Computer Communication Network

Complex Engineering Problem

SUBMITTED TO:

Dr. Gulistan Raja

SUBMITTED BY:

Azib Farooq (18-EE-43)

Noman Ishaq (18-EE-27)

Syed Irtaza Hussain (18-EE-46)

Abstract

This project is designed to assess the technical standpoint of the students on four basic assessment parameters in regard to the problem assigned. This project is dedicated to come up with the solution to design a computer network for a seven department organization. This project is focused to test investigation, design and development, communication and team work. The team has primarily come with solution which was not viable due to conflict with different provided constraints. Keen observation of the team on the loopholes of the first design has gave rise to viable design that is implemented and discussed in the report, comprehensively. Topology is implemented for different benefits and objectives, and sub-netting is done for all the individual departments for provided private IP addresses. The connectivity of all departments and access to the organizational webserver is validation for the success of the project.

TABLE OF CONTENTS

1. Introduction

1.1 Background:

The designing and implementation of the communication network can drastically differ from project to project. The projects with high complexity and larger physical constraints have surprising complexity both in design and implementation. Whereas, the projects for knowledge testing and technical evaluation do not involve much complexity and often disregard physical constraints, and mostly they are not required to be implemented physically. The evaluation of such kind of projects are based on simulated results, technical reports etc. The complexity of these knowledge based projects is mild in comparison to the real life communication project due to scale difference. The real life communication projects can also be the scaled version of the knowledge based projects. Despite these differences, knowledge based projects provide great opportunity to get aware of the design thinking, which is highly valuable in wide range of businesses.

1.2 Problem statement

The problem statement is one line of instruction explicitly explaining the problem, which require innovative solutions addressing the problem. It also provide design thinkers to revolve around it so that their solution must address the highlighted issues.

Following is the problem statement in our project.

- Use assigned Public and Private IP addresses to design seven department organization, with different sub-net for each department.

1.3 Problem objectives

The project or problem objectives are key points to keep regard of while designing the solution. These key points are often provided in the project description and in case of not providing such objectives they are derived. Unsurprisingly, the project objectives in our case are provided under the heading of deliverables. This heading adds more clarity to the objectives as we are suppose deliver these things at final completion of the project. We will only focus the technical objectives of the project in this documentation.

Following are the technical objectives of the project assigned.

- Design network layout satisfying all the imposed constraints.
- Simulate the results in Cisco Packet Tracers showing connection validation.

1.4 Progress Checkpoints

These progress checkpoints are designed to satisfy the above outlined objectives and thus are technical in essence.

i. Design

- Configure hardware infrastructure of the organization.
- Tabulate IP addresses for all departments based on subnet for each department.
- Configure router and switches.
- Enable DHCP server for all departments and assign unique IPs to all end systems.
- Configure email server for all end systems.
- Use DNS to alias the IP of email server
- Enable browser services for all end systems.

ii. Simulation

- Ping routers and end systems of different departments.
- Simulate inter-department email transfer.

1.5 Network Infrastructure

The network infrastructure is the mother plan of the design. The design process starts with drafting the network infrastructure and finishes at its accomplishment. In grand scheme, we can also stress that quality of this infrastructure governs the technical understanding of the students. The design of project infrastructure is different for different projects. As the scope of this report and the underlying project is knowledge based, so further discussion will only be in this domain.

Primarily, this seven department project can be divided into different categories based on the components used. The first and the foremost among them is end systems and the network. Although, the criticality of this project do not have significant magnitude but this kind of division give general idea about what we need to build the entire network. As the working of the project is in the simulated environment so we do not have to bother much about the end system and we will be using personal computers as end systems/devices for each departments. As the quantity of end systems/devices different for different departments then we have to make connection point to get connected to the network core. Switch is used for this purpose. Each department has one switch and all the end systems are connected to this only switch. Up till this point we have decided about the department components for developing the hardware infrastructure. The only component left is the medium through which these end systems will be connected to the switch of the department. The constraints of project allows to use only wired connections, so we will be using copper-straight through cable to connect the end systems of each department with its only switch. The hardware segment of the infrastructure design is also followed the exact same methodology for all the departments.

After building the hardware framework for all the seven departments, our team decided to choose tree topology to connect all these department to the network core. Although the size of the project is small so network core might be an in-appropriate terminology but we decided to stick with the standard terminology for the documentation. So, network core of seven department project should consist of different components to manage all the loopholes in all conditions, and must not fail to serve the assigned objectives.

In second step, we have to connect all the departments to common point so that information should be given to that point and it can easily be distributed to all seven departments. For this purpose we also have used a switch, but this time the switch will be connected to the dedicated and only switch of each department. The wire used for connection of these switches is copper crossover cable, as type of both these components are same. Creating components and making physical connections is not enough to make the network work and serve the desired objective. We have to assign IP addresses all the end systems and switches as well. As the size of the departments are large and the cumulative sum of all the end systems cannot be managed manually. So, to remove this anomaly we have to use DHCP services of a server. This server should be connected to the common of all departments. We have several options to connect this server directly to the common switch of all department or we can make separate department to handle all these servers then connect the switch of this department with the common switch. As the later approach is more viable and clean so we decided to make another department handling servers only. In this department we add three servers, which is also the requirement of the project. These servers are email, DNS, and DHCP. All three serve different purpose. Email server is used to give email service to the clients whereas DNS is used to access the email server with an alias name, to easily remember. The DHCP is responsible for providing unique IP addresses to all of the end systems.

Up till now we have completely developed hardware segment of the departments of the infrastructure. This entire circuitry we have developed so far can be called as Local Area Network (LAN). This LAN has eight total department, one department for servers, connected through one common switch. This completes our departmental LAN hardware design segment of the project infrastructure. But to satisfy other constraints we also have to include different component. The ISP (Internet Service Provider) has provided us with public IP addresses for internet access and webserver access for the organization. To include such services to our departmental end systems we also included routers, to connect LAN with the ISP provided servers.

