|  |
| --- |
| **LAPORAN TEORI JARINGAN KOMPUTER**  **VLAN & TRUNKING VLAN**  **KELOMPOK -** |
|  |
| |  |  |  |  | | --- | --- | --- | --- | | **NO** | **NIM** | **NAME** | **CONTRIBUTION** | | 1. | 13323026 | Samuel Pangaribuan | Answer What are the benefits of VLAN? | | 2. | 13323033 | Agus Pranata | Search references and typing to Document | | 3. | 13323041 | Enrogel Jeremi Sibarani | Create a topology at Cisco Packet Tracer |   **DIII TEKNOLOGI KOMPUTER** |
| **INSTITUT TEKNOLOGI DEL**  **FAKULTAS VOKASI** |

**Judul Teori**

|  |  |  |
| --- | --- | --- |
| **Minggu/Sesi** | : | XII/1 |
| **Kode Mata Kuliah** | : | 4332101 |
| **Nama Mata Kuliah** | : | JARINGAN KOMPUTER |
| **Setoran** | : | Jawaban dalam bentuk *softcopy* |
| **Batas Waktu Setoran** | : | 14 November 2024 jam 10:00 |
| **Tujuan** | : | 1. Mahasiswa dapat memahami VLAN & Trunking VLAN. |

**Petunjuk**

# What is VLAN?

Definition of VLAN from various references:

1. A VLAN is a logical subnetwork of devices in a broadcast domain that is partitioned by network switches and/or network management software to act at its own distinct LAN [1].
2. A VLAN is a custom network created form one or more existing LANs. It enables groups of devices from multiple Networks (both wired and wireless) to be combined into a single logical network [2].
3. VLAN is a custom network which is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network [3].

Please answer these questions to sharpen your initial understanding of VLAN.

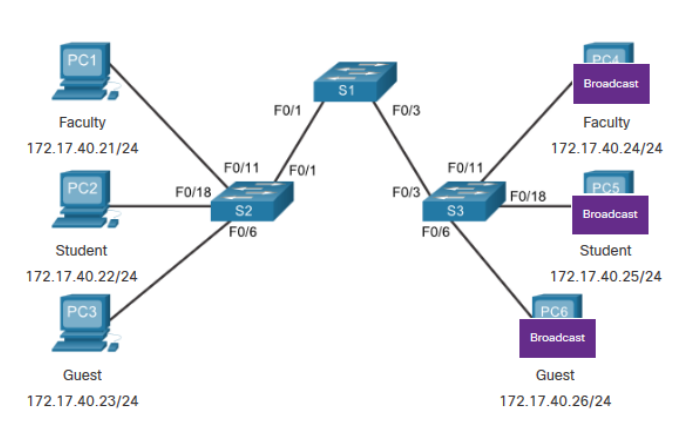
1. Can you find other definitions of VLAN from other sources?

**Answer:**

1. A Virtual Local Area Network (VLAN) is a subnetwork that can divide devices to enhance security. Ony users within the VLAN can access communication with assigned membership [4].
2. A VLAN is a group of devices in one or more LANs that are configured by software so they can communicate with each other as if they were on the same physical network [5].
3. A VLAN is a network that allows computers and users to connect in a geographic environment. This means it can also be defined as several devices in one ore more LANs that can be configured by software [6].
4. Can you illustrate how the VLAN segments of various groups of devices on the same switches?

**Answer:**

VLANs provide segmentation and organizational flexibility. They allow an administrator to segment networks based in factors such as function, project team, or application, without regard for the physical location of the user or device. Devices within a VLAN act as if they are in their own independent network, even if they share a common infrastructure with other VLANs.



*Figure 1 network without VLAN*

Figure 1 is a network without VLANs. Can you explain how communication works between nodes? For example, a host student in S2 wants to communicate with a host student in S3.

**Answer:**

1. **Sending the Frame**

A host connected to S2 (e.g. PC2) wants to communicate with a host connected to S3 (e.g. PC5). PC2 sends a frame addressed to PC5’s MAC Address.

1. **Receiving the Frame at Switch S2**

* Switch S2 receives the frame from PC2
* Switch S2 checks its MAC address table to find the port associated with PC5’s MAC address.

1. **Flooding if MAC Address is Uknown**

* If Switch S2 does not have an entry for PC5’s MAC address, it floods the frame out to all ports except the one it was received on.
* The frame is then sent to Switch S1 (if Switch S2 does not know where PC5 is located).

