

Proposal for network setup in a university

PROJECT REPORT

Submitted by

G SAI HARISH (RA2011003011185)
J VARUN KARTHIK (RA2011003011159)
V CHANDRA SHEKAR (RA2011003011180)
G V N S YASWANTH (RA2011003011161)

for the course

18CSC302J — COMPUTER NETWORKS

in partial fulfillment of the requirements for the degree of
BACHELOR OF TECHNOLOGY



SRM INSTITUTE OF SCIENCE & TECHNOLOGY

Deemed to be University u/s 3 of UGC Act, 1956

DEPARTMENT OF COMPUTING TECHNOLOGY

SCHOOL OF COMPUTING

FACULTY OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Deemed to be University u/s 3 of UGC Act, 1956)

KATTANKULATHUR - 603 203

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Deemed to be University u/s 3 of UGC Act, 1956)

KATTANKULATHUR - 603 203

Project Title: 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.

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

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 TZ 105 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 .o.o.o	255.0.o.o
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
	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 offices 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.

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.

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 node. 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.

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 I. 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).

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.

Network Topology Diagram

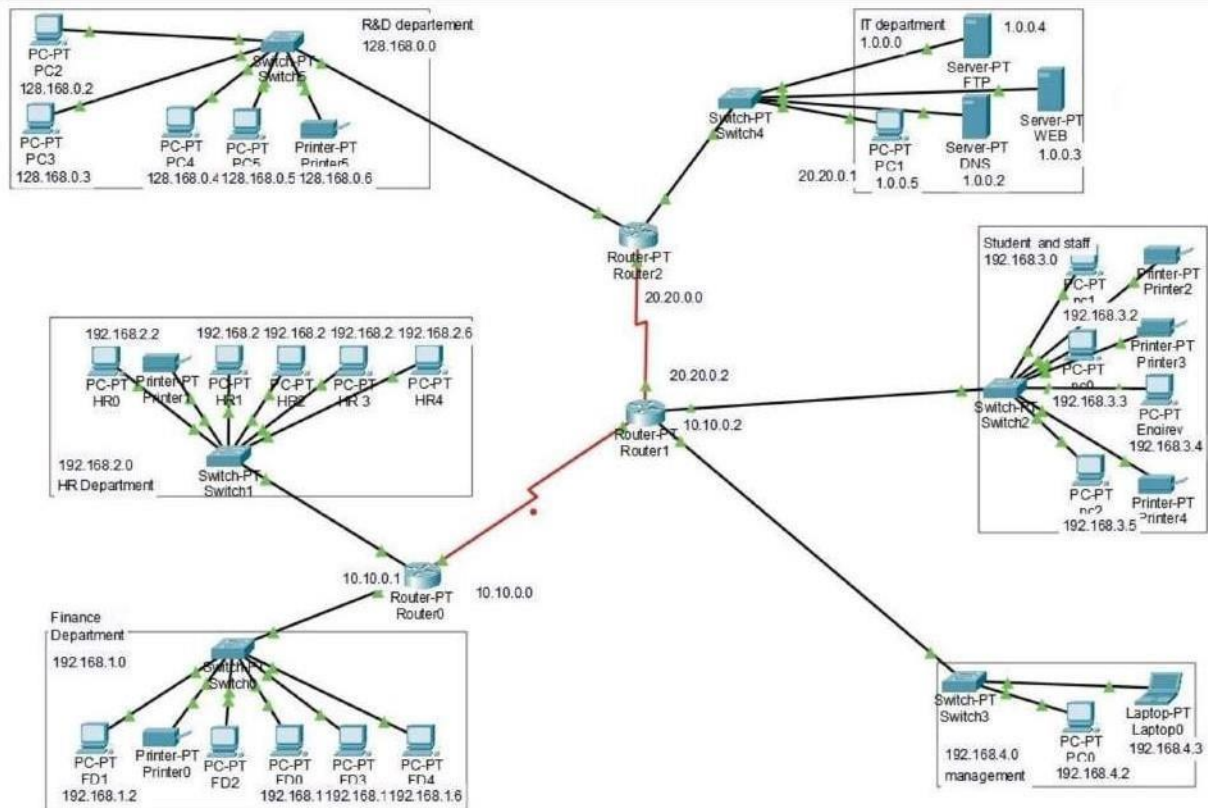


fig I : Network Topology Diagram

Access Layer

In this layer, all the end devices are connected to each other to the network and we will be having the layer I 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 the large amount of traffic very quickly.

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

2. Finance
3. HR
4. Management
5. Faculty and Students

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

IT department Network Topology:

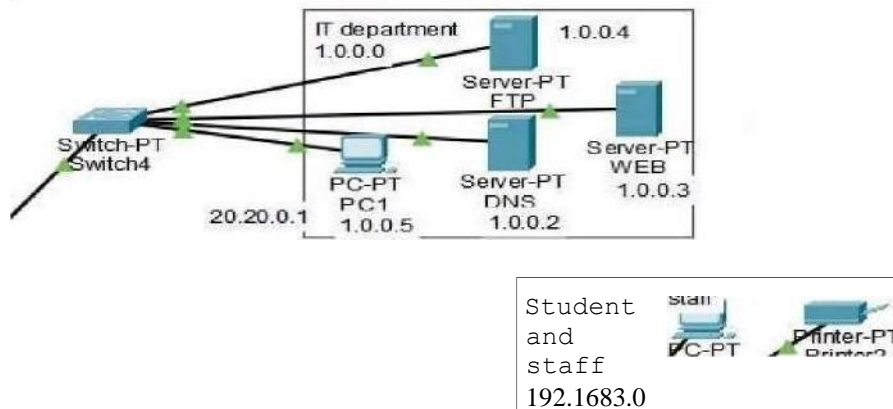


Fig 2 : IT department topology

Finance department — Network Topology:

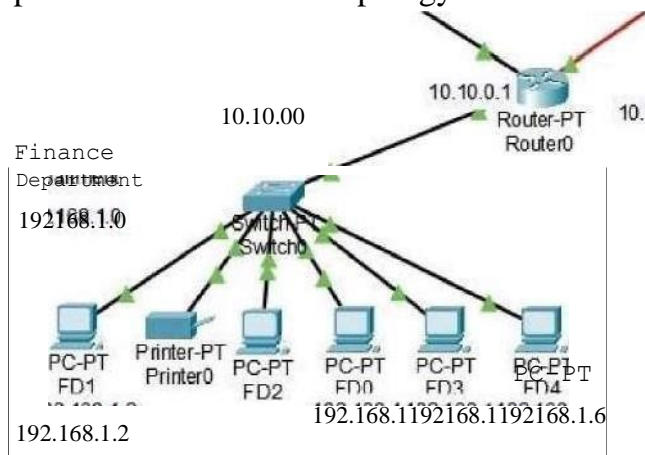
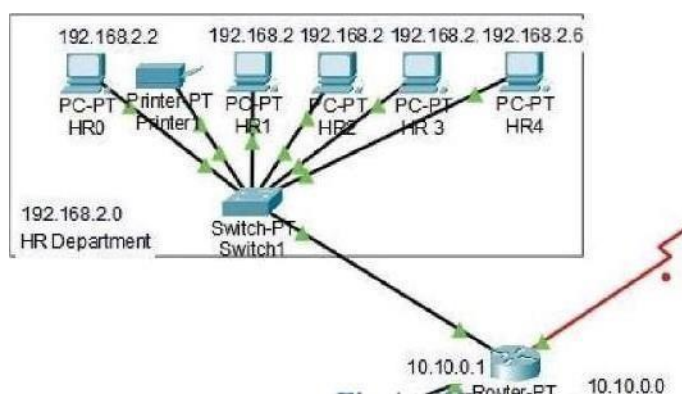


Fig 3 : Finance department topology

HR department — Network Topology:



Management department — Network Topology:

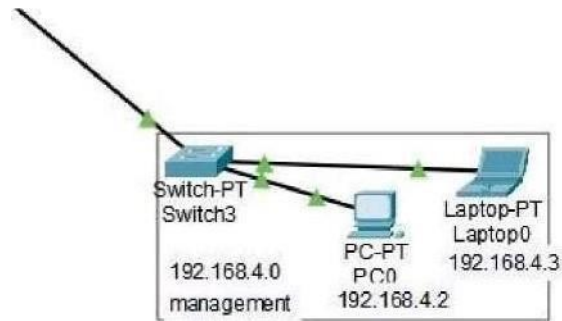


Fig 5 : Managment department topology

Faculty and Students — Network Topology:

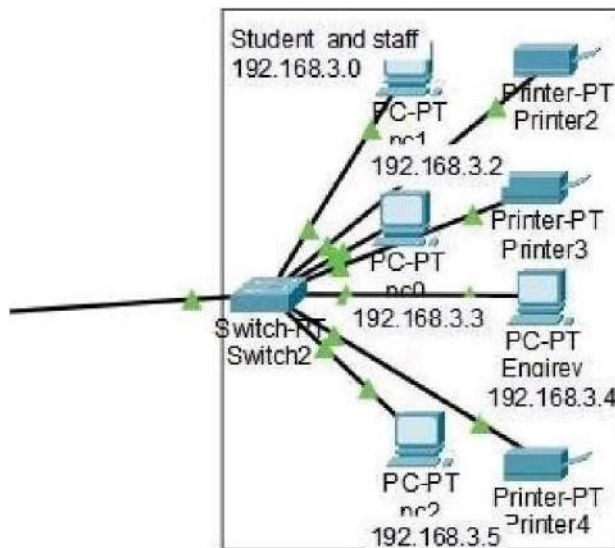


Fig 6 : _Faculty and Students topology

R&D department — Network Topology:

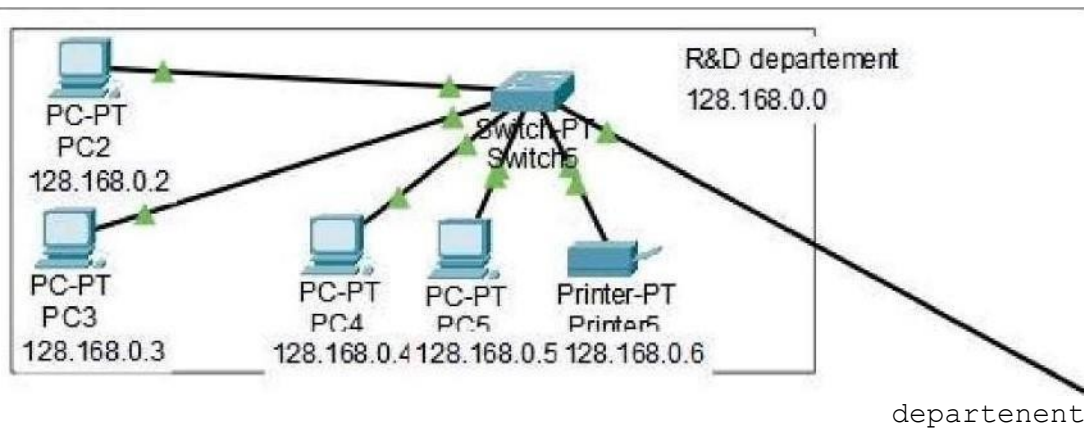


Fig 7 : R&D department topology

Network Design and configuration strategy

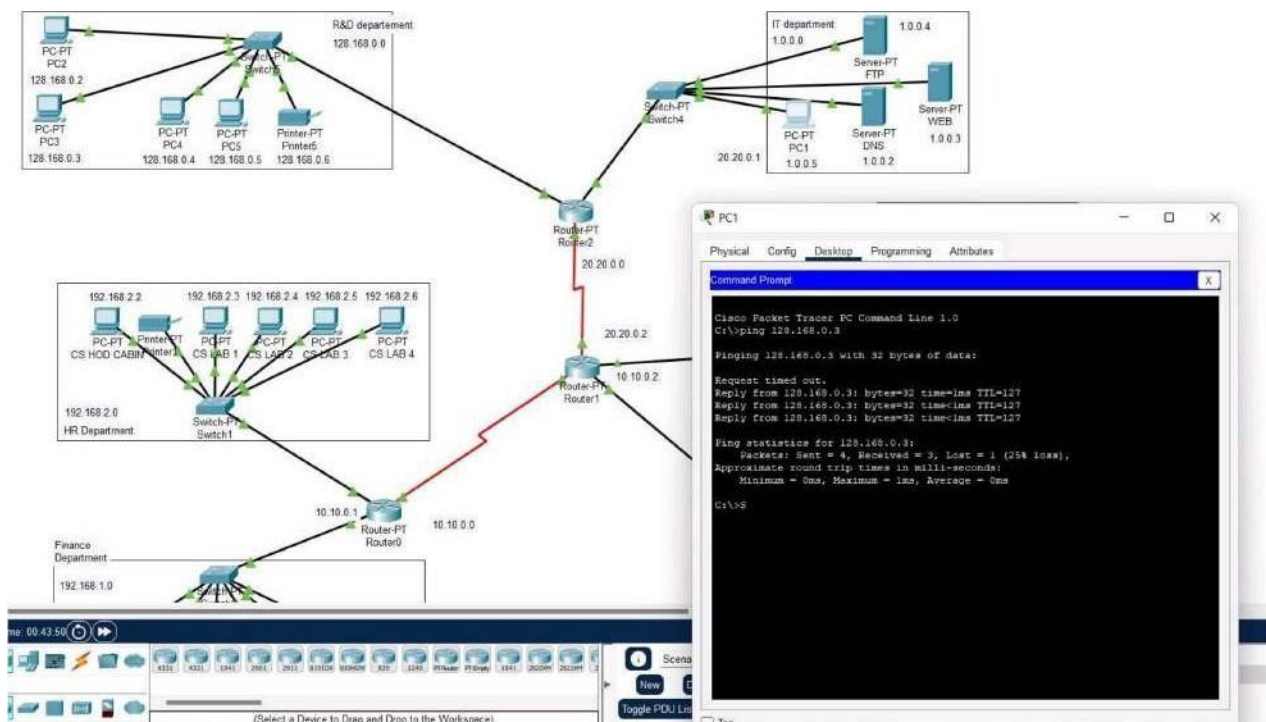
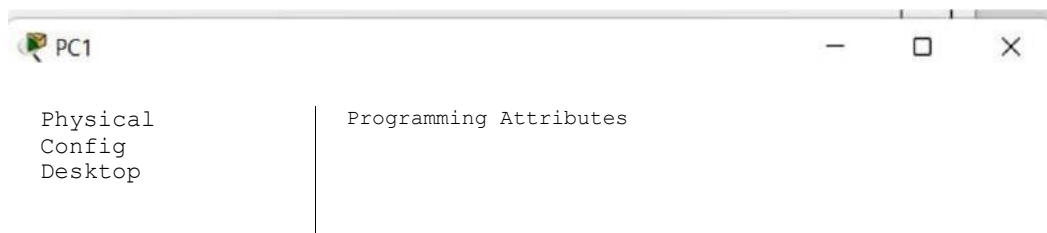


Fig 8 : Network Design

To manually check 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.



```
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 128.168.0.3

Pinging 128.168.0.3 with 32 bytes of data:

Request timed out.
Reply from 128.168.0.3: bytes=32 time=1ms TTL=127
Reply from 128.168.0.3: bytes=32 time<1ms TTL=127
Reply from 128.168.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 128.168.0.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>S
```

0 Top

Fig 9 Ping from a pc to Another PC

- 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.

Opening a website from a pc

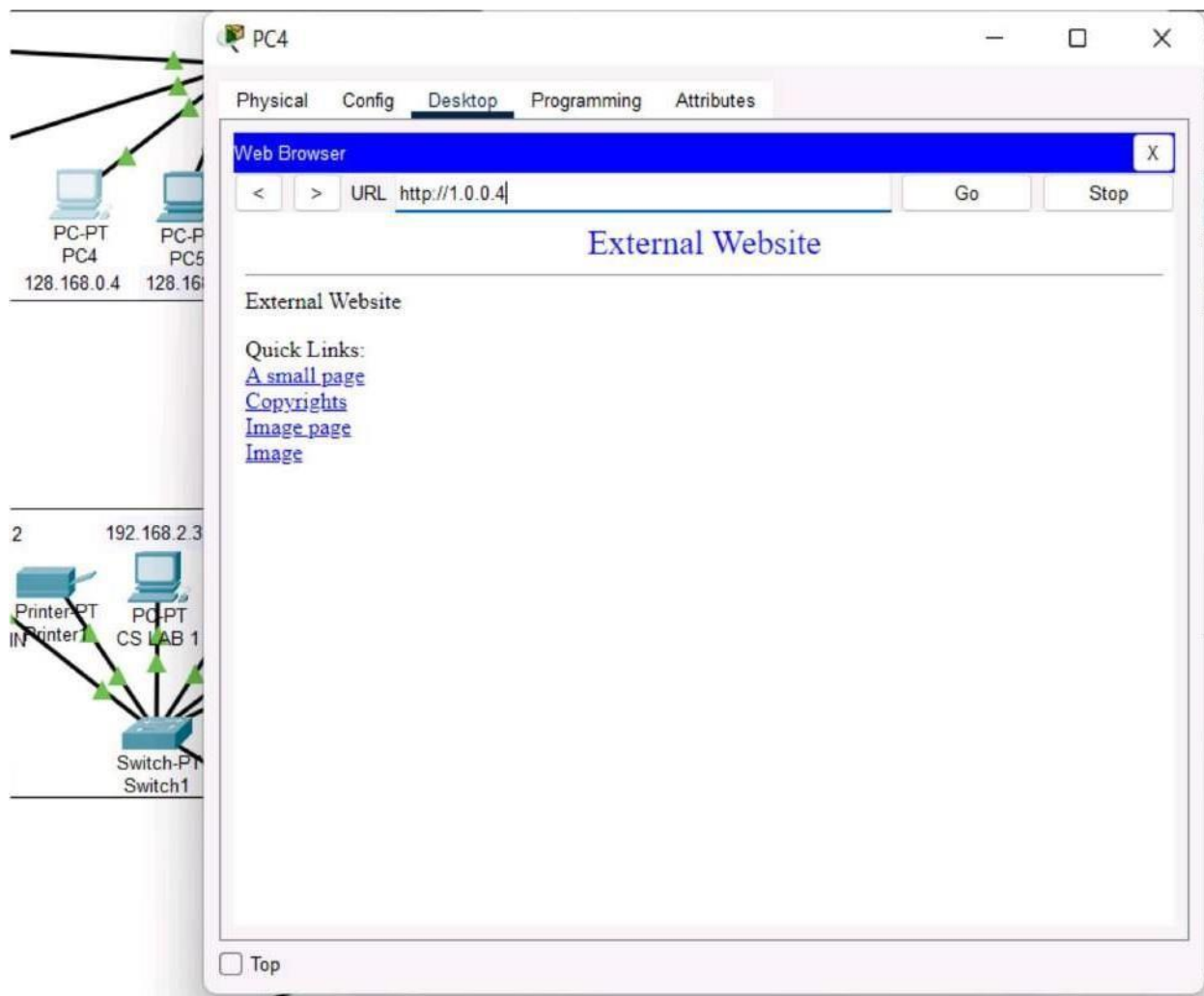


Fig 10 : Opening a website from a pc

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

REFERECE |

1. [https://brainbell.com/tutors/A+/Hardware/Basic Requirements of a Network.htm](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>