Bangabandhu Sheikh Mujibur Rahman
Digital University

Course Code: ICT 4256

Course title: Data communication and Networks Lab

Final Project Report

Submitted To:

Md. Toukir Ahmed

Lecturer,

Bangabandhu Sheikh Mujibur Rahman Digital University, Bangladesh

Submitted By:

Tanvir Ahmed

Id: 2001028

Fardin Ahmed Ashan

Id: 2001033

Sheikh Sidratul Muntaha Punno

Id: 2001047

Session: 2020-2021

Department: IoT and Robotics Engineering.

Project Name: University Network System

Abstract:

This report details the design and implementation of a University Network System using Cisco Packet Tracer. The project involved configuring a network that efficiently connects various departments and ensures robust security and seamless communication. Key tasks included selecting appropriate cables, connecting devices, creating and configuring VLANs, adding security measures, and setting up gateways. This document outlines the contributions made to the project, highlighting the specific tasks undertaken.

Introduction:

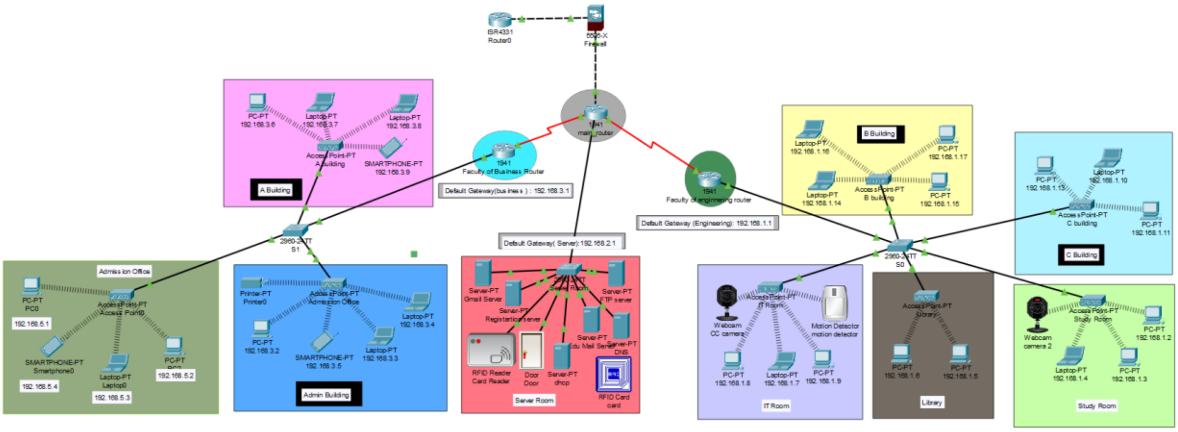
In a modern educational institution, an efficient and secure network system is crucial for seamless communication, resource sharing, and administrative operations. This project aims to design a comprehensive network for a university using Cisco Packet Tracer. The network architecture incorporates best practices in terms of cable selection, device connectivity, VLAN creation and configuration, security via firewalls, and gateway setup.

Network Design and Configuration

1. Cable Selection

Selecting the correct type of cable is fundamental to ensuring optimal network performance and reliability. The project involved choosing appropriate cables for different segments of the network:

- Copper Cross Over: Adding firewall with the router
- Copper Stright-through: Router to switch and switch to AP
- Serial DTE: Connection between Routers



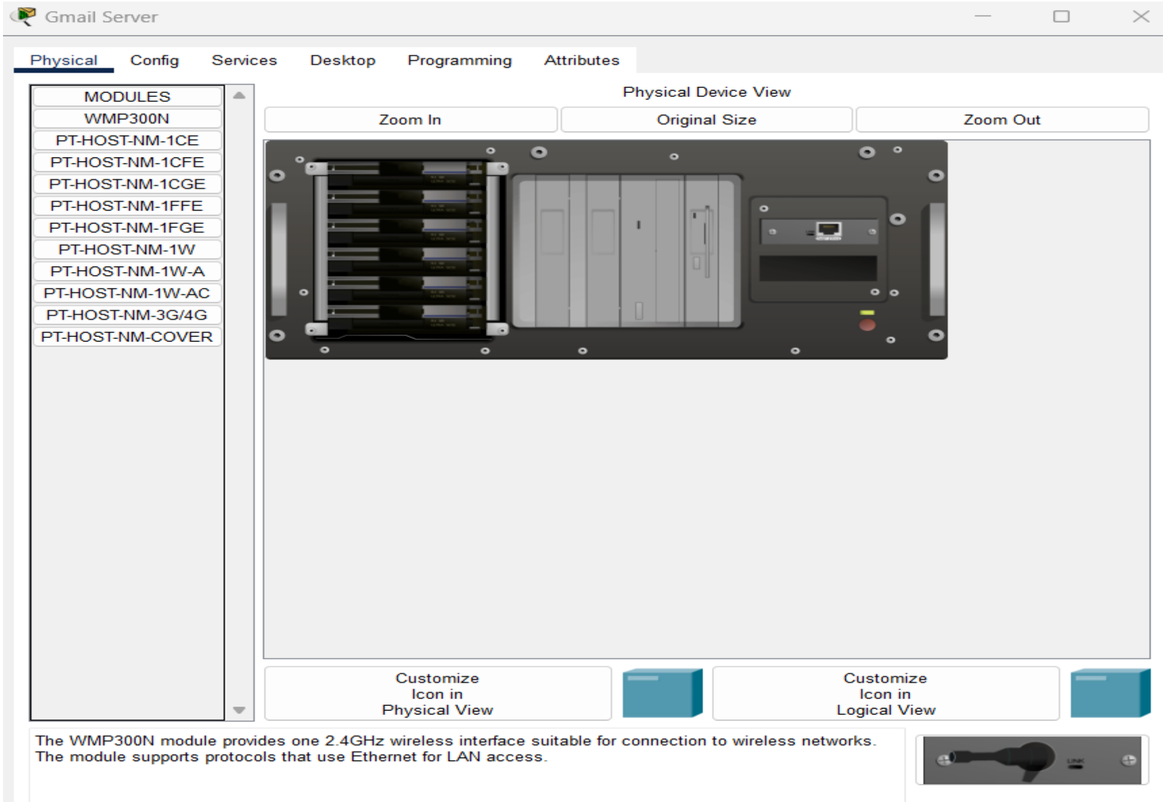
2. Connecting Devices

Connecting the network devices accurately is essential for a functional network setup. The devices connected include:

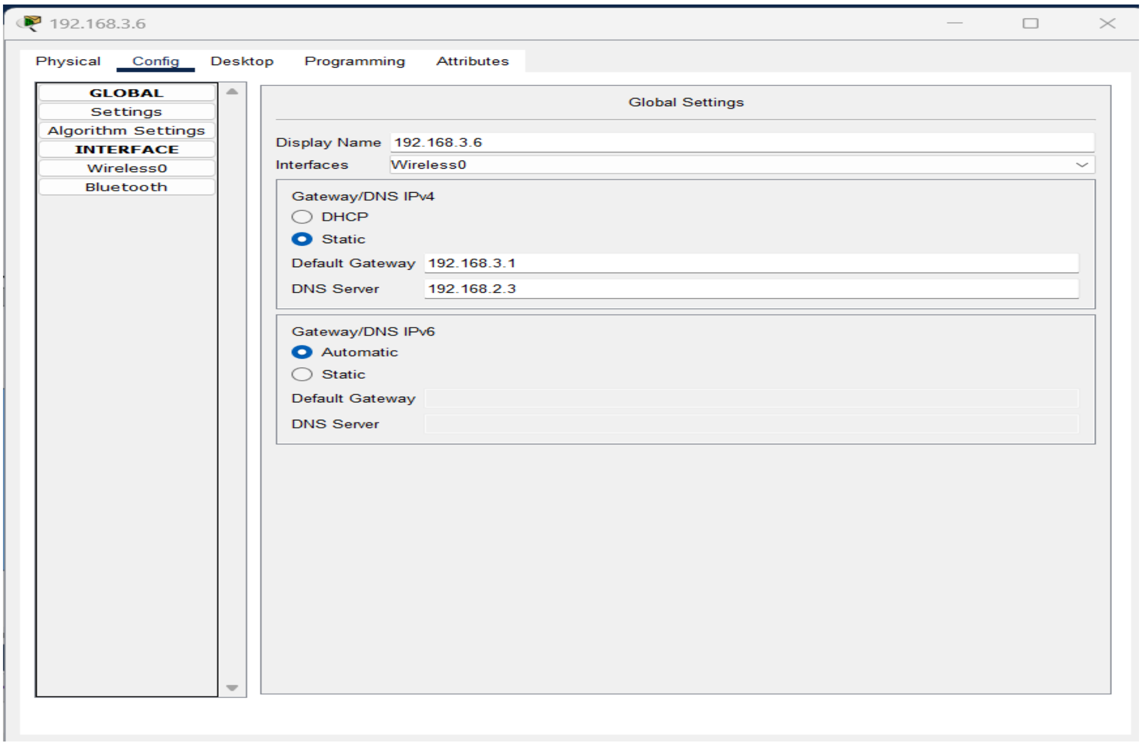
End Devices: Computers, printers, and IP phones in various departments.

Network Devices: Switches and routers that form the backbone of the network.

Servers: Centralized resources like web servers, FTP servers, DNS servers and email servers.



The WMP300N module provides one 2.4GHz wireless interface suitable for connection to wireless networks.
The module supports protocols that use Ethernet for LAN access.



Global Settings

Display Name 192.168.3.6

Interfaces Wireless0

Gateway/DNS IPv4

○ DHCP

● Static

Default Gateway 192.168.3.1

DNS Server 192.168.2.3

Gateway/DNS IPv6

● Automatic

○ Static

Default Gateway

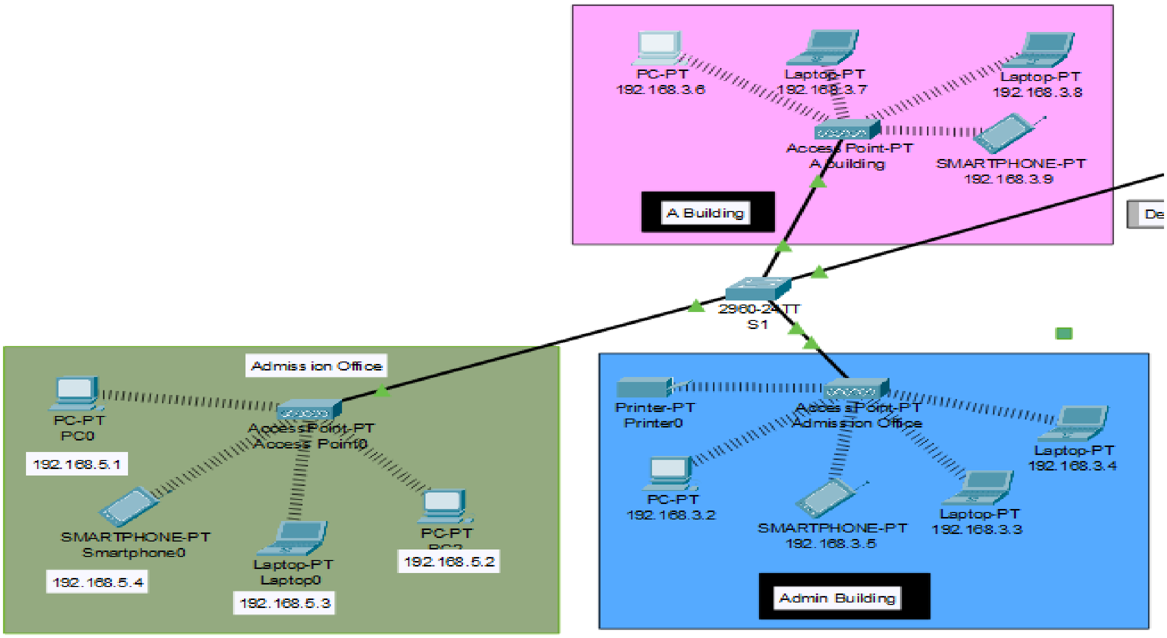
DNS Server

3. Creating VLANs

Virtual Local Area Networks (VLANs) are critical for segmenting the network to improve performance and security. The following VLANs were created:

VLAN 02: Admission.

VLAN 03:Admin Building.

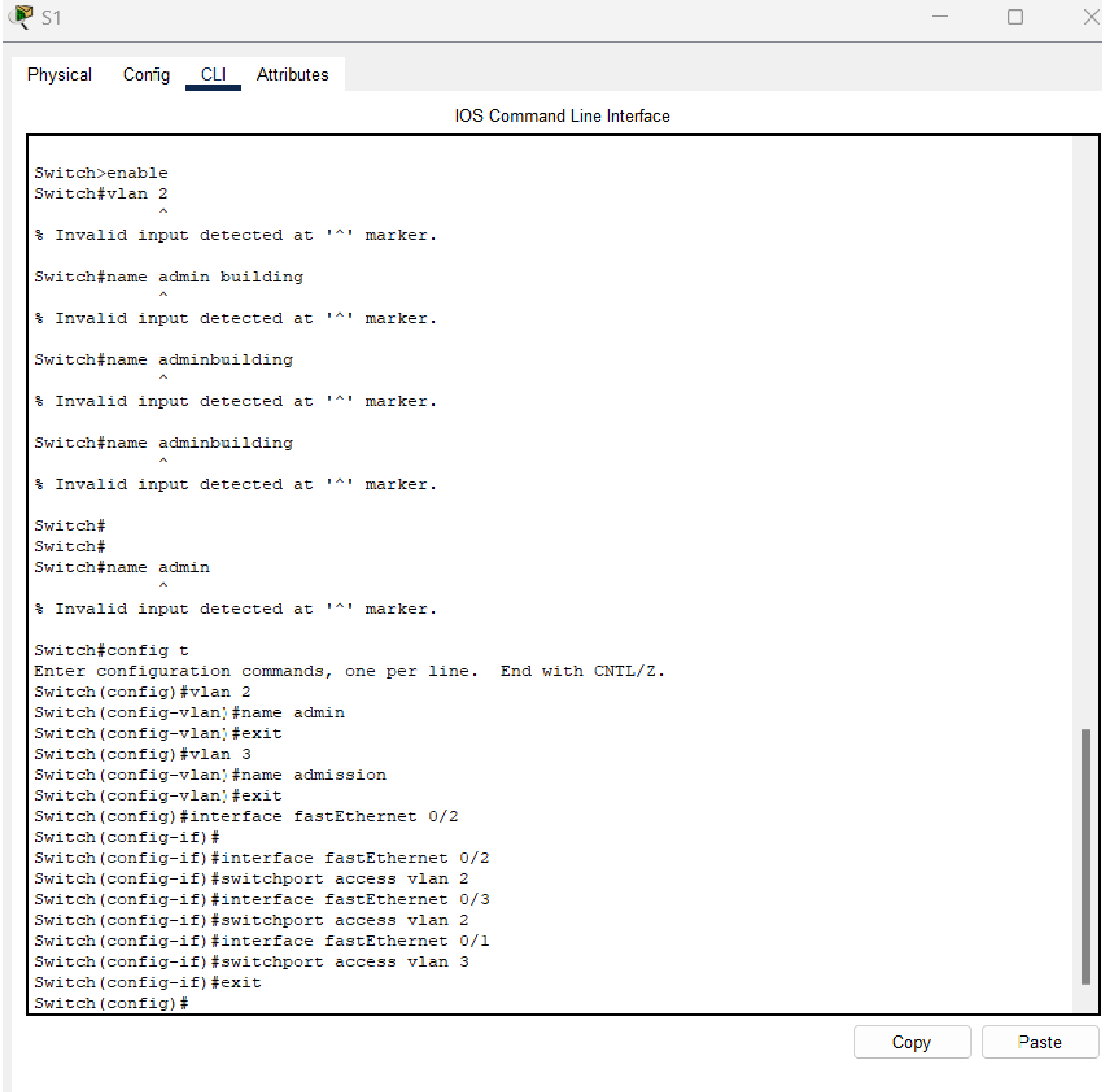


4. Configuring VLANs

Each VLAN was configured with specific parameters to ensure proper segregation and efficient communication:

VLAN Assignment: Devices were assigned to the respective VLANs based on their role.

