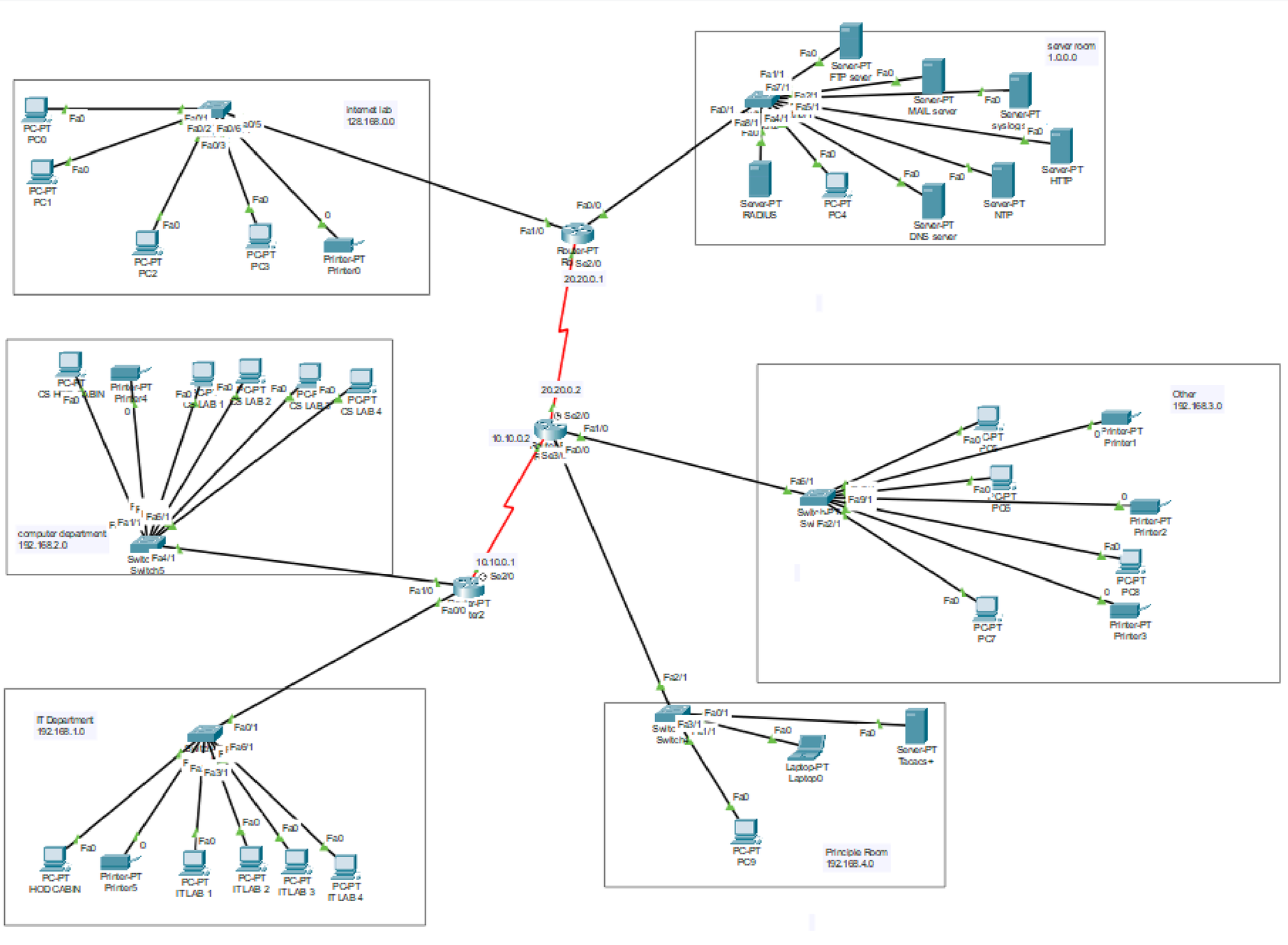
“Campus Network Design Project “

Supervisor : DR \ Mohamed Faisal

Students:

فيرينا أشرف وديع
محمد محمود مختار
محمد هاني حمدان
محمد احمد جلال
عمر وليد عمر


Internet lab
128.168.0.0
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
Printer-PT Printer0
server room
1.0.0.0
Server-PT FTP server
Server-PT MAIL server
Server-PT syslogs
Server-PT HTTP
Server-PT RADIUS
PC-PT PC4
Server-PT DNS server
Server-PT NTP
Router-PT
20.20.0.1
20.20.0.2
10.10.0.2
10.10.0.1
computer department
192.168.2.0
Printer-PT Printer4
PC-PT CS LAB 1
PC-PT CS LAB 2
PC-PT CS LAB 3
PC-PT CS LAB 4
Switch5
Other
192.168.3.0
Printer-PT Printer1
PC-PT PC6
Printer-PT Printer2
PC-PT PC8
Printer-PT Printer3
PC-PT PC7
IT Department
192.168.1.0
PC-PT HODCABIN
Printer-PT Printer5
PC-PT ITLAB 1
PC-PT ITLAB 2
PC-PT ITLAB 3
PC-PT IT LAB 4
Switch4
LaptopPT Laptop0
Server-PT Tacacs+
PC-PT PC9
Principle Room
192.168.4.0

INTRODUCTION

In this project, we designed a structured and secure network connecting multiple departments, such as:

🏫 Internet Lab | 🖥️ Server Room | 💻 Computer Dept | 🛠️ IT Dept | 🏛️ Principal Room

🧾 IP addresses are assigned dynamically using DHCP configured on routers to simplify network management.

📡 We used a combination of Static Routing and OSPF for efficient data communication between all segments.

🛠️ The network offers essential services:

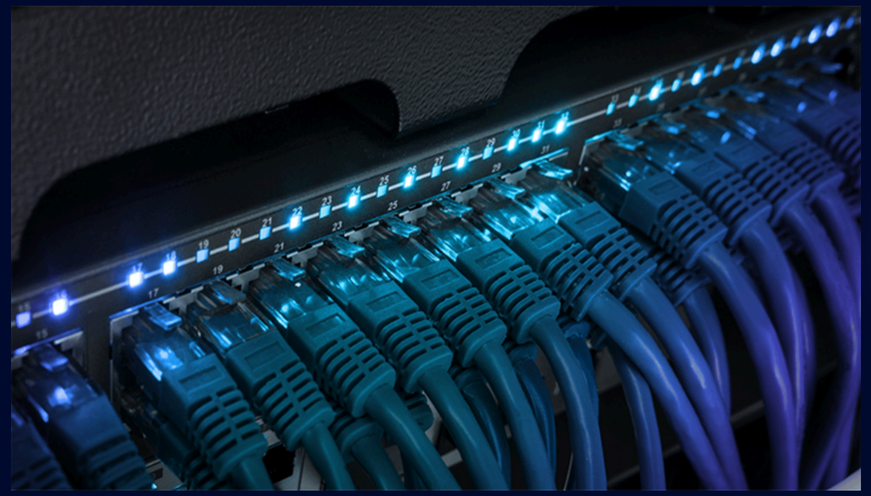
🌐 HTTP | ✉️ Mail | 🧠 DNS | 📂 FTP | ⏰ NTP

🔐 For security, we implemented:

- ✅ AAA (RADIUS & TACACS+)
- ✅ Syslog Server
- ✅ Port Security
- ✅ DHCP Snooping with trusted/untrusted ports

Presentation Outline

1. Cabling 🧵 ➡ Physical connections and network layout
2. Switching 🔀 ➡ port configuration, and internal connectivity
3. DHCP 🧩 ➡ Dynamic IP addressing through router
4. Routing 🛣️ ➡ Static routing and OSPF implementation
5. Remote Access 🌐 ➡ Access control and authentication mechanisms
6. Servers 🖥️ ➡ Services provided: HTTP, Mail, DNS, FTP, NTP
7. Security 🔐 ➡ AAA, Port Security, Syslog, DHCP Snooping



CABLING

1- Cabling :

Cabling is part of the physical layer in the OSI model and is divided into two main types:

1. Wired Connections

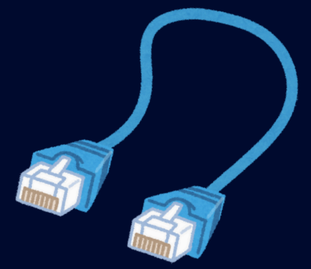
- Coaxial: An older cable type, rarely used in modern networks.
- UTP (Unshielded Twisted Pair): Common in LAN environments for PC, switch, and router connections

UTP cables are used in two main configurations:

- Straight-Through Cable: Connects different devices (e.g., PC to Switch, Router to Switch).
- Crossover Cable: Connects similar devices (e.g., PC to PC, Router to Router).

