag Field	Function
Type	• 2-Byte field with hexadecimal 0x8100 • This is referred to as Tag Protocol ID (TPID)
User Priority	• 3-bit value that supports
Canonical Format Identifier (CFI)	• 1-bit value that can support token ring frames on Ethernet
VLAN ID (VID)	• 12-bit VLAN identifier that can support up to 4096 VLANs

VLAN trunks

A trunk is a point-to-point link between two network devices.

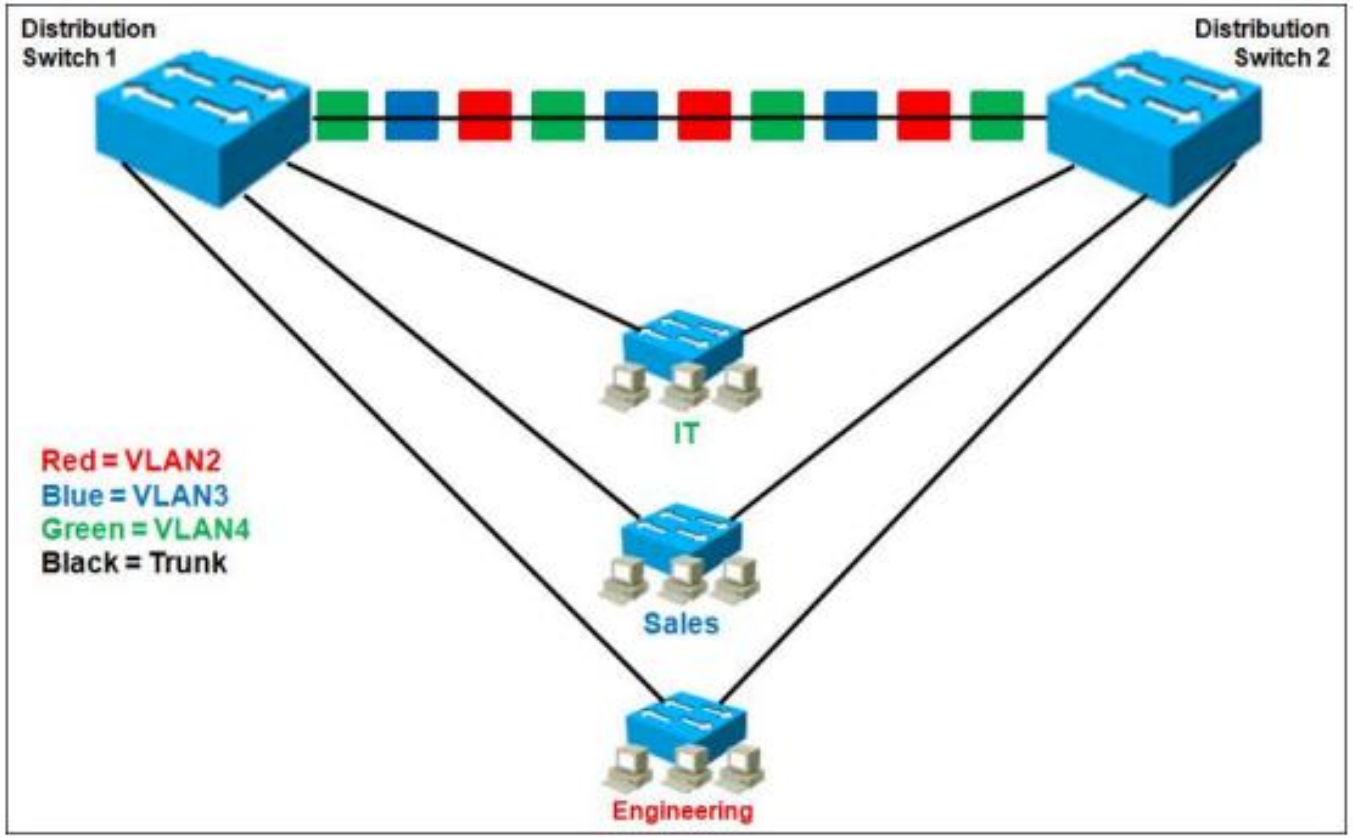
Cisco trunk functions:

- Allow more than one VLAN
- Extend the VLAN across the entire network
- By default, supports all VLANs
- Supports 802.1Q trunking



VLAN Trunk

- A **trunk port** carries traffic for **multiple VLANs** over a single physical link.
- Uses **802.1Q tagging** to identify VLANs.
- Connects **switch-to-switch** or **switch-to-router**.
- Why trunk? Saves cables and allows VLANs to span multiple switches.



Access vs Trunk

Access port: only 1 VLAN, untagged frames.

Trunk port: multiple VLANs, frames tagged with VLAN IDs.

Native VLAN: the VLAN for untagged frames on a trunk

Questions time

Can a frame be associated with multiple VLANs?

No. Each Ethernet frame belongs to one VLAN only.

How multiple VLANs traverse the same link:
trunking
The frame is tagged with a VLAN ID (802.1Q)
The switch knows which VLAN the frame belongs to

Does this mean a switch port can be associated with only one VLAN?

Yes, if it's an access port.
Access ports carry traffic for a single VLAN (untagged).
Exception:
A voice VLAN can be added on an access port → now one data VLAN + one voice VLAN
For multiple VLANs, use a trunk port, which can carry many VLANs (tagged)

Can a PC's network card be associated with multiple VLANs?

Yes, if the network card supports VLAN tagging (802.1Q).
This is called a "VLAN-aware NIC" or 802.1Q subinterfaces.
Example: We have Linux/Windows machine, you can create multiple virtual interfaces, each on a different VLAN.
Otherwise: Most PCs with a standard NIC can only belong to one VLAN at a time.