ENTERPRISE NETWORK DESIGN (CSCI-6649-03)

FUTURE TECH NATIONAL NETWORK

University of New Haven

Tagliatela College of Engineering

Enterprise Network Design Project

Network Case Study

By: **Group D**

Professor. Luis Rivera

Team

Sai Jaswanth Vadlamudi(00762306)

Akhila Parankusham(00810899)

Sai Aishwarya Edupuganti(00804915)

Sai Sruthi Mukka(00787662)

Sri Prabandha Vydya(00794465)

TABLE OF CONTENTS

Team Details……..…….01

Abstract……..…….……04

Phase 1……..…….……05
1.1 Customer Needs & Goals……..……..…….05
1.2 Business Goals……..……...……05
1.3 Technical goals……..……..…….....05
1.4 Characterizing the Existing Internetwork ……..……..…..06
1.5 Characterizing Network Traffic……..……...…07
1.6 Network Map…….……..…....……..08
1.6.1 Users…….……..08
Phase 2……09
2.1 Network Topology……..…….……09
2.2 Network Design…….…….…….……09
2.2.1 Network Diagram……....11
2.3 IP Addressing Scheme……..……..11
2.3.1 DHCP……..……...12
2.4 Network Applications…….……..13
2.4.1 User Communities…….……..14
2.4.2 Servers…….……15
2.4.3 Servers Information…….……15
2.5 Routing……..……..……...16
2.5.1 Static Routing……..…….……...16
2.5.2 Dynamic Routing……..……..16
2.5.2.1 OSPF…….……16
2.6 Redundancy……..……16
2.7 Cloud……..……...……...17
2.7.1 Blob Storage……...17
2.8 Wireless…….……...18
2.9 Network Security Strategies…….……....18
Phase 3……21
3.1 Cisco Packet Tracer……..……...….21
3.1.1 Implementation…….……..…..21
3.2 Configuring Network Devices …..……..……30
3.2.1 Configuring Switches…….……30
3.2.2 Configuring Multi-layer Switches…….……..31

3.2.3 Configuring Routers…..…….33
3.2.4 Configuring Firewall……...35
3.2.4 Configuring DHCP Server……...……...36
3.2.4 Configuring FTP Sever……...38
Phase 4……..…39
4.1 Testing……..…….39
4.1.1 Types of tests…….…….……..……..…….39
4.2 Network Testing …….……...……...…41

ABSTRACT

Future Tech National Network is a well-known and well-established software company in USA, which offers solutions and services to its clients. It started as a small enterprise which has one headquarters and one branch office, and it is successful in the market. We recognized that there are less employees and we couldn't meet the requirements for the number of hosts. We considered recruiting employees for other roles. So, we will be designing a network which can support all the employees who are working at the same time for various services and can be used for future use. As there are many employees, one of the problems in our office is that project files are often collided and misplaced with other department files as there are many departments. So, we want to isolate each department. Each department will be treated as a separate segment. As the number of employees increased, the office became crowded with people which is becoming difficult for employees to work. So, we will be extending our network by adding more departments. As the customers' requests are increasing daily, we are trying to set up branch offices of the same architecture as our headquarters and develop a safe path for the flow of data from one branch to another thus reaching the customer safely and securely.

PHASE 1

1.1 Customer Needs & Goals

- Isolation of departments.
- Secured communication between headquarters and branch network.
- Designing a network to address future requirements.
- Configuring servers to provide web, email services and file transfer.
- Perfect balance between CIA triad.
- Security measures such as firewalls to be installed.

1.2 Business Goals

- Increasing revenue and profit.
- Offering better customer support.
- Offering new customer services.
- Modernizing outdated technologies.
- Avoiding business disruptions caused by network security problems and natural disasters.
- Reliability, cost-effectiveness, flexibility, and performance.
- Increase market share.
- Expand into new markets.
- Increase employee productivity.
- Reduce telecommunications and network costs, including overhead associated with separate networks for voice, data, and video.
- Comply with IT architecture design and governance goals.

1.3 Technical Goals

Scalability: The ability of a network to grow and handle increased traffic is known as scalability. The network design proposed to a customer should be able to adapt the future usage and expansion.

Network Performance: Slow or unreliable networks can impact employee's productivity, customer satisfaction, and even the bottom line. That's why it's important to carefully design networks to ensure optimal performance. It can be

guaranteed by using the right equipment, optimizing your network traffic, and troubleshooting any potential problems. The network parameters include throughput, accuracy, delay(latency), delay variation, response time, etc..

Security: This includes firewalls, antivirus software, and intrusion detection systems. It is also important to keep systems up to date with the latest security patches.

Usability: It refers to the ease of use with which network users can access the network and services. It includes ensuring that users can easily find the resources they need, setting up adequate user permissions, and providing clear instructions on how to use the network.

Adaptability: The ability to adapt itself efficiently and fast to changed circumstances. A good network design can adapt to new technologies and changes. Changes can come in the form of new protocols, new business practices, new fiscal goals, new legislation, and many other possibilities.

Availability: It refers to the ability of a network to provide access to network resources and services at all times, without interruption or downtime. It is measured as a percentage of uptime, or the amount of time that the network is operational and accessible to users.

Manageability: It refers to the ease with which a network can be managed and maintained. This includes configuration, monitoring, troubleshooting, and upgrading.

Affordability: It refers to the cost-effectiveness of a network solution. This includes the costs of purchasing and deploying network hardware and software along with the ongoing costs of maintenance, support, and upgrades.

1.4 Characterizing the Existing Internetwork

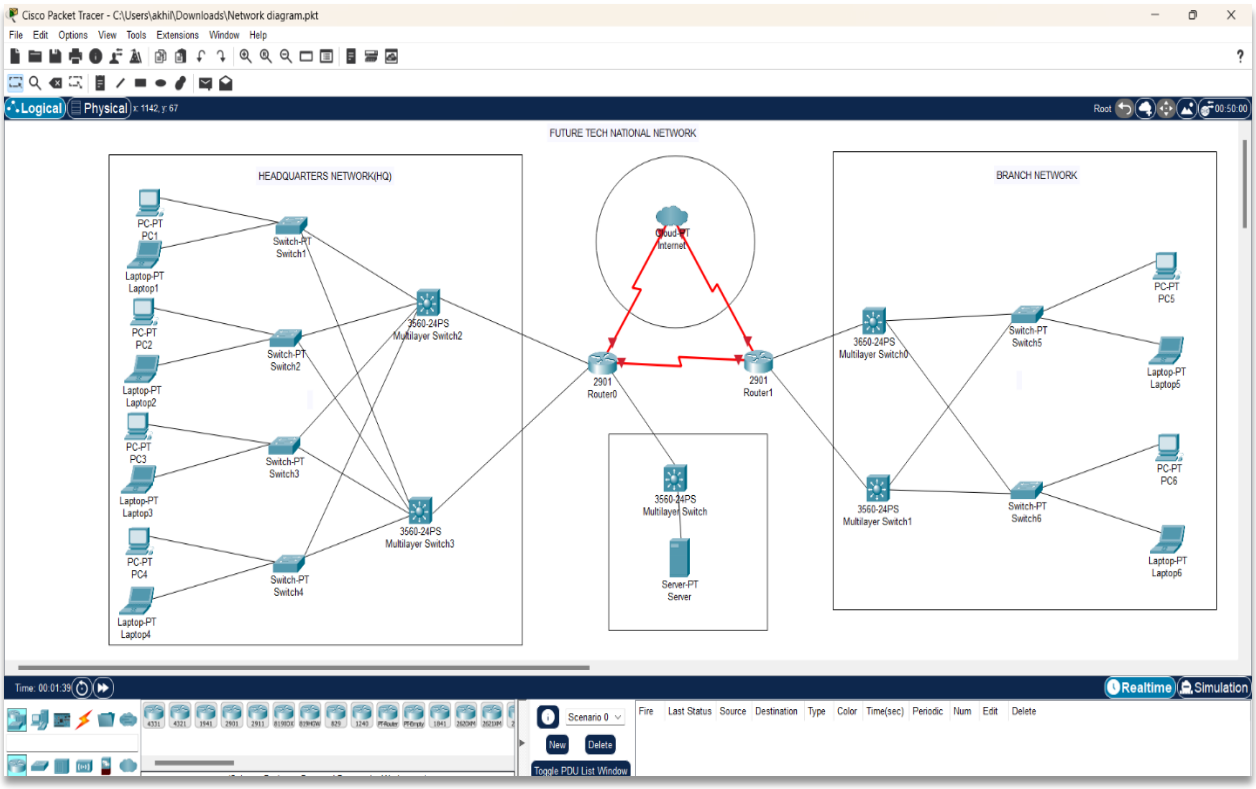
- Developing a network map.
- Characterizing large internetworks.
- Characterizing the logical architecture.
- Developing a modular block diagram.
- Characterizing Network addressing and naming.
- Characterizing wiring and media.

- Checking the health of the existing internetwork.
- Analyzing Network Availability
- Analyzing Network Utilization and Accuracy.
- Checking Architectural and Environmental Constraints.
- Checking a site for a wireless installation and checking issues for it.
- Checking the status of major routers, switches, firewalls, and other tools.

1.5 Characterizing Network Traffic

- Identifying Major Traffic Sources and Stores.
- Documenting Traffic Flow on the Existing Network.
- Characterizing Types of Traffic Flow for New Network Applications.
- Documenting Traffic Flow for New and Existing Network Applications.
- Characterizing Traffic Load.
- Calculating Theoretical Traffic Load.
- Documenting Application-Usage Patterns.
- Refining Estimates of Traffic Load caused by Applications.
- Estimating Traffic Load Caused by Routing Protocols.
- Characterizing Traffic Load.
- Network Efficiency.
- Characterizing Quality of Service requirements.
- Documenting Quality of Service requirements.

1.6 NETWORK MAP



1.6.1 Users

Number of users:

- Headquarters: 20 users.
- Branch Network: 10 to 12 users in each department.
- Server: 1

PHASE 2

2.1 NETWORK TOPOLOGY

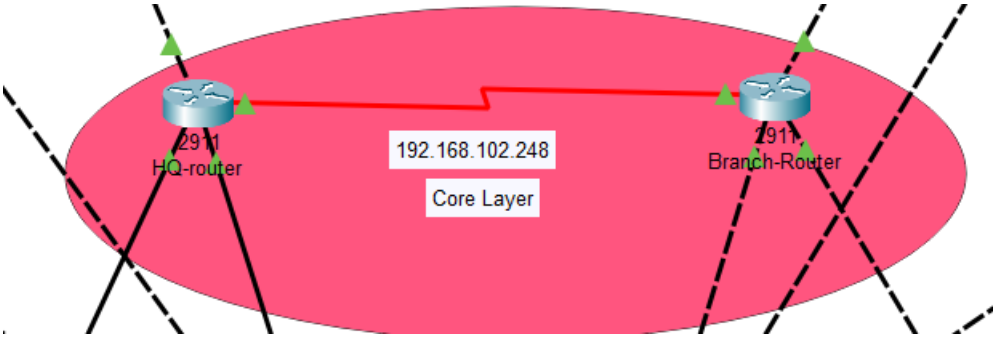
It refers to the physical and logical arrangement of network nodes and how they are connected to one another.

2.2 NETWORK DESIGN

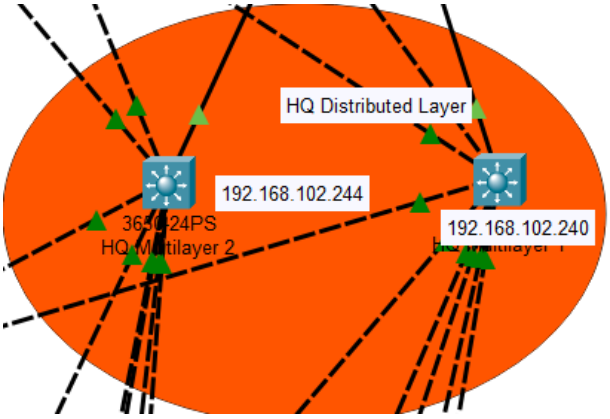
It refers to the process of planning and implementing a computer network infrastructure to meet the needs of an organization. It involves the creation of a network topology, the selection of appropriate hardware and software components, the configuration of network devices, and the implementation of security measures to protect the network.

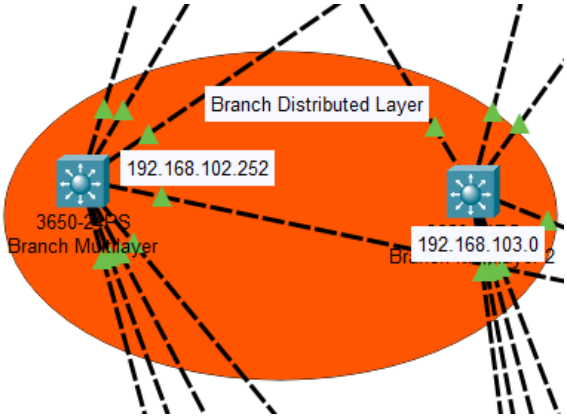
- ❖ The hierarchical network design consists of three main layers and each layer has its own specific functions and responsibilities. The three primary layers in a network design are:

Core Layer: The core layer is responsible for high-speed packet forwarding and serves as the backbone of a network. The core layer provides interconnectivity between distribution layer devices. It usually consists of high-speed devices, like high end routers and switches with redundant links.

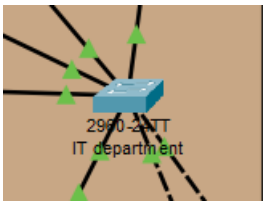


Distribution Layer: It serves as the communication point between the access layer and the core. Its primary functions are to provide routing, filtering, and WAN access and to determine how packets can access the core. This layer determines the fastest way that network service requests are accessed – for example, how a file request is forwarded to a server – and, if necessary, forwards the request to the core layer. This layer usually consists of routers and multilayer switches.

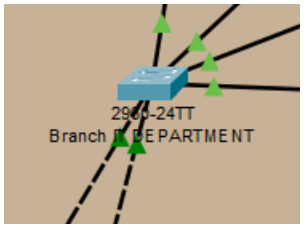




Access Layer: This layer is the closest to end-user devices, such as computers, printers, or IP phones. Its main purpose is to provide connectivity to end devices and enforce security policies at the network edge. Access layer switches connect to end devices and operate at lower speeds compared to the distribution and core layers.



Headquarters



Branch Network

The network design offers various advantages, and they are:

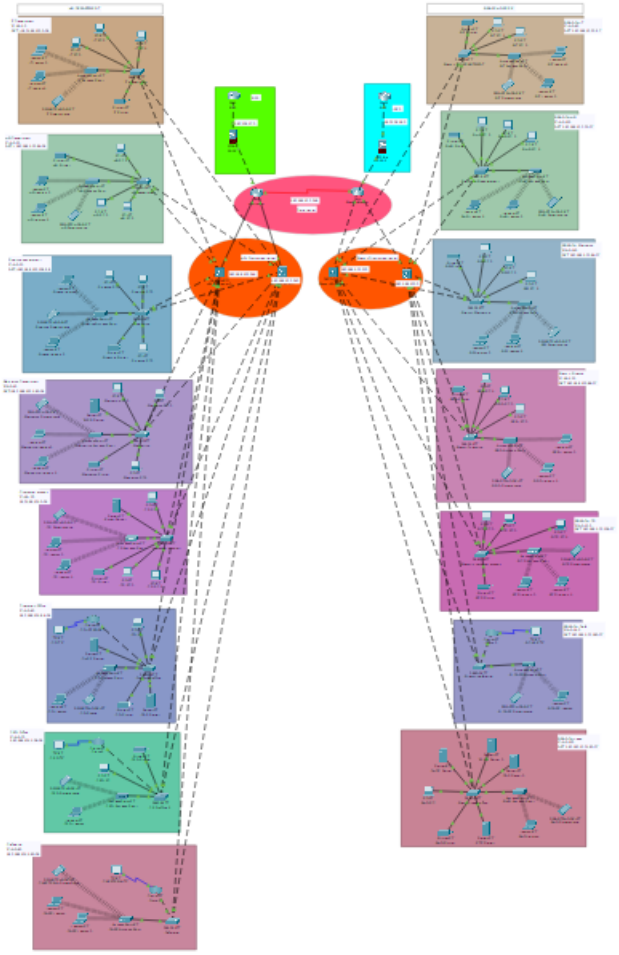
Scalability: The layered structure allows for easy scalability as new devices or users can be added at the access layer without impacting the core or distribution layers. The modular design facilitates network expansion without significant disruptions.

Improved Performance: By optimizing traffic flows and using policy-based routing at the distribution layer, the hierarchical design enhances network performance. It reduces unnecessary traffic across the core layer and enables faster and more efficient communication between devices.

Enhanced Security: The distribution layer serves as a security boundary, allowing the implementation of access control policies and traffic filtering. Controlling access at this layer enhances network security by isolating and securing different segments of the network.

2.2.1 NETWORK DIAGRAM

The logical network diagram is:



2.3 IP Addressing Scheme

An IP (Internet Protocol) address is a unique numerical identifier assigned to every device connected to a computer network that uses the Internet Protocol for communication. An IP address consists of a network portion and a host portion, and it enables devices to communicate with each other within a network and across the internet. An IP addressing scheme is a plan for allocating and managing IP addresses within a network. It is a critical aspect of network design and management, as it helps ensure that devices can communicate with each other and access network resources effectively.

We used Class C to allocate IP addresses in our network. Our base network starts from 192.168.100.0.0(192.168.100.0, 192.168.101.0 etc.) We used DHCP to assign IP addresses automatically for end users and for intermediate devices like routers, we will be assigning it manually.

2.3.1 Dynamic Host Configuration Protocol (DHCP)

It automates the assignment of IP addresses and other network configuration parameters to devices on a network. DHCP enables automated assignment of IP addresses, eliminating the need to manually configure IP addresses for every device, simplifying network management.

The advantages of using DHCP include efficient Ip address management, reduced network administration, reduced Ip address conflicts, centralized network configuration, rapid network deployment, etc.

The IP addresses are assigned to each department in headquarters and branch network. They are as follows:

HEADQUARTERS

Department	VLAN	IP Address Range
IT	10	192.168.100.0/26 - 192.168.100.63/26
HR	20	192.168.100.64/26- 192.168.100.127/26
Finance	30	192.168.100.128/26 - 192.168.100.191/26
Marketing	40	192.168.100.192/26 - 192.168.100.255/26
Customer Support	50	192.168.101.0/26 - 192.168.101.63/26
Chairman Office	60	192.168.101.64/26 - 192.168.101.127/26

CEO Office	70	192.168.101.128/26 - 192.168.101.191/26
Cafeteria	80	192.168.101.192/26 - 192.168.101.255/26

BRANCH NETWORK

Department	VLAN	IP Address Range
IT	90	192.168.102.0/27 - 192.168.102.31/27
HR	100	192.168.102.32/27 - 192.168.102.63/27
Finance	110	192.168.102.64/27 - 192.168.102.95/27
Marketing	120	192.168.102.96/27 - 192.168.102.127/27
Customer Support	130	192.168.102.128/27 - 192.168.102.159/27
CEO Office	140	192.168.102.160/27 - 192.168.102.191/27
Cafeteria	150	192.168.102.192/27 - 192.168.102.223/27

2.4 Network Applications

These are software programs designed to communicate over a network and provide services to the users. There are different types of network applications used in this design and they are :

App 1 = Email Application

App 2 = Web Application

App 3 = Cloud Application

App 4 = Customer Application

App 5 = File transfer Application

2.4.1 User Communities

A user community is a set of workers who use a particular application or set of applications.

HEADQUARTERS

Department	Community Size	Applications Used
IT	62	Web, Cloud, and Email
HR	62	Email
Finance	62	Web and Email
Marketing	62	Email
Customer Support	62	Email, Web, and File
Chairman Office	62	Email and Web
CEO Office	62	Email and Web
Cafeteria	62	Email and Customer
Outside Users	More than 5000	Surfing the website

BRANCH NETWORK

Department	Community Size	Applications Used
IT	30	Web, Cloud, and Email
HR	30	Email

Finance	30	Web and Email
Marketing	30	Email
Customer Support	30	Email, Web, and File
CEO Office	30	Email and Web
Cafeteria	30	Email and Customer
Outside Users	More than 3000	Surfing the website

2.4.2 Servers

To deliver secure and reliable services to clients, this network requires a secure datastore model. To ensure secure and dependable transactions, the company employs a range of security protocols.

Server is a computer system or a software application that provides a specific functionality or service to other devices in a network. One of the primary functions is to store and manage data that is accessible to other devices on the network.

The servers which are used in our networking include:

- Web Server.
- File Server.
- Email Server.
- DHCP Server.
- DNS Server.

2.4.3 Servers Information

Servers	Location	Application	Used by the community users
Web Server	IT Department	HTTPS	All
File Server	IT Department	FTP	All
Email Server	IT Department	SMTP	All

DHCP Server	IT Department	DHCPD	All except customers
DNS Server	IT Department	DHCPD	All except customers

SERVER

VLAN 160

IP Address Range:192.168.102.224-192.168.102.255/28

2.5 Routing: Routing plays one of the important roles in designing a network. It is defined as delivering packets from source to destination through a network of interconnected devices such as routers, switches, and other networking devices. It will also help us in deciding the efficient path for data to travel based on a set of routing protocols and other factors such as network topology, traffic load, etc.

There are two types of routing: static routing and dynamic routing.

2.5.1 Static Routing: Routes are manually configured by a network administrator in static routing. In dynamic routing, routes are automatically chosen by routing protocols based on current network knowledge.

- Firewalls and ISP's are configured using static routing in the network.

2.5.2 Dynamic Routing: In dynamic routing, routes are automatically chosen by routing protocols based on current network knowledge.

2.5.2.1 OSPF: It is a link-state routing protocol that was developed for IP networks and is based on the Shortest Path First (SPF) algorithm. It uses link-state routing protocol to create a database of network topology information. This contains information about the state of each router and the status of all links in the network. The routers use this database to calculate the shortest path to each destination in the network and will deliver the packets accordingly. With the help of this protocol, even if there are any changes in the topology, such as router is added or removed, then the network adapts to the network quickly. We can make sure that the network remains efficient and reliable, even when the conditions change.

- Multi-layer switches and routers are configured using dynamic routing in the network.

2.6 Redundancy: In networking, redundancy refers to the duplication of essential systems or components inside a network to make sure the network is still functional in the case of a breakdown. Redundant hardware, network connections, power supply, or data centers are just a few examples of this redundant infrastructure.

To ensure that important systems continue to function even if one or more components fail, redundancy aims to remove single points of failure from the network. For instance, redundant switches can easily replace a failing network switch, maintaining network connectivity.

Redundancy in networking has several advantages. They are:

- Improved network availability.
- Increased network reliability.
- Improved network performance.

2.7 Cloud

Cloud storage is a service that enables users to store, manage, and access data and files over the internet. It is an integral part of networking, providing businesses and individuals with scalable and flexible solutions for data storage and backup.

2.7.1 Blob Storage

Blob storage is a type of cloud storage that is specifically designed for storing unstructured data, such as images, videos, audio files, and documents. It offers several advantages. They are:

- Cost-Effective.
- Scalability.
- Durability.
- Accessibility.
- Security.
- Integration with other services.

2.8 Wireless

Wireless networking, also known as Wi-Fi, refers to the use of radio waves to enable devices to communicate with each other over a network without the need for physical cables. It enables users to access the internet and communicate with each other from anywhere, at any time.

The advantages of Wi-Fi are:

- Mobility.
- Ease of set-up.
- Cost-effective.
- Convenience.
- Remote management.

2.9 Network Security Strategies

Network security is the practice of protecting a computer network from unauthorized access, misuse, modification, or destruction. It involves implementing various measures and strategies to ensure the confidentiality, integrity, and availability of network resources and data.