Note: Modern devices may support Auto MDI-X, which automatically adjusts for cable type.

Note: you can also use serial cables to connect similar devices



2. Wireless Connections

Wi-Fi and Bluetooth: Used for communication without physical cables, but still part of the physical layer.

Special Notes:

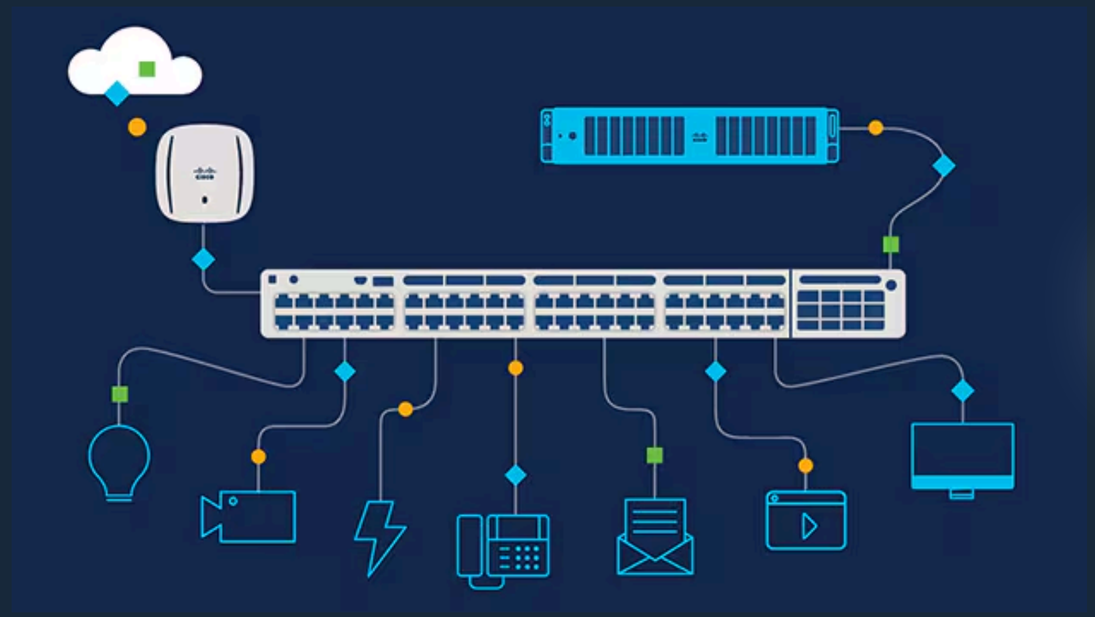
❗❗**In this network we're using Straight-Through Cable to connect different devices and serial cables to connect similar devices , Serial Cables are used to connect routers across WAN connections (e.g., via a Lease Line) through special serial ports**

Lease Line:

- A dedicated, always-on connection provided by ISPs (e.g., Orange, Vodafone, WE).
- More stable and manually configured, often used in business-grade networks.
- Example: DSL or fiber connection between two LANs over WAN.

Crossoverr Cable vs. Serial Cable

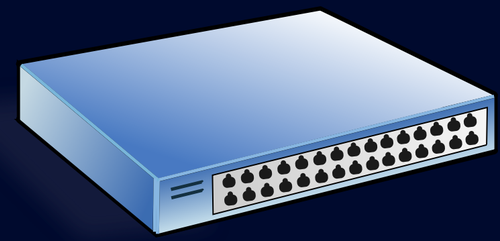
Crossover Cable		Serial Cable
Function	Connects similar devices (e.g., PC to PC)	Connects routers via a WAN
Layer	**physical layer**	Physical Layer
Type of Data	Ethernet	WAN/Serial
Port Used	RJ-45	Serial (e.g., DB-60)
Speed	Higher	Lower
Range	Shorter (LAN)	Longer (WAN)
Cost	Lower	Higher



SWITCHING

2-Switching (Layer 2 – Data Link Layer)

What is a Switch?



A switch is a Layer 2 device in the OSI model that operates at the Data Link Layer. It uses MAC addresses to forward data between devices within the same LAN. Each port on a switch represents a separate collision domain, which reduces data collision and increases performance.

How Switching Works ?

1. The switch receives a frame.
2. It checks the Source MAC address and adds it to the MAC address table.
3. It looks up the Destination MAC:
   - If found: forwards the frame directly to the correct port.
   - If not: floods the frame to all ports (except the source port) — called flooding.