Inter-VLAN Routing: Configured on the router to enable communication between different VLANs while maintaining isolation.



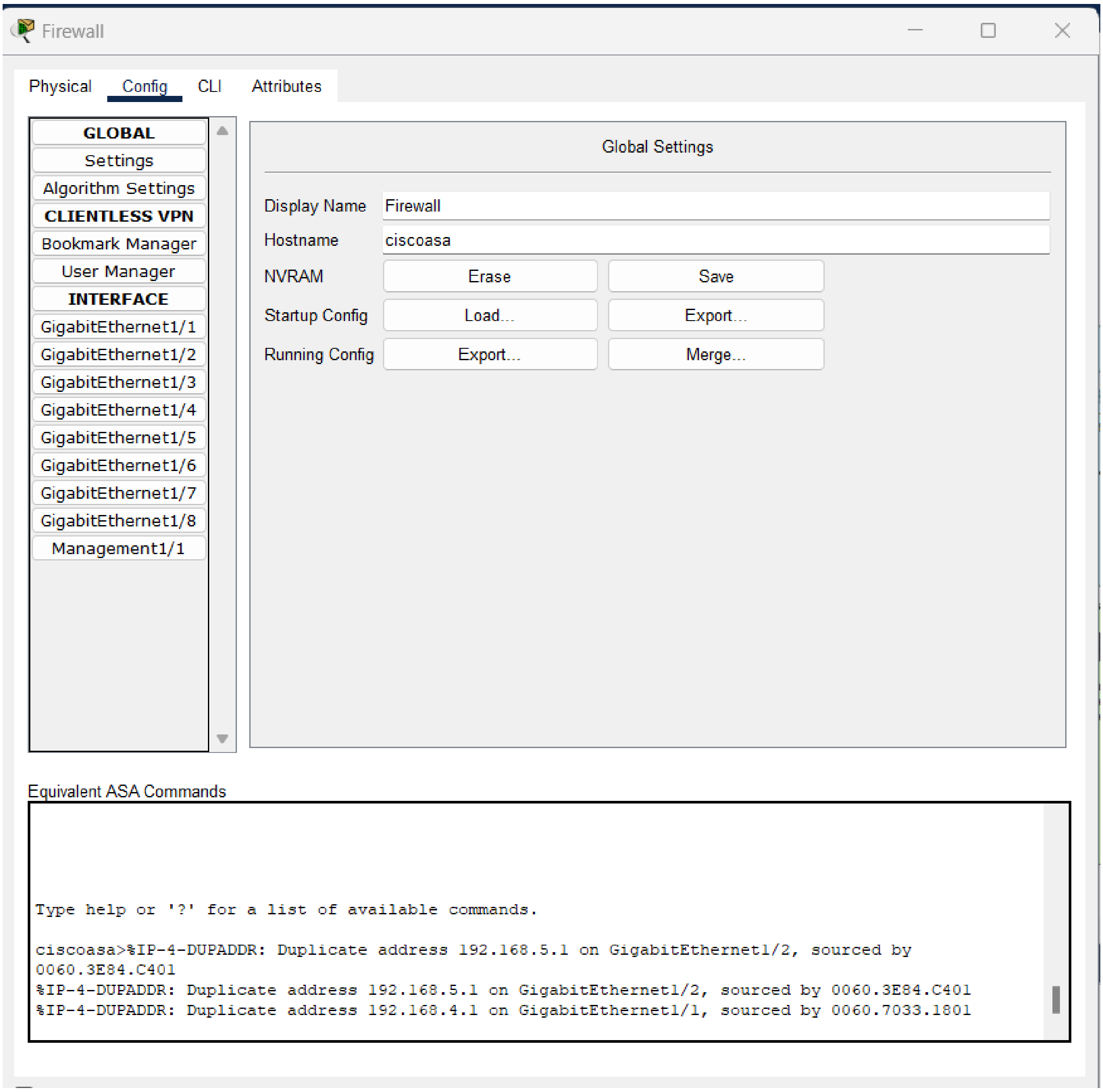
```
Switch>enable
Switch#vlan 2
            ^
% Invalid input detected at '^' marker.

Switch#name admin building
            ^
% Invalid input detected at '^' marker.

Switch#name adminbuilding
            ^
% Invalid input detected at '^' marker.

Switch#name adminbuilding
            ^
% Invalid input detected at '^' marker.

Switch#
Switch#
Switch#name admin
            ^
% Invalid input detected at '^' marker.

Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name admin
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name admission
Switch(config-vlan)#exit
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#
Switch(config-if)#interface fastEthernet 0/2
Switch(config-if)#switchport access vlan 2
Switch(config-if)#interface fastEthernet 0/3
Switch(config-if)#switchport access vlan 2
Switch(config-if)#interface fastEthernet 0/1
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#
```

5. Security (Adding Firewall)

Security is paramount in a university network to protect sensitive data and ensure safe internet usage:

Firewall Implementation: A firewall was configured to monitor and control incoming and outgoing network traffic based on predetermined security rules.

Access Control Lists (ACLs): Used to permit or deny traffic based on IP addresses and protocols, enhancing network security.



