Implementation of an IT Network Scenario Using Packet Tracer for Teaching and Learning Purposes

Submitted by

TAMILARASAN.M	**724020104022**
SIVA.R	**724020104019**

In partial fulfilment for the award of the degree

Of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

DHAANISH AHMED INSTITUTE OF TECHNOLOGY

COIMBATORE

ANNA UNIVERSITY: CHENNAI 600025

JUNE 2023

ANNA UNIVERSITY: CHENNAI 600 025

BONAFIDE CERTIFICATE

Certified that this project report **“Implementation of an IT Network Scenario Using Packet Tracer for Teaching and Learning Purpose”** is the Bonafide work of **TAMILARASN.M (724019104022), SIVA.R (724019104019),** who carried out the project work under my supervision

SIGNATURE

Mr. A. MOHAMED NOORDEEN M.Tech

HEAD OF THE DEPARTMENT

Assistant Professor

Department of CSE

Dhaanish Ahmed Institute of

Technology, Coimbatore.

SIGNATURE

Mr. R. GOWRISHANKAR

SUPERVISOR

Assistant Professor

Department of CSE

Dhaanish Ahmed Institute of

Technology, Coimbatore.

Submitted for Mini Project work viva-voice examination held on……...…………for CS8611-Mini Project during the academic year 2021-2022

INTERNAL EXAMINAR

EXTERNAL EXAMINAR

ACKNOWLEDGEMENT

We express our gratitude and thanks to our parents first for giving health as well as sound mind and financial support for taking up this project.

We extend our sincere thanks to the Management of Dhaanish Ahmed Institute of Technology, Coimbatore**. Alhaj K Moosa**, Chairman**, Mr. K. A. Akbar Basha**, Director and **Mr. A. Thameez Ahmed**, Chief Executive Officer for providing us with all sort of support in the completion of our project.

We respect and thank our **Principal Dr. K. G. Parthiban M.E., Ph.D.,** for giving us an opportunity to do the project work and provide us all support and guidance which made us to complete the project on time.

We owe profound gratitude **Mr. A. Mohamed Noordeen M.Tech** Head of the Department, Department of Computer Science and Engineering, for his plausible support and timely assistance rendered for completing this project.

We heartily thank **Mr. R. Gowrishankar** Project Guide, Department of Computer Science and Engineering, for his valuable suggestions and remarkable guidance throughout the course of this project.

We also extend our thanks to all the teaching and non-teaching staffs of the Computer Science and Engineering department, family and friends for providing their moral support in successful completion of this project.

ABSTRACT

The implementation of an IT network scenario using Packet Tracer for teaching and learning purposes aims to provide students with a practical and hands-on experience in network design, configuration, and troubleshooting. Packet Tracer, a simulation tool developed by Cisco, offers a virtual environment where students can build and simulate complex network scenarios without the need for physical equipment. This project focuses on creating a network topology that replicates real-world network environments, incorporating routers, switches, PCs, servers, and other network devices. Students learn to design IP addressing schemes using techniques like VLSM (Variable Length Subnet Masking) to optimize address allocation and sub netting. By configuring devices and services such as DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System), HTTP (Hypertext Transfer Protocol), and implementing routing protocols, students gain practical knowledge of network protocols and services. They also explore concepts like VLANs (Virtual Local Area Networks), inter-VLAN routing, and access control lists (ACLs).The project provides students with opportunities to troubleshoot network issues, apply security measures, and analyse network performance using tools like Wireshark. It enhances their understanding of network concepts, promotes critical thinking, and develops problem-solving skills. Through this project, students gain valuable hands-on experience in network design and configuration, preparing them for real-world networking challenges. It fosters a deeper understanding of networking principles, protocols, and services, enabling students to become proficient in designing and managing network infrastructures.

TABLE OF CONTENT

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1. INTRODUTION

The implementation of an IT network scenario using Packet Tracer for teaching and learning purposes offers an immersive and practical approach to educate students about network design, configuration, and troubleshooting. In today's digital age, understanding and mastering the complexities of computer networks are essential for aspiring IT professionals. Packet Tracer, developed by Cisco, provides a simulated environment where students can explore and experiment with various network configurations without the need for physical hardware. This project aims to create a dynamic learning environment that replicates real-world network scenarios, enabling students to gain hands-on experience in building and managing networks. By utilizing Packet Tracer's features and functionalities, students can design and configure complex network topologies, implement routing protocols, set up network services, and troubleshoot network issues. The primary goal of this project is to bridge the gap between theoretical knowledge and practical application.

While traditional classroom instruction is vital, providing students with opportunities to work in simulated network environments greatly enhances their understanding and retention of concepts. Through this project, students will develop critical thinking skills, problem-solving abilities, and a deeper understanding of network protocols, IP addressing, sub netting, and network services. By engaging in the implementation of an IT network scenario using Packet Tracer, students will gain hands-on experience that prepares them for real-world networking challenges. They will learn to navigate common network issues, analyse network performance, and apply security measures. This project also cultivates a collaborative learning environment where students can work together to solve problems and share insights, fostering teamwork and communication skills. Overall, the implementation of an IT network scenario using Packet Tracer serves as an effective educational tool for teaching and learning networking concepts. It provides a platform for students to explore, experiment, and develop practical skills in a risk-free environment. By combining theoretical knowledge with hands-on experience, students will be well-equipped to tackle real-world networking scenarios and contribute to the evolving field of IT.

1.1. OBECTIVES

The objectives for the implementation of an IT network scenario using Packet Tracer for teaching and learning purposes can be outlined as follows;

Practical Hands-on Experience:

The primary objective is to provide students and professionals with a practical hands-on experience in networking. By creating a simulated network scenario using Packet Tracer, learners can actively engage with the concepts and apply their knowledge in a realistic environment.

Conceptual Understanding:

Another objective is to enhance learners' conceptual understanding of networking principles. Through the implementation of different network topologies and scenarios, students can grasp fundamental concepts such as IP addressing, routing protocols, sub netting, VLANs, and network security.

Simulation and Experimentation:

Packet Tracer allows for the simulation of various network scenarios, including troubleshooting, network design, and configuration. The objective is to enable learners to experiment with different network configurations, test their solutions, and troubleshoot network issues, thereby improving their problem-solving skills.

Customization for Learning Objectives:

The project aims to create a network scenario that can be tailored to specific learning objectives. This includes adjusting the network topology, configuring devices, and implementing specific protocols or technologies. Customization enables educators to align the scenario with their curriculum and target specific learning outcomes.

Collaboration and Teamwork:

The implementation of the network scenario using Packet Tracer encourages collaboration and teamwork among learners. By working together to design, configure, and troubleshoot the network, students can develop communication skills, teamwork abilities, and a deeper understanding of network dynamics.

1.2 TECHNOLOGIES USED

Packet Tracer:

Packet Tracer is a network simulation tool developed by Cisco Systems. It allows users to create virtual network topologies, configure network devices, and simulate network behaviour. Packet Tracer provides a user-friendly graphical interface and supports a wide range of network devices, protocols, and technologies.

Networking Devices:

The project involves the use of various networking devices such as routers, switches, and end devices. These devices are simulated within Packet Tracer and can be configured to replicate real-world network scenarios. They enable the creation of a functional network infrastructure for teaching and learning purposes.

Network Protocols:

The implementation of the network scenario using Packet Tracer incorporates different network protocols. This includes protocols like IP (Internet Protocol), TCP (Transmission Control Protocol), UDP (User Datagram Protocol), routing protocols (such as OSPF or EIGRP), VLAN (Virtual Local Area Network) protocols, and others. These protocols are configured and simulated within Packet Tracer to provide a realistic networking environment.

IP Addressing:

IP addressing is a crucial aspect of networking, and it is utilized in the project tassign IP addresses to devices within the network scenario. Sub netting, IP address allocation, and addressing schemes are implemented to teach and learn IP addressing concepts effectively.

Network Security:

Network security technologies and concepts are also integrated into the project. This includes the implementation of firewalls, access control lists (ACLs), virtual private networks (VPNs), and other security measures within the simulated network scenario. It allows learners to understand and practice network security principles.

CHAPTER 2

SYSTEM ANALYSIS

2.1. EXISTING SYSTEM

The existing system for teaching and learning networking concepts typically relies on traditional classroom-based instruction and theoretical explanations. It may involve the use of textbooks, lectures, and presentations to convey networking principles and concepts to students. While these methods are valuable in building a foundational understanding, they often lack the hands-on practical experience necessary for learners to fully grasp networking concepts and apply them in real-world scenarios.

In the absence of a practical learning environment, students may face challenges in visualizing and understanding complex networking concepts. They may struggle to comprehend the intricacies of network topologies, device configurations, and network protocols without hands-on experience. Additionally, the cost and availability of physical networking equipment can be a limiting factor for educational institutions, preventing them from providing comprehensive practical training.

The lack of a practical learning environment also hampers the ability to simulate and experiment with different network scenarios. Troubleshooting network issues, designing network architectures, and implementing security measures become theoretical exercises rather than practical applications.

Furthermore, collaboration and teamwork, which are essential skills in the networking field, may not be fully developed in the existing system. Limited opportunities for students to work together on real-world networking projects may hinder their ability to communicate effectively, solve problems collectively, and understand the dynamics of team collaboration.

Overall, the existing system for teaching and learning networking concepts may be constrained by the absence of a practical hands-on learning environment, limited access to networking equipment, and a lack of opportunities for collaborative learning and experimentation.

The implementation of an IT network scenario using Packet Tracer addresses these limitations by providing a simulated network environment that offers practical experience, flexibility, and cost-effectiveness.

2.1.2 DISADVANTAGES

Simulated Environment Limitations:

Packet Tracer provides a simulated network environment, which may not accurately replicate the complexities and nuances of real-world networking. While it offers a practical learning experience, certain advanced or specialized network configurations and technologies may not be fully supported or accurately represented in the simulation.

Hardware Limitations:

Packet Tracer relies on virtualized network devices and may not provide the same performance or capabilities as physical networking equipment. Certain hardware-specific functionalities or features may not be available or may behave differently in the virtual environment. This limitation can impact the accuracy and realism of the learning experience.

Lack of Physical Interaction:

Working with virtual devices in a simulated environment eliminates the physical interaction and tactile experience that comes with handling actual networking equipment. Students may miss out on the opportunity to physically connect cables, troubleshoot hardware issues, or gain a deeper understanding of the physical aspects of networking.

Limited Scalability:

While Packet Tracer can handle a significant number of network devices, there may be limitations on the scale and complexity of the network scenarios that can be created. Extremely large or intricate network architectures may not be feasible to simulate effectively within Packet Tracer, potentially limiting the scope of certain advanced networking concepts.

Dependent on Software:

The implementation relies on the availability and functionality of Packet Tracer software. Any limitations or issues with the software itself, such as bugs or compatibility problems, could impact the learning experience and potentially introduce inaccuracies in the simulated network behaviour.