Switching Techniques

Switching Method	Error Checking	Speed	Reliability	Use Case
Store-and-Forward	Yes (FCS)	Slower	High	Common in Cisco switches
Cut-Through - Fast	No	Fastest	Low	Time-sensitive apps
Cut-Through - Fragment	Partial (64B)	Medium Fast	Moderate	Compromise of both

Key Problems in the Design

1. No VLANs

- No segmentation between departments.
- Harder to isolate traffic or apply access control.

2. No Load Balancing and No use of technologies like:

- EtherChannel
- Spanning Tree enhancements
- Redundant links

- All traffic follows a single path, which becomes a bottleneck.
- In case of heavy load, network speed decreases significantly.

3. Broadcast Overload

- A single broadcast reaches every device.
- This leads to network congestion, lower performance, and more CPU usage on end devices.

Cost Impact of Current Design

- More Switches => Higher Hardware Cost
- Separate Physical Connections = > More Cabling
- No Logical Segmentation => Higher Management Overhead
- Inefficient Traffic Flow => Lower Bandwidth

> Smarter solution :

Use fewer switches with VLANs, and apply Load Balancing techniques for redundancy and performance.

DHCP

3-DHCP (Dynamic Host Configuration Protocol)

DHCP is a network protocol used to automatically assign IP addresses and other network configuration parameters (like subnet mask, default gateway, and DNS server) to devices on a network. It reduces the need for manual IP configuration, prevents IP conflicts, and simplifies network management — especially in large networks.

How It Works? DORA Process

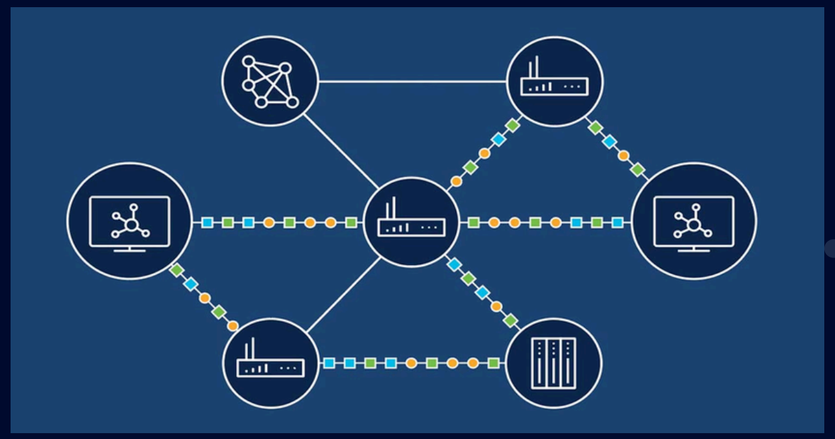
DHCP operates through a 4-step process called DORA:

1. Discover – The client broadcasts to find available DHCP servers.

2. Offer – A DHCP server responds with an IP offer.

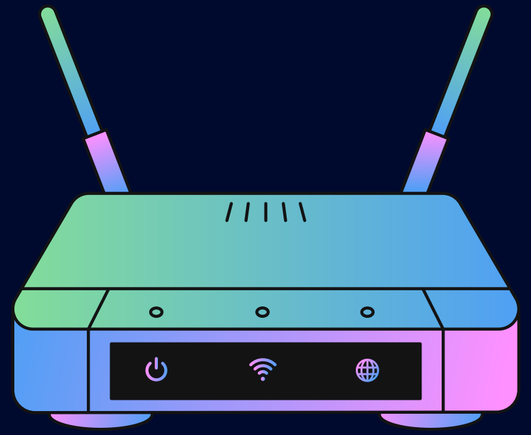
3. Request – The client requests the offered IP.

4. Acknowledge – The server confirms the lease of the IP.



ROUTING

3-Routing



Routing is the process of selecting paths in a network along which to send data packets. Routers maintain a routing table to determine the best path to a destination.

Key Problems in the Design

1. Static Routing

Definition:
Manually configured routes by the network administrator.

Use Case:
Small or simple networks where paths rarely change.

Pros:

- Simple and predictable.
- No extra CPU/memory usage.

Cons:

- Not scalable.
- Doesn’t adapt to network failures.

1. OSPF (Open Shortest Path First)

Definition:
A dynamic routing protocol that calculates the shortest path based on cost (bandwidth).

Use Case:
Large and complex networks

Pros:

- Automatically adapts to changes.
- Efficient and scalable.

