Design and Implementation of a Full-Fledged Network for Apex University

Md Sifat Ullah Sheikh
Department of Computer Science and Engineering
East West University, Aftab Nagar, Dhaka, Bangladesh
Email: 2022-1-60-029@std.ewubd.edu

***Abstract*—This report presents the design and implementation of a complex network infrastructure for Apex University, consisting of eight campuses, each with its subnet. The network incorporates multiple Local Area Networks (LANs), dynamic IP assignment via DHCP, DNS services, and dynamic routing using the OSPF protocol. The network was implemented using Cisco Packet Tracer to ensure scalability, reliability, and efficient resource management. This paper discusses the design criteria, implementation details, challenges encountered, and potential future improvements, as well as security measures, network optimization, and redundancy planning for high availability.**

***Index Terms*—Network Design, OSPF, DHCP, DNS, Subnetting, Cisco Packet Tracer, University Network, Scalability, Security, Redundancy, Optimization**

I. Introduction

Apex University operates a large-scale network infrastructure to support its academic, administrative, and business processes. The network spans eight campuses, each requiring seamless connectivity for both wired and wireless devices. This network must support services such as web hosting, DNS, DHCP, and dynamic routing.

The primary objectives of this project are:

- Design a network that reflects the university's structure and facilities.
- Implement a single DNS server for web hosting and a DHCP server for automatic IP assignment.
- Configure dynamic routing using the OSPF protocol.
- Ensure connectivity between all hosts across the eight campuses.
- Maintain scalability, redundancy, and security for future network expansion.
- Implement measures for network optimization and efficient utilization of bandwidth.

II. Background and Problem Statement

Modern universities rely on robust network infrastructures to support a wide range of services. The Apex University network must accommodate numerous wireless and wired devices across multiple campuses while supporting critical services such as admissions, advising, and library management.

Key challenges include:

- Ensuring seamless connectivity across multiple subnets.
- Automating IP address assignment using DHCP.
- Implementing dynamic routing to efficiently manage traffic.
- Providing wireless access alongside wired connections.
- Ensuring network security and minimizing vulnerabilities.
- Implementing redundancy mechanisms to ensure high availability.
- Optimizing network performance to prevent congestion.

This project addresses these challenges using Cisco Packet Tracer to create a scalable, secure, and efficient network model.

III. Network Design and Architecture

A. Design Criteria

The network design is based on the following criteria:

- **Scalability**: Support for future growth and additional subnetworks.
- **Reliability**: High availability and minimal downtime through redundancy.
- **Efficiency**: Optimal utilization of resources, including IP addresses and bandwidth.
- **Security**: Implement firewall policies, VLANs, and encrypted communication.
- **Optimization**: Load balancing and QoS implementation for enhanced performance.

B. Network Topology

The network topology consists of eight campuses interconnected using routers with serial links. Each campus has its Local Area Network (LAN) with a mix of wired and wireless hosts. The design includes the following components:

- **LANs**: Each campus has a mix of wired and wireless hosts.
- **Routers**: Eight routers manage each campus, forming a mesh topology.
- **Servers**: A central server room houses the DNS and DHCP servers.
- **IP Addressing**: A mix of Class A, B, and C addresses for efficient allocation.
- **Redundancy**: Backup connections to ensure fault tolerance.

IV. Routing Configuration for University Network Infrastructure

This section details the CLI configurations for each campus router in the university network infrastructure. The routers are

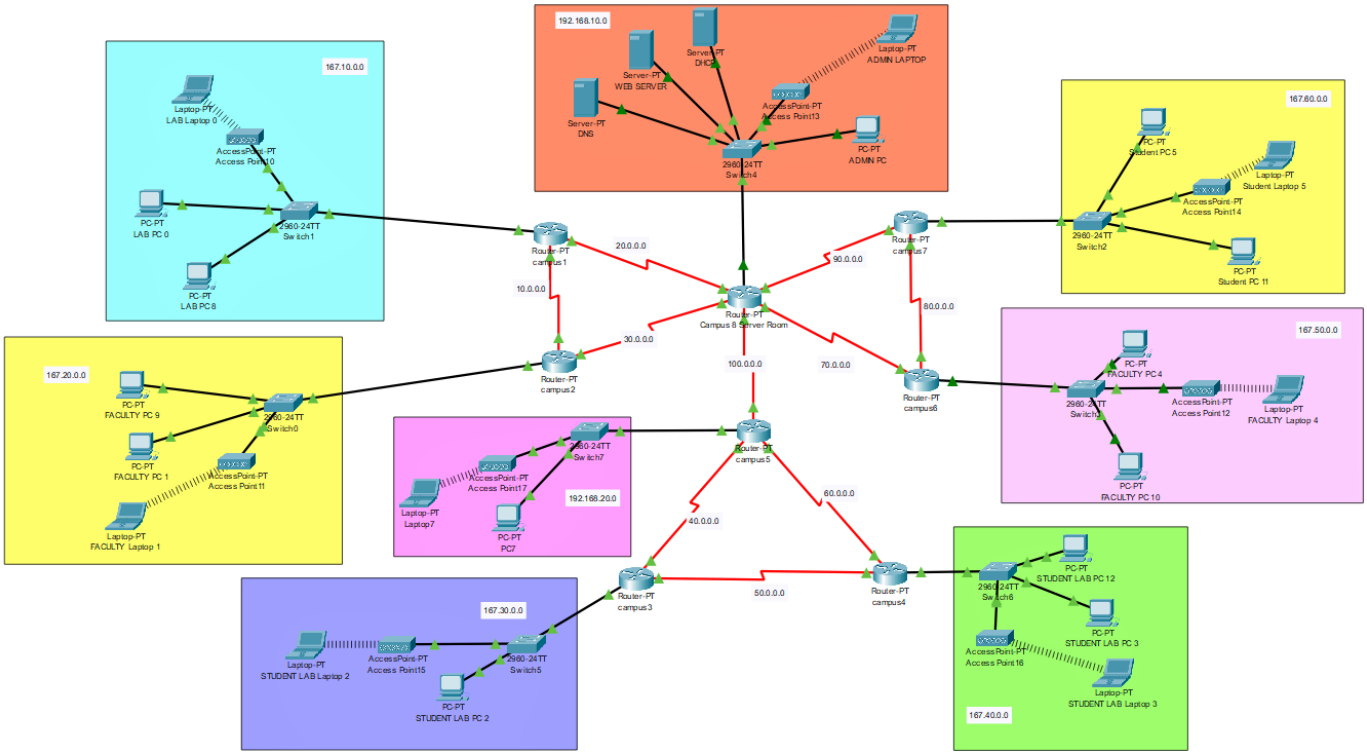

Fig. 1. Network Topology of Apex University

configured with OSPF routing protocol to ensure seamless connectivity among all campuses.