Various security mechanisms that are used in the network design to ensure the safety of the data are:

- Physical Security.
- Authorization.
- Authentication.
- Firewall.
- Data Encryption using AES.

Physical Security: Physical security applies to restricting access to critical network resources by locking them away and protecting them from natural and man-made disasters. Physical security can safeguard a network against inexperienced personnel and contractors misusing network equipment inadvertently. It can also defend the network from walk-in hackers, competitors, and terrorists who change equipment configurations.

Authentication: Authentication establishes the identity of the person requesting network services. Although it can also refer to authenticating equipment or software

processes. Some routing protocols, for example, enable route authentication, which requires a router to meet certain requirements before another router accepts its routing changes. Authentication basically depends on three important factors :

- Something the user has.
- Something the user knows.
- Something the user is.

Authorization : Authentication determines who has access to network resources; authorization determines what they can do once they have. Processes and users are granted privileges through authorization. A security administrator can control elements of a network via authorization.

Firewall: Firewalls are devices or software programs that control, and filter network traffic based on predefined security policies, preventing unauthorized access and potential threats from entering the network.

There are three types of firewalls. They are Packet filtering firewalls, Stateful inspection firewalls and Application-level gateways.

Application-level gateways: They are also known as proxy servers, work by intercepting network traffic and acting as an intermediary between the client and the server. The gateway examines the entire data stream, including the content of each packet, before forwarding it to its destination. This type of firewall is more secure than packet filtering and stateful inspection firewalls. This firewall is used in the design.

The advantages of using firewall in the network are:

- Monitors network traffic.
- Stops virus attacks.
- Stops spyware.
- Promotes Privacy.
- Network performance optimization.

Data Encryption: Encryption fumbles data to prevent it from being read by anybody other than the intended recipient. Before sending data over a network, an encryption device encrypts it. Before delivering data to an application, a decryption device decrypts it. An encryption or decryption device can be a router, server, end system,

or dedicated device. Ciphered data is data that has been encrypted. Plain text refers to data that is not encrypted. The purpose of encryption is to ensure that even if the technique is known, an intruder cannot decipher the communication without the necessary key. A secret key is the name for this type of key. A symmetric key is one in which both the sender and the recipient utilize the same secret key. A symmetric key system is well known as the Data Encryption Standard.

AES Encryption: AES (Advanced Encryption Standard) is a widely used symmetric encryption algorithm that provides strong security for data in transit or at rest.

One of the key advantages of AES is its ability to provide strong security while maintaining relatively fast encryption and decryption speeds. AES is a symmetric encryption algorithm, which means that the same key is used for both encryption and decryption. This key is kept secret to maintain the security of the encrypted data. AES is available in several different key sizes, with 128-bit, 192-bit, and 256-bit key sizes being the most used. As the key size increases, so does the security of the encrypted data, but also the computational resources required for encryption and decryption. We used 256-bit key encryption.

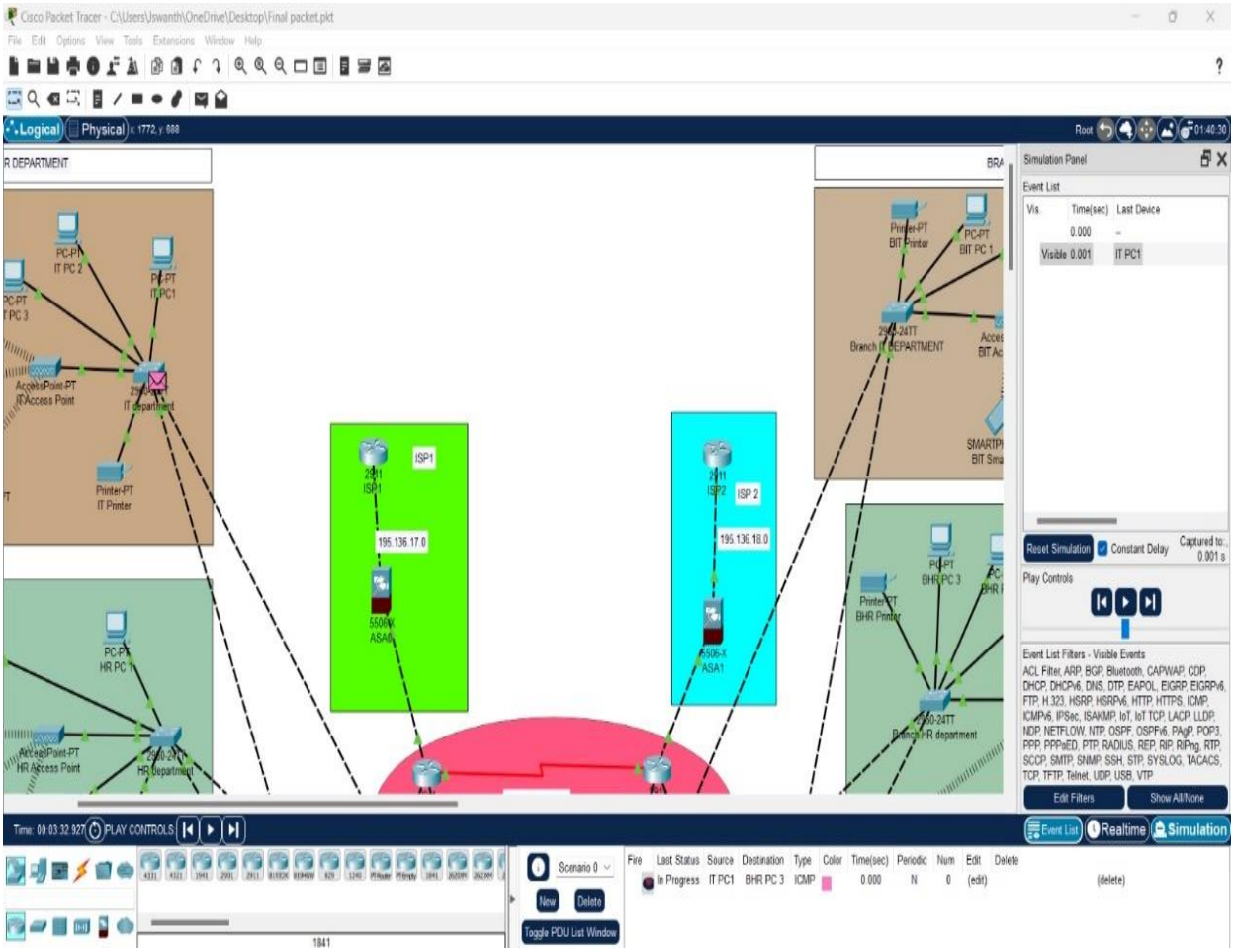
The advantages of AES encryption are strong security, wide adoption, fast and efficient, flexible key sizes, resilience to attacks, etc.

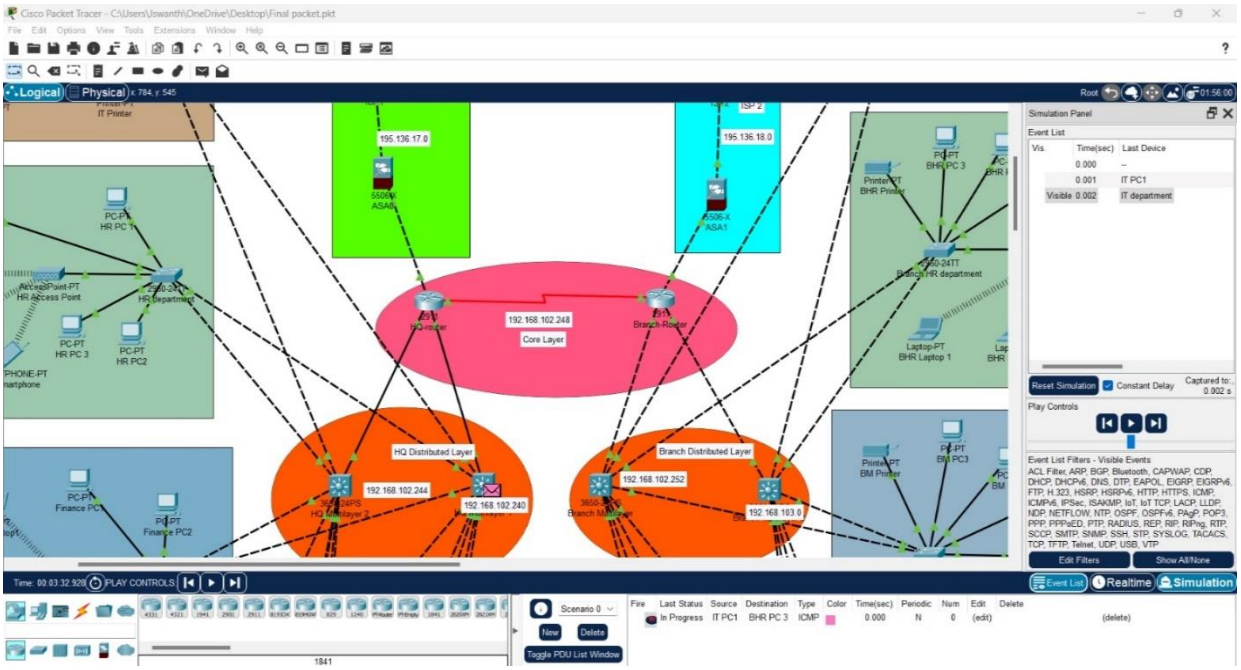
PHASE 3

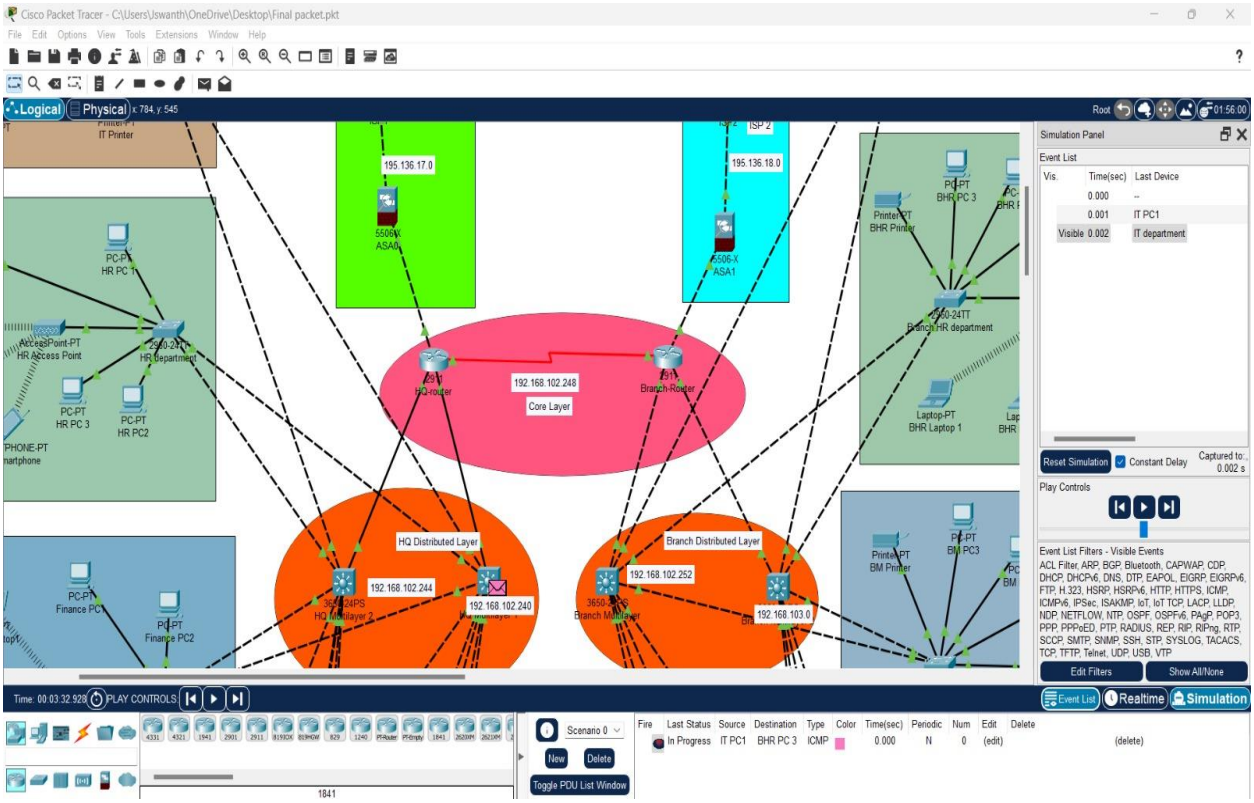
3.1 Cisco Packet Tracer

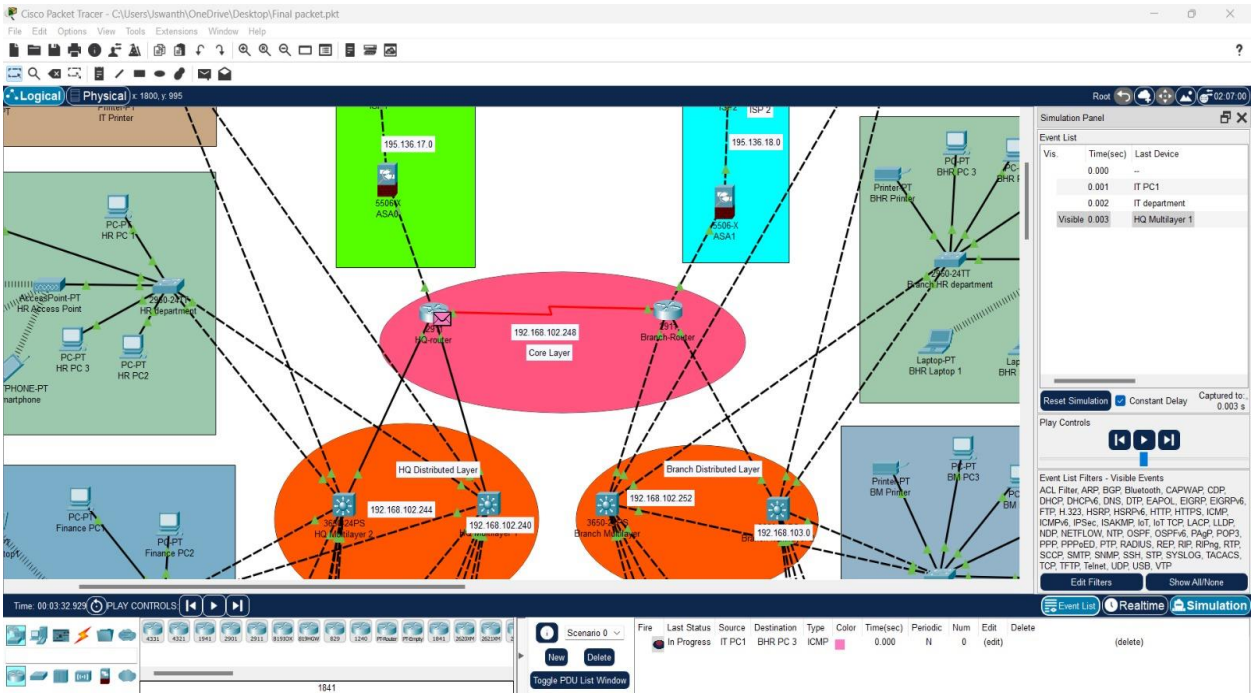
- Cisco Packet Tracer is a visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks.
- Using packet tracer, we have implemented network topology, assigned routers and switches.
- We can also configure each router and network with the IP address and test whether the data transfer is successful or not.

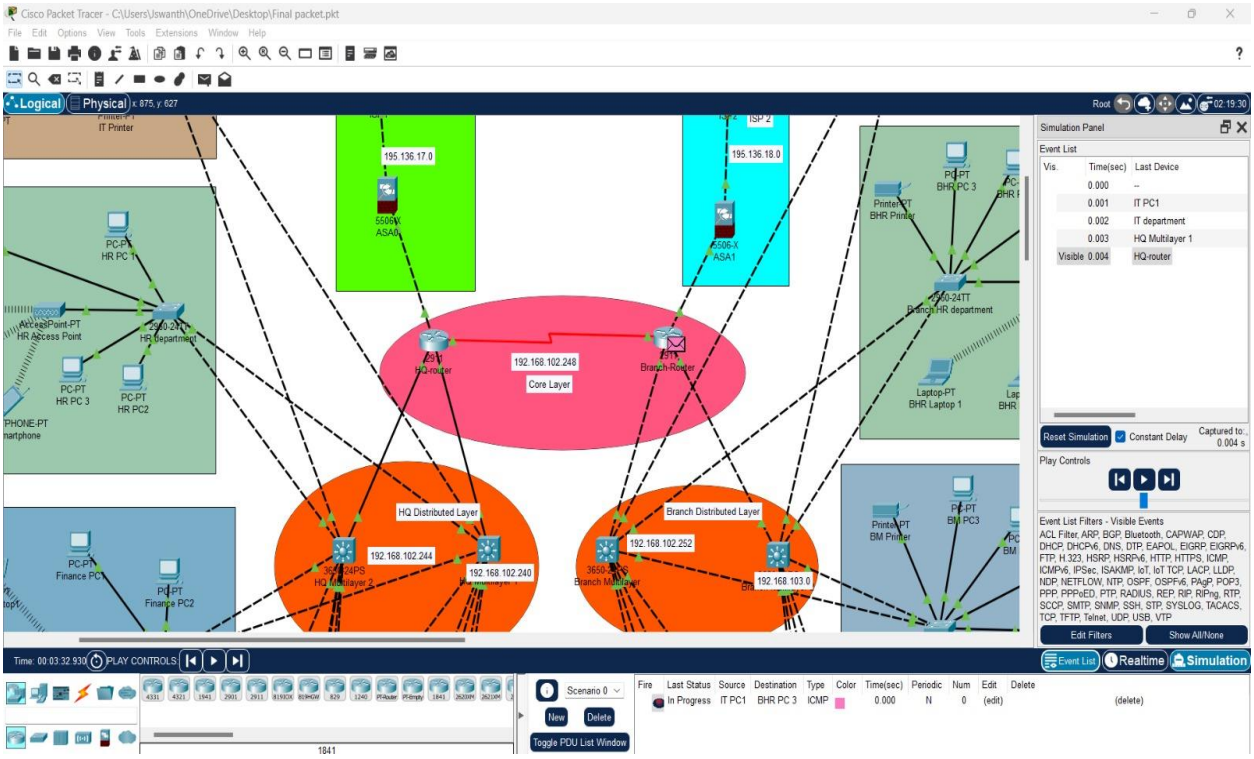
3.1.1 Implementation

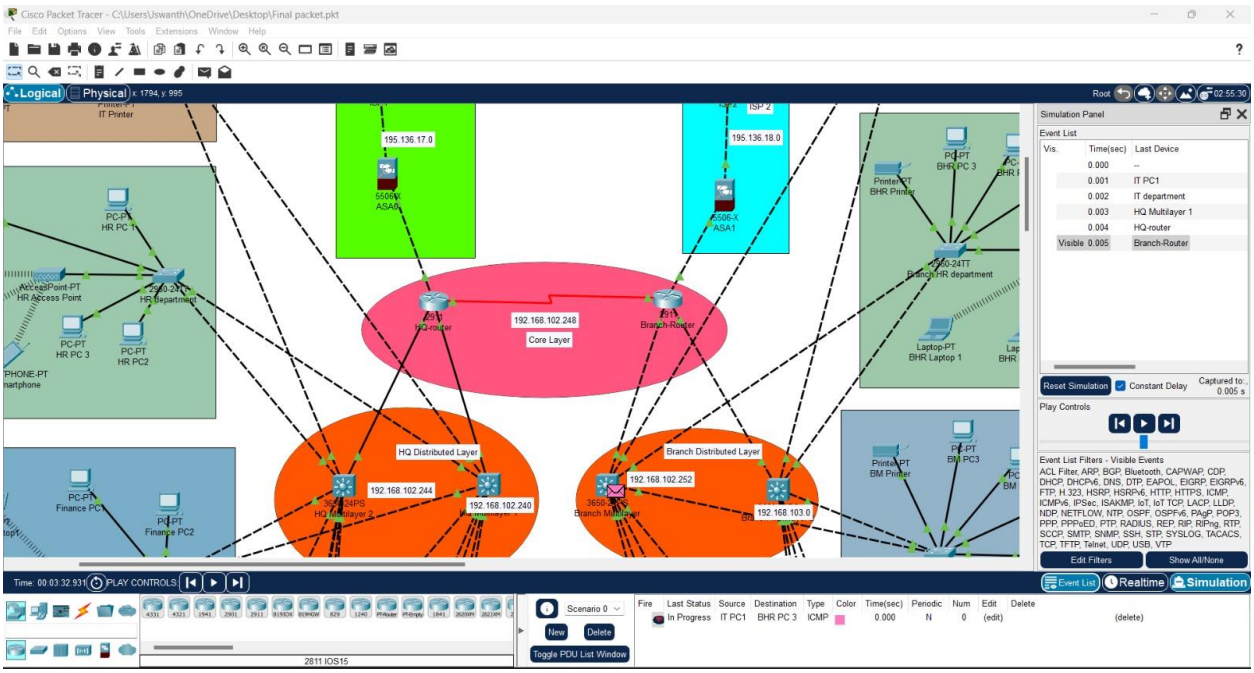


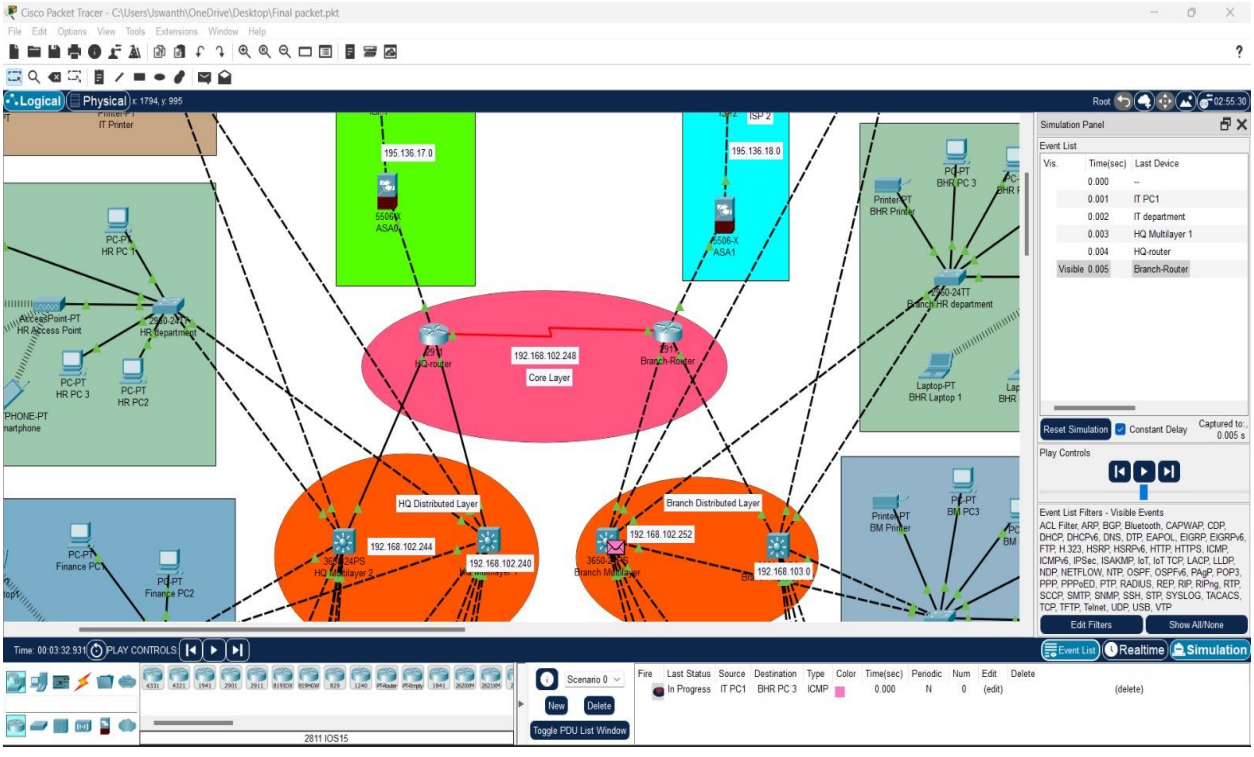

Cisco Packet Tracer - C:\Users\Jswanth\OneDrive\Desktop\Final packet.pkt
Logical
Physical
IT Printer
195.136.17.0
195.136.18.0
ISP 2
PC-PT HR PC 1
AccessPoint-PT HR Access Point
2960-24TT HR Department
PC-PT HR PC 3
PC-PT HR PC2
PHONE-PT
192.168.102.248
Core Layer
HQ-router
Branch-Router
HQ Distributed Layer
Branch Distributed Layer
192.168.102.244
192.168.102.240
192.168.102.252
192.168.103.0
PC-PT Finance PC
PC-PT Finance PC2
Printer-PT BHR Printer
PC-PT BHR PC 3
2960-24TT Branch HR department
Laptop-PT BHR Laptop 1
Printer-PT BM Printer
PC-PT BM PC3
Simulation Panel
Event List
Vis.
Time(sec)
Last Device
0.000
0.001
IT PC1
Visible 0.002
IT department
Reset Simulation
Constant Delay
Captured to:
0.002 s
Play Controls
Event List Filters - Visible Events
Edit Filters
Show All/None
Time: 00:03:32.928
PLAY CONTROLS
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
In Progress
IT PC1
BHR PC 3
ICMP
0.000
N
0
(edit)
(delete)
1841

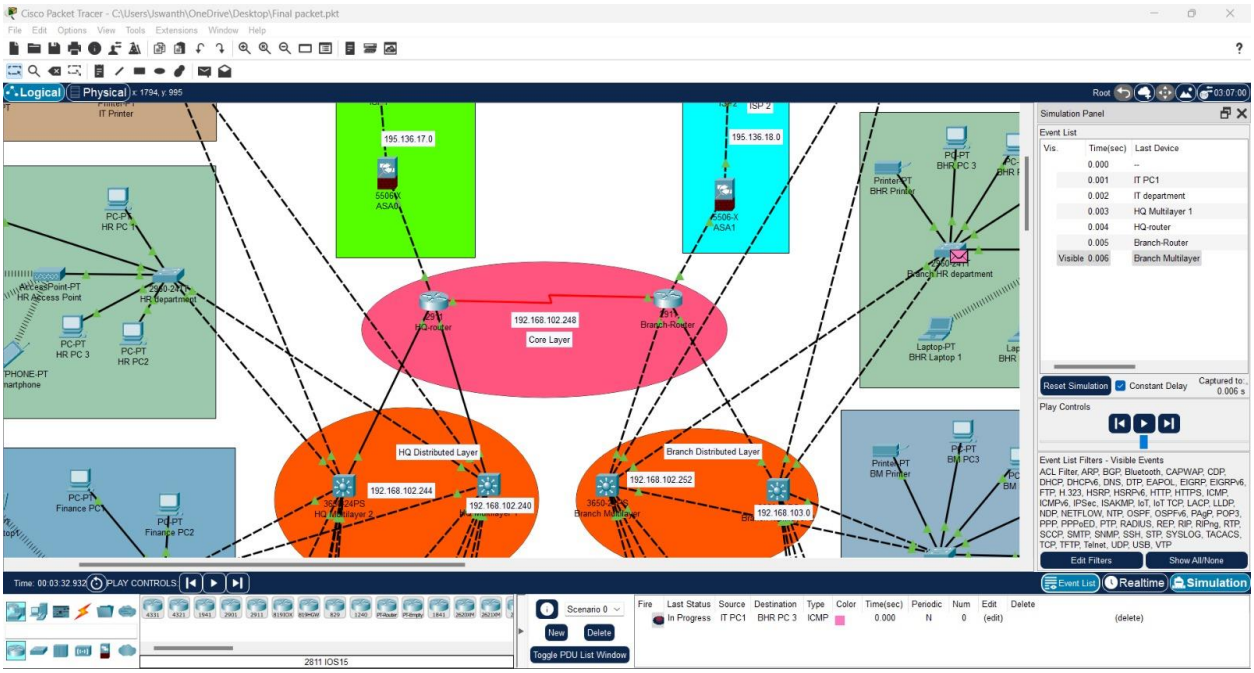

Cisco Packet Tracer - C:\Users\Jswanth\OneDrive\Desktop\Final packet.pkt
Logical
Physical
IT Printer
195.136.17.0
195.136.18.0
ISP 2
PC-PT HR PC 1
AccessPoint-PT HR Access Point
2960-24TT HR Department
PC-PT HR PC 3
PC-PT HR PC2
PHONE-PT
192.168.102.248
Core Layer
HQ-router
Branch-Router
HQ Distributed Layer
Branch Distributed Layer
192.168.102.244
192.168.102.240
192.168.102.252
192.168.103.0
PC-PT Finance PC
PC-PT Finance PC2
Printer-PT BHR Printer
PC-PT BHR PC 3
2960-24TT Branch HR department
Laptop-PT BHR Laptop 1
Printer-PT BM Printer
PC-PT BM PC3
Simulation Panel
Event List
Vis.
Time(sec)
Last Device
0.000
0.001
IT PC1
Visible 0.002
IT department
Reset Simulation
Constant Delay
Captured to:
0.002 s
Play Controls
Event List Filters - Visible Events
Edit Filters
Show All/None
Time: 00:03:32.928
PLAY CONTROLS
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
In Progress
IT PC1
BHR PC 3
ICMP
0.000
N
0
(edit)
(delete)
1841

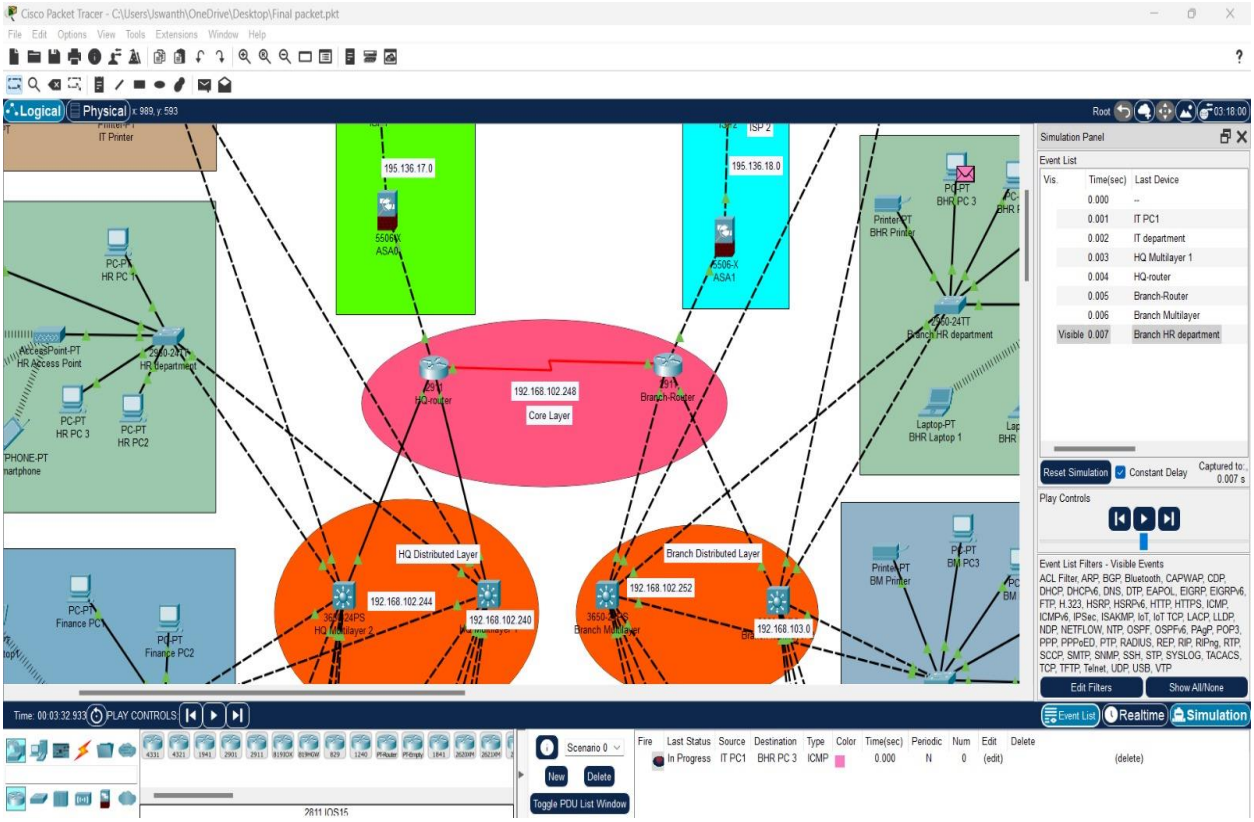

Cisco Packet Tracer - C:\Users\Jswanth\OneDrive\Desktop\Final packet.pkt
Logical
Physical
IT Printer
195.136.17.0
ASA0
195.136.18.0
ASA1
PC-PT HR PC 1
AccessPoint-PT HR Access Point
HR Department
PC-PT HR PC 3
PC-PT HR PC2
PHONE-PT
HQ-router
192.168.102.248
Core Layer
Branch-Router
Branch HR department
Laptop-PT BHR Laptop 1
HQ Distributed Layer
192.168.102.244
192.168.102.240
Branch Distributed Layer
192.168.102.252
192.168.103.0
Printer-PT BHR Printer
PC-PT BHR PC 3
Printer-PT BM Printer
PC-PT BM PC3
PC-PT Finance PC1
PC-PT Finance PC2
Simulation Panel
Event List
Vis. Time(sec) Last Device
0.000 --
0.001 IT PC1
0.002 IT department
Visible 0.003 HQ Multilayer 1
Reset Simulation
Constant Delay
Captured to: 0.003 s
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
Event List
Realtime
Simulation
Time: 00:03:32.929
PLAY CONTROLS
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
In Progress IT PC1 BHR PC 3 ICMP 0.000 N 0 (edit) (delete)
1841

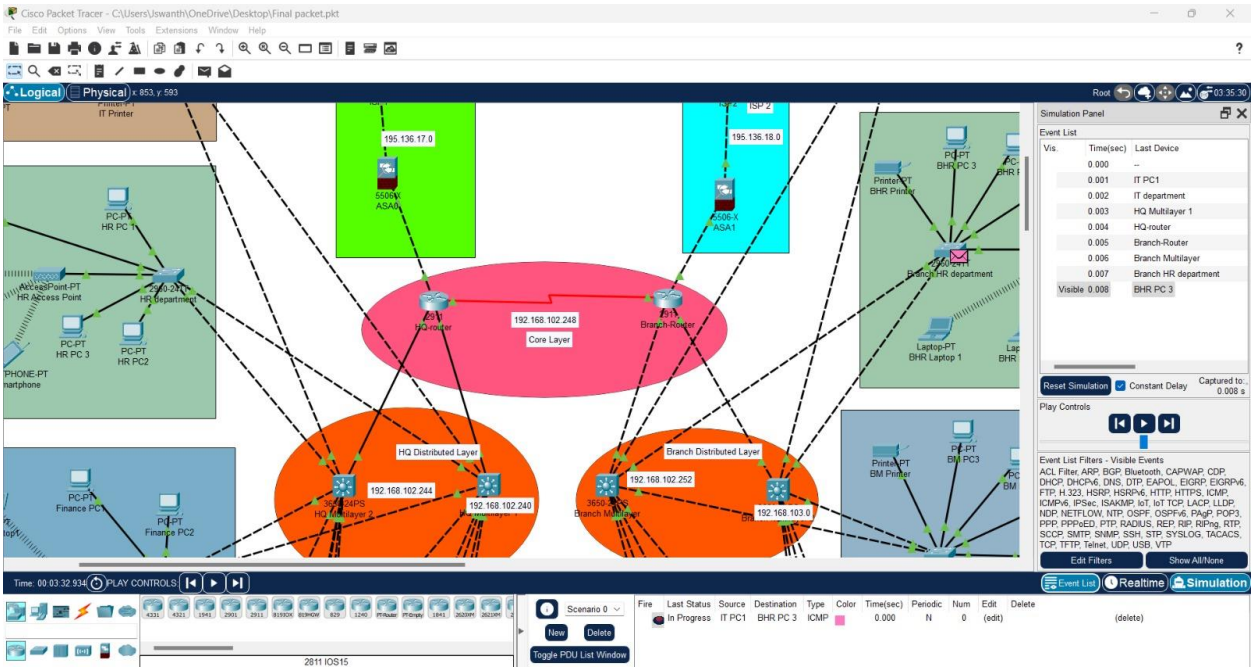

Cisco Packet Tracer - C:\Users\Jswanth\OneDrive\Desktop\Final packet.pkt
Logical
Physical
IT Printer
195.136.17.0
ASA0
195.136.18.0
ASA1
PC-PT HR PC 1
AccessPoint-PT HR Access Point
HR Department
PC-PT HR PC 3
PC-PT HR PC2
PHONE-PT
HQ-router
192.168.102.248
Core Layer
Branch-Router
Branch HR department
Laptop-PT BHR Laptop 1
HQ Distributed Layer
192.168.102.244
192.168.102.240
Branch Distributed Layer
192.168.102.252
192.168.103.0
Printer-PT BHR Printer
PC-PT BHR PC 3
Printer-PT BM Printer
PC-PT BM PC3
PC-PT Finance PC1
PC-PT Finance PC2
Simulation Panel
Event List
Vis. Time(sec) Last Device
0.000 --
0.001 IT PC1
0.002 IT department
0.003 HQ Multilayer 1
Visible 0.004 HQ-router
Reset Simulation
Constant Delay
Captured to: 0.004 s
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
Event List
Realtime
Simulation
Time: 00:03:32.930
PLAY CONTROLS
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
In Progress IT PC1 BHR PC 3 ICMP 0.000 N 0 (edit) (delete)
1841

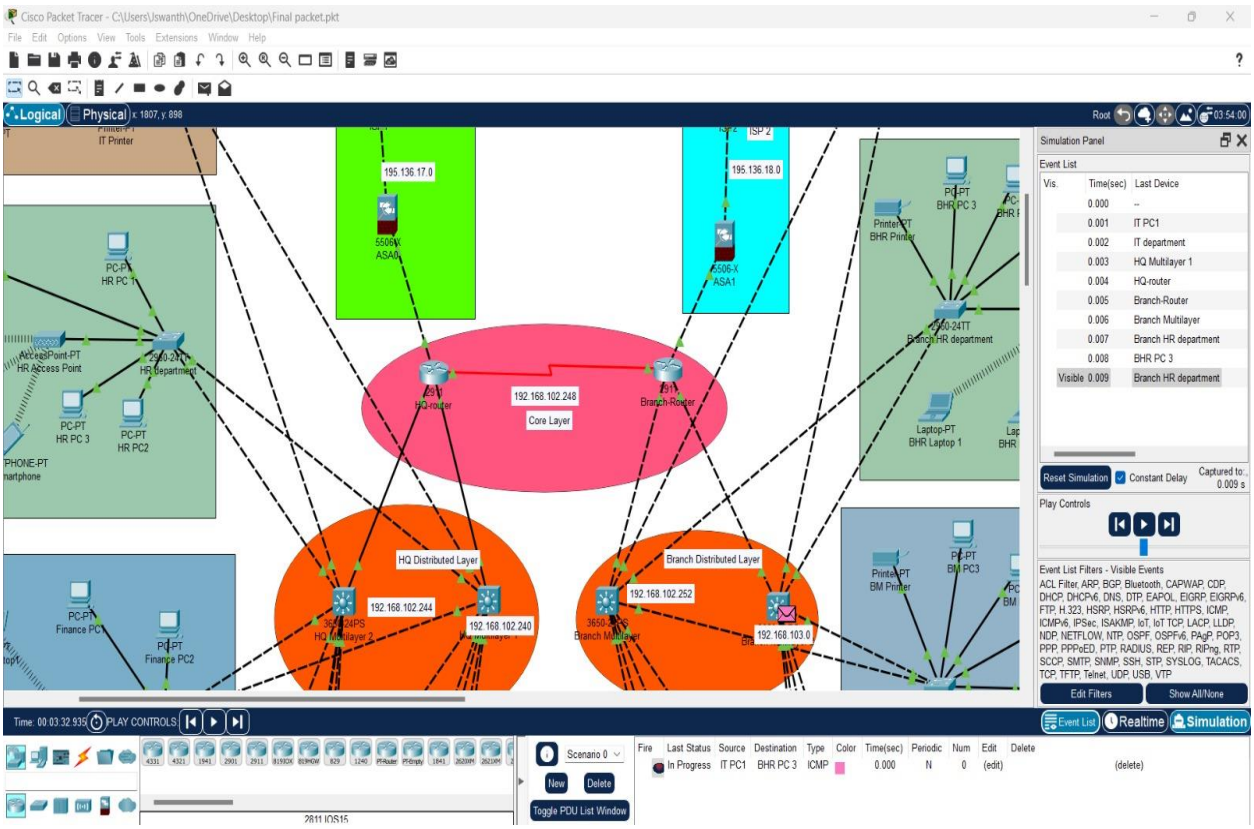

Cisco Packet Tracer - C:\Users\Jswanth\OneDrive\Desktop\Final packet.pkt
Logical
Physical
IT Printer
195.136.17.0
ISP 2
195.136.18.0
PC-PT HR PC 1
AccessPoint-PT HR Access Point
2950-24TT HR Department
PC-PT HR PC 3
PC-PT HR PC2
PHONE-PT
PC-PT BHR PC 3
Printer-PT BHR Printer
3560-24TT Branch HR department
Laptop-PT BHR Laptop 1
HQ-router
Branch-Router
192.168.102.248
Core Layer
HQ Distributed Layer
Branch Distributed Layer
192.168.102.244
192.168.102.240
192.168.102.252
192.168.103.0
PC-PT Finance PC1
PC-PT Finance PC2
Printer-PT BM Printer
PC-PT BM PC3
Simulation Panel
Event List
Vis.
Time(sec)
Last Device
0.000
0.001
IT PC1
0.002
IT department
0.003
HQ Multilayer 1
0.004
HQ-router
Visible 0.005
Branch-Router
Reset Simulation
Constant Delay
Captured to:
0.005 s
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
Time: 00:03:32.931
PLAY CONTROLS
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
In Progress
IT PC1
BHR PC 3
ICMP
0.000
N
0
(edit)
(delete)
2811 IOS15

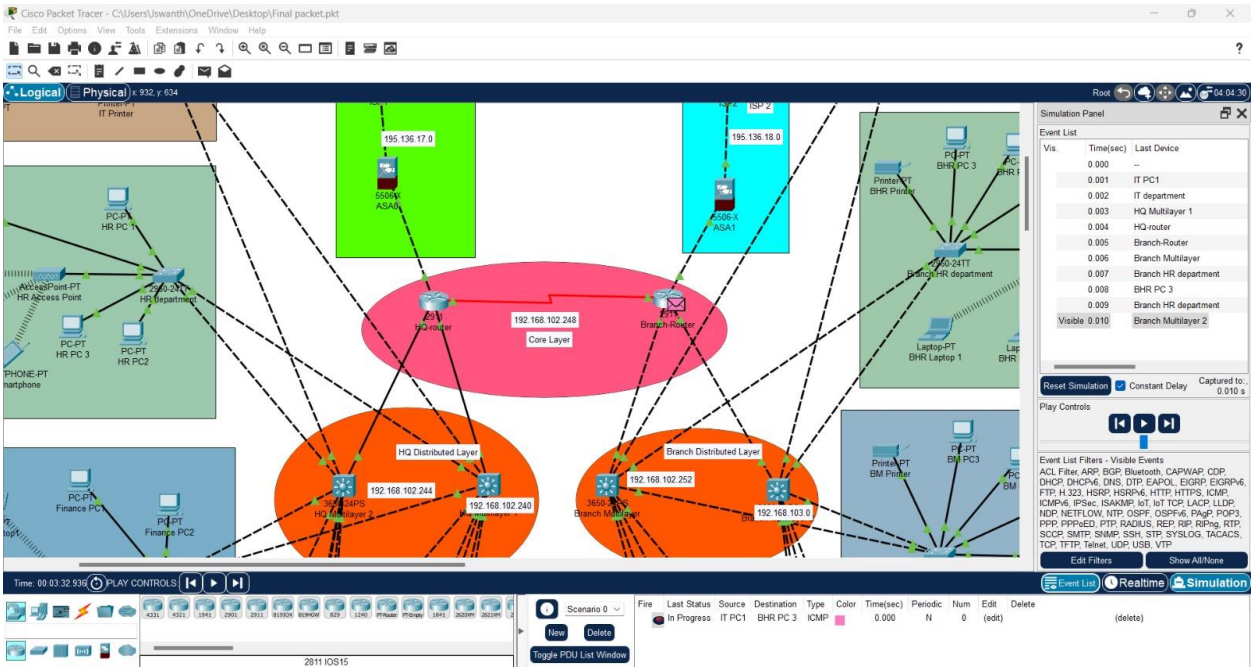

Cisco Packet Tracer - C:\Users\Jswanth\OneDrive\Desktop\Final packet.pkt
Logical
Physical
IT Printer
195.136.17.0
ISP 2
195.136.18.0
PC-PT HR PC 1
AccessPoint-PT HR Access Point
2950-24TT HR Department
PC-PT HR PC 3
PC-PT HR PC2
PHONE-PT
PC-PT BHR PC 3
Printer-PT BHR Printer
3560-24TT Branch HR department
Laptop-PT BHR Laptop 1
HQ-router
Branch-Router
192.168.102.248
Core Layer
HQ Distributed Layer
Branch Distributed Layer
192.168.102.244
192.168.102.240
192.168.102.252
192.168.103.0
PC-PT Finance PC1
PC-PT Finance PC2
Printer-PT BM Printer
PC-PT BM PC3
Simulation Panel
Event List
Vis.
Time(sec)
Last Device
0.000
0.001
IT PC1
0.002
IT department
0.003
HQ Multilayer 1
0.004
HQ-router
Visible 0.005
Branch-Router
Reset Simulation
Constant Delay
Captured to:
0.005 s
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
Time: 00:03:32.931
PLAY CONTROLS
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
In Progress
IT PC1
BHR PC 3
ICMP
0.000
N
0
(edit)
(delete)
2811 IOS15

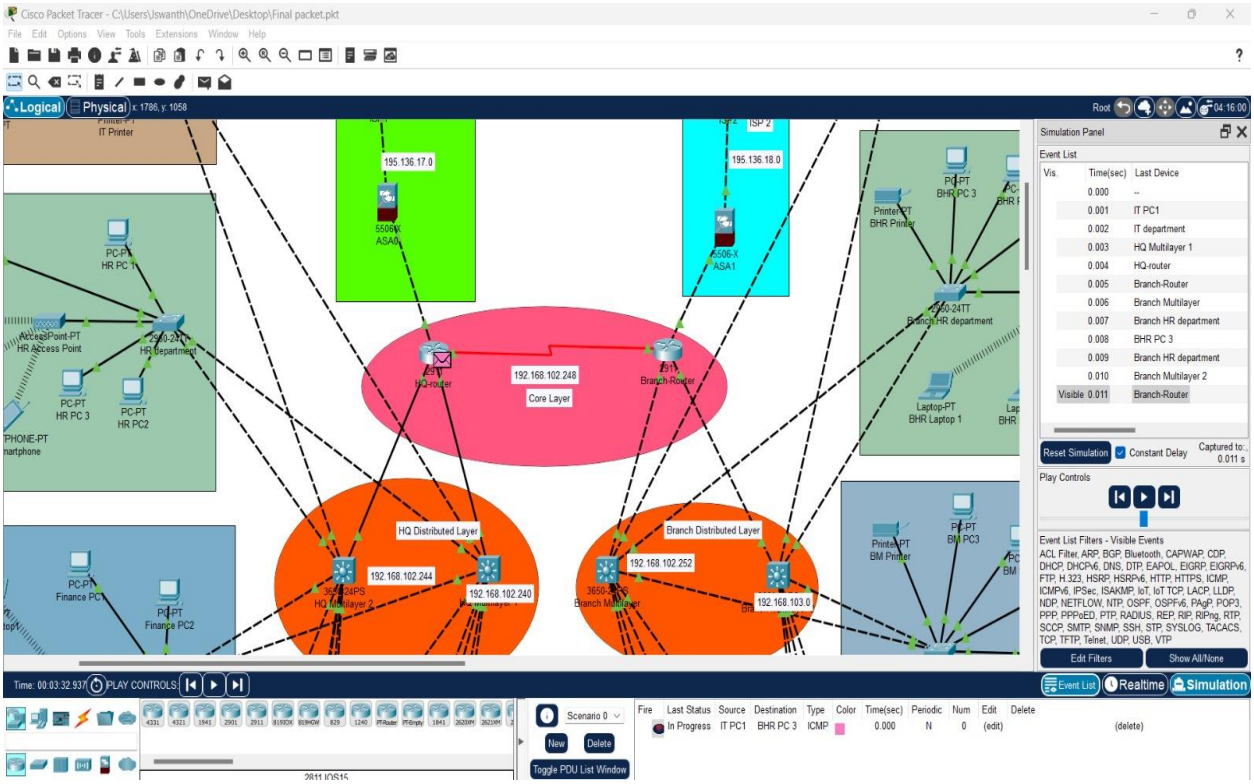

Cisco Packet Tracer - C:\Users\Jswanth\OneDrive\Desktop\Final packet.pkt
Logical
Physical
IT Printer
195.136.17.0
195.136.18.0
ISP 2
PC-PT HR PC 1
AccessPoint-PT HR Access Point
2950-24TT HR Department
PC-PT HR PC 3
PC-PT HR PC2
PHONE-PT
HQ-router
Core Layer
Branch-Router
PC-PT BHR PC 3
Printer-PT BHR Printer
Branch HR department
Laptop-PT BHR Laptop 1
HQ Distributed Layer
Branch Distributed Layer
192.168.102.244
192.168.102.240
192.168.102.248
192.168.102.252
192.168.103.0
PC-PT Finance PC1
PC-PT Finance PC2
Printer-PT BM Printer
PC-PT BM PC3
Simulation Panel
Event List
Vis.
Time(sec)
Last Device
0.000
0.001 IT PC1
0.002 IT department
0.003 HQ Multilayer 1
0.004 HQ-router
0.005 Branch-Router
Visible 0.006 Branch Multilayer
Reset Simulation
Constant Delay
Captured to: 0.006 s
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
Time: 00:03:32.932
PLAY CONTROLS
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
In Progress
IT PC1
BHR PC 3
ICMP
0.000
N
0
(edit)
(delete)
2811 IOS15

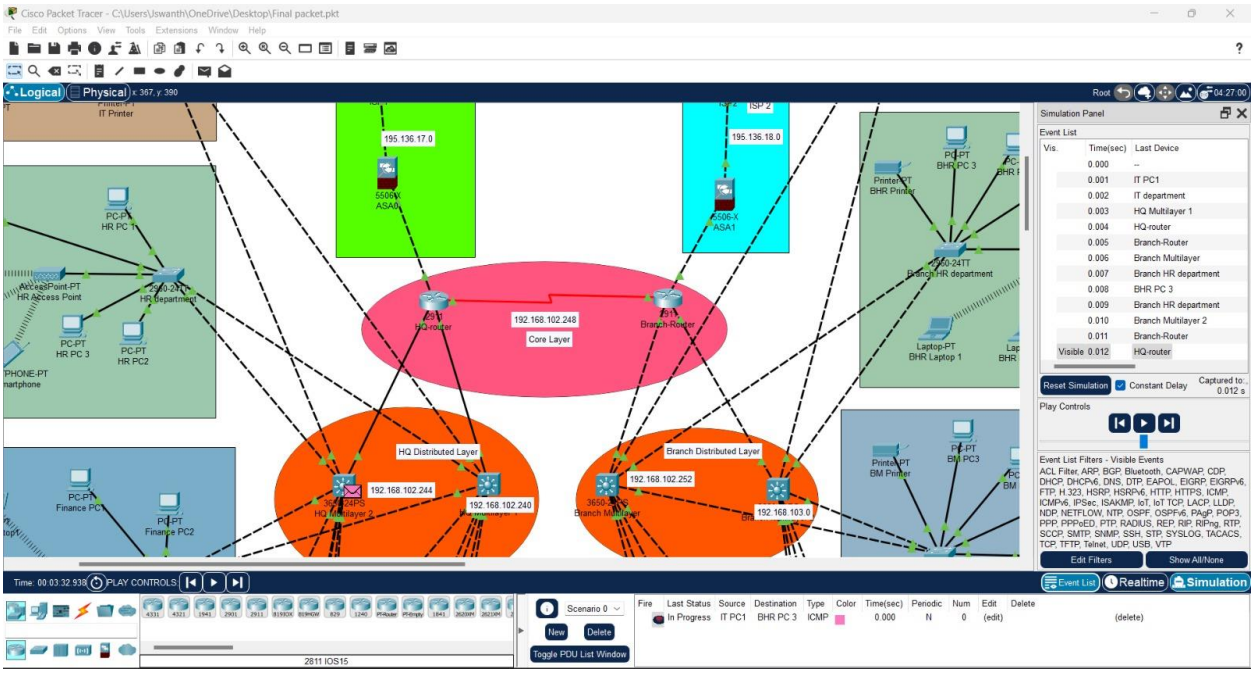

Cisco Packet Tracer - C:\Users\Jswanth\OneDrive\Desktop\Final packet.pkt
Logical
Physical
IT Printer
195.136.17.0
195.136.18.0
ISP 2
PC-PT HR PC 1
AccessPoint-PT HR Access Point
2950-24TT HR Department
PC-PT HR PC 3
PC-PT HR PC2
PHONE-PT
HQ-router
Core Layer
Branch-Router
PC-PT BHR PC 3
Printer-PT BHR Printer
Branch HR department
Laptop-PT BHR Laptop 1
HQ Distributed Layer
Branch Distributed Layer
192.168.102.244
192.168.102.240
192.168.102.248
192.168.102.252
192.168.103.0
PC-PT Finance PC1
PC-PT Finance PC2
Printer-PT BM Printer
PC-PT BM PC3
Simulation Panel
Event List
Vis.
Time(sec)
Last Device
0.000
0.001 IT PC1
0.002 IT department
0.003 HQ Multilayer 1
0.004 HQ-router
0.005 Branch-Router
0.006 Branch Multilayer
Visible 0.007 Branch HR department
Reset Simulation
Constant Delay
Captured to: 0.007 s
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
Time: 00:03:32.933
PLAY CONTROLS
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
In Progress
IT PC1
BHR PC 3
ICMP
0.000
N
0
(edit)
(delete)
2811 IOS15

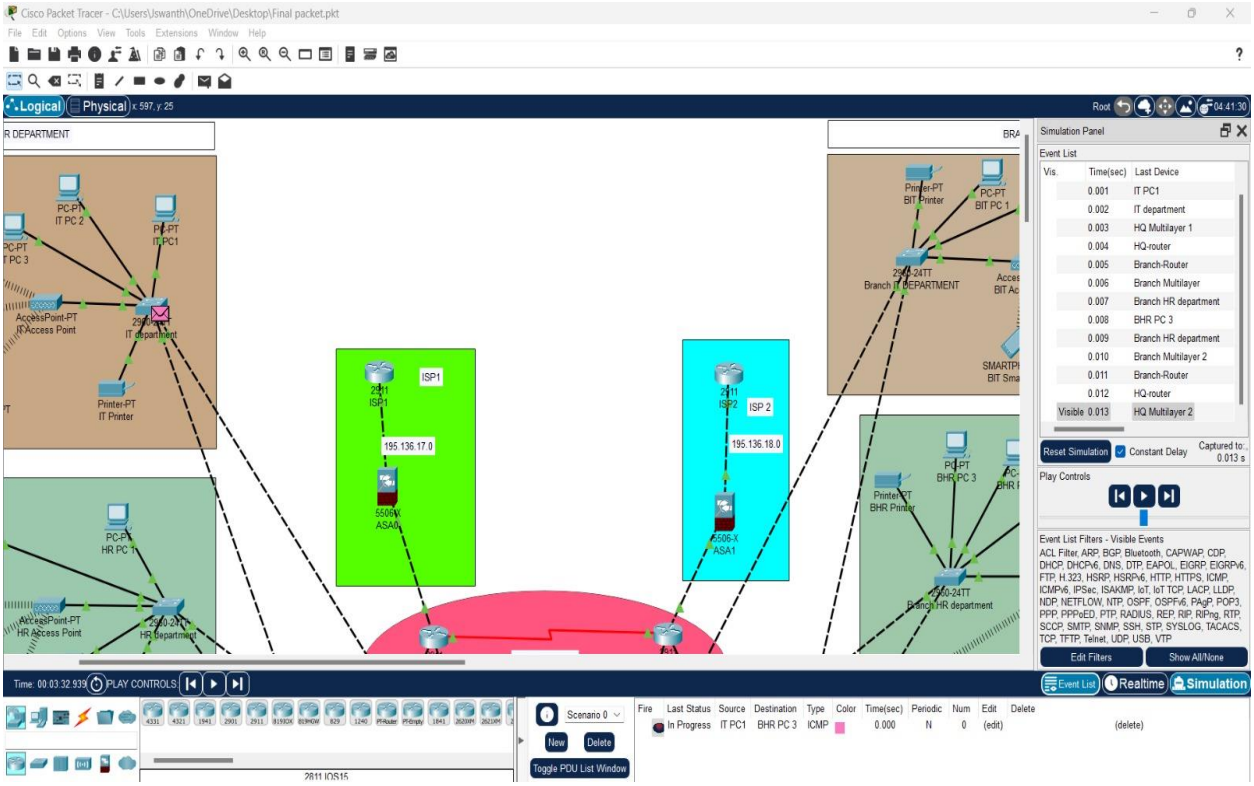

Cisco Packet Tracer - C:\Users\Jswanth\OneDrive\Desktop\Final packet.pkt
Logical
Physical
IT Printer
195.136.17.0
195.136.18.0
ISP 2
HQ-router
Branch-Router
192.168.102.248
Core Layer
HQ Distributed Layer
Branch Distributed Layer
192.168.102.244
192.168.102.240
192.168.102.252
192.168.103.0
Branch HR department
Laptop-PT BHR Laptop 1
Printer-PT BHR Printer
PC-PT BHR PC 3
Printer-PT BM Printer
PC-PT BM PC3
PC-PT HR PC 1
PC-PT HR PC 3
PC-PT HR PC2
PC-PT Finance PC1
PC-PT Finance PC2
Simulation Panel
Event List
Vis. Time(sec) Last Device
0.000 --
0.001 IT PC1
0.002 IT department
0.003 HQ Multilayer 1
0.004 HQ-router
0.005 Branch-Router
0.006 Branch Multilayer
0.007 Branch HR department
Visible 0.008 BHR PC 3
Reset Simulation
Constant Delay
Play Controls
Event List Filters - Visible Events
Edit Filters
Show All/None
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
In Progress IT PC1 BHR PC 3 ICMP 0.000 N 0 (edit) (delete)

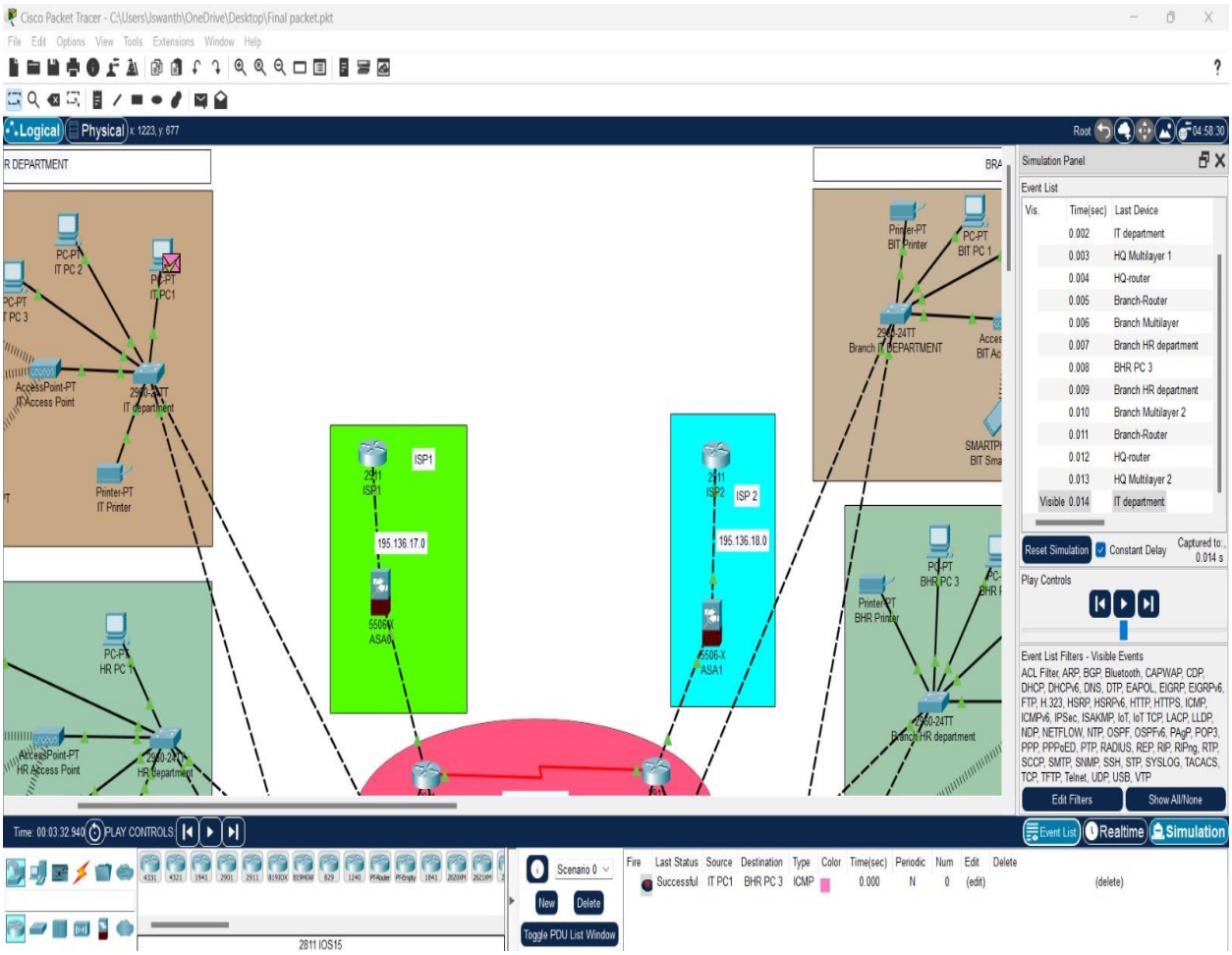

Cisco Packet Tracer - C:\Users\Jswanth\OneDrive\Desktop\Final packet.pkt
Logical
Physical
IT Printer
195.136.17.0
195.136.18.0
ISP 2
HQ-router
Branch-Router
192.168.102.248
Core Layer
HQ Distributed Layer
Branch Distributed Layer
192.168.102.244
192.168.102.240
192.168.102.252
192.168.103.0
Branch HR department
Laptop-PT BHR Laptop 1
Printer-PT BHR Printer
PC-PT BHR PC 3
Printer-PT BM Printer
PC-PT BM PC3
PC-PT HR PC 1
PC-PT HR PC 3
PC-PT HR PC2
PC-PT Finance PC1
PC-PT Finance PC2
Simulation Panel
Event List
Vis. Time(sec) Last Device
0.000 --
0.001 IT PC1
0.002 IT department
0.003 HQ Multilayer 1
0.004 HQ-router
0.005 Branch-Router
0.006 Branch Multilayer
0.007 Branch HR department
0.008 BHR PC 3
Visible 0.009 Branch HR department
Reset Simulation
Constant Delay
Play Controls
Event List Filters - Visible Events
Edit Filters
Show All/None
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
In Progress IT PC1 BHR PC 3 ICMP 0.000 N 0 (edit) (delete)


Cisco Packet Tracer - C:\Users\Jswanth\OneDrive\Desktop\Final packet.pkt
Logical
Physical
Root
IT Printer
195.136.17.0
195.136.18.0
ISP 2
PC-PT HR PC 1
AccessPoint-PT HR Access Point
2950-24TT HR Department
PC-PT HR PC 3
PC-PT HR PC2
PHONE-PT
PC-PT Finance PC
PC-PT Finance PC2
HQ-router
Branch-Router
192.168.102.248
Core Layer
HQ Distributed Layer
Branch Distributed Layer
192.168.102.244
192.168.102.240
192.168.102.252
192.168.103.0
PC-PT BHR PC 3
Printer-PT BHR Printer
2950-24TT Branch HR department
Laptop-PT BHR Laptop 1
Printer-PT BM Printer
PC-PT BM PC3
Simulation Panel
Event List
Vis.
Time(sec)
Last Device
0.000 --
0.001 IT PC1
0.002 IT department
0.003 HQ Multilayer 1
0.004 HQ-router
0.005 Branch-Router
0.006 Branch Multilayer
0.007 Branch HR department
0.008 BHR PC 3
0.009 Branch HR department
Visible 0.010 Branch Multilayer 2
Reset Simulation
Constant Delay
Captured to: 0.010 s
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
Time: 00:03:32.936
PLAY CONTROLS
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
In Progress
IT PC1
BHR PC 3
ICMP
0.000
N
0
(edit)
(delete)
2811 IOS15


Cisco Packet Tracer - C:\Users\Jswanth\OneDrive\Desktop\Final packet.pkt
Logical
Physical
Root
IT Printer
195.136.17.0
195.136.18.0
ISP 2
PC-PT HR PC 1
AccessPoint-PT HR Access Point
2950-24TT HR Department
PC-PT HR PC 3
PC-PT HR PC2
PHONE-PT
PC-PT Finance PC
PC-PT Finance PC2
HQ-router
Branch-Router
192.168.102.248
Core Layer
HQ Distributed Layer
Branch Distributed Layer
192.168.102.244
192.168.102.240
192.168.102.252
192.168.103.0
PC-PT BHR PC 3
Printer-PT BHR Printer
2950-24TT Branch HR department
Laptop-PT BHR Laptop 1
Printer-PT BM Printer
PC-PT BM PC3
Simulation Panel
Event List
Vis.
Time(sec)
Last Device
0.000 --
0.001 IT PC1
0.002 IT department
0.003 HQ Multilayer 1
0.004 HQ-router
0.005 Branch-Router
0.006 Branch Multilayer
0.007 Branch HR department
0.008 BHR PC 3
0.009 Branch HR department
0.010 Branch Multilayer 2
Visible 0.011 Branch-Router
Reset Simulation
Constant Delay
Captured to: 0.011 s
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
Time: 00:03:32.937
PLAY CONTROLS
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
In Progress
IT PC1
BHR PC 3
ICMP
0.000
N
0
(edit)
(delete)
2811 IOS15

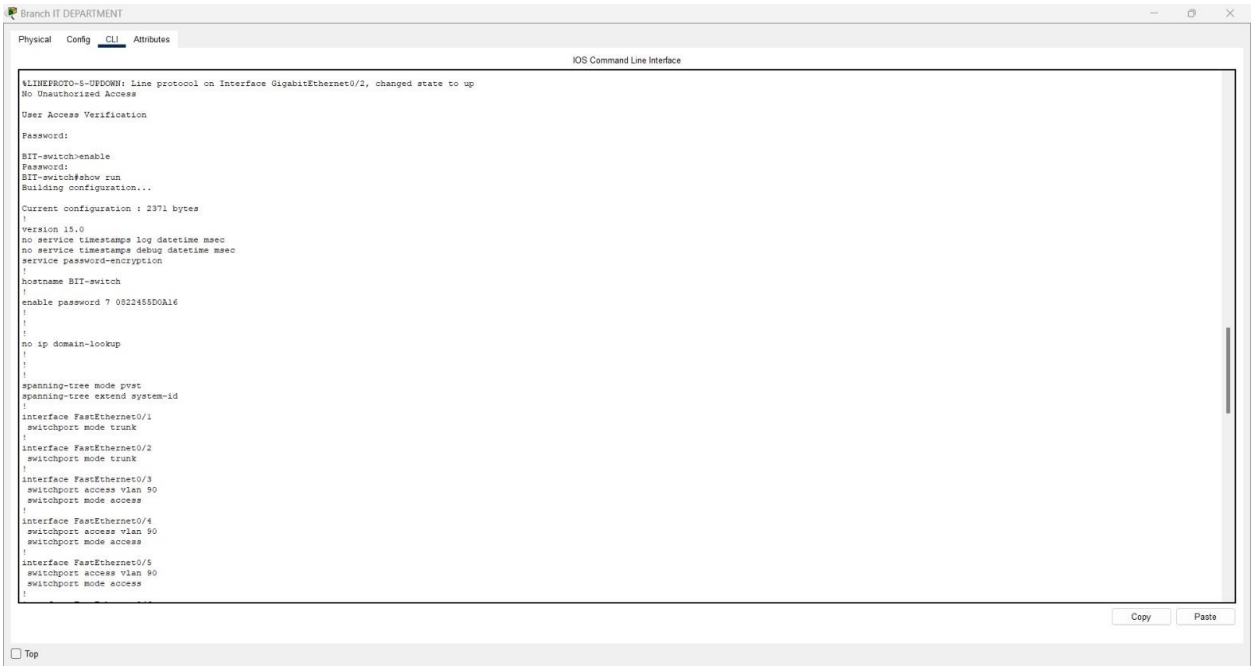

Cisco Packet Tracer - C:\Users\Jswanth\OneDrive\Desktop\Final packet.pkt
Logical
Physical
Root
Simulation Panel
Event List
195.136.17.0
195.136.18.0
ISP 2
HQ-router
Branch-Router
192.168.102.248
Core Layer
HQ Distributed Layer
Branch Distributed Layer
192.168.102.244
192.168.102.240
192.168.102.252
192.168.103.0
Reset Simulation
Constant Delay
Play Controls
Edit Filters
Show All/None
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window

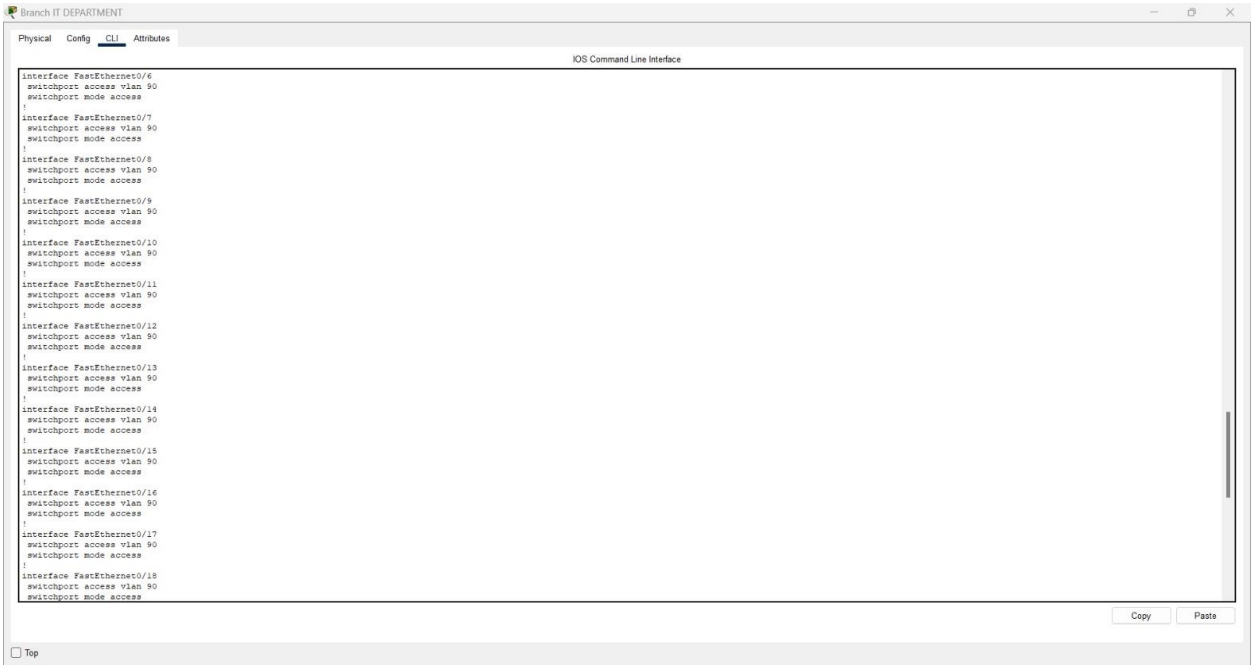

Cisco Packet Tracer - C:\Users\Jswanth\OneDrive\Desktop\Final packet.pkt
Logical
Physical
Root
Simulation Panel
Event List
ISP1
ISP 2
195.136.17.0
195.136.18.0
Reset Simulation
Constant Delay
Play Controls
Edit Filters
Show All/None
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window

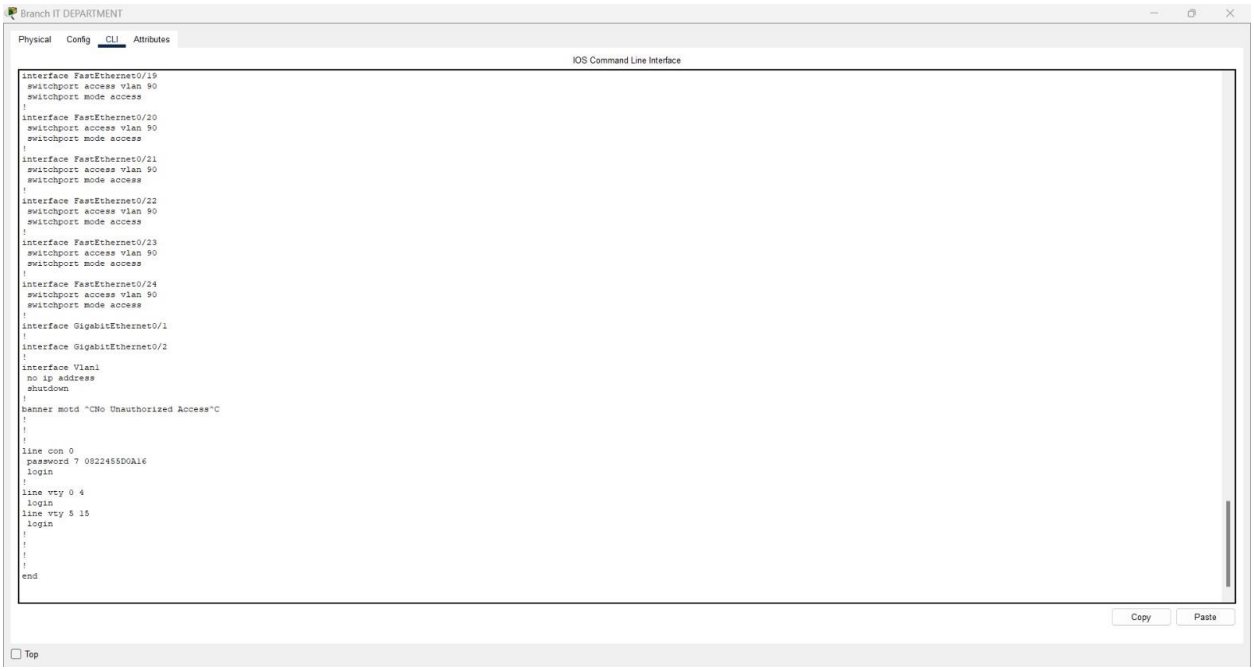

Cisco Packet Tracer - C:\Users\Jswanth\OneDrive\Desktop\Final packet.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
Root
R DEPARTMENT
PC-PT IT PC 2
PC-PT IT PC1
PC-PT T PC 3
AccessPoint-PT IT Access Point
2960-24TT IT department
Printer-PT IT Printer
ISP1
2911 ISP1
195.136.17.0
5506-X ASA0
ISP 2
2911 ISP2
195.136.18.0
5506-X ASA1
Printer-PT BIT Printer
PC-PT BIT PC 1
2960-24TT Branch IT DEPARTMENT
PC-PT HR PC 1
AccessPoint-PT HR Access Point
2960-24TT HR department
PC-PT BHR PC 3
Printer-PT BHR Printer
2960-24TT Branch HR department
Simulation Panel
Event List
Vis. Time(sec) Last Device
0.002 IT department
0.003 HQ Multilayer 1
0.004 HQ-router
0.005 Branch-Router
0.006 Branch Multilayer
0.007 Branch HR department
0.008 BHR PC 3
0.009 Branch HR department
0.010 Branch Multilayer 2
0.011 Branch-Router
0.012 HQ-router
0.013 HQ Multilayer 2
Visible 0.014 IT department
Reset Simulation
Constant Delay
Captured to: 0.014 s
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
Time: 00:03:32.940
PLAY CONTROLS:
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
Successful IT PC1 BHR PC 3 ICMP 0.000 N 0 (edit) (delete)
2811 IOS15

3.2 Configuring Network Devices

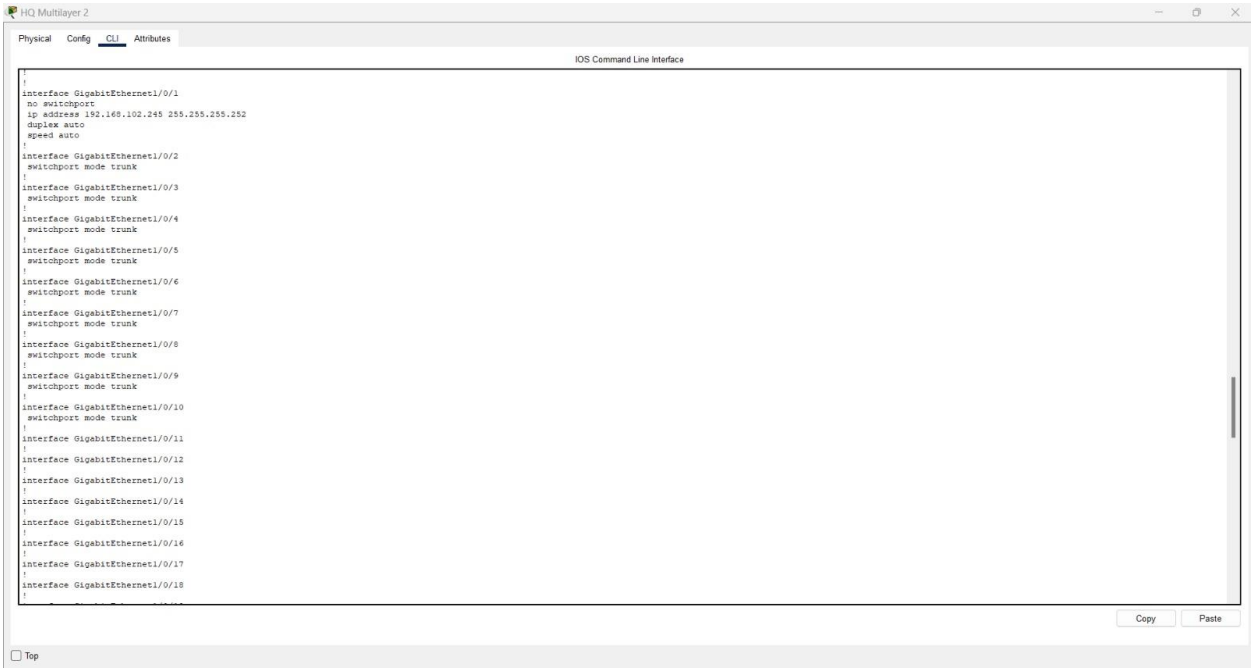
3.2.1 Configuring Switches

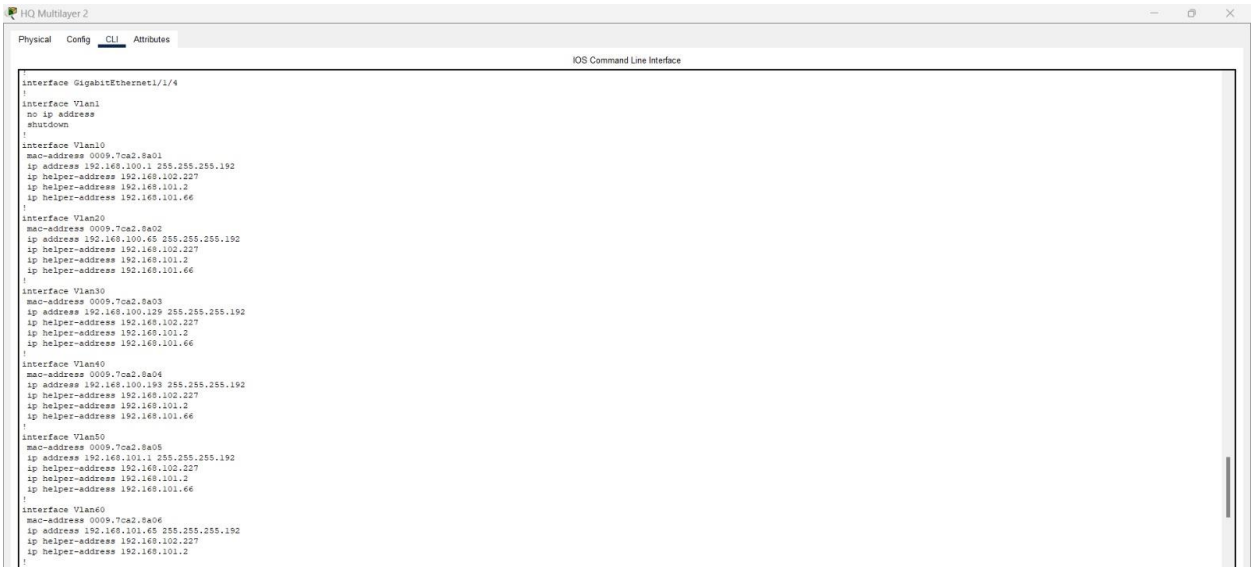


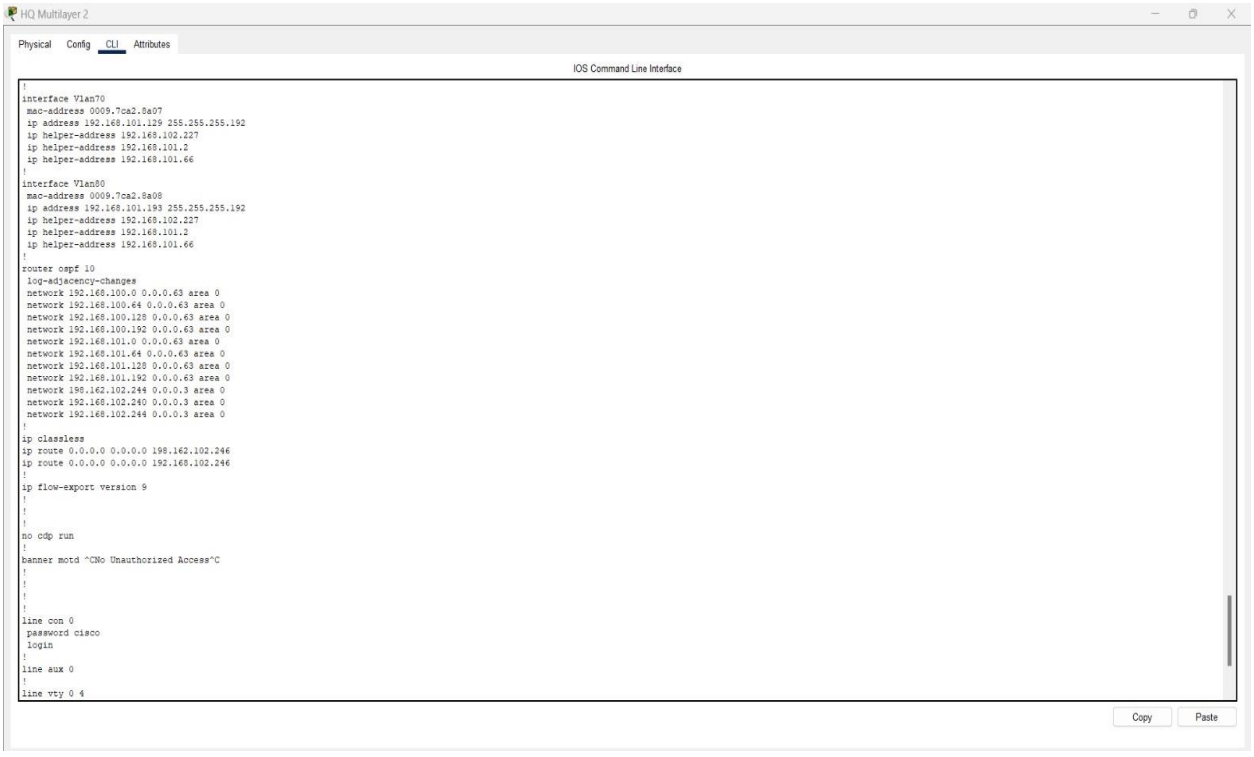




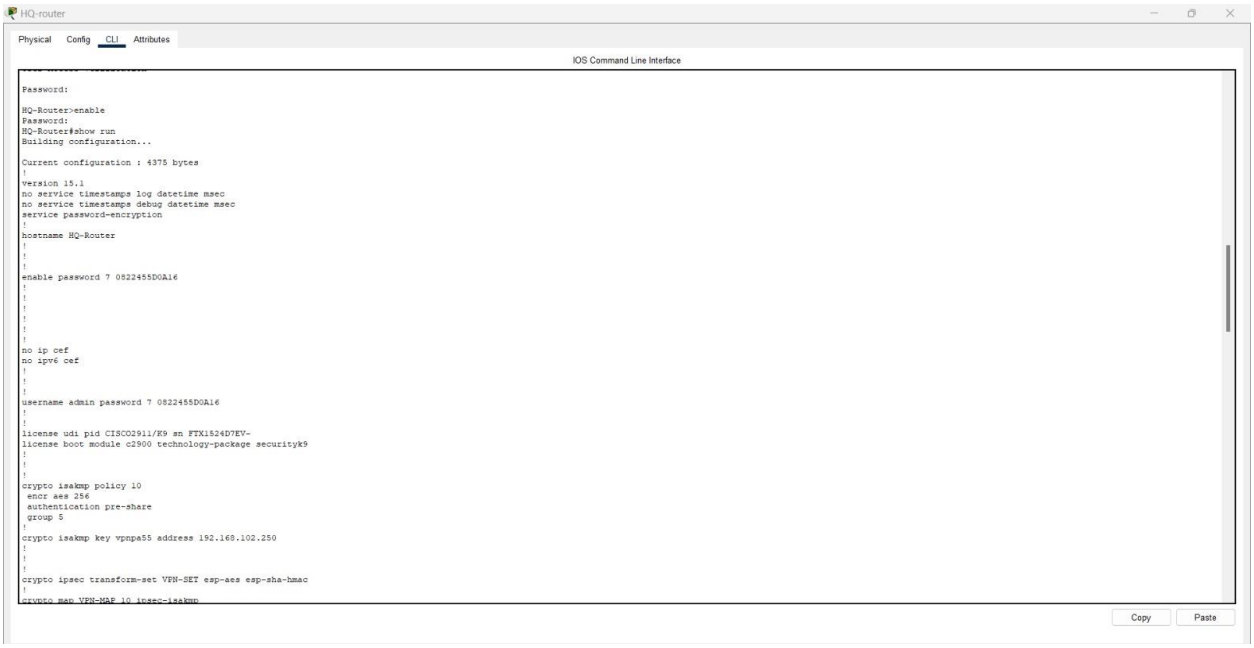
3.2.2 Configuring Multi-layer Switches

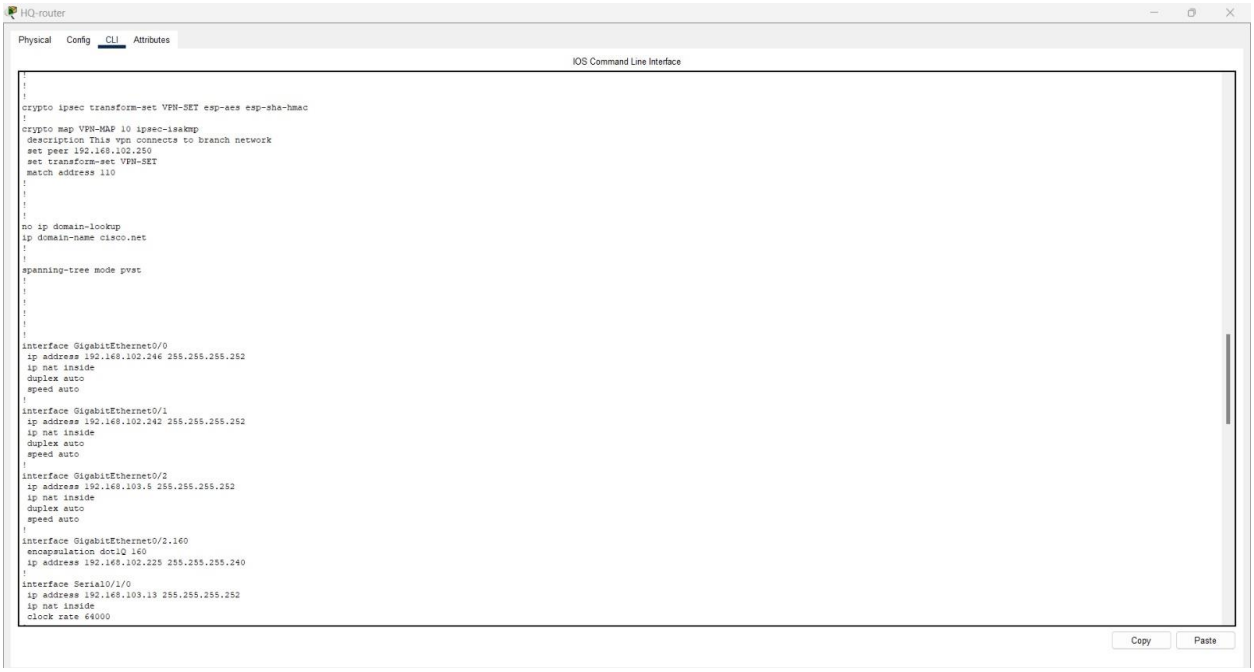


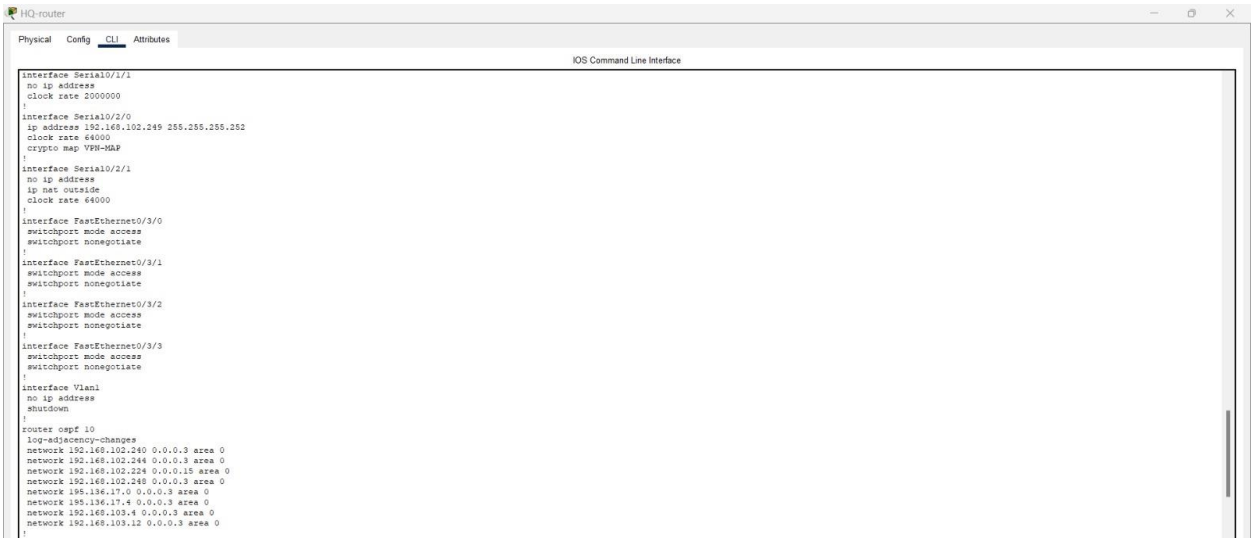

HQ Multilayer 2
Physical
Config
CLI
Attributes
IOS Command Line Interface
!
interface GigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 mac-address 0009.7ca2.8a01
 ip address 192.168.100.1 255.255.255.192
 ip helper-address 192.168.102.227
 ip helper-address 192.168.101.2
 ip helper-address 192.168.101.66
!
interface Vlan20
 mac-address 0009.7ca2.8a02
 ip address 192.168.100.65 255.255.255.192
 ip helper-address 192.168.102.227
 ip helper-address 192.168.101.2
 ip helper-address 192.168.101.66
!
interface Vlan30
 mac-address 0009.7ca2.8a03
 ip address 192.168.100.129 255.255.255.192
 ip helper-address 192.168.102.227
 ip helper-address 192.168.101.2
 ip helper-address 192.168.101.66
!
interface Vlan40
 mac-address 0009.7ca2.8a04
 ip address 192.168.100.193 255.255.255.192
 ip helper-address 192.168.102.227
 ip helper-address 192.168.101.2
 ip helper-address 192.168.101.66
!
interface Vlan50
 mac-address 0009.7ca2.8a05
 ip address 192.168.101.1 255.255.255.192
 ip helper-address 192.168.102.227
 ip helper-address 192.168.101.2
 ip helper-address 192.168.101.66
!
interface Vlan60
 mac-address 0009.7ca2.8a06
 ip address 192.168.101.65 255.255.255.192
 ip helper-address 192.168.102.227
 ip helper-address 192.168.101.2
!

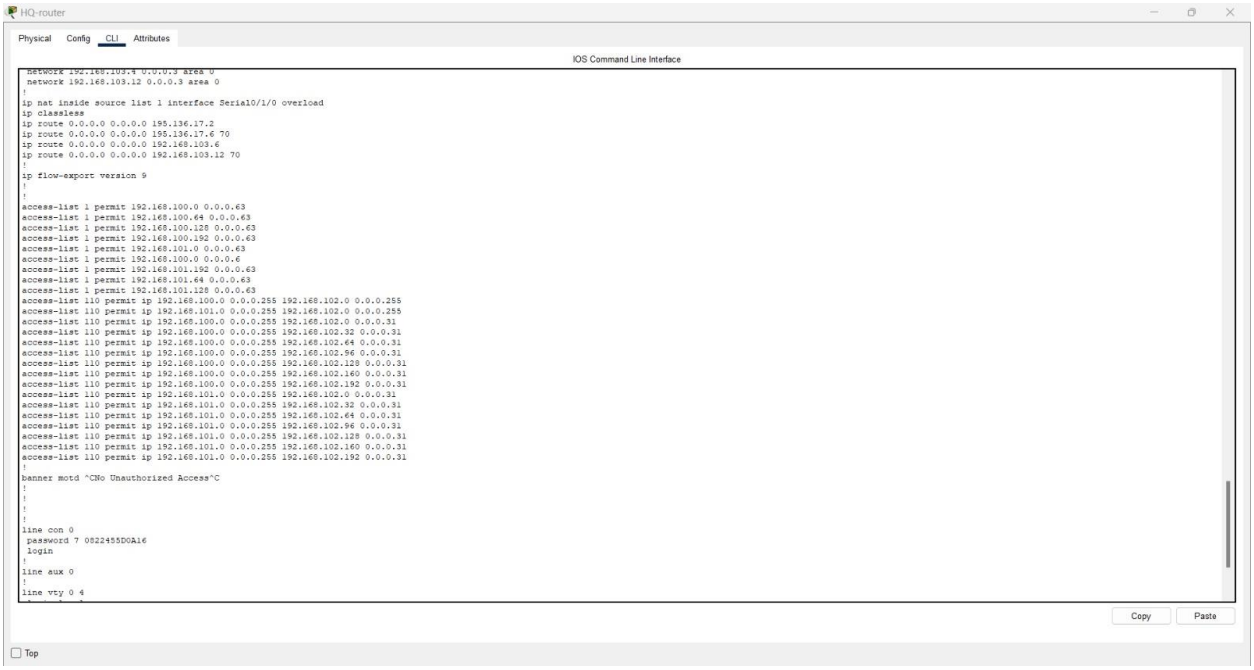

HQ Multilayer 2
Physical
Config
CLI
Attributes
IOS Command Line Interface
!
interface Vlan70
 mac-address 0009.7ca2.8a07
 ip address 192.168.101.129 255.255.255.192
 ip helper-address 192.168.102.227
 ip helper-address 192.168.101.2
 ip helper-address 192.168.101.66
!
interface Vlan80
 mac-address 0009.7ca2.8a08
 ip address 192.168.101.193 255.255.255.192
 ip helper-address 192.168.102.227
 ip helper-address 192.168.101.2
 ip helper-address 192.168.101.66
!
router ospf 10
 log-adjacency-changes
 network 192.168.100.0 0.0.0.63 area 0
 network 192.168.100.64 0.0.0.63 area 0
 network 192.168.100.128 0.0.0.63 area 0
 network 192.168.100.192 0.0.0.63 area 0
 network 192.168.101.0 0.0.0.63 area 0
 network 192.168.101.64 0.0.0.63 area 0
 network 192.168.101.128 0.0.0.63 area 0
 network 192.168.101.192 0.0.0.63 area 0
 network 198.162.102.244 0.0.0.3 area 0
 network 192.168.102.240 0.0.0.3 area 0
 network 192.168.102.244 0.0.0.3 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 198.162.102.246
ip route 0.0.0.0 0.0.0.0 192.168.102.246
!
ip flow-export version 9
!
!
!
no cdp run
!
banner motd ^CNo Unauthorized Access^C
!
!
!
!
line con 0
 password cisco
 login
!
line aux 0
!
line vty 0 4
Copy
Paste

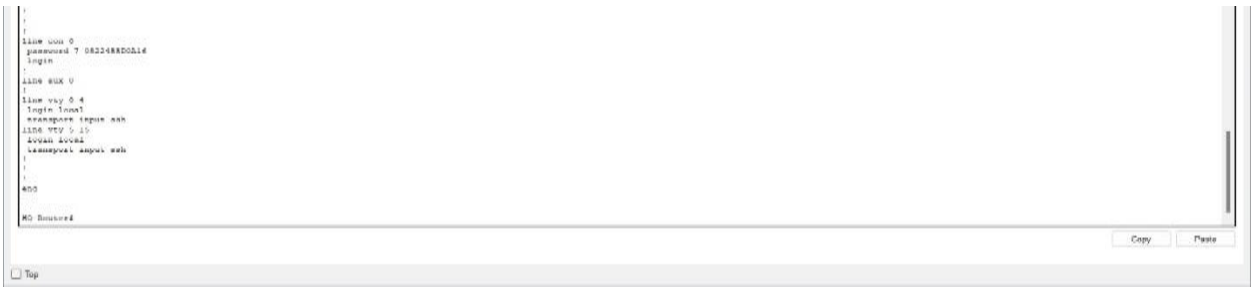
3.2.3 Configuring Routers



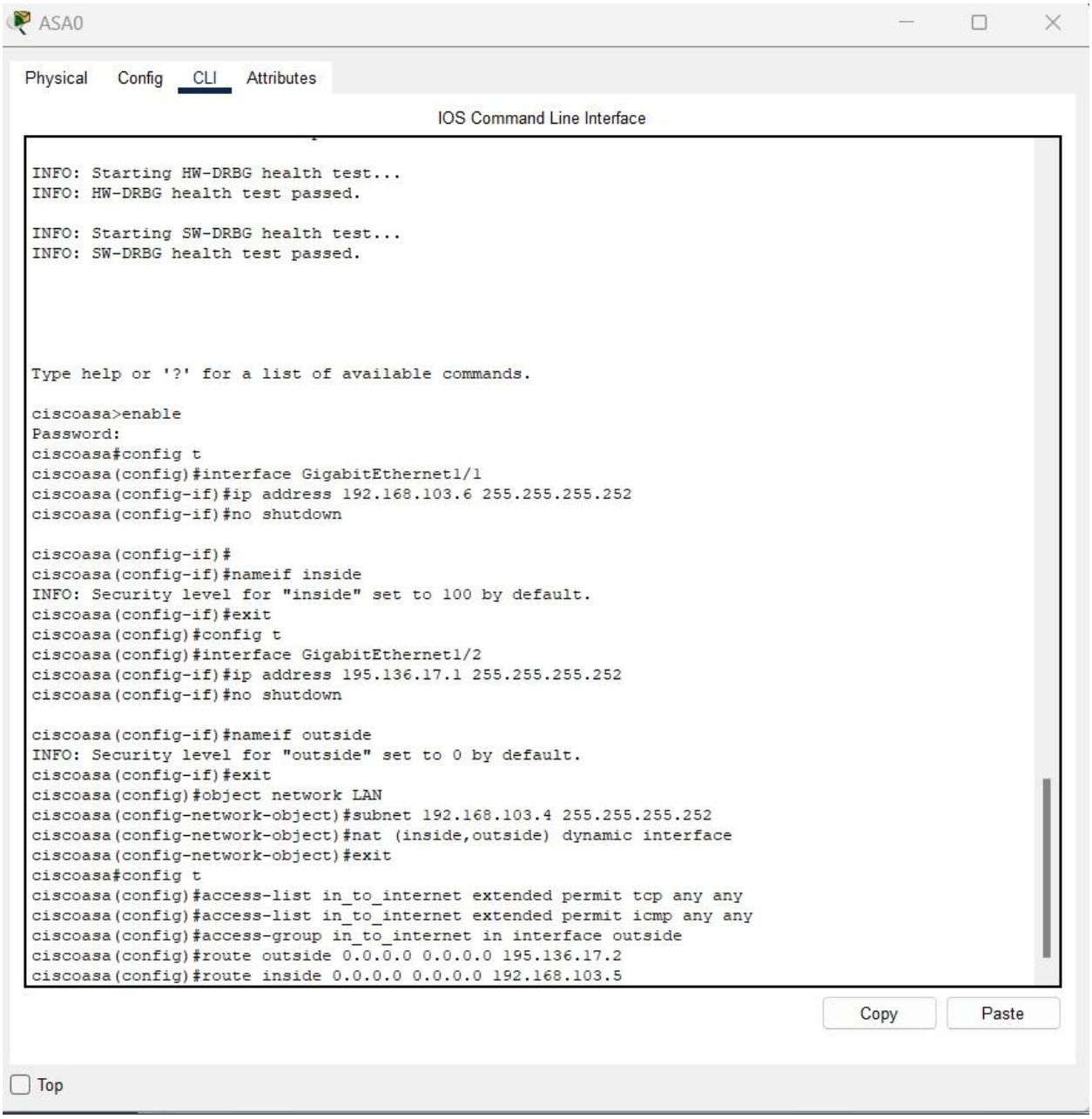



HQ-router
Physical
Config
CLI
Attributes
IOS Command Line Interface
interface Serial0/1/1
 no ip address
 clock rate 2000000
!
interface Serial0/2/0
 ip address 192.168.102.249 255.255.255.252
 clock rate 64000
 crypto map VPN-MAP
!
interface Serial0/2/1
 no ip address
 ip nat outside
 clock rate 64000
!
interface FastEthernet0/3/0
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/3/1
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/3/2
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/3/3
 switchport mode access
 switchport nonegotiate
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 10
 log-adjacency-changes
 network 192.168.102.240 0.0.0.3 area 0
 network 192.168.102.244 0.0.0.3 area 0
 network 192.168.102.224 0.0.0.15 area 0
 network 192.168.102.248 0.0.0.3 area 0
 network 195.136.17.0 0.0.0.3 area 0
 network 195.136.17.4 0.0.0.3 area 0
 network 192.168.103.4 0.0.0.3 area 0
 network 192.168.103.12 0.0.0.3 area 0
!

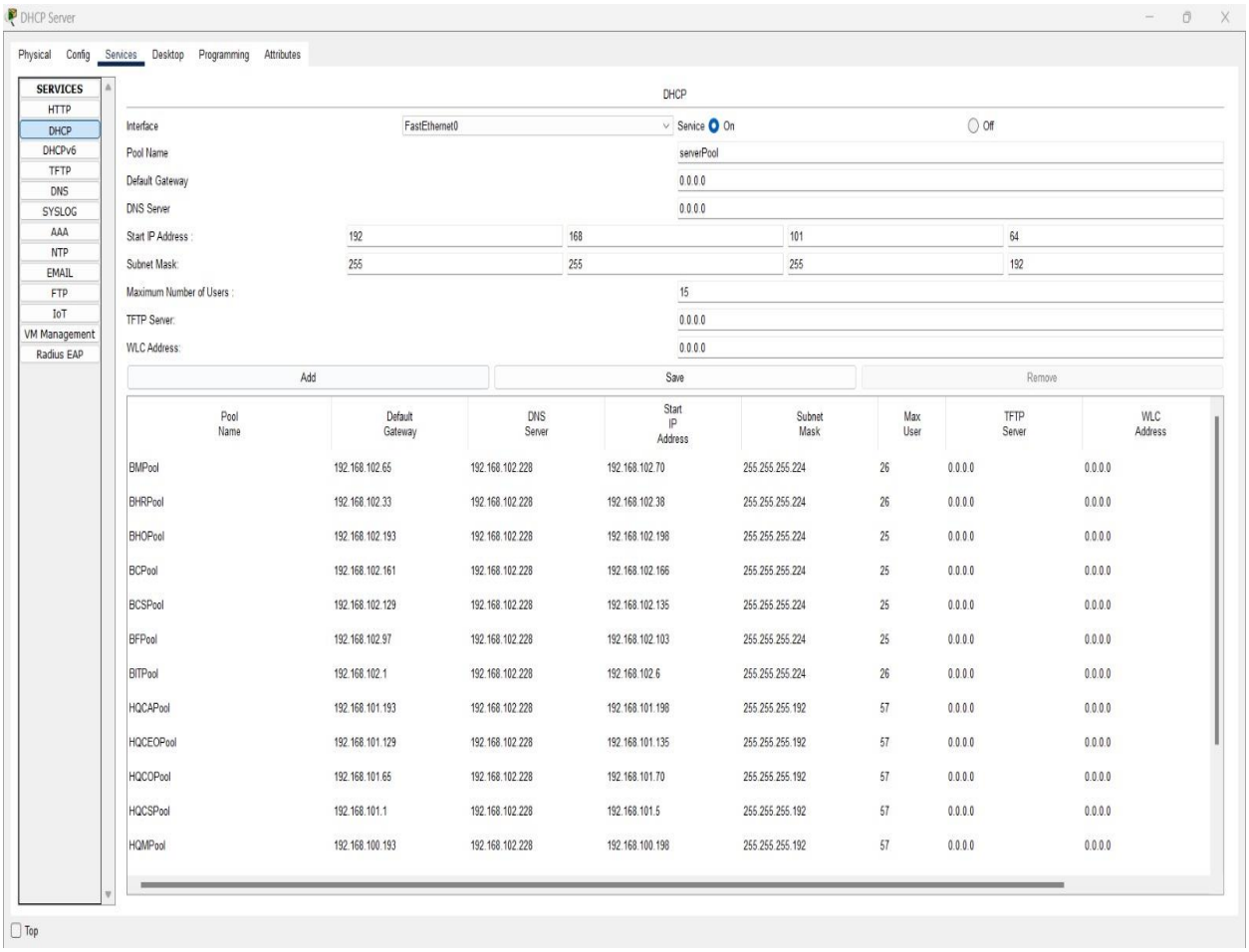

HQ-router
Physical
Config
CLI
Attributes
IOS Command Line Interface
 network 192.168.103.4 0.0.0.3 area 0
 network 192.168.103.12 0.0.0.3 area 0
!
ip nat inside source list 1 interface Serial0/1/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 195.136.17.2
ip route 0.0.0.0 0.0.0.0 195.136.17.6 70
ip route 0.0.0.0 0.0.0.0 192.168.103.6
ip route 0.0.0.0 0.0.0.0 192.168.103.12 70
!
ip flow-export version 9
!
!
access-list 1 permit 192.168.100.0 0.0.0.63
access-list 1 permit 192.168.100.64 0.0.0.63
access-list 1 permit 192.168.100.128 0.0.0.63
access-list 1 permit 192.168.100.192 0.0.0.63
access-list 1 permit 192.168.101.0 0.0.0.63
access-list 1 permit 192.168.100.0 0.0.0.6
access-list 1 permit 192.168.101.192 0.0.0.63
access-list 1 permit 192.168.101.64 0.0.0.63
access-list 1 permit 192.168.101.128 0.0.0.63
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.102.0 0.0.0.255
access-list 110 permit ip 192.168.101.0 0.0.0.255 192.168.102.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.102.0 0.0.0.31
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.102.32 0.0.0.31
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.102.64 0.0.0.31
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.102.96 0.0.0.31
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.102.128 0.0.0.31
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.102.160 0.0.0.31
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.102.192 0.0.0.31
access-list 110 permit ip 192.168.101.0 0.0.0.255 192.168.102.0 0.0.0.31
access-list 110 permit ip 192.168.101.0 0.0.0.255 192.168.102.32 0.0.0.31
access-list 110 permit ip 192.168.101.0 0.0.0.255 192.168.102.64 0.0.0.31
access-list 110 permit ip 192.168.101.0 0.0.0.255 192.168.102.96 0.0.0.31
access-list 110 permit ip 192.168.101.0 0.0.0.255 192.168.102.128 0.0.0.31
access-list 110 permit ip 192.168.101.0 0.0.0.255 192.168.102.160 0.0.0.31
access-list 110 permit ip 192.168.101.0 0.0.0.255 192.168.102.192 0.0.0.31
!
banner motd ^CNo Unauthorized Access^C
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
Copy
Paste
Top

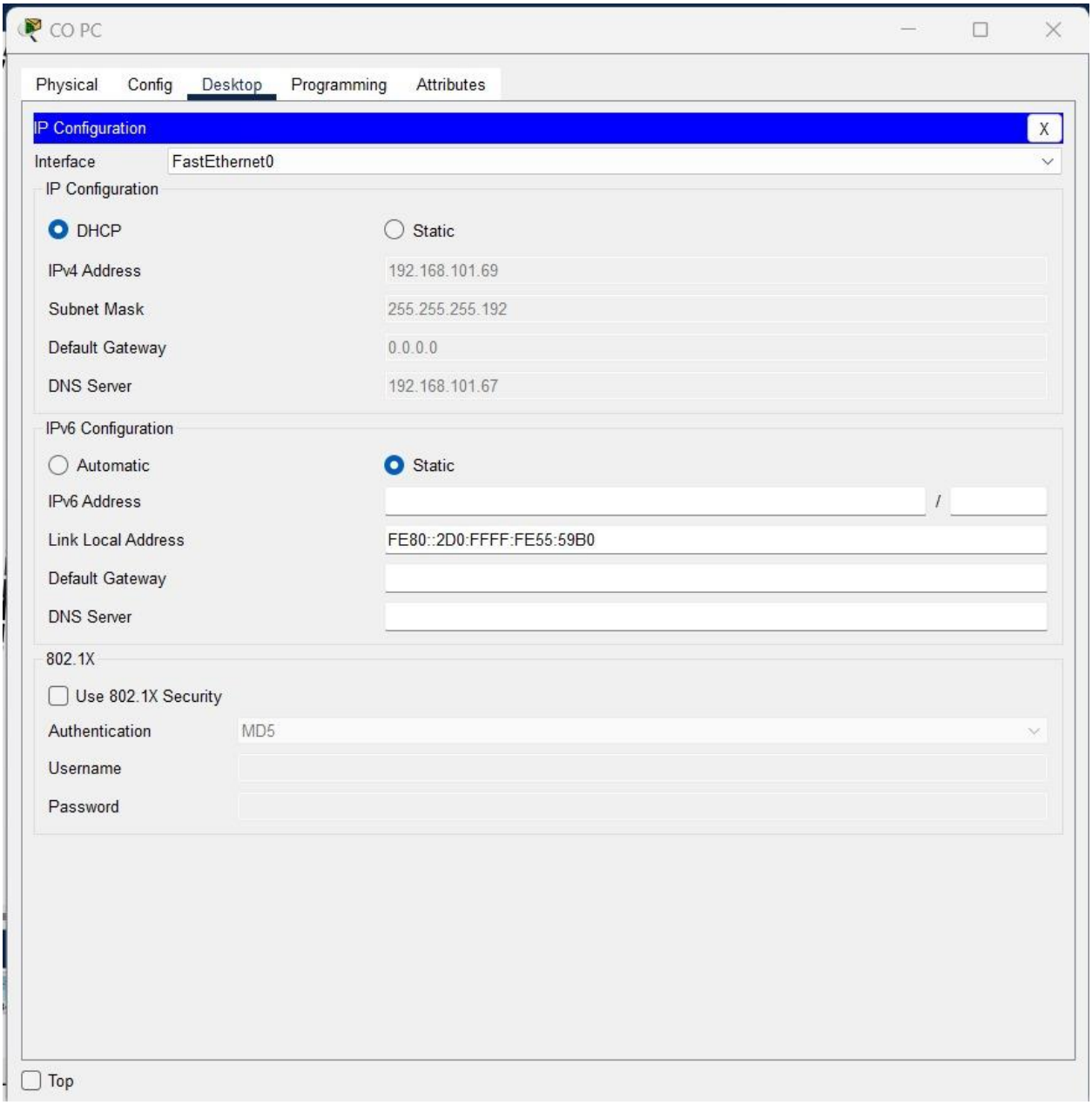

!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 access-class 23 in
 transport input ssh
!
!
!
end
HQ-Router#
Copy
Paste
Top

3.2.4 Configuring Firewall

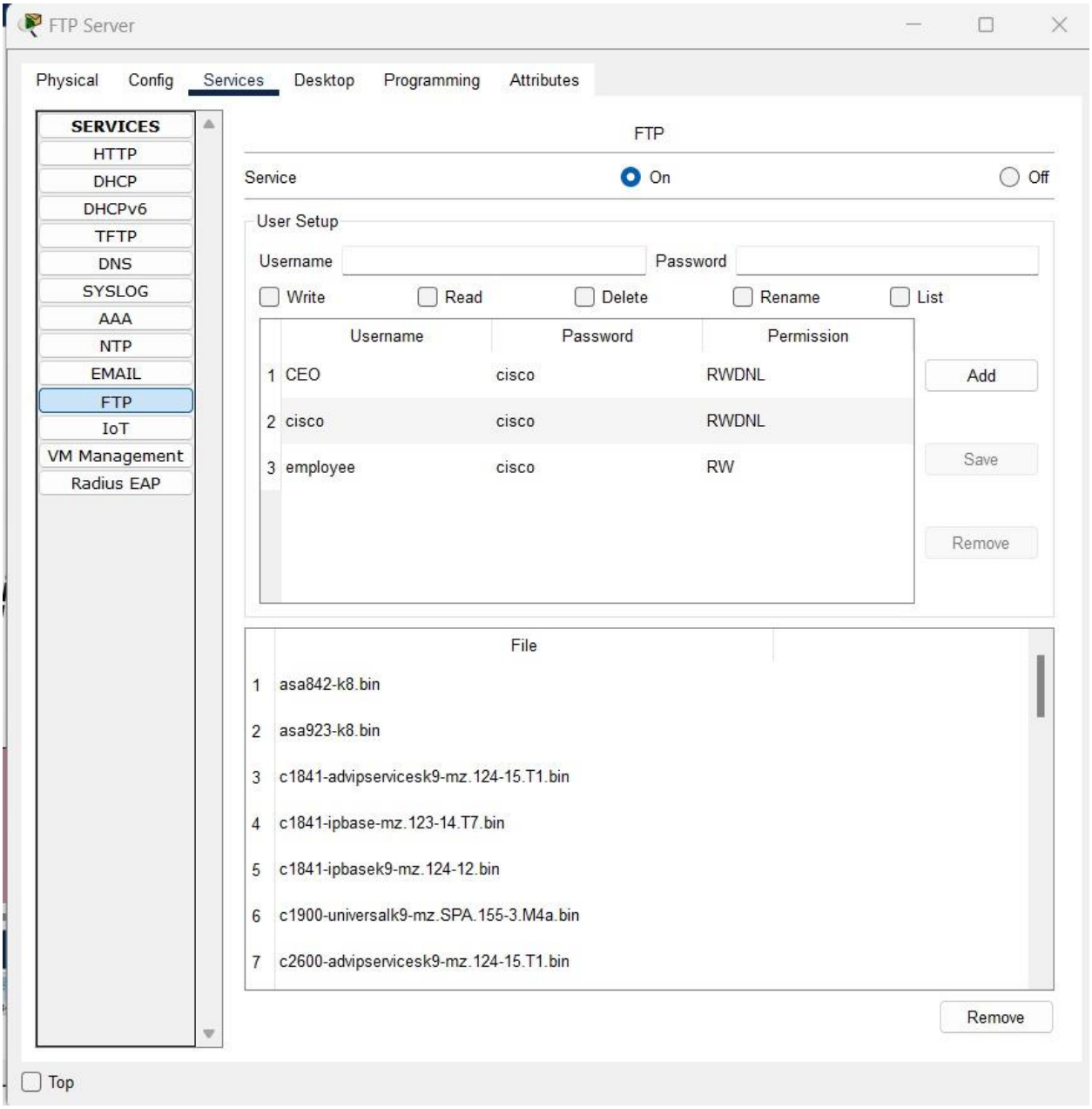


3.2.5 Configuring DHCP Server




CO PC
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.101.69
Subnet Mask
255.255.255.192
Default Gateway
0.0.0.0
DNS Server
192.168.101.67
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::2D0:FFFF:FE55:59B0
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

3.2.6 Configuring FTP Server



PHASE 4

4.1 Testing

- We should always verify whether the design meets the business goals and technical goals for the network that is desired by the clients.
- There is strict validation required for LAN and WAN selections depending upon the requirements of the network design.
- Should verify if there is any connectivity throughout the network design.
- Testing should also help as they are the deciding factor to select the correct optimizing technique which is the next step after testing.

4.1.1 Types of Tests

- Application Response-Time Testing.
- Throughput Testing.
- Availability Testing.
- AES Testing.

These are the various kinds of tests performed.

Application Response-Time Testing: Response Time Testing determines how quickly one system node responds to another's request. It is the time it takes for a system to get to a given input and complete the process.

Throughput Testing: The number of packets that successfully arrive at their destinations is measured by throughput. Throughput capacity is usually expressed in bits per second, although it can alternatively be expressed as data per second. Packet arrival is critical for high-performance network service. Testing throughput for a given network is very crucial for the design.

Availability Testing: Availability testing, also known as Durability testing, is a type of performance testing in which the application is run for a specified length of time, failure events and repair times are collected, and the availability percentage is compared to the service level agreement.

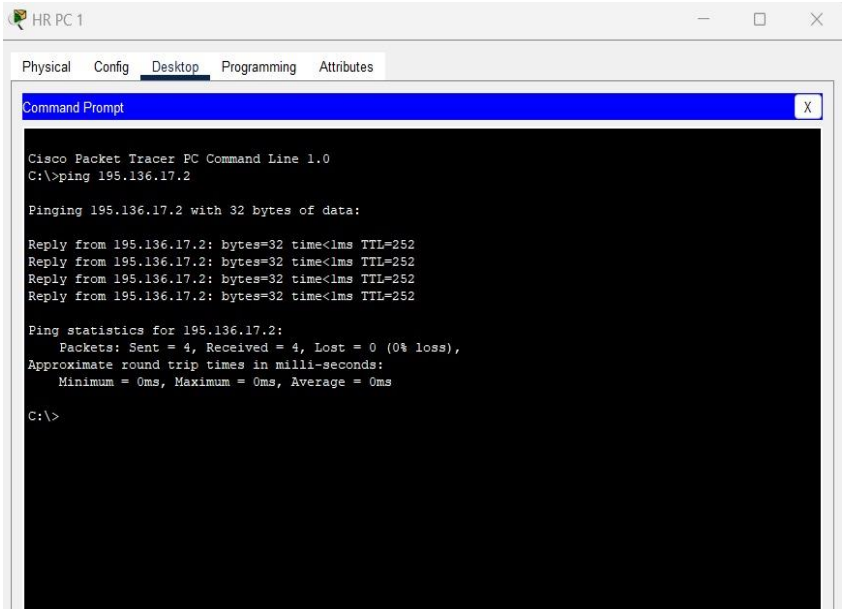
AES Testing: AES (Advanced Encryption Standard) is a widely used encryption algorithm used to protect sensitive data. AES testing typically involves evaluating the strength, speed, and efficiency of the encryption algorithm.

The advantages of AES testing include:

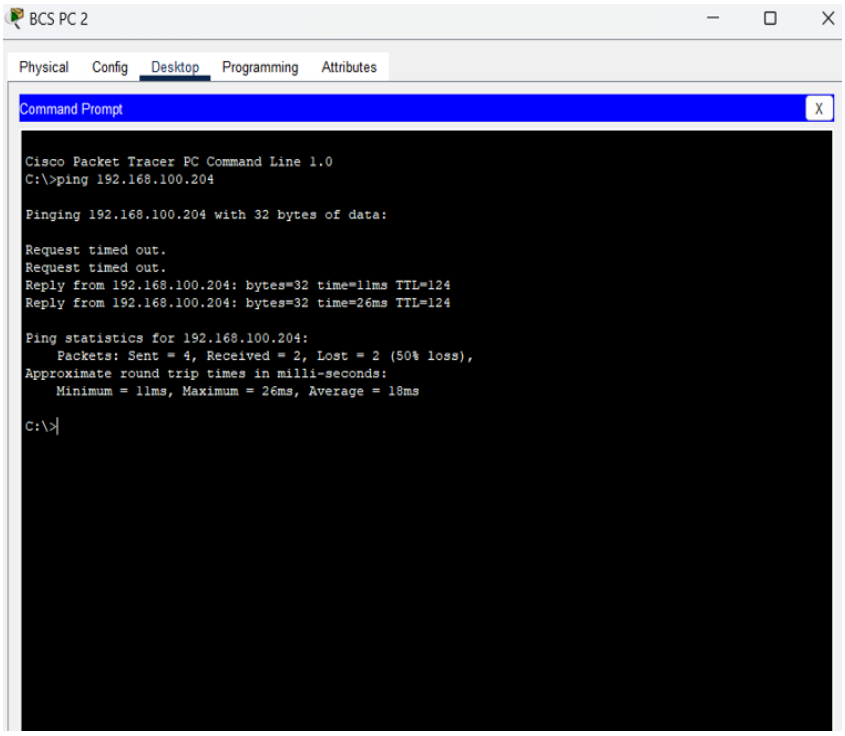
- Ensuring data security.
- Identifying vulnerabilities.
- Improving performance.
- Compliance with regulations.

4.2 NETWORK TESTING

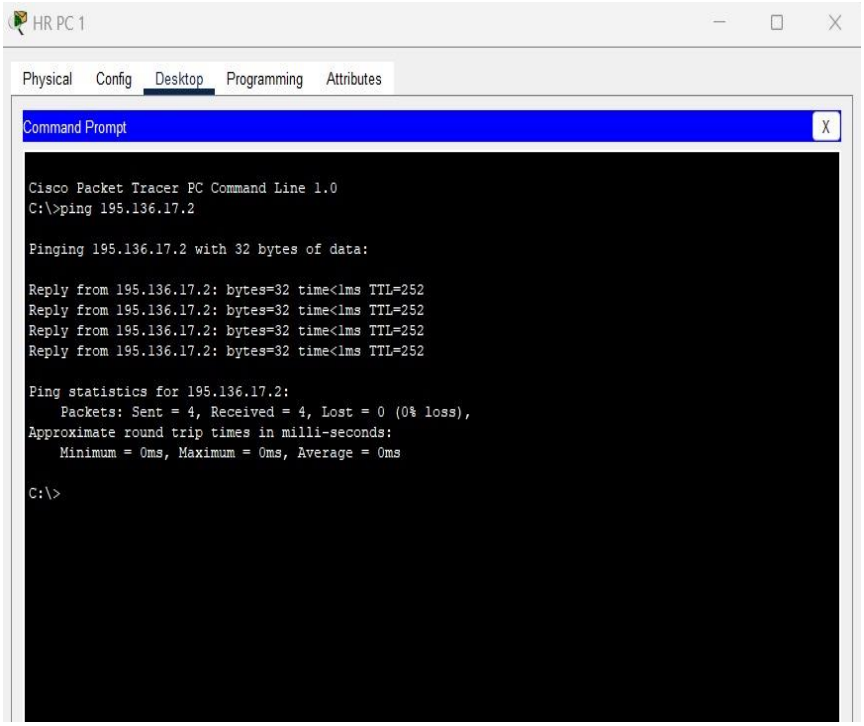
Pinging from HQ to Branch Network



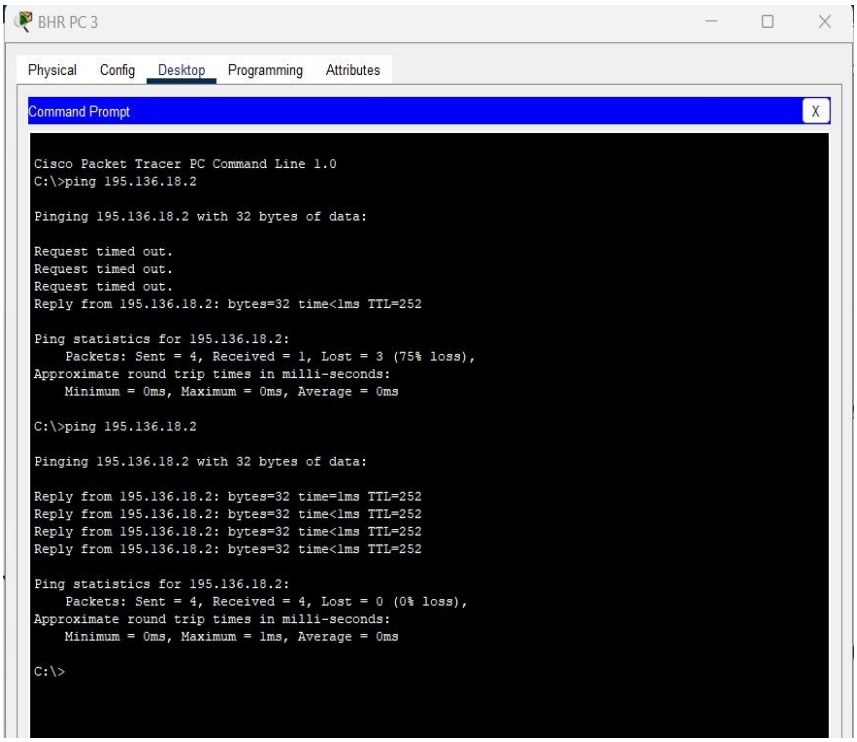
Pinging from Branch Network to HQ



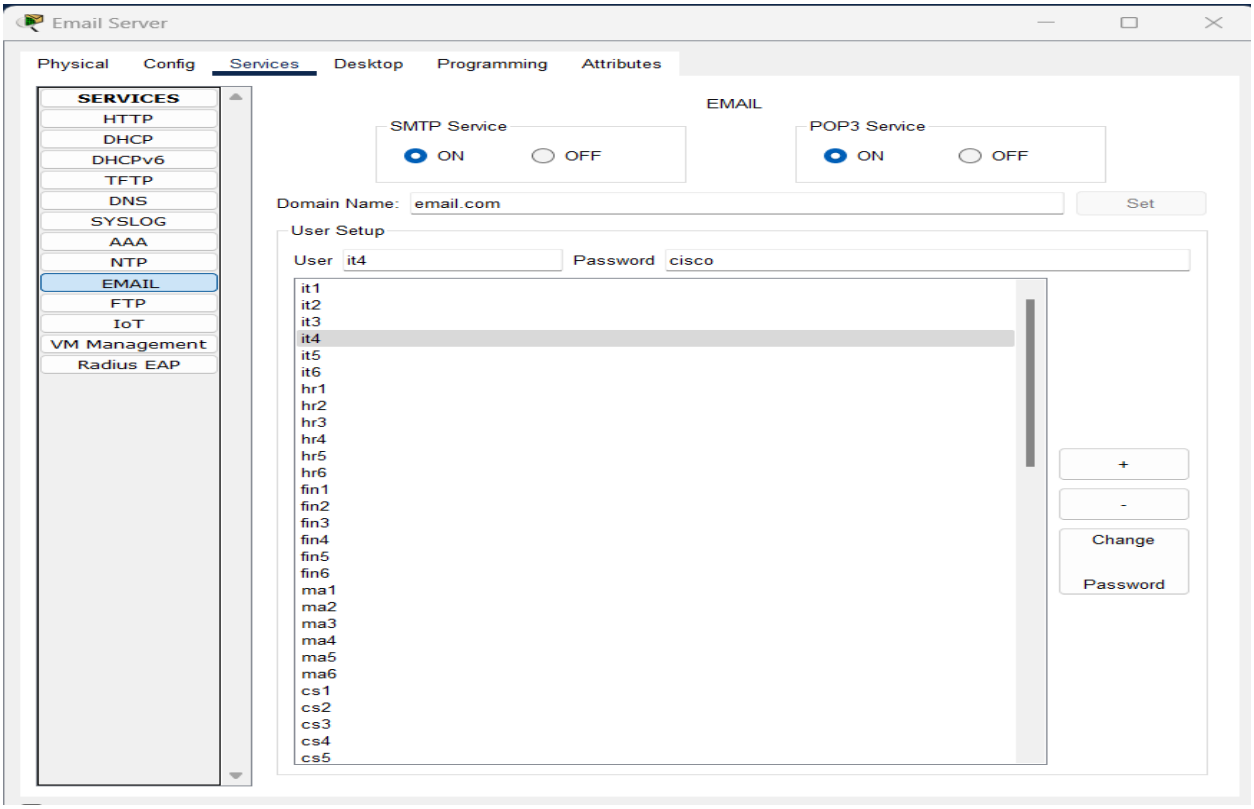
Pinging from HQ to ISP1

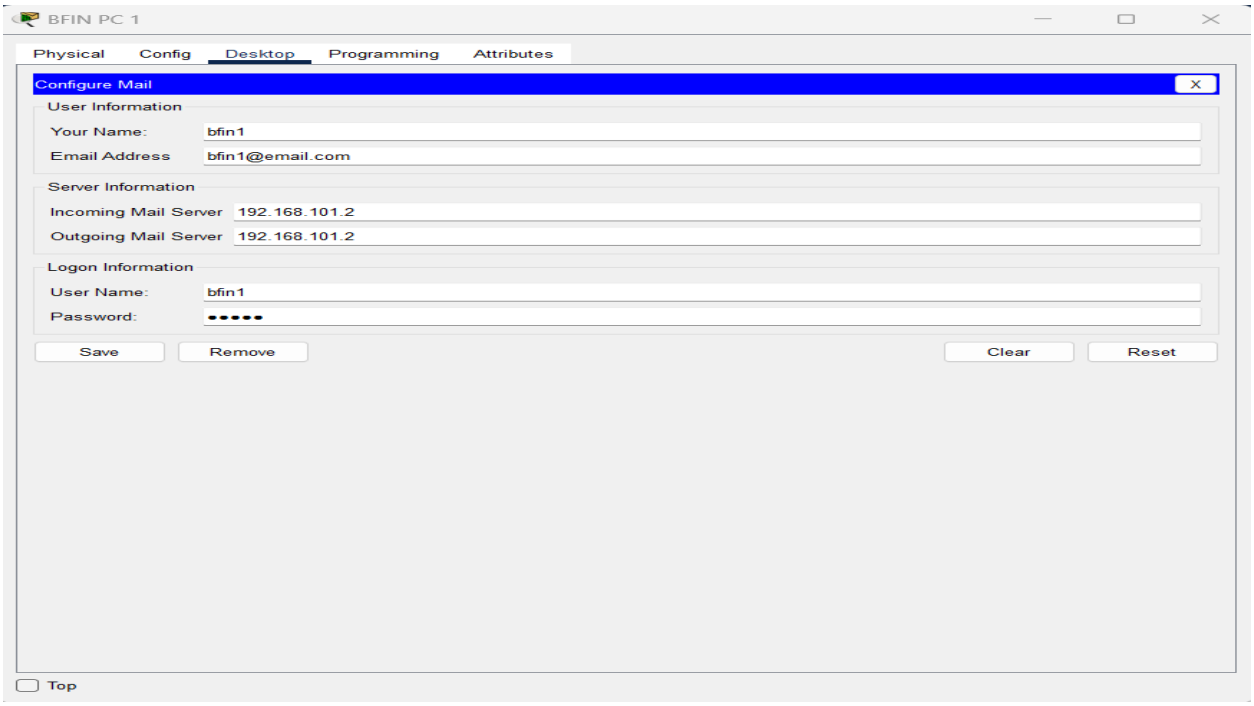


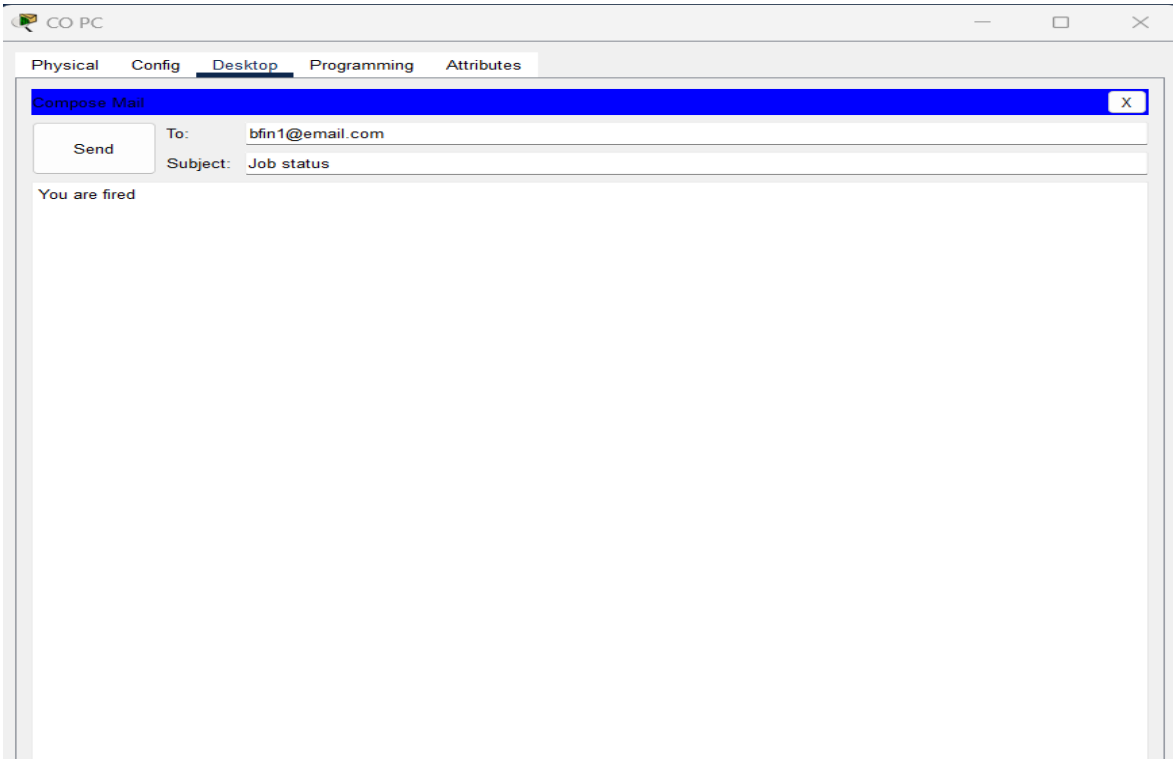
Pinging from Branch Network to ISP2

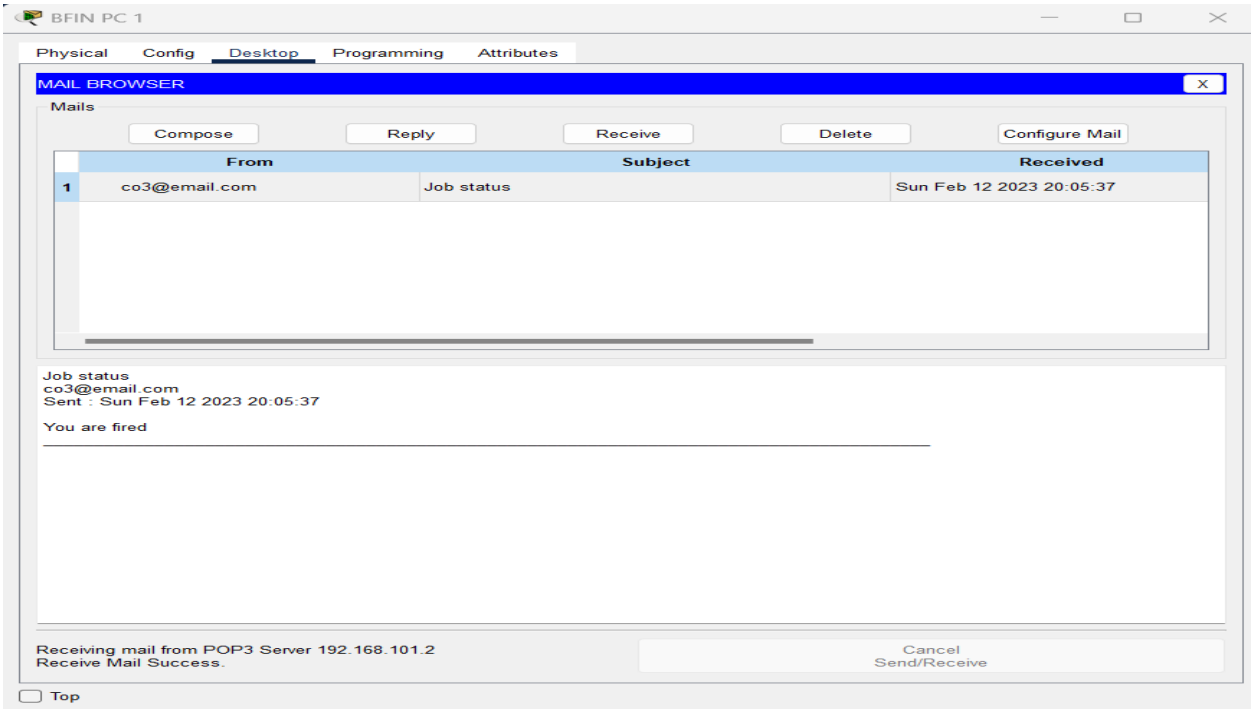


Accessing Email Server

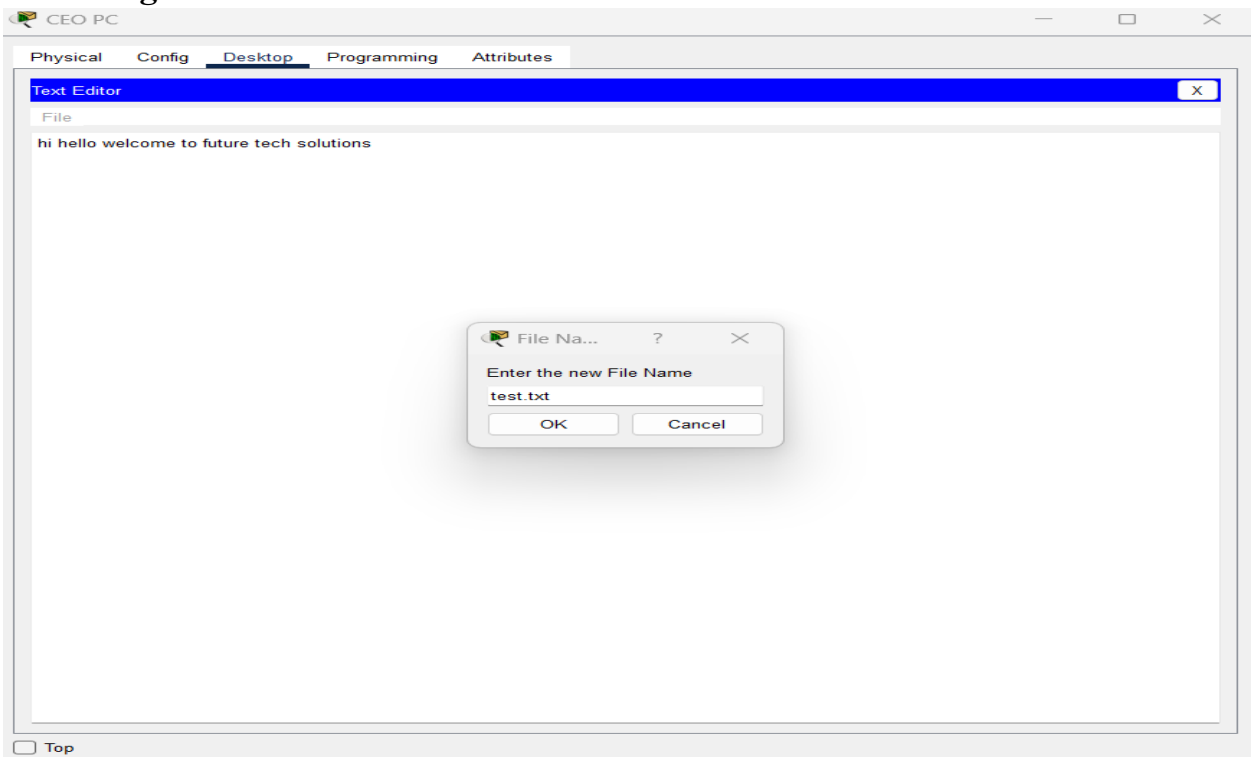


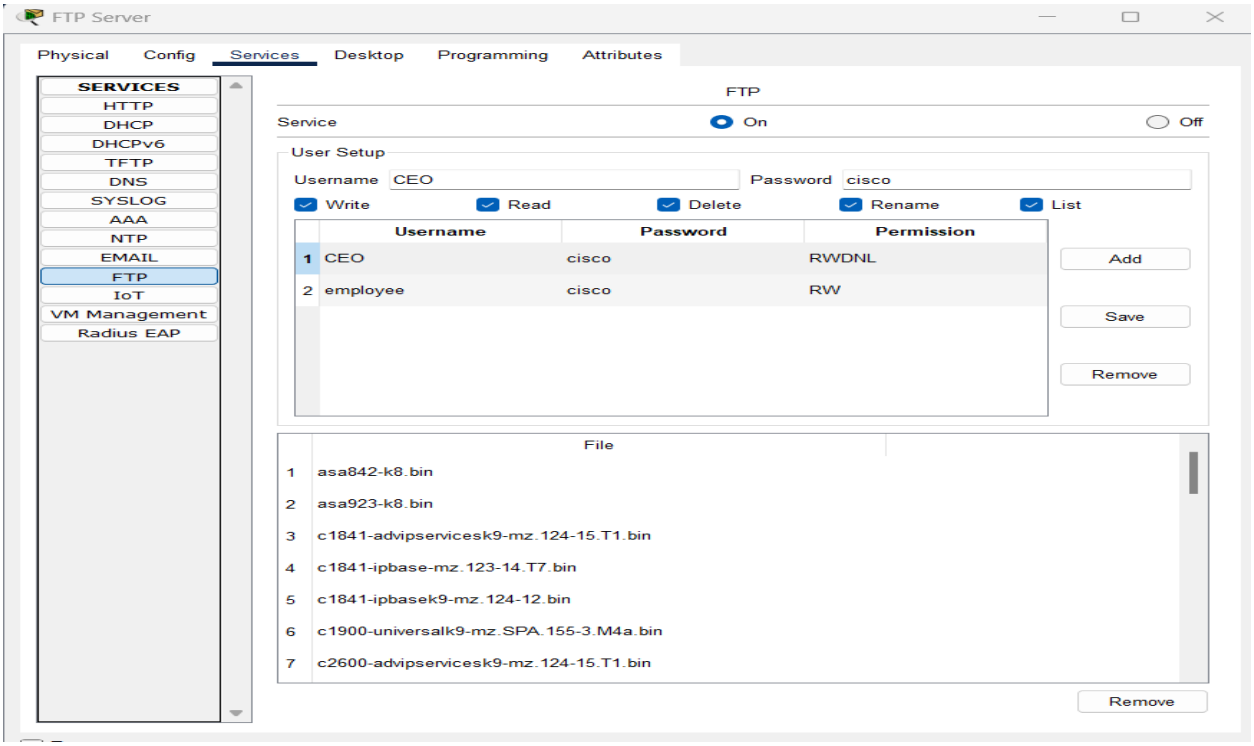


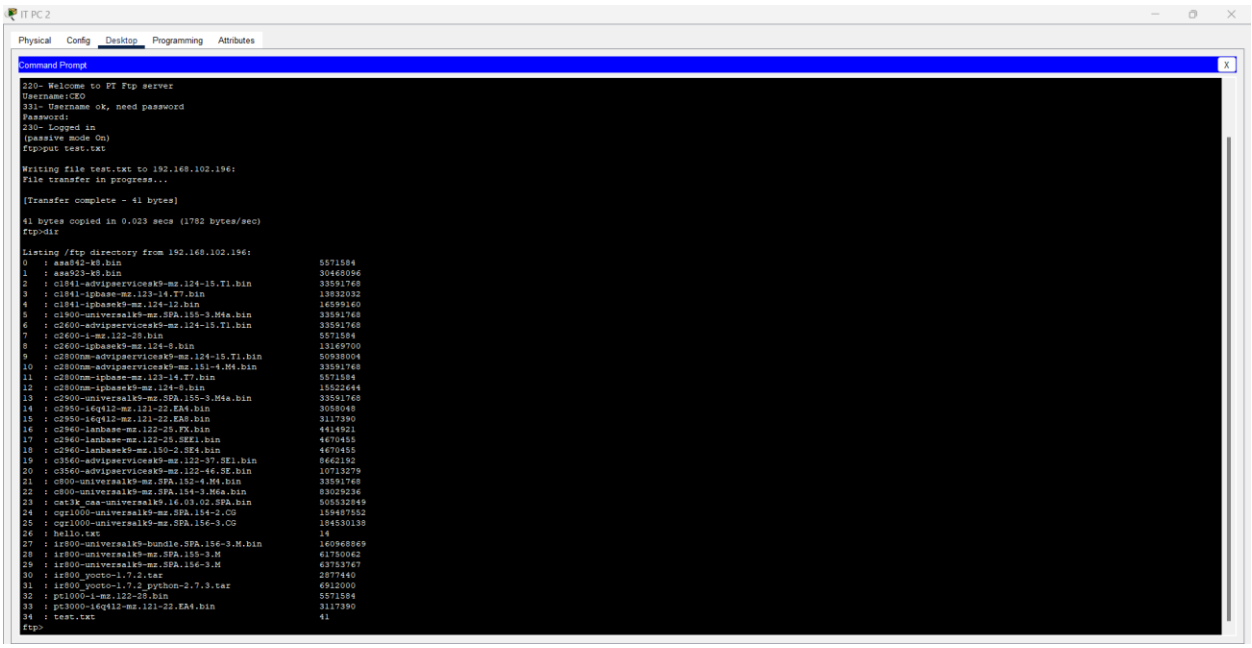

CO PC
Physical
Config
Desktop
Programming
Attributes
Compose Mail
Send
To:
bfin1@email.com
Subject:
Job status
You are fired

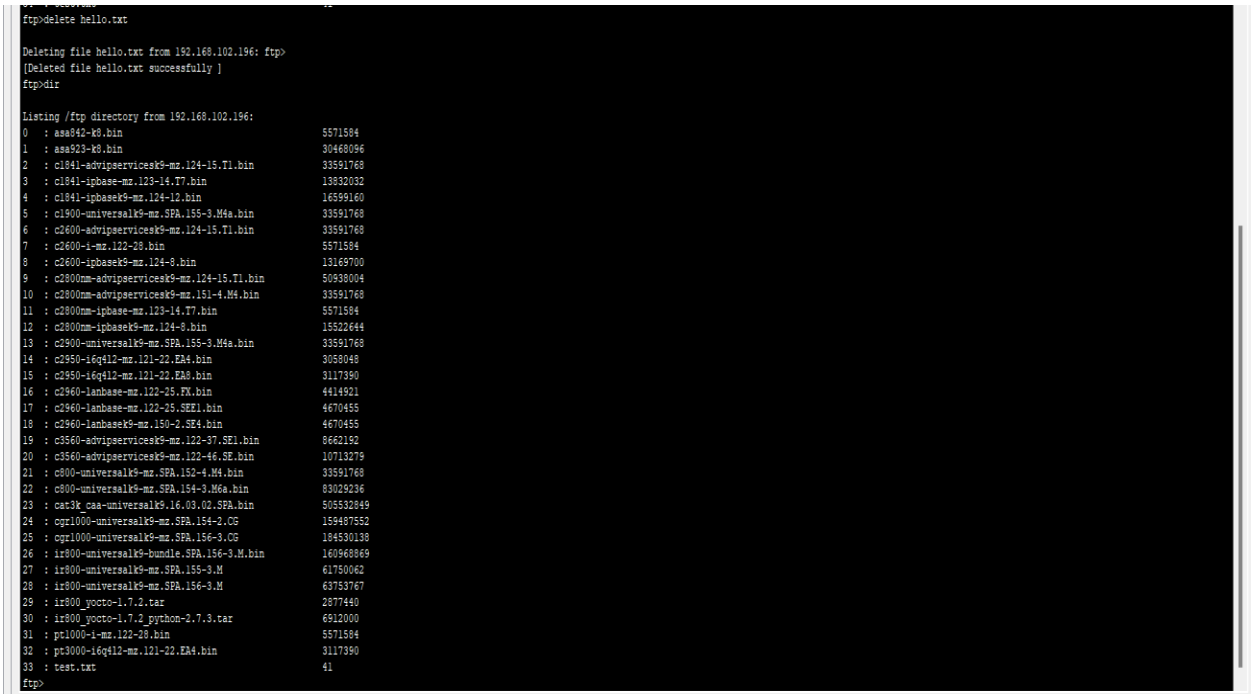

BFIN PC 1
Physical
Config
Desktop
Programming
Attributes
MAIL BROWSER
Mails
Compose
Reply
Receive
Delete
Configure Mail
From
Subject
Received
1
co3@email.com
Job status
Sun Feb 12 2023 20:05:37
Job status
co3@email.com
Sent : Sun Feb 12 2023 20:05:37
You are fired
Receiving mail from POP3 Server 192.168.101.2
Receive Mail Success.
Cancel
Send/Receive
Top

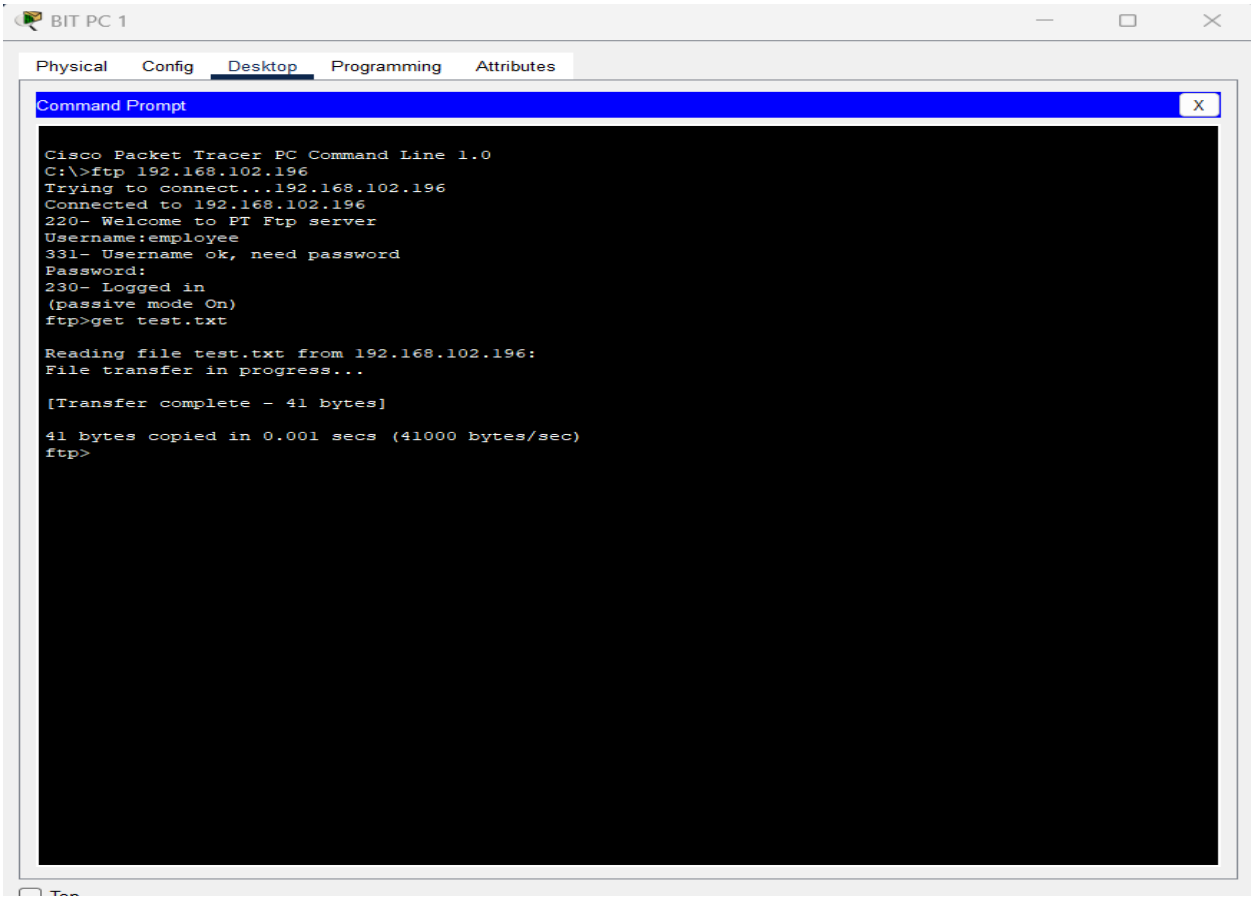
Accessing FTP Server

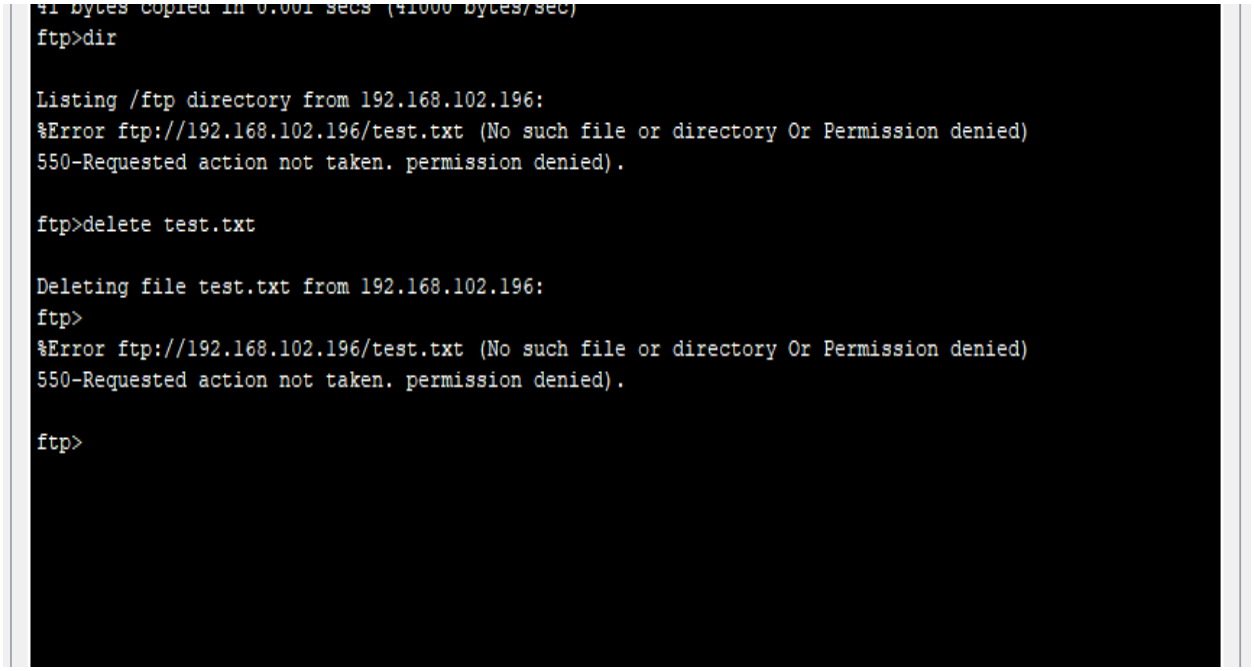


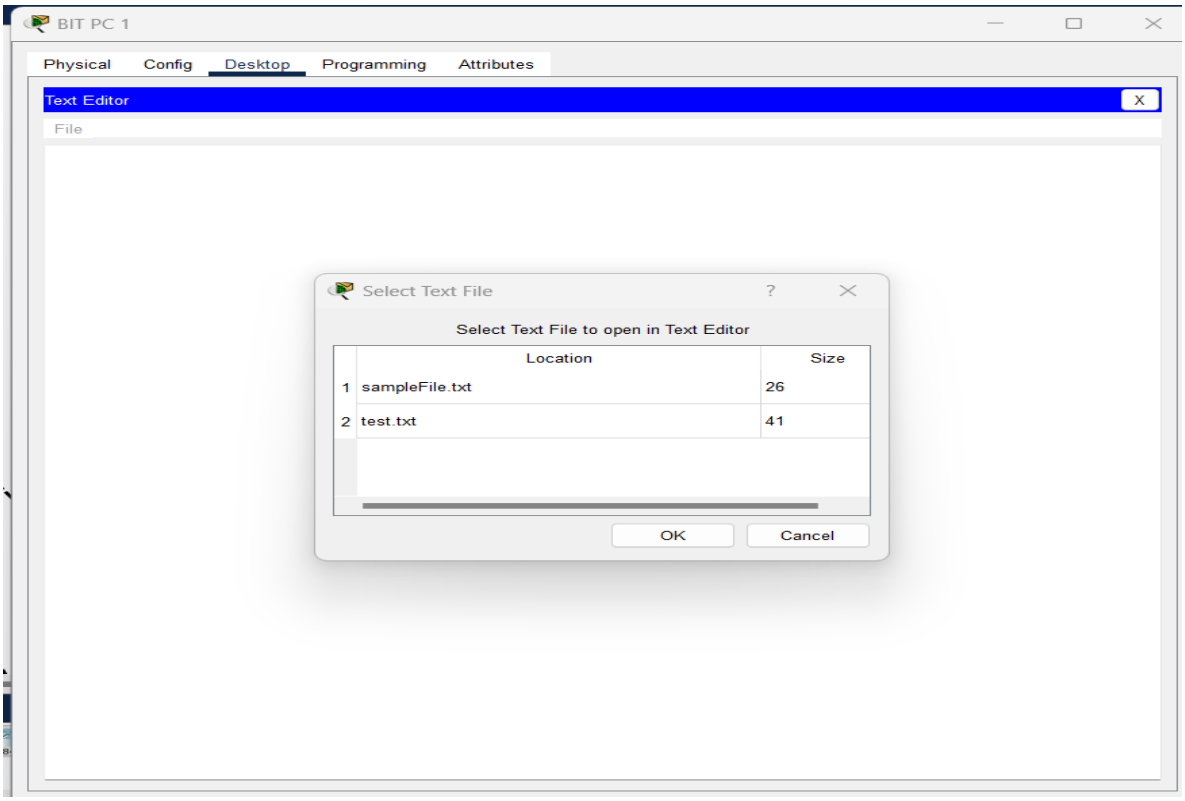



IT PC 2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
220- Welcome to PT Ftp server
Username:CEO
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put test.txt
Writing file test.txt to 192.168.102.196:
File transfer in progress...
[Transfer complete - 41 bytes]
41 bytes copied in 0.023 secs (1782 bytes/sec)
ftp>dir
Listing /ftp directory from 192.168.102.196:
0 : asa842-k8.bin 5571584
1 : asa923-k8.bin 30468096
2 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
3 : c1841-ipbase-mz.123-14.T7.bin 13832032
4 : c1841-ipbasek9-mz.124-12.bin 16599160
5 : c1900-universalk9-mz.SPA.155-3.M4a.bin 33591768
6 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
7 : c2600-i-mz.122-28.bin 5571584
8 : c2600-ipbasek9-mz.124-8.bin 13169700
9 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
10 : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
11 : c2800nm-ipbase-mz.123-14.T7.bin 5571584
12 : c2800nm-ipbasek9-mz.124-8.bin 15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin 33591768
14 : c2950-i6q412-mz.121-22.EA4.bin 3058048
15 : c2950-i6q412-mz.121-22.EA8.bin 3117390
16 : c2960-lanbase-mz.122-25.FX.bin 4414921
17 : c2960-lanbase-mz.122-25.SEE1.bin 4670455
18 : c2960-lanbasek9-mz.150-2.SE4.bin 4670455
19 : c3560-advipservicesk9-mz.122-37.SE1.bin 8662192
20 : c3560-advipservicesk9-mz.122-46.SE.bin 10713279
21 : c800-universalk9-mz.SPA.152-4.M4.bin 33591768
22 : c800-universalk9-mz.SPA.154-3.M6a.bin 83029236
23 : cat3k_caa-universalk9.16.03.02.SPA.bin 505532849
24 : cgr1000-universalk9-mz.SPA.154-2.CG 159487552
25 : cgr1000-universalk9-mz.SPA.156-3.CG 184530138
26 : hello.txt 14
27 : ir800-universalk9-bundle.SPA.156-3.M.bin 160968869
28 : ir800-universalk9-mz.SPA.155-3.M 61750062
29 : ir800-universalk9-mz.SPA.156-3.M 63753767
30 : ir800_yocto-1.7.2.tar 2877440
31 : ir800_yocto-1.7.2_python-2.7.3.tar 6912000
32 : pt1000-i-mz.122-28.bin 5571584
33 : pt3000-i6q412-mz.121-22.EA4.bin 3117390
34 : test.txt 41
ftp>


ftp>delete hello.txt
Deleting file hello.txt from 192.168.102.196: ftp>
[Deleted file hello.txt successfully]
ftp>dir
Listing /ftp directory from 192.168.102.196:
0 : asa842-k8.bin 5571584
1 : asa923-k8.bin 30468096
2 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
3 : c1841-ipbase-mz.123-14.T7.bin 13832032
4 : c1841-ipbasek9-mz.124-12.bin 16599160
5 : c1900-universalk9-mz.SPA.155-3.M4a.bin 33591768
6 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
7 : c2600-i-mz.122-28.bin 5571584
8 : c2600-ipbasek9-mz.124-8.bin 13169700
9 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
10 : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
11 : c2800nm-ipbase-mz.123-14.T7.bin 5571584
12 : c2800nm-ipbasek9-mz.124-8.bin 15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin 33591768
14 : c2950-i6q412-mz.121-22.EA4.bin 3058048
15 : c2950-i6q412-mz.121-22.EA8.bin 3117390
16 : c2960-lanbase-mz.122-25.FX.bin 4414921
17 : c2960-lanbase-mz.122-25.SEE1.bin 4670455
18 : c2960-lanbasek9-mz.150-2.SE4.bin 4670455
19 : c3560-advipservicesk9-mz.122-37.SE1.bin 8662192
20 : c3560-advipservicesk9-mz.122-46.SE.bin 10713279
21 : c800-universalk9-mz.SPA.152-4.M4.bin 33591768
22 : c800-universalk9-mz.SPA.154-3.M6a.bin 83029236
23 : cat3k_caa-universalk9.16.03.02.SPA.bin 505532849
24 : cgr1000-universalk9-mz.SPA.154-2.CG 159487552
25 : cgr1000-universalk9-mz.SPA.156-3.CG 184530138
26 : ir800-universalk9-bundle.SPA.156-3.M.bin 160968869
27 : ir800-universalk9-mz.SPA.155-3.M 61750062
28 : ir800-universalk9-mz.SPA.156-3.M 63753767
29 : ir800_yocto-1.7.2.tar 2877440
30 : ir800_yocto-1.7.2_python-2.7.3.tar 6912000
31 : pt1000-i-mz.122-28.bin 5571584
32 : pt3000-i6q412-mz.121-22.EA4.bin 3117390
33 : test.txt 41
ftp>


BIT PC 1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.102.196
Trying to connect...192.168.102.196
Connected to 192.168.102.196
220- Welcome to PT Ftp server
Username:employee
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>get test.txt
Reading file test.txt from 192.168.102.196:
File transfer in progress...
[Transfer complete - 41 bytes]
41 bytes copied in 0.001 secs (41000 bytes/sec)
ftp>


41 bytes copied in 0.001 secs (41000 bytes/sec)
ftp>dir
Listing /ftp directory from 192.168.102.196:
%Error ftp://192.168.102.196/test.txt (No such file or directory Or Permission denied)
550-Requested action not taken. permission denied).
ftp>delete test.txt
Deleting file test.txt from 192.168.102.196:
ftp>
%Error ftp://192.168.102.196/test.txt (No such file or directory Or Permission denied)
550-Requested action not taken. permission denied).
ftp>


BIT PC 1
Physical
Config
Desktop
Programming
Attributes
Text Editor
X
File
Select Text File
Select Text File to open in Text Editor
Location
Size
1
sampleFile.txt
26
2
test.txt
41
OK
Cancel

Accessing Website