1. **Forwarding to Switch 3**

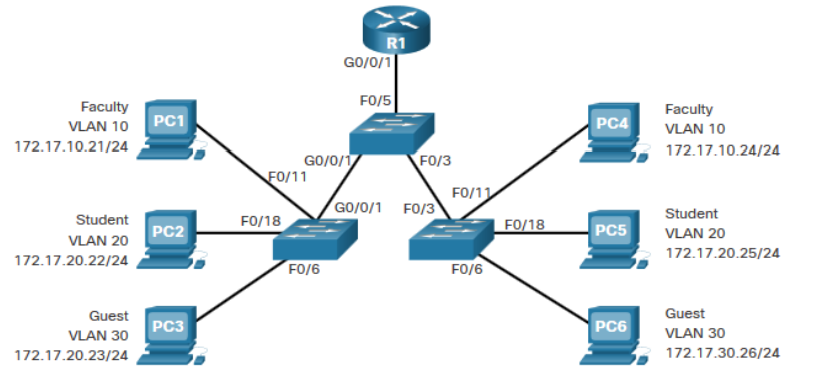
* Switch S3 receives the frame and checks its MAC address table.
* If PC5’s MAC address is in the table, Switch S3 forwards the frame to PC5.

1. **Receiving the Frame at Switch 3**

* Switch S3 receives the frame and checks its MAC address table.
* If PC5’s MAC address is in the table, Switch S3 forwards the frame to PC5.

1. **PC5 Responds**

* PC5 receives the frame and sends a response back to PC2
* The response frame follows the same path back through Switch S3 to Switch S1, and then to Switch S2, finally reaching PC2.



*Figure 2 network with VLAN*

and Figure 2 is a network with VLANs. Can you explain the difference between the two pictures?  According to Figure 2, how does the host Student (PC2) communicate with the host Student (PC5)? How does a VLAN differ from a physical LAN?

**Answer:**

**Difference Between Network Without VLANs and With VLANs**

1. **Network Without VLANs**

In a network without VLANs, all devices are part of the same broadcast domain. This means that any broadcast sent by one device will be received by all devices in the network, which can lead to increased broadcast traffic and potential performance and security issues.

1. **Network With VLANs**

In Figure2, VLANs (Virtual Local Area Networks) are configured to logically segment the network into different broadcast domains. Each VLAN acts as a separate network, even though all devices might be physically connected to the same switch or set of switches. This helps to reduce broadcast traffic, increase security, and improve network management.

**Communication Between Students in VLANs**

1. **Tagging Traffic with VLAN ID**

* When PC2 sends a frame, the switch tags the frame with VLAN ID 20.
* The tagged frame is sent through the network infrastructure, ensuring that it only reaches ports that are part of VLAN 20.

1. **Forwarding the Frame**

* The Switch receives the tagged frame and looks up the destination MAC address in its VLAN 20 MAC address table.
* The Switch the forwards the frame to the port connected to PC5.

1. **Receiving the Frame**

* PC5 receives the frame, which is still tagged with VLAN ID 20.
* Because PC5 is also in VLAN 20, it processes the frame normally.

**Difference Between VLAN and Physical LAN**

1. **VLAN (Virtual Local Area Network)**

* Logical Segmentation

VLANs allow network adminstrators to create separate broadcast domains within the same physical network. This means that devices can be grouped logically based on function, department, or any other criteria, regardless of their physical location.

* Reduced Broadcast Traffic

VLANs limit broadcast traffic to specific segments, reducing the overall amount of broadcast traffic on the network.

* Improved Security

VLANs can improve security by isolating sensitive data within specific VLANs that can only be accessed by authorized devices.

1. **Physical LAN (Local Area Network)**

* Physical Segmentation

A physical LAN is a network of devices connected within a limited geographical area, such as a building or campus, using physical connections like Ethernet Cables.

