PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

MINISTRV OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH KASDI MERBAH OUARGLA UNIVERSITY

Faculty of New Information and Communication Technologies

Department of Computer Science

Academic Master's Thesis

Field: Computer Science

Specialization: NAS

Design and Implementation of a Dynamic VLAN In Large Entreprise Network

Presented by: Bensaci Abdelkeddouss_Bettaher Hamza

Evaluation date: 15/06/2025 Before the Jury:

Djeddar Afrah	Supervisor	UKM Ouargla
Azzaoui Nadjat	President	UKM Ouargla
Messaaid Abdelssalam	Examiner	UKM Ouargla

Academic year: 2024/2025

PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

MINISTRV OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH KASDI MERBAH OUARGLA UNIVERSITY

Faculty of New Information and Communication Technologies

Department of Computer Science

Academic Master's Thesis

Field: Computer Science

Specialization: NAS

Design and Implementation of a Dynamic VLAN In Large Entreprise Network

Presented by: Bensaci Abdelkeddouss_Bettaher Hamza

Evaluation date: 15/06/2025 Before the Jury:

Djeddar Afrah	Supervisor	UKM Ouargla
Azzaoui Nadjat	President	UKM Ouargla
Messaaid Abdelssalam	Examiner	UKM Ouargla

Academic year: 2024/2025

ACKNOWLEDGMENTS

First and foremost, we praise and thank Allah (SWT) for His countless blessings, wisdom, and mercy, which guided and sustained us through every step of this research. Without His grace, this accomplishment would not have been possible.

We owe our deepest gratitude to our families, whose endless love, patience, and encouragement gave us strength during the most challenging times. Their unwavering belief in us was our greatest motivation.

A special thanks to our supervisor, Miss Djeddar, for her expert guidance, insightful feedback, and constant support throughout this journey. Her dedication and advice were instrumental in shaping this work.

We also express our sincere appreciation to the faculty and staff of the Computer Science and Information Technology Department at Kasdi Merbah University of Ouargla for their knowledge, support, and the academic foundation they provided.

Finally, we thank our friends and peers for their companionship, encouragement, and shared experiences, which made this journey more enriching and memorable.

SUMMARY

TABLE OF CONTENTS

Abstract :

This report presents a comprehensive study on Virtual Local Area Networks (VLANs), focusing on their design and implementation within traditional local networks. The main objective of this work is to explore how VLAN technology allows logical segmentation of network resources and users, overcoming the limitations imposed by physical architecture such as geographical constraints and addressing issues.

The implementation of VLANs significantly enhances overall network performance and security. By logically grouping users and resources, regardless of their physical location, VLANs provide enterprises with greater flexibility in managing internal communications and enforcing access control policies.

This project also highlights various configuration methods, inter-VLAN routing techniques, and practical deployment scenarios, demonstrating the importance of VLANs in modern network infrastructures.

Keywords: VLANs, Trunk, Access, ISL, VTP, Tagging

الملخص

يهدف هذا العمل إلى دراسة وتصميم وتنفيذ الشبكات المحلية الافتراضية (VLANs)، وذلك بهدف تمكين التقسيم المنطقي للمستخدمين والموارد داخل الشبكات المحلية التقليدية، مما يسمح بالتغلب على قيود البنية الفيزيائية مثل القيود الجغرافية ومشاكل التوجيه.

تُعد الشبكات المحلية الافتراضية حلاً فعّالًا لتحسين الأداء العام للشبكة وتعزيز الأمان فيها. وتُستخدم هذه التقنية بشكل واسع من قبل المؤسسات لتجميع المستخدمين ضمن مجموعات منطقية بغض النظر عن مواقعهم المادية، مما يسهّل إدارة الشبكة ويضمن تطبيق سياسات الأمان بكفاءة.

تضمن المشروع أيضًا استعراضًا لمختلف طرق الإعداد، وتقنيات التوجيه بين الشبكات الافتراضية، بالإضافة إلى سيناريوهات تنفيذية توضح أهمية استخدام VLANs في البنية التحتية الحديثة للشبكات.

الكلمات المفتاحية: شبكات VLAN، الربط الأساسي (Trunk)، منفذ الوصول ((Access، ISL، VTP، وضع العلامات (Tagging).

General Introduction

General Introduction

A computer network enables multiple devices (including computers in a broad sense) to communicate with each other in order to facilitate the exchange of information. This includes file transfers, resource sharing such as printers and data, messaging services, and the remote execution of applications .

From the user's perspective, the network should be as transparent as possible. In other words, applications must be able to establish communication with the rest of the network automatically, without requiring constant user intervention .

As in the broader field of computing, the evolution of successive technologies has led to the emergence of various networking solutions. These solutions are often based on very different principles, although many of them claim to conform to standardized protocols .

Among the more recent developments in networking is the concept of Virtual Local Area Networks (VLANs), which represent one of the newer technologies introduced in the last few years. Although it appeared later than many traditional networking techniques, VLAN technology has recently begun to gain widespread recognition and adoption .

The rapid expansion of local area networks (LANs), along with the need to minimize the high costs of networking equipment while maintaining performance and ensuring security, has created an ideal environment for the adoption and growth of VLANs. Today, they are widely implemented across most modern network infrastructures.

However, contrary to popular belief, VLANs are not as simple as many people assume. In fact, they involve a wide range of hardware and software components and constitute a comprehensive field of study in their own right. VLANs incorporate a combination of protocols, rules, and guidelines that every network administrator should thoroughly understand .

Unfortunately, much of the available documentation on VLANs is either insufficient or superficial. It often touches briefly on the subject without offering readers a clear and structured understanding of how VLANs actually work or how they should be properly configured and managed.

Problem Statement:

The increasing number of internet users over time has led to the widespread deployment of networks, which in turn has highlighted the inflexibility of traditional network segmentation. This growth has resulted in challenges related to network management, a noticeable decline in performance, and a reduction in overall network security an aspect that remains one of the most critical factors in effective network operation .

Given the necessity for improved security — a core principle in modern networking — various solutions have been developed. Among these, Virtual Local Area Networks (VLANs) have emerged as a powerful approach, offering the ability to overcome limitations imposed by physical network architecture, such as geographical constraints and addressing issues.

VLANs enhance overall network performance by logically grouping users and resources. Enterprises frequently use VLANs to ensure logical segmentation of user groups regardless of their physical location. Additionally, VLANs can significantly improve network scalability, security, and manageability. Routers within VLAN topologies provide services such as broadcast filtering, traffic control, and enhanced security .

When properly designed and configured, VLANs serve as powerful tools for network administrators, simplifying operations related to adding, moving, or modifying network components. They also help improve network security and facilitate control over Layer 3 broadcast domains. However, improper VLAN configuration can lead to performance degradation or even network failure. Therefore, it is essential to understand how VLANs are implemented across different switches during the network design phase .

Before diving into the details of VLANs, it is highly recommended to first provide an overview of computer networks — including their definition, topologies, classifications, and commonly used protocols — in order to establish a solid foundation for understanding VLAN technology.

Chapter 1:
Fundamentals of VLANs

1. Introduction :

This chapter provides an in-depth study of the fundamental concepts of VLANs (Virtual Local Area Networks) and outlines the essential steps required to design networks that offer improved performance and efficiency. The focus will be on achieving key objectives such as:

-Enhancing the flexibility of network segmentation .

-Simplifying network management .

-Significantly improving network performance .

-Strengthening network security.

-Implementing scalable and cost-effective networking solutions.

In addition, this chapter will explore other benefits offered by VLAN technology, with a detailed examination of their implementation, advantages, and best practices for deployment.

2. Definitions of VLANs (Architectural Model):

A VLAN (Virtual Local Area Network) is a logical local network that groups together a set of devices based on software configuration rather than physical connections.

In a traditional LAN (Local Area Network), communication between devices is determined by the physical architecture. However, with Virtual Local Area Networks (VLANs), it becomes possible to overcome the limitations imposed by physical infrastructure — such as geographical constraints and addressing issues — by implementing a logical (software-based) segmentation. This segmentation can be based on various criteria including MAC addresses, switch ports, protocols, and more.

Devices or users within a VLAN can be grouped according to function, department, or application, regardless of their physical location within the network. Devices in one VLAN can only communicate directly with other devices in the same VLAN. Just as routers are used to connect different LAN segments, they also enable communication between different VLANs.

VLANs improve overall network performance by logically grouping users and resources. Enterprises often use VLANs to ensure logical separation of user groups regardless of their physical location. For example, Marketing department users are assigned to the Marketing VLAN, while Engineering users are associated with the Engineering VLAN.

VLANs enhance network scalability, security, and manageability. Routers in VLAN topologies provide services such as broadcast filtering, traffic control, and enhanced security features.

When properly designed and configured, VLANs serve as powerful tools for network administrators. They simplify operations related to adding, moving, or modifying network

components. Additionally, VLANs improve network security and facilitate control over Layer 3 broadcasts. However, improper VLAN configuration can degrade network performance or even prevent proper network operation. Therefore, it is essential to understand how VLANs are implemented across different switches during the network design phase.