2.2. PROPOSED SYSTEM

Enhanced Realism:

While acknowledging the limitations of a simulated environment, the proposed system focuses on creating network scenarios that closely resemble real-world networking situations. Emphasis is placed on selecting and configuring network devices, protocols, and technologies that align with industry standards and best practices. This approach ensures that learners gain practical knowledge and skills applicable to real-world networking environments.

Supplemental Practical Experiences:

Recognizing the importance of physical interaction, the proposed system incorporates supplemental practical experiences alongside the simulated environment. This can include opportunities for learners to work with physical networking equipment, participate in lab sessions, or engage in networking-related projects that involve real-world implementation. By combining virtual and physical experiences, learners can gain a more holistic understanding of networking concepts.

Scalability and Complexity:

The proposed system aims to overcome the limitations on scalability and complexity by designing network scenarios that challenge learners with progressively advanced concepts. This involves creating larger networks, incorporating more sophisticated configurations, and introducing advanced protocols and technologies. By gradually increasing the complexity, students can develop their skills and knowledge in a structured manner.

Integration of Real-world Constraints:

`The proposed system strives to integrate real-world constraints into the simulated environment wherever possible. This includes simulating factors like network latency, bandwidth limitations, and security threats to provide a more realistic learning experience. By understanding and addressing these constraints, learners can better prepare for the challenges they may encounter in real-world networking scenarios.

Continuous Improvement and Updates:

To ensure the effectiveness and relevance of the proposed system, regular updates and improvements are essential.

2.2.1 ADVANTAGES

Hands-on Learning Experience:

The project provides students with a practical hands-on learning experience in networking. It allows them to actively engage with network devices, configure network settings, and troubleshoot issues, enabling a deeper understanding of networking concepts.

Safe and Controlled Environment:

Packet Tracer offers a safe and controlled environment for learners to experiment with different network scenarios. They can make configuration changes, test solutions, and simulate network behaviour without the risk of impacting actual networks or devices.

Cost-effectiveness:

Using Packet Tracer eliminates the need for expensive physical networking equipment. It significantly reduces costs for educational institutions, making it more accessible to provide practical networking training to a larger number of students.

Customizability:

The network scenarios created using Packet Tracer can be customized to fit specific learning objectives. Educators can tailor the scenarios to cover specific topics, technologies, or troubleshooting scenarios, ensuring alignment with the curriculum and desired learning outcomes.

Simulation of Diverse Network Scenarios:

Packet Tracer allows the simulation of various network scenarios, ranging from small-scale local area networks (LANs) to complex wide area networks (WANs). Students can explore different network topologies, protocols, and technologies, gaining exposure to a diverse range of networking scenarios.

Collaboration and Teamwork:

The project facilitates collaboration and teamwork among learners. They can work together on network design, configuration, and troubleshooting tasks, fostering communication skills, teamwork abilities, and a deeper understanding of network dynamics.

CHAPTER 3

SYSTEM REQUIREMENTS

Operating System:

The project requires a computer system running a supported operating system, such as Windows, macOS, or Linux. The specific operating system version should be compatible with the installed version of Packet Tracer.

Hardware Requirements:

The computer system should meet the minimum hardware specifications recommended by Cisco for running Packet Tracer. This typically includes a multicore processor, a minimum amount of RAM (usually 4 GB or higher), sufficient storage space for installing the software, and a display with a suitable resolution.

Packet Tracer Software:

The latest version of Packet Tracer software should be downloaded and installed on the computer system. It can be obtained from the official Cisco Networking Academy website or other authorized sources.

Network Device Simulation:

The Packet Tracer software provides simulated network devices such as routers, switches, and end devices. These devices should be adequately configured within the software to create the desired network topology and scenarios.

Network Connectivity:

Since Packet Tracer is primarily a standalone simulation tool, an active internet connection is not mandatory. However, if the project requires accessing online resources, downloading additional resources, or accessing network services within the simulated environment, an internet connection may be necessary.

Documentation and Learning Resources:

To effectively utilize Packet Tracer for teaching and learning purposes, access to relevant documentation, tutorials, and learning resources is essential. These resources can

be obtained from Cisco's official website, networking forums, or educational platforms.

CHAPTER 4

IMPLEMENTATION AND MODULES

4.1 DESIGN THE TOPOLOGY FOR THE PROJECT

To design the topology for the implementation of an IT network scenario using Packet Tracer for teaching and learning purposes, it is important to consider the learning objectives, the complexity level desired, and the specific network scenarios to be covered. Here is a sample topology design that can serve as a starting point:

Topology Description:

The designed topology represents a small-scale network scenario with a focus on essential networking components and concepts. It includes multiple network devices, end devices, and interconnections that enable the demonstration of various networking principles.

Devices and Connections:

- **Routers**: Two routers are included to simulate connectivity between different network segments. These routers can be configured with appropriate routing protocols (e.g., OSPF, EIGRP) to demonstrate dynamic routing.
- **Switches:** Multiple switches are incorporated to create VLANs and showcase network segmentation. VLANs help in demonstrating broadcast domain isolation and facilitate the implementation of inter-VLAN routing.
- **End Devices:** Several PCs or laptops are connected to the switches to represent end hosts. These devices can be used to demonstrate IP addressing, sub netting, and network communication.
- **Servers:** To showcase server-client interactions, one or more servers can be added to the network. These servers can be configured to provide services such as web hosting, file sharing, or database access.
- **Interconnections:** Network connections, such as Ethernet cables or fibre optic links, are established between routers, switches, and end devices as per the desired topology. The interconnections can be illustrated using appropriate cabling symbols in Packet Tracer.

4.2 BASIC SETTING ROUTER AND SWITCHES

IP addressing and sub netting can be implemented to illustrate the allocation of IP addresses to different network segments and end devices. Proper subnet masks and default gateways should be assigned to ensure accurate routing and network communication.

The servers included in the topology can provide network services such as HTTP, FTP, or DNS. Network security measures, such as firewall configurations and access control lists (ACLs), can be implemented to demonstrate network protection and traffic filtering.

By designing a topology that incorporates these elements, learners can effectively explore and understand various networking principles, configurations, and scenarios within the simulated environment of Packet Tracer. The topology can be adjusted and customized based on specific learning goals and the scope of the project.

4.3 VSLM TABLE

The network address 192.168.0.0 is divided into subnets based on the required number of subnets and hosts for each subnet. The first subnet requires 60 hosts, so a subnet mask of 255.255.255.192 (/26) is used, allowing for a usable IP address range from 192.168.0.1 to 192.168.0.62.

The subsequent subnets are divided in a similar manner, with the subnet mask and usable IP address range adjusted based on the required number of hosts for each subnet. The first subnet requires 60 hosts, so a subnet mask of 255.255.255.192 (/27) is used, allowing for a usable IP address range from 192.168.0.1 to 192.168.1.223.

4.4 ADDRESSING TABLE NETWORK 1

Router 1 is assigned the IP address 192.168.0.1 on its FastEthernet0/0 interface, with a subnet mask of 255.255.255.0. This IP address will serve as the default gateway for devices within Network 1

Switch 1 is assigned the IP address 192.168.0.2 on its VLAN 10 interface, with the same subnet mask of 255.255.255.0. Switch 1 will act as a Layer 2 device within Network 1.

PC 1 and PC 2 are assigned IP addresses within the same subnet, 192.168.0.0/24, with the default gateway set to 192.168.0.1. These devices represent end hosts within Network 1.

4.4.1 ADDRESSING TABLE NETWORK 2

Router 2 is assigned the IP address 192.168.1.1 on its FastEthernet0/1 interface, with a subnet mask of 255.255.255.0. This IP address will serve as the default gateway for devices within Network 2.

Switch 2 is assigned the IP address 192.168.1.2 on its VLAN 20 interface, with the same subnet mask of 255.255.255.0. Switch 2 will act as a Layer 2 device within Network 2.

PC 3 and PC 4 are assigned IP addresses within the same subnet, 192.168.1.0/24, with the default gateway set to 192.168.1.1. These devices represent end hosts within Network 2.

4.5 ASSIGN IP ADDRESS TO THE DEVICE

FastEthernet0/0: IP address: 192.168.0.1, Subnet mask: 255.255.255.0 VLAN 10: IP address: 192.168.0.2, Subnet mask: 255.255.255.0, Default gateway: 192.168.0.1

Ethernet: IP address: 192.168.0.3, Subnet mask: 255.255.255.0, Default gateway: 192.168.0.1Ethernet: IP address: 192.168.0.4, Subnet mask: 255.255.255.0, Default gateway: 192.168.0.1

FastEthernet0/1: IP address: 192.168.1.1, Subnet mask: 255.255.255.0VLAN 20: IP address: 192.168.1.2, Subnet mask: 255.255.255.0, Default gateway: 192.168.1.1

Ethernet: IP address: 192.168.1.3, Subnet mask: 255.255.255.0, Default gateway: 192.168.1.1Ethernet: IP address: 192.168.1.4, Subnet mask: 255.255.255.0, Default gateway: 192.168.1.1

4.6 CONFIGURE HTTP SERVER

Configure the IP address and subnet mask for the PC 1 interface. Based on the provided addressing table, PC 1 has the IP address 192.168.0.3 with a subnet mask of 255.255.255.0.

Install and set up an HTTP server software on PC 1. There are several options available, such as Apache HTTP Server, Nginx, or Microsoft IIS. Choose the one that suits your requirements and install it on PC 1.

Configure the HTTP server software with the appropriate settings. This includes specifying the root directory where the web content is stored, configuring any virtual hosts if needed, and setting up any necessary permissions or security settings.

4.7 CONFIGURE DNS SERVER

Access the configuration interface of Router 1. This can typically be done through a command-line interface (CLI) or a web-based graphical user interface (GUI) depending on the router's operating system.

Configure the IP address and subnet mask for the DNS server interface on Router 1. Based on the provided addressing table, Router 1 has the IP address 192.168.0.1 with a subnet mask of 255.255.255.0.

Install and configure a DNS server software on Router 1. There are various DNS server software options available, such as BIND (Berkeley Internet Name Domain), Windows Server DNS, or dnsmasq. Choose the appropriate DNS server software for your project and follow the installation instructions.

Configure the DNS server software with the necessary settings. This includes specifying the DNS zones, configuring DNS records (such as A, CNAME, MX records), and setting up any necessary forwarders or DNS policies

4.8CONFIGURE DHCP SERVER

Access the configuration interface of Router 1. This can typically be done through a command-line interface (CLI) or a web-based graphical user interface (GUI) depending on the router's operating system.

Configure the IP address and subnet mask for the DHCP server interface on Router 1. Based on the provided addressing table, Router 1 has the IP address 192.168.0.1 with a subnet mask of 255.255.255.0.

Enable the DHCP server functionality on Router 1. This can usually be done by enabling the DHCP service in the router's configuration settings.