Display Name: Firewall

Hostname: ciscoasa

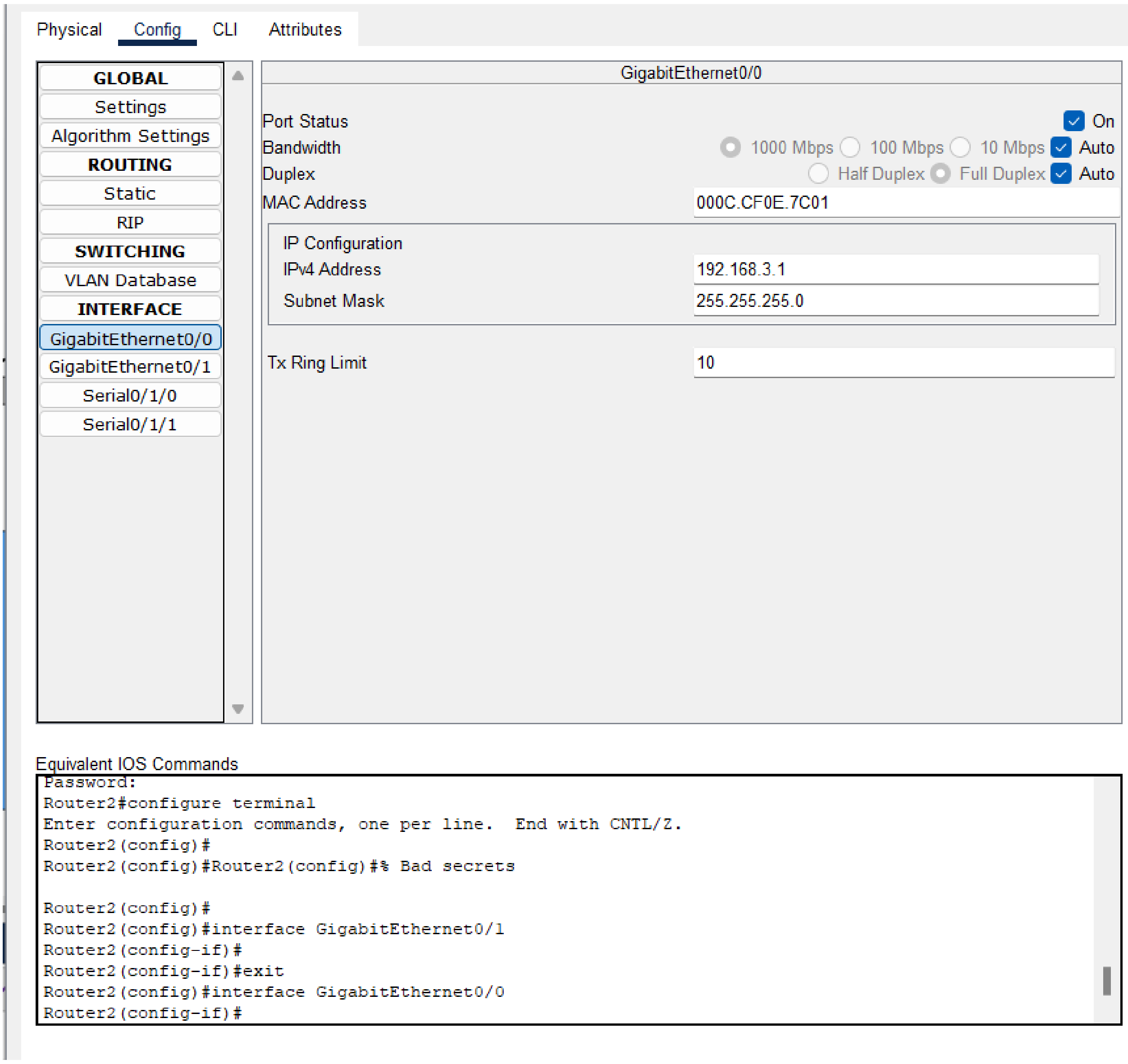
```
Type help or '?' for a list of available commands.

ciscoasa>%IP-4-DUPADDR: Duplicate address 192.168.5.1 on GigabitEthernet1/2, sourced by
0060.3E84.C401
%IP-4-DUPADDR: Duplicate address 192.168.5.1 on GigabitEthernet1/2, sourced by 0060.3E84.C401
%IP-4-DUPADDR: Duplicate address 192.168.4.1 on GigabitEthernet1/1, sourced by 0060.7033.1801
```

6. Gateway Setup

The gateway setup involved configuring routers to ensure proper routing of data packets between the internal network and the external internet:

Default Gateway Configuration: Set up on each VLAN to direct traffic to the appropriate router interface.

NAT (Network Address Translation): Configured to enable multiple devices on the internal network to access external networks using a single public IP address.



GigabitEthernet0/0

Port Status ☑ On

Bandwidth ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 000C.CF0E.7C01

IP Configuration

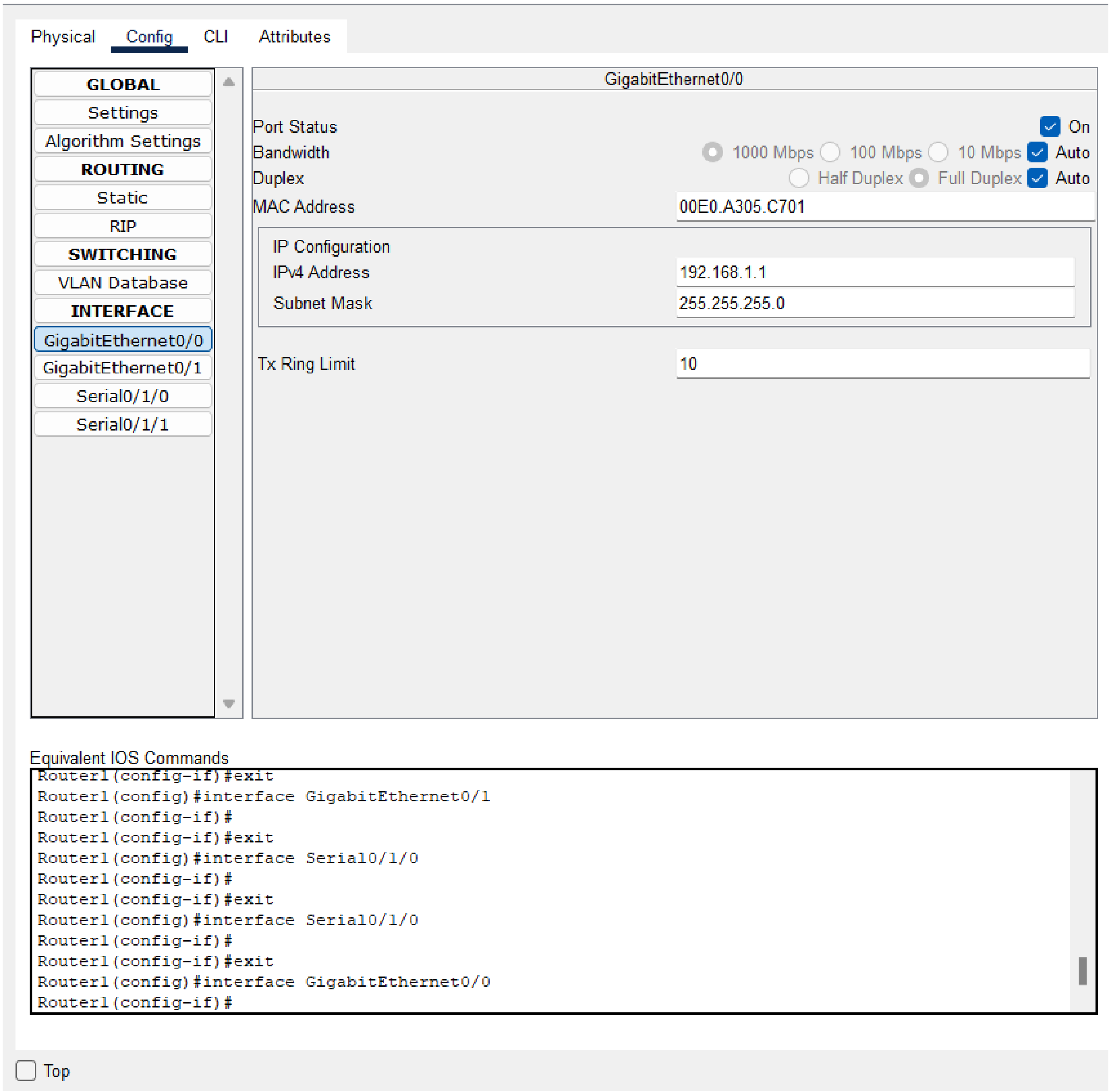
IPv4 Address 192.168.3.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Password:
Router2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#
Router2(config)#Router2(config)#% Bad secrets

Router2(config)#
Router2(config)#interface GigabitEthernet0/1
Router2(config-if)#
Router2(config-if)#exit
Router2(config)#interface GigabitEthernet0/0
Router2(config-if)#
```



GigabitEthernet0/0

Port Status ☑ On

Bandwidth ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 00E0.A305.C701

IP Configuration

IPv4 Address 192.168.1.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router1(config-if)#exit
Router1(config)#interface GigabitEthernet0/1
Router1(config-if)#
Router1(config-if)#exit
Router1(config)#interface Serial0/1/0
Router1(config-if)#
Router1(config-if)#exit
Router1(config)#interface Serial0/1/0
Router1(config-if)#
Router1(config-if)#exit
Router1(config)#interface GigabitEthernet0/0
Router1(config-if)#
```

□ Top

Mobile Phones and Laptops:

Connected to the network via wireless access points.