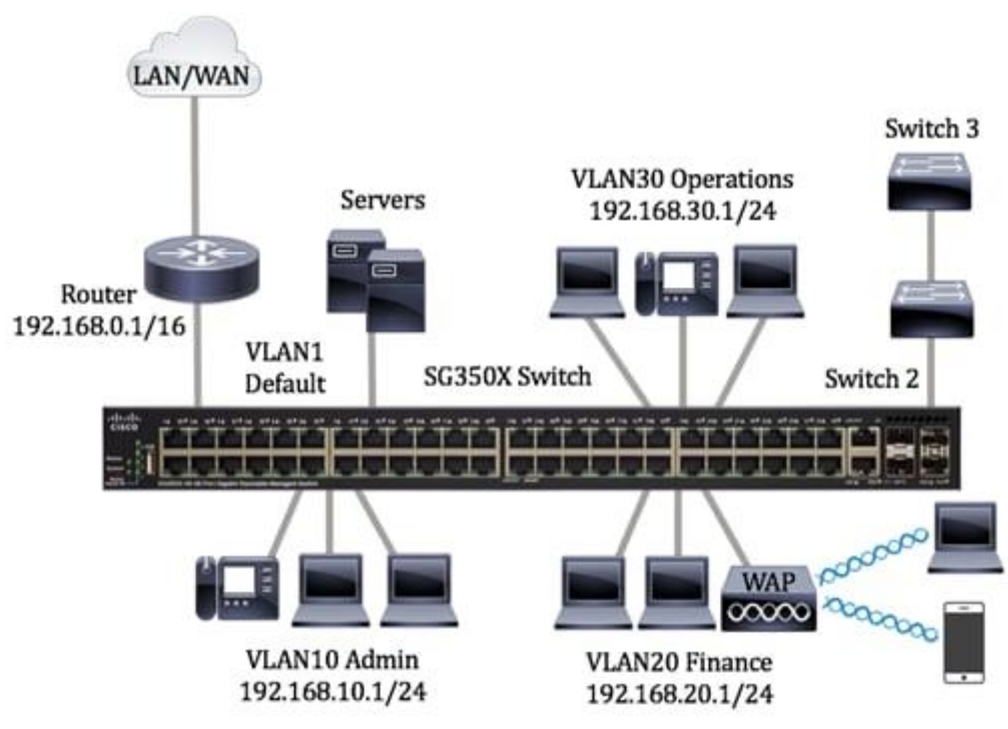
The detail and comprehensive discussion of this design will be waged in the upcoming segments of the documentation. In the upcoming segments the connectivity issues and their software implications will be discussed along with the rectification methods. The hardware segment plays minor role in the design process in comparison to the software segments, where intangible real bottlenecks appeared and their resolution require dynamic knowledge about software entities of network design.

2. Literature Survey

2.1 Switch VLAN

VLAN is acronym of Virtual LAN (Local Area Network). It is an administrative feature of the switch to allow administrators to automatically limit access to a specified group of users by dividing the connected network into isolated LAN segments [1]. In this way, it has great benefit for the relocation of the end systems from one group to the other. VLAN is created on VLAN supported switches, where each port of the each is designed for particular segment of the LAN in which the switch is working [1].

In order to better understand the VLAN, we can focus the very abbreviation of its acronym and we get the idea that this feature of the switch is responsible for creating virtual LANs in one main LAN.



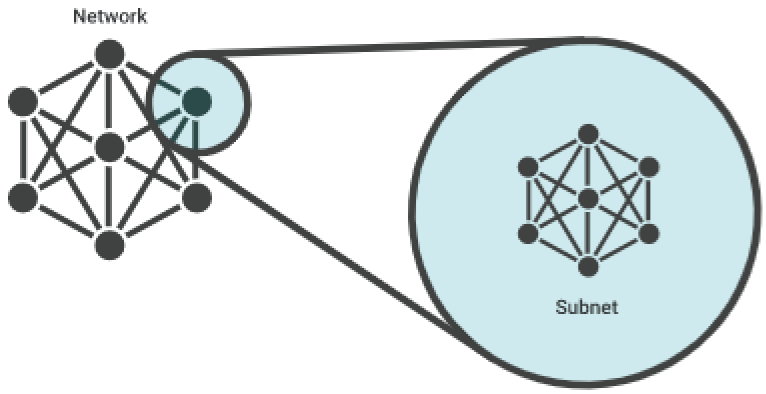
In the above illustration it is possible to that the switch is working in one LAN but different ports of switch is dedicated for particular department, and other switches and thus this port dedication comes from VLAN feature of the switch.

2.2 DOT1Q Encapsulation

While using VLANs in the switch, host do not have any idea about the VLAN it is connected to and it simply send Ethernet frame, which do not contains any information about VLAN to which the host is desiring to communicate. When the Ethernet frame arrives at the switches then switch adds a tag which contain information about VLAN id. On the switch with desired VLANs, this tag will be removed, and the Ethernet frame is transmitted to the desired host. Thus the link between the two switches is called trunk. And the protocol used on this link is called trunking protocols. The most common among these protocol is the 802.1Q and it is also called dot1q protocol [3].

2.3 Sub-netting

Sub-netting or sub-networking is among the highly used techniques in the domain of computer communication networks. In simple words, sub-net is the small network within a network. In order to better understand sub-netting we have to first understand the IP address. The IP (Internet Protocol) address is the address of the components working in the network and this address basically represent their point of connection to the other device. For example a host system has one port then it should have one IP address. On the other hand switch having multiple ports can have multiple IP address and on that basis it also create VLANs. There are many types of IP addressing schemes but the most common is IPv4 addressing scheme. In this scheme IP address is 4B or 32 bits in size [3]. While designing a network we have to ensure that the delivery of data from one end system to other end system is efficient and do not travel to un-necessary nodes. In this way we design subnet to divide bigger network into small and manageable networks called subnet. The subnet is made by tempering the host bits of the IP address.



Suppose, an organization is provided with the IP address of 200.23.16.0/20, where the number after slash present the prefix bits and which will be fix for all system in the organization. The organization has three departments and in order to better manage these department the organization decided to divide the provided IP address to 3 subnets. There are many possible combinations of subnets in this case following are some of them.

Subnet – 0: 200.23.16.0/23

Subnet – 1: 200.23.18.0/23

Subnet – 2: 200.23.20.0/23

2.4 DHCP and IP Helper address

Dynamic Host Configuration Protocol is protocol for assigning IP addresses to the end systems dynamically, eliminating the need to give them static IP addresses. While dealing in the projects of large organizations where end systems are variable and are in enough quantity to make static IP assigning process painful than DHCP services gives great advantage in such scenarios. In simple words, DHCP is responsible to automate IP configuration process [4].