Configure the DHCP server settings on Router 1. This includes specifying the DHCP address pool range, default gateway, DNS server addresses, and any additional DHCP options you want to configure, such as domain name or lease duration.

4.9 CONFIGURE THE CISCO ACCESS POINT

Access the AP's command-line interface (CLI) or web-based graphical user interface (GUI) depending on the model and software version.

Configure the basic settings of the AP, such as the hostname, domain name, and management IP address. This can typically be done through the configuration interface or CLI commands.

Set up wireless SSIDs (Service Set Identifiers) on the AP. Determine the SSID names, security settings (WPA2, WPA3, etc.), and passphrase or authentication method (PSK, EAP, etc.) for each SSID.

Configure the wireless channels and radio settings for each SSID. Choose the appropriate channel and radio mode (e.g., 2.4 GHz or 5 GHz) based on your requirements and network environment.

4.9CONFIGURE SSH AND TELNET ON DEVICE

Access the configuration interface of the device through a console cable or an existing management connection.

Enter privileged EXEC mode by typing "enable" and providing the appropriate password if required.

Configure a hostname for the device using the "hostname" command. For example: "hostname Router1".

Generate encryption keys for secure communication. Use the "crypto key generate rsa" command and specify the desired key length, such as 2048 or 4096 bits.

Configure the VTY (Virtual Terminal) lines to enable SSH and/or Telnet access. Access the line configuration mode by typing "line vty 0 15".

4.10 TEST END-TO-END CONNECTIVITY

Ensure that all devices in the network are powered on and properly connected to each other according to the designed topology.

Verify that the devices have been configured correctly with the appropriate IP addresses, subnet masks, default gateways, and other necessary network settings.

From a device in Network 1 (e.g., PC 1), open a command prompt or terminal and attempt to ping the IP address of the default gateway (Router 1). For example, use the command "ping 192.168.0.1". If the ping is successful, it indicates that there is connectivity between PC 1 and Router 1.

Next, attempt to ping a device in Network 2 (e.g., PC 3) from a device in Network 1 (e.g., PC 1). Use the command "ping" followed by the IP address of PC 3 (e.g., "ping 192.168.1.3"). If the ping is successful, it confirms that there is connectivity between the two networks.

Repeat the above steps from a device in Network 2 (e.g., PC 3) to test connectivity to devices in Network 1.

4.12 FINAL OUTPUT

The output of the project would depend on various factors, including the specific configurations, devices, and network setup implemented. It would involve the successful establishment of connectivity between devices, successful configuration and operation of services like DHCP, DNS, HTTP, and the ability to communicate between different networks. To obtain the output of the project, you would need to implement and execute the project in a real or simulated network environment, and then observe the behaviour and functioning of the network components, services, and communication between devices. If you encounter any specific issues or have further questions regarding the project or its implementation, please feel free to ask, and I'll be happy to assist you to the best of my knowledge and abilities.

CHAPTER 5

SYSTEM TESTING

Several types of system testing are commonly performed to ensure the application

Function as expected. Here are some of the key system testing types:

Functional Testing:

This testing verifies the functional requirements of the application. It ensures that each function or feature of the application performs as intended. Examples of functional tests include:

- Input validation testing
- User interface (UI) testing
- Integration testing
- Regression testing
- User acceptance testing (UAT)

Performance Testing:

Performance testing evaluates the application's performance under different load conditions. It measures response times, throughput, scalability, and stability of the system.
Common performance tests include:

- Load testing
- Stress testing
- Endurance testing
- Spike testing

Security Testing:

Security testing assesses the application's ability to protect data and prevent unauthorized access. It identifies vulnerabilities, weaknesses, and potential security risks. Security testing may include:

- Vulnerability scanning
- Penetration testing
- Authentication and authorization testing

Usability Testing:

Usability testing focuses on the application's user-friendliness and ease of use. It involves gathering feedback from actual users to evaluate the application's user interface, navigation, and overall user experience.

CHAPTER 6

CONCLUSION

In conclusion, the above project aimed to implement an IT network scenario using Packet Tracer for teaching and learning purposes. Throughout the project, various technologies and modules were utilized to create a functional network environment. The project focused on designing the network topology, implementing VLSM (Variable Length Subnet Masking) for efficient IP address allocation, configuring devices such as routers and switches, setting up services like DHCP, DNS, and HTTP, and testing end-to-end connectivity. By successfully completing the project, several key benefits and outcomes were achieved. Firstly, students were provided with a hands-on learning experience in network design and configuration, gaining practical knowledge in network protocols, IP addressing, and service implementation. The project also fostered an understanding of troubleshooting techniques and problem-solving skills in a network environment. Additionally, the project allowed for the exploration of different technologies, including Cisco devices, routing protocols, and network services. provided students with exposure to real-world network scenarios, preparing them for future networking challenges and industry demands.

CHAPTER 7

FUTURE ENHANCEMENT

Security Implementation:

Integrate security measures into the network scenario to enhance students' understanding of network security concepts. This could involve implementing firewall rules, access control lists (ACLs), VPN connections, or Intrusion Detection Systems (IDS) to protect the network from unauthorized access or attacks.

Advanced Routing Protocols:

Introduce more complex routing protocols, such as OSPF (Open Shortest Path First) or EIGRP (Enhanced Interior Gateway Routing Protocol), to provide students with hands-on experience in configuring and managing dynamic routing protocols.

Virtualization and Cloud Integration:

Incorporate virtualization technologies and cloud services into the network scenario. This could involve deploying virtual machines, utilizing software-defined networking (SDN) concepts, or integrating cloud services like AWS or Azure. This enhancement will expose students to modern network deployment models and cloud integration strategies.

Network Monitoring and Management:

Integrate network monitoring and management tools to enable students to monitor network performance, analyze network traffic, and troubleshoot issues effectively. This could involve using tools like Wireshark, SNMP (Simple Network Management Protocol), or network monitoring platforms to provide students with practical experience in network monitoring and troubleshooting.

Multi-site Connectivity:

Expand the network scenario to include multiple sites connected through wide area networks (WANs). This enhancement will expose students to concepts like VPN tunnels, MPLS (Multi-Protocol Label Switching), and WAN optimization techniques, providing a more realistic and comprehensive network deployment scenario.

CHAPTER 8

APPENDINX

8.1 SOURCE CODE

```
Router>ENABLE
Router#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#service password-enc
R1(config)#service password-encryption
R1(config)#banner motd "authorized access only"
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#log synch
R1(config-line)#line console 0
R1(config-line)#log synch
```

Similarly done in IT-Switch, HR-Switch, Farm-Server

Then,

```
IT-Switch (config)#
IT-Switch (config)# ip ssh version 2
IT-Switch (config)# username admin password admin
IT-Switch (config)# line vty 0 15
IT-Switch (config-line)# transport input a11
IT-Switch (config-line)# login local
IT-Switch (config-line)# end
```

```
IT-Switch # copy run start

Destination filename [startup-config]?

Building configuration…..

[ok]

IT-Switch >enable

Password:

IT-Switch #conf t

Enter configuration commands, one per line. End with CNTL/Z.
IT-Switch (config)#inteface vlan 1

IT-Switch (config-if )# ip address 192.168.1.2   255.255.255.128

IT-Switch (config-if)#description SVI for IT-Switch

IT-Switch (config-if)# no shutdown

IT-Switch (config-if)#

%LINK -5-CHANGED: Interface Vlan1 , changed startup to up

%LINKPROTO -5-UPDOWN:Line Protocol on  Interface Vlan1 , changed startup to up

IT-Switch (config-if)#
```

