**A logo of a university

Description automatically generated**

**DEPARTMENT OF COMPUTER SCIENCE**

**BAHRIA UNIVERSITY ISLAMABAD**

**Spring 2024**

**Data Communication and Networking**

May 31,2024

**supervisd by**

**HIna Ayaz**

March 7,2024

**SECURE CAMPUS NETWORK** **SYSTEM**

AHSAN RASHEED

(01-134222-019)

RABIYAH HABIB

(01-134222-122)

SYED ABDULLAH SHAH

(01-134222-143)

**Semester Project Report**

*Submitted by*

**ABSTRACT**

This report outlines the design and implementation of a secure campus network system for XYZ University, encompassing two campuses located 100 miles apart. The network design aims to ensure top-tier performance, redundancy, scalability, and availability, safeguarding the confidentiality, integrity, and availability of data and communication. Utilizing Cisco Packet Tracer, the project incorporates robust network design models and various Cisco technologies to meet the university's requirements*.*

**Table of Contents**

[**1.** **Introduction** 4](#_Toc167815881)

[**2.** **History** 4](#_Toc167815882)

[**3.** **What is Secure System and Secure Campus** 4](#_Toc167815883)

[**System** 4](#_Toc167815884)

[**4.** **Software Requirements** 4](#_Toc167815885)

[Cisco Packet Tracer 4](#_Toc167815886)

[**5.** **Objectives** 5](#_Toc167815887)

[**6.** **Functions of Secure Campus Network System** 5](#_Toc167815888)

[**7.** **Problem Definition** 6](#_Toc167815889)

[**8.** **Features of Secure Campus Network System** 6](#_Toc167815890)

[**9.** **Methodology** 7](#_Toc167815891)

[Initiation 7](#_Toc167815892)

[Implementation 7](#_Toc167815893)

[Further Usage 7](#_Toc167815894)

[**10.** **Network Protocols Overview** 8](#_Toc167815895)

[IPsec VPN (Internet Protocol Security Virtual Private Network) 8](#_Toc167815896)

[LACP (Link Aggregation Control Protocol) 8](#_Toc167815897)

[STP (Spanning Tree Protocol) 9](#_Toc167815898)

[DHCP (Dynamic Host Configuration Protocol) 10](#_Toc167815899)

[HSRP (Hot Standby Router Protocol) 10](#_Toc167815900)

[OSPF (Open Shortest Path First) 11](#_Toc167815901)

[SSH (Secure Shell) 11](#_Toc167815902)

[HTTP/HTTPS (Hypertext Transfer Protocol / Secure) 12](#_Toc167815903)

[SMTP (Simple Mail Transfer Protocol) 12](#_Toc167815904)

[DNS (Domain Name System) 13](#_Toc167815905)

[FTP (File Transfer Protocol) 13](#_Toc167815906)

[NAT (Network Address Translation) 14](#_Toc167815907)

[**11.** **SnapShots** 15](#_Toc167815908)

[**12.** **Conclusion** 34](#_Toc167815909)

# **Introduction**

XYZ University is a prominent institution with two campuses positioned 100 miles apart. The university comprises four faculties: Health and Sciences, Business, Engineering/Computing, and Art/Design, catering to approximately 30,000 users. Anticipating significant growth, the university aims to double its user count by 2025. This project involves designing a secure, scalable, and robust network system to meet the future needs of the university.

# **History**

The university has a long-standing reputation for excellence in education and research. With the expansion of its campuses and the growing need for secure and reliable network infrastructure, the university has prioritized upgrading its IT systems to ensure seamless connectivity and technological cohesion.

# **What is Secure System and Secure Campus**

# **System**

A secure network system involves protecting data and resources within a network through various security measures, including firewalls, encryption, and access controls. A secure campus network system extends these principles to an academic environment, ensuring that students, staff, and faculty can access necessary resources securely and efficiently.

# **Software Requirements**

## Cisco Packet Tracer

Cisco Systems, Inc. is a leading multinational technology conglomerate renowned for its networking hardware, telecommunications equipment, and high-technology services and products. Cisco's robust suite of networking solutions, including routers, switches, and security devices, have established the company as a global leader in the field of networking and cybersecurity.

For the design and implementation of the secure campus network system at Martin Luther King University, we utilized Cisco Packet Tracer, a powerful network simulation tool developed by Cisco. Cisco Packet Tracer provides a comprehensive platform for modeling, designing, and simulating network configurations and topologies, enabling network engineers to visualize and test complex network setups before actual deployment.

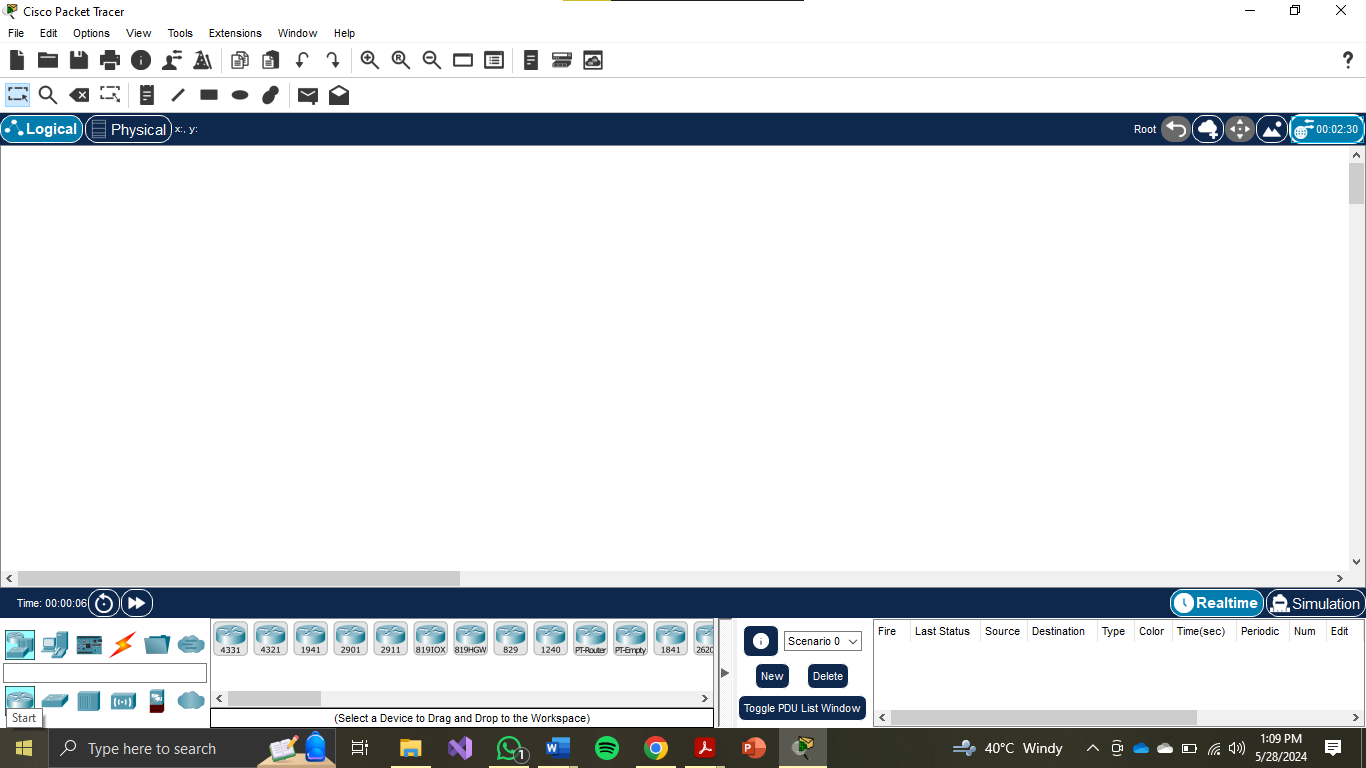


Figure 1: Cisco Packet Tracer Interface

# **Objectives**

The major objective of this system is to:

* Design a secure, scalable, and robust network system for both campuses.
* Ensure redundancy, scalability, and high availability.
* Implement secure communication channels between campuses.
* Centralize wireless network management.
* Facilitate seamless access to university resources and services.

# **Functions of Secure Campus Network System**

* Provide secure and reliable internet connectivity.
* Ensure secure access to centralized servers and resources.
* Enable wireless access for users across both campuses.
* Implement network security measures to protect against threats.
* Ensure high availability and redundancy in the network infrastructure.

# **Problem Definition**

The current network infrastructure needs to be upgraded to handle the anticipated growth and ensure secure, reliable, and efficient communication and resource access across both campuses. The new design must address scalability, redundancy, and security requirements.

# **Features of Secure Campus Network System**

* Hierarchical network design with redundancy.
* Secure site-to-site IPsec VPN between campuses.
* Centralized wireless management via WLC.
* VLANs for network segmentation.
* EtherChannel for link aggregation.
* STP PortFast and BPDUguard for efficient port management.
* Dynamic IP addressing via DHCP.
* Static addressing for critical server infrastructure.
* OSPF for dynamic routing.
* HSRP for high availability.
* Access control via standard ACLs and firewall policies.

# **Methodology**

### Initiation

1. Assess current network infrastructure and requirements.
2. Define project scope and objectives.
3. Gather hardware and software resources.

### Implementation

* Design network topology using Cisco Packet Tracer.
* Configure VLANs, EtherChannel, and STP settings on switches.
* Set up wireless infrastructure with WLC and LAPs.
* Implement IPsec VPN on Cisco ASA Firewalls.
* Configure OSPF routing and HSRP for high availability.
* Set up DHCP servers and static addressing for critical devices.
* Implement security policies and ACLs on firewalls and network devices.
* Test network connectivity, performance, and security measures.

### Further Usage

* Continuous monitoring and maintenance of the network.
* Regular updates to hardware and software components.
* Scalability planning for future growth.

# **Network Protocols Overview**

### IPsec VPN (Internet Protocol Security Virtual Private Network)

IPsec is a suite of protocols designed to ensure secure communication over IP networks. It authenticates and encrypts each IP packet within a communication session.