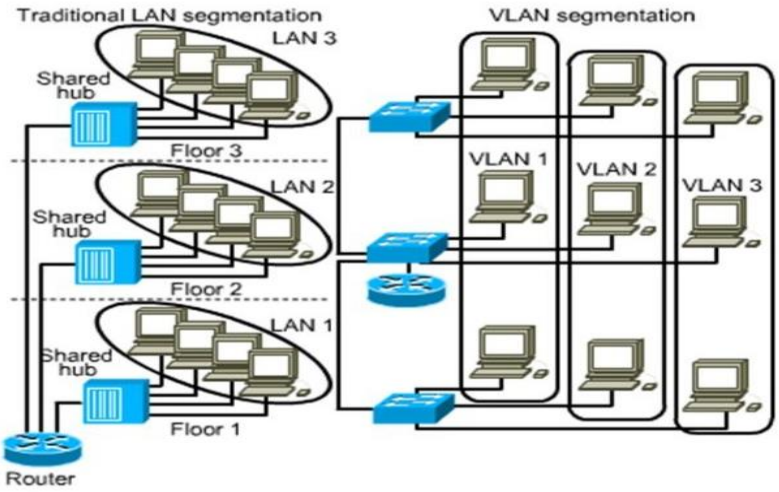

Fig 1: comparison between classic network and virtual network.

3. Objectives and Characteristics of VLANs:

3.1. Objectives of VLANs:

The primary objective of a VLAN is to define logical subnetworks that function as separate broadcast domains. This mechanism allows multiple virtual networks to be configured and managed from a single central console, even though they may operate as distinct physical networks.

Generally, enterprises choose VLAN technology for the following key reasons:

-Security / Mobility :

VLANs provide an additional layer of security that is not available in shared-media networks. In a switched network, data packets are delivered only to the intended recipient. Administrators can logically isolate sensitive information within specific VLANs, regardless of the physical location of the devices. Moreover, traffic monitoring on a specific port using a traffic analyzer will only capture data related to that particular port.

-Performance / Quality of Service (QoS) :

Originally, switching improved network performance compared to shared media by reducing the size of collision domains. By grouping users into logical networks, VLANs further enhance performance by limiting broadcast traffic to relevant users within the same functional or workgroup. Additionally, less traffic needs to be routed between VLANs, which reduces the latency introduced by routers.

-Network Management :

VLANs allow for easy, flexible, and cost-effective reconfiguration of logical groups. They make large networks more manageable by enabling centralized configuration of devices located in different physical locations. Since VLANs are independent of the physical network topology, logically grouped users can be separated physically yet remain part of the same network. This offers great flexibility when evolving an existing network architecture without changing its physical layout.

-Ease of Relocation :

Even when relocating equipment, the software-based nature of VLANs eliminates the need to reconfigure the physical topology. As a result, VLANs offer administrators greater freedom in organizing their network infrastructure through logical configuration rather than physical adjustments.

3.2. Characteristics of VLANs:

VLANs are characterized by the following common features:

-Eliminates Physical Constraints :

VLANs remove the physical limitations associated with communication within a workgroup, allowing devices to be logically grouped regardless of their physical location.

-Scalability Across Locations :

A VLAN can span an entire building, connect multiple buildings, or even extend across a wider network (WAN), providing flexibility in network design and expansion.

-Support for Multiple VLAN Membership :

A single workstation or device can belong to multiple VLANs simultaneously, enabling flexible access to different network segments based on user needs or roles.

4. Advantages and Limitations of VLANs :

4.1. Advantages of VLANs:

-Flexible Network Segmentation :

Devices and resources that frequently exchange data can be logically grouped together, regardless of their physical location . This allows for a more efficient organization based on function or department rather than physical placement.

-Support for Multiple VLAN Membership :

A single device may belong to multiple VLANs at the same time, allowing flexible access to various network segments depending on user roles or needs.

-Simplified Network Management :

Adding new devices or relocating existing ones is made easier without the need to reconfigure physical connections in the wiring closet . This significantly reduces administrative overhead and minimizes service interruption.

-Improved Network Performance :

By limiting traffic within the associated VLAN, unnecessary broadcast traffic is minimized, which results in better use of available bandwidth and enhanced overall performance.

-Better Utilization of Network Servers :

When a server supports VLAN tagging, it can be assigned to multiple VLANs simultaneously. This reduces the amount of routed traffic (processed at higher protocol layers such as IP), thus optimizing communication efficiency. Similar to partitioning a hard drive to reduce fragmentation and improve system performance,VLANs help optimize network usage

-Enhanced Network Security :

The logical boundaries created by VLANs can only be crossed through routing mechanisms, which allows administrators to enforce stricter access control policies and isolate sensitive information from unauthorized users.

-Cost-Effective and Scalable Technology :

Thanks to its simplicity and compatibility with existing technologies, VLAN deployment over Ethernet provides a scalable and affordable solution suitable for organizations of all sizes.

-Bandwidth Regulation :

One of the key features of Ethernet networks is the ability to send messages to all connected devices via broadcast or multicast. However, this type of transmission increases overall network traffic within switching components. VLANs help address this issue by restricting broadcasts to only those devices within the same VLAN.

4.2. Limitations of VLANs:

-Increased Latency in Inter-Subnet Communications :

Communication between different VLANs often requires routing, which can introduce additional latency compared to communication within the same broadcast domain.

-More Complex IP Address Management :

The use of multiple VLANs may complicate the administration of IP addresses, as each VLAN typically requires its own subnet, leading to more planning and coordination.

5. Types of VLANs:

In network devices, VLANs are associated with switch ports using a mapping table. VLAN membership can be determined based on the port, MAC address, network protocol, or IP subnet. Trunk ports are configured to allow specific VLANs to pass through.

- **Port-Based VLAN:**

This is the default and most widely used method in enterprise networks. Each port is assigned a Port VLAN ID (PVID), and any device connected to that port automatically becomes part of the corresponding VLAN.

-**Security:** Prevents unauthorized access unless the attacker connects to a port assigned to the target VLAN.

-Limitation: Inflexible when moving devices — requires manual reconfiguration. Can be enhanced with 802.1X authentication for dynamic VLAN assignment based on user identity.

- **MAC Address-Based VLAN:**

VLAN assignment is based on the source MAC address of the device. Switches maintain MAC-to-VLAN mappings.

-**Advantages:** More flexible and centralized management.

-**Limitations:** Vulnerable to MAC spoofing attacks.

- **Protocol-Based VLAN**

Frames are assigned to VLANs based on the Layer 3 protocol (e.g., IP, IPX.(

-Use Case: Useful for traffic prioritization using 802.1p tagging.

-Limitation: Rarely used due to processing overhead from packet inspection.

- **Subnet (IP-Based) VLAN**

Devices are grouped into VLANs based on their source IP subnet.

-**Advantages:** Enables centralized VLAN management.

-**Limitations:** Slower performance due to packet decapsulation; vulnerable to IP spoofing. Not commonly used in enterprises.

- **Rule-Based VLAN**

A newer approach where switches analyze frame content to determine VLAN membership. Rules can be based on various criteria such as TCP ports, multicast addresses, or service types.

-**Flexibility:** Allows advanced segmentation beyond traditional methods.

-**Use Cases**: Suitable for dynamic environments requiring fine-grained control.

6. Operation of VLANs:

VLANs that span multiple switches are categorized into two types:

-Implicit VLANs: When an Ethernet frame is forwarded from one switch to another, a lookup table determines which VLAN the frame belongs to.

-Explicit VLANs: A VLAN membership tag is added to each Ethernet frame, explicitly identifying its associated VLAN

The switch follows rules defined by the VLAN standard to ensure that frames are delivered to the appropriate network ports (connection points for devices), even when devices are connected to different switches.

It is through these tags and the set of rules configured by the network administrator that the switch can determine where a frame should be forwarded, broadcasted, or filtered.

6.1. VLANs and Standards:

Early VLAN implementations were complex and difficult to manage across networks. Initially, VLANs had to be configured individually on each switch, making it challenging to deploy them across large or distributed networks. Each switch manufacturer used a different approach, which added to the complexity.

To address these issues, the concept of VLAN trunking was introduced. Trunking allows multiple VLANs to be defined across an organization by adding special tags to Ethernet frames, identifying the VLAN to which they belong. This tagging enables multiple VLANs to share a common backbone or trunk link.

VLAN trunking is standardized through the widely adopted IEEE 802.1Q protocol. In contrast, Cisco's ISL (Inter-Switch Link) is a proprietary trunking protocol that can be used in most Cisco networks.

6.2. Trunking:

The concept of *trunking* originated in radio and telephone technologies. In radio communication, a trunk is a single channel that carries multiple radio signals.

In the telecommunications industry, trunking refers to the communication channel between two points, typically used to carry multiple phone calls over a shared line.

This principle was later adopted in data networking, where it is now widely applied in network switching technologies. Today, a trunk represents both a physical and logical connection between two switches, allowing network traffic from multiple VLANs to be transmitted across a single link.

7. Principles of the VTP Protocol

The VLAN Trunking Protocol (VTP) is essential for propagating VLAN configurations across multiple switches in a network. To achieve this, a trunk link is established between switches to carry traffic from multiple VLANs.

This trunk link allows frames from different VLANs to be transmitted between switches. In order for switches to identify which VLAN a frame belongs to, frame tagging is used. VTP supports two tagging protocols: Cisco ISL (proprietary) and IEEE 802.1Q (standard). The latter is widely used and is typically the default method.

The main function of VTP is to maintain consistent VLAN configuration across a common administrative domain. It is a Layer 2 messaging protocol that manages the addition, deletion, and renaming of VLANs within a network . VTP enables centralized configuration changes to be automatically propagated to all other switches in the same domain.