Similarly done in IT-Switch, HR-Switch, Farm-Server

Then,

PINK COMMENTS,

AND GET OUTPUT

8.2 SCREEN SHOTS

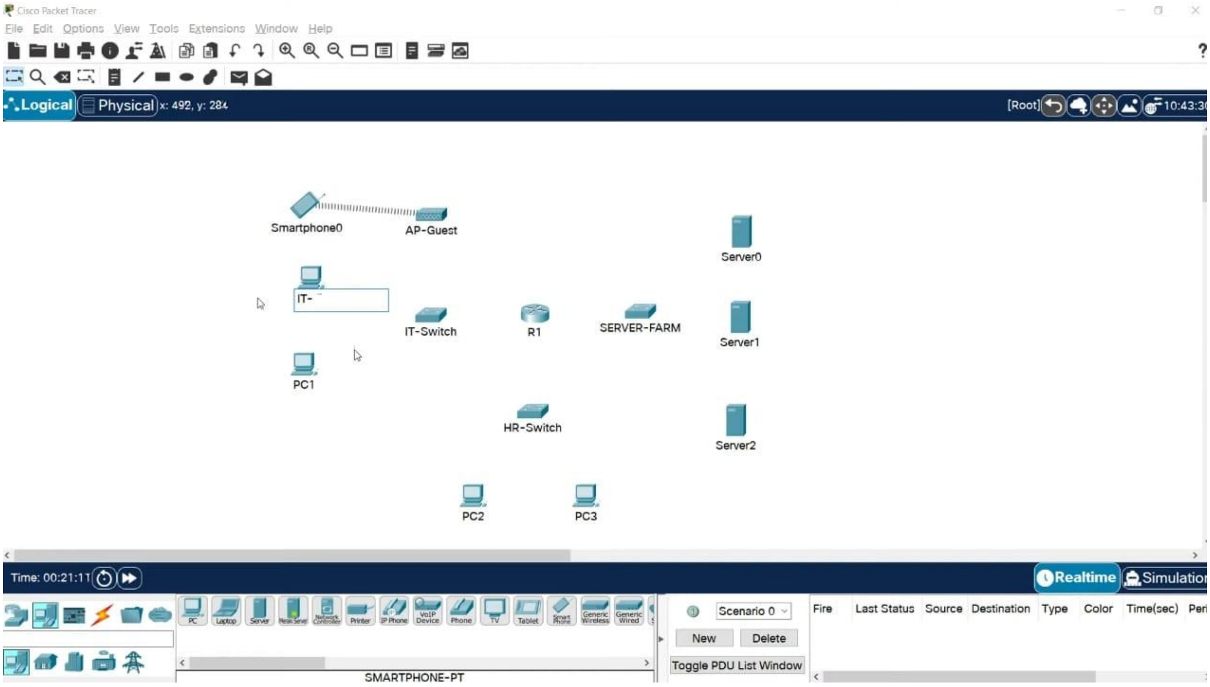


Figure 1

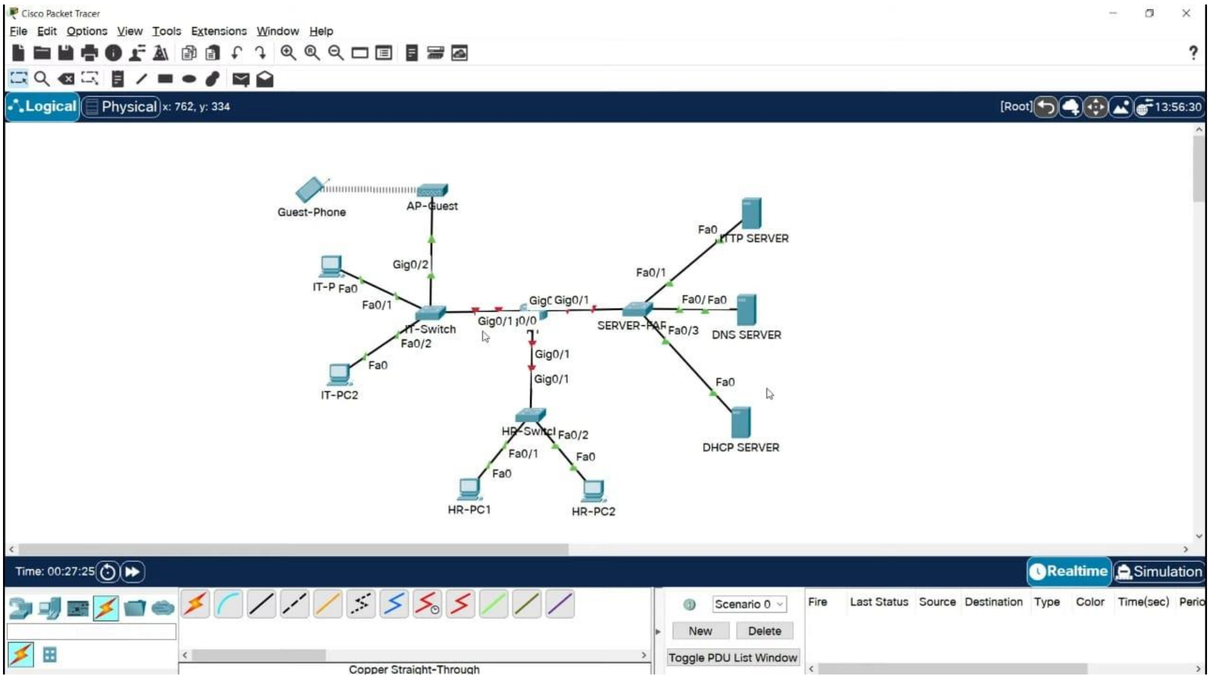
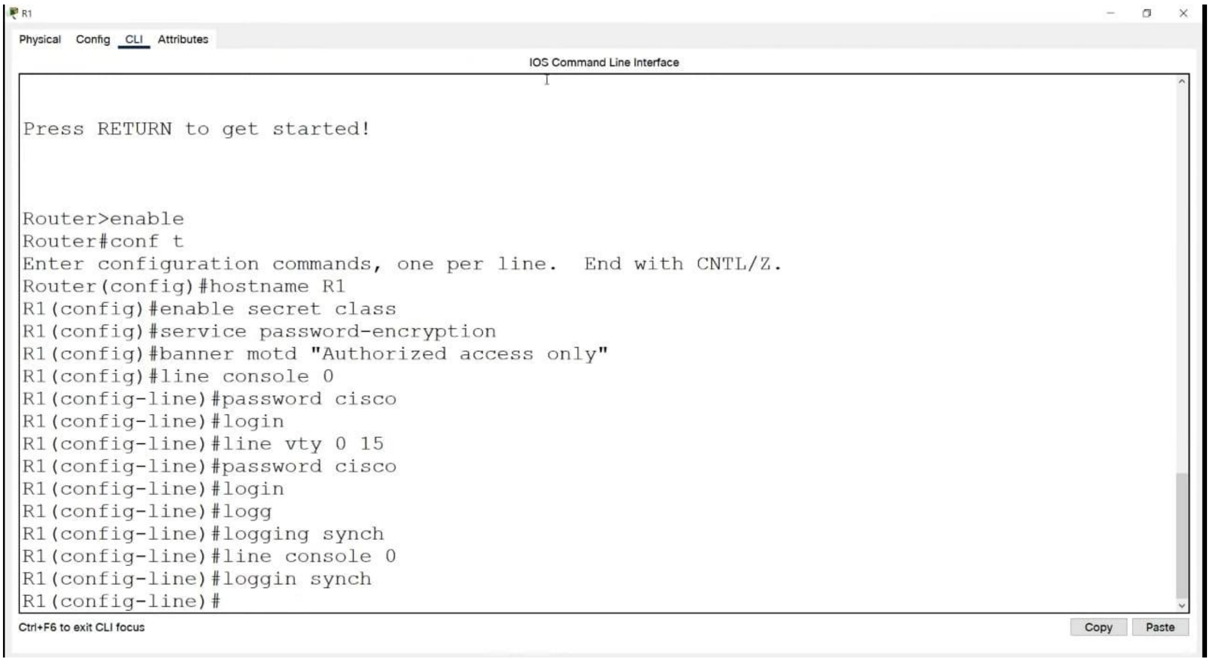
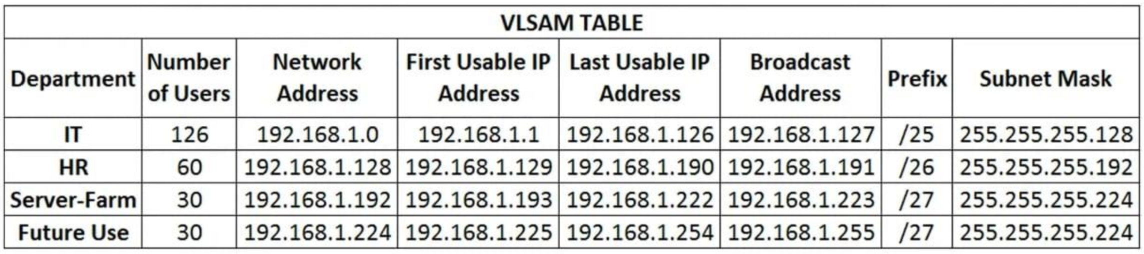


Figure 2



```
Press RETURN to get started!



Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#service password-encryption
R1(config)#banner motd "Authorized access only"
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logg
R1(config-line)#logging synch
R1(config-line)#line console 0
R1(config-line)#loggin synch
R1(config-line)#
```

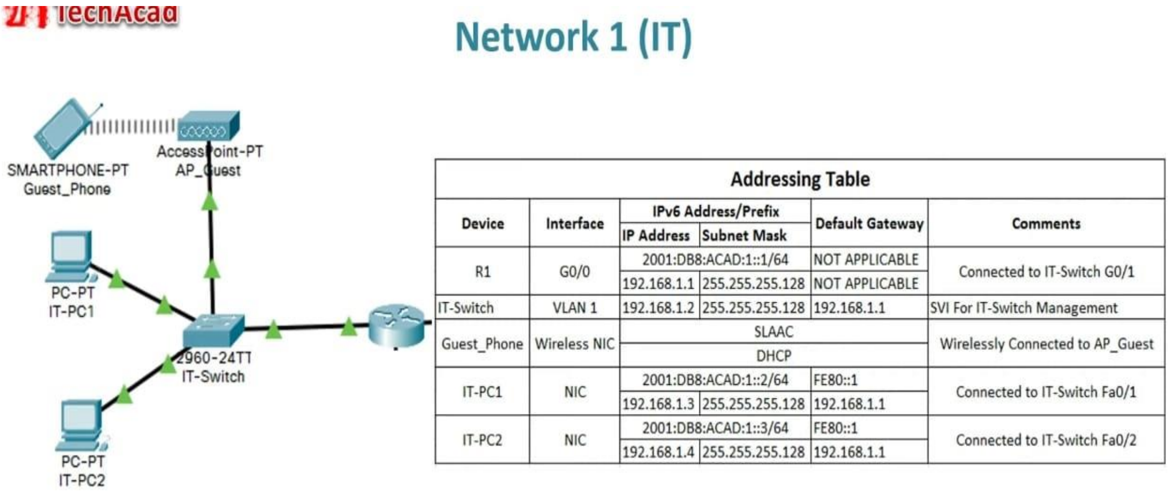
Figure 3



VLSAM TABLE

Department	Number of Users	Network Address	First Usable IP Address	Last Usable IP Address	Broadcast Address	Prefix	Subnet Mask
IT	126	192.168.1.0	192.168.1.1	192.168.1.126	192.168.1.127	/25	255.255.255.128
HR	60	192.168.1.128	192.168.1.129	192.168.1.190	192.168.1.191	/26	255.255.255.192
Server-Farm	30	192.168.1.192	192.168.1.193	192.168.1.222	192.168.1.223	/27	255.255.255.224
Future Use	30	192.168.1.224	192.168.1.225	192.168.1.254	192.168.1.255	/27	255.255.255.224

Figure 4

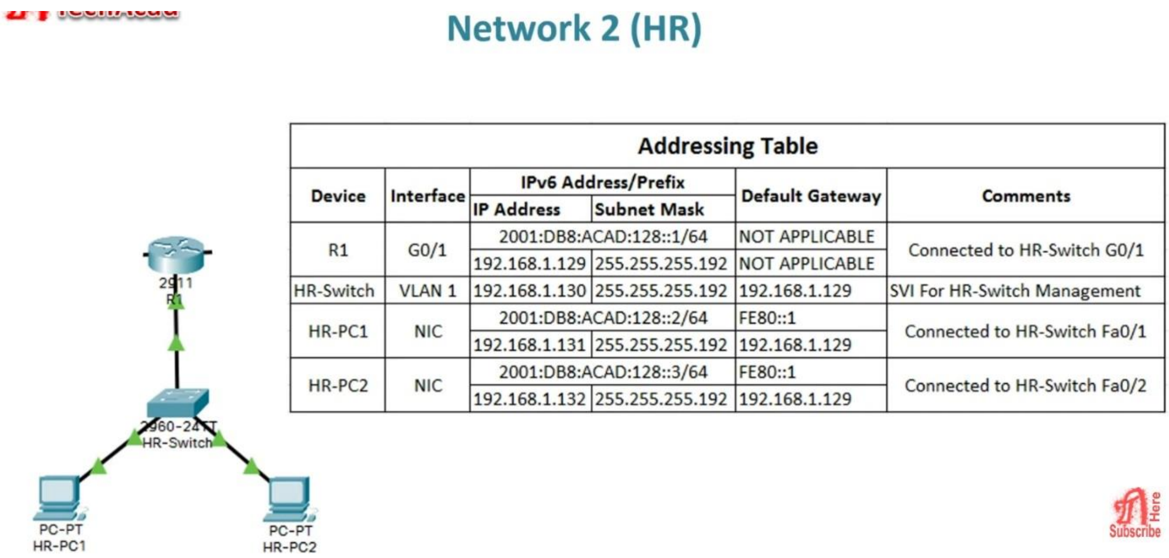


Network 1 (IT)

