Cisco Cybersecurity Engineer
DEPI2_CAI2_ISS5_S2
Project Number : 10

Campus Area Network (CAN)

Prepared by:

Name	DEPI_ID
▪ Khaled Abdelnaser Mohamed	
▪ Ali Mohamed Ali	
▪ Khaled Gamal	
▪ Kerolos Maged Kamal	
▪ Mohamed Omar	
▪ Mohamed Karam	

Under supervision of Professor : Elhosein Ahmed

Table of Contents

Abstract

This project focuses on the design and implementation of a secure and efficient corporate data center network using Cisco Packet Tracer. The network is engineered to meet enterprise-level requirements for high availability, scalability, and robust security. Key technologies implemented include VLANs for logical segmentation, OSPF for dynamic and scalable routing, HSRP for gateway redundancy, STP for loop prevention, and a structured IP addressing scheme to ensure organized and manageable communication.

Redundancy is built into both the routing and switching layers to minimize downtime and maintain uninterrupted service. Security is enhanced through the use of firewalls and Access Control Lists (ACLs), which help control and restrict unauthorized access between network segments. The overall architecture promotes reliable performance, simplified troubleshooting, and ease of future expansion.

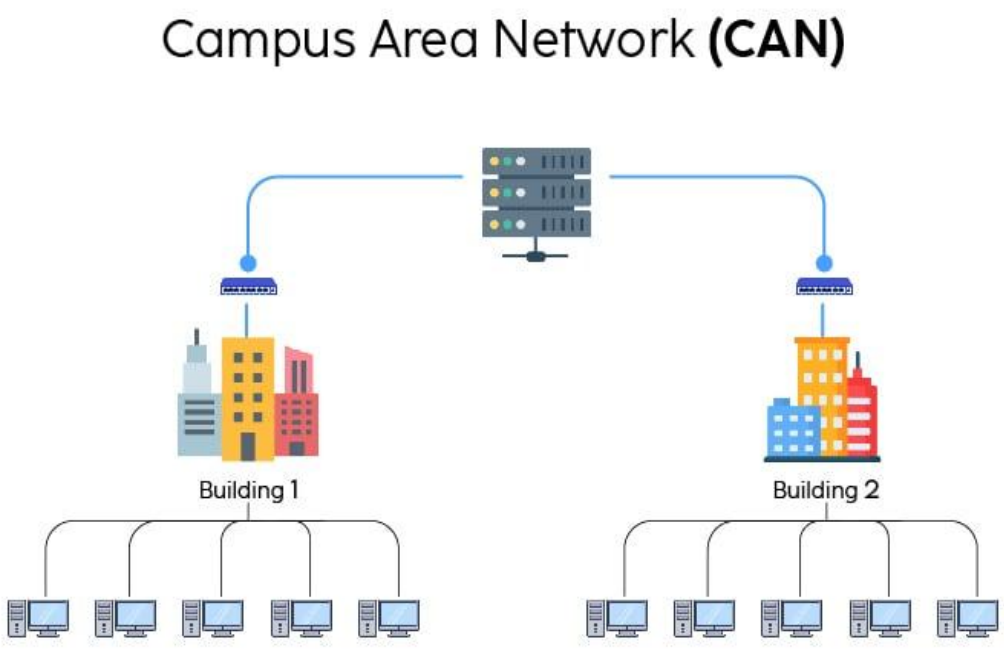

Figure1. example of Campus Area Network 1

Introduction & Overview:

The goal of this project is to design and implement a highly available, scalable, and secure corporate campus area network (can). The network supports critical applications, and services, meeting enterprise-grade performance and reliability standards. Key configurations include HSRP for redundant routing, STP for loop prevention, and VLANs for efficient segmentation. Security measures were integrated to protect against potential threats, ensuring a resilient and future-ready infrastructure.