VTP messages are encapsulated in ISL or IEEE 802.1Q frames and sent over multi-VLAN links. In IEEE 802.1Q, a 4-byte field is added to the Ethernet frame to carry the VLAN ID.

While regular switch ports are assigned to a single VLAN, trunk ports can carry traffic from all VLANs by default. This allows VLANs to be configured on one switch and then automatically shared with others in the same VTP domain via VTP updates.

7.1. VTP Modes:

A switch running VTP can operate in one of three modes:

-Server Mode :

VTP servers can create, modify, and delete VLANs. They store VLAN configuration in NVRAM and send VTP advertisements through all trunk ports. This is the default mode for most Cisco switches.

-Client Mode :

VTP clients receive and apply VLAN changes from VTP servers but cannot make any local modifications. This mode is useful for switches with limited memory.

-Transparent Mode :

Transparent switches forward VTP advertisements but do not process or apply the received VLAN information. In VTP Version 1, transparent switches do not relay VTP messages; in Version 2, they relay them without applying the changes.

7.2. Revision Number

When VTP is enabled, the server sends VLAN information in special frames called advertisements. Each advertisement includes a revision number. Every time a change is made

on the server, the revision number increases. When a client receives an advertisement with a higher revision number, it replaces its local VLAN database with the updated one.

It's important to ensure that when adding a new switch to the network, its revision number is set to zero, to prevent it from overwriting the existing VLAN database. To reset the revision number:

-Change the switch mode to Transparent, then back to Server.

-Temporarily change the VTP domain name, then restore the correct one.

7.3. Operation of VTP

A VTP domain consists of interconnected switches that share the same domain name. A switch can only belong to one VTP domain at a time.

When a VTP message is sent, it is encapsulated in a trunking protocol frame such as ISL or IEEE 802.1Q.

In ISL-based VTP, the VTP header varies depending on the message type, but generally includes the following fields:

-VTP Version: either Version 1 or 2

-Message Type: indicates one of four types of VTP messages

-Domain Name Length: specifies the length of the domain name

-Domain Name: the configured name of the VTP domain

8 .Types of VTP Advertisements and Messages:

Using VTP, each switch advertises its management domain, configuration revision number, known VLANs, and their parameters through multi-VLAN ports. These advertisements are sent to a multicast address so that all neighboring switches can receive them, although they are not forwarded using standard bridging methods . All switches in the same management domain learn about new VLAN configurations from the sending switch. A new VLAN only needs to be created on one switch within the domain; other switches will automatically update their VLAN databases.

By default, VTP advertisements start with a revision number of 0. Each time a change is made, the revision number increases by 1. This number can go up to 2,147,483,648, after which it resets to zero.

There are two main types of VTP advertisements:

-Requests — Sent by clients when they need VLAN information at startup.

-Responses — Sent by servers in reply to client requests.

There are three types of VTP messages:

-Advertisement Request — Triggered when a client requests VLAN information.

-Summary Advertisement — Contains the VTP domain name and the current revision number. Servers send these every 5 minutes to ensure consistency across the network.

-Subset Advertisement — Carries detailed VLAN information such as VLAN ID, name, type, and status. These are generated when a VLAN is created, deleted, renamed, or activated/deactivated.

When a receiving switch detects an advertisement with a higher revision number than its own, it sends an advertisement request to obtain the updated VLAN data.

VTP advertisements may include the following information:

-Management Domain Name: Advertisements with mismatched domain names are ignored.

-Configuration Revision Number: A higher number indicates a more recent configuration.

-MD5 Digest: Used for authentication when a password is set. If the digest does not match, the update is rejected.

-Updater Identity: Identifies the switch that sent the summary advertisement.

8.1. IEEE 802.1Q:

The IEEE 802.1Q standard provides a widely adopted tagging mechanism implemented in network equipment from various vendors. This document is based on this standard. Similar to the Cisco ISL encapsulation method, IEEE 802.1Q adds a 4-byte tag to the Ethernet frame header.

IEEE 802.1Q Tag Structure

-Tag Protocol Identifier (TPID):

The first 16 bits identify the tagging protocol. For IEEE 802.1Q, this value is set to 0x8100.

-Priority Field :

A 3-bit field used to define frame priority according to IEEE 802.1p. It supports 8 levels (0–7) of prioritization within VLANs, independent of IP-based priority mechanisms.

-Canonical Format Indicator (CFI):

A 1-bit field ensuring compatibility between Ethernet and Token Ring MAC addresses. In Ethernet networks, this bit is always set to 0. If a switch receives a frame with CFI set to 1, it will not forward it, as it is intended for untagged ports.

-VLAN Identifier (VID):

A 12-bit field that identifies the VLAN to which the frame belongs. It allows up to 4094 VLANs (values 1 to 4094), as values 0 and 4095 are reserved.

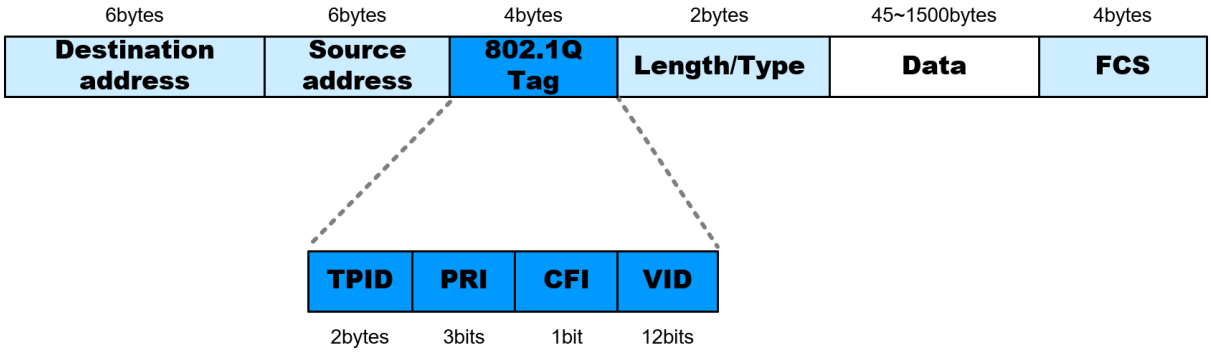

Fig 2: IEEE 802.1Q

9. Conclusion

At the end of this chapter, we have presented an overview of the mechanisms used to simplify the creation of VLANs, whether at the switch or router level.

We are now able to distinguish between the different techniques used to design a more secure and efficient network.

In the next chapter, we will go into detail about the configuration steps and the various methods used in practice.

Chapter 2:
VLAN Configuration

1. Introduction :

By the end of this chapter, we will be able to:

-Install, configure, and maintain routers or switches .

-Implement VLAN switching or inter-VLAN routing .

-Interconnect LAN networks using virtual networking solutions, regardless of the router/switch model .

-Manage routers and switches under optimal security conditions.

2 .Configuration Methods (Switch-Router):

- Connecting via Console Cable (Initial Setup):

When to Use?

First time setup (no IP configured).

Password recovery.

When network access is unavailable.

Hardware Needed:

Console Cable (RJ-45 to USB/Serial).

Terminal Emulator (PuTTY, Tera Term, SecureCRT).

- Connecting via SSH (Secure Remote Access)

When to Use?

Secure remote management over the network Steps:

Prerequisites:

The device must have an IP address configured.

SSH must be enabled (on Cisco: ip ssh version 2).

- Connecting via Telnet (Unencrypted Remote Access)

When to Use?

Legacy systems (not recommended due to security risks).

Steps:

Prerequisites:

Telnet must be enabled (transport input telnet in Cisco) .

3. Inter-VLAN Switching:

3.1. Definition of a Switch :

A switch is a network device that serves as a central connection point for workstations, servers, hubs, and other switches .

Modern switches are essentially multi-port bridges, and they represent the current standard technology for Ethernet LANs using a star topology. A switch provides multiple dedicated point-to-point virtual circuits, making data collisions practically nonexistent .

When a new switch is deployed, it typically comes with default factory settings, which rarely meet all the requirements of a network administrator. Therefore, switches can be configured and managed via a Command Line Interface (CLI). Increasingly, network devices are also managed through a web-based graphical interface for ease of use .

3.2. Switching Modes:

3.2.1. Cut-Through Switching :

In cut-through mode, the switch starts forwarding a frame to the destination port as soon as it reads the MAC address. This method results in very low latency, making it ideal for high-speed networks where speed is more critical than error checking .

3.2.2. Store-and-Forward Switching :

In this mode, the switch waits until it receives the entire frame before forwarding it. It checks the Frame Check Sequence (FCS) for errors and discards corrupted frames. While this method introduces more delay, it ensures better data integrity .

3.2.3. Fragment-Free Switching:

This is an intermediate approach. The switch reads the first 64 bytes of the frame (which includes the header), then begins forwarding the frame. It checks the header information to ensure correct handling and delivery while reducing processing time compared to store-and-forward .

3.3. Command Modes of Switches :

Switches support multiple command-line interface (CLI) modes for configuration and management .

-User EXEC Mode :

This is the default mode when logging into a switch. It allows basic monitoring commands and terminal settings. The prompt is typically indicated by .<

-Privileged EXEC Mode :

Accessed using the enable command, this mode provides all User EXEC commands plus additional ones like configure. The prompt changes to .#

-Global Configuration Mode :

Entered from Privileged EXEC mode using the configure command. This mode is used to apply configuration changes to the device .