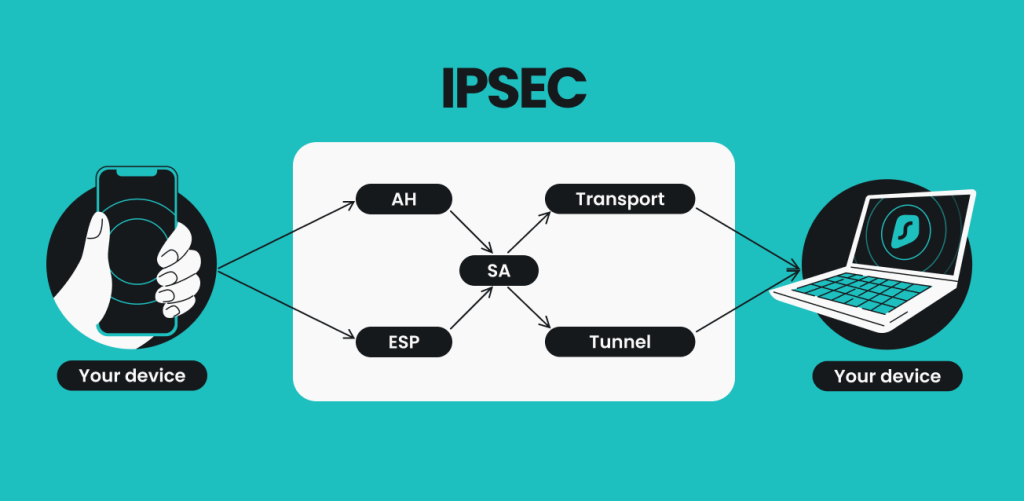


Figure 2: Internet Protocol Security Virtual Private Network

* **Application in Project**: Used to establish secure site-to-site VPN connections between the main and branch campuses.

### LACP (Link Aggregation Control Protocol)

LACP is used to combine multiple physical links into a single logical link to increase bandwidth and provide redundancy.

* **Application in Project**: Implemented for EtherChannel configuration to enhance link aggregation efficiency.

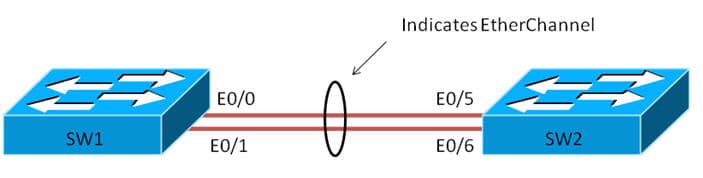


Figure 3: Link Aggregation Control Protocol

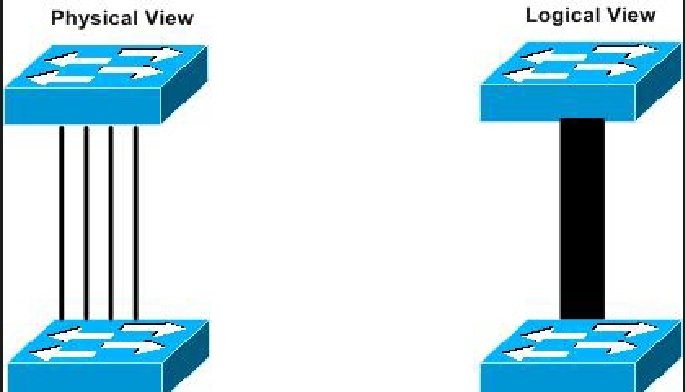


Figure 4: logical and Physical View of Link Aggregation Control Protocol

### STP (Spanning Tree Protocol)

STP prevents network loops by creating a spanning tree within a network of connected layer-2 bridges.

* **Application in Project**: Configured with PortFast and BPDUguard to expedite port transitions and enhance network stability.

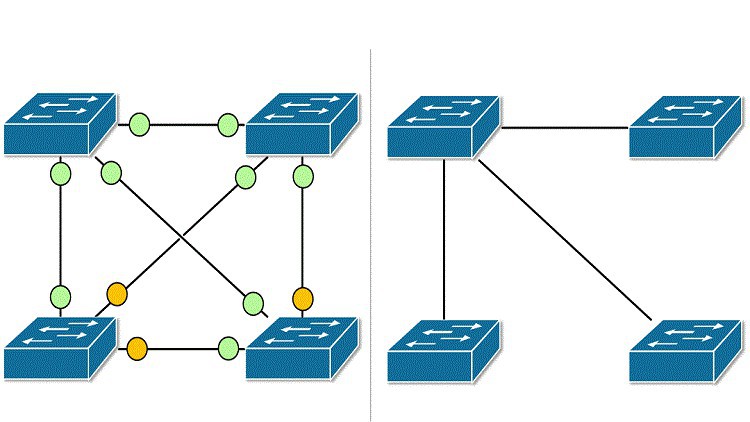


Figure 5: Spanning Tree Protocol

### DHCP (Dynamic Host Configuration Protocol)

DHCP dynamically assigns IP addresses to devices on a network, ensuring efficient IP address management.

* **Application in Project**: Used for automatic IP address allocation to devices within the network.

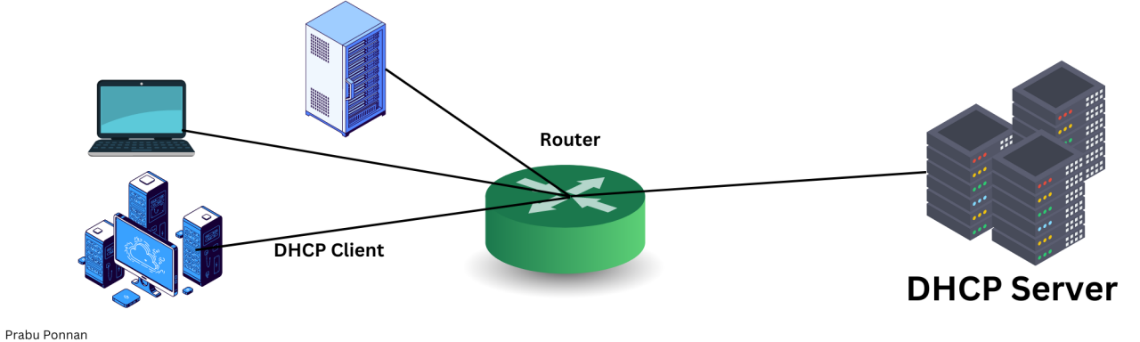


Figure 6: Dynamic Host Configuration Protocol

### HSRP (Hot Standby Router Protocol)

HSRP provides network redundancy for IP networks, ensuring high availability by routing traffic through standby routers if the active router fails.

* **Application in Project**: Implemented to achieve redundancy, load balancing, and failover capabilities.

### OSPF (Open Shortest Path First)

OSPF is a routing protocol for Internet Protocol (IP) networks that uses a link state routing algorithm.

* **Application in Project**: Utilized for dynamic routing to advertise routes on firewalls, routers, and multilayer switches.

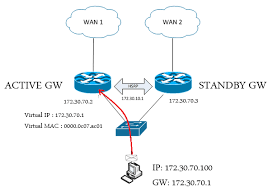


Figure 7: Open Shortest Path First

### SSH (Secure Shell)

SSH is a cryptographic network protocol for operating network services securely over an unsecured network.

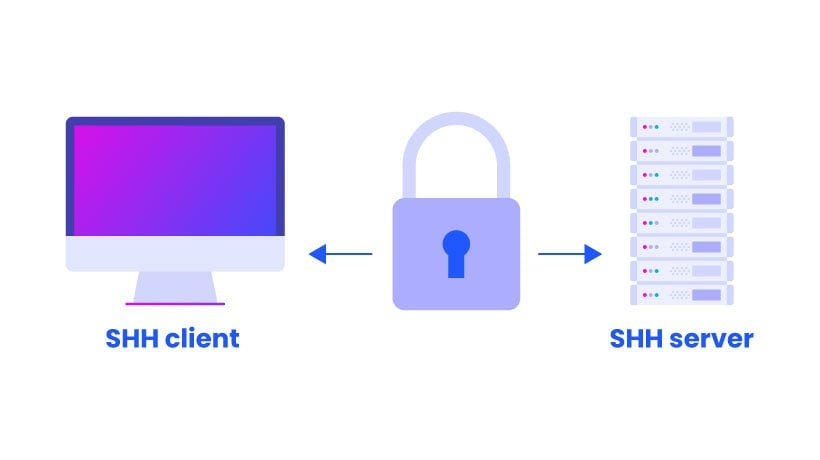
* **Application in Project**: Used for secure remote administrative access to network devices.  
    
  

Figure 8: Secure Shell

### HTTP/HTTPS (Hypertext Transfer Protocol / Secure)

HTTP and HTTPS are protocols for transmitting hypertext requests and information on the internet.

* **Application in Project**: Used for web services hosted on the university’s servers.

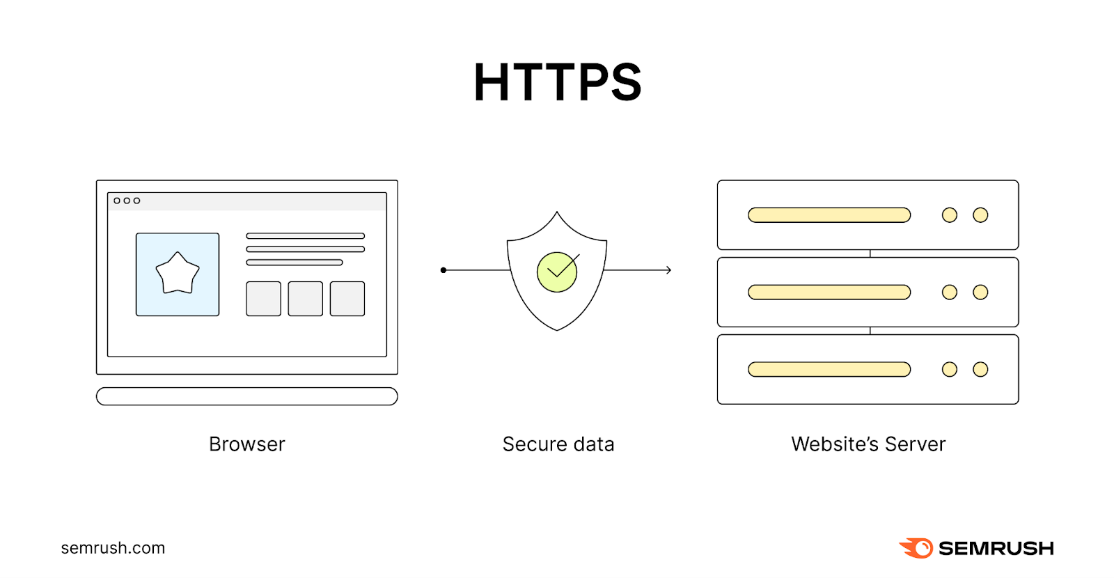


Figure 9: Hypertext Transfer Protocol / Secure

### SMTP (Simple Mail Transfer Protocol)

SMTP is a protocol for sending email messages between servers.