Technology Stack:

- **Simulation Tool:** Cisco Packet Tracer
- **Routing Protocol:** OSPF (Open Shortest Path First)
- **Redundancy Protocol:** HSRP (Hot Standby Router Protocol)
- **Switching Protocol:** STP (Spanning Tree Protocol)
- **Network Segmentation:** VLANs (Virtual LANs)
- **IP Management:** Structured IPv4 Addressing Scheme
- **Security Features:**
    - Access Control Lists (ACLs)
    - Port Security
    - DHCP Snooping
- **Network Layers:** Core, Distribution, and Access Layers

Network Toplogy:

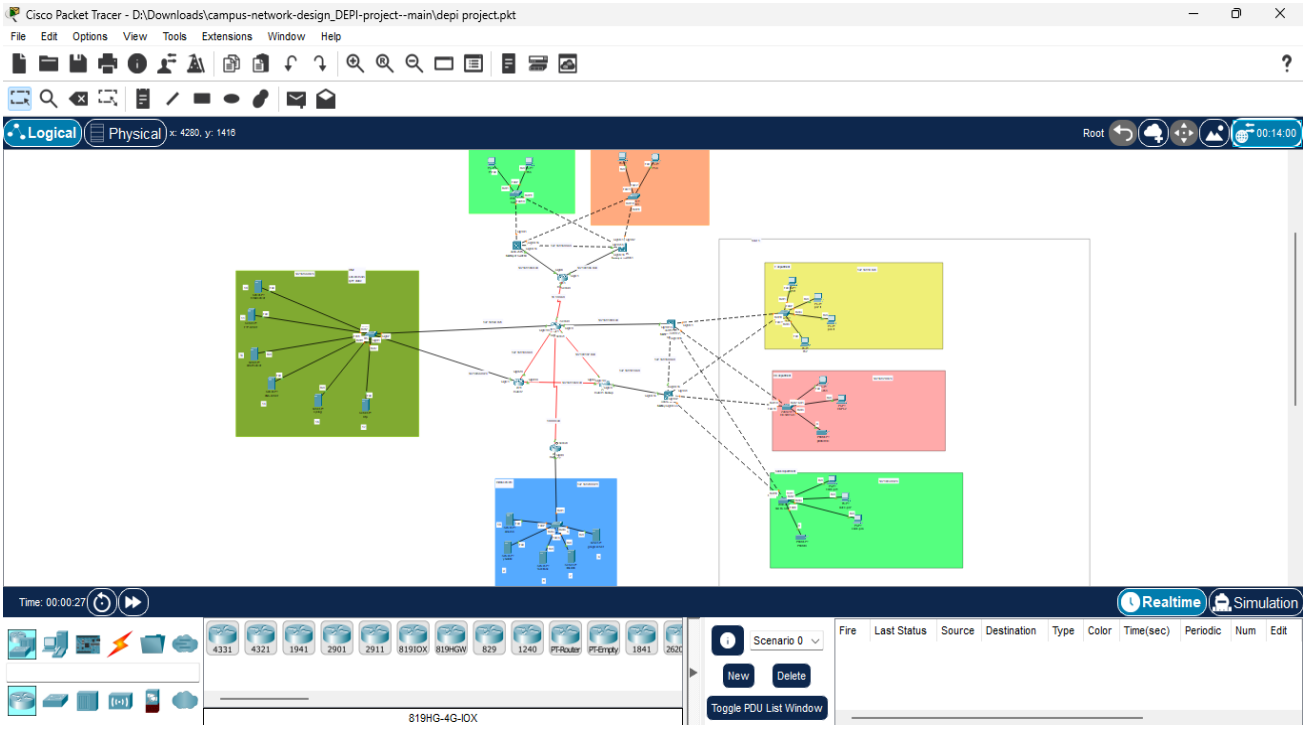

Figure2. The complete toplogy design of the network

Network Topology Overview

Site 1:

- IT VLAN – for technical and support staff.
- HR VLAN – for human resources operations.
- Sales VLAN – for the sales department and related activities.

Site 2:

- Includes **two VLANs**:
    - **Management VLAN** – for administrative access and control.
    - **Healthcare VLAN** – for health service operations and systems.

