University Network Infrastructure

Dec 26, 2023
CE-313 Project

Group Members

Abdul Moiz Ghumman
2021015
M. Waiz Hamid
2021486
Haseeb Ahmer
2021903

Documentation

Introduction

Purpose:

To establish a robust, secure, and scalable network infrastructure that supports the university's academic, administrative, and research activities.

Scope:

Our vision stretches beyond departmental silos, encompassing the entirety of the university network, from the central arteries of the core layer to the capillaries reaching every device in the remotest corner. This comprehensive approach not only guarantees seamless and robust connectivity, but also lays the foundation for future expansion and innovation.

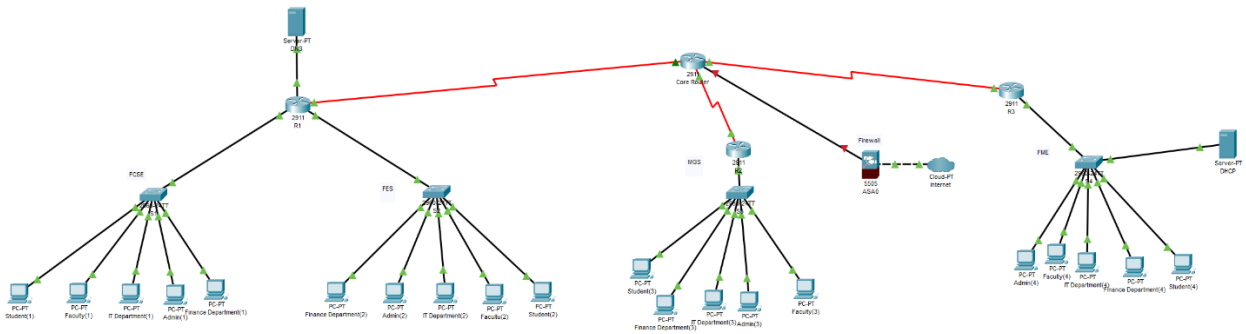
Motivation:

Driven by the need for seamless connectivity, enhanced collaboration, and robust security in a rapidly evolving digital landscape. We want everyone to have a super-fast, reliable connection, so they can learn, work, and share ideas without any hiccups. We also want everyone to feel safe and protected online, with strong security walls keeping their information private. Ultimately, we're building a digital world where everyone has the tools they need to succeed, whether they're a student doing research, a professor sharing knowledge, or someone keeping the university running smoothly.

Network Design Topology

Hierarchical topology:

Comprises core, distribution, and access layers for efficient traffic flow, manageability, and scalability.



Key components:

Core layer:

High-performance switches for backbone connectivity.

Distribution layer:

Routers for inter-VLAN routing and traffic management.

Access layer: Managed switches for connecting end devices and enforcing security policies.

VLANs:

Used for logical segmentation, security, and performance optimization.

Implemented Tools and Techniques

Managed switches:

For intelligent traffic handling and security features.

Inter-VLAN routing:

Facilitates communication between different VLANs using routers and dynamic routing protocols like OSPF.

DNS:

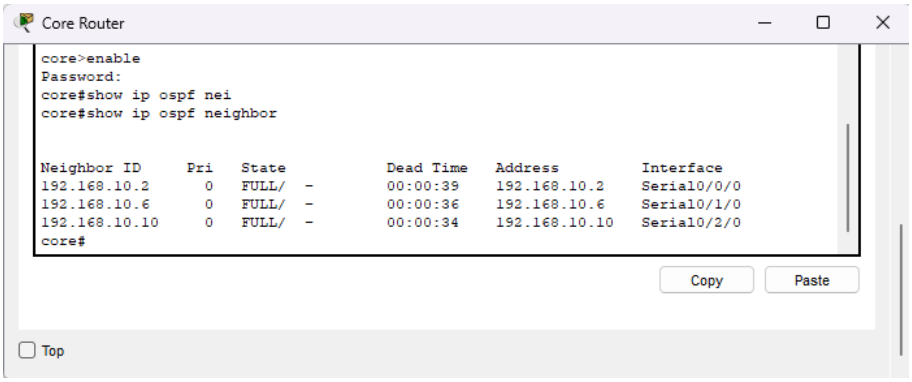
Domain Name System for domain name resolution.

NAT:

Network Address Translation for conserving public IP addresses and enhancing security.