* **Application in Project**: Used for email services within the university’s network.

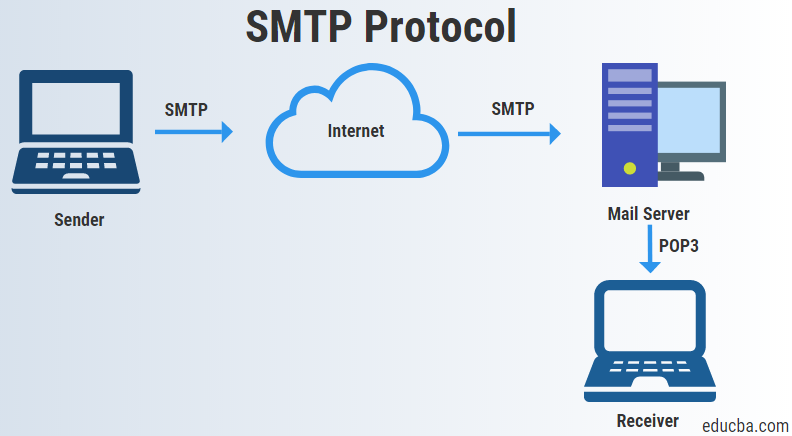


Figure 10: Simple Mail Transfer Protocol

### DNS (Domain Name System)

DNS translates domain names into IP addresses, allowing users to access websites using human-readable names.

* **Application in Project**: Employed for name resolution services.

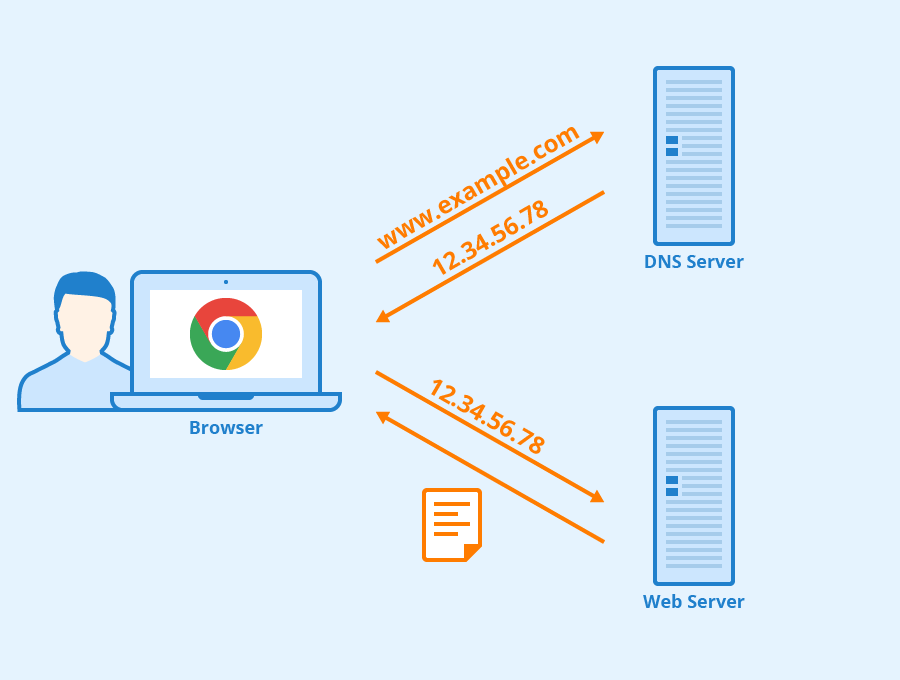


Figure 11: Domain Name System

### FTP (File Transfer Protocol)

FTP is used to transfer files between a client and server on a network.

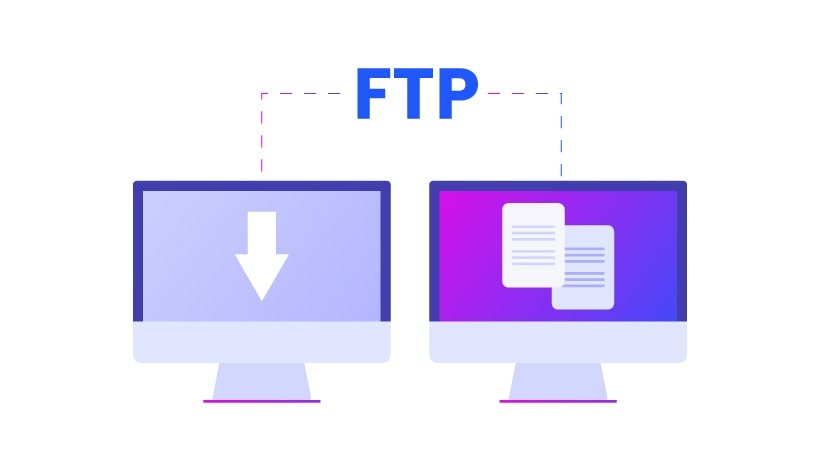
* **Application in Project**: Used for file transfer services within the university’s network.   
  

Figure 12: File Transfer Protocol

### NAT (Network Address Translation)

NAT is used to remap one IP address space into another by modifying network address information in the IP header of packets while they are in transit.

* **Application in Project**: Facilitates the sharing of a single public IP address among multiple devices on the private network, enhancing security and reducing the number of public IP addresses required.

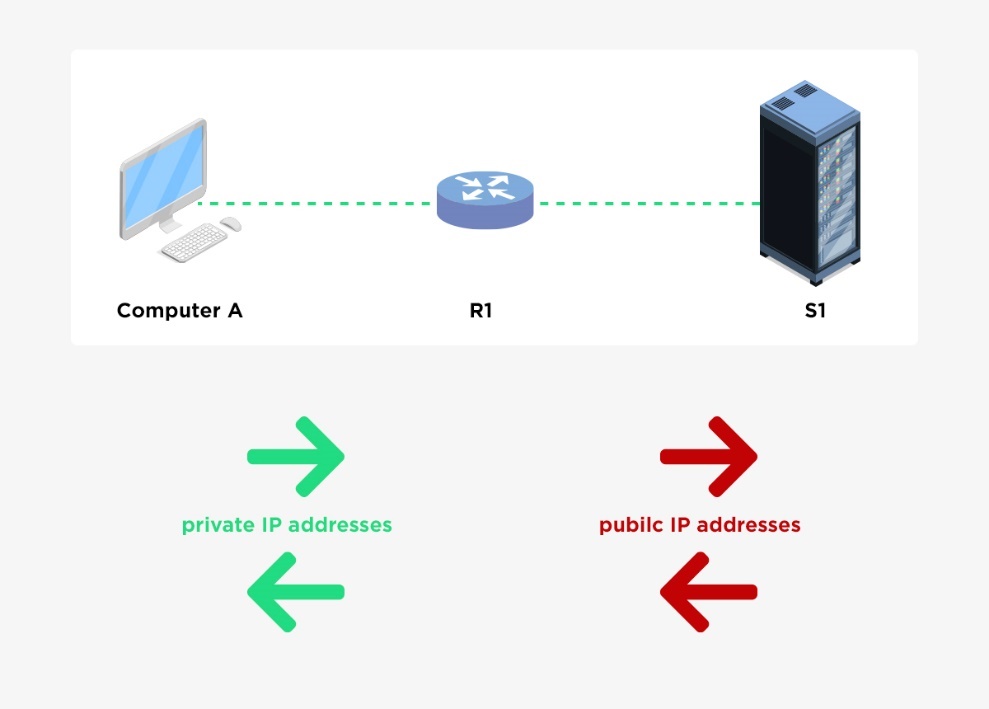
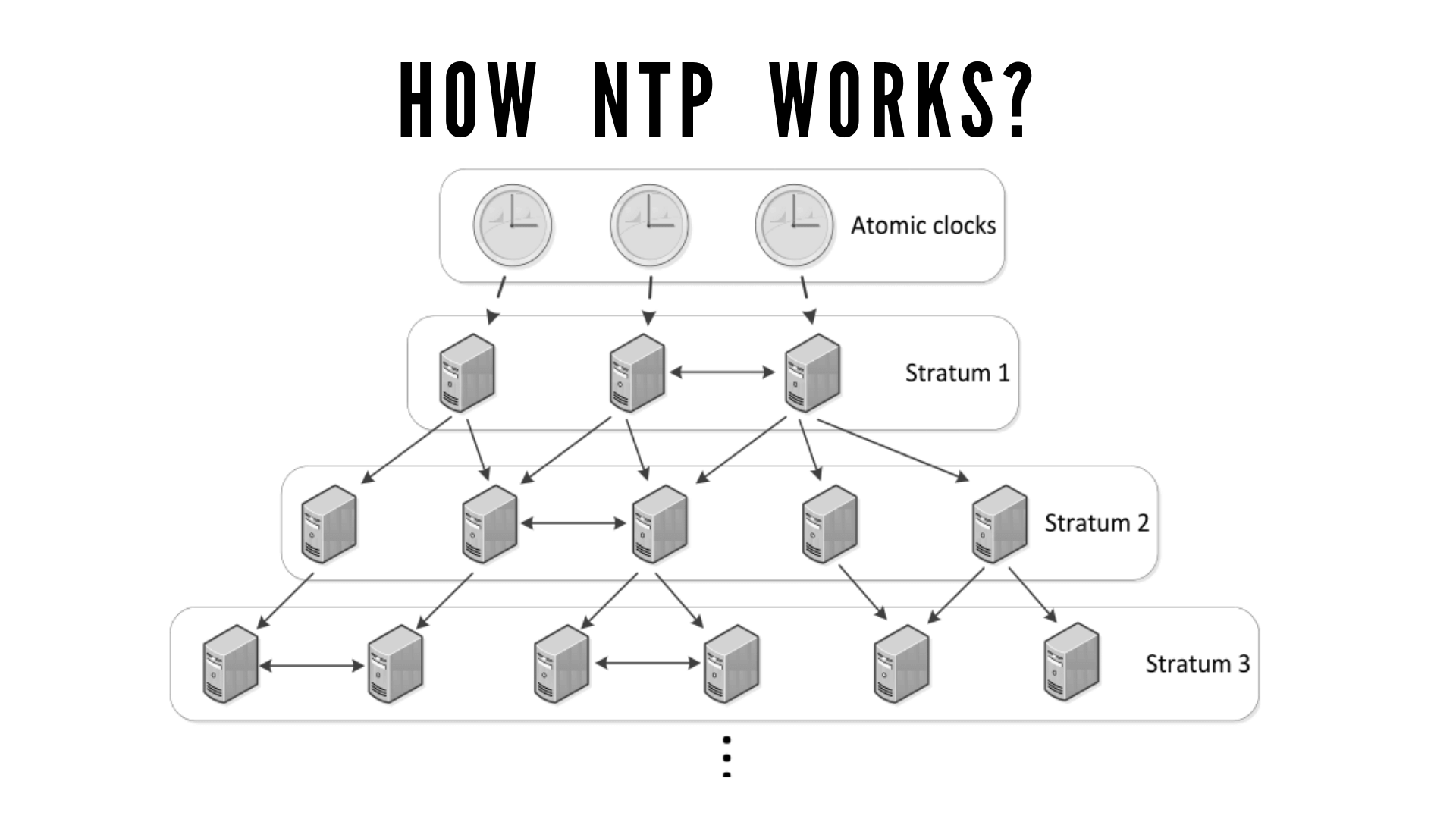