Configured IP addresses and subnet masks to ensure proper connectivity.

Computers:

Connected to the network via wired connections to switches and hubs.

Assigned IP addresses within the appropriate subnets.

Access Points:

Configured to provide wireless access to mobile devices and laptops.

Ensured proper integration with the wired network.

7. IP Addressing and Subnetting

IP addressing and subnetting are foundational tasks in network design. IP addresses ensure that each device on the network can be uniquely identified and communicated with, while subnetting divides the network into smaller, more manageable segments to enhance performance and security.

IP Addressing

For this project, the following IP addresses were used:

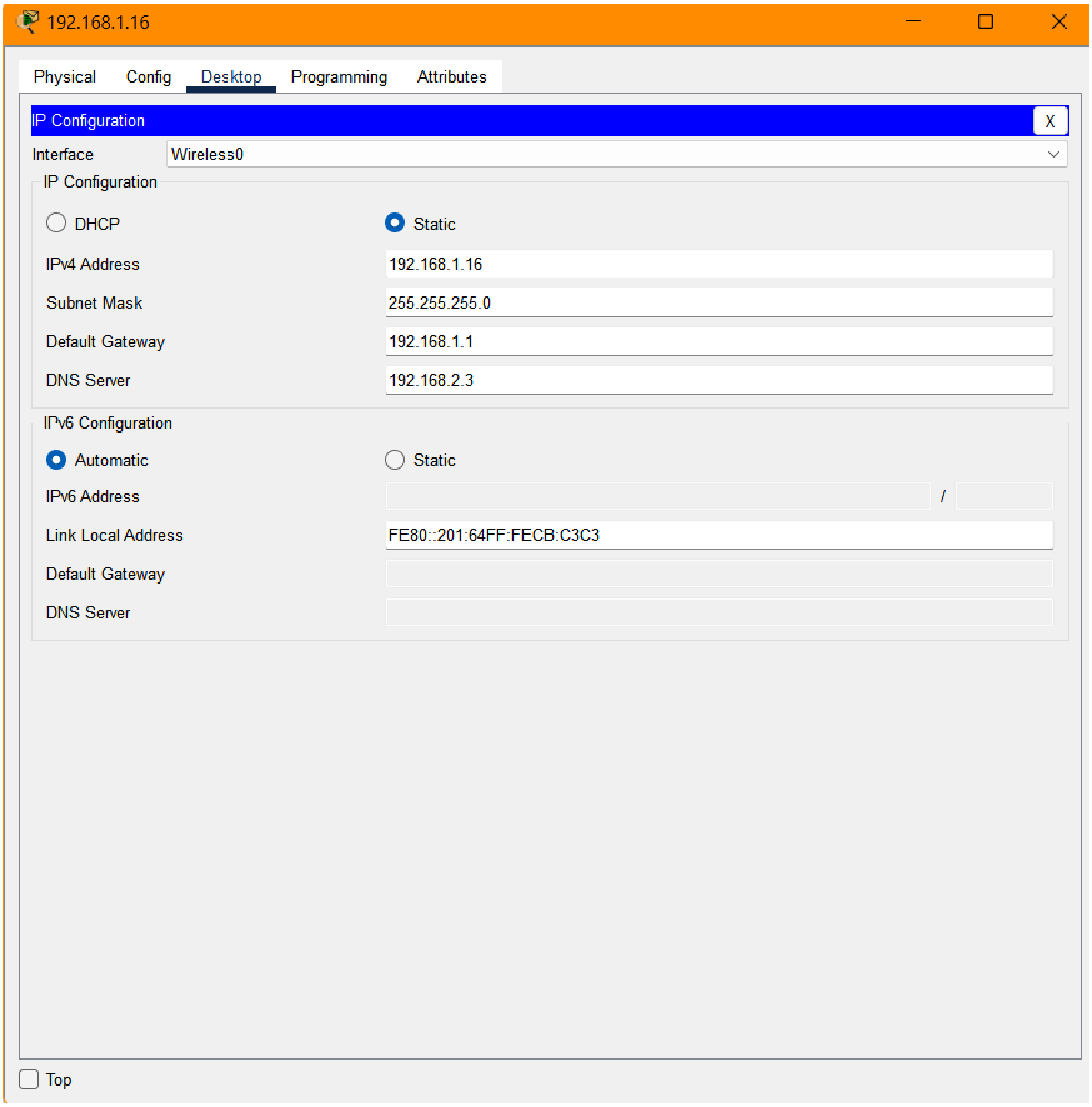
192.168.1.1

192.168.5.1

192.168.3.1

192.168.2.1

These addresses are part of the Class C IP range, which typically uses a subnet mask of 255.255.255.0. Each department within the university was assigned specific IP addresses within designated subnets to optimize traffic flow and improve network management.



Interface: Wireless0

IP Configuration

○ DHCP ● Static

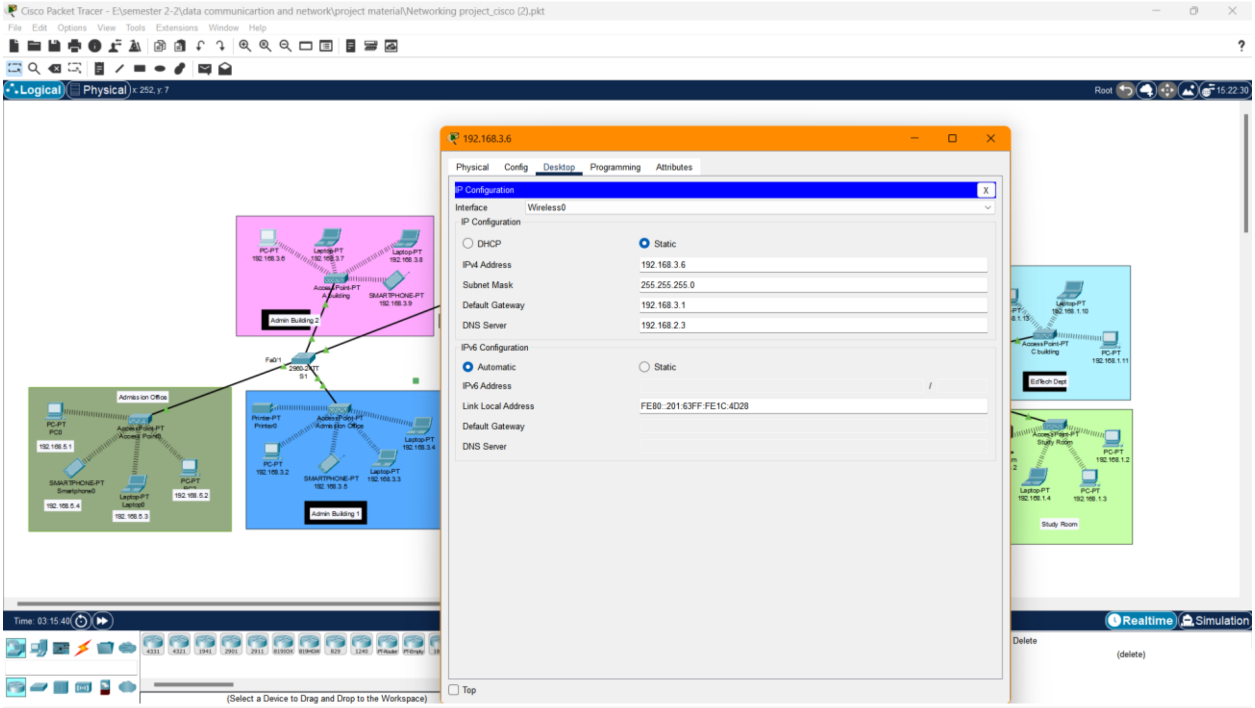
IPv4 Address	192.168.1.16
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	192.168.2.3