Cons:

- More complex to configure.

Routing comparsion

Feature	Static Routing	OSPF
Type	Manual	Dynamic
Scalability	Low	High
Adaptability	No	Yes
Configuration	Simple	Complex
Cost Metric	Manual/None	Based on bandwidth (cost)

Key Problems in the Design

- **Single Point of Failure in Routing: If one router fails, some networks may become unreachable. Consider adding redundancy (e.g., HSRP or backup routes).**
- **Cost Consideration:**
  Static routing is cost-free but labor-intensive in large networks.
  OSPF is scalable but needs routers that support it and admin knowledge.

REMOTE ACCESS

3-Remote Access

key Benefits of Remote Access:

·Flexibility: Enables users to access network resources from anywhere, at any time, which is especially beneficial for remote learning and telecommuting.
·Security: Ensures data is encrypted and secure during transmission over public networks, protecting sensitive information from interception.
·Productivity: Allows users to work remotely without losing access to essential tools and resources, thereby maintaining productivity

Secure Shell (SSH):

Description: Provides a secure way to access and manage network devices and servers remotely via command-line interface.

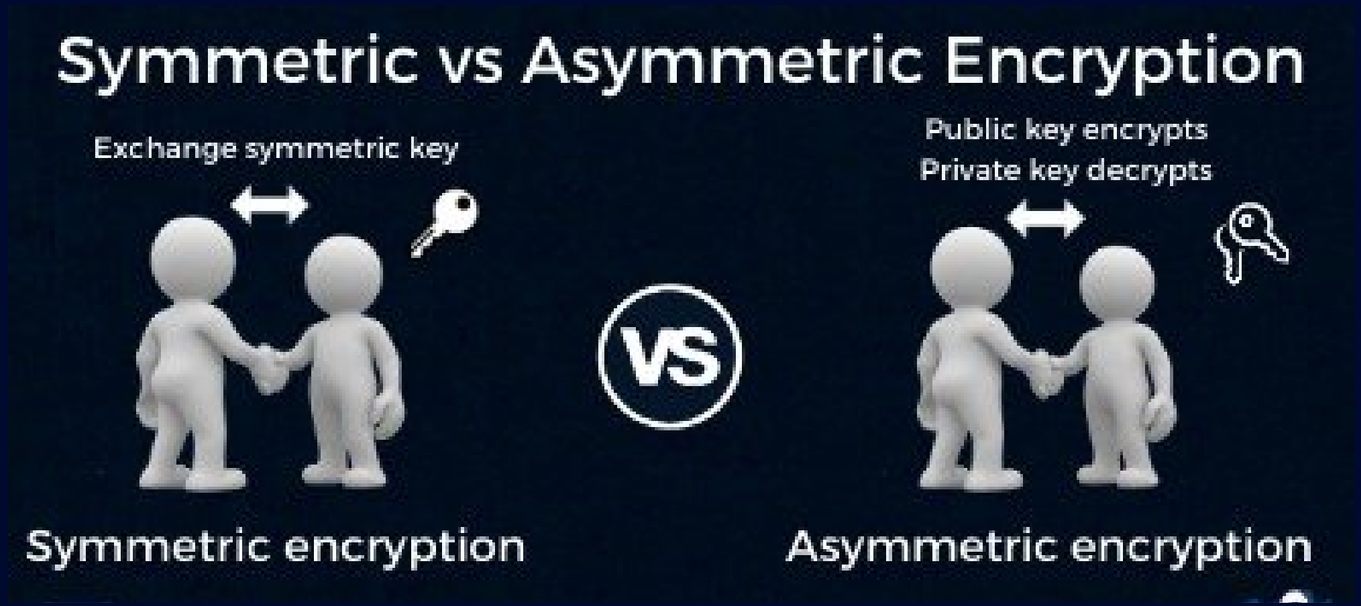
Use Case: IT staff and researchers can remotely manage servers and network infrastructure securely, ensuring that administrative tasks can be performed from any location.