* Single Broadcast Domain

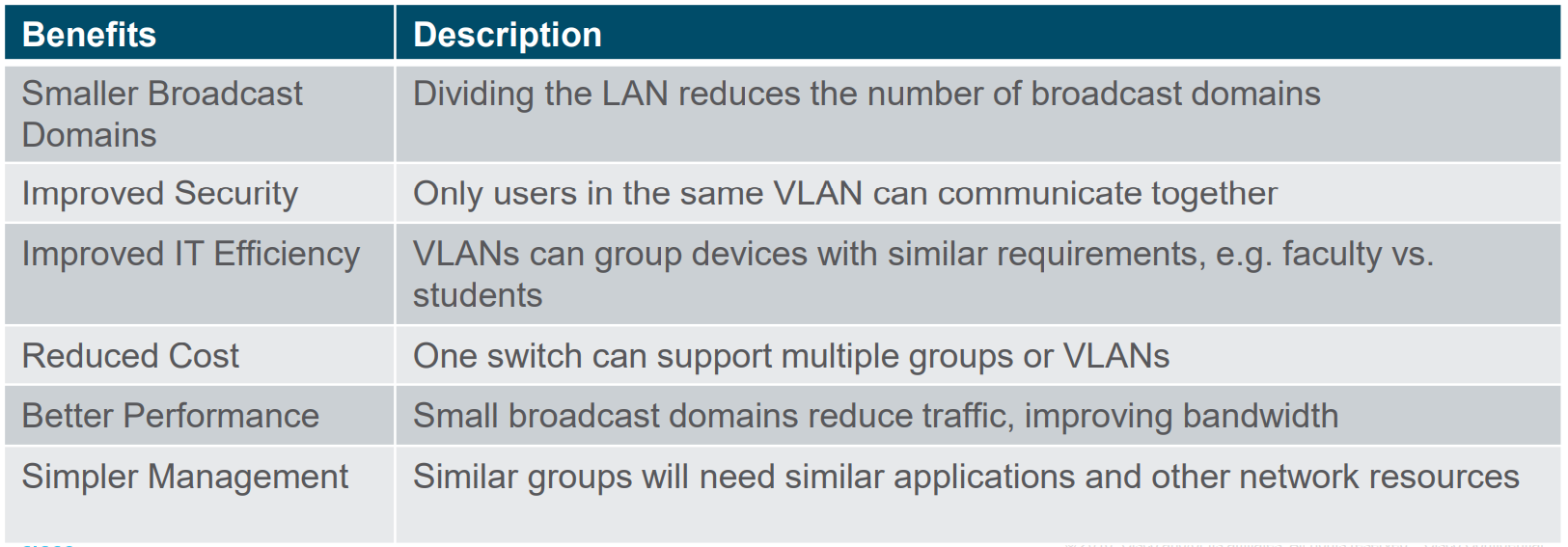
All devices in a physical LAN share the same broadcast domain unless segmented by VANs or other network devices.

* Security and Traffic Management

Without VLANs, managing security and traffic can be more challenging due to the lack of logical segmentation.

# What are the benefits of VLAN?

According to CISCO below are the benefits of using VLAN:



Please answer these questions:

1. What does the term broadcast domain mean about VLANs?

**Answer:**

A broadcast domain refers to a logical division of a computer network where all nodes can reach each other by broadcast at the data link layer [7].

VLAN (Virtual Local Area Networks) help create smaller broadcast domains by segmenting a larger network into smaller, isolated networks. This reduces the amount of broadcast traffic and limits the broadcast domain to the devices within the same VLAN [8].

1. Can you identify where are the smaller broadcast domains of the VLAN above? You can put a mark in the picture to show the broadcast domain.

**Answer:**

The image provided does not visually depict the broadcast domains, so it is not possible to mark them directly on the image. However, the concept of smaller broadcast domains is described in the first row under “Smaller Broadcast Domains”, which states that dividing the LAN reduces the number of broadcast domains [7].

1. Elaborate your answer to why VLAN improved security and has better performance.

**Answer:**

Improved Security:

1. VLANs improve security by isolating network traffic

Only users within the same VLAN can communicate with each other, which means that sensitive data can be confined to specific VLANs, reducing the risk of unauthorized access [8].

1. Better Performance

VLAN enhance performance by reducing the size of broadcast domains. Smaller broadcast domains mean that broadcast traffic is limited to a smaller number of devices, reducing network congestuon and improving overall bandwidth [8].

1. Explain types of VLAN (data VLAN, Native VLAN, Management VLAN, Voice VLAN)!

**Answer:**

Data VLAN:

1. This type of VLAN is used to separate user-generated data traffic [9].
2. It is the most common type of VLAN and is used to segment network traffic based on different user groups or departments within an organization [9].

