

INDEX

1. Project title
2. Abstract
3. Introduction
4. The objective of the project
5. Network requirements
 - 5.1 Network requirement analysis
 - 5.2 Hardware and software requirement analysis
 - 5.3 Additional requirements
6. Implementation- Cisco packet tracer
 - 6.1 IP address design
7. Features and services
 - 7.1 Vlan
 - 7.2 Access control list
 - 7.3 Rip
8. network topology diagram
 - 8.1 Access layer
 - 8.2 Distribution layer
 - 8.3 Core layer
 - 8.4 All topologies diagram
9. Table of address
10. Pining
11. Website
12. Conclusion
13. References

Project Title: Pre-sales proposal for network setup in a university

Abstract:

In this project, we will primarily focus on the design and implementation of network setup in a university using Cisco Packet Tracer (CPT). This job with respect to the College's Networking Scenario is to provide systematic, secure, valid, and dependable communication among different departments. This network will provide access to the Internet or LAN to users located in two or more buildings or in the campus. This network can be used for an office, labs, and also in libraries.

The purpose of this project is to design a suitable network system for universities in developing countries. The aim was to design a network with high-quality security and low cost, in such a way that network devices of universities in developing countries, will meet standards associated with the universities in developed countries. This project will help to enhance education in developing countries. There are many devices that were used in designing the network, such as routers, switches, backup, firewall, and servers. All devices were connected to each other to make integration network system and configured by putting IP addresses to all devices. Although the budget for this design network was low, it needed to have a high level of security. Accordingly, it incorporated several mechanisms including a firewall device that prevents any unfavorable data from entering into the network. Additionally, all devices in the network were secured by passwords, and these passwords were encrypted to be more secure. Moreover, each computer in the network was secured by antivirus programs and a backup system. This research discussed in details the budget challenges that the network faced in developing countries. Developing countries have a limited budget that affects choosing devices in the network such as servers. The servers used for this network design are DHCP server and DNS servers. This presentation and design included additional components such as a web server, mail server, etc.

Introduction:

Technology has reached its highest peak of development, especially in making life easier for people. Well implemented technology is faster than human in processing calculation and is more accurate. Technology has become an important concept in our life. It assists in connecting communities together. Obviously, people have started to use technology in every field of life including education, health, the military, etc. The computer network represents a component, especially on how it enhances the functional performance in different fields and organizations, such as companies and schools. A school's computer network performs so many functions, such as connecting students with the university, faculty, and the library. Most universities today use the network to provide online education by connecting widely dispersed students with their professors directly. For this reason, computer networks play a vital role in the education area by providing efficient communications for the university environment. However, the design of computer networks differs from one university to another. This is as a result of many factors which determine the differences. Such factors include; adaptability, integration, resilience, security, and cost. Installing networks in a university relies on the university's budget, which differs by institution and from country to country. For instance, there are many countries whose universities do not have the financial capability for designing the 'perfect' or ideal network. Yet these universities from these third world countries still need to have good quality and more secure network equipment with less

cost. This is because these schools aspire to deliver capability in line with the leading prestigious universities despite low budgets. Therefore, this design will be focusing on factors that will enhance computer network for universities in developing countries to be able to compete favorably with another computer network in modern country universities.

Objectives:

The main objective of this project is to design a network for a university with the given constraints. In this, we have 1 main branch and 5 sub-branches for each department.

The university has the following 7 departments.

1. IT
2. Finance
3. HR
4. Management
5. Faculty
6. Students
7. R&D

The university has an ADSL internet connection which would be used by the departments except for the R&D department which should not have access to the same. All the departments should be able to communicate with each other.

Network Requirements:

1. The active network components are required (Routers, Switches).
2. The number of switches, and routers that are required for the design.
3. The IP Design schema for the department.
4. Explanation of the details required to be configured on the Switch and how to create different departments with VLAN.
5. Explanation of how to restrict internet connection for the R&D Department and allow access for the other departments with Access control lists on the Router.
6. Identify the feature on the router which is required for sharing the Internet with the users.
7. Identify the TCP/IP adapter parameters (IP address, Subnet mask, Default Gateway, DNS Server IP address) for the users.
8. Network Design Diagram

Network requirement analysis:

As the locations of the banks are spanned across different geographical locations, a VPN solution is recommended as it would be more economical as compared with a leased line solution. VPN appliances are required for the same. The application server is recommended as Windows 2008 / Windows 2012, with appropriate failover clustering to provide high availability to the application. The application server should be set up on a DMZ, where the only access to https protocol (TCP port 443), should be made available to users accessing from the outside. Antivirus with desktop firewall should be installed on the server, which would provide host level protection. An appliance, which would perform deep packet inspection, should be setup on the network, to filter incoming traffic to the application server. This would scan the traffic for security threats and attacks.

Hardware and software requirement analysis:

1. At the main office, a VPN appliance would be required, which would have integrated firewall and deep packet inspection. The recommended VPN appliance is Sonic wall NSA 220/W, which has the capacity to support site to site VPN tunnels and also has deep packet inspection and firewall capabilities.
2. There are 200 users in the main office. A total of 5 no of 48 port switches are recommended considering ports for servers, VPN appliance and expansion plan. The Cisco Catalyst 2960S- 48FPD-L is recommended for the same.
3. At the branch offices, the Sonicwall TZ105 series is recommended to establish site to site VPN connectivity with the main office.
4. There are a total of 100 users each at the branch office. A total of 3 nos of 48 port switches is recommended, which are Cisco Catalyst 2960S-48FPD-L, considering future expansion plans.
5. Windows 2008/2012 is recommended for the application server with server hardware.

Additional requirements:

1. All the locations have high speed internet connection. At the main office, an additional public IP address would be required to host the application server. The IP address would be registered with a domain name, which would enable users on the outside world (internet), to access the application.

Implementation – Cisco Packet Tracer:

For implementing this bank prototype we have used Router-PT which have serial ports, So that it will be easy for us to connect to 6 branches and we have also used 2960-24TT switches

all over the network to connect to various campuses among the cities which are then interconnected to the servers and users. All the serial ports are assigned with IP addresses so they can be recognized between the cities without confusion.

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 and every router and network with the IP address and tested whether the data transfer is successful or not.

IP Address Design:

TABLE 1: IP Address Design:

Branch	IP Address	Subnet Mask
IT	Switch-1.0.0.0	255.0.0.0
Finance	Switch-192.168.1.0	255.255.255.0
HR	Switch-192.168.2.0	255.255.255.0
Management	Switch-192.168.4.0	255.255.255.0
Faculty and Students	Switch-192.168.3.0	255.255.255.0
R&D	Switch-128.168.0.0	255.255.0.0

Feature and Services:

1. VLAN

Two networks are required at the main office. One network would be for the LAN, where the office users would be connected. The second network would be the DMZ network, where the application server is hosted. This is required since the application server would require access from outside. Two VLANs would be created which would be mapped with the LAN and DMZ network. VLANs would be configured on the switches.

VLAN is a custom network which is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN. The full form of VLAN is defined as Virtual Local Area Network.

Without VLANs, a broadcast sent from a host can easily reach all network devices. Each and every device will process broadcast received frames. It can increase the CPU overhead on each device and reduce the overall network security.

In case if you place interfaces on both switches into separate VLAN, a broadcast from host A can reach only devices available inside the same VLAN. Hosts of VLANs will not even be aware that the communication took place.

2. Access control lists

Access control lists are configured on the VPN appliance at the main office. The ACLs are used to restrict communication from the internet to only the allowed port, which is TCP port 443 on the application server in the DMZ. ACL is also configured to allow all traffic from the branch office networks to the DMZ and LAN network in the main office.

Access control lists can be approached in relation to two main categories:

Standard ACL

An access-list that is developed solely using the source IP address. These access control lists allow or block the entire protocol suite. They don't differentiate between IP traffic such as UDP, TCP, and HTTPS. They use numbers 1-99 or 1300-1999 so the router can recognize the address as the source IP address.

Extended ACL

An access-list that is widely used as it can differentiate IP traffic. It uses both source and destination IP addresses and port numbers to make sense of IP traffic. You can also specify which IP traffic should be allowed or denied. They use the numbers 100-199 and 2000-2699.

3. RIP (Routing Information Protocol)

This protocol are the intradomain (interior) routing protocol which is based on distance vector routing and it is used inside an autonomous system. Routers and network links are called nodes. The first column of routing table is destination address. The cost of metric in this protocol is hop count which is number of networks which need to be passed to reach destination. Here infinity is defined by a fixed number which is 16 it means that using a Rip, network cannot have more than 15 hops.

The Routing Information Protocol (RIP) is one of a family of IP Routing protocols, and is an Interior Gateway Protocol (IGP) designed to distribute routing information within an Autonomous System (AS).

RIP is a simple vector routing protocol with many existing implementations in the field. In a vector routing protocol, the routers exchange network reachability information with their nearest neighbors. In other words, the routers communicate to each other the sets of destinations ("address prefixes") that they can reach, and the next hop address to which data should be sent in order to reach those destinations. This contrasts with link-state IGPs; vectoring protocols exchange routes with one another, whereas link state routers exchange topology information, and calculate their own routes locally.

A vector routing protocol floods reachability information throughout all routers participating in the protocol, so that every router has a routing table containing the complete set of destinations known to the participating routers.

In brief the RIP protocol works as follows.

- Each router initializes its routing table with a list of locally connected networks.
- Periodically, each router advertises the entire contents of its routing table over all of its RIP-enabled interfaces.
- Whenever a RIP router receives such an advertisement, it puts all of the appropriate routes into its routing table and begins using it to forward packets. This process ensures that every network connected to every router eventually becomes known to all routers.
- If a router does not continue to receive advertisements for a remote route, it eventually times out that route and stops forwarding packets over it. In other words, RIP is a "soft state" protocol.
- Every route has a property called a metric, which indicates the "distance" to the route's destination.
- Every time a router receives a route advertisement, it increments the metric.
- Routers prefer shorter routes to longer routes when deciding which of two versions of a route to program in the routing table.
- The maximum metric permitted by RIP is 16, which means that a route is unreachable. This means that the protocol cannot scale to networks where there may be more than 15 hops to a given destination.

RIP also includes some optimizations of this basic algorithm to improve stabilization of the routing database and to eliminate routing loops.

- When a router detects a change to its routing table, it sends an immediate "triggered" update. This speeds up stabilization of the routing table and elimination of routing loops.

- When a route is determined to be unreachable, RIP routers do not delete it straightaway. Instead they continue to advertise the route with a metric of 16 (unreachable). This ensures that neighbors are rapidly notified of unreachable routes, rather than having to wait for a soft state timeout.
- When router A has learnt a route from router B, it advertises the route back to B with a metric of 16 (unreachable). This ensures that B is never under the impression that A has a different way of getting to the same destination. This technique is known as "split horizon with poison reverse."
- A "Request" message allows a newly-started router to rapidly query all of its neighbors' routing tables.

RIPv1:

RIPv1 uses classful routing. The periodic routing updates do not carry subnet information, lacking support for variable length subnet masks (VLSM). This limitation makes it impossible to have different-sized subnets inside of the same network class. In other words, all subnets in a network class must have the same size. There is also no support for router authentication, making RIP vulnerable to various attacks.

RIP Version-2:

Due to some deficiencies in the original RIP specification, RIP version 2 was developed in 1993. It supports classless Inter-Domain Routing (CIDR) and has the ability to carry subnet information, its metric is also hop count, and max hop count 15 is same as rip version 1. It supports authentication and does subnetting and multicasting. Auto summary can be done on every router. In RIPv2 Subnet masks are included in the routing update. RIPv2 multicasts the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast (255.255.255.255).

RIPv2 :

RIPv2 is a classless, distance vector routing protocol as defined in RFC 1723. Being a classless routing protocol, means, it includes the subnet mask with the network addresses in its routing updates.

Due to the deficiencies of RIPv1, RIP version 2 (RIPv2) was developed in 1993 and was equipped with the ability to support subnet information and supports Classless Inter-Domain Routing (CIDR).

Advantages of RIP version-2

1. It's a standardized protocol.
2. It's VLSM compliant.
3. Provides fast convergence.
4. It sends triggered updates when the network changes.
5. Works with snapshot routing – making it ideal for dial networks.

Differences between RIPv1 and RIPv2 :

SR.NO	RIPv1	RIPv2
1.	RIPv1 is a Distance-Vector Routing protocol.	RIPv2 is also Distance-Vector Routing Protocol.
2.	It can supports class full network only.	It can support class full and classless networks.
3.	It does not support for authentications.	It support for authentications.
4.	It hop count limit is 15.	It hop count limit is 15.
5.	It does not support for VLSM and discontinuous networks.	It supports for VLSM and discontinuous networks.
6.	It is less secure.	It is more secure.
7.	RIPv1 use Broadcast traffic for updates.	RIPv2 use Multicast traffic for updates.
8.	RIPV1 does not provide trigger updates.	RIPv2 provides trigger updates.
9.	RIPV1 not send subnet mask to routing table.	RIPv2 send subnet mask to routing table.
10.	RIPv1 don't support manual route summarization.	RIPv2 support manual route summarization.

Network Topology:

A network topology defines how hosts are connected to a computer network. It characterizes how the PCs and other hosts are organized, and linked to each other. There are many types of network topology such as Point-to-Point, Bus, Star, Ring, and Mesh topology. Each type has a different set of advantages and disadvantages.

Point to Point Topology Point to Point topologies connect two computers together with a single line connection. The advantage of Point to Point Topology is that it gives a faster connection, and it is also less expensive than other topologies. The strength of this topology is more than other kinds of connection. However, Point-to-Point topology is mainly used for small networks, and the computers must be near to each other for a better connection. However, this topology will not be useful for big networks because it does not scale effectively. Big, in this case, includes a network of hosts such as that needed to serve a reasonable-sized college or university.

Security:

Due to the constant development of software programs which has led to the increase in the theft and the number of cyber security attacks, security has become important for all hosts on a network. Network security must protect all information and users supplied by a network. Security involves a pro-active prevention process to avert any danger or attack in a network. A computer administrator must be present in order to enforce the security of data access in the network. In terms of securing the network, there are three major aspects to consider. These include Infrastructure, Individual Systems/Components, and Individual Hosts

Infrastructure:

Infrastructure powers all functions on the network. They include all base devices in the network. When all base devices are protected, the network system will be secured. This is because the data passing from the outside of the local network must pass through those devices into the local network. The devices used for infrastructure in this network design are a virtual switch, back-up systems, firewall, and DNS.

Virtual Switch:

A virtual switch or (vSwitch) is a software application that permits correspondence between virtual machines. A virtual switch accomplishes more than simply forward information bundles. It keenly coordinates the correspondence on a network by checking information parcels before moving them to a destination. In this network design, the vSwitch is used between the access point and the personal computers.

DNS:

It is hard for people to remember numbers or the normal form of IP addresses easily. Human readable host name, be that as it may, are much less demanding to utilize, yet require a technique to take steps to the genuine address of the server or remote computer. The Domain Name System (DNS)

Network Topology Diagram:

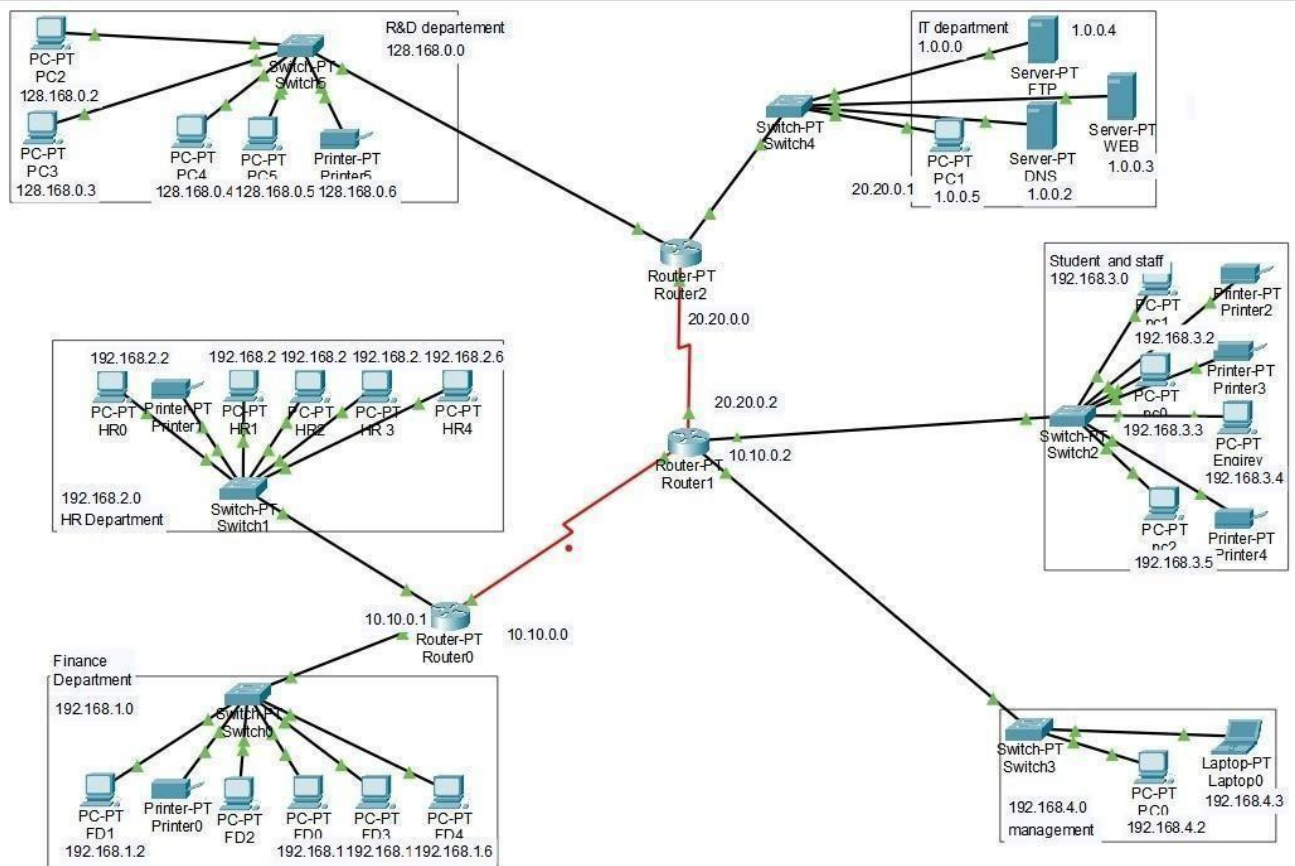


fig 1: Network Topology Diagram

Access Layer

In this layer, all the end devices are connected to each other to the network and we will be having the layer 1 switch for the further connections.

Distribution Layer

Distribution layer, mostly the routers are used to connect the end devices and make the network correspond and this connects to the access and core layers of the network design.

Core Layer

The core layer is the main source of all the layers, where this layer is used to transfer a large amount of traffic very quickly.

There will be 6 sub-branches for this network topology:

1. IT
2. Finance
3. HR
4. Management
5. Faculty and Students
6. R&D

Each branch is explained separately for a better understanding of the network.

IT department – Network Topology:

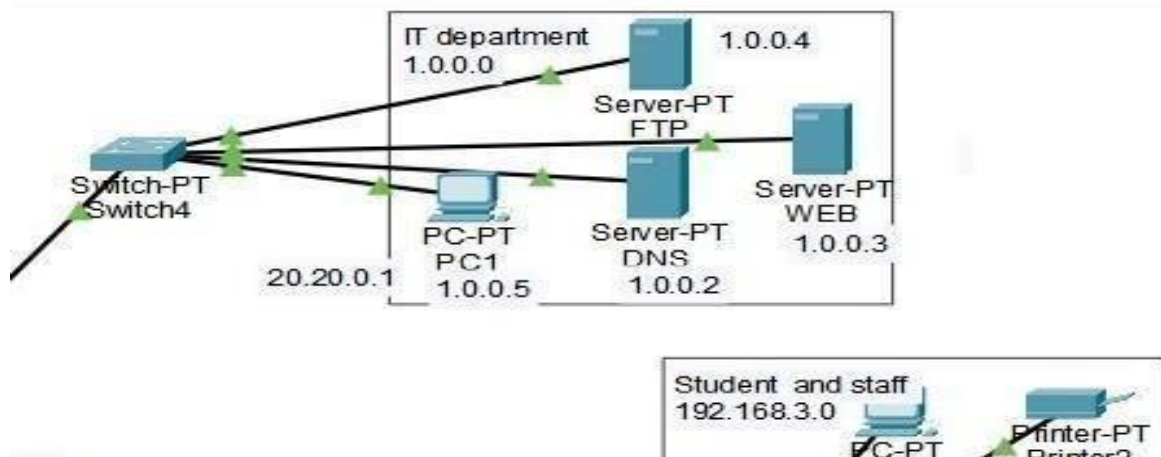


Fig 2 : IT department topology

Finance department – Network Topology:

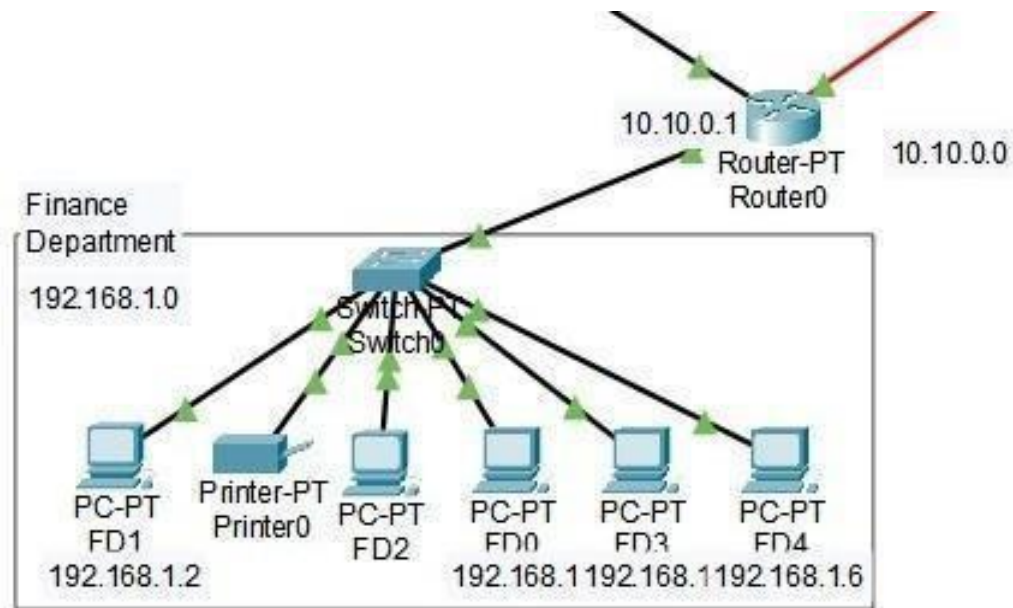


Fig 3 : Finance department topology

HR department – Network Topology:

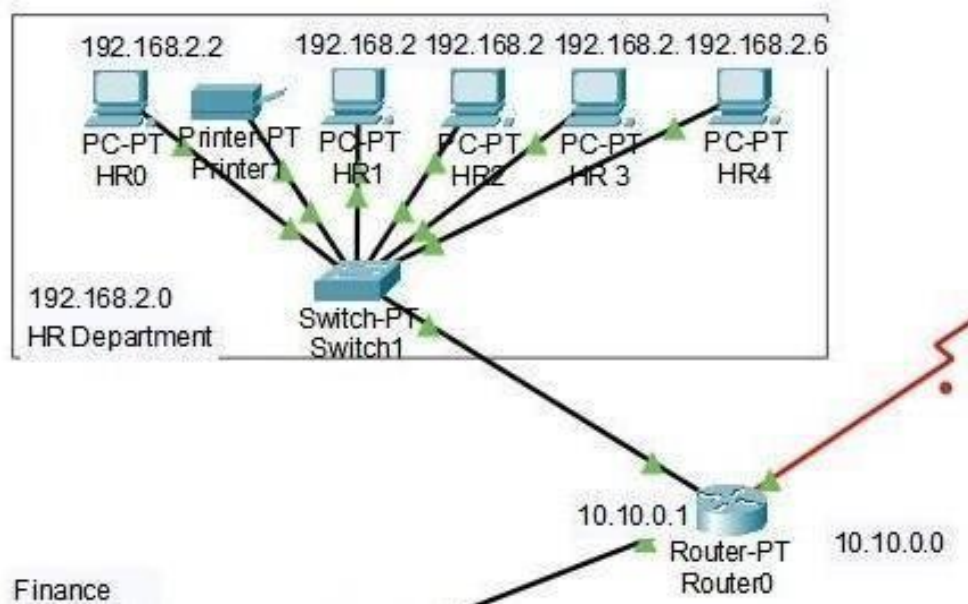


Fig 4 : HR department topology

Managment department – Network Topology:

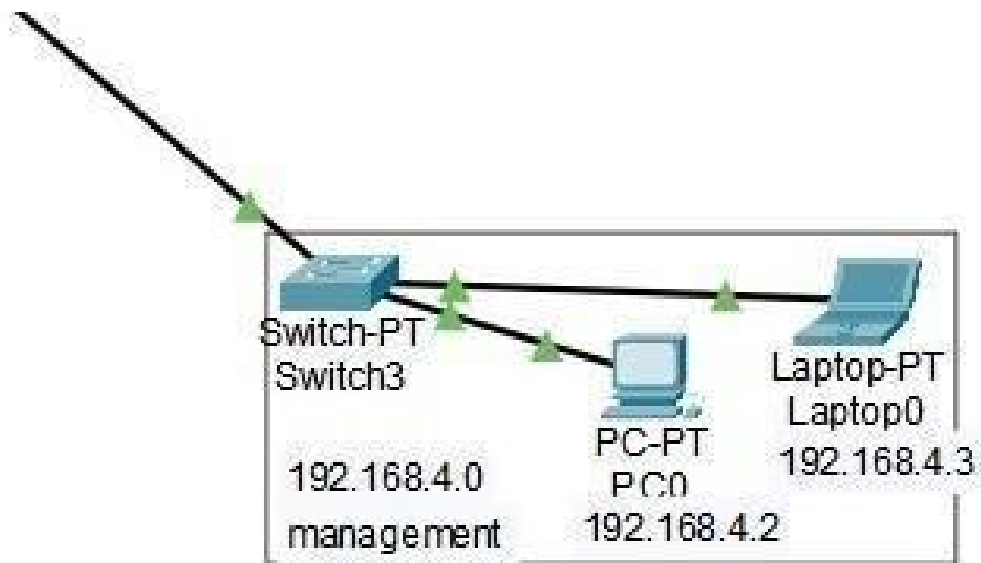


Fig 5 : Management department topology

Faculty and Students – Network Topology:

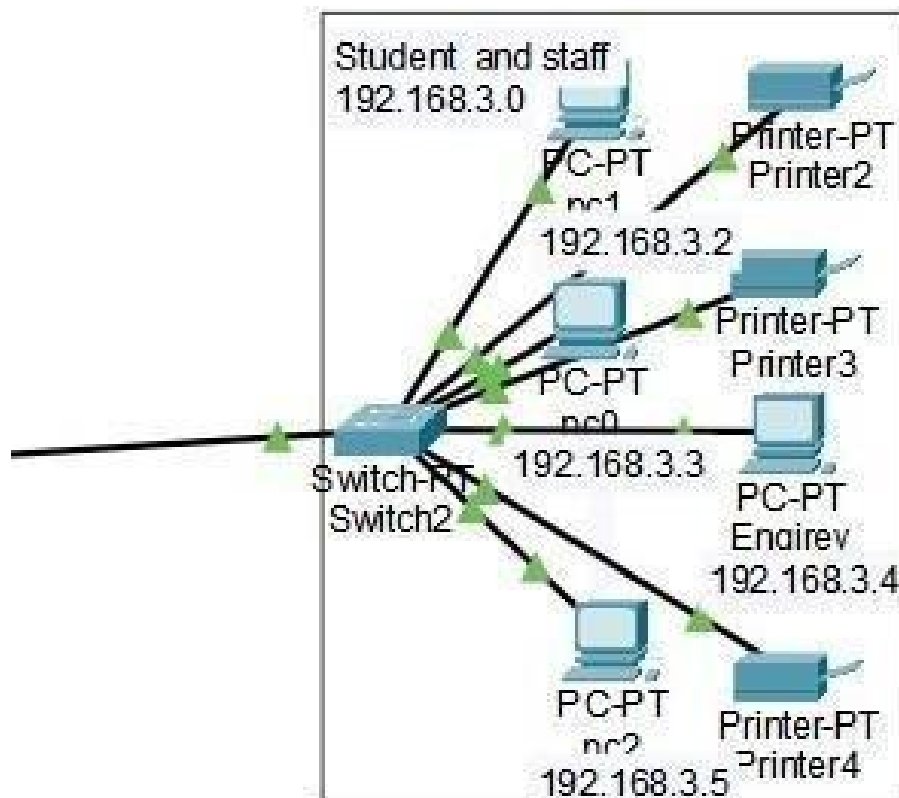


Fig 6 : Faculty and Students topology

R&D department – Network Topology:

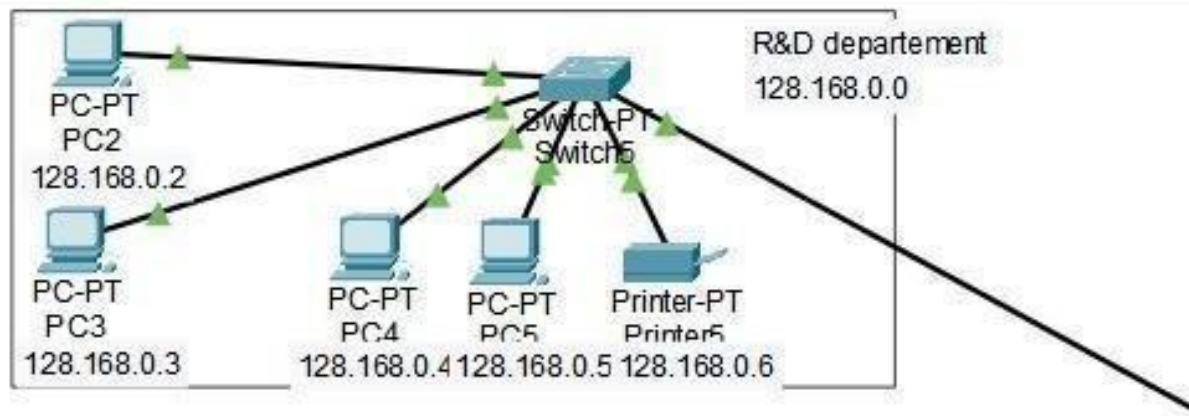


Fig 7 : R&D department topology

Network Design and configuration strategy:

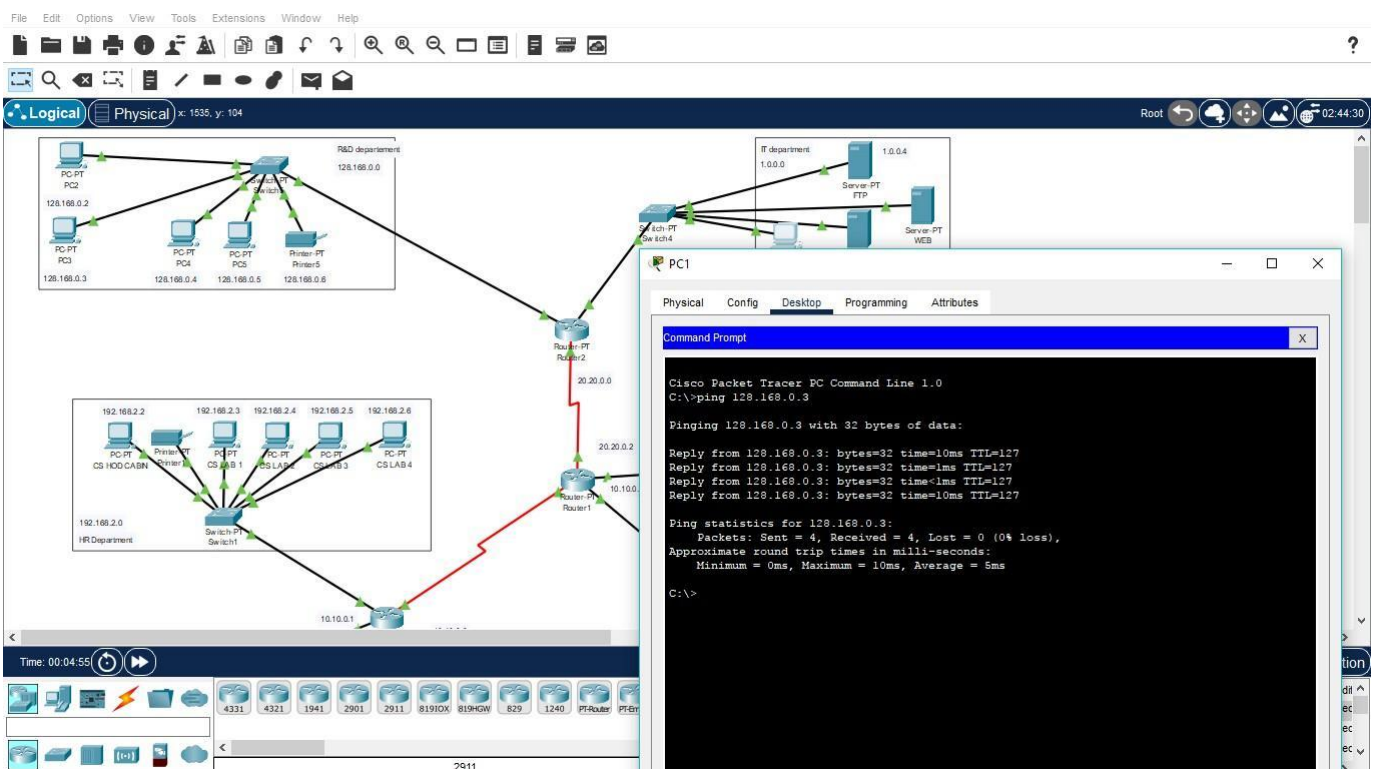
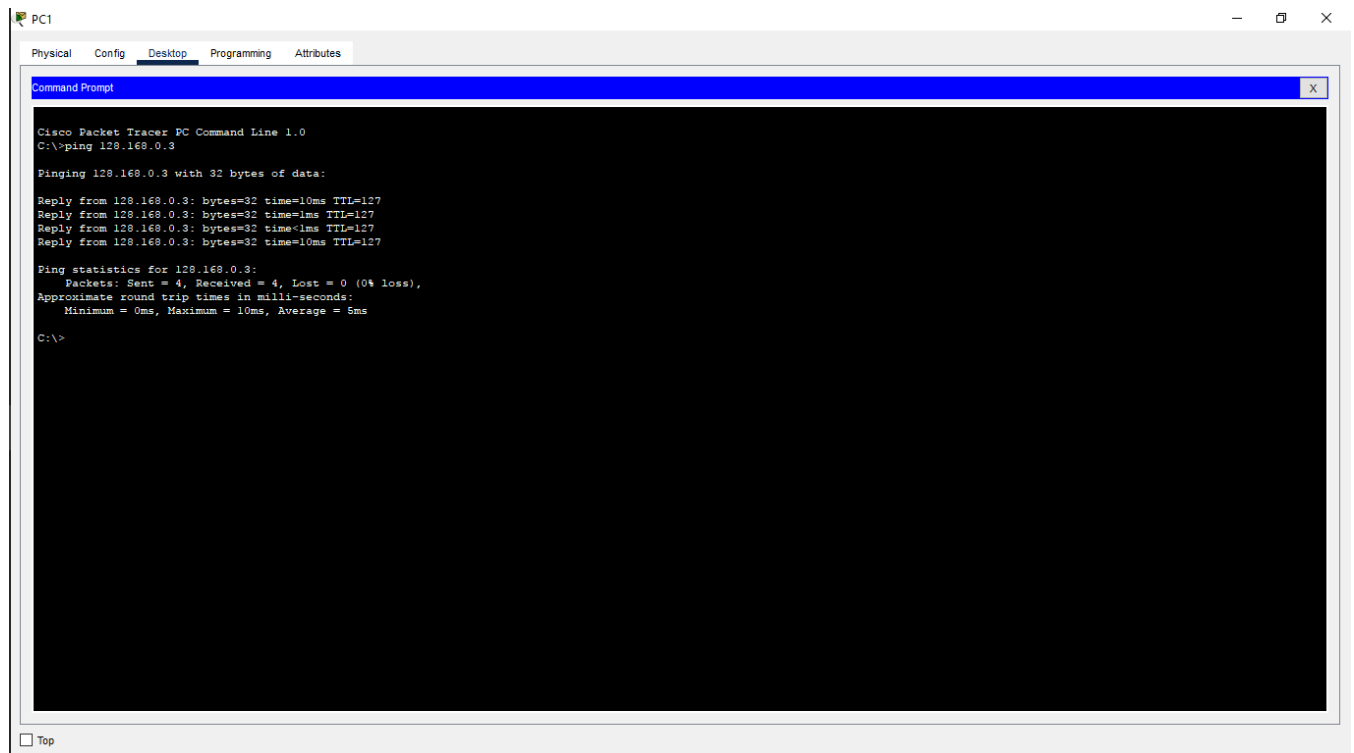


Fig 8 : Network Design

To manually check the connection between pcs we can do this individually with testing from 1 pc from one branch device to other branch devices instead of buffer manager interface.

After testing this manually buffer testing is implemented and checked.

Ping from a PC to Another PC:



Pc1 in IT department is used to ping pc3 in HR department to check logical connection.

We used ping command to check connectivity between the pcs

Click on Pc1-> click on desktop-> go to command prompt->

Type ping command

“ping 128.168.0.3”

Use of ping command:

The ping command is a Command Prompt command used to test the ability of the source computer to reach a specified destination computer. It's a simple way to verify that a computer can communicate with another computer or network device.

The ping command operates by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination computer and waiting for a response. The two major pieces of information that the ping command provides are how many of those responses are returned and how long it takes for them to return.

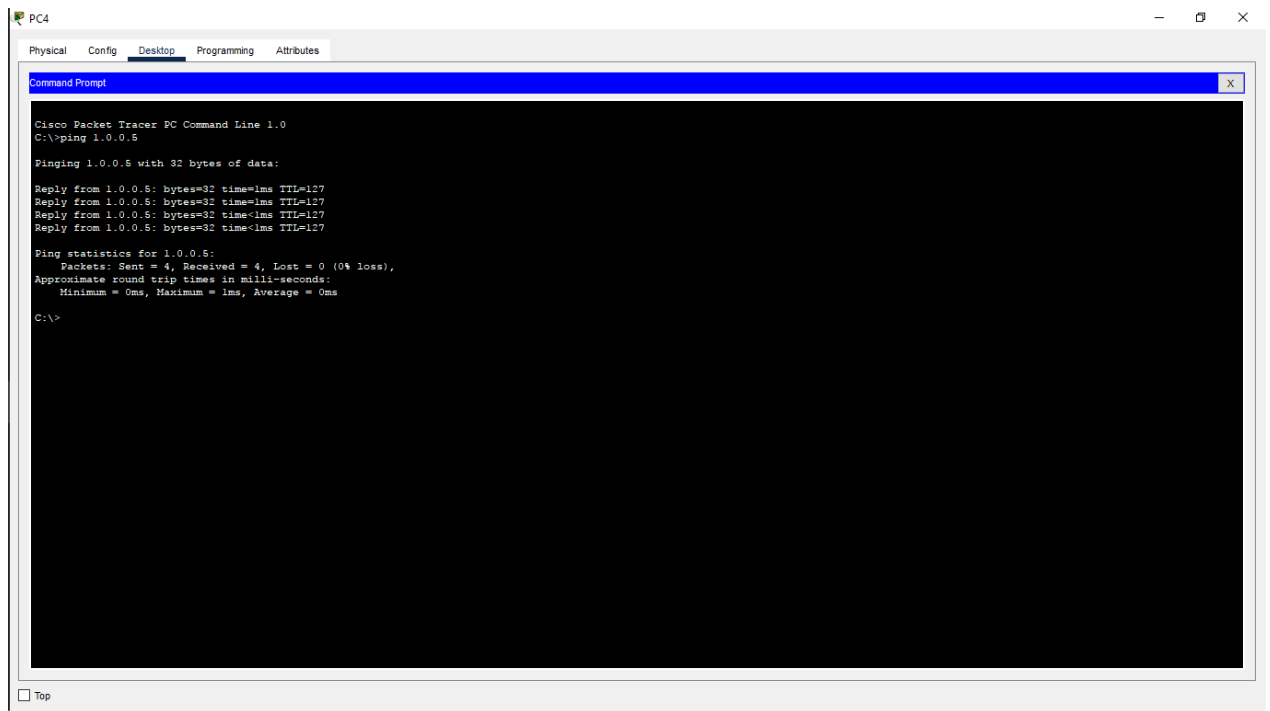


Fig 9 : Ping from a PC to Another PC

Ping command used between pc4 and pc1

Click on pc4 go to desktop click on command

prompt Type ping 1.0.0.5

Which is the ip address of pc1

- The above screenshot shows the successful implementation of the connection across two different systems, where it executes perfectly.
- All the data packets are received without any loss of data.
- Ping is a command-line utility, available on virtually any operating system with network connectivity, that acts as a test to see if a networked device is reachable.
- The ping command sends a request over the network to a specific device. A successful ping results in a response from the computer that was pinged back to the originating computer.
- The Ping utility uses the echo request, and echo reply messages within the Internet Control Message Protocol (ICMP), an integral part of any IP network. When a ping command is issued, an echo request packet is sent to the address specified. When the remote host receives the echo request, it responds with an echo reply packet.
- By default, the ping command sends several echo requests, typically four or five. The result of each echo request is displayed, showing whether the request received a successful response, how many bytes were received in response, the Time to Live (TTL), and how long the response took to receive, along with statistics about packet loss and round trip times.

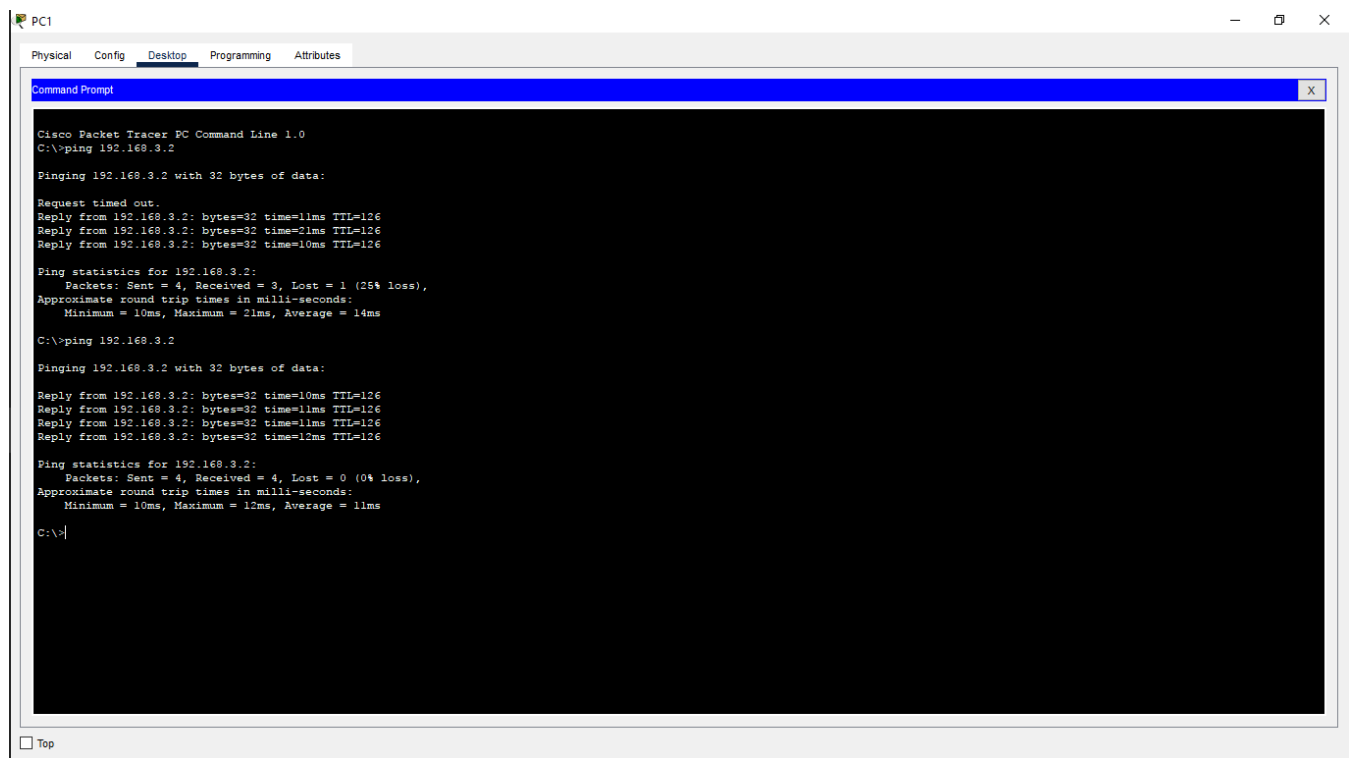
PCs and their ip addresses, subnet mask, and gateway address:

Device	Department	IP address	Subnet mask	Gateway address
Server Pt DNS	IT Department	1.0.0.2	255.0.0.0	1.0.0.1
Sever WEB	IT Department	1.0.0.3	255.0.0.0	1.0.0.1
Sever FTP	IT Department	1.0.0.4	255.0.0.0	1.0.0.1
Pc1	IT Department	1.0.0.4	255.0.0.0	1.0.0.1
Pc2	R&D Department	128.168.0.2	255.255.255.0	128.168.0.1
Pc3	R&D Department	128.168.0.3	255.255.255.0	128.168.0.1
Pc4	R&D Department	128.168.0.4	255.255.255.0	128.168.0.1
Pc5	R&D Department	128.168.0.5	255.255.255.0	128.168.0.1
Printer pt Printer 5	R&D Department	128.168.0.5	255.255.255.0	128.168.0.1
Pc/HR0	HR Department	192.168.2.2	255.255.255.0	192.168.2.1
Pc/HR1	HR Department	192.168.2.3	255.255.255.0	192.168.2.1
Pc/HR2	HR Department	192.168.2.4	255.255.255.0	192.168.2.1
Pc/HR3	HR Department	192.168.2.5	255.255.255.0	192.168.2.1
Pc/HR4	HR Department	192.168.2.6	255.255.255.0	192.168.2.1
Printer pt Printer 1	HR Department	192.168.2.7	255.255.255.0	192.168.2.1
Pc/FD0	Finance Department	192.168.1.2	255.255.255.0	192.168.1.1
Pc/FD1	Finance Department	192.168.1.3	255.255.255.0	192.168.1.1
Pc/FD02	Finance Department	192.168.1.4	255.255.255.0	192.168.1.1
Pc/FD3	Finance Department	192.168.1.5	255.255.255.0	192.168.1.1
Pc/FD4	Finance Department	192.168.1.6	255.255.255.0	192.168.2.1
Printer pt Printer 0	Finance Department	192.168.1.7	255.255.255.0	192.168.2.1
Pc0	Management	192.168.4.2	255.255.255.0	192.168.4.1
Laptop 0	Management	192.168.4.3	255.255.255.0	192.168.4.1
Pc0	Student and staff	192.168.3.2	255.255.255.0	192.168.3.1
Pc1	Student and staff	192.168.3.3	255.255.255.0	192.168.3.1
Pc/enqiry	Student and staff	192.168.3.4	255.255.255.0	192.168.3.1
Pc2	Student and staff	192.168.3.5	255.255.255.0	192.168.3.1
Printer pt Printer2	Student and staff	192.168.3.6	255.255.255.0	192.168.3.1
Printer3	Student and staff	192.168.3.7	255.255.255.0	192.168.3.1
Printer 4	Student and staff	192.168.3.8	255.255.255.0	192.168.3.1

Checking connection between all departments:

IT Department and students & staff:

Click on pc1 of IT department and desktop -> command prompt Type ping 192.168.3.2:



The screenshot shows the Cisco Packet Tracer interface for PC1. The 'Desktop' tab is selected, and the 'Command Prompt' window is open. The command prompt displays the results of a ping command to 192.168.3.2. The first ping attempt shows a 'Request timed out.' followed by three successful replies with varying round trip times (11ms, 21ms, 10ms). The statistics show 4 packets sent, 3 received, and 1 lost (25% loss). The second ping attempt shows four successful replies with round trip times of 10ms, 11ms, 11ms, and 12ms. The statistics show 4 packets sent, 4 received, and 0 lost (0% loss).

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.2: bytes=32 time=11ms TTL=126
Reply from 192.168.3.2: bytes=32 time=21ms TTL=126
Reply from 192.168.3.2: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 21ms, Average = 14ms

C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

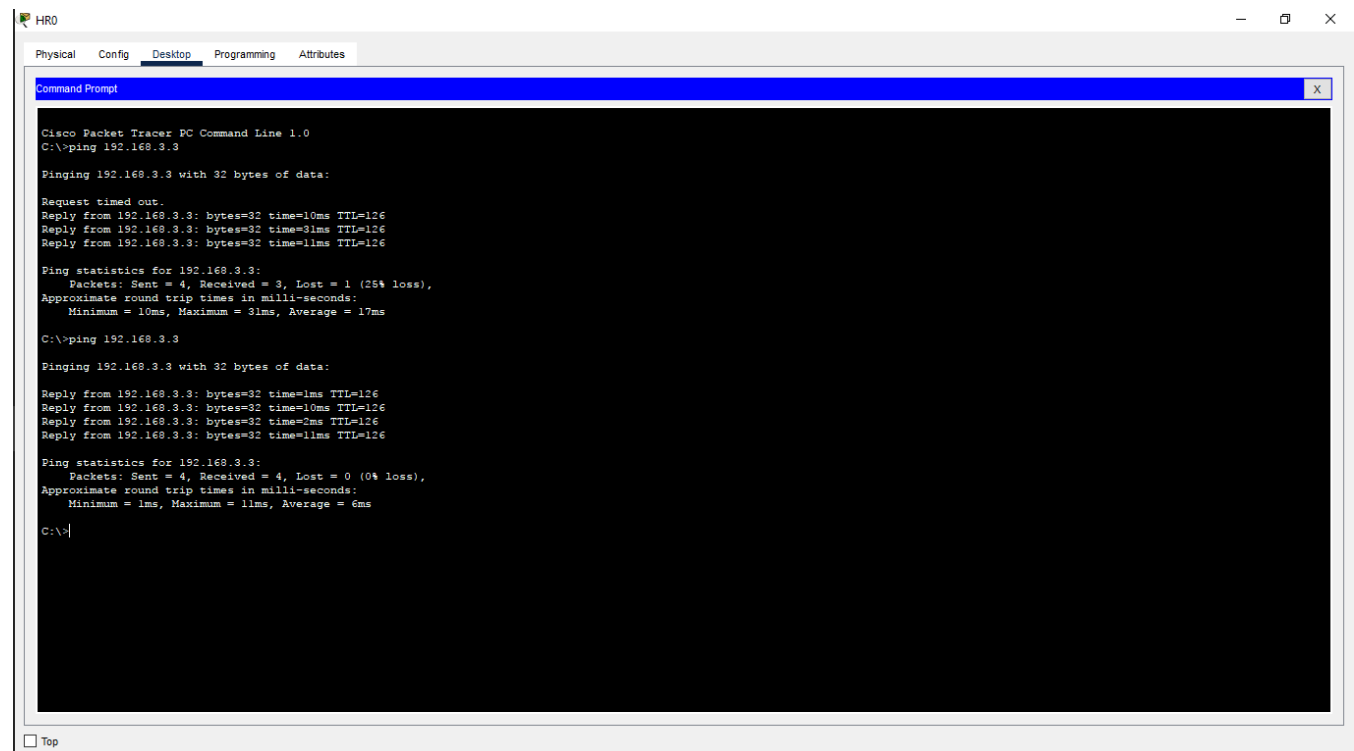
Reply from 192.168.3.2: bytes=32 time=10ms TTL=126
Reply from 192.168.3.2: bytes=32 time=11ms TTL=126
Reply from 192.168.3.2: bytes=32 time=11ms TTL=126
Reply from 192.168.3.2: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 12ms, Average = 11ms

C:\>
```

HR Department and student & staff:

Click on HR0 Desktop -> command prompt Type ping 192.168.3.3:



The screenshot shows the Cisco Packet Tracer interface for HR0. The 'Desktop' tab is selected, and the 'Command Prompt' window is open. The command prompt displays the results of a ping command to 192.168.3.3. The first ping attempt shows a 'Request timed out.' followed by three successful replies with round trip times of 10ms, 31ms, and 11ms. The statistics show 4 packets sent, 3 received, and 1 lost (25% loss). The second ping attempt shows four successful replies with round trip times of 1ms, 10ms, 2ms, and 11ms. The statistics show 4 packets sent, 4 received, and 0 lost (0% loss).

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.3: bytes=32 time=10ms TTL=126
Reply from 192.168.3.3: bytes=32 time=31ms TTL=126
Reply from 192.168.3.3: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 31ms, Average = 17ms

C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

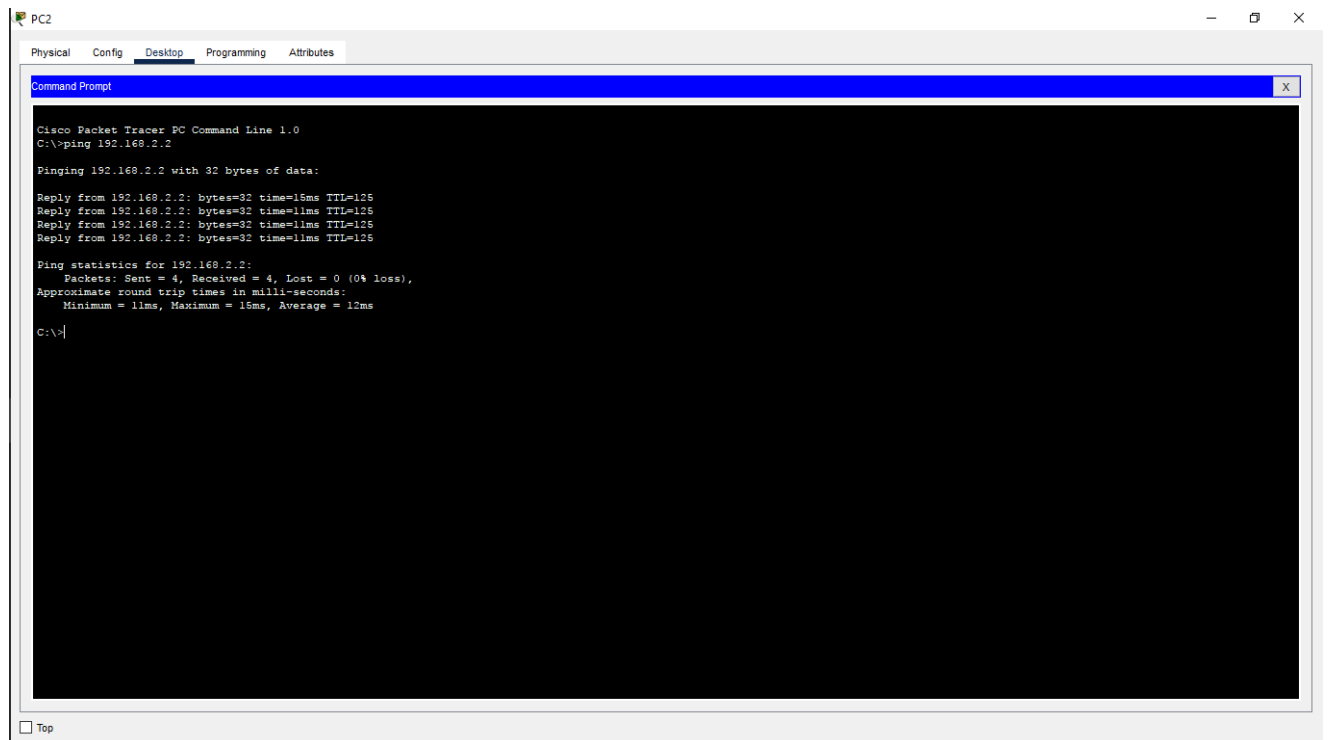
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=10ms TTL=126
Reply from 192.168.3.3: bytes=32 time=2ms TTL=126
Reply from 192.168.3.3: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 6ms

C:\>
```

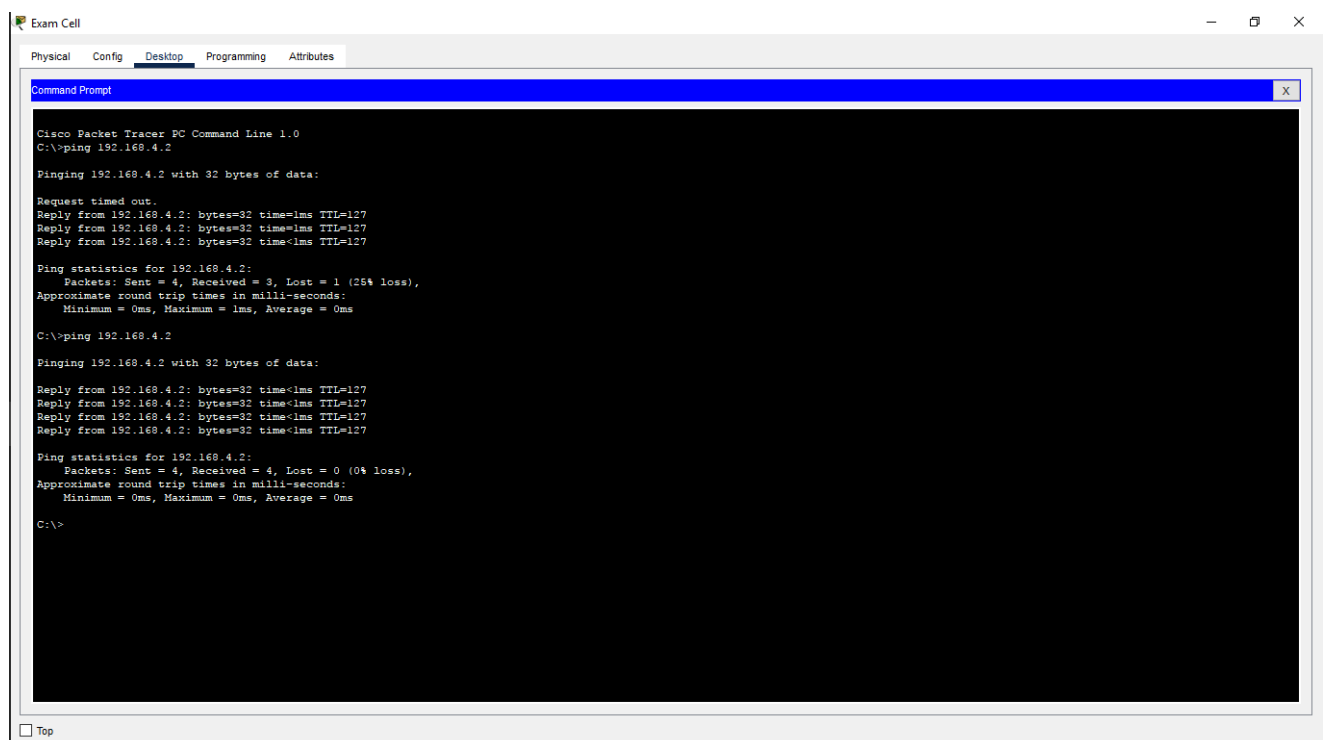
IT Department and HR Department:

Click on Pc2 -> desktop -> command prompt Type 192.168.2.2:



Management and student & staff:

Click on exam cell pc -> desktop-> command prompt Type ping 192.168.4.2:



Opening a website from a pc

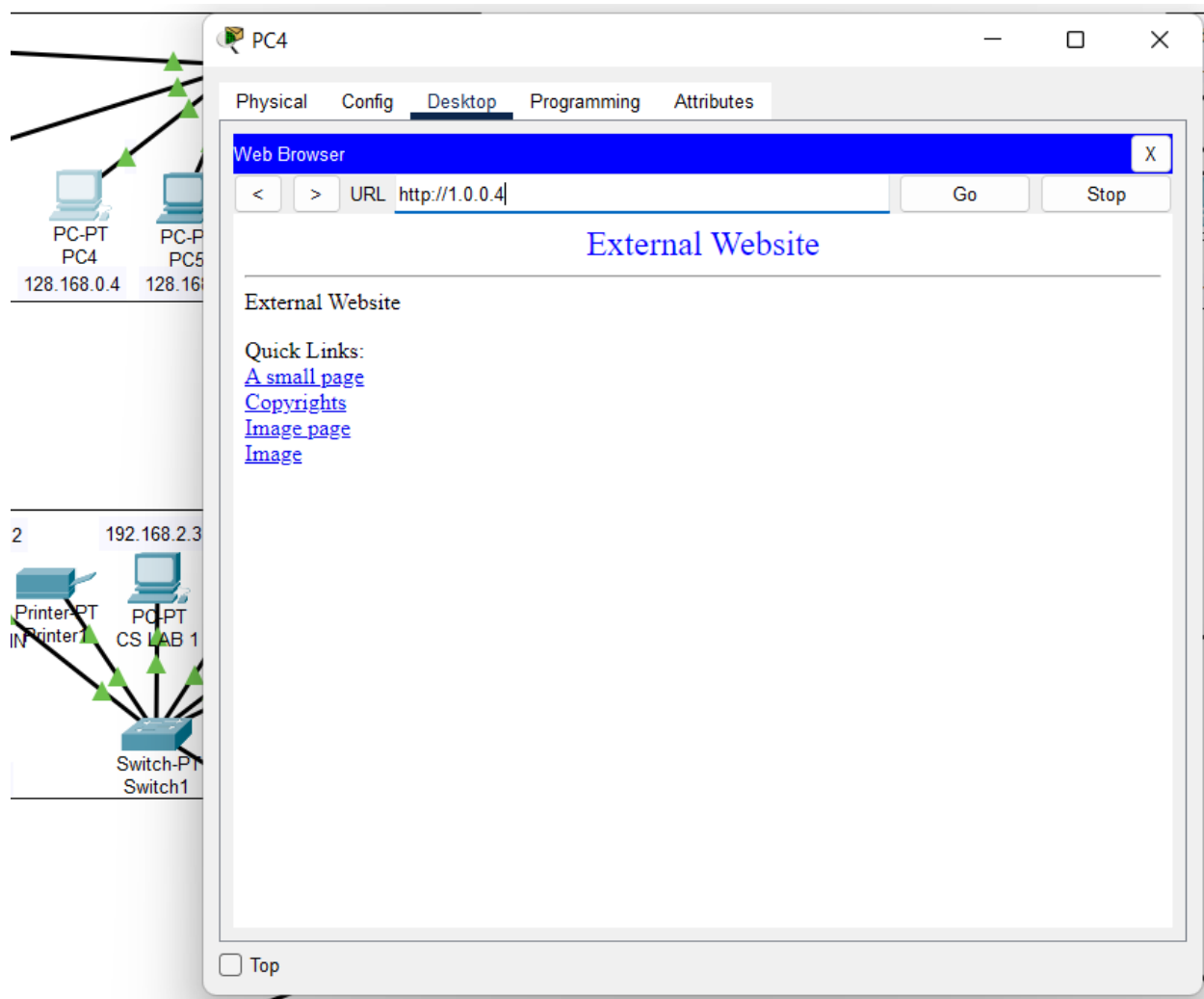
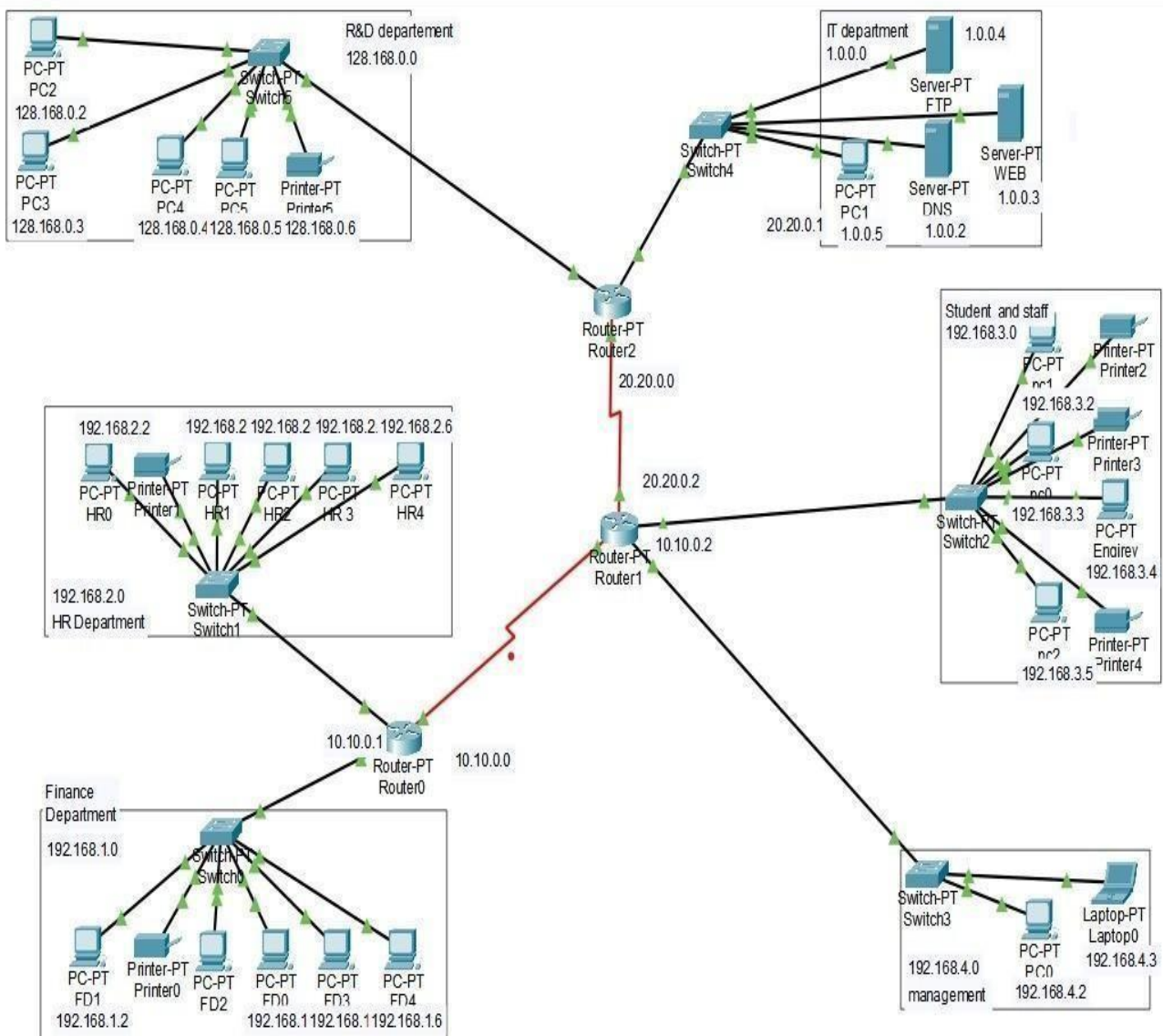


Fig 10 : Opening a website from a pc

CONCLUSION

Network designing is one of the vital roles in making sure that it needs the objective. Network is a connected collection of devices and end systems, such as computers and servers, which can communicate with each other. The physical components are the hardware devices that are interconnected to form a computer network. Software and firewalls play a major role in making sure that data is protected. Apart from the physical devices, selecting software products for installing in the network is a challenging task.

To improve college campus network design service, the technology used was creating LAN, WLAN ,rip v2 and using cheap device to reduce cost of the network. But the network can also become more enhanced using better routing protocols and many other protocols can be used to improve the security. So, we are going to try many such protocols using less number of devices and will try to keep the cost of the network less. To design such network we used software known as Cisco-Packet Tracer



REFERENCES

1. https://brainbell.com/tutors/A+/Hardware/Basic_Requirements_of_a_Network.htm
2. <https://www.geeksforgeeks.org/local-area-network-lan-technologies/>
3. <https://www.netacad.com/courses/packet-tracer>
4. <https://www.geeksforgeeks.org/man-full-form-in-computer-networking/>
5. <https://www.tutorialspoint.com/Wide-Area-Network-WAN>
6. <https://www.geeksforgeeks.org/project-idea-college-network/>
7. <https://www.tanaza.com/tanazaclassic/blog/network-configuration-wifi-in-school-and-universities/>
8. <https://www.educause.edu/ir/library/html/cem/cem99/cem9916.html>
9. <https://www.cloudflare.com/en-in/learning/network-layer/what-is-a-campus-area-network/>
10. <https://www.techtarget.com/searchnetworking/definition/campus-network>