SSH Functions :

There are multiple functions performed by SSH Function, here below are some functions:

- SSH provides high security as it encrypts all messages of communication between client and server.
- SSH provides confidentiality
- SSH allows remote login, hence is a better alternative to TELNET
- SSH provides a secure File Transfer Protocol, which means we can transfer files over the Internet securely
- SSH supports tunneling which provides more secure connection communication

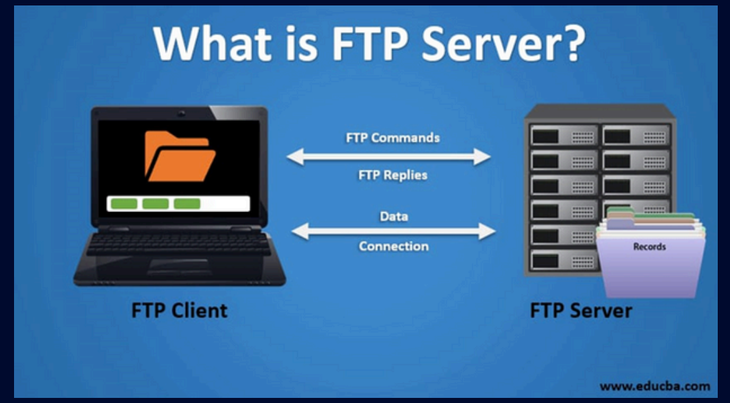
SSH use Symmetric Cryptography and asymmetric Cryptography



SERVERS

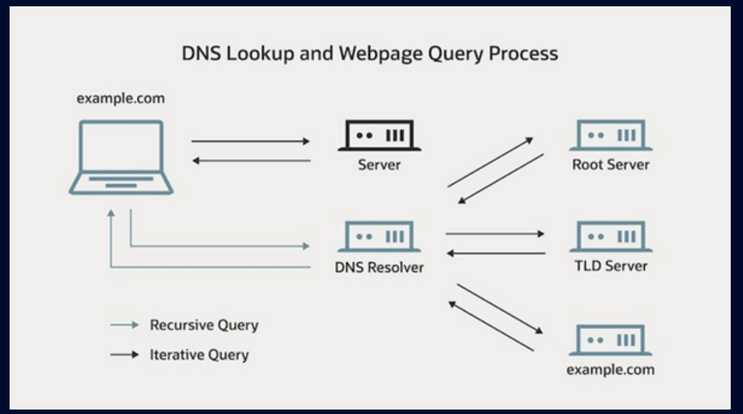
1-FTP Server (File Transfer Protocol)

An FTP server is a server that uses the File Transfer Protocol to transfer files between a client and server over a network. It supports authentication (usually requiring a username and password) and can provide various levels of access control. FTP servers are widely used for uploading, downloading, and managing files on remote servers.



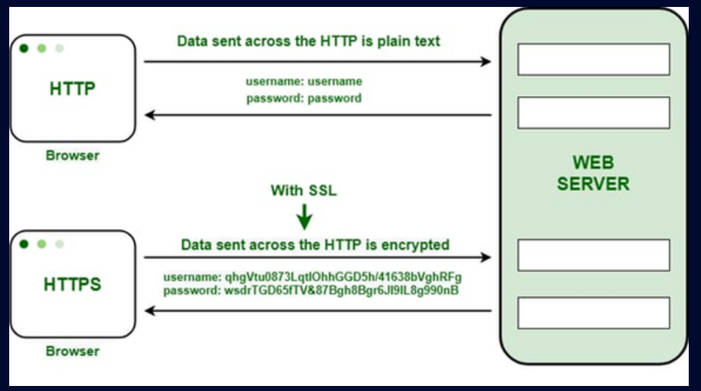
3-DNS Server (Domain Name System)

A DNS server translates human-readable domain names (like www.example.com) into IP addresses that computers use to identify each other on the network. This process, called domain name resolution, is essential for routing internet traffic and making it possible for users to access websites using easy-to-remember names instead of numerical IP addresses.