IP helper address is a command commonly used to assist end systems to get address of the DHCP server. This command is used in the configuration mode for routers and switches, where the particular port of the components is configured to the IP address of the DHCP server. In this way, whenever that particular port of the component gets DHCP request, it redirects this request to the DHCP server in the network. On the contrary if this command is not used then end systems connected at particular port of the component may not be able discover the DHCP server and the IP configuration of that system may get failed.

2.5 Routing

Router is the principal device to connect different LANs and allow their communication using different algorithms and protocols. The algorithms used in finding route in router is called routing algorithm. Routing algorithm and protocols are different things and the working of one depends upon the other [5]. The routing protocol gives variables to the algorithm and algorithm in turn gives IP address of the next node to the protocol. In this way, routing in router is a two stranded process supported router protocols and algorithms.

i. OSPF

Open Shortest Path First (OSPF) is a routing protocol for routing in IP networks. The algorithm used by this protocol is Link state, and it also falls in the category of interior gateway protocols (IGP). In large enterprise, OSPF is widely used routing protocol to connect different LANs through routers. OSPF protocol makes copy of the Link State Database (LSDB) in all routers of the network along with the information of all sub-nets within the system and all the routers should be connected to the area 0, which is the principal area [6].

2.6 Sub-Interfacing

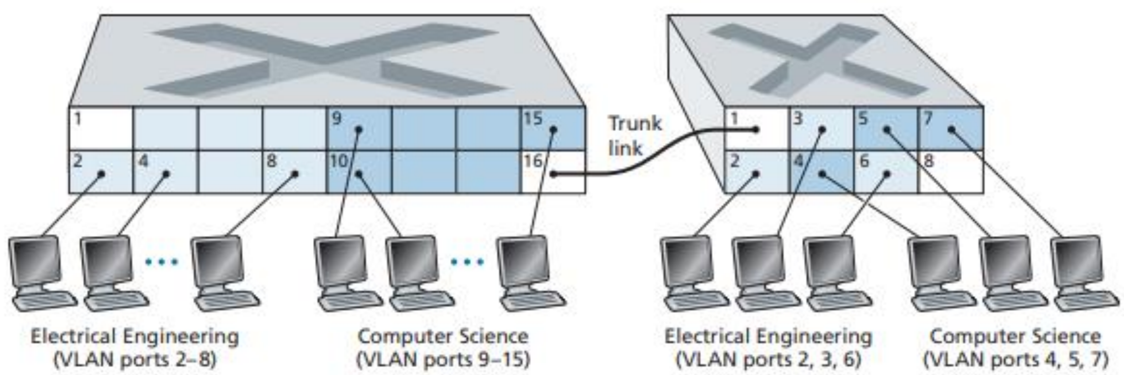
The division of one physical interface into multiple logical interfaces of the router is called sub-interfacing. There are limitations of the physical interface that it can serve only one LAN which connected to that physical port, but due to sub-interfaces we can support 4094 VLANs on one physical interface [8].

2.7 Network Address Translation (NAT)

The devices within the organization uses private IP addresses which are different from public IP addresses. There are multiple reasons beyond that but the foremost and prime reason is the wide spread of the internet and end systems. If every end system has unique IP address and then we might ran out of public IP addresses which are limited to 4 billion [9]. To avoid this problem the organizational and houses IP addresses are translated into different set of IP address through router, which are private and cannot directly be accessible through internet. In this way, two organizations can use same private IP addresses and when they access something thing from internet than their private IP address will be translated to public IP address. This process of translation is called Network Address Translation (NAT) and it occurs at edge of the network.

2.8 Trunking:

Using trunking a special port is configured on each switch which is called Trunk Port. A trunk is a single channel of communication that allows multiple elements at one end to connect with the correct element at the other end. It kind of a "link" that contains many signals at the same time and creating more efficient network access between two nodes in which the communication has to be made. An example of trunk linkage is shown in figure where port 16 of one Group is connected to port 1 of the other group using Trunk Link. [10]



3. Proposed Design:

The requirements of the Project are:

The Local ISP should have assigned two Public IP addresses 128.03.04.08 for internet access and 128.0.72.75 for organization webserver to an organization.

The organization should have decided to use a private IP address block 10.0.0.0 for internal IP address assignment to 7 different departments.

The six departments should have at least 100 users and the one department should have variable number of users and it could accommodate more users in future.

The other properties that the Network should have are:

- The organization should have its own webserver.
- DNS server for web server, to translate the URL to IP address.
- Email server to allocate email addresses to users of its organization.
- There should be only a single DHCP server for entire organization. Use the DHCP server for only one appropriate department.

The design to be proposed should be understandable, coherent and with less expense. To accommodate all above properties there can be two designs for this project:

3.1 Design 1:

A. Components Required:

PCs

One PC is going to be connected with switch to make a Department and total number of seven departments are required.

Switches

One switch as Trunk Switch, seven switches for departments and one switch for connecting Servers.

Servers

One server will act as Web Server which needs to be connected with one of the department which don't have specific number of users but variable users. One server is DNS Server, one is DHCP Server and the last server is an Email server

Routers:

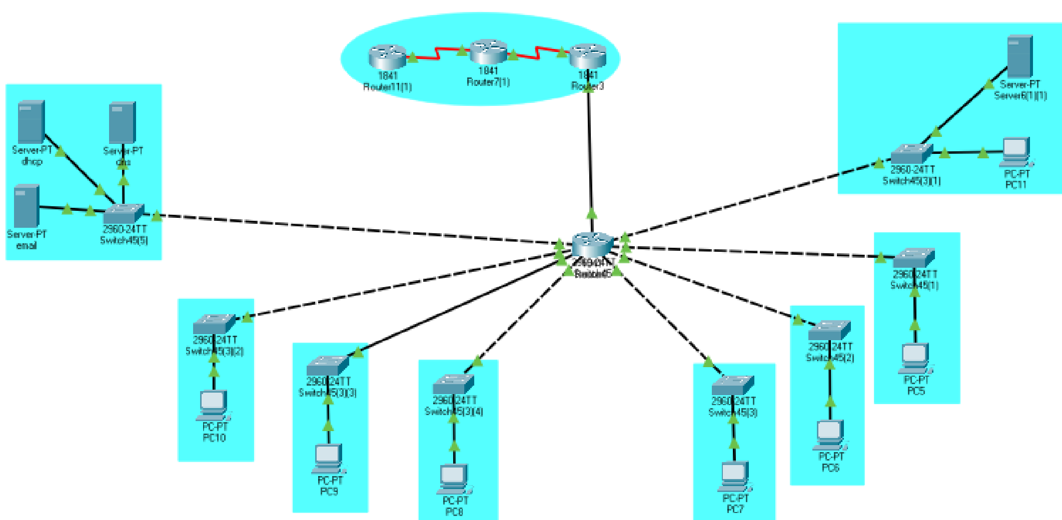
One router that is a Web Router is going to be connected with the switch that connects it with web server. The other three are going to be an ORG Router, NAT Router and the last one is ISP Router.