Native VLAN:

1. The native VLAN is used for untagged traffic on a trunk port [9].
2. It is a special VLAN that carries untagged frames and is typically used for backward compatibility with older network devices that do not support VLAN tagging [9].

Management VLAN:

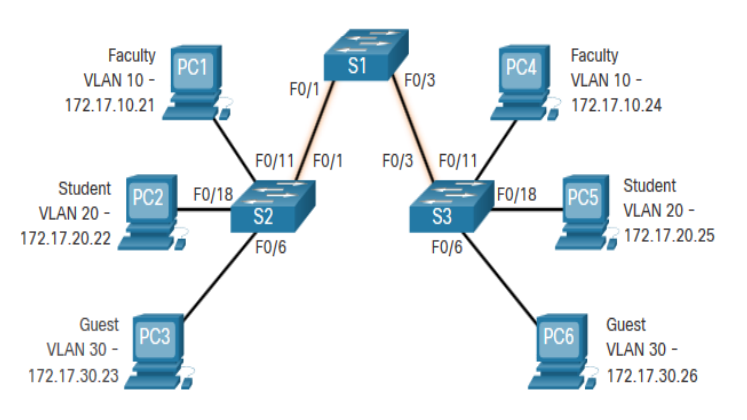
1. This VLAN is designated for network management traffic, such as SNMP, Telnet, SSH, and other management protocols [9].
2. It provides a secure and isolated environment for managing network devices and ensures that management traffic is not mixed with user data traffic [9].

Voice VLAN:

1. This type of VLAN is specifically designed for VoIP (Voice over IP) traffic [9].
2. It prioritizes voice traffic to ensure high-quality voice communication by providing dedicated bandwidth and reducing latency and jitter [9].

# VLANs in a Multi-Switched Environment

This picture depicts more than one VLAN in a multi-switched environment. What protocol is used to connect switches so communication between VLANs can happen? Please highlight which line the protocol should be applied to and briefly explain the function of the protocol!



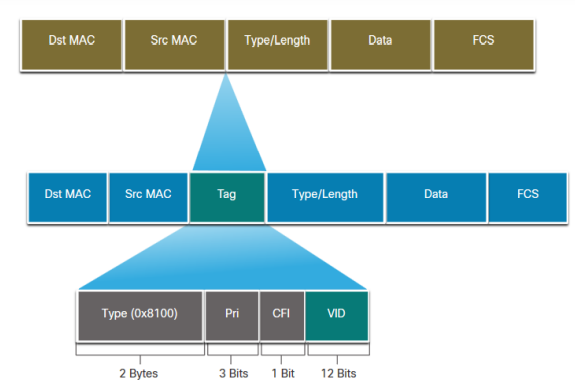
**Answer:**

The protocol used to connect switches so communication between VLANs can happen is the IEEE 802.1Q protocol, also known as VLAN tagging. This protocol should be applied to the lines connecting the switches, specifically the connections between S1 and S2 (F0/1 to F0/11), and S1 and S3 (F0/3 to F0/11).

Function of IEEE 802.1Q Protocol: The IEEE 802.1Q protocol allows multiple VLANs to be carried over a single physical link between switches. It inserts a VLAN tag into the Ethernet frame, which identifies the VLAN to which the frame belongs. This tagging enables the switches to properly route the traffic to the correct VLAN, ensuring that devices in different VLANs can communicate with each other through the switch infrastructure.

Image Description: The image shows a network diagram with three switches (S1, S2, and S3) and six PCs (PC1 to PC6) connected to them. The PCs are divided into three VLANs: Faculty (VLAN 10), Student (VLAN 20), and Guest (VLAN 30). Each VLAN has its own subnet, with IP addresses assigned to the PCs accordingly. The switches are interconnected, allowing for VLAN communication across the network. This setup is interesting and relevant as it demonstrates a typical VLAN configuration in a multi-switched environment, highlighting the importance of VLAN tagging for inter-VLAN communication.

# VLAN Identification with a Tag



A VLAN tag is embedded to a frame header consists of field Type, User priority, Canonical Format Identifier (CFI), and VLAN ID (VID). Explain the function of all VLAN tag field.

