Version 1.0

NAMAL INSTITUTE
MIANWALI

Department of Electrical Engineering

EE– 432L – Computer Networks Lab

Complete Design of a Network For Software House

Student Name	UET's ID	Marks
Mureed Qasim Shah	**2018-UET-NML-ELECT-37**	

Date: December 20, 2021

Instructor: Dr. Hamza Zad Gul

Lab Engineer: Engr. Muhammad Waqas

Table of Contents

Introduction 3
Equipment 3
Network Design 3
Corporate Building 4
Administration Building 5
Programming Building 6
Services Installed: 7
Email Service 8
FTP Service 9
ICMP Service 10
Routing Table 10
MAC/Forwarding Table 11
Ping Operation 13
Network Devices Information: 14
Potential point of weakness in the network: 14
An Estimated Cost for the Network Devices 15
Suggestion for Improvement 15
Conclusion 15
References 16

Introduction

In this project, we will design and simulate a complete computer network for a software house with essential services using Packet Tracer. Packet Tracer is a simulator that offers different network services to configure and build networks ranging from small to medium scale both in physical and logical mode. These services include Email, HTTP, DNS, FTP, DHCP etc. We will get hands on experience of Packet Tracer Physical Layer system, medium scale network deployment, and basic configuration of Software House network and end devices. We will also practice setting up network and its configuration at medium scale to check and simulate the whole network topology.

Equipment

- Software
  - Packet Tracer

Network Design

We are required to design a network which is consisted of 3 buildings each in a different city using Physical layer in Packet Tracer as shown in the *figure 1*. The logical view of this network is also shown in *figure 2*. These buildings are connected via fiber cable. These buildings include:

1. Corporate Building
2. Administration Building
3. Programming Building

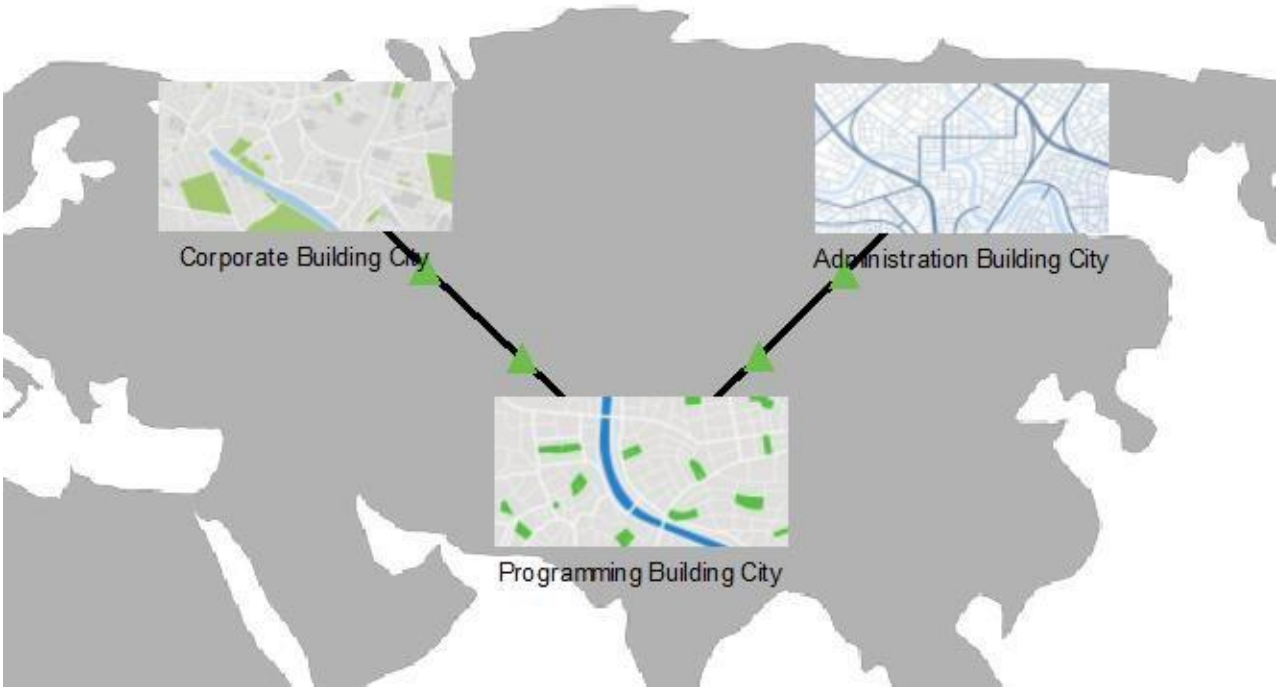

Figure 1: Software House Network in 3 Different Cities – Physical View

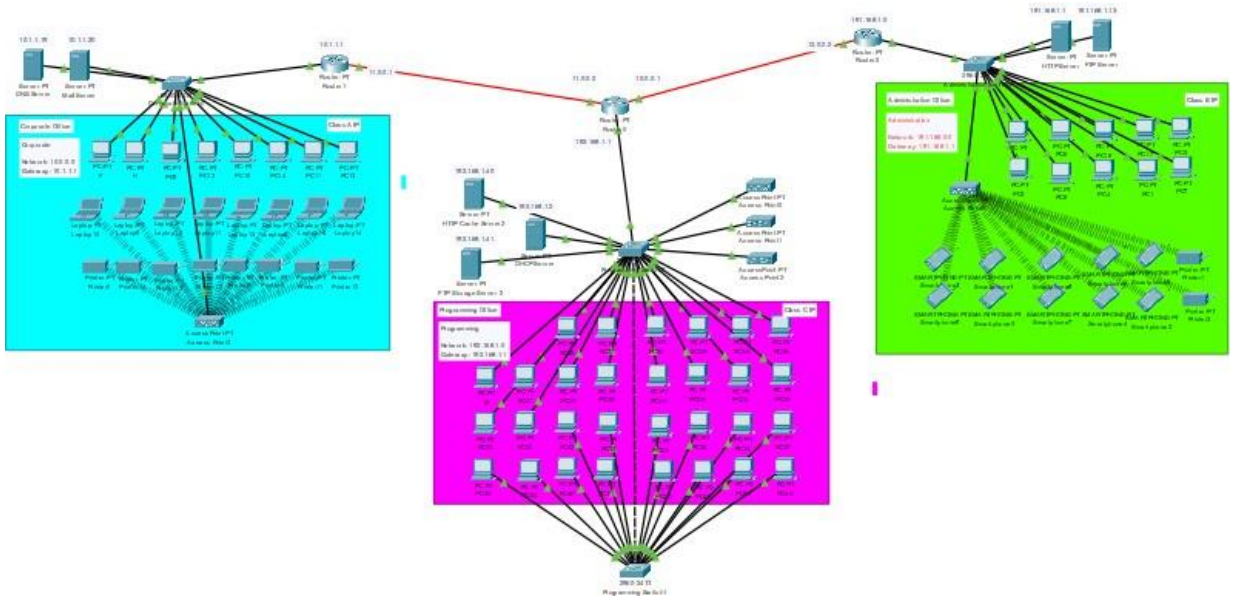

Figure 2: Software House Network in 3 Different Cities – Logical View

Corporate Building

The corporate office has the 8 offices with each office having a computer, wireless printer and laptop as shown in *figure 3*. We have placed a Mail Server in this Building and assigned **Class A** IP addresses in this building. These are static IP addresses assigned manually to each end device. The details are shown in figure below:

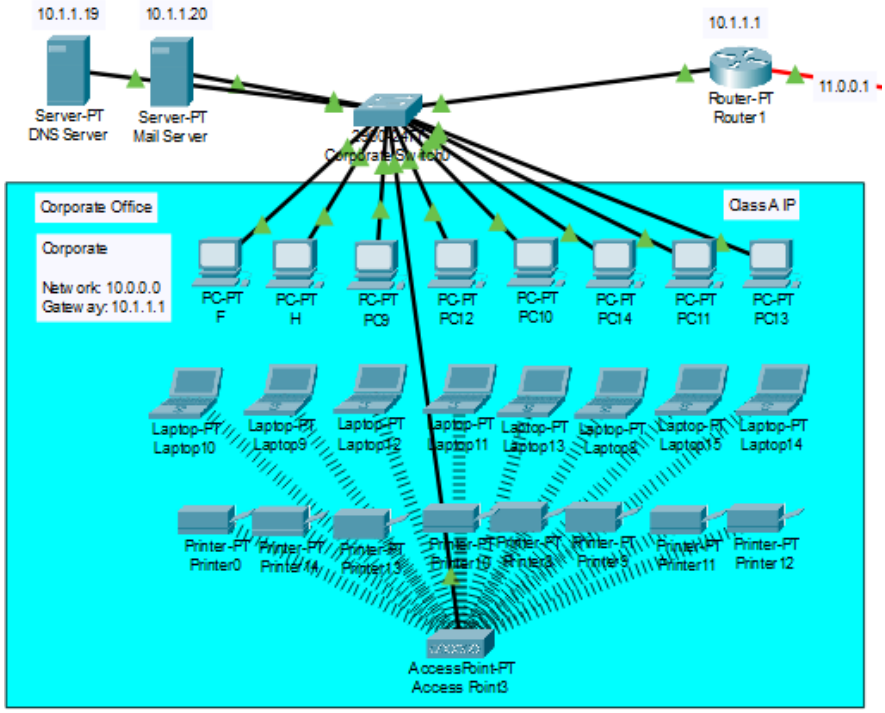

Figure 3: Corporate Building Network– Logical View

Figure 4: Corporate Building –Physical View

Administration Building

The administration office has the 10 offices with each office having a computer and mobile as shown in *figure 5*. We have placed a Web Server and Storage Server in this Building and assigned **Class B** IP addresses in this building. These are static IP addresses assigned manually to each end device.

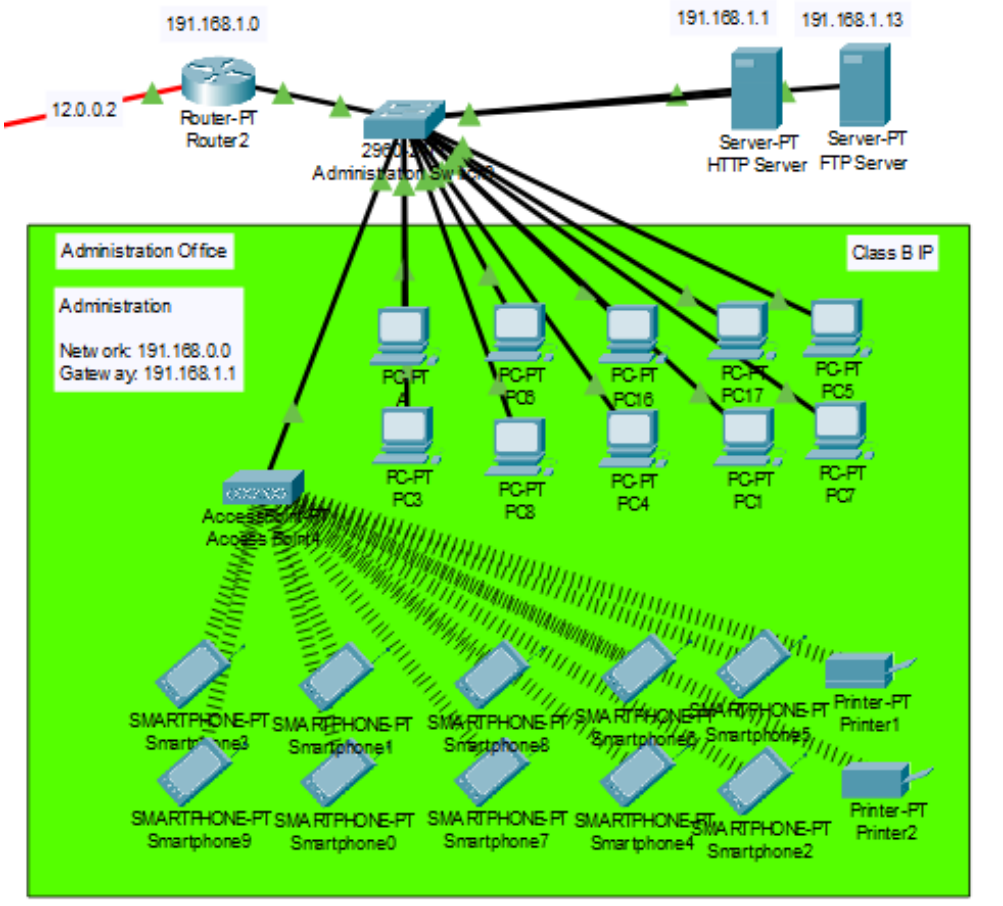

Figure 5: Administration Building Network –Logical View

Figure 6: Administration Building Network: Physical View

Programming Building

The programming office has 30 computers connected to a LAN (Static IP addressing) and 3 wireless access point to connect wireless devices as shown in *figure 7*. An internet connection from ISP is provided in this building. We have placed a Storage Server, Web cache and DHCP Server in this Building and assigned **Class C** IP addresses in this building. These are static IP addresses assigned manually to each end device. We have used DHCP Services for only wireless devices in this building.

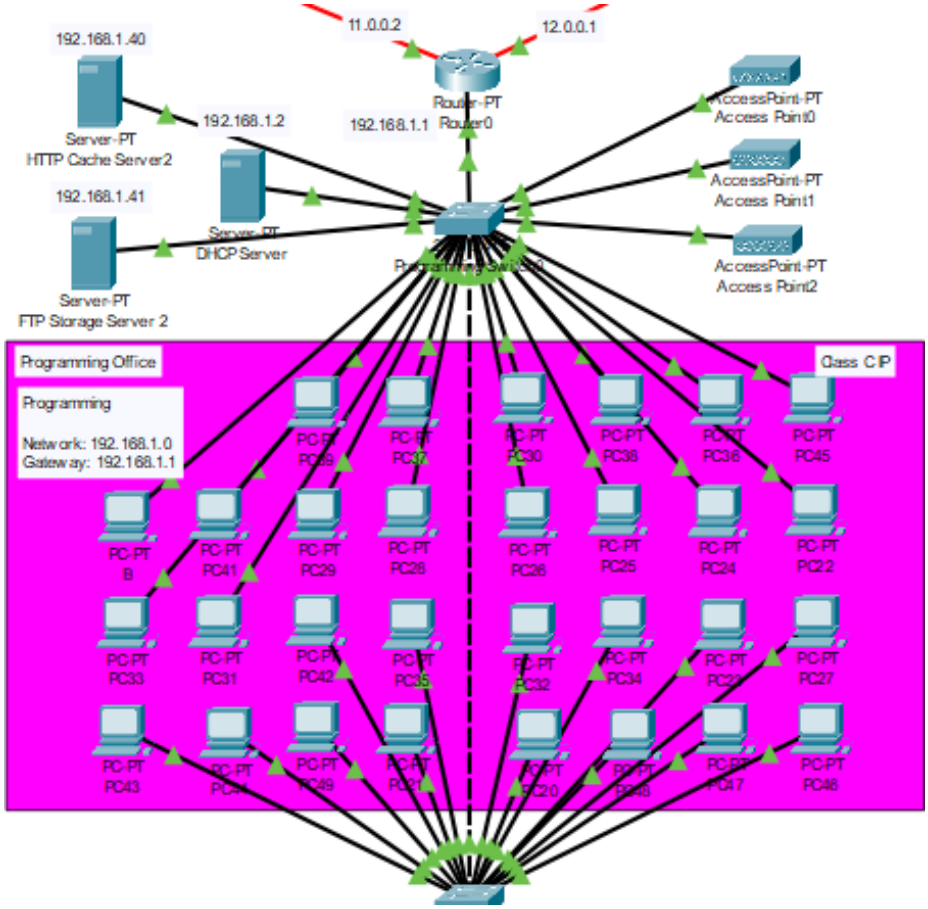

Figure 7: Programming Building Network: Logical View

Figure 8: Programming Building Network: Physical View

In this whole network, we have used PCs, printers and as well as wireless devices in all three buildings and configured them with all Servers of different services. These servers are connected to switches and these switches are connected with the routers that are acting as Internet Service Providers (ISP). These buildings are connected via **Fiber connection** (*red color in figure 9*) with each other as shown in *figure 9* below:

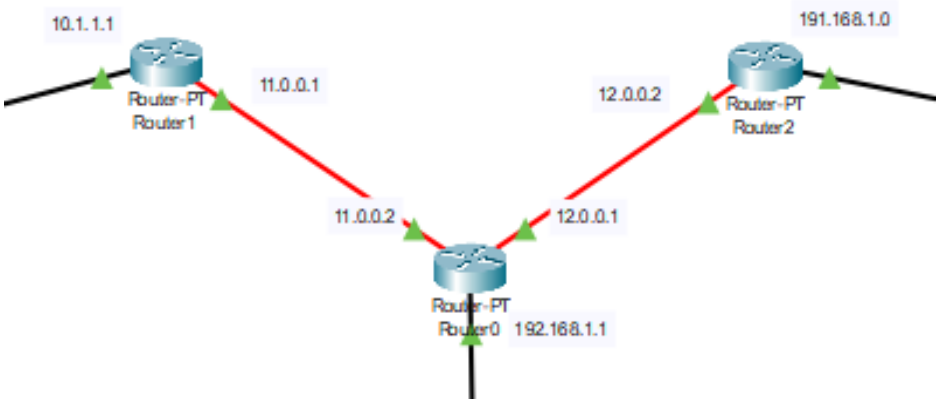

Figure 9: Router Connection via Fiber: Logical View

Services Installed:

We have installed the basic services that are required by the network. These include Email service, FTP service, ICMP service etc. We have configured these services to work in the whole network and between all buildings. We have seen that using Fiber connection, we can connect these buildings internally as shown in figure above and install the services that we want to use. The snapshots of different services working in the network are listed below:

Email Service:

Email service is configured to send email from one end device to another end device using Email server with DNS configuration for server email.com.

Email Send from Faizan to Haider:

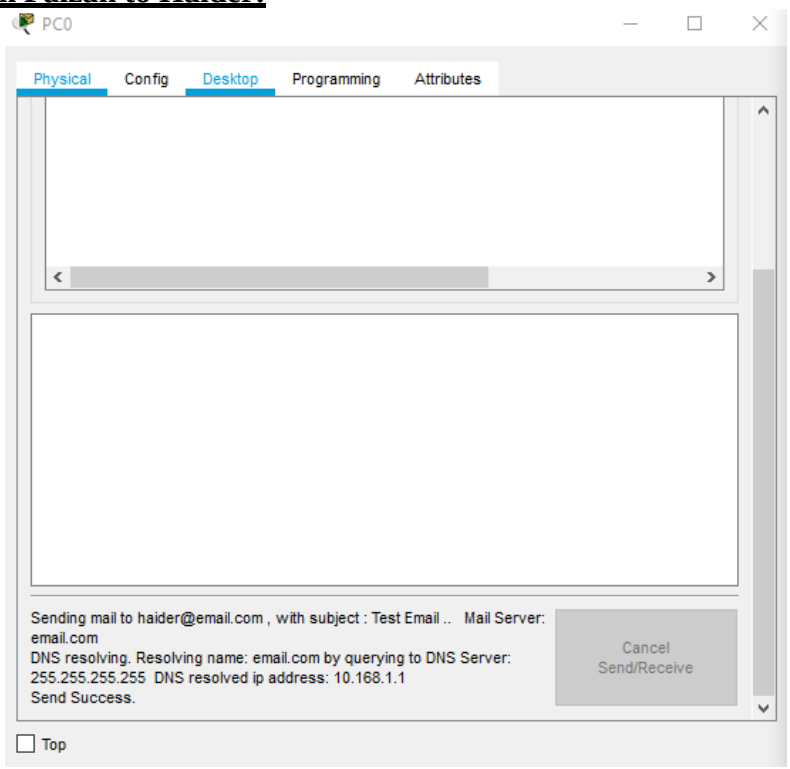

Figure 10: Email Sent Success

Email Receive by Haider from Faizan:

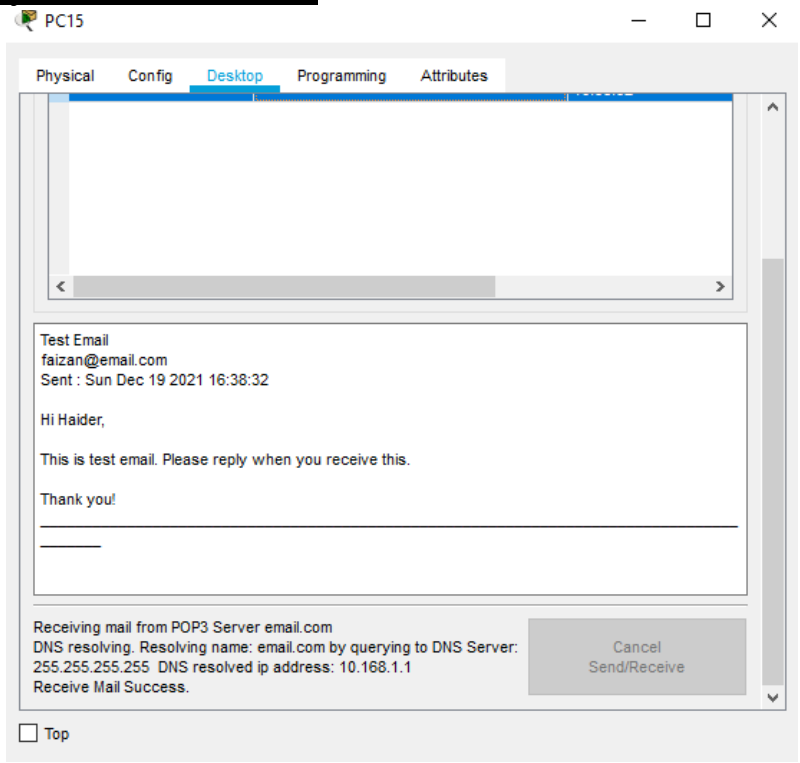

Figure 10: Email Receive Success

FTP Service:

The storage server is utilized to use the FTP Services between hosts of all buildings. We have configured the FTP server in Administration Building to perform file management and store them on server so that each host from any building can access these files by login into the FTP server.

PC – B accessing FTP Server in Programming Building: *Put File Action*

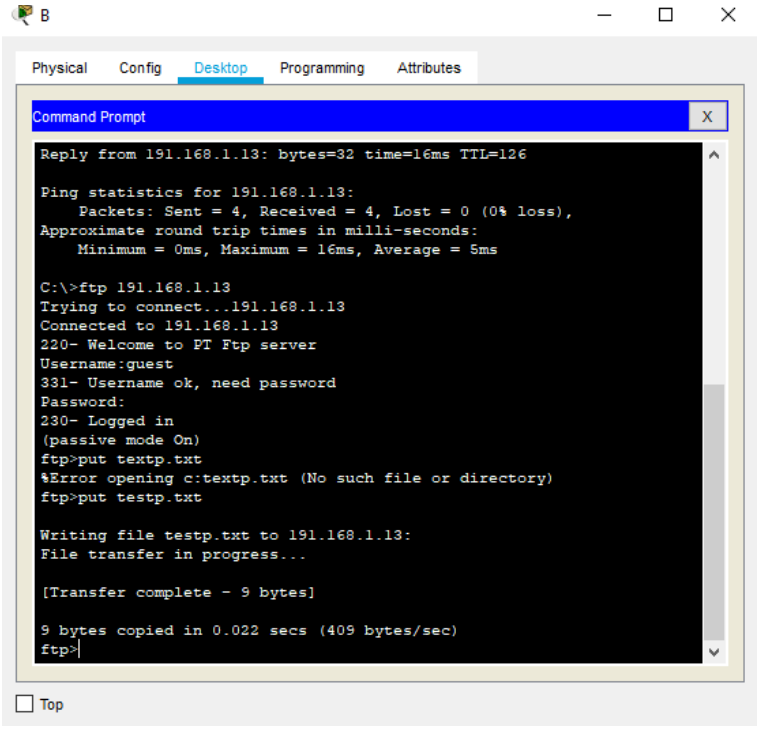

Figure 11: FTP Service – Put File Action

PC – A accessing FTP Server in Administration Building: *Get File Action*

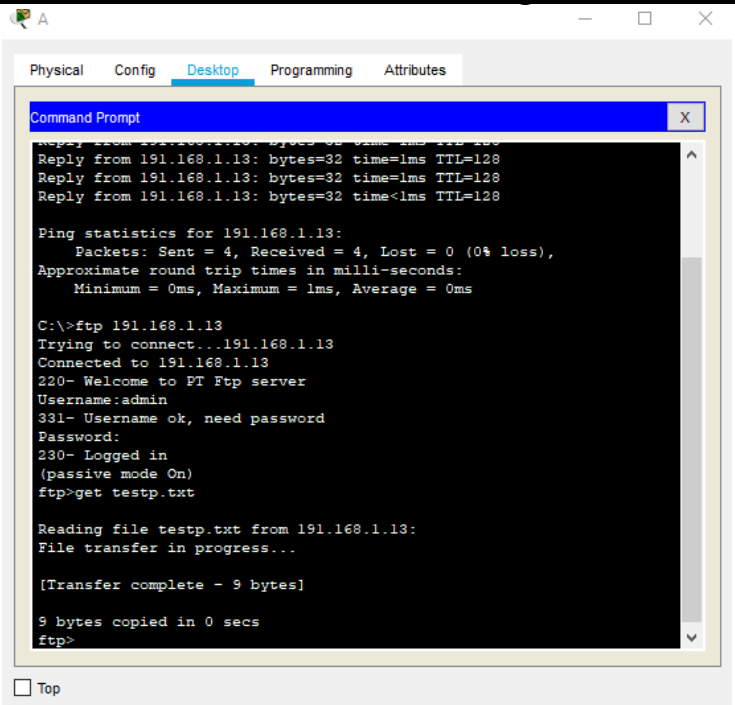

Figure 12: FTP Service – Get File Action

ICMP Service

Internet Control Message Protocol (ICMP) is a network level protocol. ICMP messages communicate information about network connectivity. It gives information of connection issues back to the source of the packet. It sends control messages such as destination network successful, unreachable, source route failed, and source quench. We have used this service and checked it between different buildings. It works perfectly in the network as shown in the *figure 13* below:

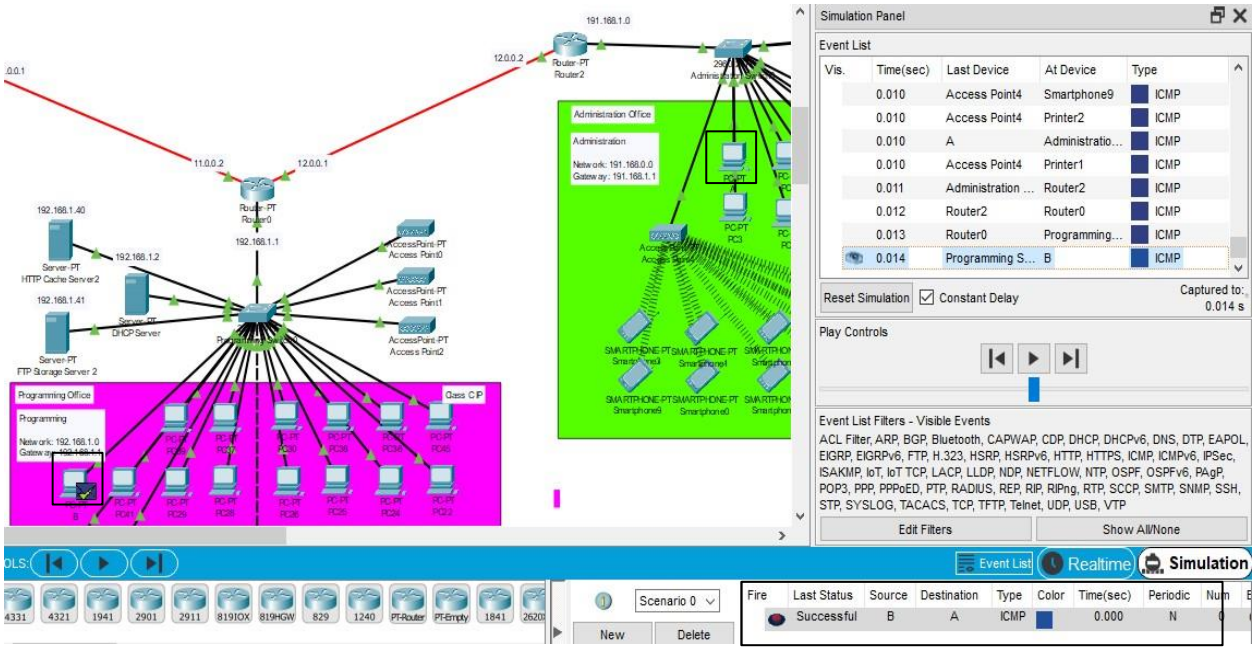

Figure 13: ICMP Service between Source B - Programming Building and Destination A - Administration Building

We have checked Email, FTP and ICMP Services between all buildings and these are working fine. We have successfully installed all services in the network for our use.

Routing Table

Here are the snapshots of the routing table for the routers we have used in our network.

Corporate Building Router

Routing Table for Corporate Building Router

Type	Network	Port	Next Hop IP	Metric
C	10.0.0.0/8	FastEthernet0/0	---	0/0
C	11.0.0.0/8	GigabitEthernet4/0	---	0/0
S	12.0.0.0/8	---	11.0.0.2	1/0
S	191.168.0.0/16	---	11.0.0.2	1/0
S	192.168.1.0/24	---	11.0.0.2	1/0

Figure 14: Corporate Building Routing Table

Administration Building Router

Routing Table for Administration Building Router

Type	Network	Port	Next Hop IP	Metric
S	10.0.0.0/8	---	12.0.0.1	1/0
S	11.0.0.0/8	---	12.0.0.1	1/0
C	12.0.0.0/8	GigabitEthernet4/0	---	0/0
C	191.168.0.0/16	FastEthernet0/0	---	0/0
S	192.168.1.0/24	---	12.0.0.1	1/0

Figure 15: Administration Building Routing Table

Programming Building Router

Routing Table for Programming Building Router

Type	Network	Port	Next Hop IP	Metric
S	10.0.0.0/8	---	11.0.0.1	1/0
C	11.0.0.0/8	GigabitEthernet4/0	---	0/0
C	12.0.0.0/8	GigabitEthernet5/0	---	0/0
S	191.168.0.0/16	---	12.0.0.2	1/0
C	192.168.1.0/24	FastEthernet0/0	---	0/0

Figure 16: Programming Building Routing Table

MAC/Forwarding Table

Here are the snapshots of the MAC table for the Switches we have used in our network.

Corporate Building Switch

MAC Table for Corporate Switch0

VLAN	Mac Address	Port
1	0040.0B27.3945	FastEthernet0/10
1	0060.47A4.0ACA	FastEthernet0/10
1	00D0.BC7E.C3AB	FastEthernet0/10
1	00E0.8F87.07C5	FastEthernet0/10
1	00E0.F7CE.AAE5	FastEthernet0/10
1	00E0.F95D.A04D	FastEthernet0/10

Figure 17: Corporate Building MAC Table

Administration Building Switch

MAC Table for Administration Switch0

VLAN	Mac Address	Port
1	0030.F2B7.7CB9	FastEthernet0/12
1	0040.0B20.E765	FastEthernet0/4
1	0060.2FEE.8E2C	FastEthernet0/12
1	0060.3EB6.A946	FastEthernet0/12
1	0090.2163.34D1	FastEthernet0/12
1	0090.2173.021A	FastEthernet0/12

Figure 18: Administration Building MAC Table

Programming Building Switch

MAC Table for Programming Switch0

VLAN	Mac Address	Port
1	0001.C901.8C78	FastEthernet0/1
1	0050.0FE9.1C0F	FastEthernet0/17
1	00E0.F759.7091	FastEthernet0/24

MAC Table for Programming Switch1

VLAN	Mac Address	Port
1	0001.C901.8C78	FastEthernet0/15
1	0004.9A6A.B611	FastEthernet0/15

Figure 19: Programming Building MAC Table

Description: We have attached routing tables for the routers we have used in our network. A routing table contains the necessary packet information to forward with the best path to its destination. Each packet contains information about its origin and destination. It also provides the instructions to device for sending the packet to the next hop on its route across the network.

Description: We have also attached the forwarding table or MAC table for all switches used in our network. A forwarding table or MAC table, is most commonly used in network routing or bridging to find the best output interface for packet forwarding. It contains MAC addresses of the device while router contains IP information.

Ping Operation

We will now use the Ping operation between different end devices in different buildings. The snapshots of the ping operation are given below:

Ping between Corporate Building and Administration Building

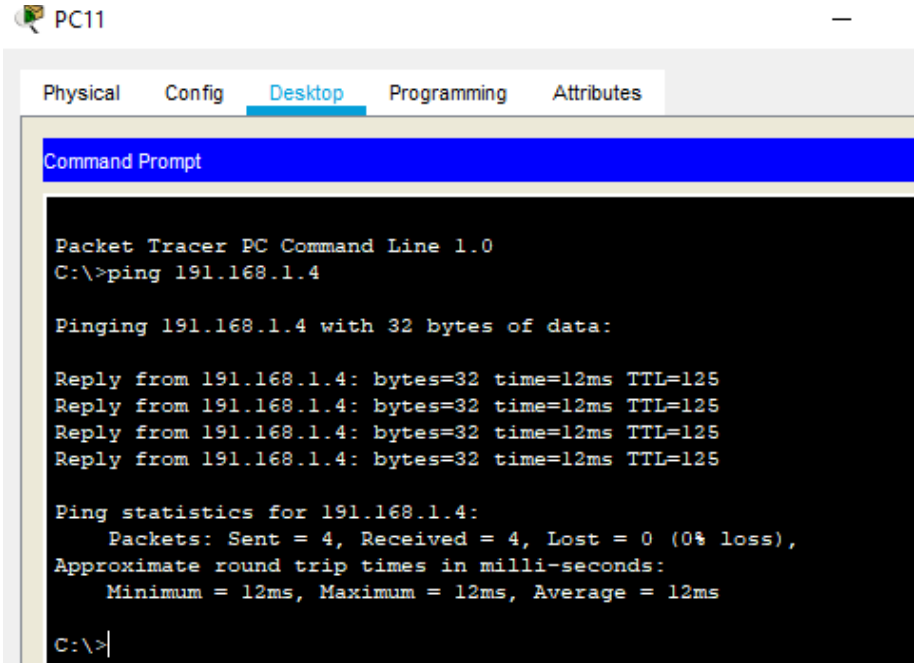

Figure 20: Ping Operation between end devices

Ping between Administration Building and Programming Building

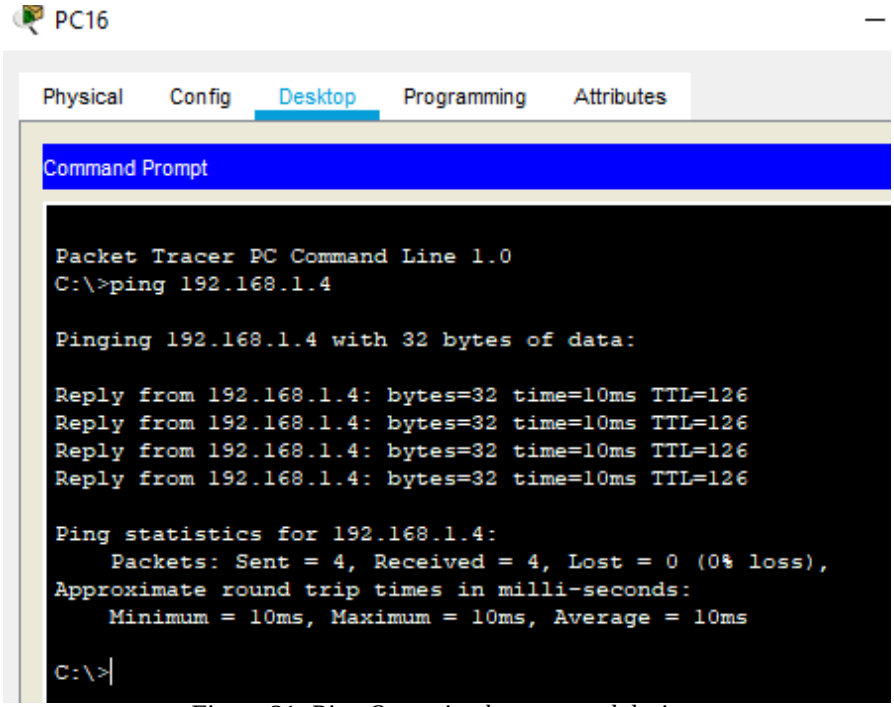

Figure 21: Ping Operation between end devices

Ping between Programming Building and Corporate Building

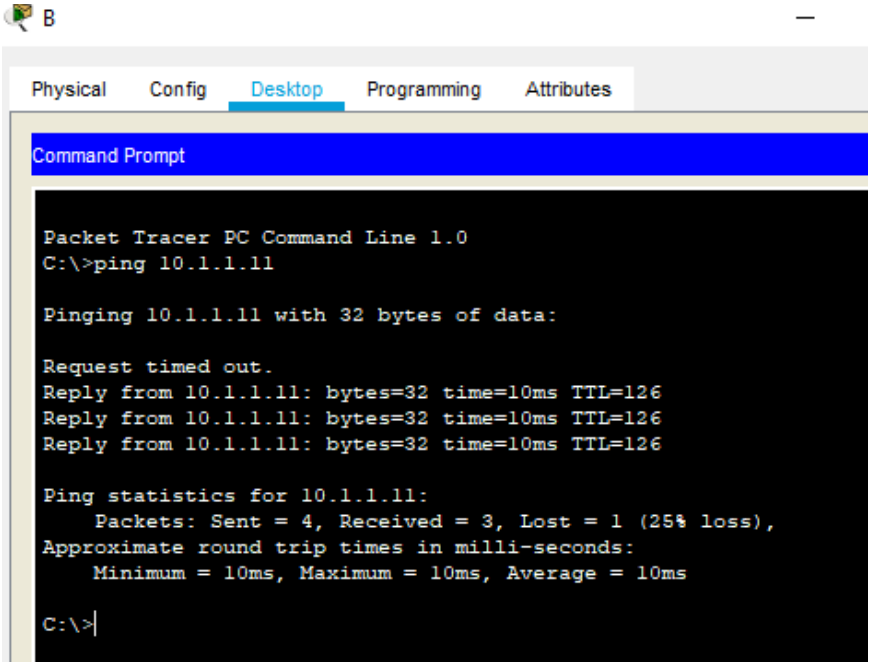

Figure 22: Ping Operation between end devices

Network Devices Information:

We are using Cisco Internetwork Operating System and IOS Software and have used following Network devices (Routers/Switches) in our network.

PT Router **(Same in all three buildings)**	**Name:** Cisco Internetwork Operating System Software **Modal:** PTSC2005 processor (revision 0x200) **Memory:** 60416K/5120K bytes. **Price:** Rs. 6899/- Reference Link
Switch **(Same in all three buildings)**	**Name:** Cisco WS-C2960-24TT **Modal:** RC32300 processor (revision C0) **Memory:** 21039K bytes. **Price:** Rs. 12,000/- Reference Link

Potential point of weakness in the network:

We have installed basic services in our network and they are working perfectly. However, there is always space of improvement in any network that is configured. We have highlighted some potential points of weakness in our network as:

- Client-Server networks are highly vulnerable to link failures and when client or end device want to communicate with server they are unable to connect and services are denied. We have experienced this issue in our network as well.
- We have observed that when we send a packet first time, the packet is broadcasted to all end devices and often it is failed to reach destination. This is because the router IP and switch MAC addresses are not known in first time. But the packet is successfully delivered after that as now all the addresses are

known and packet is delivered to exact destination. But first time connection is often failed which is a serious networking issue.

- Wireless networks are subject to many serious attacks including DOS, spoofing attacks, and physical tampering that can affect the network badly [1, 2]. This is also a weakness in our network as we have used wireless devices and access points in buildings.
- In our network, we have also used fiber optic cables and wired networking. In wired networks, fiber optic cables and other media are clearly subjected to the intentional or unintentional destruction [3] which is also a weak point in the network.

An Estimated Cost for the Network Devices

We have used the Switches, Routers and Access Points in our Network. The estimated cost for these devices is calculated below:

Device Name	Quantity	Cost
Router (PTSC2005)	3	6899*3 = Rs. 20,697/-
Switch (RC32300)	4	12,000*4 = Rs. 48,000/-
	Total Cost	**Rs. 68, 697/-**

Suggestion for Improvement

Although we have used best practices while implementing the network and deployment different services in the whole network of three buildings, but still there might be some suggestion that will help in reducing cost and improved efficiency and performance.

- We have used Fiber Optic cables to connect three buildings. Although, fiber is best cable for large distance and enterprise installations but it is also very expensive. So best option can be a Microwave Fixed Wireless if this is available in the area where network is deployed. Microwave fixed wireless can easily achieve these speeds with higher reliability than fiber optic networks. These are almost 50% more faster than fiber and will be a best option.
- If this brings costs over budget, a good second choice is Category 5 cable with a Category 5 protector at each end.
- We haven't used any protection scheme for the network. So installing a Firewall can help save and protect the end devices and data by managing network traffic. It will block unsolicited and unwanted incoming network traffic and also validate access by malware or hacker.
- VLANs can also help in improving performance and security of the network.
- We have used protected access points. So providing a different network for Guest user can help manage traffic and improve performance.
- Along with this, proper monitoring and updates can help network work for long time effectively.

Conclusion:

At the end of this project, we conclude that using Packet Tracer, we can build small to medium level Logical Topology of any network with essential services available in Packet Tracer. We have seen that Packet Tracer simulator also offers Physical view of the network which makes it easy to analyze and troubleshoot while connecting nodes and physical layout of the network. We can configure different services between two or more networks and calculate the cost, design architecture and analyze potential points of failure in these large distanced networks. In this lab project, we used ICMP, HTTP, FTP, DHCP and Email services to design and configure Software House Network which was situated in three different buildings each in different city. We used these services and configured them for all end devices. We have also practiced troubleshooting and configuration of the network to check the proper working of end devices in whole Software House Network.

References

[1] Y. W. Law, L. van Hoesel, J. Doumen, P. Hartel, and P. Havinga. Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols. In SASN, Nov 2005.

[2] A. Perrig, J. Stankovic, and D. Wagner. Security in wireless sensor networks. Wireless sensor networks, 2004.

[3] S. Aref and B. Miller. Damage information and reporting tool. Technical report, Common Ground Alliance, 2005.

Lab Evaluation Rubrics								
Domain	**CLOs**	**Assessment Type**	**Excellent 10**	**Good 9-7**	**Satisfactory 6-4**	**Unsatisfactory 3-1**	**Poor 0**	**Marks Obtained**
Cognitive (100% of lab marks)	CLO1	Report	Report submitted with proper content, grammar, punctuation, and good formatting	Report submitted with proper content with good formatting but some grammatical mistakes or proper grammar but not with very good formatting	Some correct/ meaningful content. Some parts of the document not properly formatted or some grammatical mistakes	Content not based on observation/ exploration. Bad formatting with no proper grammar/punctuation	Report not submitted	
Total								