Figure 13: Network Address Translation



# **SnapShots**

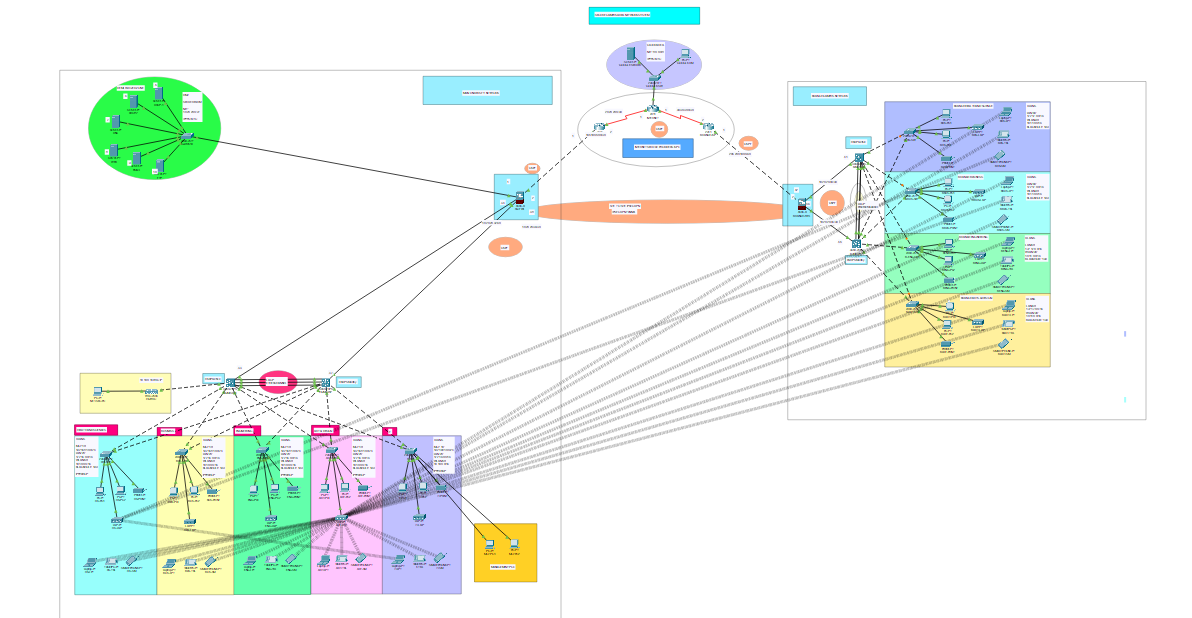


Figure 14: Secure Campus Network System Topology

A screenshot of a computer

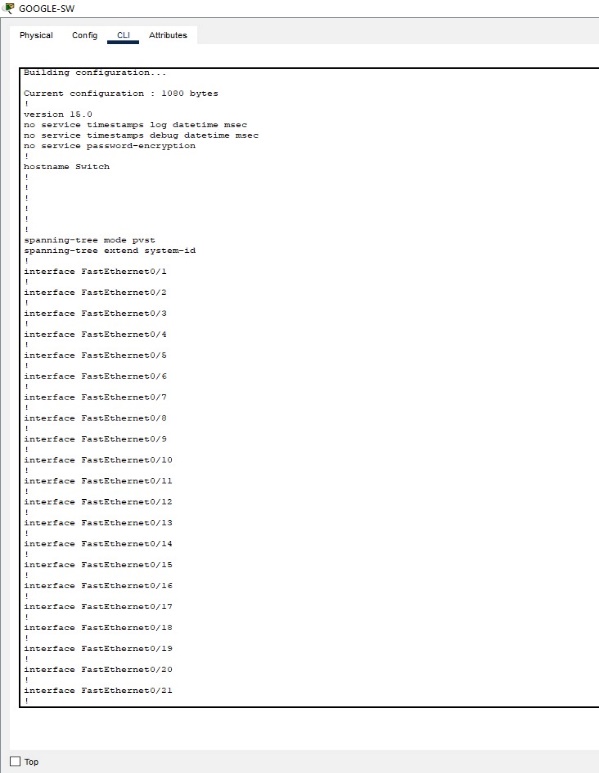
Description automatically generated

Figure 15: Google Switch Configuration

A screenshot of a computer

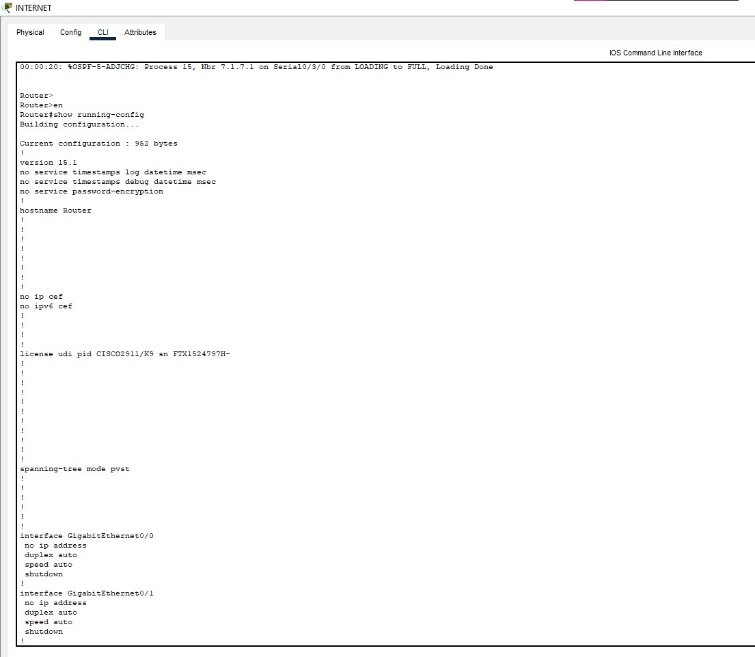
Description automatically generated

Figure 16: Internet Router Configuration

A screenshot of a computer

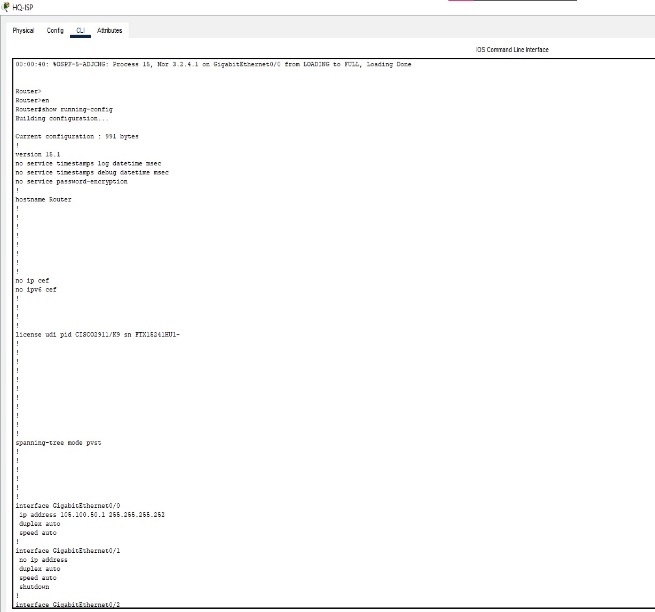
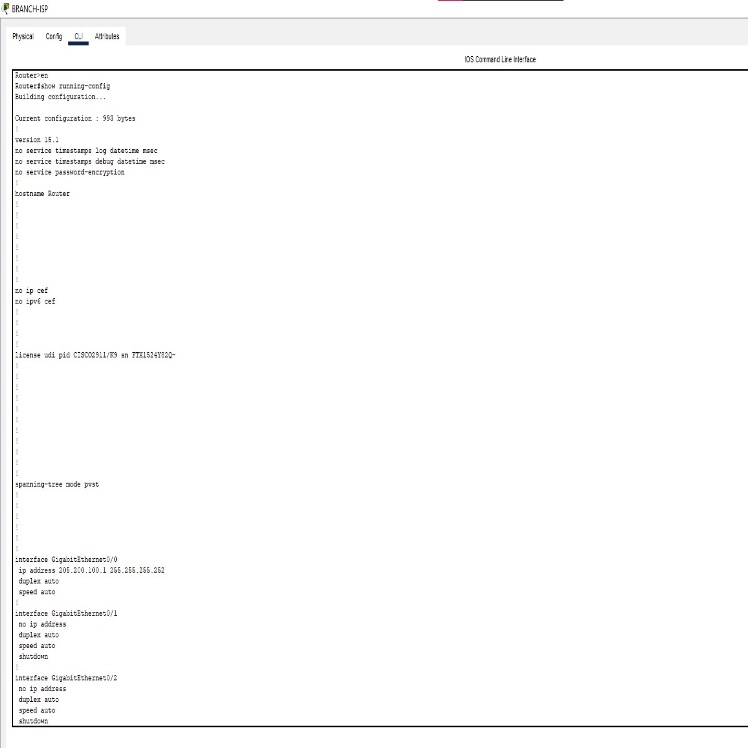
Description automatically generated