Access to Privileged EXEC mode should be secured with a password to prevent unauthorized configuration changes .

4. Port Modes :

On a switch, ports are typically categorized as either access ports or trunk ports .

-An access port carries traffic for only one VLAN and is usually used to connect end devices such as PCs or printers.

-A trunk port, on the other hand, can carry traffic from multiple VLANs simultaneously. It is commonly used to connect switches, routers, or servers equipped with 802.1Q network cards .

In short, an access port is not a trunk port, and vice versa .

However, on Cisco switches, it is possible to configure a port in dynamic mode using the Dynamic Trunking Protocol (DTP) — a Cisco proprietary protocol that negotiates the port's mode (access or trunk) automatically with the connected device .

5. Different Types of VLANs :

There are four main types of VLANs:

-Default VLAN: The VLAN assigned to all ports of a switch by default, usually VLAN 1 .

-User VLAN: A VLAN used to separate user traffic from other types of network traffic .

-Management VLAN: A dedicated VLAN used for managing network devices (e.g., switches and routers) remotely .

-Native VLAN: A special VLAN used on trunk ports to carry untagged traffic in IEEE 802.1Q trunking .

6. Verifying the Switch’s Default Configuration :

When a switch is powered on for the first time, it loads default settings from its running configuration. By default :

-The hostname is set to "Switch ."

-No passwords are configured on the console or virtual terminal (VTY) lines.

An IP address can be assigned to the switch for management purposes. This is done by configuring the VLAN 1 interface. By default, the switch does not have an IP address assigned .

All physical ports are set to auto-negotiation mode and are assigned to VLAN 1 by default .

The default flash directory contains :

-The IOS image file

-A file named env_vars

-A subdirectory named html

After configuration, this directory may also include:

-config.text (the saved configuration file(

-vlan.dat (the VLAN database .(

However, initially, the flash memory does not contain any saved configuration or VLAN database files .

6.1. Switch Configuration :

A switch may already be preconfigured and only require setting passwords to access user or privileged mode. You can access the configuration mode from the privileged EXEC mode .

In the CLI (Command Line Interface), the default command prompt for privileged mode is Switch#, while in user mode it is Switch .

To ensure the new configuration replaces any existing one, follow these steps :

-Delete all existing VLAN information by removing the VLAN database file (vlan.dat) from flash memory .

-Delete the saved startup configuration file (startup-config) .

-Reload the switch to apply the changes .

6.2. Managing the MAC Address Table :

Switches learn the MAC addresses of connected devices by examining the source address of received frames. These addresses are stored in the MAC address table, which is used to forward frames to the correct destination port .

To display the learned MAC addresses, use the command :

```
show mac-address-table
```

Instead of waiting for dynamic entries to expire, the network administrator can manually clear the table using the command :

```
clear mac-address-table
```

Both commands are executed in privileged EXEC mode .

6.3. Configuring Static MAC Addresses:

You may want to assign a static MAC address to a specific interface for several reasons, such as:

- The MAC address should never be automatically removed by the switch.

- A server or specific workstation is connected to the port and its MAC address is known.

- To enhance network security.

To configure a static MAC address entry on a switch, use the following command in global configuration mode:

```
Switch(config)# mac-address-table static <host-mac-address> interface
FastEthernet<interface-number> vlan <vlan-name>
```

To remove the static entry, use the no form of the command:

```
Switch(config)# no mac-address-table static <host-mac-address> interface
FastEthernet<interface-number> vlan <vlan-name>.
```

7 .Creating VLANs :

To create a VLAN, you must enter the VLAN configuration mode using the command :

```
Switch_A# vlan database
```

Then, create a VLAN using the following command :

```
Switch_A(vlan)# vlan <number> [name <name>?]
```

After creating the VLAN, exit the mode :

```
Switch_A(vlan)# exit
```

This saves the VLAN configuration in the vlan.dat file stored in flash memory .

In a static VLAN configuration, assign switch ports to the VLAN by entering interface configuration mode:

```
Switch_A(config)# interface fastEthernet <interface-number>
Switch_A(config-if)# switchport mode access
Switch_A(config-if)# switchport access vlan <vlan-number>
```

These commands assign the specified interface to the desired VLAN .

Once completed, the VLAN configuration is applied on the switch .

7.1. Saving the VLAN Configuration :

It is often useful to keep a copy of the VLAN configuration as a text file for backup or auditing purposes .

The switch configuration, including VLAN settings, can be saved using the following command :

```
copy running-config tftp
```

Alternatively, you can use the HyperTerminal capture feature to save the configuration by starting a capture session and then entering commands such as :

```
show running-config
```

```
show vlan
```

This allows you to store the configuration output in a text file on your computer .

7.2. Deleting a VLAN :

Deleting a VLAN on a Cisco IOS-based switch is similar to removing a configuration command on a router .

You can remove the VLAN assignment by using the no form of the command .

To delete an entire VLAN from the switch, use the following commands :

```
Switch# vlan database
```

```
Switch(vlan)# no vlan <vlan-id>
```

When a VLAN is deleted, all ports assigned to that VLAN become inactive. However, these ports remain associated with the deleted VLAN until they are manually reassigned to another VLAN.

To set the VTP mode on the switch, use the following command:

```
Switch(vlan)# vtp {client | server | transparent}
```

This allows the switch to operate in the appropriate VTP mode for VLAN management .

8 .Configuring a VTP Domain

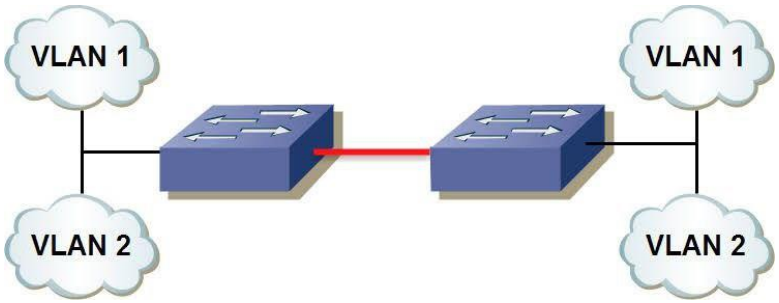

Fig 3: Use of Trunk between switches

To propagate VLAN configurations between switches, they must belong to the same VTP domain. This domain operates in a hierarchical structure: the VTP server sends VLAN updates, while the VTP client receives and applies these changes automatically .

Assume Switch_A is the VTP server and Switch_B is the VTP client. The required commands are as follows :

On Switch_A (VTP Server):

```
Switch_A# vlan database
Switch_A(vlan)# vtp domain <domain-name>
Switch_A(vlan)# vtp server
Switch_A(vlan)# exit
```

On Switch_B (VTP Client):

```
Switch_B# vlan database
Switch_B(vlan)# vtp domain <domain-name>
Switch_B(vlan)# vtp client
Switch_B(vlan)# exit
```

A trunk link must be configured between the two switches to carry tagged VLAN traffic. A crossover cable is typically used between switches. A trunk is a physical connection that carries multiple logical VLANs. To configure trunking on both switches:

```
Switch_A(config)# interface fastEthernet <interface-number>
Switch_A(config-if)# switchport mode trunk
Switch_A(config-if)# switchport trunk encapsulation dot1q
Switch_B(config)# interface fastEthernet <interface-number>
Switch_B(config-if)# switchport mode trunk
Switch_B(config-if)# switchport trunk encapsulation dot1q
```

Once this is done, the VLAN configuration from the VTP server will be sent to the client. However, you still need to manually assign ports on the client switch to the appropriate VLANs, as the received configuration only lists the VLAN names and IDs:

```
Switch_B(config)# interface fastEthernet <interface-number>
Switch_B(config-if)# switchport mode access
Switch_B(config-if)# switchport access vlan <vlan-id>
```

9 .Physical and Logical Interfaces :

In a traditional setup, a network with four VLANs would require four separate physical connections between the switch and the router .

With the introduction of technologies like ISL (Inter-Switch Link), network designers began using single physical links to carry traffic from multiple VLANs between routers and switches .

While various trunking protocols such as ISL, IEEE 802.1Q, 802.10, and LANE can be used, Ethernet-based solutions like ISL and 802.1Q are the most common .

Both Cisco ISL and the IEEE 802.1Q standard allow multiple VLANs to share a single physical link using Fast Ethernet .

In this setup:

-The solid line represents the physical connection between the switch and the router.

-The dashed lines represent logical (virtual) interfaces created on the same physical link using subinterfaces .

A router can support multiple logical interfaces over a single physical interface. For example, the physical interface FastEthernet 0/0 can be divided into virtual subinterfaces such as FastEthernet 0/0.1, FastEthernet 0/0.2, and FastEthernet 0/0.3 .

The main advantage of using a multi-VLAN link is the reduction in the number of physical ports required on both the switch and the router. This approach lowers costs and simplifies configuration, making it more scalable than using one link per VLAN .

9.1. Splitting Physical Interfaces into Subinterfaces :

A subinterface is a logical interface created on a physical interface, such as a Fast Ethernet port on a router .

Multiple subinterfaces can be configured on a single physical interface. This allows the router to handle traffic from multiple VLANs using just one physical connection .