B. Structure:

Total number of switches connected to the ORG router is eight. The required number of departments are seven so number of switches connected to the ORG Router must be seven for departments. One switch connected to that router is connected to three servers which are DNS, DHCP and Email Servers.

All switches are connected to servers or PCs by Copper Straight thorough wire as these are different devices. The web router is also connected to the switch by Copper Straight Through wire. But routers are connected to each other by subnetting.

The network formed by this is:



C. Limitations of this design:

Since router is a layer-3 device so connecting each switch to a router will need more number of interfaces. Suppose if number of departments are increased so number of interfaces will increase accordingly which will cause the design to be much more expensive.

3.2 Design 2:

i. Components Required:

PCs

Each PC is going to represented as Department and total number of seven departments are required.

Switches

One switch as Trunk Switch, seven switches for departments and one switch for connecting Servers.

Servers

One server will act as Web Server which needs to be connected with one of the switch. One server is DNS Server, one is DHCP Server and the last server is an Email server

Routers:

One is an ORG Router, one is NAT Router and the last one is ISP Router.

ii. Changes with respect to first design:

To decrease number of interfaces we use a layer-2 device which is a switch supporting VLAN (virtual local area network) to connect all departments to a router. This switch will allow multiple VLANs to define a single LAN structure. So PCs can communicate within the network. The Hosts within a VLAN communicate with each other as if they were connected to the switch without any other host. In port based Virtual Local Area Network the switch's ports which are interfaces are divided into groups by the manager of network. Each group constitutes a virtual local area network, with the ports in each VLAN forming a broadcast domain or limit and the broadcasting can only be possible within a group. [11]

The VLANs cannot interconnect outside the groups and for different departments we need communication outside the group so it's not possible to communicate different departments this way. The solution for this problem is **Trunking.**

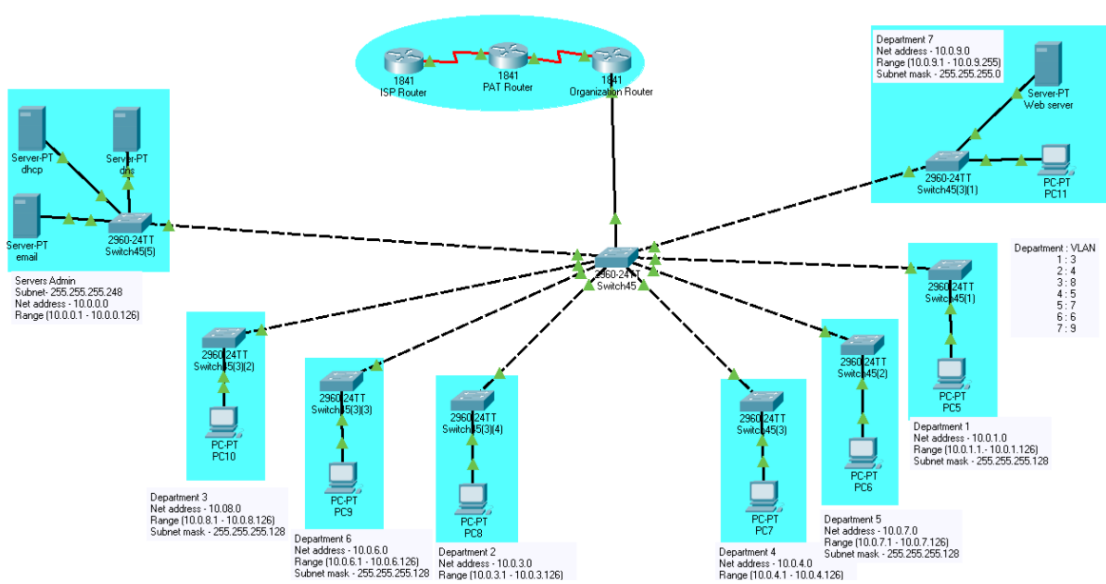
iii. Structure:

The trunk switch is connected to eight switches in which seven are going to represent each department and one is going to connect the DNS, DHCP and Email servers. All these servers are connected to one switch that is connected to Trunk Switch.

Six switches are connected to one PC each so it can handle a particular number of users e.g 100. One switch is connected to a PC and a web server. The web server can be connected to any switch in the whole circuit. For connecting switch with switch use Copper Cross-Over wire as for connecting same devices Copper Cross over is used. To connect Switch with PC and Server we use Copper Straight Through wire as all these are different devices.

The ORG Router is connected with Trunk switch and other routers are connected by subnetting.

The structure that is formed is:



iv. Advantage of this design:

This design doesn't need so many interfaces like design 1 so this design is way cheaper than above in terms of Cost.

3.3 Design steps :

Following steps we will follow for the design 2:

- Make the subnet for seven departments from the given block of IP addresses i.e. 10.0.0.0 .
- Specifying the VLAN for each of the department separately (mentioned on the topology design) .
- Selection of the routing Algorithm. (For communication).
- Selection of VLAN for web server 128.0.72.75 (mentioned on the Topology)
- Designing the Topology on the CISCO packet tracer.
- Make the VLAN from 2-10 on the switches for departments and servers.
- Making Sub interfaces on organizational router for each of the VLAN and setting the IP address of each sub interface. We will use the first address of Subnet as default gateway and as IP of the sub interface. Applying DOT1Q encapsulation on each interface for communication among the VLAN.
- Till now we have set up the VLAN structure.
- Now DHCP and DNS are assigned with the static IP's (mentioned in the subnetting) . DHCP's service is on with the Sub interface IP's as default gateway and. DHCP is configured. The email server can now be configured. The IP of mail server is added in the DNS server and is switched on.
- Now interfaces of the switches (except the departmental interfaces which will be assigned the access mode for VLAN mentioned in the topology) will be made trunked.
- Now going to the org router, and applying the ip helper-address 10.0.0.5 to each sub interface. Which will help to the find the DHCP server in the entire organization.