DMZ Zones:

- **Service DMZ** – hosts internal service servers like DNS, DHCP, and FTP.
- **Media DMZ** – simulates public-facing servers (YouTube, Facebook.etc).

Project Phases:

Phase 1: Network Planning and Design

- Defined business and technical requirements for availability, scalability, and security.
- Designed a hierarchical network topology incorporating core, distribution, and access layers.
- Identified VLAN structure, IP addressing scheme, and redundancy requirements.

Phase 2: Core Infrastructure Implementation

- Deployed inter-VLAN routing and IP addressing across all network segments.
- Implemented HSRP on key routers for high availability and gateway redundancy.

Phase 3: Security and Threat Protection

- Applied access control lists (ACLs) to restrict unauthorized access between VLANs.
- Enabled port security and DHCP snooping to prevent common Layer 2 attacks.

Phase 4: Testing and Optimization

- Conducted functionality and failover tests for HSRP, STP, and VLAN communication.
- Validated network performance under simulated load conditions.

Network Design:

Logical Design

This sub-section explains how the network is logically structured, including VLANs, ,DMZ services, subnets, routing protocols .

VLAN Addressing Table :

VLAN	Network	Subnet Mask	Gateway
IT	192.168.10.0/24	255.255.255.0	192.168.10.1
HR	192.168.20.0/24	255.255.255.0	192.168.20.1
Sales	192.168.30.0/24	255.255.255.0	192.168.30.1
Health & Care	192.168.40.0/24	255.255.255.0	192.168.40.1
Management	192.168.50.0/24	255.255.255.0	192.168.50.1

Table1. VLAN Configuration Summary

DMZ (Isolated Services):

Purpose	Network	Subnet Mask	Gateway
DMZ Communication Servers	192.168.10.0/24	255.255.255.0	192.168.10.1
DMZ Media Servers	192.168.20.0/24	255.255.255.0	192.168.200.1

Table2. DMZ Network Configuration 1

Why /24 and /30 subnets Were Chosen?

Subnet	Use Case	Purpose
/24 (255.255.255.0)	Internal networks	• (254 usable IPs) for medium-sized segments. • Simple to manage and maintain. • Controls broadcast domains, reducing traffic
/30 (255.255.255.252)	Point-to-point links	• 2 usable IPs, optimizing address usage. • Ideal for WAN links minimizing waste.

Table3. Subnet Allocation and Use Cases

Routing protocols

Why we use both static and dynamic routing ?

1. **Control & Simplicity**
   • Static routing provides precise control for small, stable routes (e.g., default routes or management traffic).
2. **Scalability**
   • Dynamic routing (OSPF Protocol) automatically manages large and growing networks without manual updates.
3. **Redundancy & Failover**
   • Dynamic protocols detect link failures and reroute traffic quickly, ensuring high availability.
4. **Reduced Administrative Overhead**
   • Dynamic routing reduces manual configuration in multi-router environments, saving time and minimizing errors.
5. **Optimized Design**
   • Using static routes for predictable paths and dynamic routing for complex segments balances efficiency, control, and resilience.

OSPF in the Network

OSPF (Open Shortest Path First) is implemented as the dynamic routing protocol to enable efficient and scalable route exchange between routers across the campus network.

- Area: Area 0 (backbone, simple flat design).

Configuration of OSPF protocol on the core router (R1)

```
R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 192.168.100.0    0.0.0.3 area 0
R1(config-router)# network 192.168.102.0    0.0.0.3 area 0
R1(config-router)# network 192.168.104.0    0.0.0.3 area 0
R1(config-router)# network 192.168.99.0     0.0.0.3 area   0
R1(config-router)# network 10.0.0.0          0.0.0.3 area 0
R1(config-router)# network 10.1.0.0          0.0.0.3 area 0
```

Physical Topology:

Devices used:

- **5 Routers** – Handle inter-network communication and dynamic routing.
- **4 Multilayer Switches (Layer 3)** – Support Inter VLAN Routing
- **5 Access Switches (Layer 2)** – Provide connectivity to end-user devices.
- **6 Servers** – Host internal applications and network services.
- **5 Media Servers** – Deliver media content across the network.
- **2 Network Printers** – Shared printing resources accessible across VLANs.
- **15 PCs** – End-user workstations for various departments.