To configure subinterfaces, perform the following steps :

-Identify the physical interface

Use the interface command in global configuration mode :

```
Router(config)# interface fastethernet <port-number>
```

-Define VLAN encapsulation

Use the encapsulation command to specify the VLAN associated with the subinterface :

```
Router(config-subif)# encapsulation dot1Q <vlan-id>
```

-Assign an IP address

Set the IP address and subnet mask for the subinterface :

```
Router(config-subif)# ip address <ip-address> <subnet-mask>
```

In this setup :

> -port-number> refers to the physical interface (e.g., FastEthernet 0/0) .

> -vlan-id> identifies the VLAN whose traffic will be handled by that subinterface .

For example, a router may have three subinterfaces — FastEthernet 0/0.1, FastEthernet 0/0.2, and FastEthernet 0/0.3 — each handling traffic for VLANs 1, 20, and 30 respectively .

This approach enables efficient inter-VLAN routing, allowing a single physical link to route traffic for multiple VLANs using standardized trunking protocols like IEEE 802.1Q.

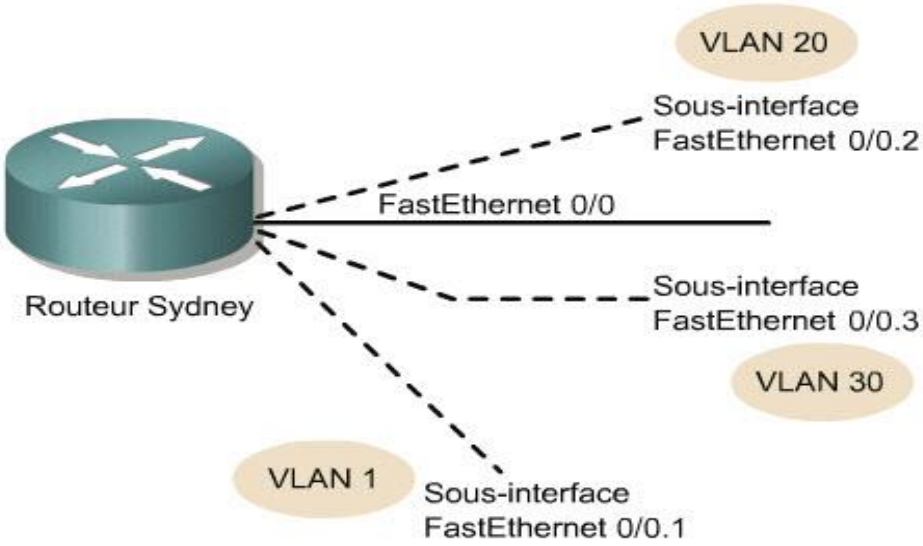

Fig 4: VLAN by IP address

10.Conclusion

At the end of this chapter, we have covered all the essential steps required to properly configure both **routers** and **switches**, and explored the different types of VLANs — whether **static** or **dynamic** .

After presenting the theoretical procedures, the next chapter will focus on **practical implementation**, allowing us to better illustrate these concepts through hands-on examples and clarify some of the more abstract ideas presented here.

Chapter 3:
Inter-VLAN Routing

1 .Introduction :

A router is a physical component of a network. In simple terms, it acts as a guide: you send it a data packet, and it directs it to the correct destination based on its final target .

In a network like the Internet, many routers work together, communicating with each other to route traffic efficiently. You can think of them as highway interchanges for digital information. If one fails, another can often take over, depending on the overall network architecture .

In our case, the router will be used to implement dynamic VLANs at Layer 3, based on IP addresses and subnets .

2 .Introduction to Inter-VLAN Routing :

2.1. Introduction to Routers :

A router is a specialized type of computer that shares the same basic components as a standard desktop computer .

Just like computers require an operating system to run applications, routers need a software platform — typically Cisco IOS (Internetwork Operating System) — to execute configuration files. These files contain instructions and settings that control incoming and outgoing traffic. More specifically, routers use routing protocols to determine the best path for data packets. The configuration file provides all the necessary information for properly setting up and using the selected routing protocols on the router .

2.2. Router Components :

-CPU :

The Central Processing Unit (CPU) runs the IOS operating system. It is responsible for initializing the system, managing routing processes, and controlling network interfaces. It is typically a microprocessor .

-RAM :

Random Access Memory stores the routing table, fast-switching cache, current configuration file, and packet queues during operation .

-Flash Memory :

Flash memory holds the full IOS software image. By default, the router loads the IOS from flash memory, and it can be executed directly from there. Additional flash memory can be added using SIMM modules or PCMCIA cards .

-NVRAM :

Non-Volatile RAM stores the startup configuration file. It retains data even when the router is powered off and is usually implemented using EEPROM technology .

-ROM :

Read-Only Memory contains the bootstrap code and diagnostic software used during startup. Its main tasks are running hardware diagnostics and loading the IOS from flash into RAM .

-Interfaces :

A router connects to other networks through its interfaces, which are generally categorized as:

-LAN interfaces (e.g., Ethernet or Token Ring ports)

-WAN interfaces (used for wide-area connectivity)

-Console/AUX interfaces (used for management and configuration).

These interfaces may be fixed or modular, depending on the router model.

-In the context of VLANs, routers play a key role in determining the best path for traffic between VLANs, ensuring minimal delay and optimal routing.

Fig 5: the components of a router

2.3. Router User Interface Modes :

The Cisco IOS Command-Line Interface (CLI) uses a hierarchical structure that requires users to enter specific modes depending on the task they want to perform. For example, to configure a router interface, the user must enter interface configuration mode, where all entered commands apply only to that specific interface.

Each configuration mode is indicated by a unique prompt and allows only the relevant commands for that mode.

IOS includes a command interpreter called EXEC mode, which validates and executes user-entered commands.

For security reasons, IOS separates EXEC sessions into two access levels:

-User EXEC mode (basic monitoring commands).

-Privileged EXEC mode (advanced configuration and management)

To enter global configuration mode from privileged mode, use the following command :

Router# configure terminal

Router(config) #

Global configuration mode is the main mode used to make changes to the device's settings. From this mode, you can access several submodes, including :

-Interface mode – for configuring physical or logical interfaces

-Line mode – for managing console, Telnet, or SSH access

-Router mode – for configuring routing protocols

-Subinterface mode – for VLAN tagging and inter-VLAN routing

-Controller mode – for low-level hardware configurations

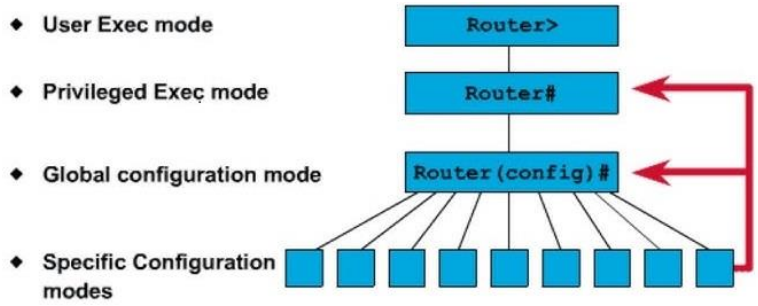

Fig 6: interface modes of Router

2.4. Initialization Cisco Routers :

When a Cisco router starts up, it goes through a boot process that includes loading the bootstrap code, the IOS operating system, and a startup configuration file. If the configuration file is not found, the router enters setup mode. After completing setup, a backup copy of the configuration can be saved to NVRAM.

The main goal of the Cisco IOS boot routines is to start the routing operations. During the boot process, the following steps are performed :

-Verify that the hardware has passed diagnostics and is functioning properly

-Locate and load the Cisco IOS software

-Locate and apply the startup configuration file, or enter setup mode if no configuration is found.

2.5. Management Port Connections:

The console port and the auxiliary (AUX) port are management interfaces on a Cisco router.

These asynchronous serial ports are not intended for regular network connectivity.

At least one of these ports — usually the console port — is required for initial router configuration, as the router has no network settings configured at first boot. A terminal or PC running terminal emulation software (like PuTTY or Tera Term) must be connected to the console port to perform basic setup tasks.

Once the initial configuration is completed via the console or AUX port, the router can be connected to the network for further management and troubleshooting.

Remote configuration can also be done using:

-Telnet/SSH sessions over an IP network

-Modem access connected to the console or AUX .

For troubleshooting and recovery purposes, the console port is preferred because it displays boot messages, debug output, and error logs by default. It can also be used before network services are started or when they fail, making it essential for password recovery and disaster recovery procedures.

2.6. Connecting to the Router Interface:

In most LAN environments, a router connects to the network using an Ethernet or Fast Ethernet interface, typically through a hub or switch. This type of connection requires a straight-through cable. A 10/100BaseTX router interface needs an unshielded twisted pair (UTP) cable of Category 5 or higher.

In some cases, the router may connect directly to a computer or another router. In such situations, a crossover cable is required instead.

It’s important to use the correct type of cable and port. Using the wrong one may prevent communication or even damage the router and other network devices.

Many different types of connections use the same physical connector style. For example:

-Ethernet interfaces

-Basic ISDN ports

-Console and AUX ports

-Integrated CSU/DSU

-Token Ring

All commonly use 8-pin connectors such as RJ-45, RJ-48, or RJ-49.

2.7. Router User Interface:

Cisco IOS uses a Command-Line Interface (CLI) as its primary management environment. This interface is central to almost all Cisco networking devices, although its behavior may vary slightly depending on the device.