IPv6 Configuration

● Automatic ○ Static

IPv6 Address	/
Link Local Address	FE80::201:64FF:FECB:C3C3
Default Gateway	
DNS Server	

□ Top


192.168.3.6

IP Configuration

Interface: Wireless0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.3.6

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.3.1

DNS Server: 192.168.2.3

IPv6 Configuration

● Automatic ○ Static

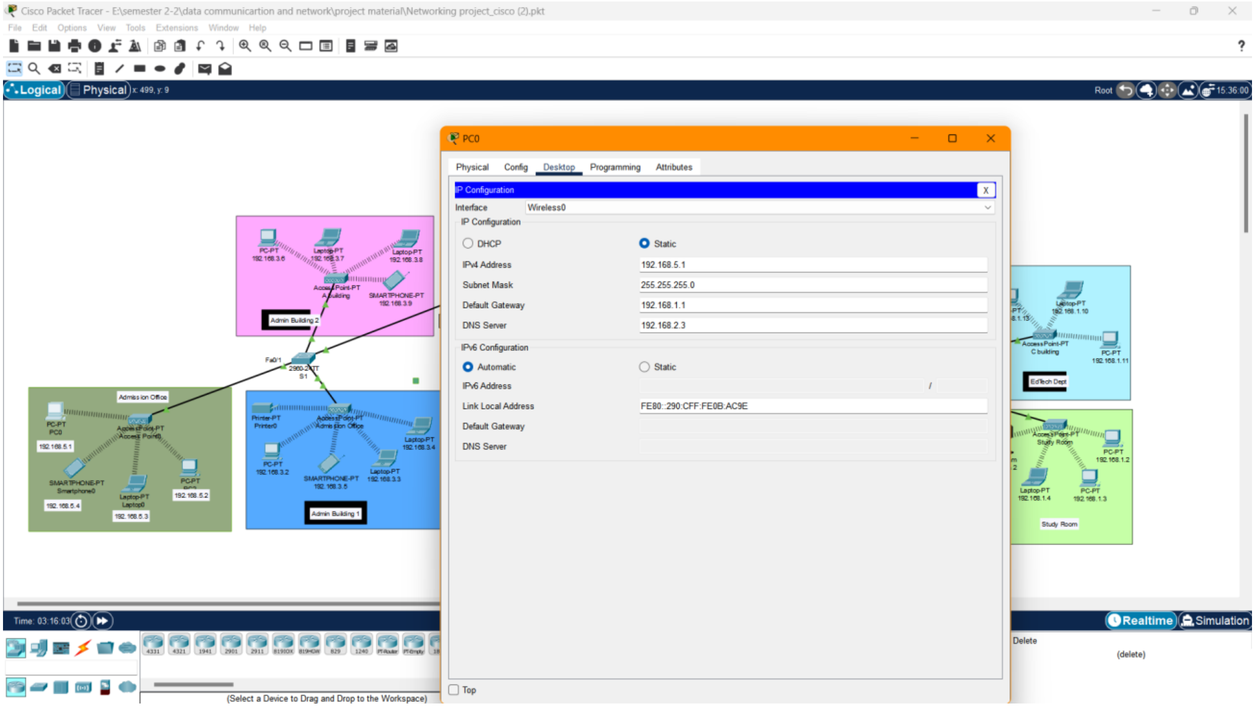
IPv6 Address:

Link Local Address: FE80::201:63FF:FE1C:4D28

Default Gateway:

DNS Server:

Cisco Packet Tracer - E:\semester 2-2\data communicartion and network\project material\Networking project_cisco (2).pkt
Logical
Physical
Physical
Config
Desktop
Programming
Attributes
Admin Building 2
Admission Office
Admin Building 1
EdTech Dept
Study Room
Realtime
Simulation
(Select a Device to Drag and Drop to the Workspace)


PC0

IP Configuration

Interface: Wireless0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.5.1

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 192.168.2.3

IPv6 Configuration

● Automatic ○ Static

IPv6 Address:

Link Local Address: FE80::290:CFF:FE0B:AC9E

Default Gateway:

DNS Server:

Cisco Packet Tracer - E:\semester 2-2\data communicartion and network\project material\Networking project_cisco (2).pkt
Logical
Physical
Physical
Config
Desktop
Programming
Attributes
Admin Building 2
Admission Office
Admin Building 1
EdTech Dept
Study Room
Realtime
Simulation
(Select a Device to Drag and Drop to the Workspace)

Subnetting

Each IP address was assigned to a separate subnet, and specific IP ranges were allocated to different departments and areas within the university:

Admin Building 1:

Subnet Address: 192.168.3.0/24

Assigned IPs: 192.168.3.6, 192.168.3.7, 192.168.3.8, 192.168.3.9

Admin Building 2:

Subnet Address: 192.168.3.0/24

Assigned IPs: 192.168.3.2, 192.168.3.3, 192.168.3.4, 192.168.3.5

IRE Department:

Subnet Address: 192.168.1.0/24

Assigned IPs: 192.168.1.14, 192.168.1.15, 192.168.1.16, 192.168.1.17

Edutech Department:

Subnet Address: 192.168.1.0/24

Assigned IPs: 192.168.1.10, 192.168.1.11, 192.168.1.13

Study Room:

Subnet Address: 192.168.1.0/24

Assigned IPs: 192.168.1.2, 192.168.1.3, 192.168.1.4

Library:

Subnet Address: 192.168.1.0/24

Assigned IPs: 192.168.1.5, 192.168.1.6

IT Room:

Subnet Address: 192.168.1.0/24

Assigned IPs: 192.168.1.7, 192.168.1.8, 192.168.1.9

Admission Office:

Subnet Address: 192.168.5.0/24

Assigned IPs: 192.168.5.1, 192.168.5.2, 192.168.5.3, 192.168.5.4

This ensures that each department and area has its own network segment, reducing broadcast traffic and enhancing security.

8. Network Monitoring

Network monitoring involves observing network operations to ensure optimal performance and identify potential issues. Effective monitoring helps maintain network health and supports proactive troubleshooting.

DHCP Configuration:

To automatically assign IP addresses to devices within each subnet.

To streamline network management by centralizing IP address allocation.

DHCP Server Setup:

Designate a server in the Server Room (192.168.2.0/24) to act as the DHCP server.