**Answer:**

A VLAN tag embedded in a frame header plays a crucial role in network segmentation and traffic management. Here's a breakdown of each field in the VLAN tag and their functions:

1. Type (0x8100):

Function: This 2-byte field identifies the frame as containing a VLAN tag. The specific value, 0x8100, is used to indicate that the frame is an IEEE 802.1Q-tagged frame. This tells the receiving device that the frame includes VLAN information.

1. User Priority (Pri):

Function: This 3-bit field is used for Quality of Service (QoS) purposes. It allows traffic to be prioritized, ensuring that important data (like voice or video) can be sent with higher priority over less critical data. This helps in managing bandwidth and improving the performance of time-sensitive applications.

1. Canonical Format Identifier (CFI):

Function: This 1-bit field indicates whether the MAC addresses are in canonical format. A value of 0 means the addresses are in canonical format, while a value of 1 means they are in non-canonical format. This field is primarily used in bridging between Ethernet and Token Ring networks, ensuring compatibility.

1. VLAN ID (VID):

Function: This 12-bit field specifies the VLAN to which the frame belongs. It allows for the identification and segregation of traffic within different VLANs, supporting up to 4096 unique VLANs. This is crucial for managing network traffic and ensuring that devices in the same VLAN can communicate while being isolated from other VLANs.

# Simple VLAN example

1. Explain the commands to create a VLAN in a CISCO switch, and give an example complete with illustration and the command.

To create a VLAN, you typically need to follow these steps:

1. Enter global configuration mode:



|  |
| --- |
| Switch> enable  Switch# configure terminal |

1. Create the VLAN and assign it a number (e.g., VLAN 10):



|  |
| --- |
| Switch(config)# vlan 10 |

1. (Optional) Name the VLAN:



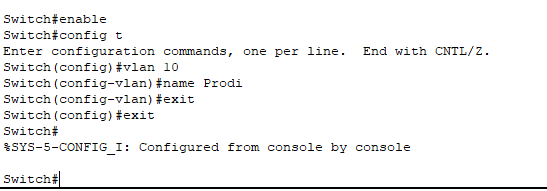
|  |
| --- |
| Switch(config-vlan)# name Prodi |

1. Exit VLAN configuration mode:



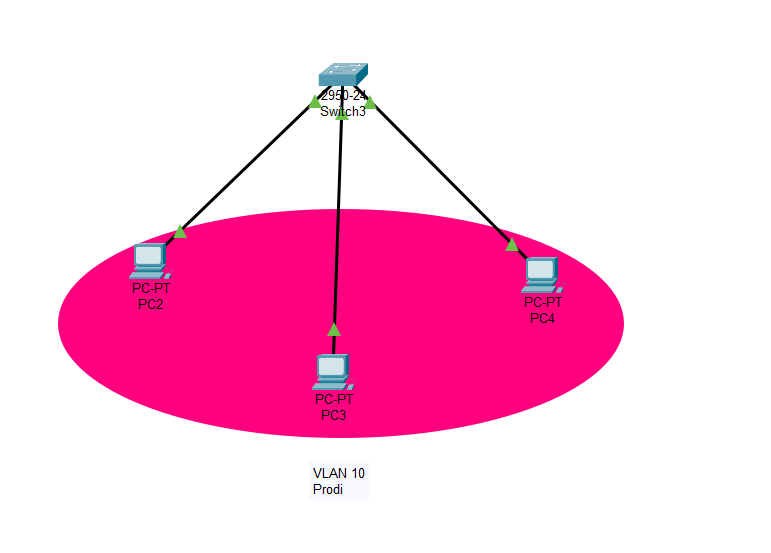
|  |
| --- |
| Switch(config-vlan)# exit |

Example and Illustration: Let's assume we have a switch where we want to create VLAN 10 named "Prodi."



|  |
| --- |
| Switch> enable  Switch# configure terminal  Switch(config)# vlan 10  Switch(config-vlan)# name Prodi  Switch(config-vlan)# exit  Switch(config)# exit  Switch# |

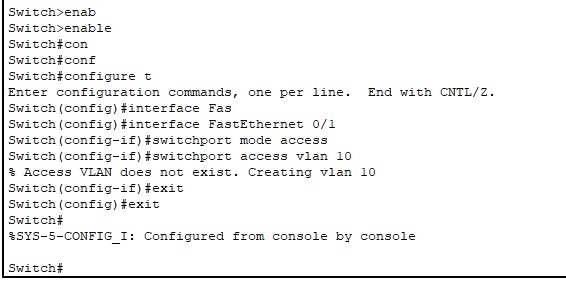
Illustration:



1. Explain what switchport mode access is!

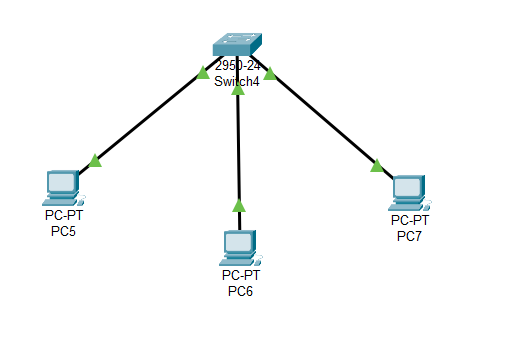
The switchport mode access command is used to set a switch port into access mode. This means the port will only accept frames from a single VLAN (the default or a specified VLAN) and will not participate in VLAN tagging. Essentially, it is used for connecting end devices like PCs, printers, or servers that are part of a single VLAN.

To set a switch port (e.g., FastEthernet 0/1) to access mode and assign it to a specific VLAN (e.g., VLAN 10):



|  |
| --- |
| Switch# configure terminal  Switch(config)# interface FastEthernet 0/1  Switch(config-if)# switchport mode access  Switch(config-if)# switchport access vlan 10  Switch(config-if)# exit  Switch(config)# exit  Switch# |

Physical Topology:



This configuration ensures that the port FastEthernet 0/1 will only communicate with devices in VLAN 10, effectively isolating it from traffic in other VLANs.

# VLANs Case

Write a scenario of a Multi-switched VLAN environment consisting of at least five switches and two PCs connected to each switch. You can create your scenario to determine the VLAN name, IP address, etc. Provide your physical and logical topology based on your scenario. You can find more examples on the internet. Do not hesitate to surf.

Scenario:

Imagine an office environment where different departments need to be separated for security and management purposes. The network is segmented into VLANs for the IT department, HR department, Sales department, and Guests. The VLANs will be set up as follows:

* VLAN 10: IT Department

1. IP Range : 192.168.10.0/24
2. Subnet Mask : 255.255.255.0
3. Default Gateway : 192.168.10.1
4. PCs : IT1 and IT2
5. IP Address used : 192.168.10.2 and 192.168.10.3

* VLAN 20: HR Department

1. IP Range : 192.168.20.0/24
2. Subnet Mask : 255.255.255.0
3. Default Gateway : 192.168.20.1
4. PCs : HR1 and HR2
5. IP Address used : 192.168.20.2 and 192.168.20.3

* VLAN 30: Sales Department

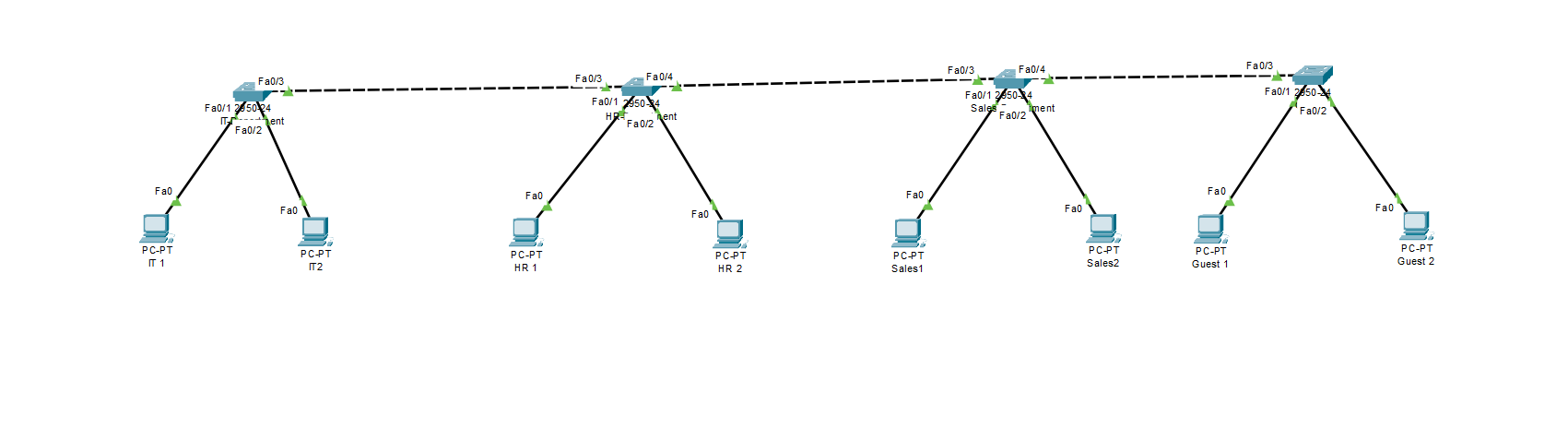
1. IP Range : 192.168.30.0/24
2. Subnet Mask : 255.255.255.0
3. Default Gateway : 192.168.30.1
4. PCs : Sales1 and Sales2
5. IP Address used : 192.168.30.2 and 192.168.30.3