Addressing Table

Device	Interface	IPv6 Address/Prefix		Default Gateway	Comments
		IP Address	Subnet Mask		
R1	G0/0	2001:DB8:ACAD:1::1/64		NOT APPLICABLE	Connected to IT-Switch G0/1
		192.168.1.1	255.255.255.128	NOT APPLICABLE	
IT-Switch	VLAN 1	192.168.1.2	255.255.255.128	192.168.1.1	SVI For IT-Switch Management
Guest_Phone	Wireless NIC	SLAAC			Wirelessly Connected to AP_Guest
		DHCP			
IT-PC1	NIC	2001:DB8:ACAD:1::2/64		FE80::1	Connected to IT-Switch Fa0/1
		192.168.1.3	255.255.255.128	192.168.1.1	
IT-PC2	NIC	2001:DB8:ACAD:1::3/64		FE80::1	Connected to IT-Switch Fa0/2
		192.168.1.4	255.255.255.128	192.168.1.1	

Figure 5

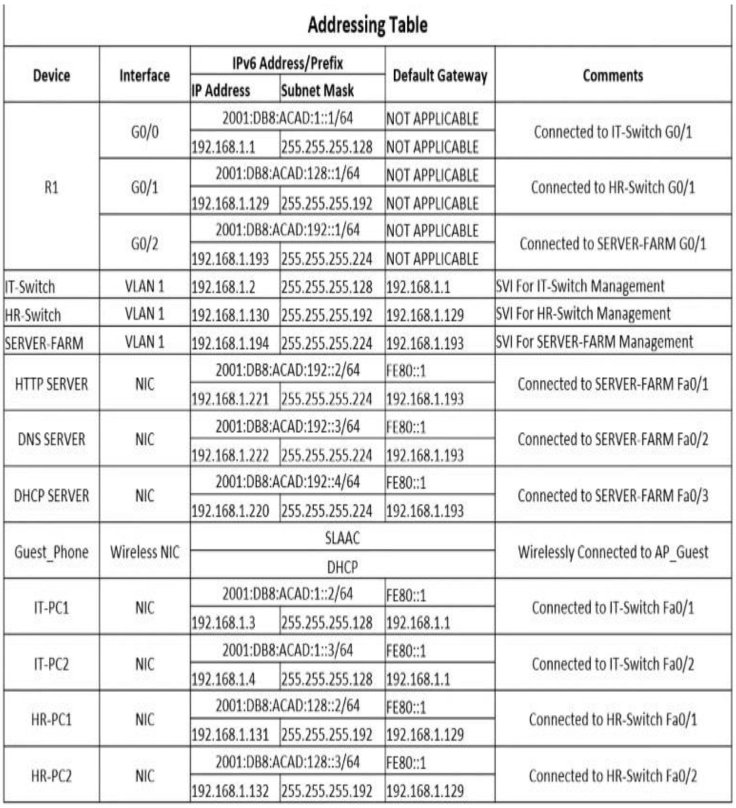


Network 2 (HR)

Addressing Table

Device	Interface	IPv6 Address/Prefix		Default Gateway	Comments
		IP Address	Subnet Mask		
R1	G0/1	2001:DB8:ACAD:128::1/64		NOT APPLICABLE	Connected to HR-Switch G0/1
		192.168.1.129	255.255.255.192	NOT APPLICABLE	
HR-Switch	VLAN 1	192.168.1.130	255.255.255.192	192.168.1.129	SVI For HR-Switch Management
HR-PC1	NIC	2001:DB8:ACAD:128::2/64		FE80::1	Connected to HR-Switch Fa0/1
		192.168.1.131	255.255.255.192	192.168.1.129	
HR-PC2	NIC	2001:DB8:ACAD:128::3/64		FE80::1	Connected to HR-Switch Fa0/2
		192.168.1.132	255.255.255.192	192.168.1.129	

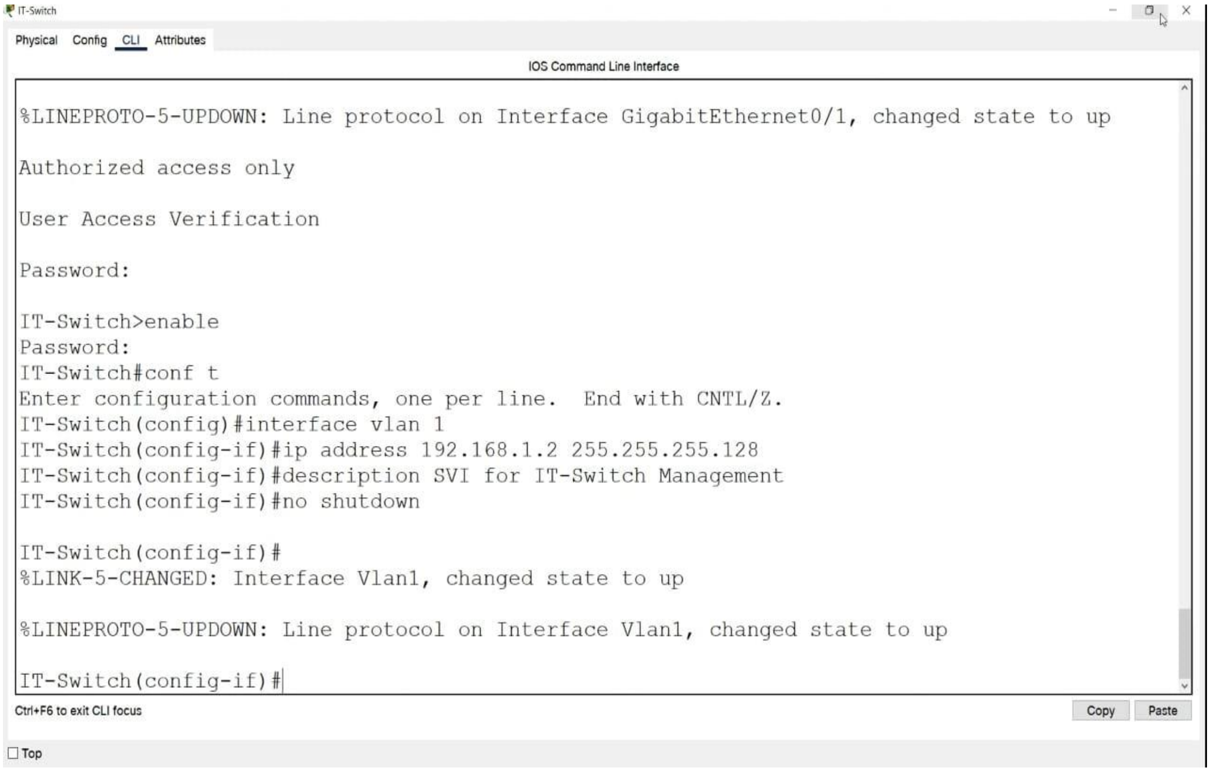
Figure 6



Addressing Table

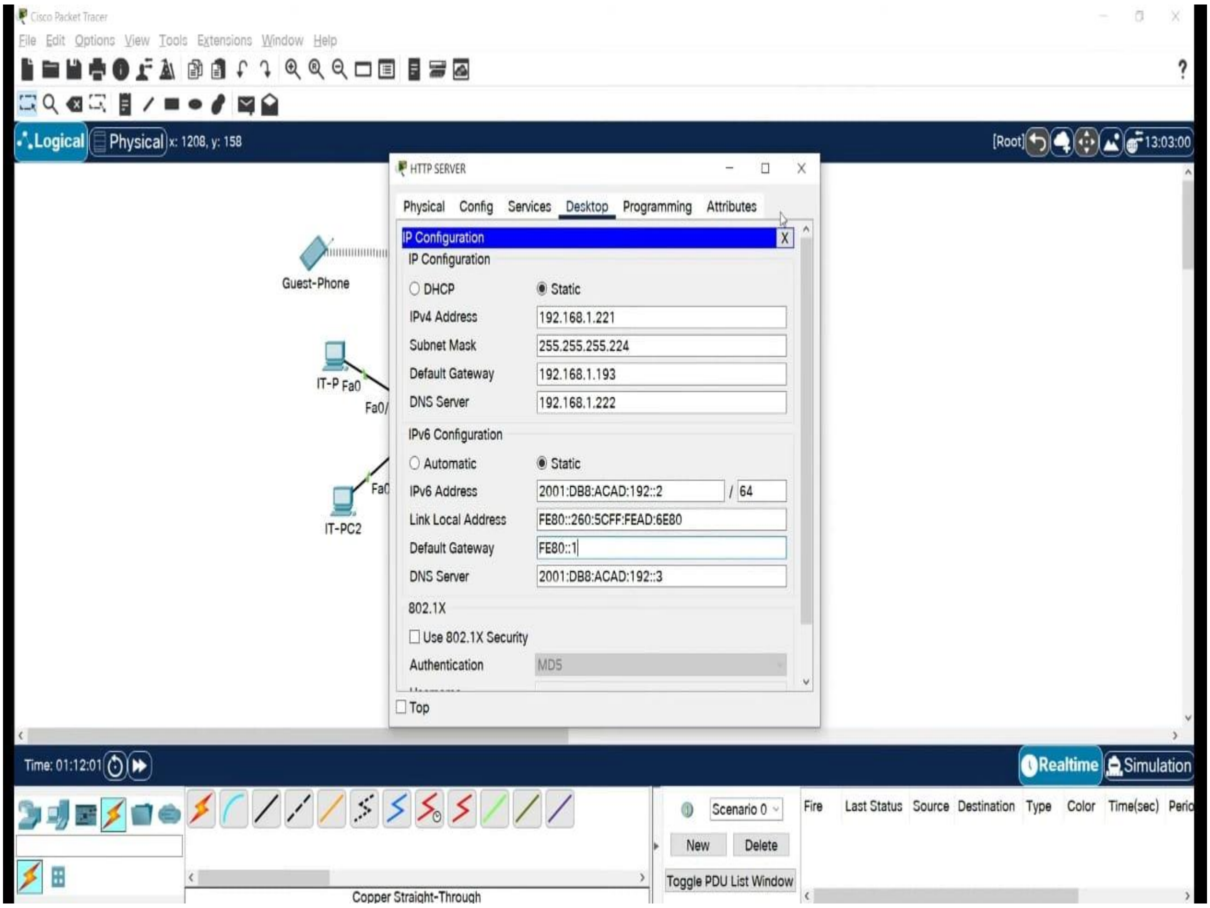
Device	Interface	IPv6 Address/Prefix		Default Gateway	Comments
		IP Address	Subnet Mask		
R1	G0/0	2001:DB8:ACAD:1::1/64		NOT APPLICABLE	Connected to IT-Switch G0/1
		192.168.1.1	255.255.255.128	NOT APPLICABLE	
	G0/1	2001:DB8:ACAD:128::1/64		NOT APPLICABLE	Connected to HR-Switch G0/1
		192.168.1.129	255.255.255.192	NOT APPLICABLE	
	G0/2	2001:DB8:ACAD:192::1/64		NOT APPLICABLE	Connected to SERVER-FARM G0/1
		192.168.1.193	255.255.255.224	NOT APPLICABLE	
IT-Switch	VLAN 1	192.168.1.2	255.255.255.128	192.168.1.1	SVI For IT-Switch Management
HR-Switch	VLAN 1	192.168.1.130	255.255.255.192	192.168.1.129	SVI For HR-Switch Management
SERVER-FARM	VLAN 1	192.168.1.194	255.255.255.224	192.168.1.193	SVI For SERVER-FARM Management
HTTP SERVER	NIC	2001:DB8:ACAD:192::2/64		FE80::1	Connected to SERVER-FARM Fa0/1
		192.168.1.221	255.255.255.224	192.168.1.193	
DNS SERVER	NIC	2001:DB8:ACAD:192::3/64		FE80::1	Connected to SERVER-FARM Fa0/2
		192.168.1.222	255.255.255.224	192.168.1.193	
DHCP SERVER	NIC	2001:DB8:ACAD:192::4/64		FE80::1	Connected to SERVER-FARM Fa0/3
		192.168.1.220	255.255.255.224	192.168.1.193	
Guest_Phone	Wireless NIC	SLAAC			Wirelessly Connected to AP_Guest
		DHCP			
IT-PC1	NIC	2001:DB8:ACAD:1::2/64		FE80::1	Connected to IT-Switch Fa0/1
		192.168.1.3	255.255.255.128	192.168.1.1	
IT-PC2	NIC	2001:DB8:ACAD:1::3/64		FE80::1	Connected to IT-Switch Fa0/2
		192.168.1.4	255.255.255.128	192.168.1.1	
HR-PC1	NIC	2001:DB8:ACAD:128::2/64		FE80::1	Connected to HR-Switch Fa0/1
		192.168.1.131	255.255.255.192	192.168.1.129	
HR-PC2	NIC	2001:DB8:ACAD:128::3/64		FE80::1	Connected to HR-Switch Fa0/2
		192.168.1.132	255.255.255.192	192.168.1.129	