Define IP address ranges for each subnet:

Admin Building 1 & 2: 192.168.3.10 - 192.168.3.50

Admission Office: 192.168.5.10 - 192.168.5.50

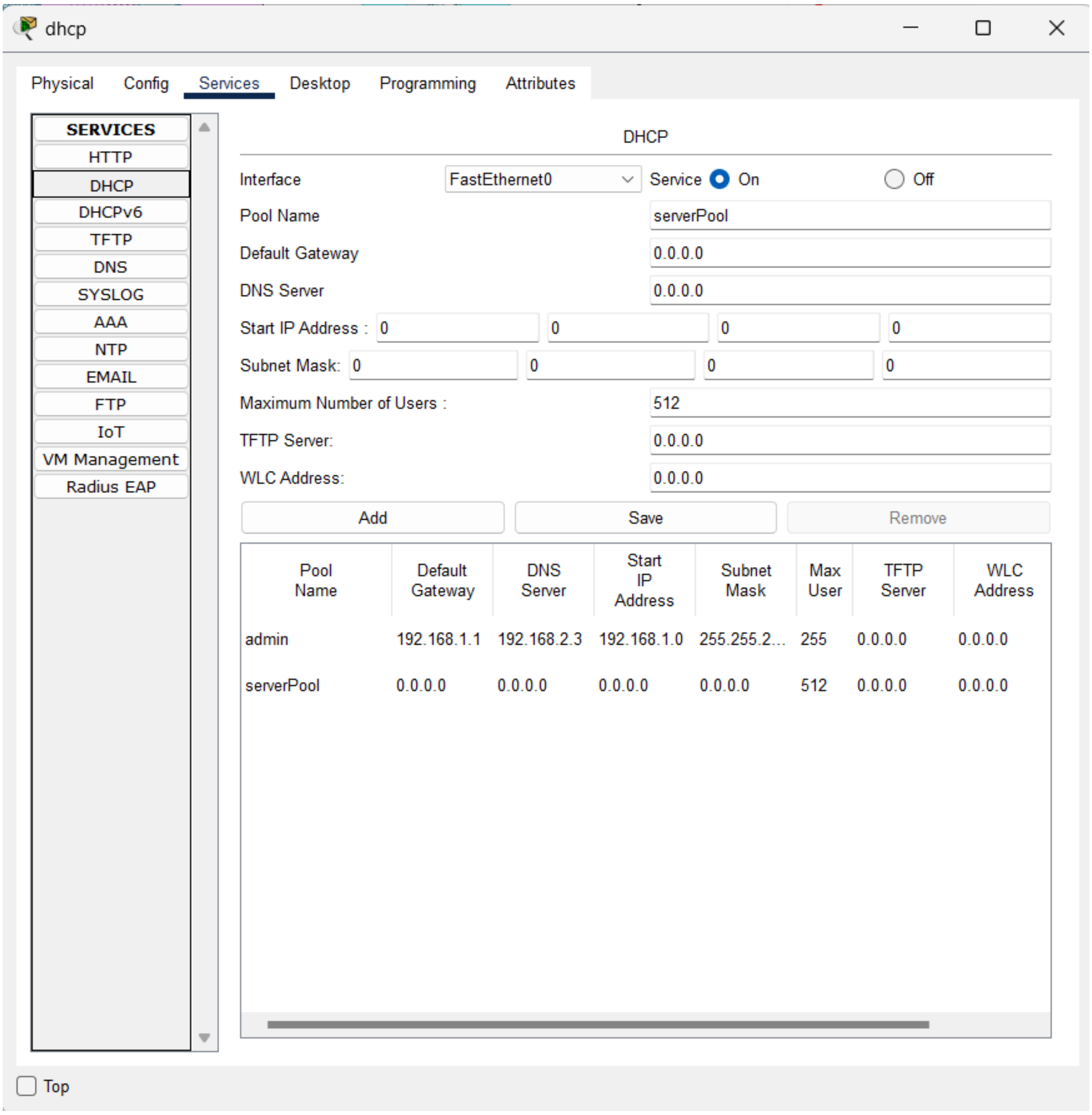
IRE Dept: 192.168.1.110 - 192.168.1.150

EdTech Dept: 192.168.1.10 - 192.168.1.50

Library: 192.168.2.10 - 192.168.2.50

Study Room: 192.168.1.210 - 192.168.1.250

IT Room: 192.168.1.60 - 192.168.1.100



DHCP

Interface: FastEthernet0 Service ● On ○ Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address : 0 0 0 0

Subnet Mask: 0 0 0 0

Maximum Number of Users : 512

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
admin	192.168.1.1	192.168.2.3	192.168.1.0	255.255.2...	255	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	512	0.0.0.0	0.0.0.0

DHCP Options:

Set the default gateway for each subnet:

Admin Building 1 : 192.168.3.1

Admission Office: 192.168.5.1

IRE Dept: 192.168.1.1

EdTech Dept: 192.168.1.1

Library: 192.168.2.1

Study Room: 192.168.1.1

IT Room: 192.168.1.1

9. Host Device Configuration:

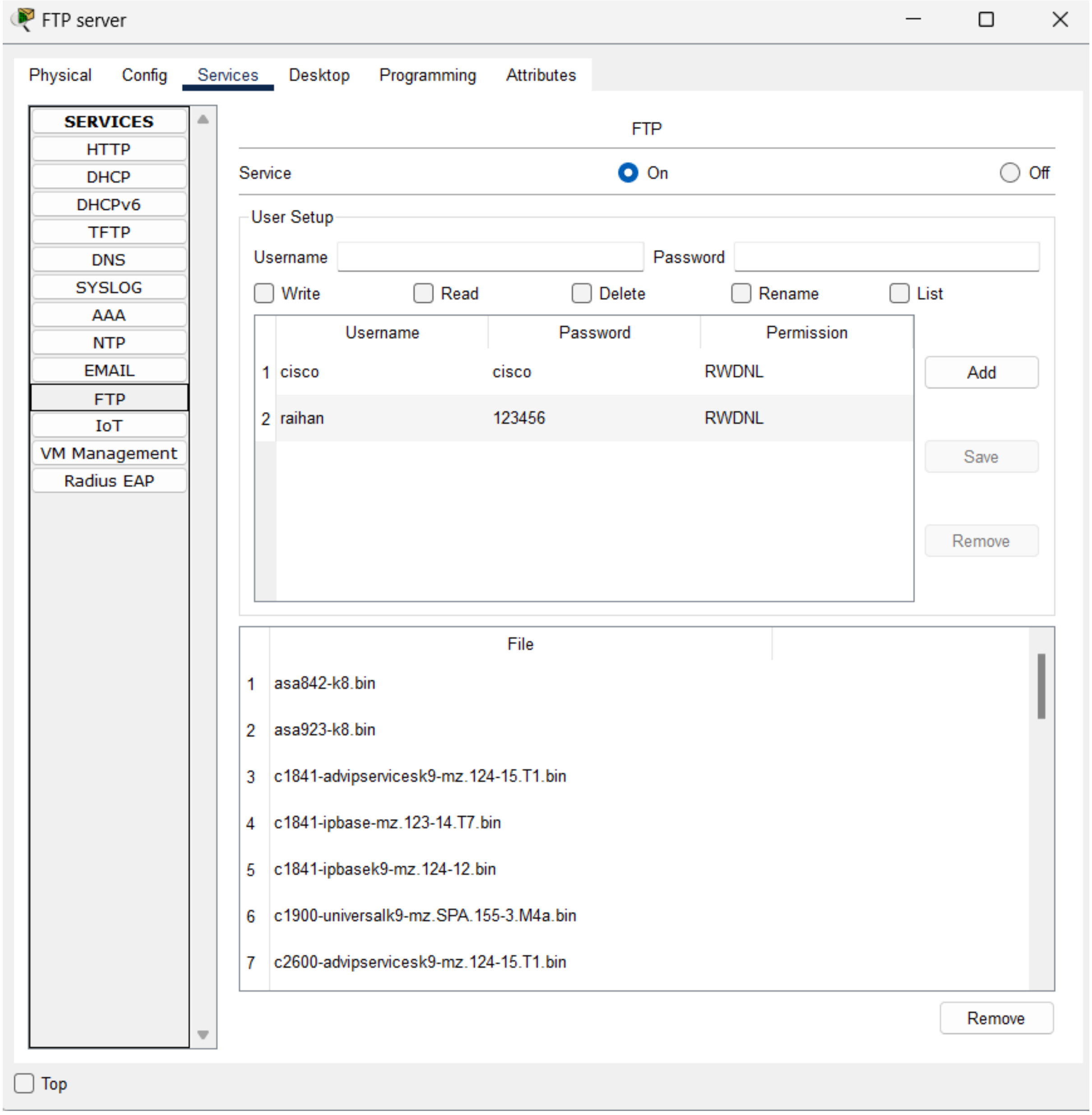
To configure IP addresses, subnet masks, and default gateways on host devices.