The CLI can be accessed in several ways:

-Console connection: A direct serial connection from a computer or terminal to the router's console port, typically used for initial setup.

-AUX port connection: Allows access via a modem or null modem cable connected to the router's AUX port — also useful for remote management.

-Telnet/SSH connection: Requires at least one network interface with an IP address and configured virtual terminal sessions with passwords.

Unlike the first two methods, Telnet requires prior network configuration on the router.

2.7.1. Configuring the Serial Interface :

A serial interface can be configured either from the console or through a virtual terminal line. To configure a serial interface, follow these steps:

1 .Enter global configuration mode

2 .Enter interface configuration mode

3 .Assign an IP address and subnet mask

4 .If a DCE cable is connected, set the clock rate (skip this step if using a DTE cable(

```
Router(config)# interface serial 0/0
Router(config-if)# clock rate 56000
Router(config-if)# no shutdown
```

5 .Activate the interface using the no shutdown command

If the interface is used for IP routing, each serial interface must have an IP address and subnet mask assigned. Use the following commands to configure the IP address:

```
Router(config)# interface serial 0/0
Router(config-if)# ip address <ip-address> <subnet-mask>
```

2.7.2. Configuring the Ethernet Interface:

An Ethernet interface can be configured either from the console or through a virtual terminal session.

If the interface will be used for IP routing, it must be assigned an IP address and a subnet mask.

To configure an Ethernet interface, follow these steps:

1 .Enter global configuration mode

2 .Enter interface configuration mode

3 .Assign an IP address and subnet mask

4 .Activate the interface using the no shutdown command

By default, interfaces are disabled when a router starts. Use the no shutdown command to enable them. If you need to disable an interface (e.g., for maintenance or troubleshooting), use the shutdown command .

3 .Main Router Configurations:

3.1. Changing Configuration:

To modify a configuration, enter the appropriate mode and execute the required command. For example, to enable an interface, enter global configuration mode, then interface mode, and use the command :

```
Router(config-if)# no shutdown
```

To verify the changes, use the following command in privileged EXEC mode:

Router# show running-config

This displays the current running configuration. If the displayed settings are not as expected, you can:

-Use the “no” form of the command to undo a configuration change

-Reload the router to restore the original configuration NVRAMAM

-Copy a saved configuration file fromTFTP serverer

-Delete the startup configuration using erase startup-config, then reboot the router and en setup mode de To save the current configuration to startup configurationon in NVRAM, use the following command in privileged mode:

```
Router# copy running-config startup-config
```

3.2. Interface Passwords :

Passwords are used to restrict access to routers and should always be configured for the console line and VTY (remote access) lines. They also help control entry to privileged EXEC mode, ensuring that only authorized users can modify the configuration .

Setting a password for the console line :

```
Router(config)# line console 0
Router(config-line)# password <password>
Router(config-line)# login
```

Setting a password for VTY lines (used for remote access) :

```
Router(config)# line vty 0 4
Router(config-line)# password <password>
Router(config-line)# login
```

Two types of passwords control access to privileged mode :

-enable password – basic password (not encrypted by default)

-enable secret – stronger and encrypted using MD5, making it more secure

It is recommended to use only enable secret, as it offers better security.

Commands to set enable passwords:

```
Router(config)# enable password <password>
Router(config)# enable secret <password>
```

To encrypt all non-encrypted passwords in the configuration file, use:

Router(config)# service password-encryption

This applies basic encryption, while enable secret uses a stronger MD5 hashing algorithm.

3.3. Managing Configuration Files Using TFTP:

In Cisco routers and switches, the running configuration is stored in RAM, while the startup configuration is saved in NVRAM by default. To prevent data loss, it’s important to back up the configuration to an external server.

One common method is to use a TFTP server for backup and recovery.

To save the configuration to a TFTP server:

```
Router# copy running-config tftp
```

Follow these steps:

-Enter the IP address of the TFTP server

-Provide a filename for the configuration (or accept the default)

-Confirm your choices with "yes" when prompted

To restore the configuration from a TFTP server:

```
Router# copy tftp running-config
```

Then :

-Select the host or network configuration file

-Enter the TFTP server IP address

-Specify the configuration filename (or use the default (

-Confirm the details and proceed

This method ensures that configurations can be quickly recovered in case of device failure or misconfiguration.

3.4. Managing Configuration Files by Copy-Paste

Another way to create a backup of the router configuration is to capture the output of the show running-config command using a terminal emulator such as Cisco .

To save the configuration:

1 .Go to Transfer > Capture Text

2 .Specify a filename for the text capture and click Start

3 .Run the command :

```
Router# show running-config
```

4 .Press Spacebar when “--More--” appears

5 .Once the full configuration is displayed, stop the capture via Transfer > Capture Text > Stop

After capturing the configuration:

-Open the file in a text editor like Notepad

-Remove unnecessary lines such as:

```
-Building configuration...
-Current configuration:
-- -More--
```

-The word End at the end of the file

-Add no shutdown at the end of each interface section if needed

-Save the cleaned-up file

You can also use this file to restore the configuration:

To restore the configuration:

1 .Enter global configuration mode on the router

2 .In HyperTerminal, go to Transfer > Send Text File

3 .Select the saved configuration file

4 .The contents will be pasted into the router as if typed manually

5 .Check for any errors

6 .Press Ctrl+Z to exit configuration mode

7 .Save the configuration to startup memory :

```
Router# copy running-config startup-config
```

This method provides a simple and effective way to back up and restore Cisco device configurations without requiring a TFTP server.

4 .Basic Switch Configuration:

When users are on different VLANs, they typically belong to different subnets. To enable communication between them, traffic must pass through a common gateway — usually a router interface connected to the switch.

To define this default gateway on the switch, use the following command:

```
Switch_A(config)# ip default-gateway <ip-address<
```

The connection between the router and the switch is usually a trunk link, which allows traffic from multiple VLANs to pass over a single physical link using subinterfaces on the router.

Each VLAN requires a router subinterface with:

-An IP address from the corresponding VLAN subnet

-VLAN tagging configured using the encapsulation command

Example configuration:

```
R1(config)# interface fastEthernet 0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
```

In addition, the main physical interface should have an IP address if used as a gateway:

```
R1(config)# interface fastEthernet 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
```

With this setup, hosts in one VLAN can now communicate with hosts in another VLAN. When a host sends a frame to a destination in a different subnet, the switch forwards it to the default gateway via the trunk. The router then decapsulates the frame, processes it, and re-encapsulates it for the destination VLAN before sending it out the appropriate subinterface .

5 .Common VLAN Issues and Their Solutions:

When multiple VLANs are interconnected, several technical problems may occur. The two most common issues in a multi-VLAN environment are:

-End-user devices need to reach remote hosts

-Hosts in different VLANs must communicate with each other

When a router needs to connect to a remote host, it checks its routing table for a known path. If the destination belongs to a subnet that the router knows how to reach, it verifies whether the interface is reachable. If no known routes work, the router uses the default route as a last resort.

Example of setting a default route:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

In this example, 192.168.1.1 represents the gateway. Connectivity between VLANs can be achieved using either physical or logical links.

It’s important to follow a systematic troubleshooting approach when dealing with switch-related issues. Here are some helpful steps:

-Check physical indicators such as LED statuses

-Start with a basic configuration and gradually expand

-Verify Layer 1 (physical layer) connectivity

-Confirm Layer 2 functionality (data link layer (

-Troubleshoot VLANs that span multiple switches

Useful Commands for VLAN Troubleshooting:

-show vlan: Displays VLAN information, including VLAN IDs, names, states, and assigned ports.

-show vlan <vlan-id> Shows details about a specific VLAN, including associated subinterfaces and protocols.

-debug sw-vlan packets Provides information about received VLAN packets that are not configured on the router.

-Packets that the router can process are counted and displayed using the command:

```
show sw-vlan
```

By applying these commands and following a structured approach, you can identify and resolve most VLAN-related issues in switched networks .

6 .Conclusion :

At the end of this chapter, and after going through the previous sections, we now have a solid theoretical understanding of the different methods used to implement VLANs — whether based on ports or IP addresses. This knowledge prepares us for the final step: putting these concepts into practice.

In the next chapter, we will move on to practical implementation, where we will configure and test different types of VLANs using real (or simulated) network equipment — specifically Cisco Catalyst 2950 switches and Cisco 1700 series routers, and through various scenarios.

Chapter 4:
VLAN Implementation

1. Introduction :

In this chapter, we transition from the theoretical foundations and design considerations of VLANs to their practical implementation within a large enterprise network.

The objective is to demonstrate how VLANs can be deployed effectively to enhance network segmentation, improve security, and optimize performance.

This implementation is based on the dynamic VLAN architecture previously proposed in the design phase.

Using simulation tools such as Cisco Packet Tracer (or real-world configuration where applicable), we illustrate the configuration of switches and routers, the assignment of VLANs to different departments, and the procedures for enabling inter-VLAN communication using Layer 3 routing. We also explore access control mechanisms that support secure communication between VLANs.

This chapter aims to provide a detailed and structured approach to VLAN deployment that aligns with enterprise needs, ensuring scalability, flexibility, and security in a dynamic network environment.

2. Implementation:

This chapter is dedicated to the practical implementation of three different scenarios involving VLAN assignment to switch ports and inter-switch communication.