- Now configuring the org router serial port and NAT router with NA address 192.168.1.0 255.255.255.252 . while NAT router and ISP router are also configured.
- Now PAT is applied at the NAT router, So that IP of every pc of the organization will be changed to the assigned internet access IP of 128.03.04.08 . So the address translation will occur at the NAT router.
- Now coming to the email server ,which is set up with the Domain name **an.com.** Then PC's are configured with their email.
- DNS are given names of webserver and its ip along with email server.

Let us begin with

i. **Subnetting :**

After selecting the design 2 we will go for the subnetting technique so that we can use the assigned IP address efficiently. Lets begin with subnet for the server VLAN

Subnet 1 (for server)

Need only few IP's in first subnet. let us take 3 bits for host so the

2^3 = 8 Hosts can be supported . which means three bits of subnet will be zero rest will be one, giving us the following mask as

Subnet mask : 255.255.255.248

Network Address : 10.0.0.0

First IP : 10.0.0.1

Last IP : 10.0.0.6

Broadcast Address : 10.0.0.7

In this server we have fixed DHCP IP as

DHCP IP : 10.0.0.5 255.255.255.248

DNS IP :10.0.0.2 255.255.255.248

Subnet 2 (department 1)

We have to 100 users in first 6 departments. So we surely need 7 bits for 100 users Which means that the 2^7 - 2 = 128-2 = 126 users can be supported. Sor for each of six departments subnet mask will be having seven left most bits will be zero. So subnet mask will be

Subnet mask : 255.255.255.128

Network IP : 10.0.1.0

First IP : 10.0.1.1

Last IP : 10.0.1.126

Broadcast IP : 10.0.1.127

We will make subnets with same subnet mask till the departments . So we go with the following as under we have as the

Subnet 3 (for department 2) :

Subnet mask : 255.255.255.128

Network IP : 10.0.3.0

First IP : 10.0.3.1

Last IP : 10.0.3.126

Broadcast IP : 10.0.3.127

Subnet 4 (for department 4) :

Subnet mask : 255.255.255.128

Network IP : 10.0.4.0

First IP : 10.0.4.1

Last IP : 10.0.4.126

Broadcast IP : 10.0.4.127

Subnet 5 (department 6)

Subnet mask : 255.255.255.128

Network IP   : 10.0.6.0

First IP : 10.0.6.1

Last IP : 10.0.6.126

Broadcast IP : 10.0.6.127

Subnet 6 (for department 5):

Subnet mask : 255.255.255.128

Network IP   : 10.0.7.0

First IP : 10.0.7.1

Last IP : 10.0.7.126

Broadcast IP : 10.0.7.127

Subnet 7 (department 3)

Subnet mask : 255.255.255.128

Network IP   : 10.0.8.0

First IP : 10.0.8.1

Last IP : 10.0.8.126

Broadcast IP : 10.0.8.127

Now we are designing the Subnet for the seventh department as under we have as under we have as the

Subnet 8 (department 7)

We have to choose variable number of the host. we took 8 host bits that will support 256 hosts with the Subnet mask as under we have

Subnet mask : 255.255.255.0

Network Address : 10.0.9.0

First IP address : 10.0.9.1

Last IP address : 10.0.9.254

Broad cast address : 10.0.9.255

If you want to increase the number of hosts , you can use more number of the host bits such as 12 0r 24 .The range for variable user will increase .

ii. Choosing Protocol :

- 802.1Q is used for the communication within organization i.e. which is used to communicate among the VLAN's of different department.
- OSPF is used to communicate among the router

  .

iii. Specifying VLAN :

Server : VLAN 2

Web Server : VLAN 2

Now specifying VLAN for each of the of the department.

Department : VLAN

1 : 3

2 : 4

3 : 8

4 : 5

5 : 7

6 : 6

7 : 9

Now our specification is complete for each of the network device Now moving toward the next section of the report.

4. Result interpretations and Investigation:

4.1 Routers CLI programming :

i. Organizational Router:

Router>enable

Router#

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#

Router#configure terminal

Using organization as the password. When you are finished, exit from line configuration mode.

Router(config)#line console 0

Router(config-line)#password organization

Router(config-line)#login

Router(config-line)#exit

Router(config)#

Router(config)#line vty 0 4

Router(config-line)#login

Router(config-line)#exit

```
Router(config)

Router(config)#interface fa0/0.1
Router(config-subif)#encapsulation dot1q 2

Router(config-subif)#ip address 10.0.0.1 255.255.255.248

Router(config-subif)#ip helper-interface 10.0.0.5

Router(config-subif)#exit

Router(config)#interface fa0/0.1
Router(config-subif)#encapsulation dot1q 2

Router(config-subif)#ip address 10.0.0.1 255.255.255.248

Router(config-subif)#ip helper-interface 10.0.0.5

Router(config-subif)#exit

Router(config)#interface fa0/0.2
Router(config-subif)#encapsulation dot1q 3

Router(config-subif)#ip address 10.0.1.1 255.255.255.128

Router(config-subif)#ip helper-interface 10.0.0.5

Router(config-subif)#exit

Router(config)#interface fa0/0.3
Router(config-subif)#encapsulation dot1q 4

Router(config-subif)#ip address 10.0.3.1 255.255.255.128

Router(config-subif)#ip helper-interface 10.0.0.5

Router(config-subif)#exit

Router(config)#interface fa0/0.4
```