Figure 7



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Authorized access only

User Access Verification

Password:

IT-Switch>enable
Password:
IT-Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IT-Switch(config)#interface vlan 1
IT-Switch(config-if)#ip address 192.168.1.2 255.255.255.128
IT-Switch(config-if)#description SVI for IT-Switch Management
IT-Switch(config-if)#no shutdown

IT-Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

IT-Switch(config-if)#
```

Figure 8



HTTP SERVER

Physical Config Services Desktop Programming Attributes

IP Configuration

IP Configuration

○ DHCP ● Static

IPv4 Address 192.168.1.221

Subnet Mask 255.255.255.224

Default Gateway 192.168.1.193

DNS Server 192.168.1.222

IPv6 Configuration

○ Automatic ● Static

IPv6 Address 2001:DB8:ACAD:192::2 / 64

Link Local Address FE80::260:5CFF:FEAD:6E80

Default Gateway FE80::1

DNS Server 2001:DB8:ACAD:192::3

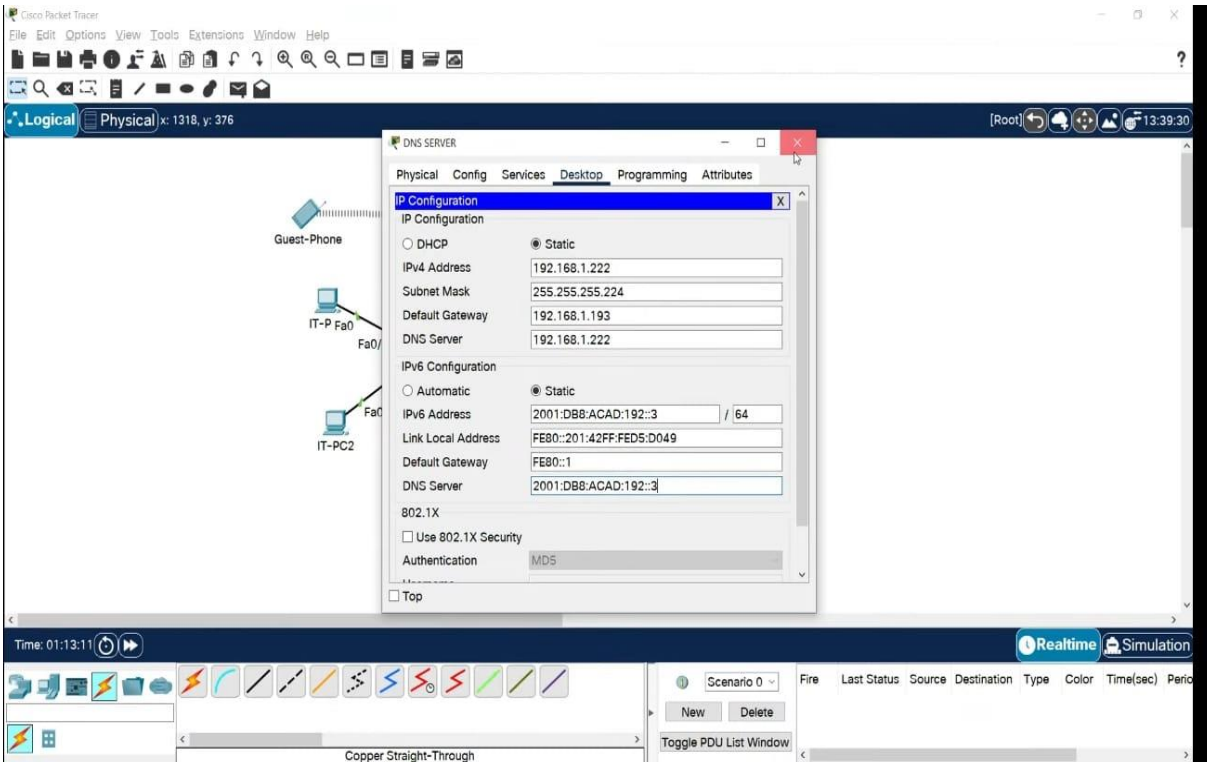
802.1X

□ Use 802.1X Security

Authentication MD5

□ Top

Figure 9



DNS SERVER

Physical Config Services Desktop Programming Attributes

IP Configuration

IP Configuration

○ DHCP ● Static

IPv4 Address 192.168.1.222

Subnet Mask 255.255.255.224

Default Gateway 192.168.1.193

DNS Server 192.168.1.222

IPv6 Configuration

○ Automatic ● Static

IPv6 Address 2001:DB8:ACAD:192::3 / 64

Link Local Address FE80::201:42FF:FED5:D049

Default Gateway FE80::1

DNS Server 2001:DB8:ACAD:192::3

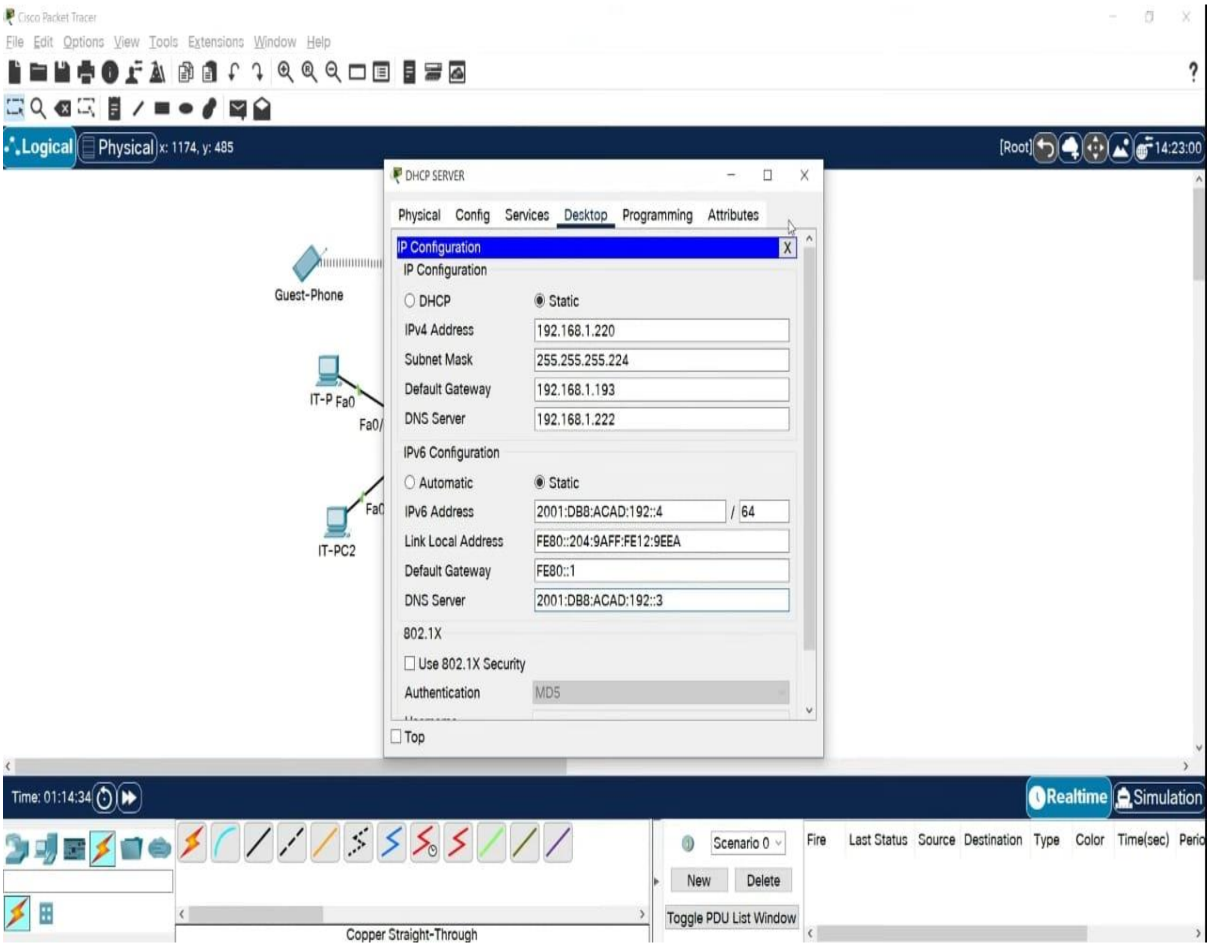
802.1X

□ Use 802.1X Security

Authentication MD5

□ Top

Figure 10



DHCP SERVER

Physical | Config | Services | Desktop | Programming | Attributes

IP Configuration

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.220

Subnet Mask: 255.255.255.224

Default Gateway: 192.168.1.193

DNS Server: 192.168.1.222

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: 2001:DB8:ACAD:192::4 / 64

Link Local Address: FE80::204:9AFF:FE12:9EEA

Default Gateway: FE80::1

DNS Server: 2001:DB8:ACAD:192::3

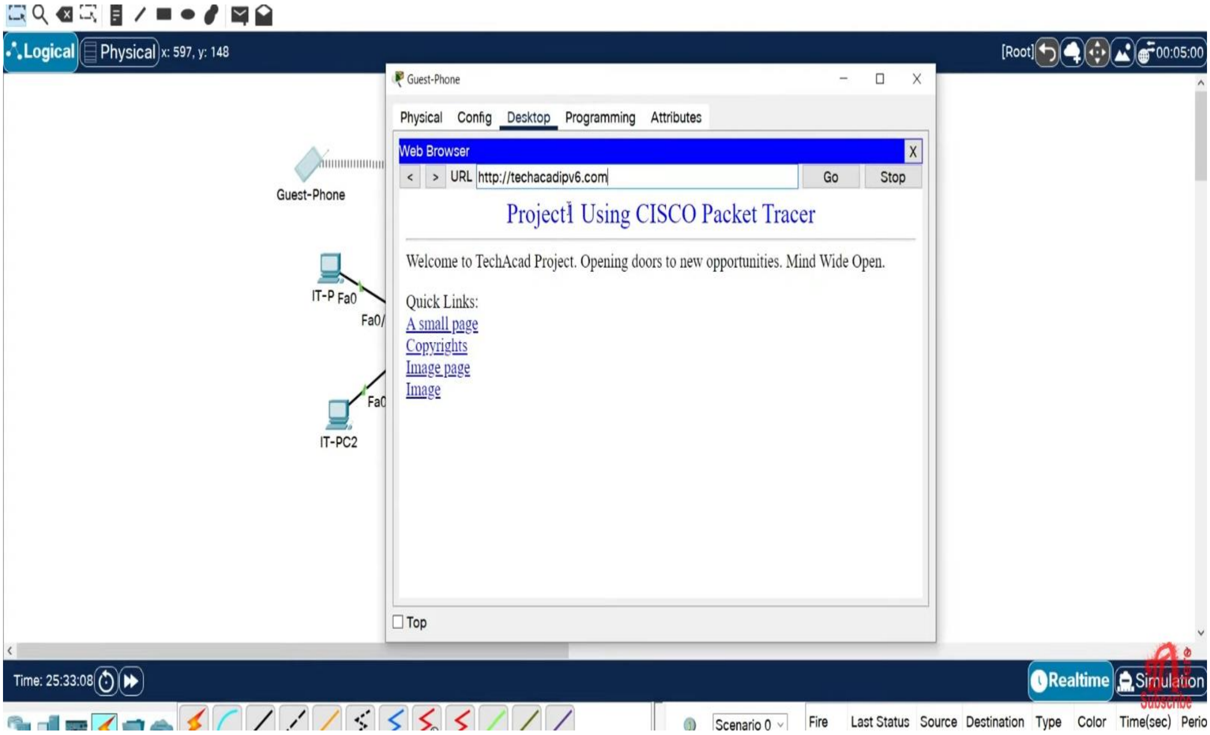
802.1X

□ Use 802.1X Security

Authentication: MD5

□ Top

Figure 11



Guest-Phone

Physical | Config | Desktop | Programming | Attributes

Web Browser

URL: http://techacadipv6.com

Go | Stop

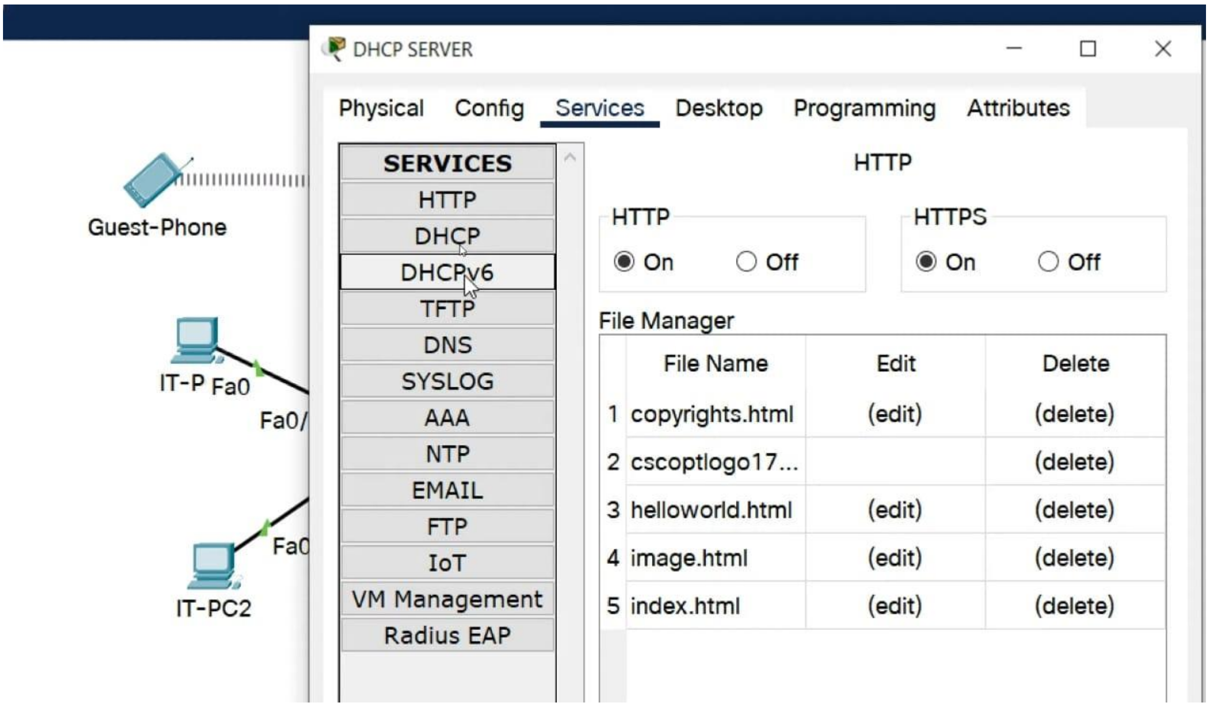
Project1 Using CISCO Packet Tracer

Welcome to TechAcad Project. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

□ Top

Figure 12



HTTP

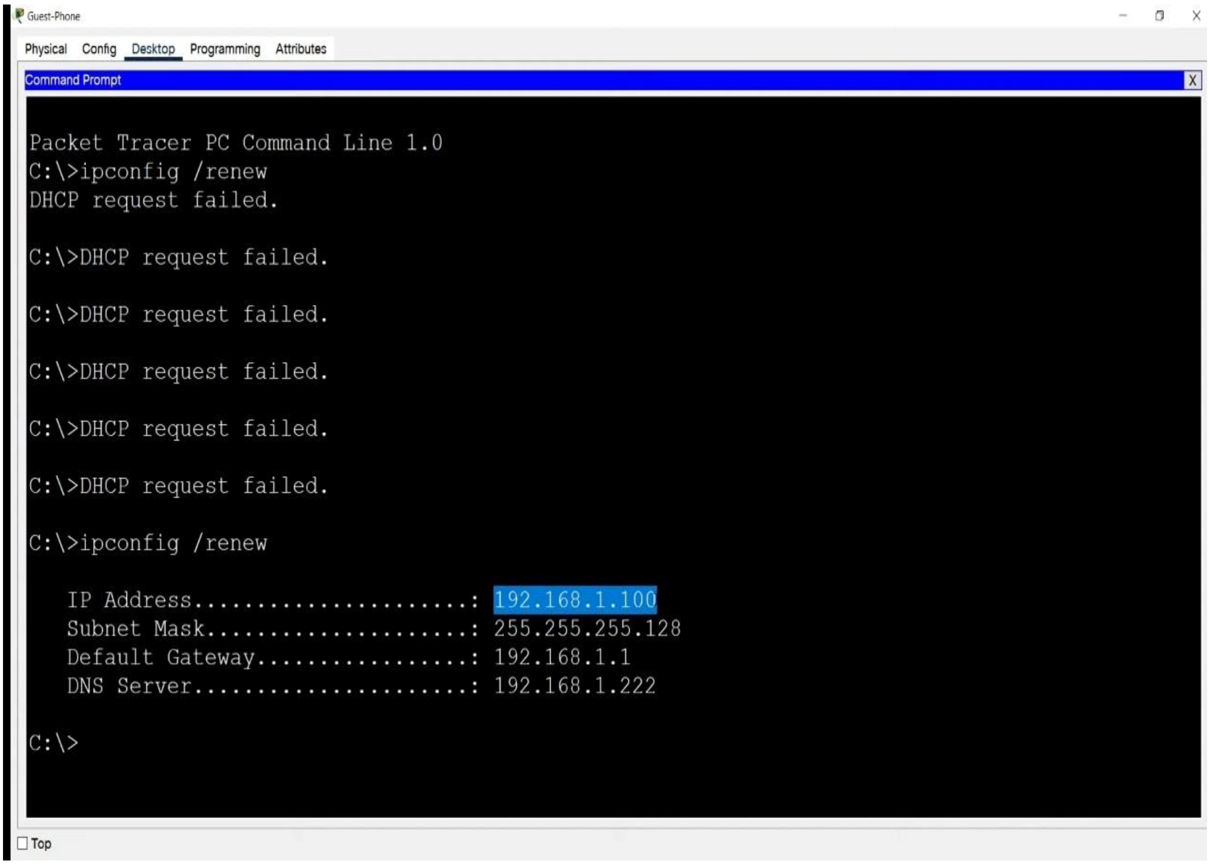
HTTP ● On ○ Off

HTTPS ● On ○ Off

File Manager

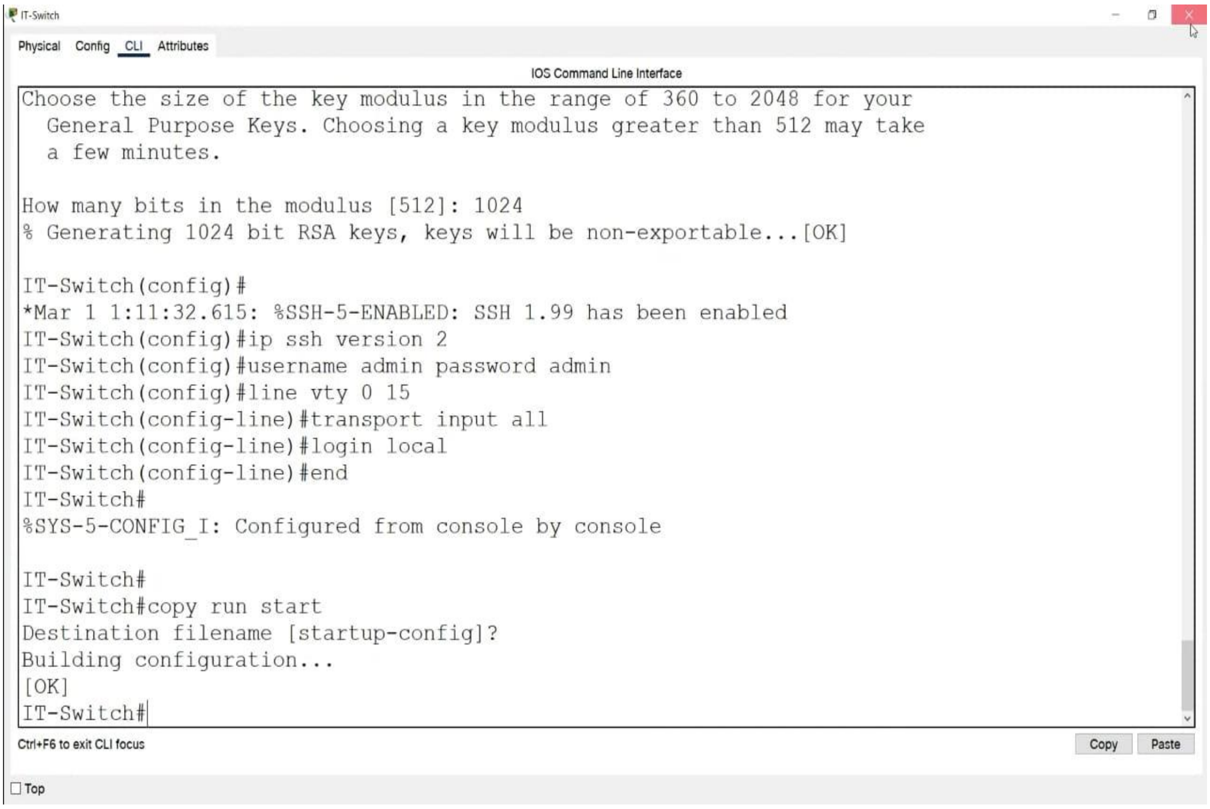
	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo17...		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

Figure 13



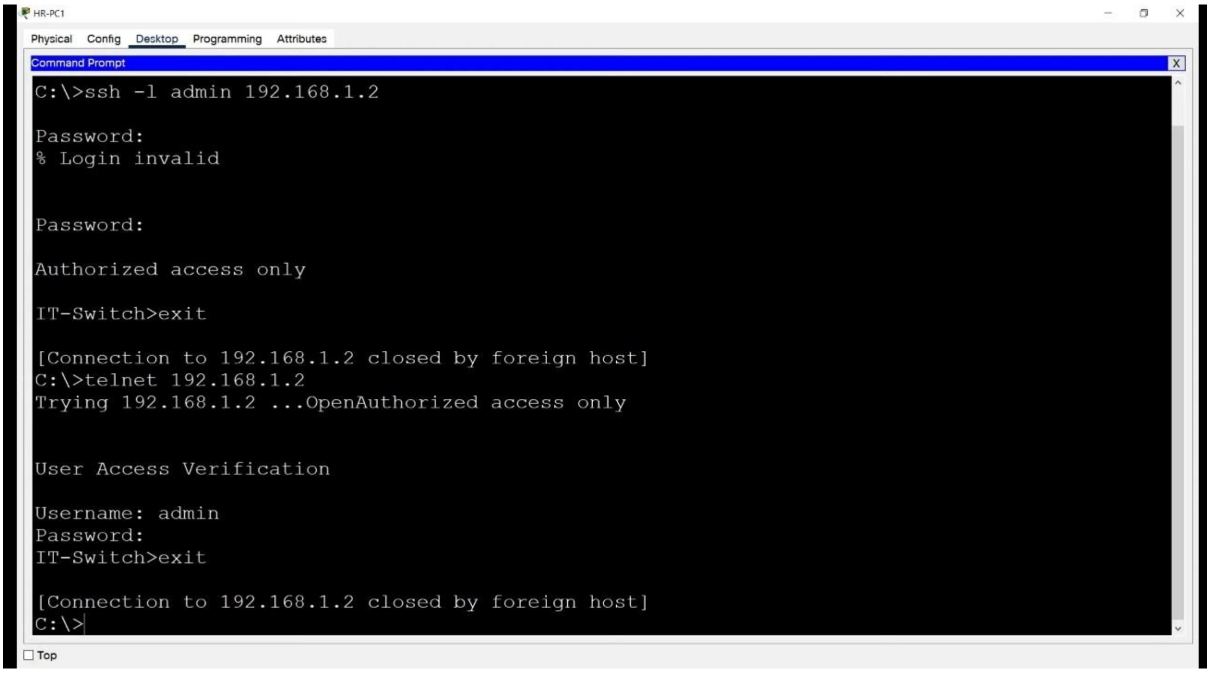
```
Packet Tracer PC Command Line 1.0
C:\>ipconfig /renew
DHCP request failed.