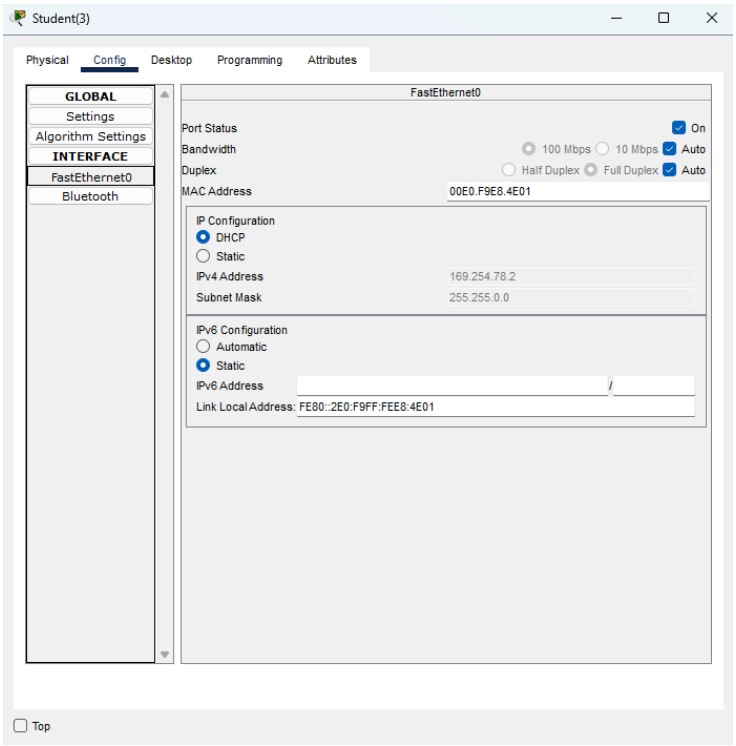
OSPF:

We used ospf as the routing protocol as required.



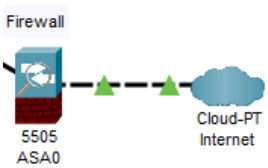
DHCP:

Dynamic Host Configuration Protocol for automatic IP address assignment.



Firewalls:

For traffic filtering, access control, and intrusion prevention.



Switch port security:

To prevent unauthorized access and protect network integrity.

Implemented Tools and Techniques

Designing and Testing:

To carefully plan and test the network before implementation, we used Packet Tracer, a powerful simulation tool that allowed us to create a virtual version of our network and experiment with different configurations. This helped us ensure everything would work smoothly before making any physical changes.

Routers:

At the heart of our network, we placed Cisco 2911 routers to form the core layer. These high-performance routers are responsible for handling massive amounts of data traffic and ensuring efficient communication across different parts of the campus.

Connecting Departments and Users:

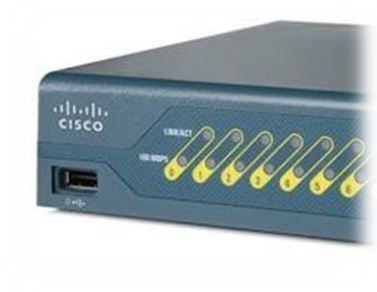
To extend the network's reach and connect various departments and user groups, we strategically deployed three additional Cisco routers. These routers act as distribution layer devices, responsible for routing traffic between different VLANs (virtual local area networks) and managing communication flows.

Switches:

At the access layer, we installed Cisco 2960-24T managed switches to provide reliable connections for computers, printers, and other devices. These intelligent switches offer advanced features like VLAN support, port security, and traffic prioritization, ensuring a secure and efficient network experience for all users.

Firewall:

Guarding our digital gates, the Cisco ASA 5505 firewall stands vigilantly. Like a digital knight in shining armor, it wields a powerful arsenal of access controls, deep packet inspection, and even an intrusion prevention system to shield our network from unauthorized access and lurking threats. This robust protector ensures seamless connectivity while keeping sensitive information safe, allowing us to focus on what truly matters - learning, research, and the pursuit of knowledge within our secure digital walls.



Workflow and Troubleshooting Steps

Planning and design phase:

Gather requirements, analyze existing infrastructure, and design the network topology.

Select hardware and software components.

Implementation phase:

Install and configure network devices.

Implement VLANs, routing, DHCP, DNS, NAT/PAT, and firewalls.

Conduct testing and validation.

Documentation and training phase:

Create comprehensive documentation for network configuration and troubleshooting.

Provide training for IT staff and users.

Troubleshooting steps:

Use network monitoring tools to identify issues.

Check logs and configurations.

Employ diagnostic tools to isolate problems.

Conclusion

The project has successfully established a secure, scalable, and efficient network infrastructure that meets the project's needs.
Key features include hierarchical topology, advanced switching, and routing technologies, DHCP and DNS services, NAT/PAT, firewalls, and switch port security.

PKT file (attached separately)