Figure 17: HQ ISP Router Configuration

Figure 18: Branch ISP routerA screenshot of a computer

Description automatically generated Configuration

A screenshot of a computer

Description automatically generated

A screenshot of a computer

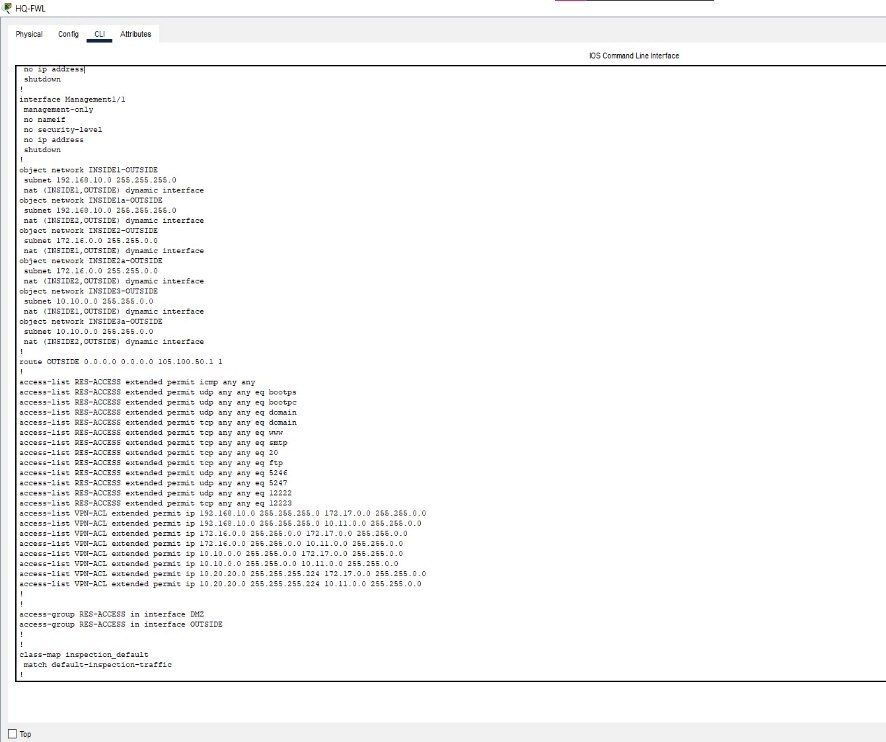
Description automatically generated

Figure 19: HQ FWL Configuration

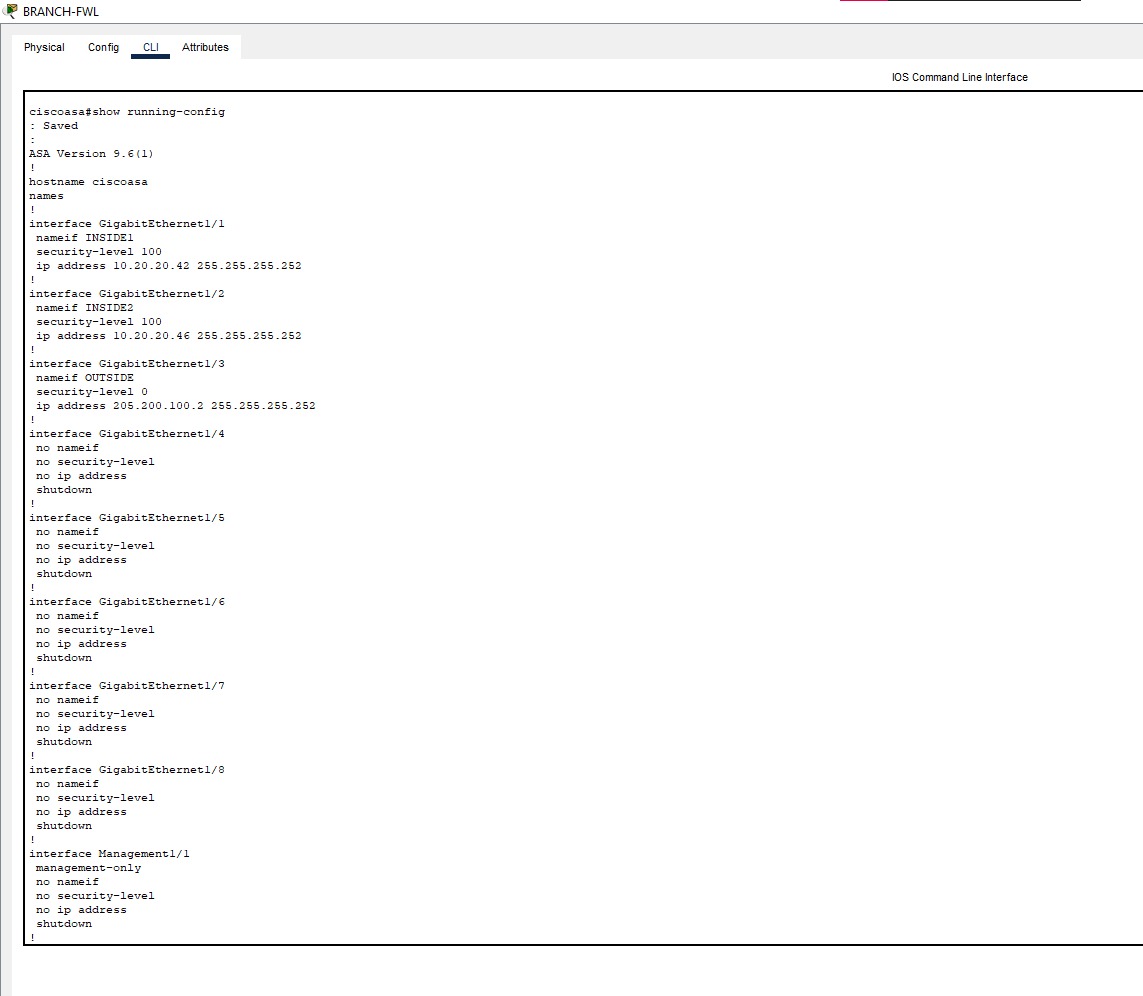


Figure 20: Branch FWLA screenshot of a computer

Description automatically generated Configuration

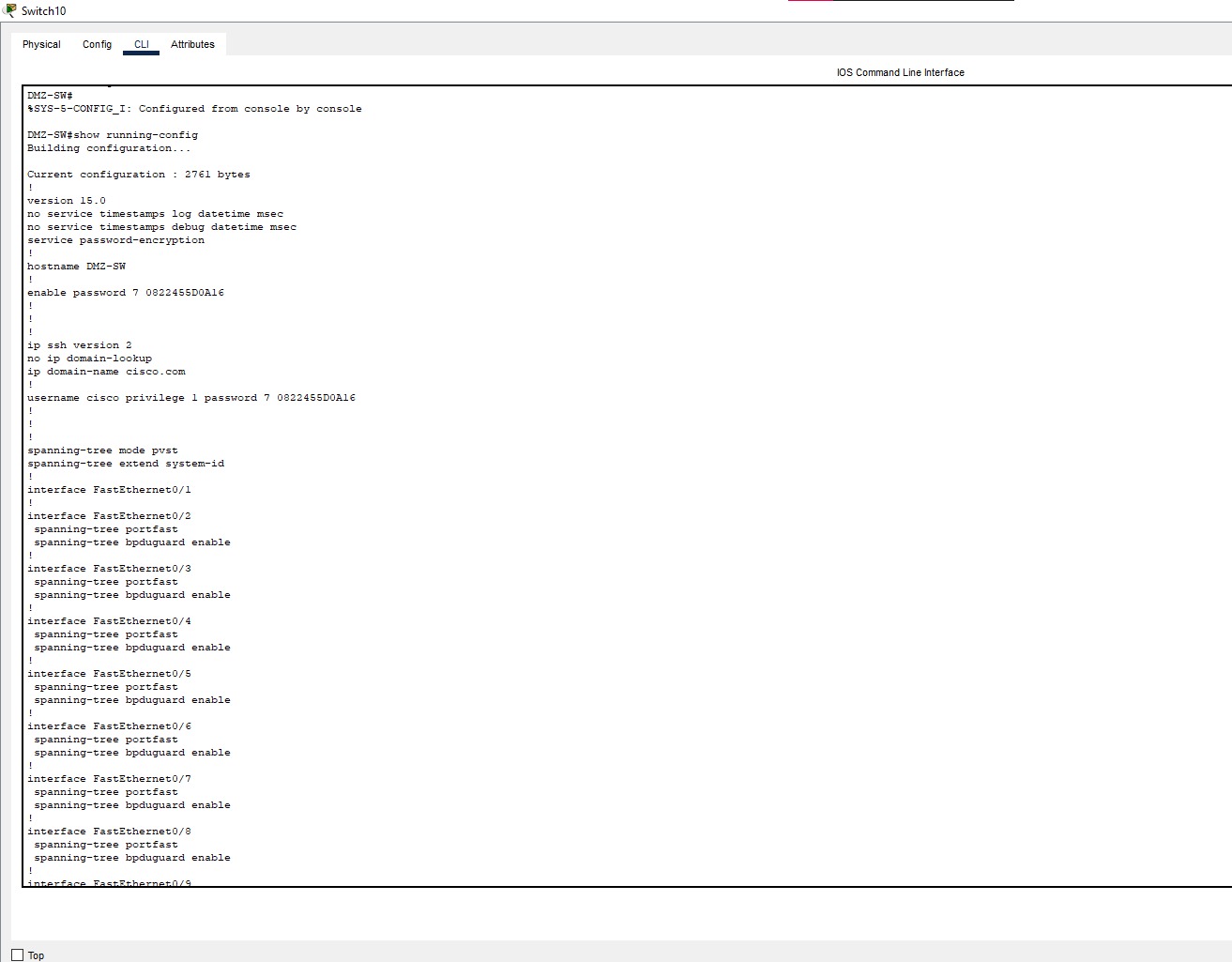
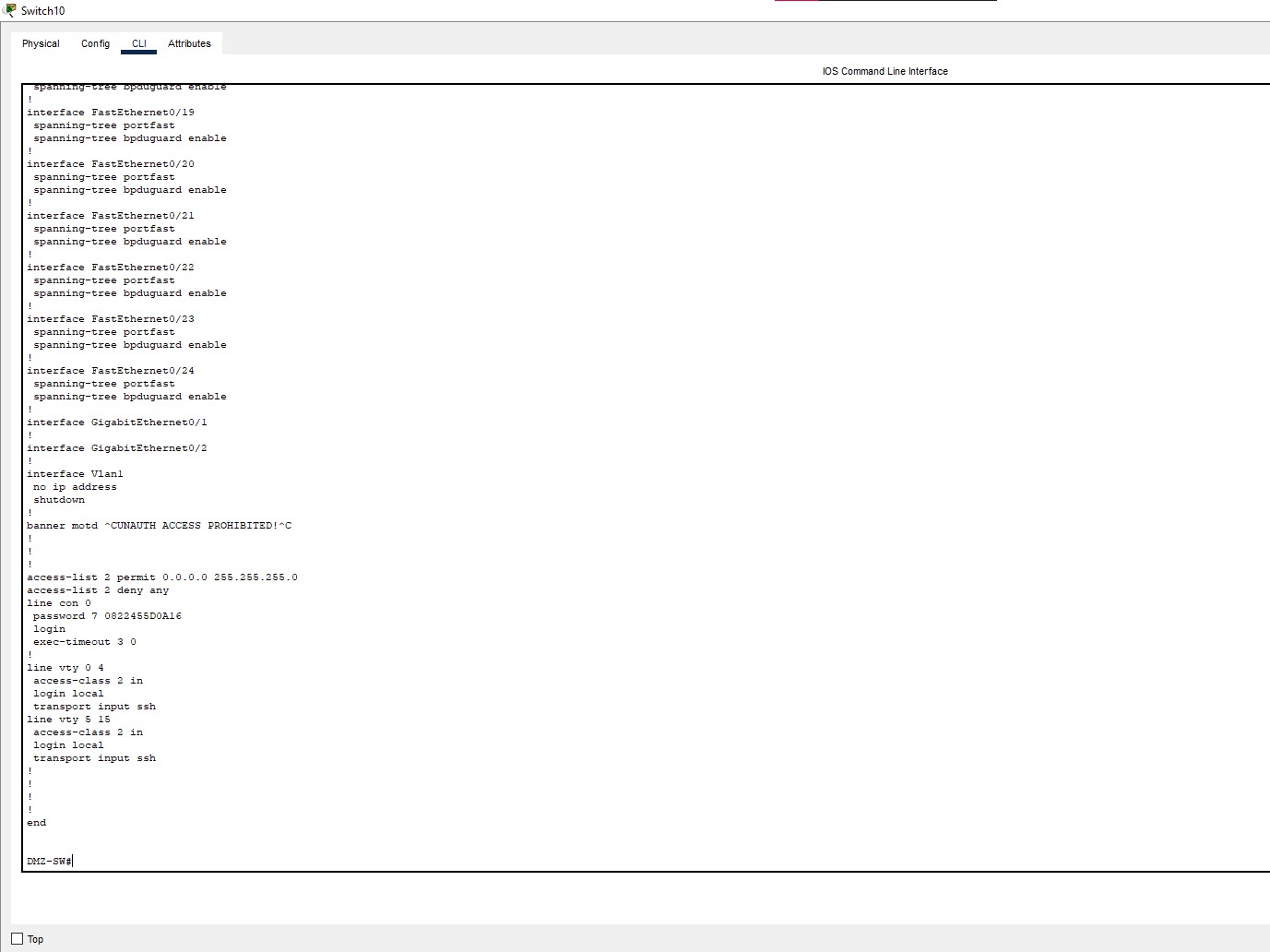


Figure 21: DMZ Switch Configuration

Figure 22: HQ MLS1A screenshot of a computer

Description automatically generated Configuration

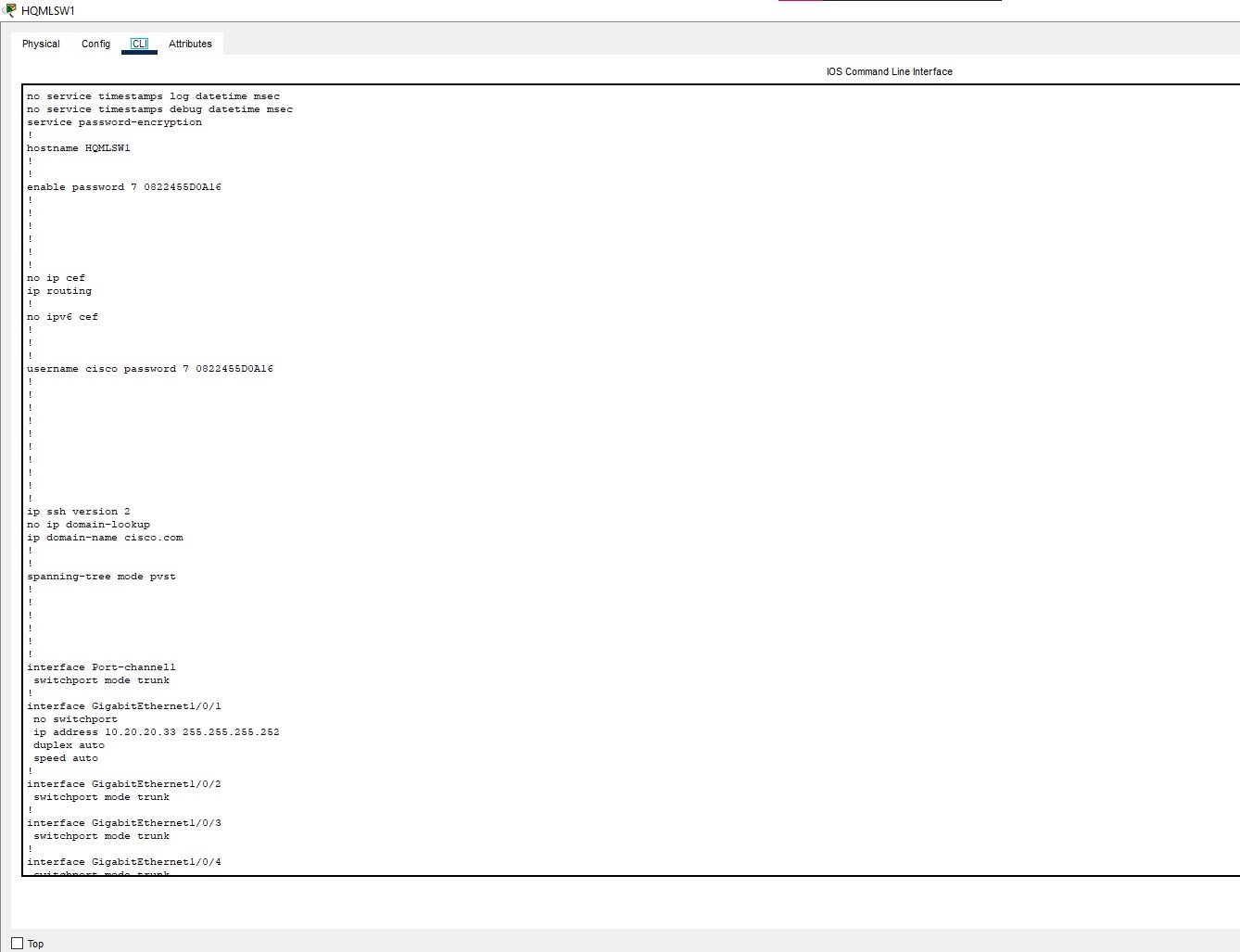


Figure 23: HQ MLS2A screenshot of a computer

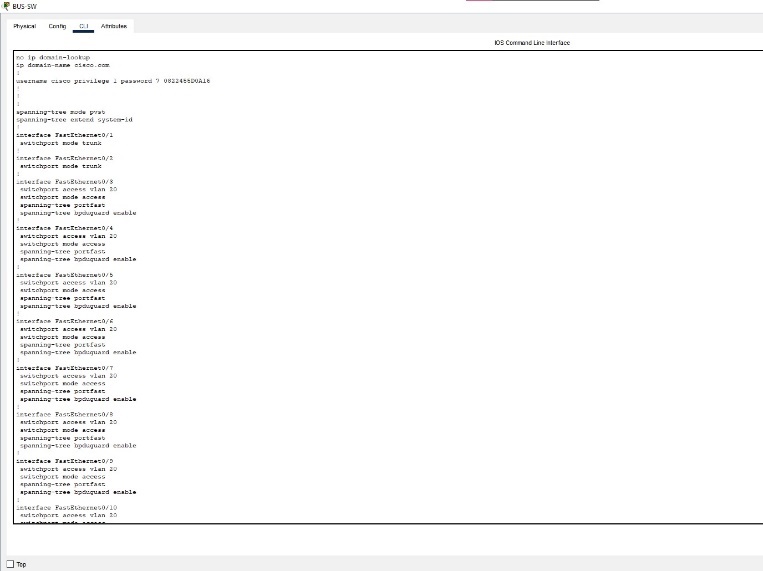
Description automatically generated Configuration

Figure 24: Bus Switch Configuration

A screenshot of a computer

Description automatically generated

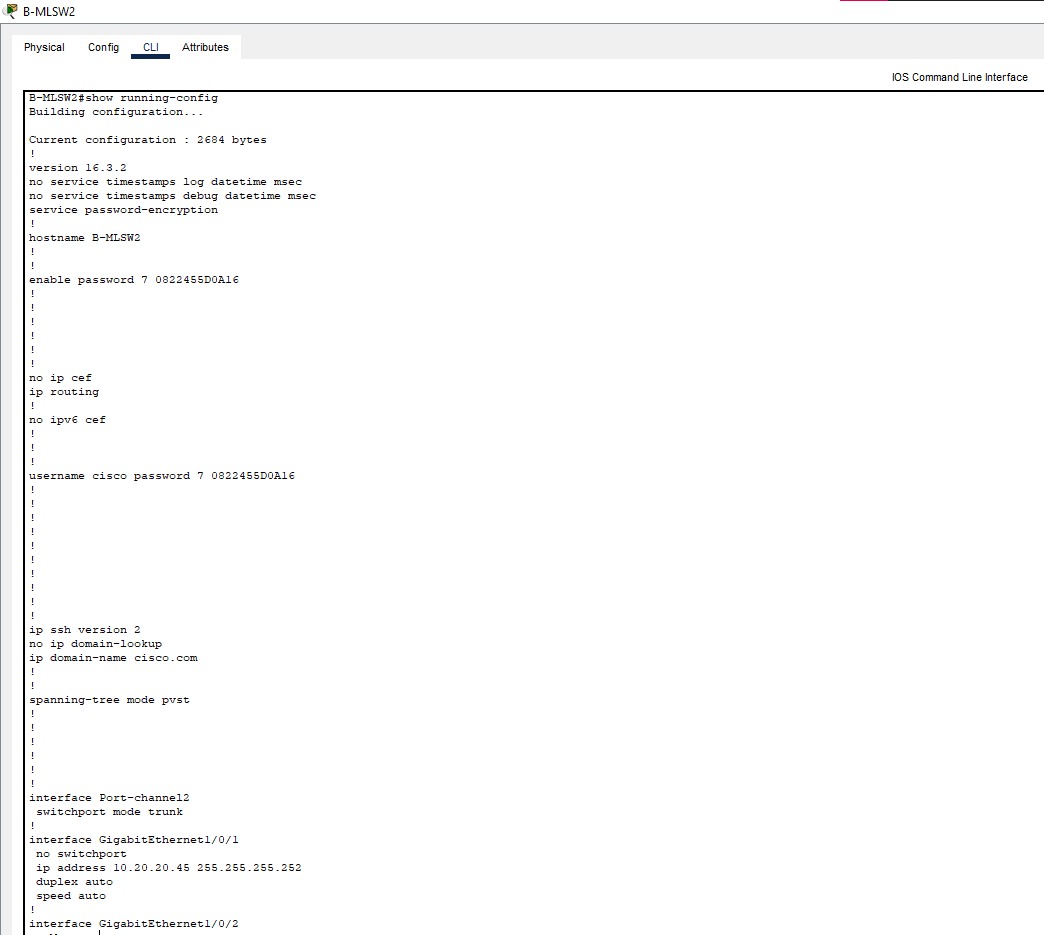
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