Router(config-subif)#encapsulation dot1q 8

Router(config-subif)#ip address 10.0.8.1 255.255.255.128

Router(config-subif)#ip helper-interface 10.0.0.5

Router(config-subif)#exit

Router(config)#interface fa0/0.5

Router(config-subif)#encapsulation dot1q 5

Router(config-subif)#ip address 10.0.4.1 255.255.255.128

Router(config-subif)#ip helper-interface 10.0.0.5

Router(config-subif)#exit

Router(config)#interface fa0/0.6

Router(config-subif)#encapsulation dot1q 6

Router(config-subif)#ip address 10.0.6.1 255.255.255.128

Router(config-subif)#ip helper-interface 10.0.0.5

Router(config-subif)#exit

Router(config)#interface fa0/0.7

Router(config-subif)#encapsulation dot1q 7

Router(config-subif)#ip address 10.0.7.1 255.255.255.128

Router(config-subif)#ip helper-interface 10.0.0.5

Router(config-subif)#exit

Router(config)#interface fa0/0.8

Router(config-subif)#encapsulation dot1q 9

Router(config-subif)#ip address 10.0.9.1 255.255.255.0

Router(config-subif)#ip helper-interface 10.0.0.5

Router(config-subif)#exit

Router(config)#interface fa0/0.9

Router(config-subif)#encapsulation dot1q 10

Router(config-subif)#ip address 10.0.72.1 255.255.255.0

Router(config-subif)#exit

Configure a message-of-the-day banner using the banner motd command.

Route(config)#banner motd &

Enter TEXT message. End with the character '&'.

****

!!!ORGANIZATIONAL ACCESS ONLY!!!

****

&

Router(config)#

Router(config)#enable secret organization

Router(config)#Router ospf 1

Router(config-router)#network 10.0.0.0 0.255.255.255

Router(config-router)#network 192.128.1.0 0.0.0.252

Router(config-router)#exit

Router(config)#exit

Router#exit

ii. PAT Router:

We have assigned the IP for the PAT router then PAT. So the CLI config of PAT router at which the PAT is occurring is as under we have the

PAT router running config command as under:

```
interface Serial0/0/0
 ip address 192.168.1.2 255.255.255.252
 ip nat inside
 clock rate 2000000
!
interface Serial0/0/1
 ip address 192.168.10.1 255.255.255.0
 ip nat outside
 clock rate 64000
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.3 area 0
!
router ospf 11
 log-adjacency-changes
!
ip nat pool jkr 128.3.4.8 128.3.4.8 netmask 255.255.0.0
ip nat inside source list 1 pool jkr overload
ip classless
!
ip flow-export version 9
!
!
access-list 1 permit 10.0.0.0 0.255.255.255
!
```

After doing PAT we look towards the switches.

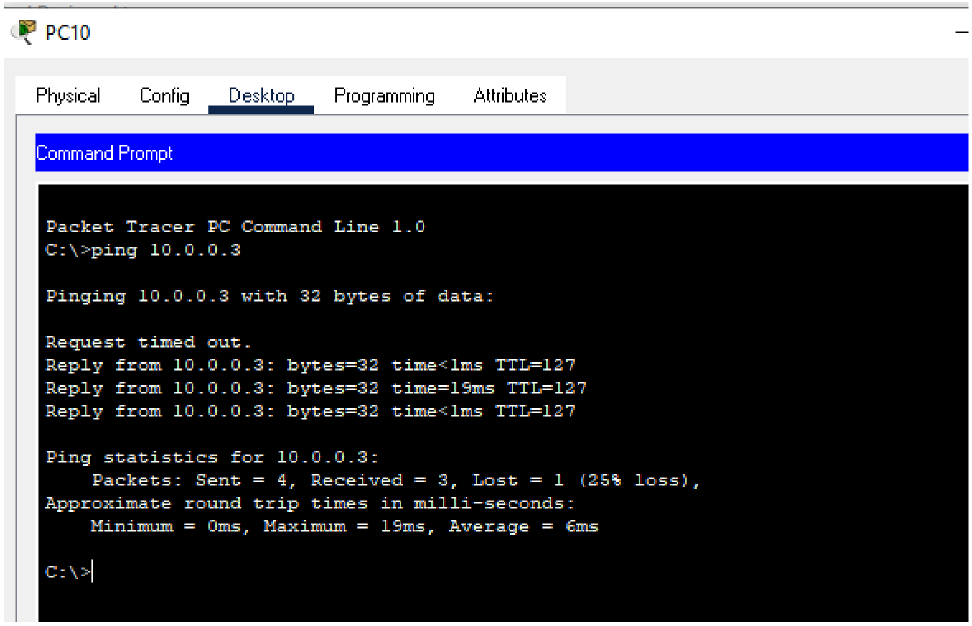
4.2 Switch CLI programing

We have done the basic configuration of switch after running config command become as under:

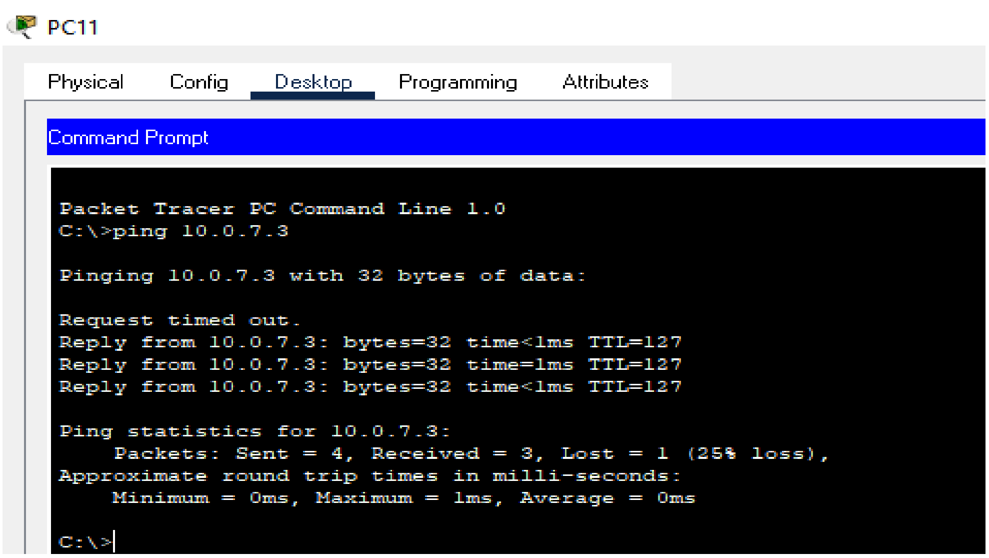
```
i

nterface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan 2
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 3
switchport mode trunk
!
interface FastEthernet0/4
 switchport access vlan 4
 switchport mode trunk
!
interface FastEthernet0/5
switchport access vlan 5
switchport mode trunk
!
interface FastEthernet0/6
switchport access vlan 4
switchport mode trunk
!
interface FastEthernet0/7
switchport access vlan 6
switchport mode trunk
!
interface FastEthernet0/8
switchport access vlan 7
 switchport mode trunk
!
interface FastEthernet0/9
 switchport access vlan 8
 switchport mode trunk
!
interface FastEthernet0/10
 switchport access vlan 9
 switchport mode trunk
```

4.3 Ping Result and connectivity :

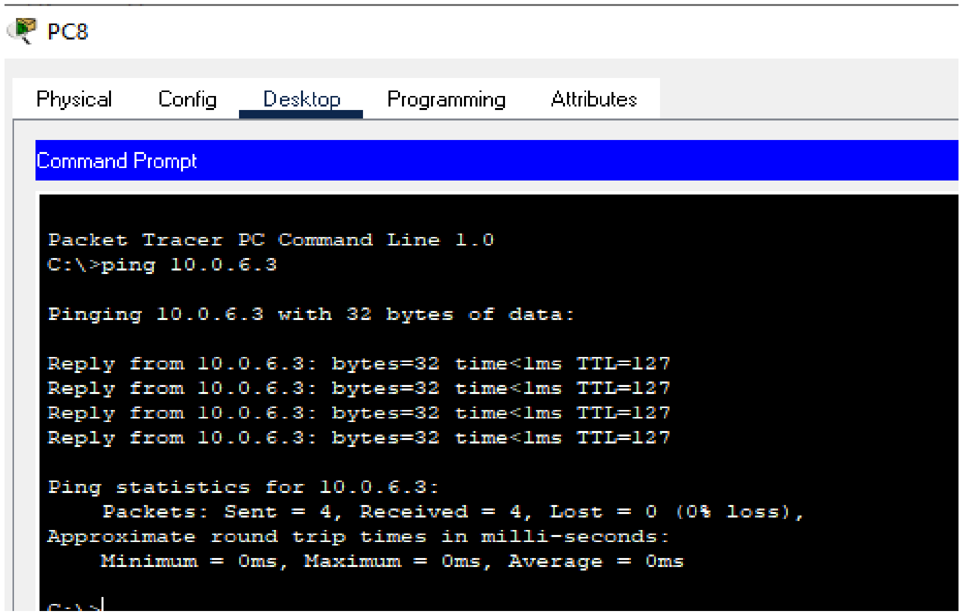
i. Ping Department 2 from department 3:



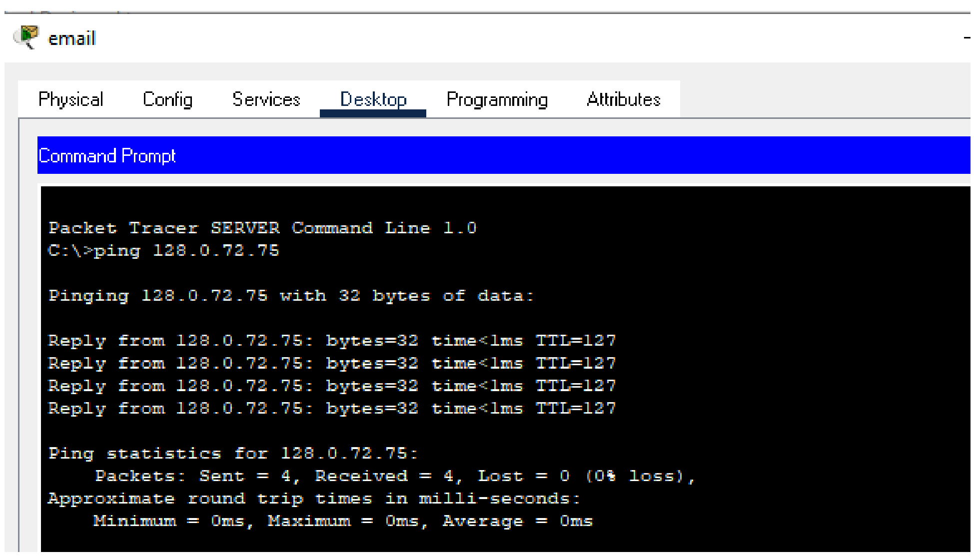
ii. Ping Department 5 from department 7:



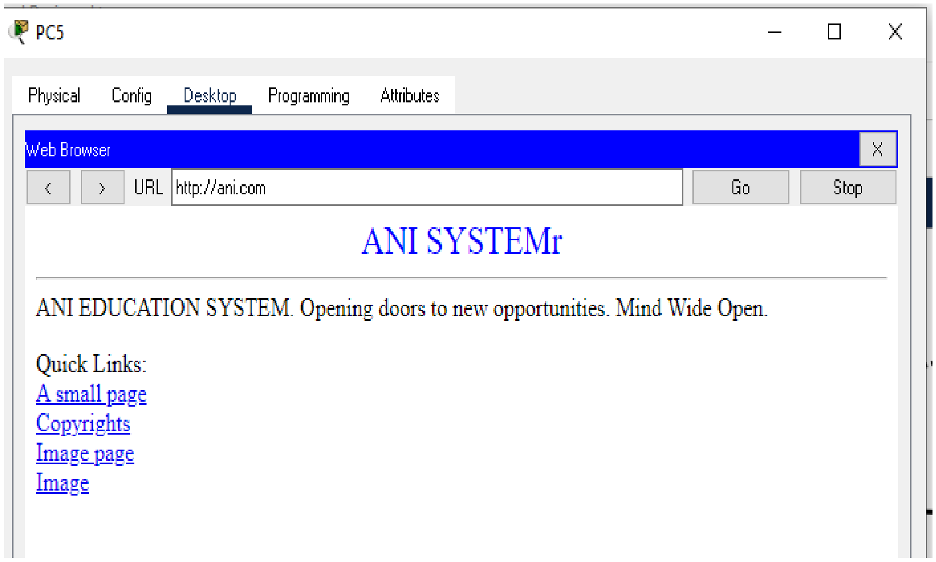
iii. Ping Department 6 from department 2:



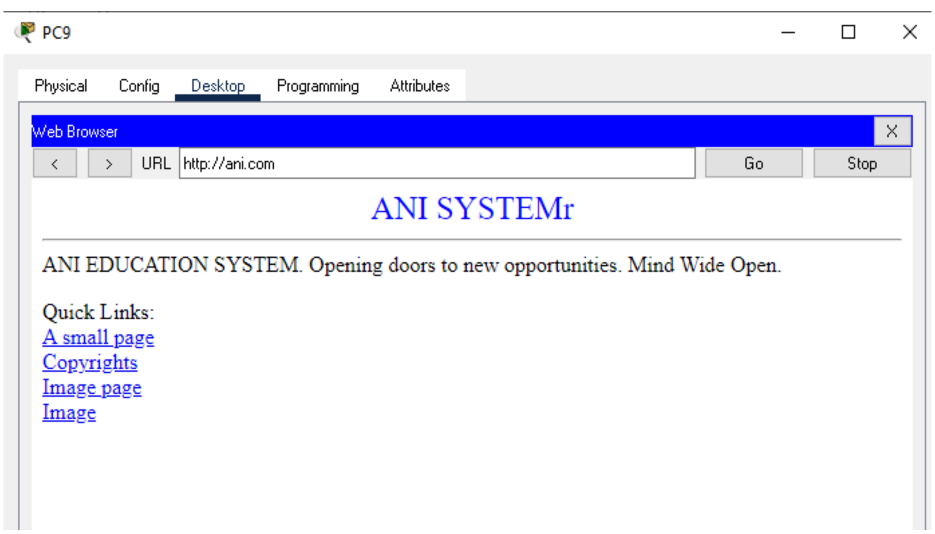
iv. Ping web server from the mail server:



v. **Excess website from department 1:**

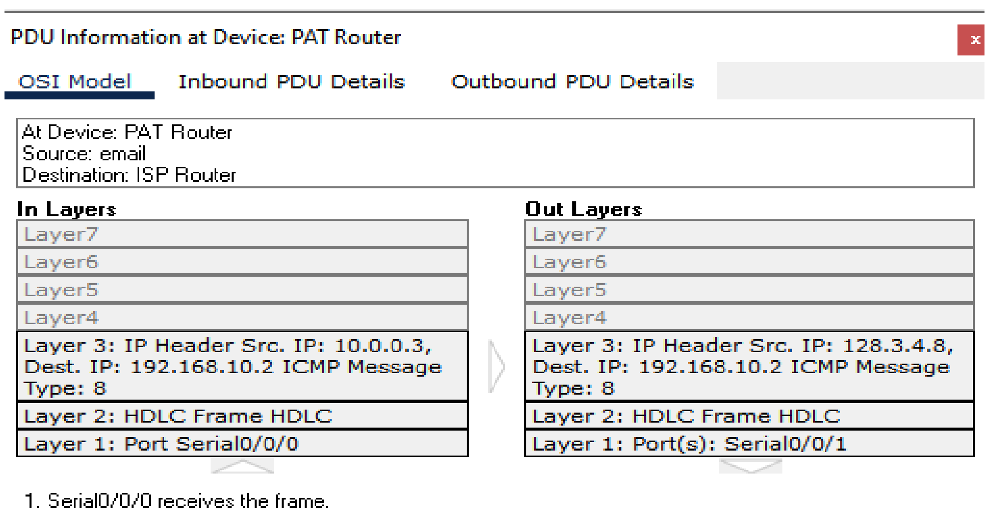


vi. **Excess website from the department 6:**



vii. Send mail from user pc1 to pc2:

viii. Excess ISP router from user 1 pc1 with public IP address:



Analysis:

We haven’t assigned 128.3.4.8 to any PC but the diagram is showing it as the source IP. This is definitely due to the PAT. The IP of all the host in the network are translated to the Public IP address.

5. Conclusion:

Network can be designed in many ways. Our design focused on least cost. That’s we have chosen the VLAN, that helped us to decrease the cost of the network. Using the second layer switch will also help to decrease the cost of the network. All of the requirements has been achieved in this lab. Beginning From the web server to the dynamic addressing has been met in this project.

References

[1] Online, "What is a virtual LAN (VLAN) and how does it work with my managed switch?," netgear, 28 11 2016. [Online]. Available: https://kb.netgear.com/21574/What-is-a-virtual-LAN-VLAN-and-how-does-it-work-with-my-managed-switch. [Accessed 20 June 2021].

[2] V. Rajaravivarma, "Virtual local area network technology and applications," *Proceedings The Twenty-Ninth Southeastern Symposium on System Theory*, pp. 49-52, 1997.

[3] Online, "802.1Q Encapsulation Explained," networklessions.com, 2017. [Online]. Available: https://networklessons.com/switching/802-1q-encapsulation-explained. [Accessed 20 June 2021].

[4] CloudFlare, "What is a subnet? | How subnetting works," CloudFlare, 2020. [Online]. Available: https://www.cloudflare.com/learning/network-layer/what-is-a-subnet/. [Accessed 20 June 2021].

[5] efficientip, "What is DHCP?," efficientip, 2020. [Online]. Available: https://www.efficientip.com/what-is-dhcp-and-why-is-it-important/. [Accessed 20 June 2021].

[6] Online, "Routing 101: Routing Algorithms," informit, 21 June 2002. [Online]. Available: https://www.informit.com/articles/article.aspx?p=27267. [Accessed 20 June 2021].

[7] Online, "Open Shortest Path First," Wikipedia.org, 10 June 2021. [Online]. Available: https://en.wikipedia.org/wiki/Open_Shortest_Path_First. [Accessed 20 June 2021].

[8] Online, "Understanding Layer 3 Subinterfaces," Juniper, 30 August 2018. [Online]. Available: https://www.juniper.net/documentation/en_US/junos/topics/concept/interfaces-layer3-subinterfaces-ex-series.html. [Accessed 20 June 2021].

[9] Online, "Network Address Translation (NAT) FAQ," cisco, 18 November 2020. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html. [Accessed 20 June 2021].

[10] Online "https://www.n-able.com/blog/vlan-trunking"

[11] Book "Computer Networking by Kurose Ross 8th Edition"