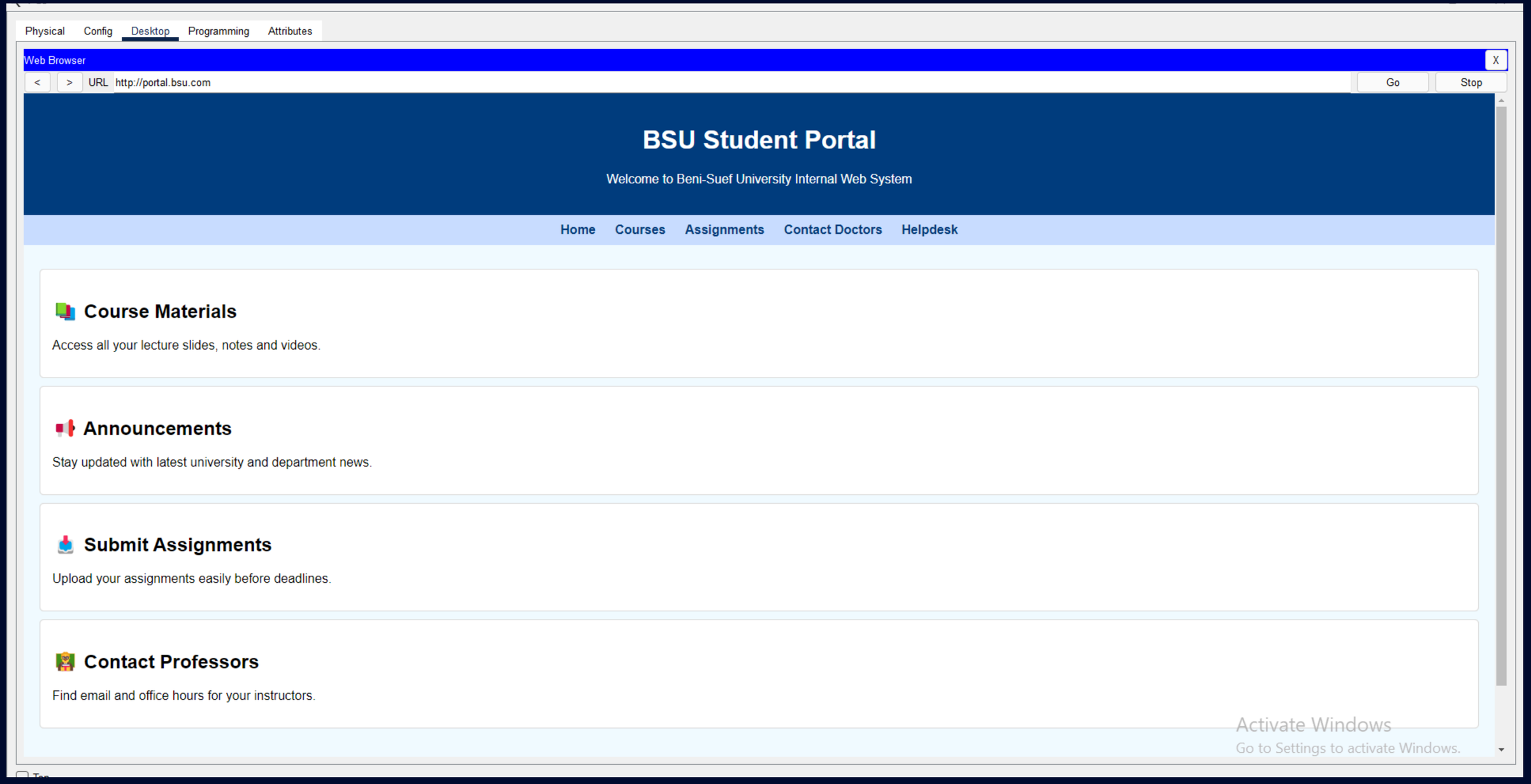


4-HTTPS Server (Hypertext Transfer Protocol Secure)

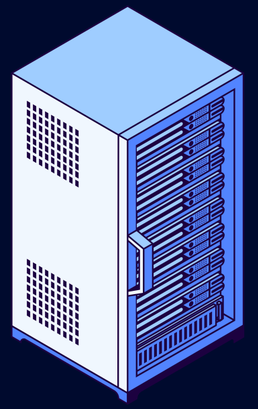
An HTTPS server is a web server that uses HTTPS to secure communication between the client (usually a web browser) and the server. HTTPS combines HTTP with SSL/TLS encryption to protect data transmitted over the internet, ensuring that sensitive information like login credentials, payment details, and personal data remains confidential and secure from eavesdropping or tampering.



Features :
we made a web page as a student portal for our university



5-NTP SERVER Network Time Protocol



(NTP) is a protocol that helps the computers clock times to be synchronized in a network. This protocol is an application protocol that is responsible for the synchronization of hosts on a TCP/IP network.

6-SYSLOG SERVER

All network devices such as routers, servers, firewalls, etc. create or prompt logs about statuses and the events that occur. For a small system tracking these logs is not a problem, the problem arises when we are dealing with big systems where tracking all these logs and information becomes challenging. To overcome this problem we use Syslog with a logging server known as Syslog server (such as Kiwi Syslog server, Graylog, Solarwind Syslog server, etc.).

A Syslog server allows us to send the log information of all our network devices to one centralized place. The log messages are sent on UDP port 514 to the Syslog server. From here we can search, manage and archive all of the log information.