A. Router Configurations

1) Campus 1 Router Configuration:

```
enable
config
interface fa0/0
ip address 167.10.255.254 255.255.0.0
no shut
do wr
exit

interface se2/0
ip address 20.0.0.1 255.0.0.0
clock rate 64000
no shut
do wr
exit

interface se3/0
ip address 10.0.0.1 255.0.0.0
clock rate 64000
no shut
do wr
exit

router ospf 1
network 167.10.0.0 0.0.255.255 area 1
network 10.0.0.0 0.255.255.255 area 1
network 20.0.0.0 0.255.255.255 area 1
exit
```

2) Campus 2 Router Configuration:

```
enable
config
interface fa0/0
ip address 167.20.255.254 255.255.0.0
no shut
do wr
exit

interface se2/0
ip address 10.0.0.2 255.0.0.0
no shut
do wr
exit

interface se3/0
ip address 30.0.0.1 255.0.0.0
clock rate 64000
no shut
do wr
exit

router ospf 1
network 167.20.0.0 0.0.255.255 area 1
```

```
network 10.0.0.0 0.255.255.255 area 1
network 30.0.0.0 0.255.255.255 area 1
exit
```

3) Campus 3 Router Configuration:

```
enable
config
interface fa0/0
ip address 167.30.255.254 255.255.0.0
no shut
do wr
exit

interface se2/0
ip address 40.0.0.1 255.0.0.0
clock rate 64000
no shut
do wr
exit

interface se3/0
ip address 50.0.0.1 255.0.0.0
clock rate 64000
no shut
do wr
exit

router ospf 1
network 167.30.0.0 0.0.255.255 area 1
network 40.0.0.0 0.255.255.255 area 1
network 50.0.0.0 0.255.255.255 area 1
exit
```

4) Campus 4 Router Configuration:

```
enable
config
interface fa0/0
ip address 167.40.255.254 255.255.0.0
no shut
do wr
exit

interface se2/0
ip address 50.0.0.2 255.0.0.0
no shut
do wr
exit

interface se3/0
ip address 60.0.0.1 255.0.0.0
clock rate 64000
no shut
do wr
exit

router ospf 1
network 167.40.0.0 0.0.255.255 area 1
network 50.0.0.0 0.255.255.255 area 1
network 60.0.0.0 0.255.255.255 area 1
exit
```

5) Campus 5 Router Configuration:

```
enable
config
interface fa0/0
ip address 192.168.20.254 255.255.255.0
no shut
do wr
exit

interface se2/0
ip address 40.0.0.2 255.0.0.0
no shut
do wr
exit

interface se3/0
ip address 60.0.0.2 255.0.0.0
no shut
do wr
exit

interface se6/0
ip address 100.0.0.1 255.0.0.0
clock rate 64000
no shut
do wr
exit


router ospf 1
network 192.168.20.0 0.0.0.255 area 1
network 40.0.0.0 0.255.255.255 area 1
network 60.0.0.0 0.255.255.255 area 1
network 100.0.0.0 0.255.255.255 area 1
exit
```

6) Campus 6 Router Configuration:

```
enable
config
interface fa0/0
ip address 167.50.255.254 255.255.0.0
no shut
do wr
exit

interface se2/0
ip address 80.0.0.1 255.0.0.0
clock rate 64000
no shut
do wr
```

```
exit

interface se3/0
ip address 70.0.0.1 255.0.0.0
clock rate 64000
no shut
do wr
exit


router ospf 1
network 167.50.0.0 0.0.255.255 area 1
network 70.0.0.0 0.255.255.255 area 1
network 80.0.0.0 0.255.255.255 area 1
exit
```

7) Campus 7 Router Configuration:

```
enable
config
interface fa0/0
ip address 167.60.255.254 255.255.0.0
no shut
do wr
exit

interface se2/0
ip address 80.0.0.2 255.0.0.0
no shut
do wr
exit

interface se3/0
ip address 90.0.0.1 255.0.0.0
clock rate 64000
no shut
do wr
exit


router ospf 1
network 167.60.0.0 0.0.255.255 area 1
network 80.0.0.0 0.255.255.255 area 1
network 90.0.0.0 0.255.255.255 area 1
exit
```

8) Campus Router Configuration:

```
enable
config
interface fa0/0
ip address 192.168.10.254 255.255.255.0
no shut
do wr
exit

interface se2/0
ip address 20.0.0.2 255.0.0.0
no shut
do wr
exit

interface se3/0
ip address 30.0.0.2 255.0.0.0
no shut
do wr
exit

interface se6/0
ip address 100.0.0.2 255.0.0.0
no shut
do wr
exit

interface se7/0
ip address 70.0.0.2 255.255.0.0
no shut
do wr
exit

interface se8/0
ip address 90.0.0.2 255.255.0.0
no shut
do wr
exit



router ospf 1
network 192.168.10.0 0.0.0.255 area 1
network 20.0.0.0 0.255.255.255 area 1
network 30.0.0.0 0.255.255.255 area 1
network 70.0.0.0 0.255.255.255 area 1
network 90.0.0.0 0.255.255.255 area 1
network 100.0.0.0 0.255.255.255 area 1
exit
```

9) DHCP Helper Configuration: To establish the connection between the server and all other networks, an IP helper address is used, as the DHCP server is remote. The configuration is as follows:

```
interface fa0/0
ip helper-address 192.168.10.200
exit
```

This configuration ensures that DHCP requests from different subnets can be forwarded to the centralized DHCP server for IP address assignment.

B. IP Addressing and OSPF Configuration

The network configuration for each campus, including IP addressing, subnetting, and OSPF routing, is detailed in Table 1.

TABLE I
IP ADDRESS, IP CLASS, AND OSPF CONFIGURATION FOR APEX UNIVERSITY CAMPUSES

Campus	Interface	IP Address	Subnet Mask	IP Class	Connected To	OSPF Network
Campus 1	Fa0/0	167.10.255.254	255.255.0.0	Class B	Internal LAN	167.10.0.0/16
	Se2/0	20.0.0.1	255.0.0.0	Class A	Campus 8	20.0.0.0/8
	Se3/0	10.0.0.1	255.0.0.0	Class A	Campus 2	10.0.0.0/8
Campus 2	Fa0/0	167.20.255.254	255.255.0.0	Class B	Internal LAN	167.20.0.0/16
	Se2/0	10.0.0.2	255.0.0.0	Class A	Campus 1	10.0.0.0/8
	Se3/0	30.0.0.1	255.0.0.0	Class A	Campus 8	30.0.0.0/8
Campus 3	Fa0/0	167.30.255.254	255.255.0.0	Class B	Internal LAN	167.30.0.0/16
	Se2/0	40.0.0.1	255.0.0.0	Class A	Campus 5	40.0.0.0/8
	Se3/0	50.0.0.1	255.0.0.0	Class A	Campus 4	50.0.0.0/8
Campus 4	Fa0/0	167.40.255.254	255.255.0.0	Class B	Internal LAN	167.40.0.0/16
	Se2/0	50.0.0.2	255.0.0.0	Class A	Campus 3	50.0.0.0/8
	Se3/0	60.0.0.1	255.0.0.0	Class A	Campus 5	60.0.0.0/8
Campus 5	Fa0/0	192.168.20.254	255.255.255.0	Class C	Internal LAN	192.168.20.0/24
	Se2/0	40.0.0.2	255.0.0.0	Class A	Campus 3	40.0.0.0/8
	Se3/0	60.0.0.2	255.0.0.0	Class A	Campus 4	60.0.0.0/8
	Se6/0	100.0.0.1	255.0.0.0	Class A	Campus 8	100.0.0.0/8
Campus 6	Fa0/0	167.50.255.254	255.255.0.0	Class B	Internal LAN	167.50.0.0/16
	Se2/0	80.0.0.1	255.0.0.0	Class A	Campus 7	80.0.0.0/8
	Se3/0	70.0.0.1	255.0.0.0	Class A	Campus 8	70.0.0.0/8
Campus 7	Fa0/0	167.60.255.254	255.255.0.0	Class B	Internal LAN	167.60.0.0/16
	Se2/0	80.0.0.2	255.0.0.0	Class A	Campus 6	80.0.0.0/8
	Se3/0	90.0.0.1	255.0.0.0	Class A	Campus 8	90.0.0.0/8
Campus 8 (Server)	Fa0/0	192.168.10.254	255.255.255.0	Class C	Internal LAN	192.168.10.0/24
	Se2/0	20.0.0.2	255.0.0.0	Class A	Campus 1	20.0.0.0/8
	Se3/0	30.0.0.2	255.0.0.0	Class A	Campus 2	30.0.0.0/8
	Se6/0	100.0.0.2	255.0.0.0	Class A	Campus 5	100.0.0.0/8
	Se7/0	70.0.0.2	255.255.0.0	Class A	Campus 6	70.0.0.0/8
	Se8/0	90.0.0.2	255.255.0.0	Class A	Campus 7	90.0.0.0/8

C. Subnetting

Each campus network is divided into multiple subnets to ensure efficient IP address management and to minimize IP conflicts.

V. IMPLEMENTATION

A. Tools Used

The following tools were used for designing and implementing the network:

- **Cisco Packet Tracer Software (version 8.2.2)**: For network simulation and design [4] .
- **End Devices**: Laptop-Pt, Pc-Pt
- **Network Devices**: Switches (2960), Routers (Router-pt), Wireless Access Points
- **Server**: Server-PT for Web, DHCP, and DNS services.
- **Connectors**: Copper straight-through, Serial DCE.

B. Configuration Details

DHCP Server: Configured to assign IP addresses across all campuses using multiple scopes.

DNS Server: Configured to resolve http://www.apex.edu.bd to the university's Web server IP.

OSPF Routing: Configured to dynamically manage routing and optimize traffic flow.

Security Measures: VLAN segmentation, firewalls, and encrypted data communication were implemented to secure the network.

VI. RESULTS AND DISCUSSION

The implemented network model meets the project requirements:

- **Connectivity**: All hosts across campuses communicate seamlessly.

- **IP Assignment**: DHCP automatically assigns IP addresses.
- **Dynamic Routing**: OSPF manages inter-campus routing efficiently.
- **Scalability**: The design supports future expansions.
- **Security**: VLANs and firewalls improve security.
- **Redundancy**: Backup links ensure continuous network availability.

A. Server Configuration

Figure 2 shows the DNS server configuration, ensuring proper domain name resolution (e.g., www.apex.edu.bd) for seamless access to university resources.

Figure 3 presents the DHCP server configuration, which dynamically assigns IP addresses to student lab hosts, automating network setup and preventing conflicts.

Figure 4 demonstrates the Web Server [3] configuration, enabling reliable access to university webpages with optimized settings for performance and security.

Together, these configurations ensure efficient network management, seamless browsing, and secure web access within the university.

B. From PC to DNS server ping configuration

Figure 5 shows the results of a ping connection between the DNS server and Student Lab -2. This test was conducted to verify the connectivity and responsiveness of the DNS server [1]. within the university network. Successful ping responses indicate that the DNS server is properly configured and accessible from the student lab environment.

The results also help assess latency, packet loss, and overall network stability in resolving domain names.

C. Random Host Student Lab 2 Results (One by One)

This section presents the results of the "Random Host Student Lab 2" experiment, assessing the connectivity, accessibility, and functionality of the university network under different conditions. The findings highlight key interactions within the student lab environment.

Figures 6-14 illustrate various network functionalities and user interactions. Figure 6 shows the Student Lab -2 interface as the primary access point. Figure 7 tests DNS [1]. resolution by searching www.apex.edu.bd, confirmed in Figure 8, which displays the loaded webpage. Figures 9-10 verify access to university programs, while Figures 11-12 confirm facilities are retrievable. Figures 13-14 ensure seamless access to alumni network details.

These results demonstrate the effectiveness of the university's network in providing stable and efficient access to critical resources without connectivity issues.

VII. Limitations

- The current network [1]. design relies heavily on IPv4, which may face limitations in address availability and future scalability.
- Security mechanisms, while robust, are primarily focused on perimeter defense and lack advanced internal threat detection capabilities.
- The network's scalability is constrained by the existing hardware infrastructure, which may require significant upgrades to support future expansion.
- Integration with cloud-based services is currently limited, potentially restricting flexibility and remote access capabilities.
- The implementation of dynamic routing with OSPF, while effective, may introduce complexity in troubleshooting and maintenance.

VIII. Future Work

- Upgrade to IPv6 for broader compatibility.
- Enhancement of network monitoring and management tools to simplify troubleshooting and maintenance.

IX. Conclusion

This report successfully outlines the design and implementation of a complex, scalable, and secure network for Apex University. The network incorporates key services such as DHCP, DNS, and dynamic routing with OSPF. While the current design meets the university's needs, there are limitations in terms of IPv4 dependency, security depth, and scalability. Future work can focus on enhancing network performance, implementing deeper security protocols, integrating cloud-based solutions for further scalability, and addressing the identified limitations to ensure the network remains robust and future-proof.

References

[1] P. T. R. Nishant, "Understanding Computer Networks: A Comprehensive Overview of Types, Configurations, and the OSI Model," *arXiv preprint arXiv:2403.11296*, 2024.

[2] A. Purnomo, "Implementation of DHCP Snooping Method to Improve Security on Computer Networks," *bit-Tech*, vol. 6, no. 3, 2024.

[3] K. W. Hon, "Networking and IP addresses," in *Technology and Security for Lawyers and Other Professionals*. Edward Elgar Publishing, 2024, pp. 266–287.

[4] Cisco Systems, "Cisco Packet Tracer: Network Simulation Tool," Cisco Networking Academy, 2024. [Online]. Available: https://www.netacad.com/courses/packet-tracer. [Accessed: Oct. 10, 2024].

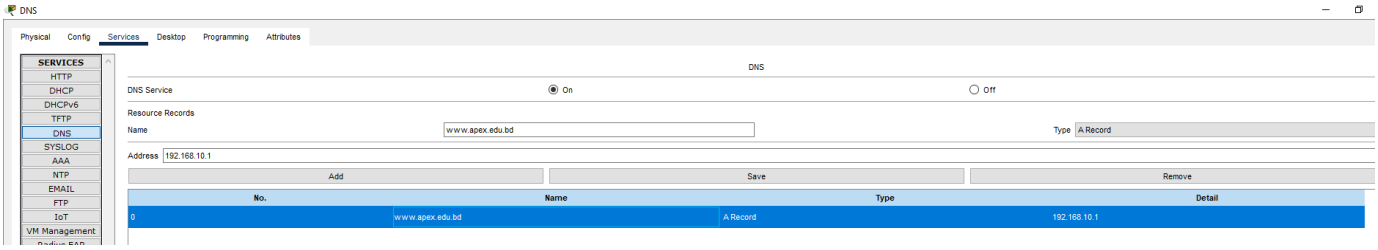

Fig. 2. Configuration of Apex University DNS Server in Cisco Packet Tracer

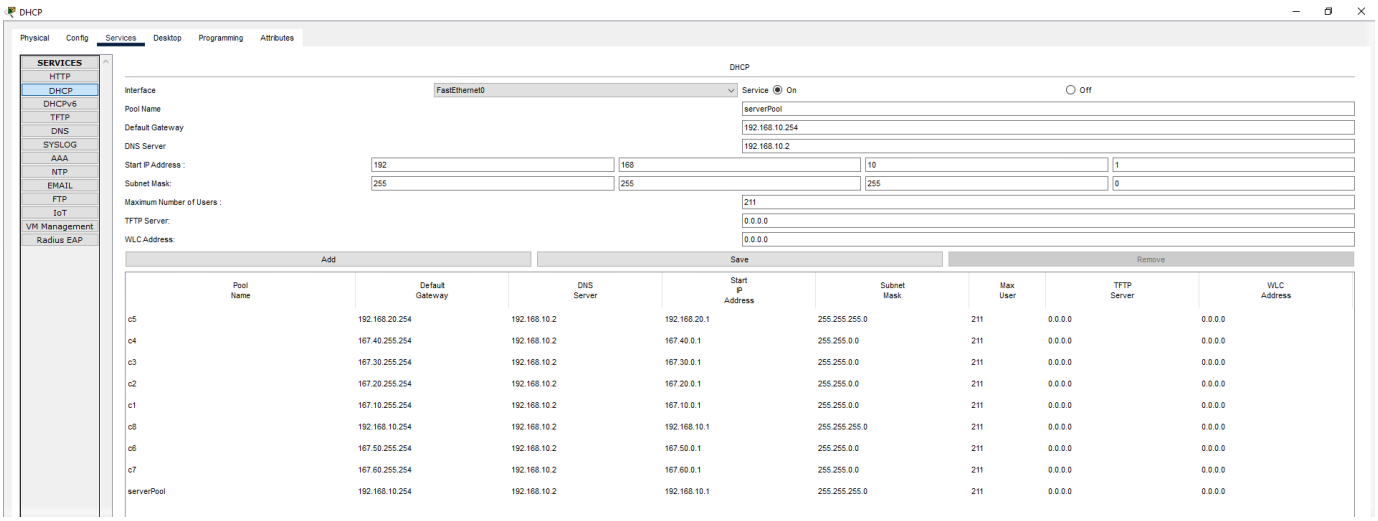

Fig. 3. Configuration of DHCP Server in Cisco Packet Tracer

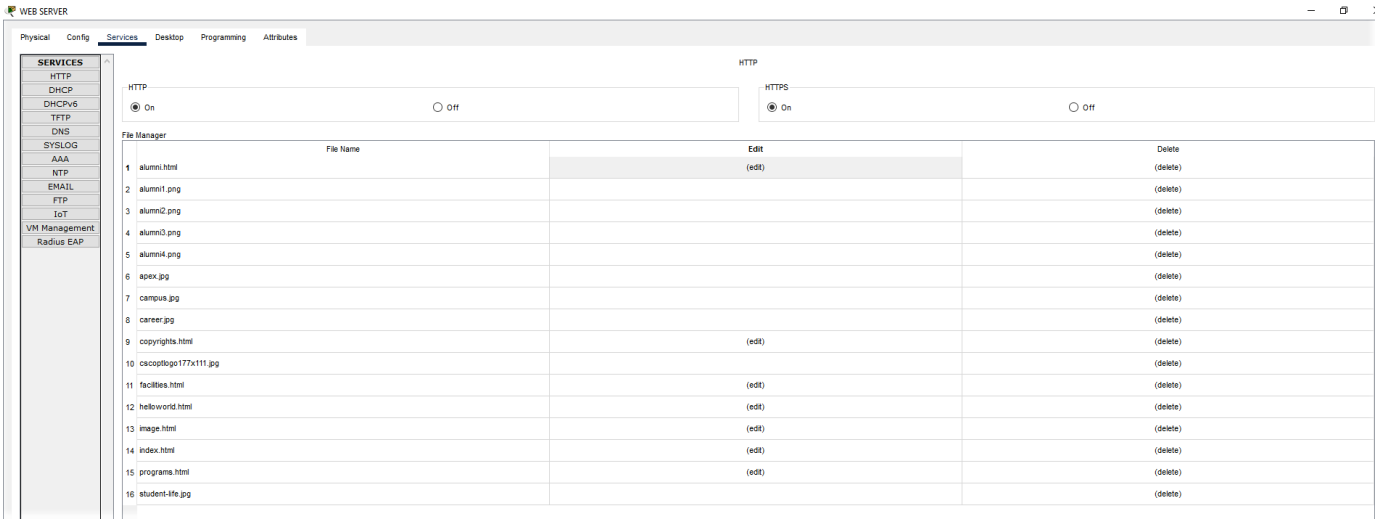

Fig. 4. Configuration of WEB Server in Cisco Packet Tracer

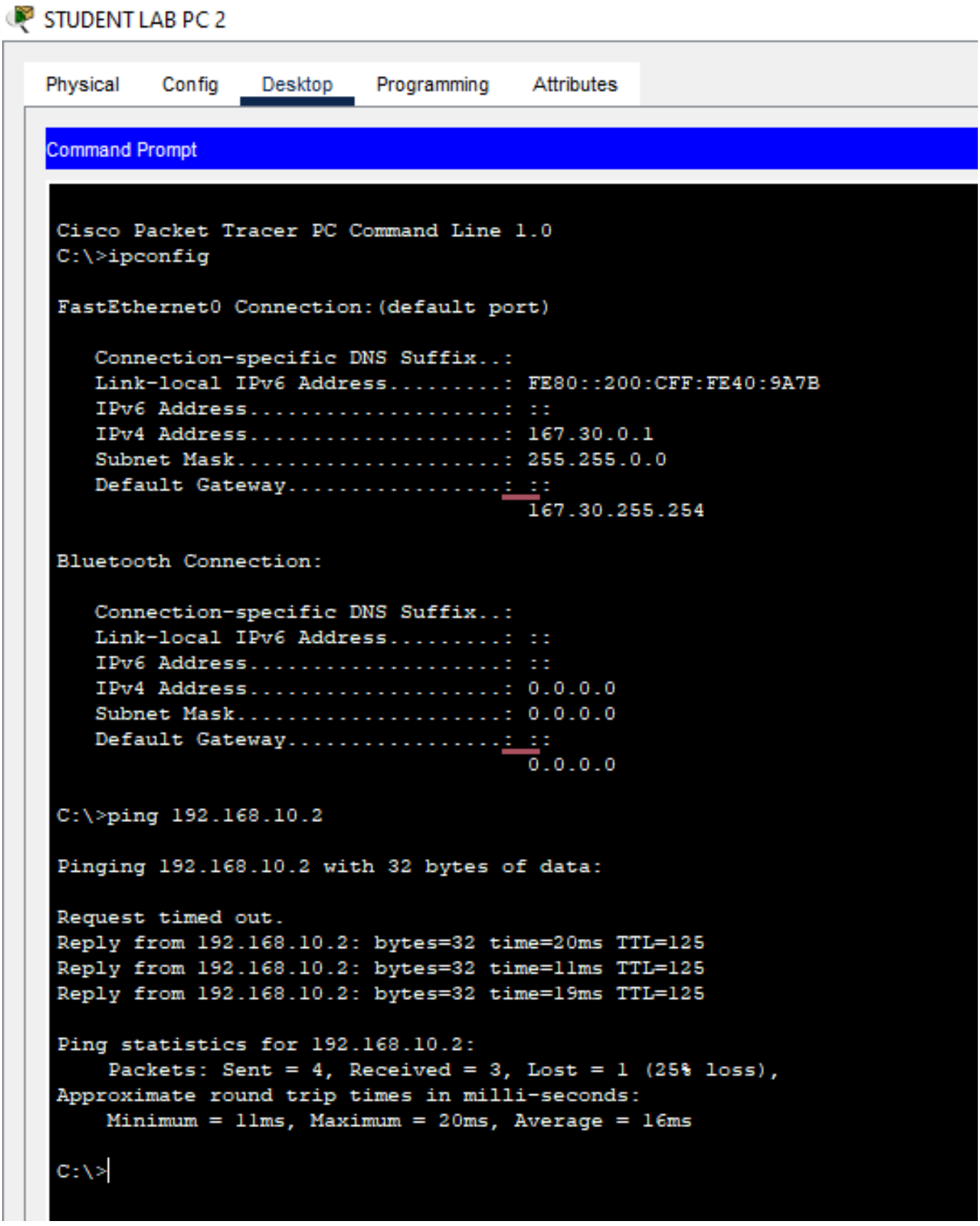

Fig. 5. Ping connection DNS Server with Student Lab -2

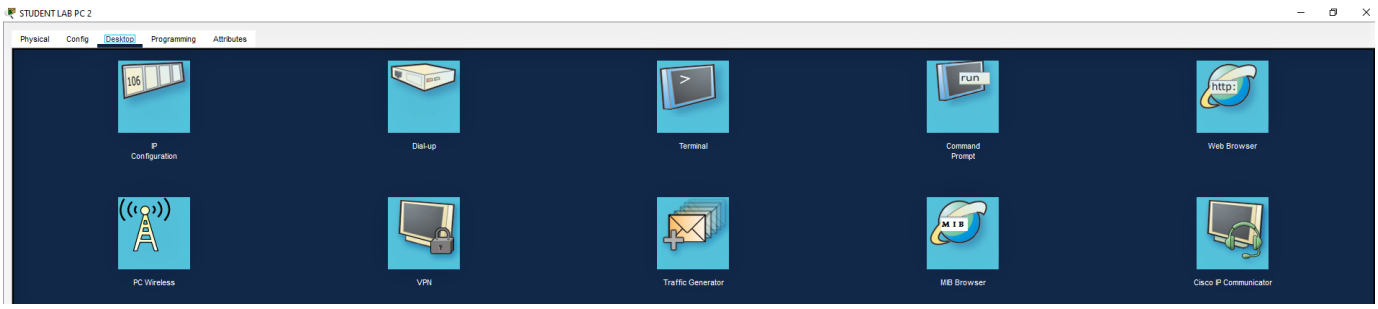

Fig. 6. Interface of Student Lab -2

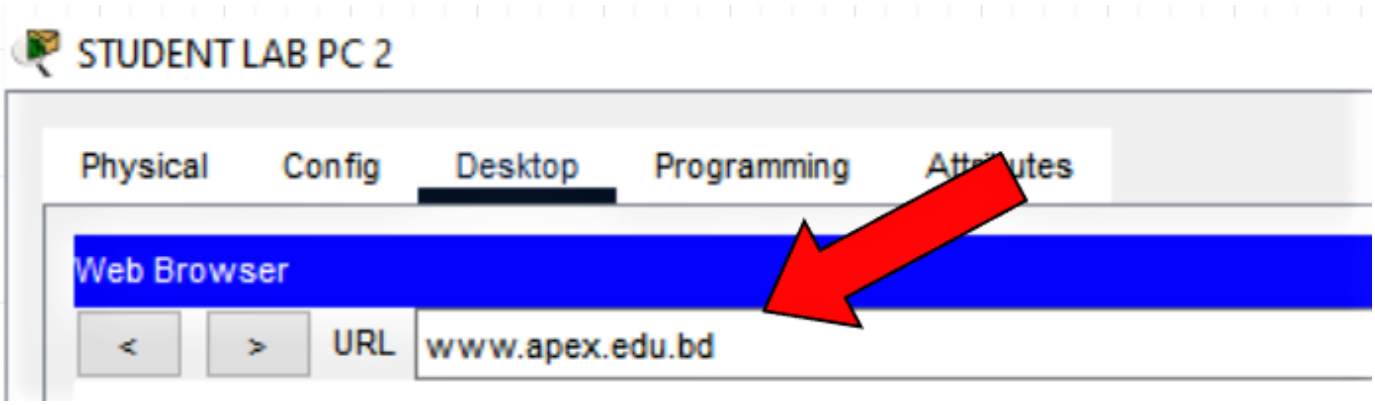

Fig. 7. Search www.apex.edu.bd Interface of Student Lab -2

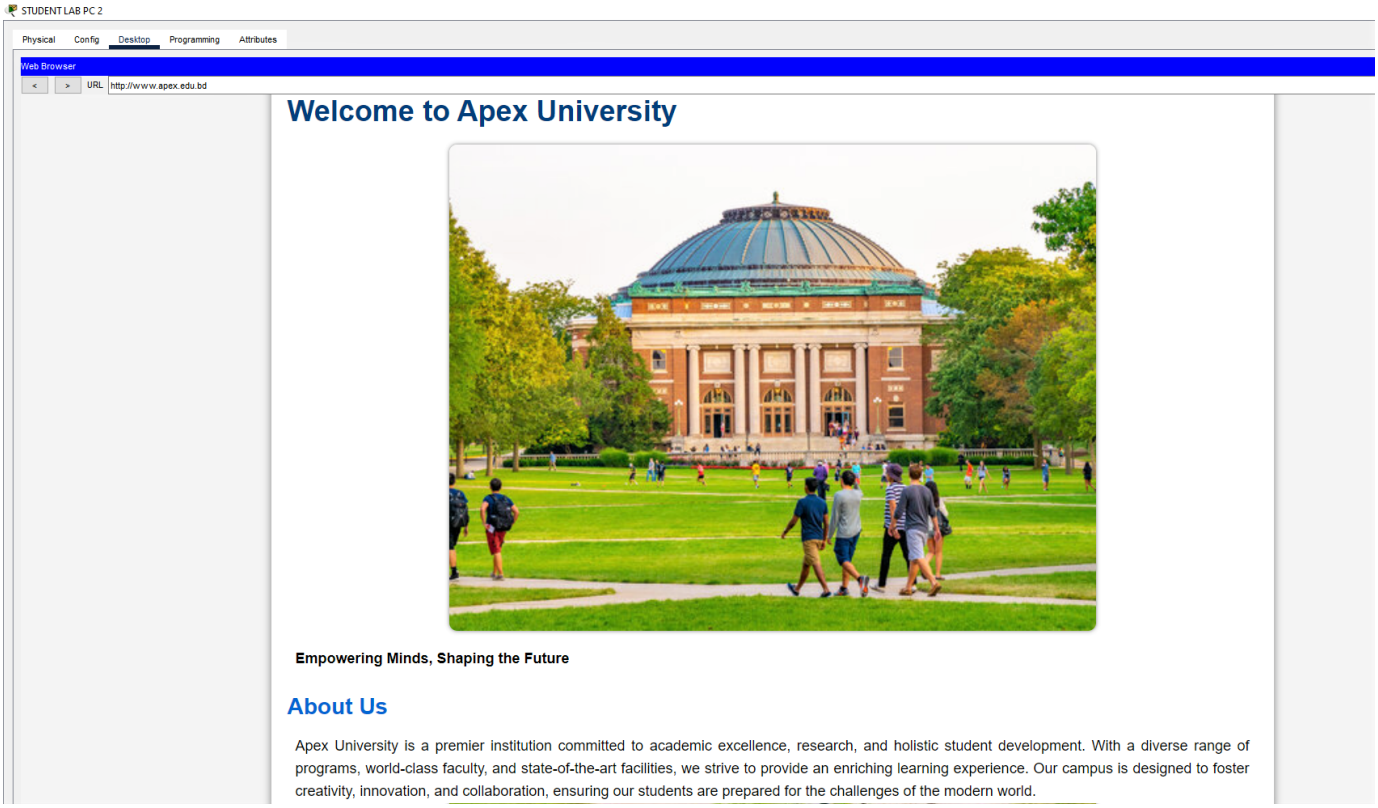

Fig. 8. www.apex.edu.bd

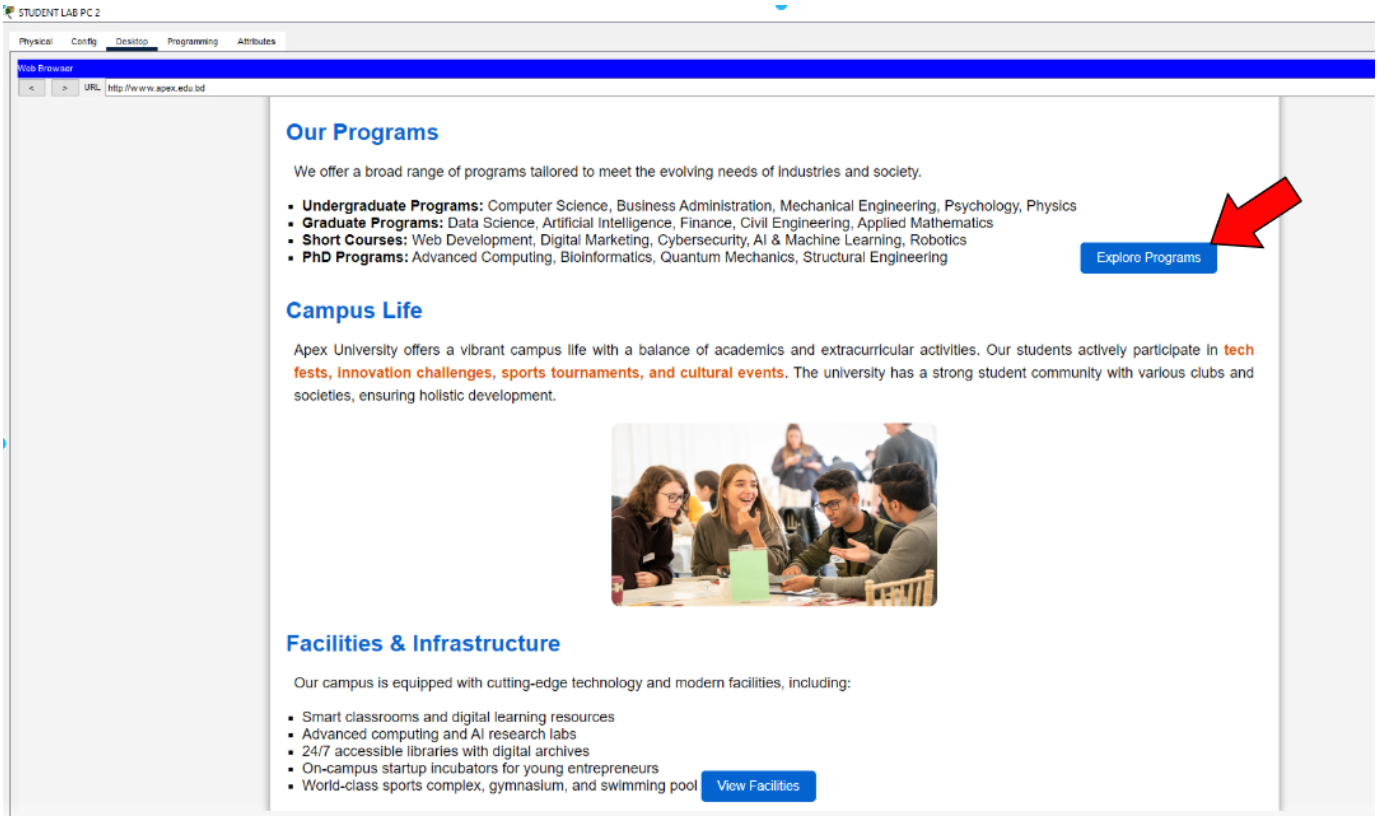

Fig. 9. Host can enter to check programs of Apex University

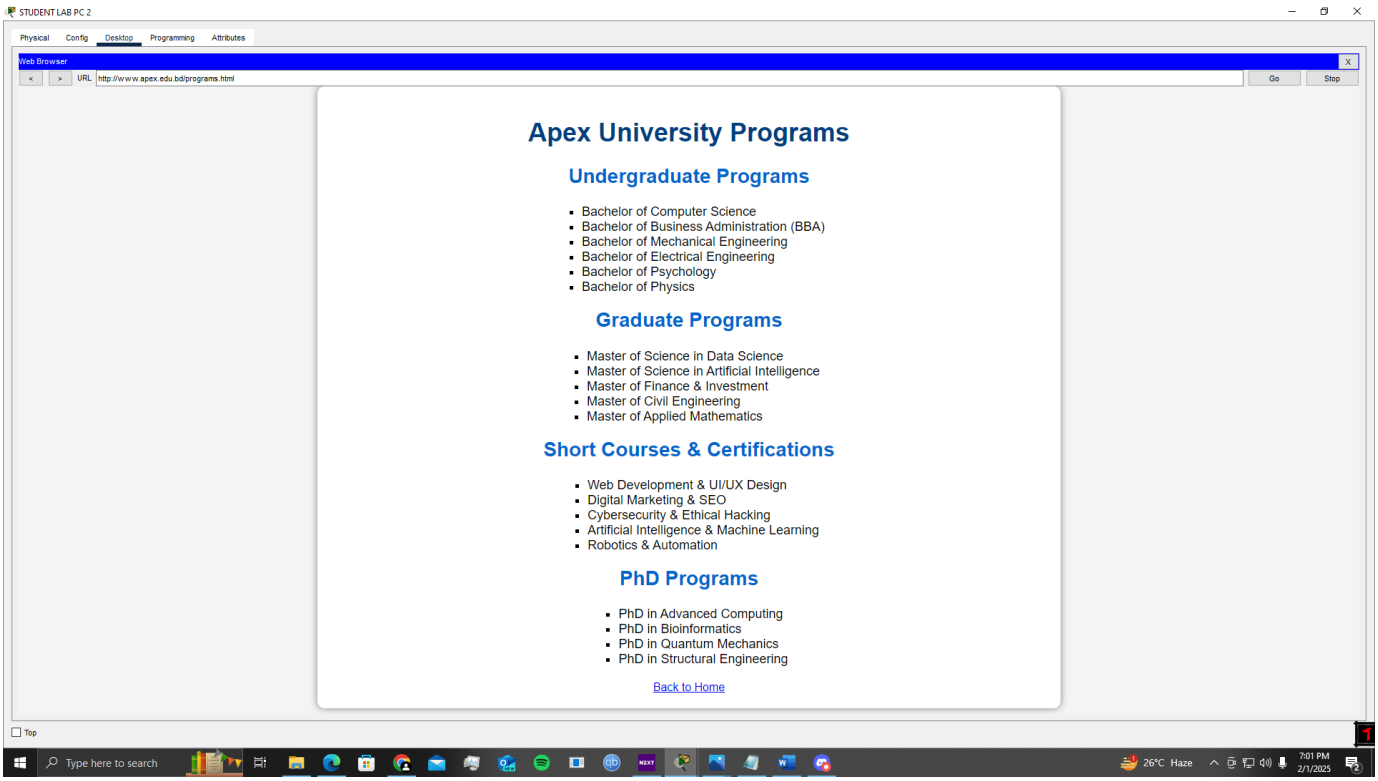

Fig. 10. List of Programs

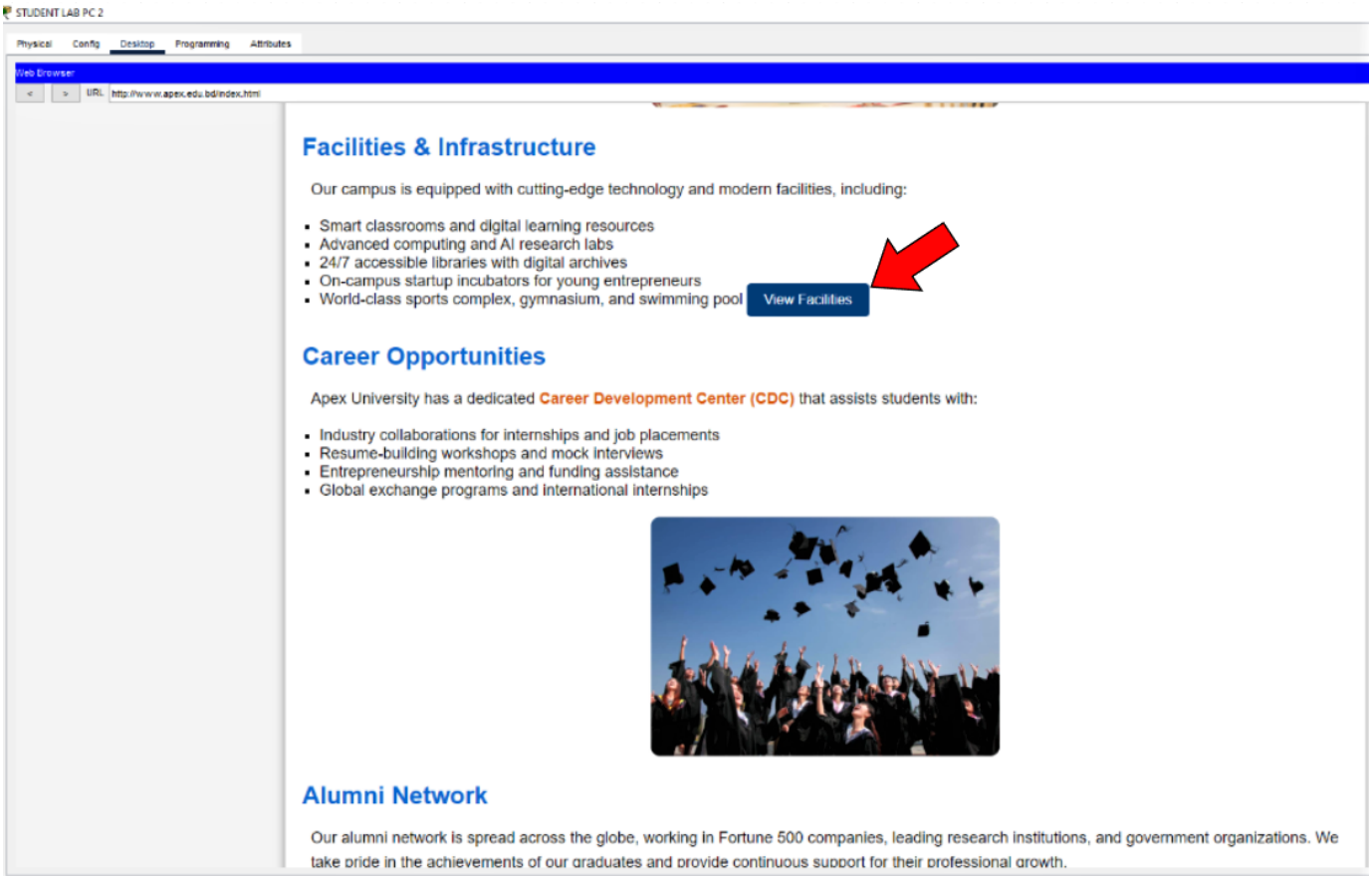

Fig. 11. Host can enter to check facilities of Apex University

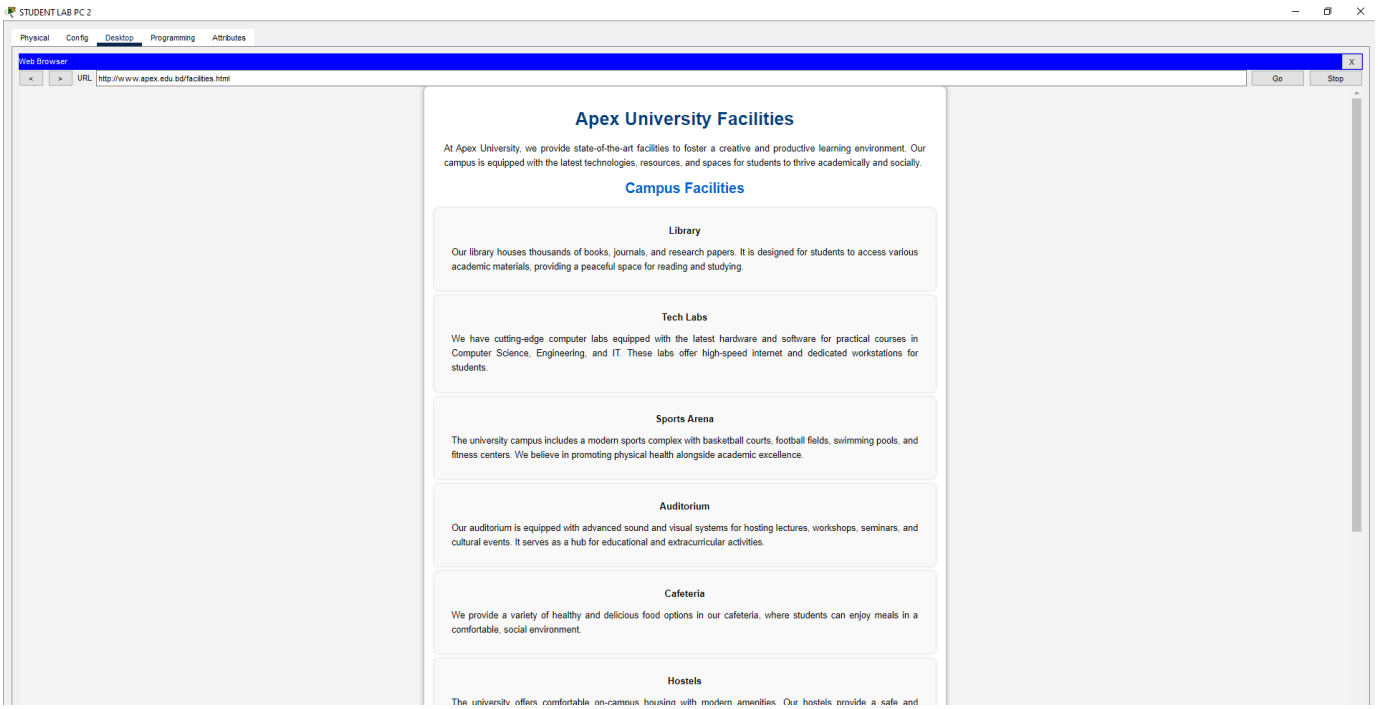

Fig. 12. List of Facilities

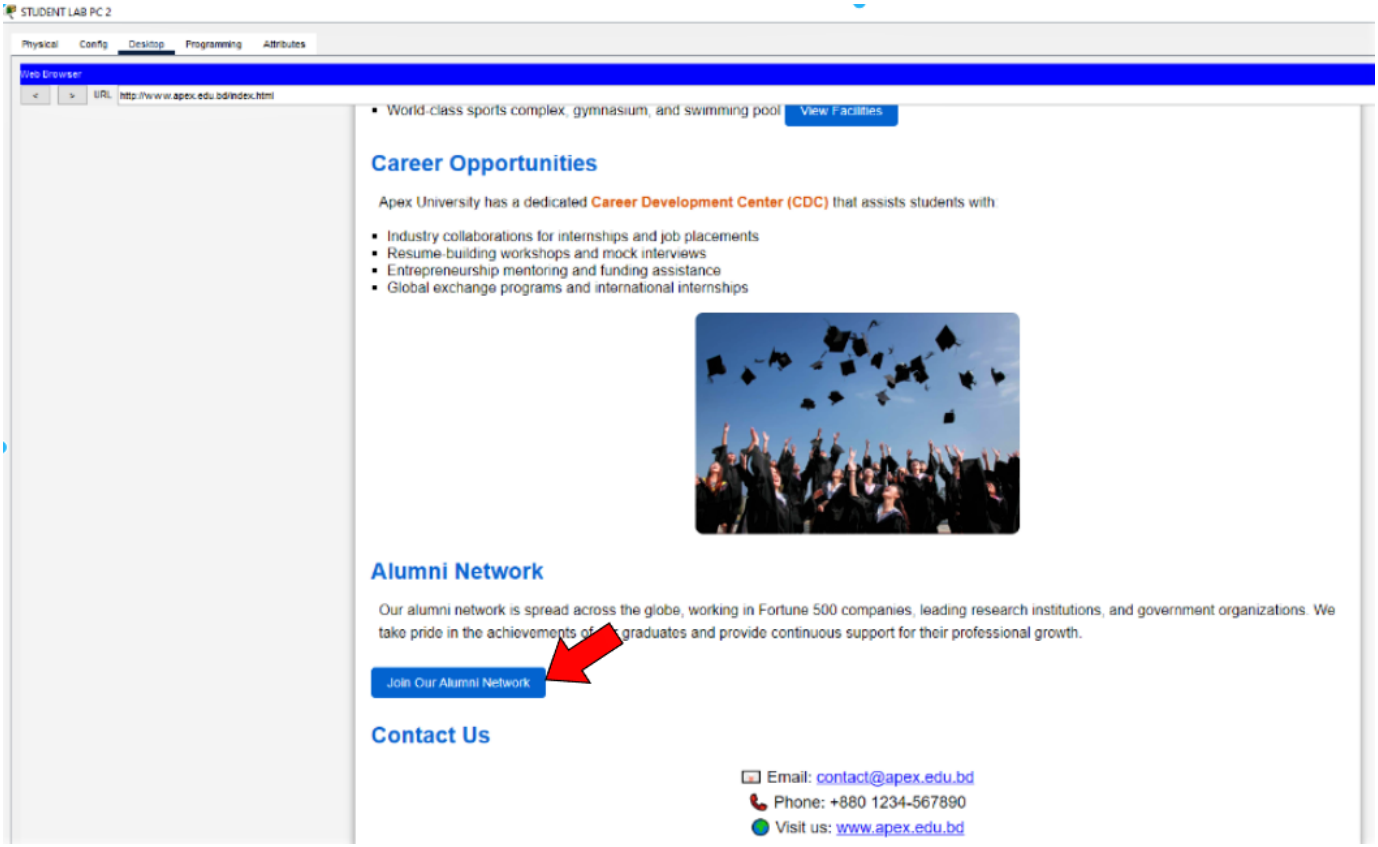

Fig. 13. Host can enter to check the alumni network of Apex University

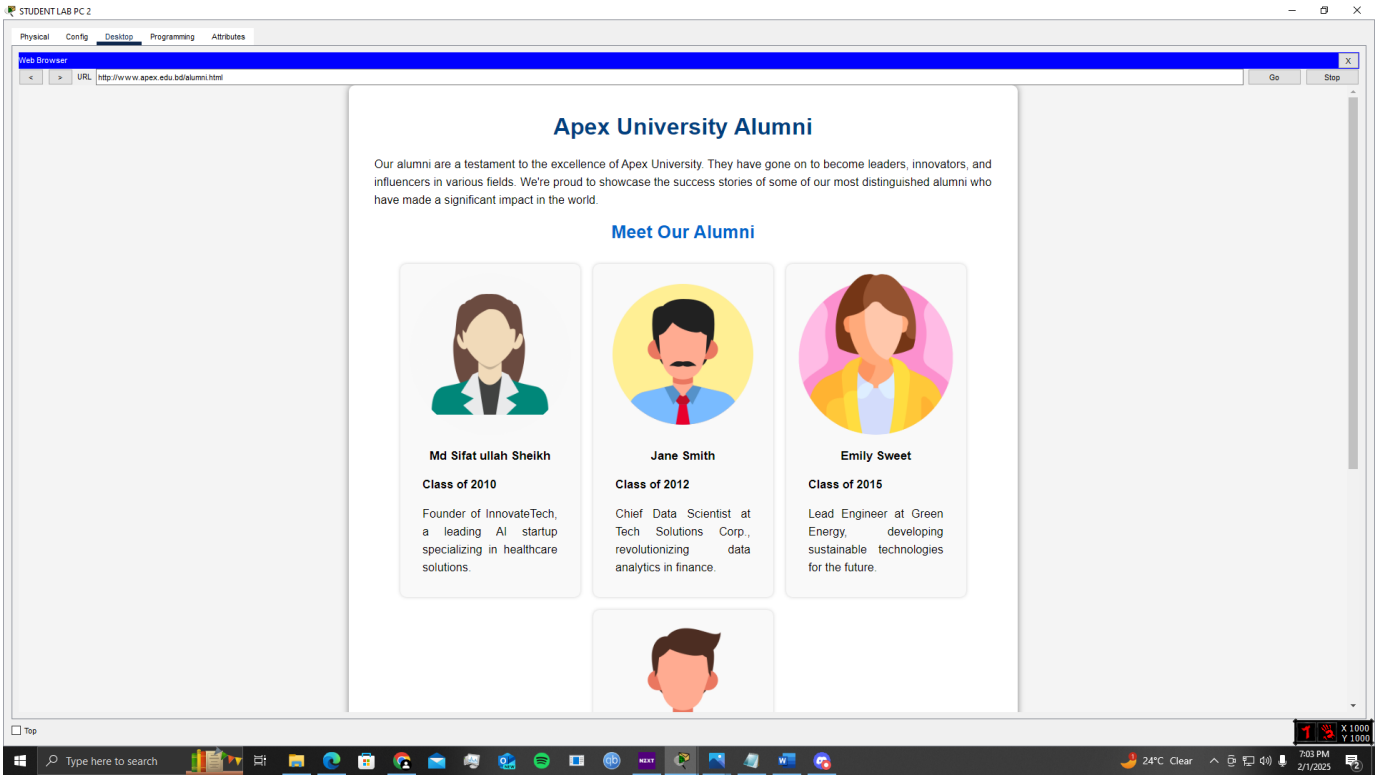

Fig. 14. List of Alumni