Figure 25: Branch MLS1 Configuration   
  
  
  


A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

Figure 26: Branch MLS2 Configuration

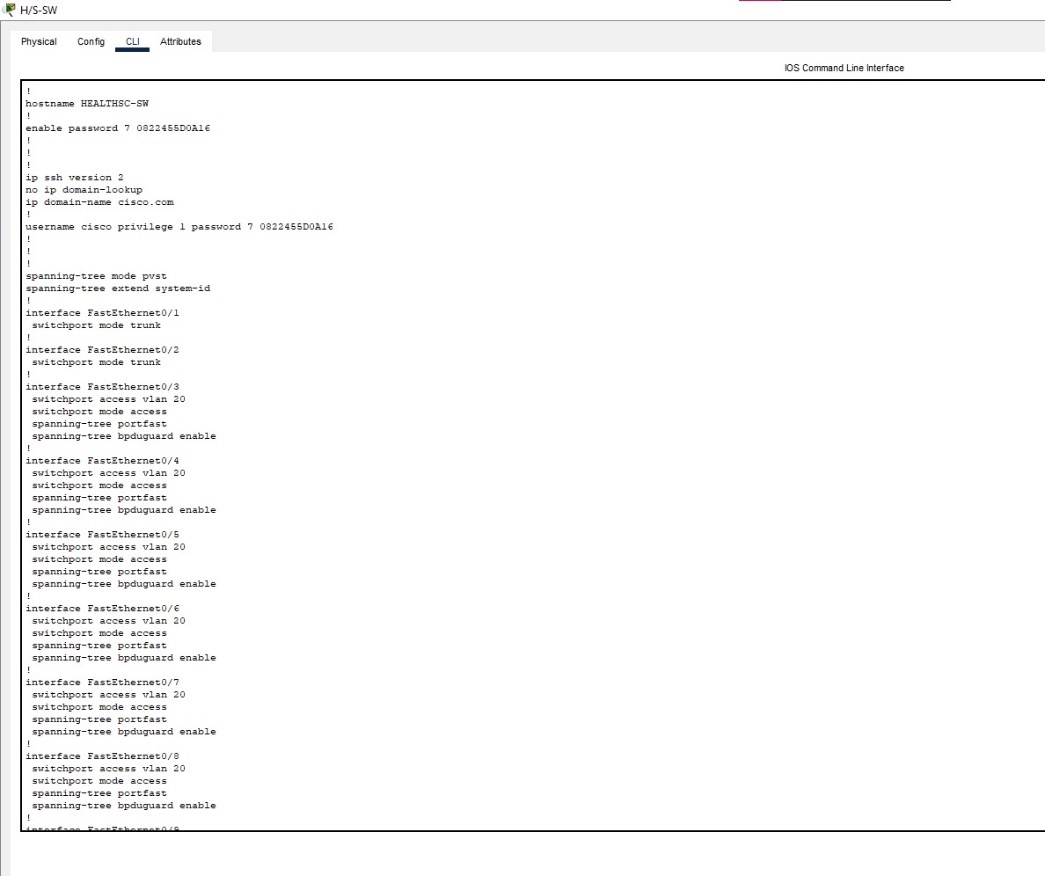


Figure 27: Health and Science Department Switch Configuration

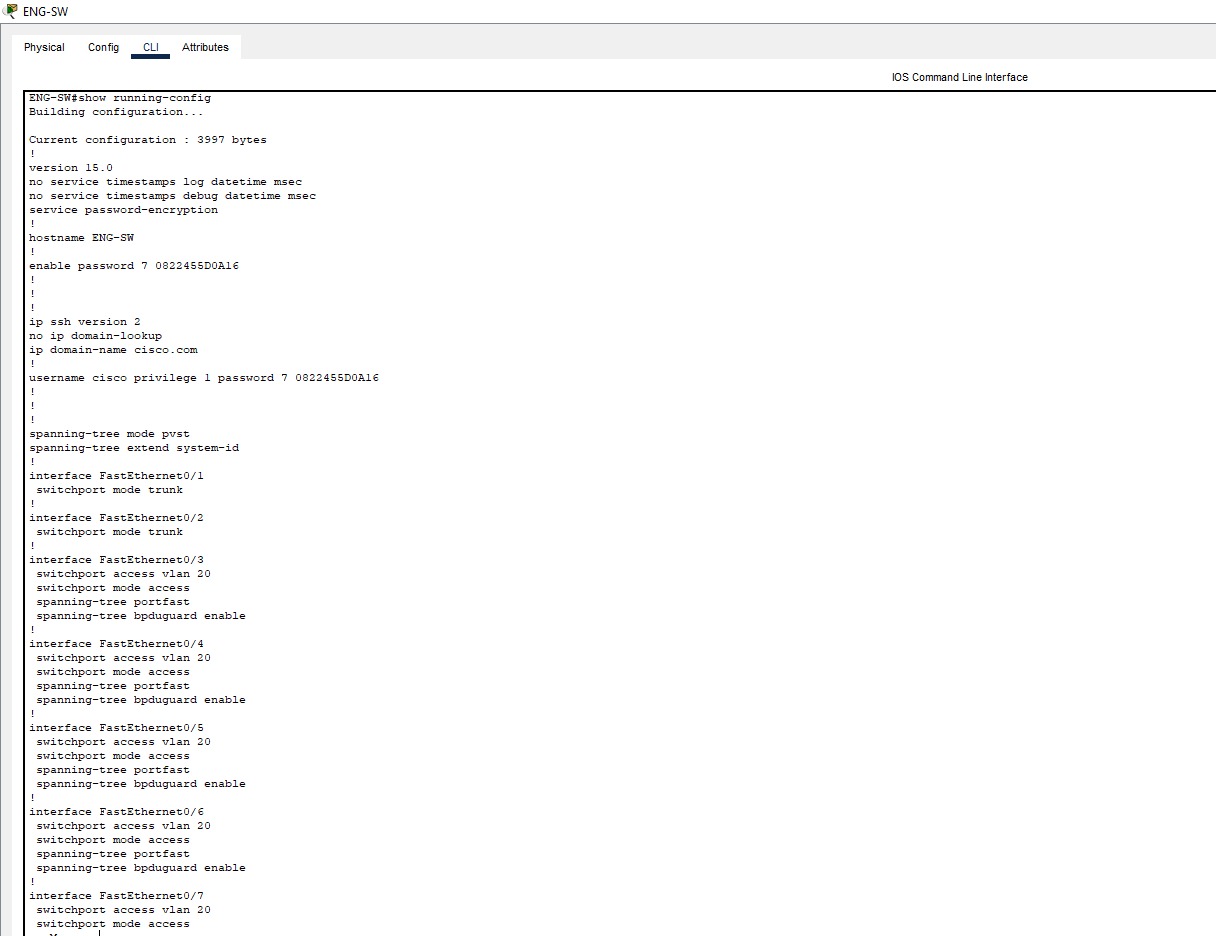


Figure 28: Engineering Department Switch Configuration

Figure 29: Art Department Switch Configuration

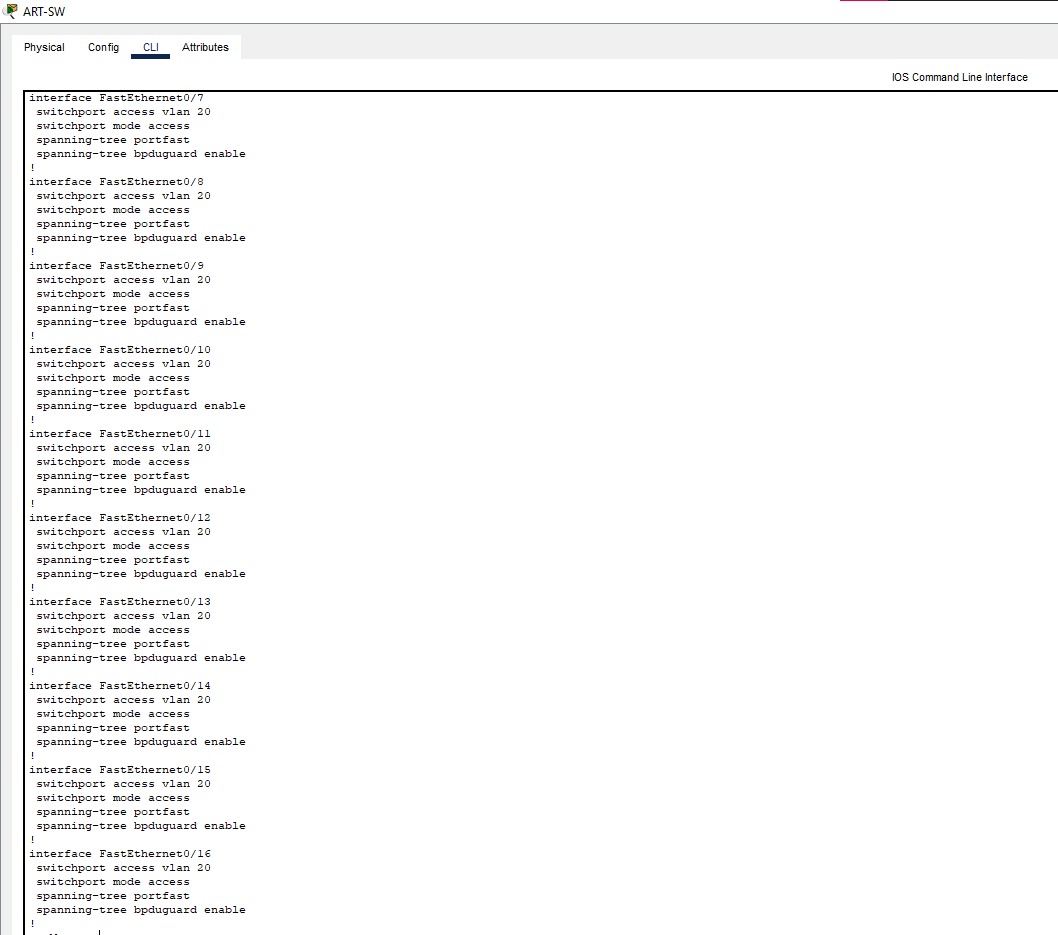
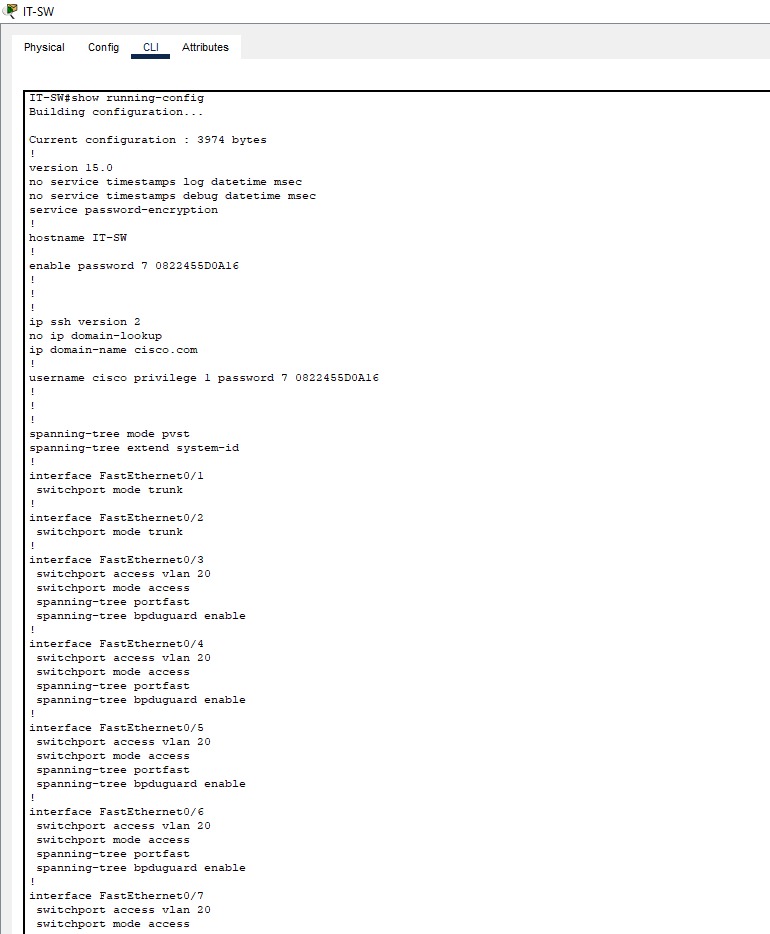


Figure 30: IT Department Switch Configuration



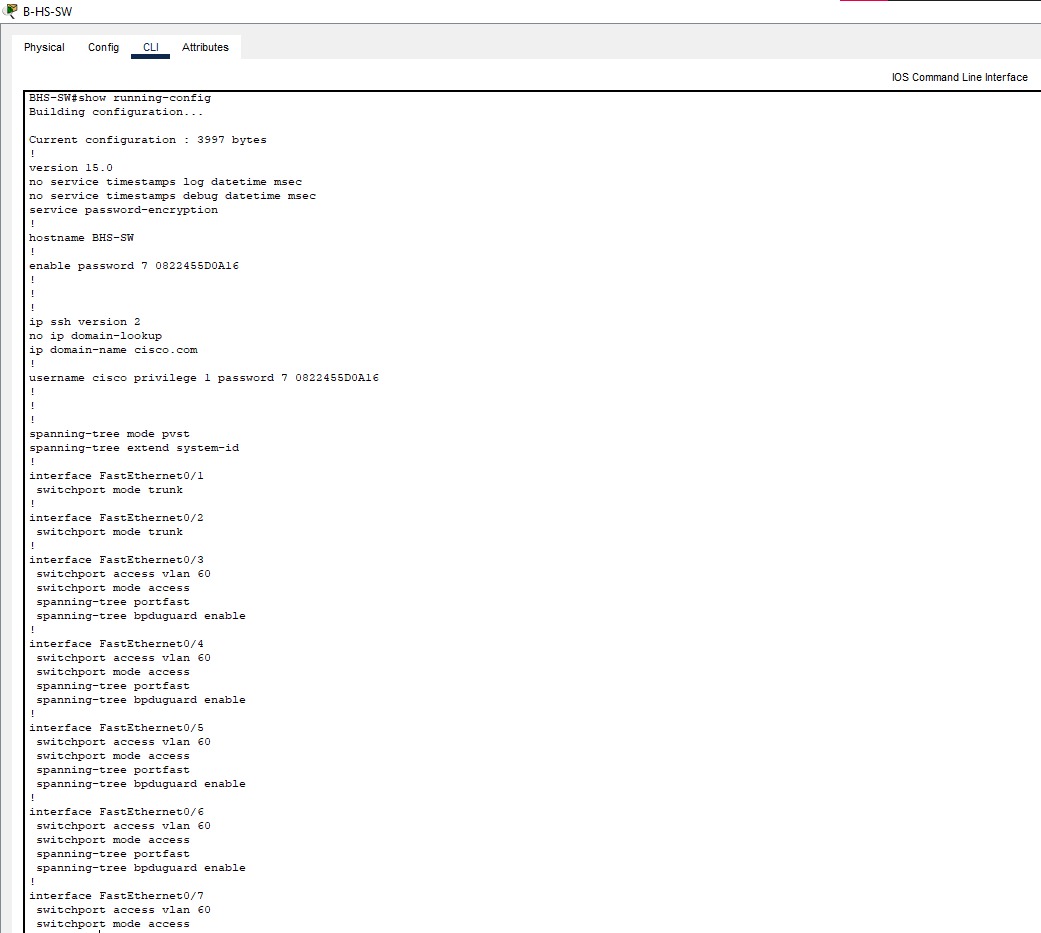


Figure 31: Branch H/S Department Switch Configuration

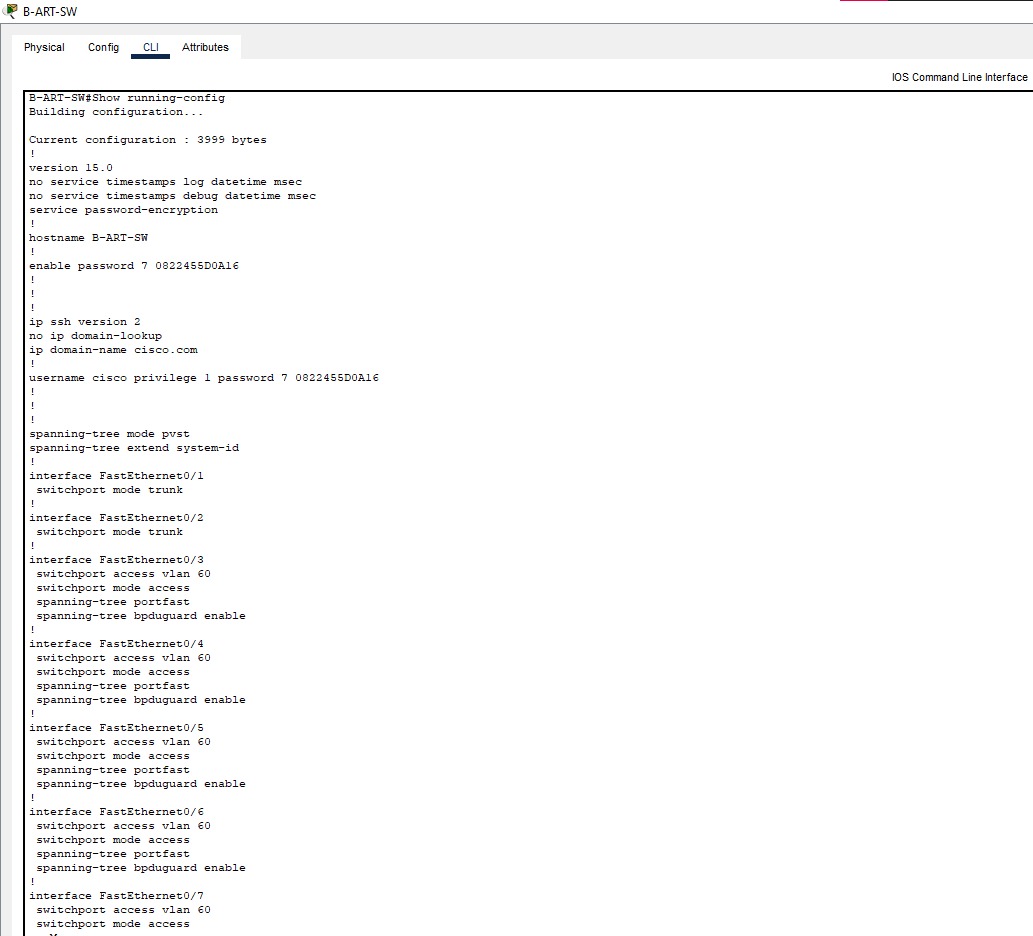
Figure 32: Branch Business SwitchA screenshot of a computer

Description automatically generated Configuration

A screenshot of a computer

Description automatically generated

Figure 33: Branch Engineering Department Switch Configuration

Figure 34: Branch Art Department Switch Configuration

# **Conclusion**

The design and implementation of the secure campus network system at XYZ University will provide a robust, scalable, and secure infrastructure to support the growing needs of the university. By leveraging Cisco technologies and best practices in network design, the university can ensure seamless connectivity, high availability, and secure access to resources across both campuses.