Example for FTP Server:

IP Address: 192.168.2.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1



Service ● On ○ Off

Username Password

□ Write □ Read □ Delete □ Rename □ List

	Username	Password	Permission
1	cisco	cisco	RWDNL
2	raihan	123456	RWDNL

	File
1	asa842-k8.bin
2	asa923-k8.bin
3	c1841-advipservicesk9-mz.124-15.T1.bin
4	c1841-ipbase-mz.123-14.T7.bin
5	c1841-ipbasek9-mz.124-12.bin
6	c1900-universalk9-mz.SPA.155-3.M4a.bin
7	c2600-advipservicesk9-mz.124-15.T1.bin

DHCP Configuration for Client Devices:

Ensure that all PCs, laptops, and smartphones are set to obtain IP addresses automatically from the DHCP server.

10. Network Protocols:

To ensure seamless communication between devices using standard network protocols.

TCP/IP: Foundation protocol suite for communication across the network.

DHCP: Dynamic IP address assignment.

DNS: Domain Name System for resolving domain names to IP addresses.

HTTP/HTTPS: Web traffic management for internal and external communication.

FTP: File Transfer Protocol for file sharing and storage.

11. Configuring ASA Firewall:

To enhance network security by controlling incoming and outgoing traffic.

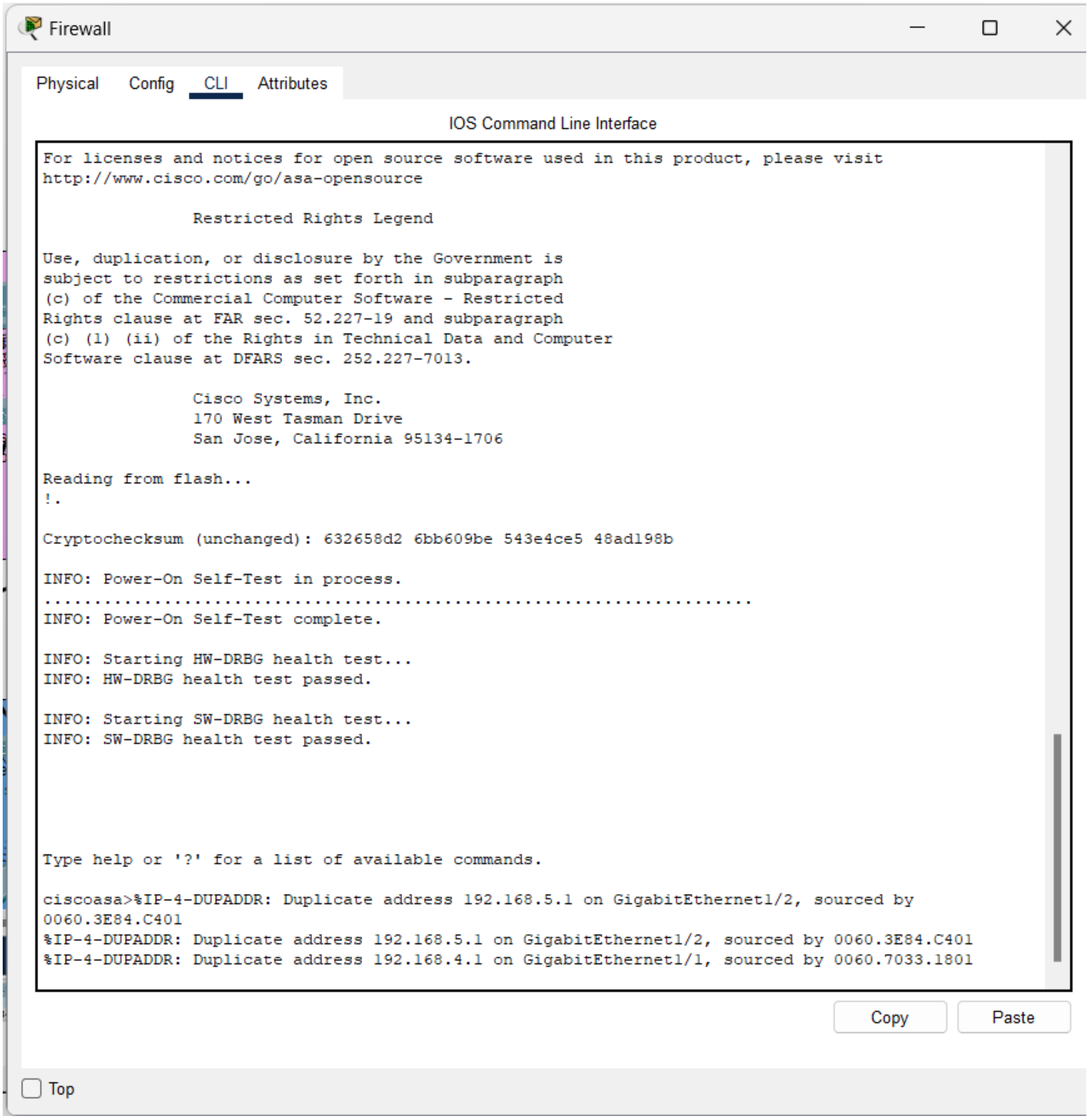
To prevent unauthorized access to sensitive resources.

Assign IP addresses to the ASA interfaces.

Define security levels (e.g., inside, outside, DMZ).

Access Control Lists (ACLs):

Create ACLs to permit or deny traffic based on source/destination IP addresses and ports.



```
For licenses and notices for open source software used in this product, please visit
http://www.cisco.com/go/asa-opensource

               Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

               Cisco Systems, Inc.
               170 West Tasman Drive
               San Jose, California 95134-1706

Reading from flash...
!.

Cryptochecksum (unchanged): 632658d2 6bb609be 543e4ce5 48ad198b

INFO: Power-On Self-Test in process.
.......................................................................
INFO: Power-On Self-Test complete.

INFO: Starting HW-DRBG health test...
INFO: HW-DRBG health test passed.

INFO: Starting SW-DRBG health test...
INFO: SW-DRBG health test passed.




Type help or '?' for a list of available commands.

ciscoasa>%IP-4-DUPADDR: Duplicate address 192.168.5.1 on GigabitEthernet1/2, sourced by
0060.3E84.C401
%IP-4-DUPADDR: Duplicate address 192.168.5.1 on GigabitEthernet1/2, sourced by 0060.3E84.C401
%IP-4-DUPADDR: Duplicate address 192.168.4.1 on GigabitEthernet1/1, sourced by 0060.7033.1801
```

12. NAT Configuration:

Configure Network Address Translation (NAT) to allow internal devices to access external networks securely.

Assign IP addresses to interfaces

interface GigabitEthernet0/0

nameif outside

security-level 0

ip address 198.51.100.1 255.255.255.0

```
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface

access-list OUTSIDE_IN extended permit tcp any object obj_any eq 80
access-list OUTSIDE_IN extended permit tcp any object obj_any eq 443
```

Conclusion:

The University Network System project was successfully implemented using Cisco Packet Tracer. The network design ensures efficient connectivity, robust security, and seamless communication across the university. The tasks undertaken, from cable selection to gateway setup, were crucial in achieving the project's objectives. This report highlights the comprehensive approach and detailed work carried out to establish a reliable and secure network infrastructure for the university.