Core structure :

Purpose	Network	Subnet Mask	Gateway
Active-Standby L3 Switches	192.168.150.0/30	255.255.255.252	N/A (Point-to-Point)
Active Switch ↔ Primary Router	192.168.100.0/30	255.255.255.252	N/A
Standby Switch ↔ Backup Router	192.168.101.0/30	255.255.255.252	N/A
Router-to-Router Links	192.168.102.0/30	255.255.255.252	N/A
Router-to-Router Links	10.0.0.0/30	255.255.255.252	N/A

Figure3. Point-to-Point Network Subnet Allocation

Purpose	Network	Subnet Mask	Notes
Switch-to-Switch Link	192.168.160.0/30	255.255.255.252	Redundant core link
Active ↔ Router	192.168.105.0/30	255.255.255.252	Primary uplink
Standby ↔ Router	192.168.106.0/30	255.255.255.252	Backup uplink

Figure4. Core Network Link Allocation

Servers used in the project :

- **DHCP Server**
  Automatically assigns IP addresses to devices on the network, simplifying IP management and reducing manual configuration.
- **DNS Server**
  Resolves domain names to IP addresses, enabling users to access services and websites using human-readable names.
- **FTP Server**
  Facilitates file sharing and transfer between devices, useful for backups, software distribution, or centralized file access.
- **Syslog Server**
  Collects and stores system logs from network devices, aiding in centralized monitoring, auditing, and troubleshooting.
- **NTP Server**
  Synchronizes time across all network devices, ensuring consistent timestamps for logs, security events, and scheduling tasks.
- **Email Server**
  Manages the sending, receiving, and storage of email communications, providing a centralized solution for internal and external email exchange.