A wide variety of devices supports the Syslog protocol hence, it can be used to log various types of events like logs from a web server, a router, etc

7-Mail server

deliver email messages between mail clients by using email protocols

SECURITY

1-ACL - (Access Control List)

An Access Control List (ACL) is a set of rules used to control network traffic and reduce network attacks.
ACLs can permit or deny traffic based on various criteria such as IP address, protocol type, and port number. They are commonly used in routers and firewalls to filter inbound and outbound traffic and to enhance network security by controlling which devices or users can access specific resources.

Mitigate Attacks with ACLs

IP Spoofing Attack

An attacker from outside the network may try to spoof an IP address to affect the internal network in several ways. IP spoofing is the act of forging source IP addresses to impersonate other devices. Common techniques used in IP spoofing attacks:

- DHCP Starvation: The attacker floods the DHCP server with many DHCP requests using spoofed IPs, exhausting the pool of available addresses.
- Using Reserved or Invalid IPs:
  IPs like 0.0.0.0 should not be used as a source address; it's reserved and invalid.
- Broadcast Storms:
  Using the IP 255.255.255.255 can cause broadcast storms, potentially overwhelming the CPU of network devices like routers and switches.
- Multicast Attacks:
  Spoofing multicast IPs (e.g., 224.0.0.0) to send traffic to multiple devices at once, which can disrupt network operations.
- Mitigation Using ACLs:
  You can apply Access Control Lists (ACLs) to drop traffic from suspicious or invalid source IP addresses before it reaches the internal network.

2-mitigate brute force attack using SSH

A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks. The hacker tries multiple usernames and passwords, often using a computer to test a wide range of combinations, until they find the correct login information.
The name "brute force" comes from attackers using excessively forceful attempts to gain access to user accounts.

How to mitigate it by SSH ??

1-using asymmetric encryption algorithms such as RSA
2- Using a large encryption key such as 1024
3-SSH retries : by default 3 you can modify it
4- using SSH timeout : by default 120 you can modify it

3-AAA authentication

A -----> Authenication (user name & password)
A ------> Authorization (privilleges)
A ------> accounting (monitoring)

I applied AAA on a router using three different methods:

1. Local Database (Local AAA)

- **Authentication is handled directly on the router using a locally configured username and password.**
- **This method is simple and effective for small networks or backup access when external servers are unavailable.**

2. TACACS+ (Terminal Access Controller Access-Control System Plus)

- **Used for centralized AAA.**
- **Encrypts the entire packet, making it more secure.**
- **Separates the AAA functions (authentication, authorization, accounting) — which allows for more granular control.**
- **Often used in enterprise environments for device administration.**
- **Communicates over TCP (port 49), which is more reliable than UDP.**

3. RADIUS (Remote Authentication Dial-In User Service)

- **Also used for centralized AAA, especially for user access to services like VPN, Wi-Fi, etc.**
- **Only the password is encrypted, not the full packet.**
- **Combines authentication and authorization in a single process.**
- **Uses UDP (ports 1812/1813), making it lightweight.**

4-common switch attacks and how to mitigate it

2-MAC Address Table Attack (MAC Flooding)

Definition: An attacker floods a switch with thousands of fake MAC addresses using a tool (e.g., Kali Linux).

Effect: The switch's MAC address table becomes full and overflows.

Result: The switch acts like a hub and floods all traffic to every port, leading to possible data leakage and reduced performance.

Solution:
- Enable Port Security on switch ports.
- Limit the number of MAC addresses allowed on each port.

2-DHCP Attacks

1.DHCP Starvation Attack

Definition:
The attacker uses tools like DHCP Gobbler to send many DHCP requests using fake MAC addresses.

Effect:
The DHCP pool becomes exhausted, and legitimate users cannot get IP addresses.

Solution:
- Enable DHCP Snooping on the switch.
- Limit the rate of DHCP Discover messages per port.

2. DHCP Spoofing Attack

Definition:
The attacker sets up a fake DHCP server (e.g., using Windows Server or Linux PC).

Effect:
The attacker sends fake IP configurations to clients, leading to Man-in-the-Middle (MITM) attacks.

Solution: Use DHCP Snooping and define:
- Trusted Ports: Ports connected to the real DHCP server (usually routers).
- Untrusted Ports: Ports connected to user devices (e.g., PCs).

This prevents DHCP replies on untrusted ports.

THANK YOU