* VLAN 40: Guests

1. IP Range : 192.168.40.0/24
2. Subnet Mask : 255.255.255.0
3. Default Gateway : 192.168.40.1
4. PCs : Guest1 and Guest2
5. IP Address used : 192.168.40.2 and 192.168.40.3

**Answer:**

1. Physical Topology



Configuration Example on a Cisco Switch:

Switch 1 Configuration for VLANs:

|  |
| --- |
| Switch1> enable  Switch1# configure terminal  # Creating VLAN 10 for IT Department  Switch1(config)# vlan 10  Switch1(config-vlan)# name IT\_Department  # Creating VLAN 20 for HR Department  Switch1(config)# vlan 20  Switch1(config-vlan)# name HR\_Department  # Creating VLAN 30 for Sales Department  Switch1(config)# vlan 30  Switch1(config-vlan)# name Sales\_Department  # Creating VLAN 40 for Guests  Switch1(config)# vlan 40  Switch1(config-vlan)# name Guests  # Assigning ports to VLANs  Switch1(config)# interface FastEthernet 0/1  Switch1(config-if)# switchport mode access  Switch1(config-if)# switchport access vlan 10  Switch1(config)# interface FastEthernet 0/2  Switch1(config-if)# switchport mode access  Switch1(config-if)# switchport access vlan 20  Switch1(config)# interface FastEthernet 0/3  Switch1(config-if)# switchport mode access  Switch1(config-if)# switchport access vlan 30  Switch1(config)# interface FastEthernet 0/4  Switch1(config-if)# switchport mode access  Switch1(config-if)# switchport access vlan 40  Switch1(config)# exit  Switch1# write memory |

This scenario provides a structured network design with different VLANs for various departments, ensuring both segregation and security in a multi-switched environment. This kind of setup can be applied to any modern office to efficiently manage and secure network traffic.

# References

[1] J. Vance, “What is a VLAN and how does it work?,” NetworkWorld. [Online]. Available: https://www.networkworld.com/article/971100/what-is-a-vlan-and-how-does-it-work.html

[2] P. Christensson, “VLAN,” TechTerms.com. [Online]. Available: https://techterms.com/definition/vlan

[3] B. Leo, “What is VLAN? Types, Advantages, Example,” Guru99. [Online]. Available: https://www.guru99.com/vlan-definition-types-advantages.html

[4] A. Fariza Noor, “VLAN: Pengertian, Fungsi, Cara Kerja, dan Jenis-Jenisnya,” Sekawan Media. [Online]. Available: https://www.sekawanmedia.co.id/blog/pengertian-vlan/

[5] A. Nugroho, “VLAN: Pengertian, Fungsi dan Cara Kerjanya,” Qwords. [Online]. Available: https://qwords.com/blog/vlan-adalah/

[6] M. Maulana, “VLAN Adalah : Definisi , Manfaat, Contoh & Jenisnya,” ITBOX. [Online]. Available: https://itbox.id/blog/vlan-adalah/

[7] Admin, “Broadcast domain,” Network Lesson.

[8] N. Brightwood, “How VLANs Influence Broadcast Domains: A Detailed Guide,” Net Sec Cloud (NSC). [Online]. Available: https://netseccloud.com/vlan-influence-broadcast-domains

[9] H. Andrea, “8 Different Types of VLANs in TCP/IP Networks,” Networks Training. [Online]. Available: https://www.networkstraining.com/different-types-of-vlans/