Photos of the servers working

1. **Syslog server:**

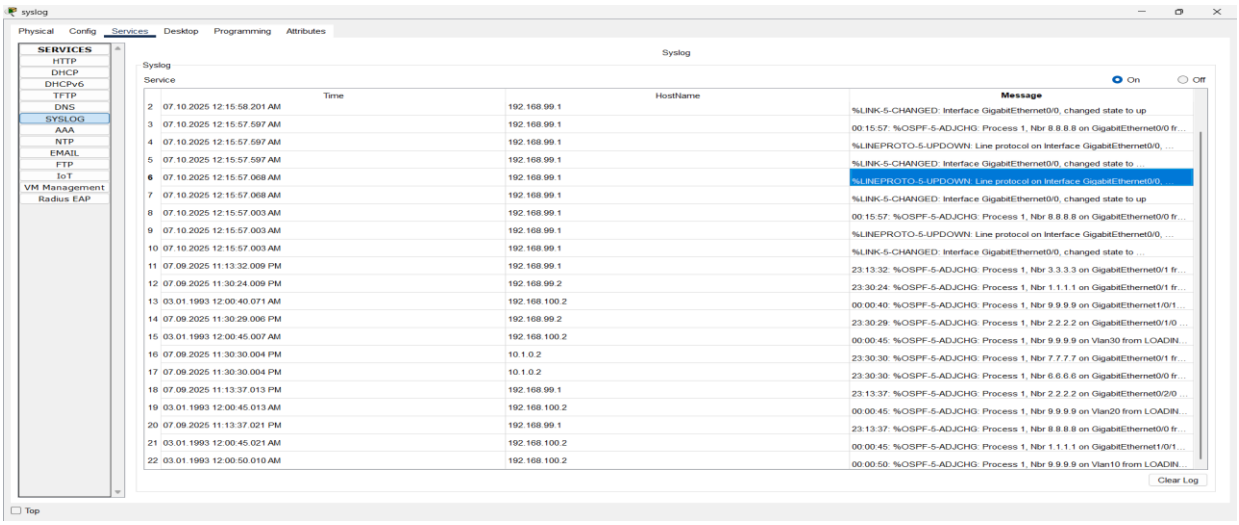

figure5. Syslog sever working on packet tracer

2. Dns server :

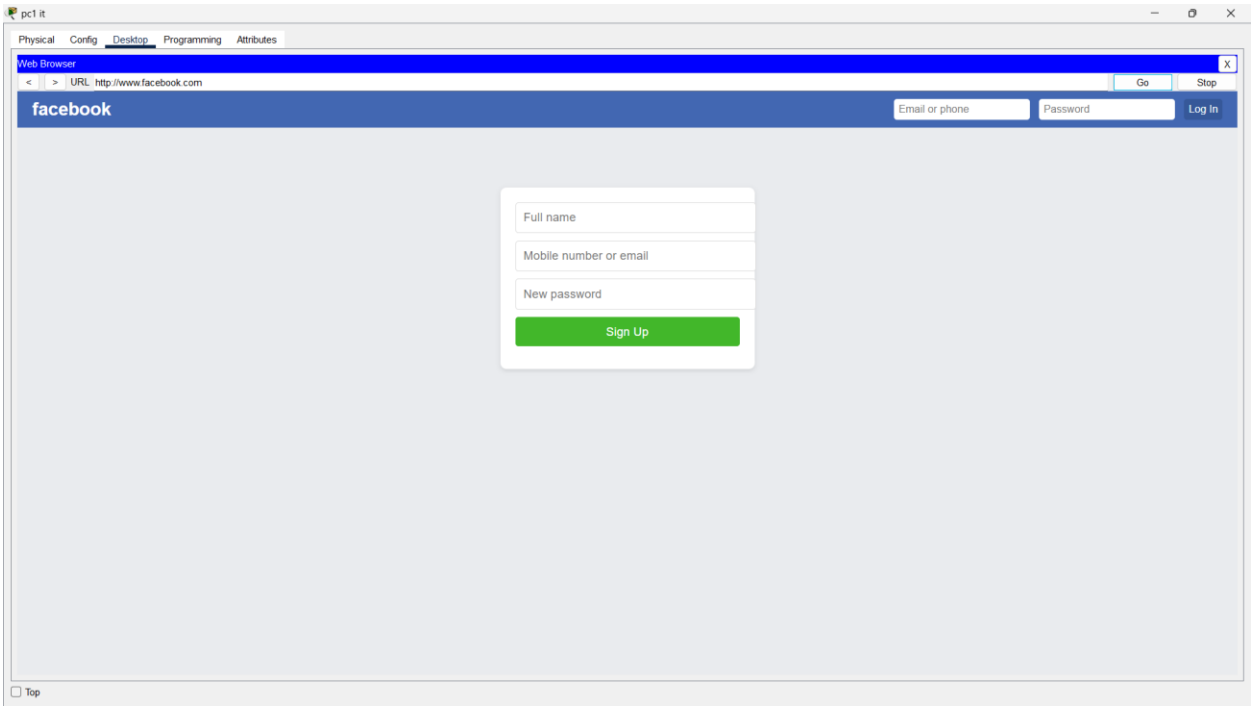

Figure6. Facebook Sign-Up Page Accessed from PC

3.DHCP server

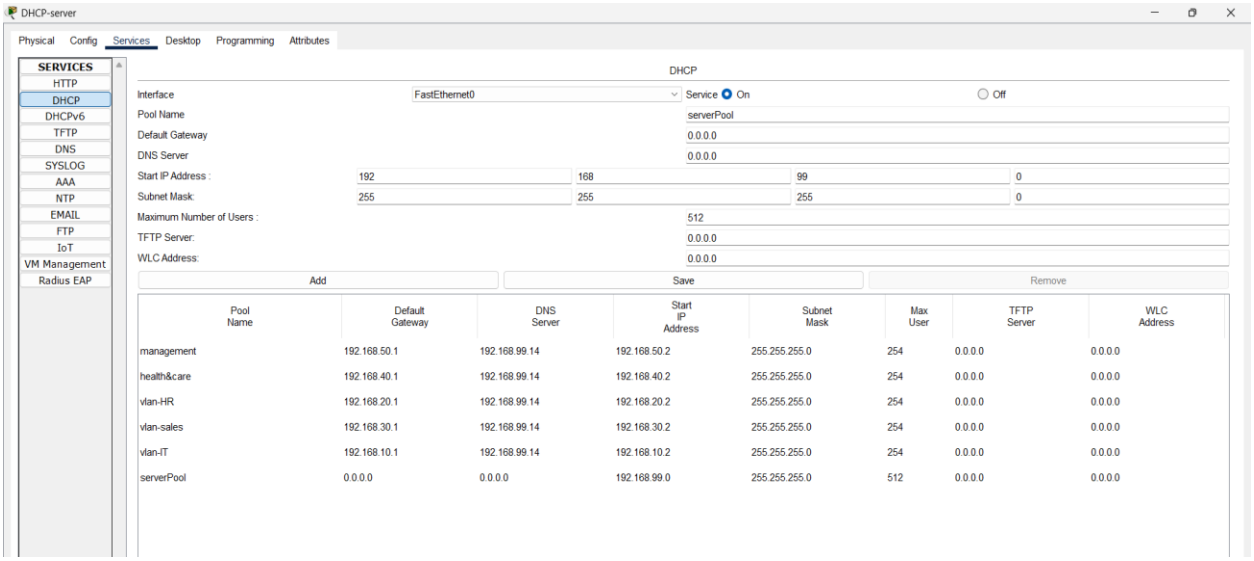

Figure7. All networks in the DHCP server

Challenges & Resolutions

The Campus Area Network (CAN) design faced several challenges, each resolved to ensure optimal performance, scalability, and security.

1. Network Scalability and Growth

- **Challenge:** Scaling the network to accommodate future growth and emerging technologies.
- **solution:** VLANs were used for traffic segmentation, and OSPF enabled seamless network expansion.

2. Broadcast Traffic Management

- **Challenge:** Excessive broadcast traffic causing congestion and inefficiency.
- **solution:** VLANs segmented broadcast domains, reducing unnecessary traffic and improving bandwidth usage.

3. Redundancy and High Availability

- **Challenge:** Minimizing disruption due to hardware or link failures.
- **solution:** HSRP provided router redundancy, and spanning-tree protocols ensured switch failover.

4. Network Security

- **Challenge:** Securing the growing network against unauthorized access and threats.
- **solution:** ACLs, secure routing, and VLANs were implemented to isolate traffic and ensure security**.**

5. Network Monitoring and Troubleshooting

- **Challenge:** Managing and troubleshooting a large-scale network.
- **solution:** syslog server provided centralized monitoring and real-time performance tracking.

Future Enhancements

1. Enhanced Network Security

Deploy next-generation firewalls (NGFW), intrusion detection systems (IDS), and multi-factor authentication (MFA).

2. Network Automation

Implement network automation with tools like Ansible or Python for configuration and monitoring.

3. Integration of Cloud Services

Integrate with cloud platforms (AWS, Azure) to offload storage and computational tasks.

4. Software-Defined Networking (SDN)

Implement SDN to decouple the network control plane from the data plane for more dynamic management and control.

5. Integration of Artificial Intelligence and Machine Learning

Use AI and ML to optimize network performance, detect anomalies, and automate troubleshooting tasks.

6. Disaster Recovery and Backup Solutions

Implement improved disaster recovery protocols and offsite backup solutions for network resilience.

Conclusion

The design of the Campus Area Network (CAN) integrates redundancy across both the routing and switching layers to ensure high availability and minimize service disruption. Security is prioritized through the deployment of firewalls and Access Control Lists (ACLs), which effectively regulate and prevent unauthorized access between critical network segments.

This architecture is engineered to deliver reliable performance, simplify troubleshooting, and facilitate seamless future expansion. By adhering to best practices for scalability, security, and efficiency, the network is positioned to meet current operational demands while supporting growth and innovation in the years to come.

Protocols used in our Project:

Distribution Layer Services and Protocols:

HSRP (Hot Standby Router Protocol)

- *Purpose*: Provides router redundancy by creating a virtual IP shared by multiple routers.
- *Importance*: Ensures high availability—if one router fails, the backup takes over instantly.

Inter-VLAN Routing

- *Purpose*: Allows communication between devices in different VLANs through a router or Layer 3 switch.
- *Importance*: Critical for segmented networks where departments (VLANs) need to communicate securely.

OSPF (Open Shortest Path First)

- *Purpose*: A dynamic routing protocol that calculates the best path using link-state info.
- *Importance*: Enables efficient, automated routing, supports scalability and fast convergence.

DHCP Relay (IP Helper Address)

- *Purpose*: Forwards DHCP requests from clients in different subnets to a centralized DHCP server.
- *Importance*: Ensures centralized IP management even across different VLANs/subnets.

Core Layer Services and Protocols:

DNS Server

- *Purpose*: Resolves domain names to IP addresses.
- *Importance*: Enables easier access to servers and services by name.

DHCP Server

- *Purpose*: Automatically assigns IP addresses to hosts.
- *Importance*: Reduces manual configuration and ensures consistent IP management.

NTP Server (Network Time Protocol)

- *Purpose*: Synchronizes time across all devices in the network.
- *Importance*: Ensures accurate timestamps for logs and security audits.

Syslog Server

- *Purpose*: Collects logs from network devices.
- *Importance*: Centralized monitoring and troubleshooting, useful for security and compliance.

FTP Server

- *Purpose*: Transfers configuration files, backups, or updates between devices.
- *Importance*: Supports network maintenance and backup strategies.

SSH (Secure Shell)

- *Purpose*: Provides secure remote access to devices.
- *Importance*: Ensures encrypted management of switches, routers, and servers.

Access Layer Services and Protocols:

Port Security

- *Purpose*: Limits access to switch ports based on MAC addresses.
- *Importance*: Prevents unauthorized devices from connecting.

DAI (Dynamic ARP Inspection)

- *Purpose*: Validates ARP packets to prevent spoofing.
- *Importance*: Protects against Man-in-the-Middle attacks.

DHCP Snooping

- *Purpose*: Monitors DHCP traffic to block rogue servers.
- *Importance*: Secures IP address assignment and prevents attacks like starvation or spoofing.

VLANs (Virtual LANs)

- *Purpose*: Logically separates network segments on the same physical switch.
- *Importance*: Enhances security, performance, and traffic management.

References

- **Cisco Networking Academy**
  Cisco's official website has many tutorials and exercises with Packet Tracer to help students learn networking and practice.
  Website: https://www.netacad.com
- **Free CCNA Study**
  This website has free labs, exercises, and tutorials for CCNA, including great examples using Packet Tracer.
  Website: https://www.freeccnastudy.com
- **Packet Tracer Tutorial (Networking Academy)**
  This site offers direct access to Packet Tracer and many tutorials to practice and improve your networking skills.
  Website: https://www.packettracer.com
- **TechNet (Microsoft Networking)**
  TechNet provides resources for learning networking with tools like Packet Tracer, and focuses on Windows-based networking
  Website: https://technet.microsoft.com.
- **Ahmed Yousry (YouTube)**
  This channel has lots of Arabic tutorials about Packet Tracer, great for learning CCNA topics step by step.
  YouTube Channel: Ahmed Yousry
- **Abeer Hosny (YouTube)**
  Abeer’s channel is in Arabic and offers useful Packet Tracer lessons for beginners and people preparing for networking certifications.
  YouTube Channel: Abeer Hosny