-Case 1: Involves one (01) switch connected to six (06) PCs .

-Case 2: Involves four (04) switches interconnected with six (06) PCs .

-Case 3: Involves one (01) router connected to two (02) switches, each linked to two PCs.

Before starting the configuration, follow these steps to set up each switch:

1 .Connect the switch's console port to a PC using an RJ-45 to DB-9 adapter.

2 .Open a terminal emulator

All switches are initially configured with factory default settings, including predefined passwords, IP addresses, subnet masks, switch names, and management interfaces. These settings will be modified during the configuration process to meet the requirements of each scenario.

2.1. Initial Configuration og a Switch:

configuring global parameters:

Enter host name [Switch]: 2950

The enable secret is a password used to protect access to Privileged EXEC and configuration modes. This password, after entered, becomes encrypted in the configuration.

Enter enable secret: cisco

The enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images.

Enter enable password: cisco1

The virtual terminal password is used to protect access to the router over a network interface.

Enter virtual terminal password: cisco2

Configure SNMP Network Management? [no]: n

current interface summary

Any interface listed with OK? value "NO" does not have a valid configuration.

Interface	IP-Address	OK?	Method	Status	Protocol
VLAN1	unassigned	NO	unset	up	up
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	up	up
FastEthernet0/3	unassigned	YES	unset	down	down
...	...	...	...	...	...

Enter interface name used to connect to the management network from the above interface summary: vlanl

Configuring interface Vlan1:

Configure IP on this interface? [yes]: y

IP address for this interface: 192.168. 0 .201

Subnet mask for this interface [255.255.255.0] [255.255.255.0]

Class C network is 192.168.0.0, 24 subnet bits; mask is /24

Would you like to enable as a cluster command switch? [yes/no]: n

The following configuration command script was created:

```
hostname 2960
enable secret 5 $1$3xAQ$GlzOnEYHWBX8Mr1uCn8TO0
enable password cisco1

line vty 0 15
password cisco2
no snmp-server
interface Vlan1
```

```
 no shutdown
 ip address 192.168.0.201 255.255.255.0

interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
```

[0] Go to the IOS command prompt without saving this config .

[1]Return back to the setup without saving this config .

[2]Save this configuration to NVRAM and exit .

Enter your selection [2]: 2

Building configuration...

[oK]

Use the enabled mode 'configure' command to modify this configuration.

Press RETURN to get started!

2960>

(Cette étape se répète à chaque commutateur /routeur avec des petites différences a savoir la configuration prévu).

3 .Practical Implementation:

3.1. First Case (One Switch + Six PCs) :

(The following setup is implemented using Cisco's network simulator called Packet Tracer)

In this example, we aim to create VLANs and group PCs into different VLANs while belonging to the same network.

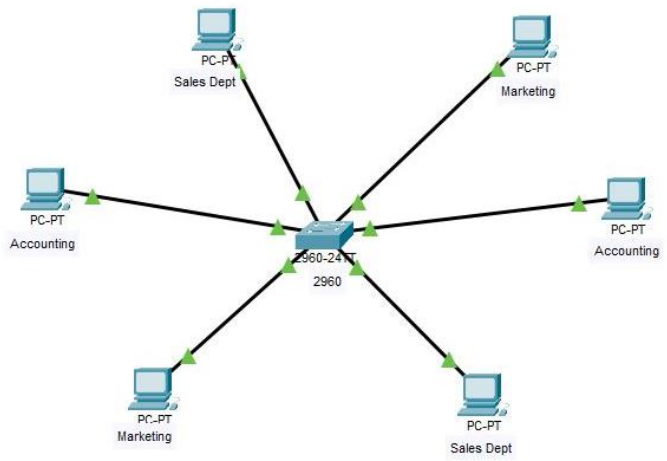

Fig 7: Vlan by port

In the command prompt, the following configuration is applied:

```
2960> enable
2960# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
```

3.1.1. VLANs Configuration:

```
2960(config)#vlan 2
2960(config-vlan)#name Marketing
2960(config-vlan)#interface range fa0/1, fa0/4
2960(config-if-range)#switchport mode access
2960(config-if-range)#switchport access vlan 2
2960(config-if-range)#exit
```

These configuration steps are repeated for the remaining VLANs.

3.1.2. Saving the configuration:

```
2950#copy running-config startup-config
Destination filename [startup-config]?
Building configuration ...
[OK]
```

The configuration can be saved in a text file as illustrated in the following figure (this is a better way to keep the configuration.(

3.1.3 Verifying Configuration:

After configuring Switch 0 with three different VLANs, named VLAN 2, VLAN 3, and VLAN 4 respectively, we can verify if the configuration is operational using the following command :

2960#show vlan

```
2960#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    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, Gig0/1, Gig0/2
2    Marketing                         active    Fa0/1, Fa0/4
3    Accounting                        active    Fa0/2, Fa0/5
4    Sales_Dept                        active    Fa0/3, Fa0/6
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
4    enet  100004     1500  -      -      -        -    -        0      0
```

The configuration is correct .

In this case, we can verify the connectivity between PCs that belong to the same VLAN. However, PCs that do not belong to the same VLAN cannot communicate with each other. We can observe that one of the advantages of VLANs is the invisibility of PCs within the same network, which can be a very important aspect in terms of computer network security.

3.2 Second Case (Four (04) Switches + Six (06) PCs) :

The second example describes the switching scheme of four (04) switches connected to six (06) PCs, as illustrated in the image below:

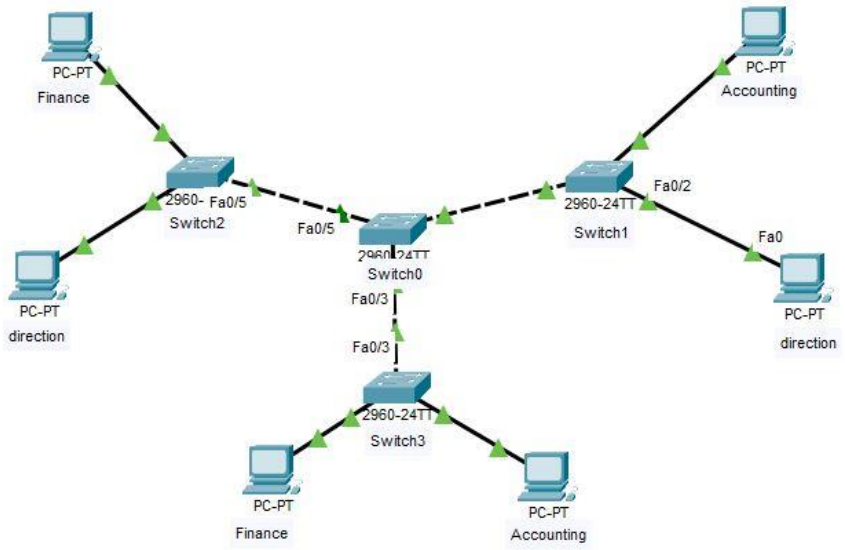

Fig 8: Port-based VLAN with Trunk

The configuration at the Switch level is done as follows:

3.2.1. Specific configuration of Switch 1, 2 and 3:

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name direction
Switch(config-vlan)#int fa0/2
Switch(config-if)#sw mo ac
Switch(config-if)#sw ac vlan 2
Switch(config-if)#ex
Switch(config)#
Switch(config)#vl 3
Switch(config-vlan)#name Accounting
Switch(config-vlan)#int fa0/1
Switch(config-if)#sw mo acc
Switch(config-if)#sw acc vlan 3
Switch(config-if)#ex
Switch(config)#int fa0/4
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan all
Switch(config-if)#exit
Switch(config)#ex
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

3.2.2. Specific configuration of Switch 0 :

At the level of Switch 0, we need to configure the ports as trunks instead of VLANs, as follows (trunks allow different VLANs to pass through a single port:(

```
Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int range fa0/3-5
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk allowed vlan all
Switch(config-if-range)#
Switch(config-if-range)#exit
Switch(config)#ex
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

3.2.3. Verifying the configuration of switch 1:

```
Switch 1#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, 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, Gig0/1, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

The configuration is correct.

Switch 0 is fully dedicated to trunks on ports Fa0/1, Fa0/3, and Fa0/2.

In this case, we can also verify connectivity between PCs that belong to the same VLAN. However, PCs that do not belong to the same VLAN cannot communicate with each other.

3.3. Third Case (Two (02) Switches + Four (04) PCs + Two (02) Routers):

In the third example, we will use routers to route traffic between VLANs across different switches. The routers operate at Layer 3 (Network Layer) of the OSI model, using the concept of IP routing, rather than relying directly on VLANs, even though VLANs are still present and used within the switches.