C:\>DHCP request failed.

C:\>DHCP request failed.

C:\>DHCP request failed.

C:\>DHCP request failed.

C:\>DHCP request failed.

C:\>ipconfig /renew

   IP Address......................: 192.168.1.100
   Subnet Mask.....................: 255.255.255.128
   Default Gateway.................: 192.168.1.1
   DNS Server......................: 192.168.1.222

C:\>
```

Figure 14



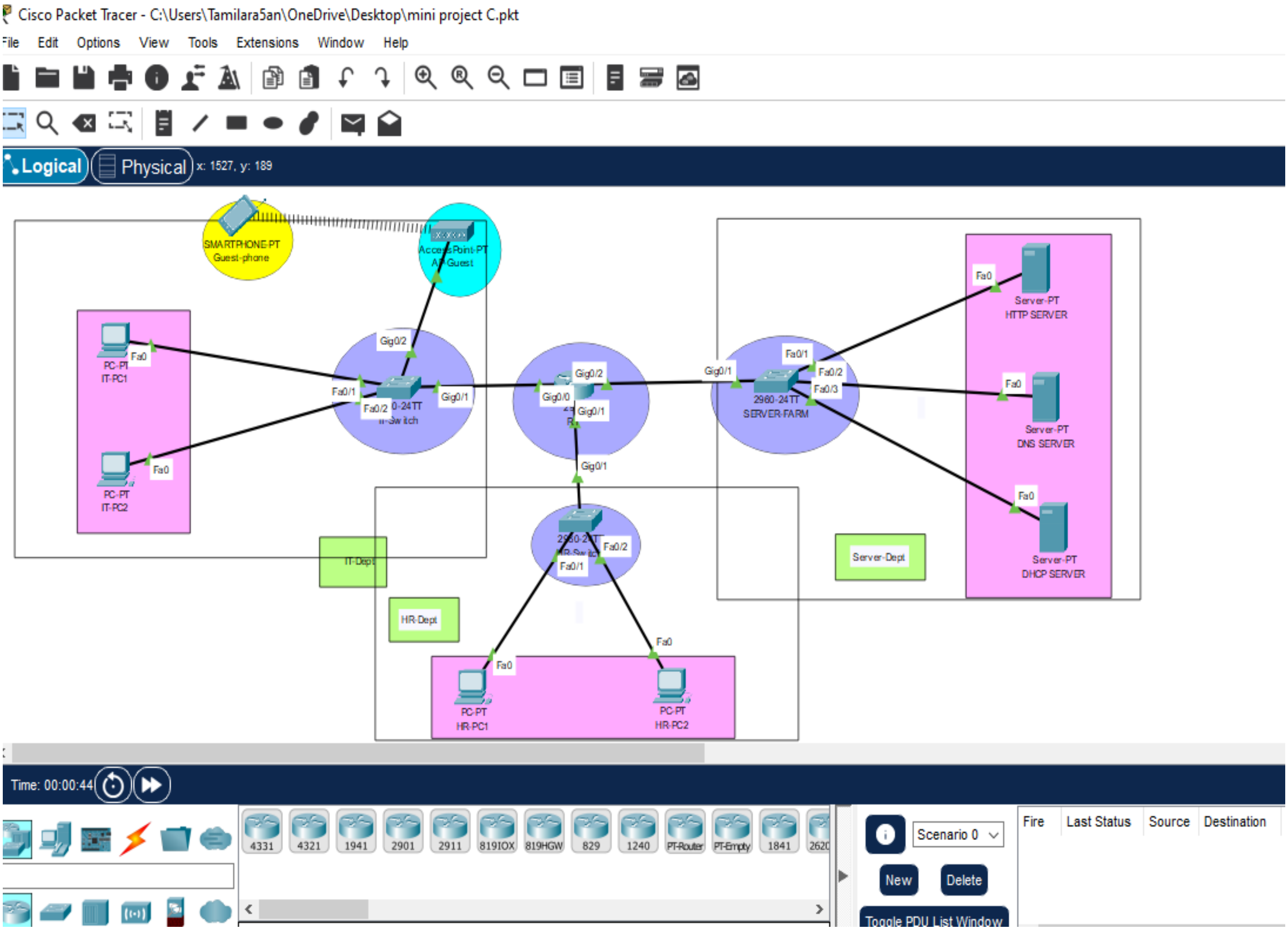
```
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

IT-Switch(config)#
*Mar 1 1:11:32.615: %SSH-5-ENABLED: SSH 1.99 has been enabled
IT-Switch(config)#ip ssh version 2
IT-Switch(config)#username admin password admin
IT-Switch(config)#line vty 0 15
IT-Switch(config-line)#transport input all
IT-Switch(config-line)#login local
IT-Switch(config-line)#end
IT-Switch#
%SYS-5-CONFIG_I: Configured from console by console

IT-Switch#
IT-Switch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
IT-Switch#
```

Figure 15



```
C:\>ssh -l admin 192.168.1.2

Password:
% Login invalid


Password:

Authorized access only

IT-Switch>exit

[Connection to 192.168.1.2 closed by foreign host]
C:\>telnet 192.168.1.2
Trying 192.168.1.2 ...OpenAuthorized access only


User Access Verification

Username: admin
Password:
IT-Switch>exit

[Connection to 192.168.1.2 closed by foreign host]
C:\>
```

Figure 16



Cisco Packet Tracer - C:\Users\Tamilara5an\OneDrive\Desktop\mini project C.pkt

Figure 17

CHAPTER 9

REFERECES

- Cisco Certified Network Associate Study Guide fifth edition by Todd Laemmle
- http://www.ciscopress.com/articles/article.asp?p=328773&seqNum=3
- Interconnecting Cisco Devices by Cisco
- Computer Networks-A top-down approach by Kurose and Ross.
- http://www.cisco.com/en/US/products/hw/routers/ps214/products _tech_note09186a00801f5d85.shtml
- http://www.symantec.com/connect/forums/sep-client-switch-computer-mode-user-mode-automatically and-moving-other-group

http://en.wikipedia.org/wiki/Router_(computing)