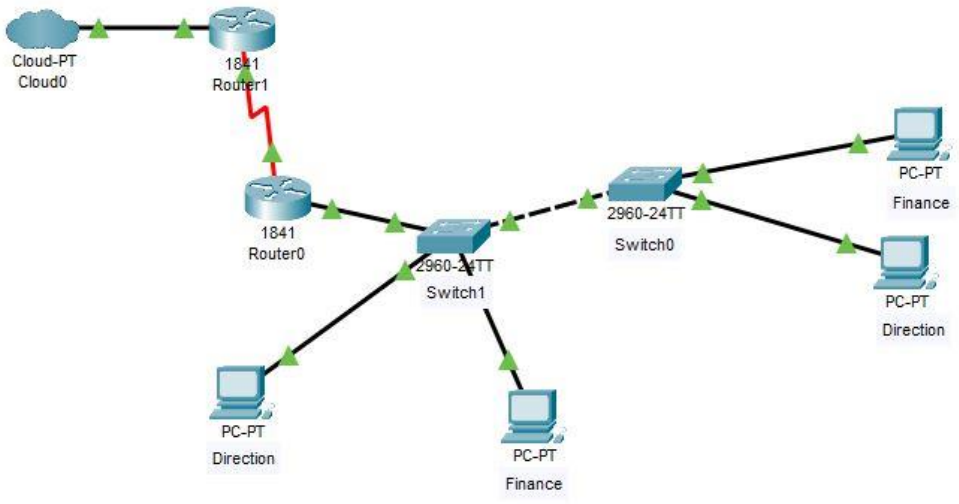

Fig 9: VLAN per subnet

3.3.1. Specific Configuration of Switch 0,1:

Same configuration as in the previous example.

3.3.2 Specific Configuration of Router 0 :

We must assign an IP address to the FastEthernet interface and configure each sub-interface with an IP address and encapsulation corresponding to a specific VLAN.

```
Router>en
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip address 9.0.0.1 255.0.0.0
Router(config-if)#no sh
Router(config-if)#
Router(config-if)#
Router(config-if)#ex
Router(config)#int se0/0/0
Router(config-if)#ip address 192.168.0.2 255.255.255.0
Router(config-if)#clock rate 56000
Router(config-if)#no sh
Router(config-if)#
Router(config-if)#ex
Router(config)#router rip
Router(config-router)#ip host router 1 10.0.0.1 192.168.0.1
Router(config)#router rip
Router(config-router)#network 9.0.0.0
Router(config-router)#network 192.168.0.0
Router(config-router)#ex
Router(config)#int fa 0/0.1
```

```
Router(config-subif)#enca
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip address 192.168.0.30 255.255.255.0
Router(config-subif)#ex
Router(config)#in fa0/0.2
Router(config-subif)#
Router(config-subif)#encapsulation dot1Q 4
Router(config-subif)#ip address 100.0.0.31 255.255.255.0
Router(config)#ex
Router#copy ru startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

3.3.3 Specific Configuration of Router 1:

```
Router(config)#int se0/0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#ex
Router(config)#int fa0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no sh
Router(config-if)#ex
Router(config)#router rip
Router(config-router)#ip host router 0 9.0.0.1 192.168.0.2
Router(config)#router rip
Router(config-router)#network 10.0.0.0
Router(config-router)#network 192.168.0.0
Router(config-router)#ex
Router(config)#ex
Router#copy ru st
Destination filename [startup-config]?
Building configuration...
[OK]
```

3.3.4 Summary :

1 .Hosts can now communicate across different VLANs thanks to IP addressing. This is possible because each host's subnet matches the subnet of the router interface it is connected to, even if the hosts belong to different VLANs .

2 .Hosts cannot communicate within the same VLAN if their subnets do not match the router interface they are connected to, even if they are in the same VLAN .

This leads us to conclude that packet switching between VLANs operates across two different layers. Each layer has its own switching conditions:

-In **Layer 2 switching**, communication is allowed only if hosts belong to the same VLAN.

-In **Layer 3 routing**, IP addressing overrides VLAN boundaries, allowing communication between different VLANs through routers.

General Conclusion :

This project provided a comprehensive understanding of VLAN technology and its role in modern network design. Through practical implementation using Cisco Packet Tracer, we were able to simulate different network scenarios involving VLAN segmentation, inter-VLAN communication, and the integration of Layer 2 switching with Layer 3 routing.

We observed that in a Layer 2 environment, devices can only communicate if they belong to the same VLAN. This isolation enhances network security and reduces unnecessary traffic. However, by introducing a router or a Layer 3 switch, it becomes possible to enable communication between different VLANs while maintaining logical separation.

Furthermore, this study highlighted the importance of proper network planning, including IP addressing schemes, VLAN assignment, and interface configuration on both switches and routers. It also demonstrated how combining Layer 2 and Layer 3 technologies allows for building scalable, secure, and efficient network infrastructures tailored to enterprise needs.

In conclusion, mastering the concepts of VLANs and inter-VLAN routing is essential for designing and managing modern networks that meet today's demands in terms of performance, flexibility, and security. This knowledge serves as a solid foundation for further exploration into advanced networking topics such as network virtualization, Quality of Service (QoS), and network automation .

Bibliography:

Books:

1 .Djillali Seba, "Interconnexion des réseaux à l'aide des routeurs et commutateurs", Paris, 1998.

2 .Edittel professeur d'informatique à Austin Community College), "Réseaux", Dunod, Paris, 2003 pour l'edition francaise

3 .Held Gilbert, "Les réseaux locaux virtuels : conception, mise en œuvre et administration", édition originale publiée aux États-Unis par John Wiley & Sons, Paris, 1998.

4 .Held Gilbert, "Les réseaux locaux virtuels", Paris, 1998.

5 .Lagrand Xavier, Dominique Seret, "Introduction aux réseaux", édition Hermès, Paris, 1998.

6 .Servin Glaude, "L'architecture des réseaux", première édition Dunod, Paris, 2000.

Webgraphie:

7 .Cisco Systems, VLAN Trunking Protocol (VTP)*, Available: https://www.cisco.com

8 .IEEE Standards Association, IEEE 802.1Q Standard for Local and Metropolitan Area Networks – Media Access Control (MAC) Bridges*, 2014 .

9 .William Stallings, Data and Computer Communications, 10th Edition*, Prentice Hall, 2013 .

10 .Andrew S. Tanenbaum, Computer Networks, 5th Edition*, Pearson Education, 2011 .

11 .Cisco Networking Academy, CCNA Routing and Switching Courseware*, Cisco Press, 2016 .

12 .David Hucaby, Cisco CCNP SWITCH 300-115 Official Certification Guide*, Cisco Press, 2017.

13 .Odom, Wendell. (2020). *CCENT/CCNA ICND1 Official Exam Certification Guide*. Cisco Press .

14 .Lammle, Todd. (2018). *CCNA: Cisco Certified Network Associate Study Guide*. Wiley Publishing .

15 .Packet Tracer Help Documentation – Cisco Systems. (2023). *Packet Tracer User Manual*. Retrieved from [https://www.netacad.com](https://www.netacad.com [

16 .Cisco IOS Command Reference – *Basic Router and Switch Configuration Commands*. Retrieved from

[https://www.cisco.com/c/en/us/support/docs/switches.html](https://www.cisco.com/c/en/us/support/docs/switches.html[

17 .Dell Support - Switch Documentation :

https://docs.us.dell.com/support/edocs/network/pc5324/fr/ug/switch.htm

18 .Wikipedia - Classification des réseaux hydrographiques :

https://fr.wikipedia.org/wiki/Classification_des_r%C3%A9seaux_hydrographiques

19 .Wikipedia - Topologie de réseau :

https://fr.wikipedia.org/wiki/Topologie_de_r%C3%A9seau

20 .Hautrive.free.fr - Topologie des réseaux :

http://hautrive.free.fr/reseaux/architectures/topologie-des-reseaux.html

21 .SourceForge - VLANs :

http://psnmp.sourceforge.net/rapport-enseirb2002/node4.html

22 .AWT.be - Réseaux informatiques :

http://www.awt.be/web/fic/index.aspx

23 .Kh.Références - Cours Réseaux :

http://www.kh.refer.org/cbodg_ct/cours_en_lignes/cours_reseau/Page/chapl_lecon2.htm

24 .Linktionary - VLAN Definition :

http://www.linktionary.com/v/vlan.html

Appendix:

ARPA: Advanced Research Projects Agency

802.1Q: Norme IEEE

ANSI: American National Standards Institute

AUX: AUXiliary Port

CCITT: Comité Consultatif International Téléphonique et Télégraphique

CLI: Command Line Interface

CSU/DSU: Channel Service Unit / Digital Service Unit

DSL: Digital Subscriber Line

EIA: Electronic Industries Alliance

ETCD: Equipement de Terminaison de Circuit de Données

ETTD: Equipement de Terminaison de Traitement de Données

FDDI: Fiber Distributed Data Interface

HTTP: HyperText Transfer Protocol

ICMP: Internet Control Message Protocol

IEEE: Institute of Electrical and Electronic Engineers

IOS: Internetworking Operating System

IP: Internet Protocol

IPX: Internetwork Packet Exchange

ISL: Inter Switch Link

ISO: International Standard Organisation

ITU: International Telecommunications Union

LAN: Local Area Network

MAC: Medium Access Control

MAN: Metropolitan Area Network

MAU: Multi station Access Unit

MD5: Message Digest 5

NVRAM: Non Volatile Random Access Memory

OSI: Open System Interconnection

RNIS: Réseau Numérique à Intégration de Service

SAN: Storage Area Network

SNMP: Simple Network Management Protocol

SONET: Synchronous Optical Network

TCP: Transmission Control Protocol

TFTP: Trivial File Transfer Protocol

TIA: Telecommunications Industry Association

VLAN: Virtual Local Area Network

VTP: Virtual Trunking Protocol

VTY: Virtual Tele tYpe

WAN: Wide Area Network

List of Figures: