Building of a Network using Cisco Packet Tracer

Ajileye Jemimah
Department of Computer Science
Tuskegee University
Tuskegee, AL, USA.
jajileye1490@tuskegee.edu

Sameeruddin Mohammed
Department of Computer Science
Tuskegee University
Tuskegee, AL, USA.
smohammed8703@tuskegee.edu

ABSTRACT

Given the network address (192.168.1.0/16) by our Internet Service Provider, this paper highlights how to build a network for a small organization, taking into accounts certain requirements that must be met to please the organization. We found the subnet mask, usable IP addresses and the broadcast address for each department on each floor. Devices such as Printers, PCs, receive IP addresses automatically through the Dynamic Host Configuration Protocol and we configured a DNS, web server, email server and file server for users (let's say the number of hosts/users in each department is 150) and it is being managed in the IT department. OSPF routing protocol is configured to share routing information and every department has its own separate VLANs while mapping is used for Network Address Translation (NAT). The computer in the IT department is used to enable remote SSH login. After all configurations and set up, the organization can fully utilize all resources as requested.

Keywords— SSH, VLAN, DHCP, IP, OSPF, NAT.

I. Introduction

Every successful firm that hopes to prosper in the cutthroat market sector must have a strong network infrastructure since it will operate as a conduit for communication between the company and its customers. IT has made business easier, improved performance and flexibility, raised digital awareness, automated services, and many other benefits, IT infrastructure will now determine whether your company succeeds or fails. Consequently, before network infrastructure is put into service, it must be carefully planned, built, executed, and tested while considering all recommended network design principles.

II. DESIGN

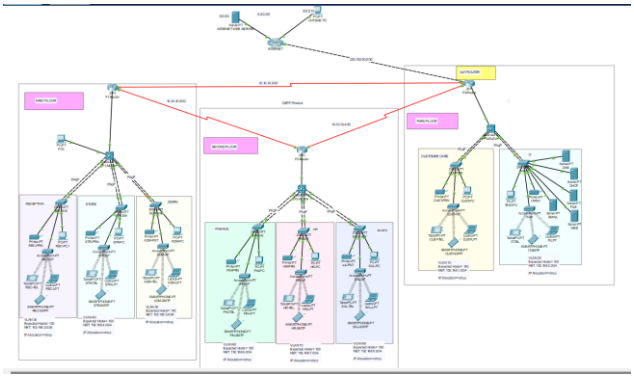
In this case, we want to create a network for a small organization which would consist of 3 floors (8 departments) and enable communication as well as the sharing of network resources and services between them. This network would require high performance, increased redundancy to limit the chances of any sort of failure and increased security to secure the organizations network from outside intrusions and possible threats.

IP Addressing

The table below outlines the network's IP planning:

No.	Devices	Network Address & Subnet Mask	Usable Addresses	Broadcast Address
1	INTERNET Zone	8.0.0.0/8	8.0.0.1 to 8.255.255.254	8.255.255.255
2	INTERNET to F3-Router	200.100.50.0/30	200.100.50.1 and 200.100.50.2	200.100.50.3
3	F1-Router to F2-Router	10.10.10.8/30	10.10.10.9 and 10.10.10.10	10.10.10.11
4	F1-Router to F3-Router	10.10.10.0/30	10.10.10.1 and 10.10.10.2	10.10.10.3
5	F3-Router to F2-Router	10.10.10.4/30	10.10.10.5 and 10.10.10.6	10.10.10.7
6	F1-Reception	192.168.3.0/24	192.168.3.1 to 192.168.3.254	192.168.3.255
7	F1-Stores	192.168.4.0/24	192.168.4.1 to 192.168.4.254	192.168.4.255
8	F1-Admin	192.168.5.0/24	192.168.5.1 to 192.168.5.254	192.168.5.255
9	F2-FIN	192.168.6.0/24	192.168.6.1 to 192.168.6.254	192.168.6.255
10	F2-HR	192.168.7.0/24	192.168.7.1 to 192.168.7.254	192.168.7.255
11	F2-SALES	192.168.8.0/24	192.168.8.1 to 192.168.8.254	192.168.8.255
12	F3-CUSTOMER	192.168.1.0/24	192.168.1.1 to 192.168.1.254	192.168.1.255
12	F3-IT	192.168.2.0/24	192.168.2.1 to 192.168.2.254	192.168.2.255

III. IMPLEMENTATION



a) The Layered Hierarchical Network Design

This hierarchical model is fostered together with a redundant topology that includes all nodes cooperating to distribute data amongst each other, and while connecting the end devices, there is star topology that includes all nodes connecting to a central device. Bus topology is also seen from the access switches to multilayer switches and finally to the routers.

b) Redundancy and Scalability in the Network

In this network system, redundancy was implemented using EtherChannel and multiple links between the devices i.e. between the access and multilayer switches as shown in the topology. Future expansion is also a very vital design; therefore, the network was designed in such a way that more modules can be added without affecting the network's performance.

c) Security in the Company Network

Security is a very important aspect in every network and in this network, the following security measures were put in; only authorized users have access because all the devices have passwords (for line console, VTY, and privilege EXEC), SSH for remote login, the Virtual Local Area Network (VLAN) provides segmentation and security.

NAT also helps prevent outside computers from directly accessing your private device.

Access Control Lists have been used in two aspects; one is to filter who can remotely access the devices via SSH and another is used to specify the subnet to be translated during the NAT process.

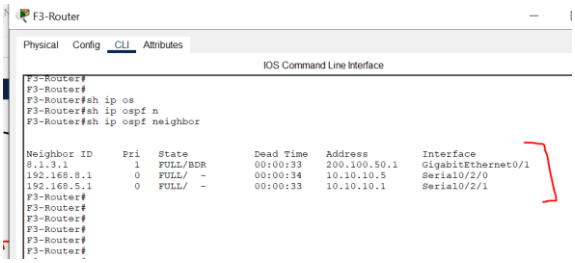
d)Basic Device Configurations or Settings

In the network, we have carried out basic device settings using the CLI and configured settings such as the hostnames, banner messages, line console password, privilege mode password, line VTY password and SSH,

username and password, domain name, disabling IP domain lookup, exec-timeout and logging synchronous, and finally, encrypted all the configured passwords.
These were implemented to provide device entry security and additional importance features in every devices as show in the attached figure;
Using the following commands in privilege-exec mode: *show start or show startup-config*

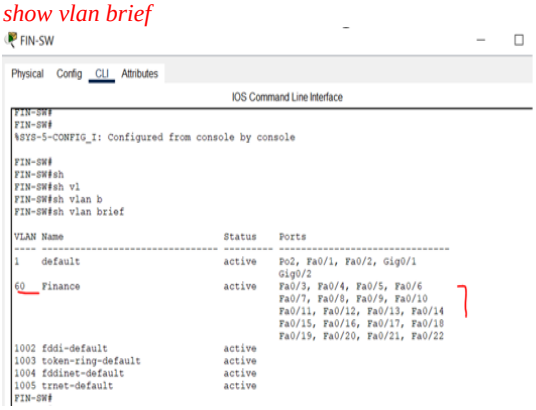
e) OSPF Routing Protocol Configuration

To advertise routes in the network, a dynamic routing and link-state protocol called OSPF was employed during configuration to create an algorithm for forwarding traffic based on the created routing table. During this configuration, OSPF was applied in the routers to advertise the directly attached networks.
Using the following commands in privilege-exec mode: *show IP ospf neighbor*



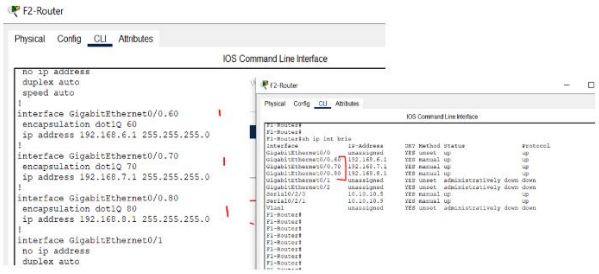
f) VLAN Configuration

For improved security, segmentation, and easy maintenance, each department in every branch in the network is in a different VLAN and assigned to a different subnet. Several VLANs were implemented for example VLANs 10, 20, 30, 40, 50, 60, 70, and 80.
These VLANs were implemented on both access and multilayer switches, also, each port was assigned a respective VLAN ID. This is shown below;
Using the following commands in privilege-exec mode: *show vlan brief*



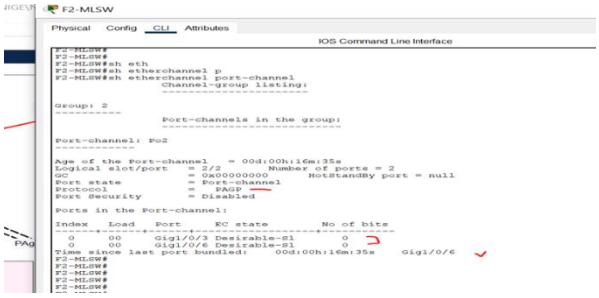
g) Inter-VLAN Routing

By default, devices in different VLANs do not communicate and thus we have to implement protocols to help them communicate. During the configuration, we used Router-on-a-Stick (ROAS) as the protocol for inter-VLAN routing, in which the technique was applied to all the routers by creating sub-interfaces and assigning them IP addresses and encapsulation VLAN ID to enhance the process.
Using the following commands in privilege-exec mode: *show IP interface brief or show start*



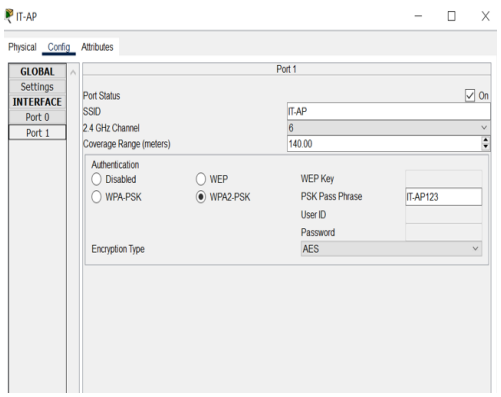
h) EtherChannel or Link Aggregation Configuration

Link aggregation technique allows multiple switch links to combine into one logical channel and act as a single channel of forwarding data. Cisco states that a maximum of 8 links can be aggregated to form a single logical link. This allows load sharing of traffic among the links in the channel as well as redundancy if one or more links in the channel fail. Through the use of this technology, the network will have no wastage of bandwidth, no loops, and there will be redundancy. In the topology, we used PAgP protocol (Port Aggregation Protocol) to create the EtherChannel. This is shown below;
Using the following commands in privilege-exec mode: *show etherchannel port-channel*



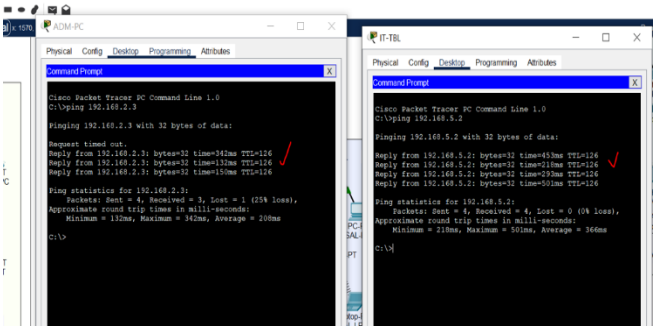
i) Wireless Network using Access Points

In the network, departments were equipped with Wireless Access Points that were used to propagate the signals to the hosts.



j) Communication in the Network

After all the good design and configurations, the network is fully functional and of high performance. All hosts in the network can communicate with each other. Sending a ping request from one PC is seen receiving a ping reply from the other PC.



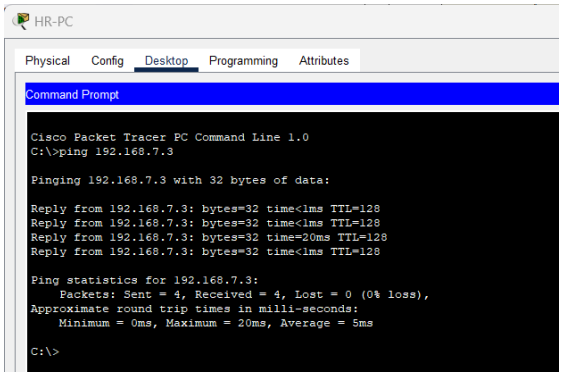
IV. RESULTS

Testing cases in this network, we have:

a) The printer is correctly shared and accessible within the local area network (LAN)

The picture below shows the result of the PC in the HR department trying to reach the printer in the HR department.

Using the command**: ping 192.168.7.3(IP address of the HR printer)**

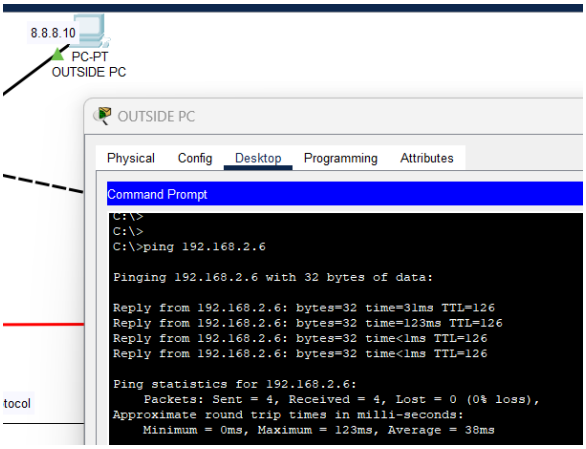


We record 0% loss of packets between the pc and printer.

(b) Any PC, whether it is located inside or outside the organization, can reach the webserver or website

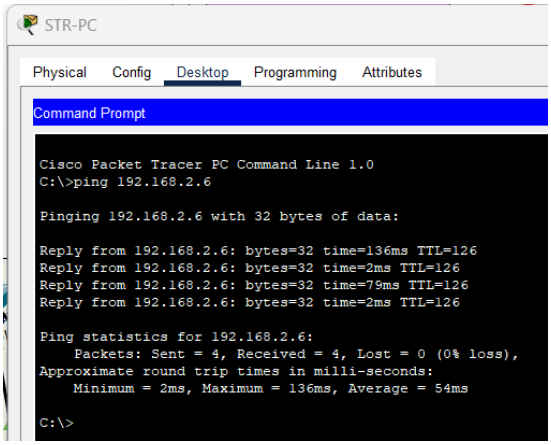
The picture below shows the result of a PC **outside the organization** reaching the webserver successfully**.**

Using the command**: ping 192.168.2.6** (IP address of the web server)



The picture below shows the result of **a PC inside the organization** reaching the webserver successfully**.**

Using the command**: ping 192.168.2.6 (IP address of the web server)**



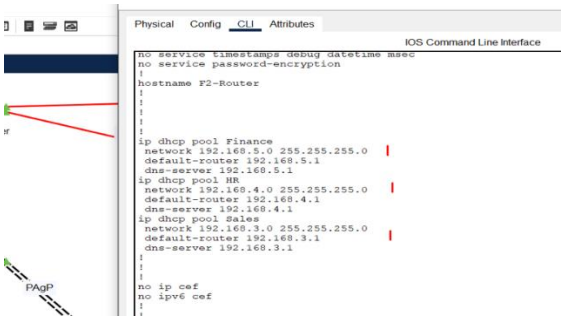
We record 0% loss of packets between both pcs and the web server.

d) A computer can obtain its IP address through DHCP

All the host devices in the network except the server are allocated IPv4 addresses dynamically. The host devices are allocated IPv4 addresses dynamically by the gateway device located at each department.

Each site was equipped with a DHCP server as shown below:

Using the following commands in privilege-exec mode: *show start*



e) Network address translation (NAT) is operational

The protection of private network resources is protected by NAT while connecting them to the Internet. In this case, NAT was deployed on F3-Router which enables connection to the internet while allowing multiple devices on a local area network (LAN) to

share one public IP address, which improves security and cost reduction.

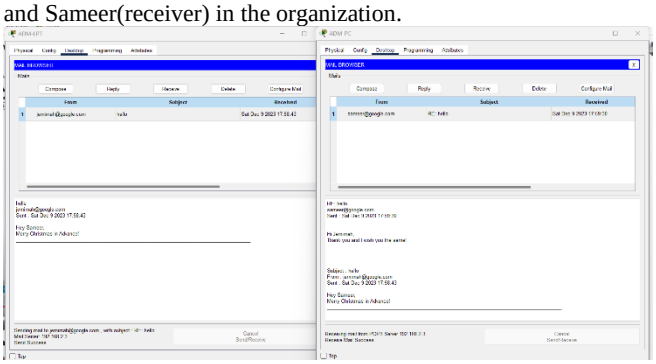
Using the following commands in privilege-exec mode: ***show start or show IP nat translations***

```
F3-Router#
F3-Router#
F3-Router#
F3-Router#
F3-Router#
F3-Router#sh ip nat
F3-Router#sh ip nat  tr
F3-Router#sh ip nat  translations
F3-Router#sh ip nat  translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.100.50.2:1    192.168.7.4:1      8.8.8.8:1          8.8.8.8:1
icmp 200.100.50.2:3    192.168.7.4:3      8.8.8.8:3          8.8.8.8:3
icmp 200.100.50.2:4    192.168.7.4:4      8.8.8.8:4          8.8.8.8:4

F3-Router#sh ip nat  translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.100.50.2:1    192.168.7.4:1      8.8.8.8:1          8.8.8.8:1
icmp 200.100.50.2:3    192.168.7.4:3      8.8.8.8:3          8.8.8.8:3
icmp 200.100.50.2:4    192.168.7.4:4      8.8.8.8:4          8.8.8.8:4

F3-Router#sh ip nat  translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.100.50.2:1024 192.168.6.4:3      8.8.8.8:3          8.8.8.8:1024
icmp 200.100.50.2:1025 192.168.6.4:4      8.8.8.8:4          8.8.8.8:1025
icmp 200.100.50.2:1    192.168.7.4:1      8.8.8.8:1          8.8.8.8:1
icmp 200.100.50.2:2    192.168.6.4:2      8.8.8.10:2         8.8.8.10:2
icmp 200.100.50.2:3    192.168.7.4:3      8.8.8.8:3          8.8.8.8:3
icmp 200.100.50.2:4    192.168.7.4:4      8.8.8.8:4          8.8.8.8:4

F3-Router#
```

(f) Email functions both internally and externally for the organization

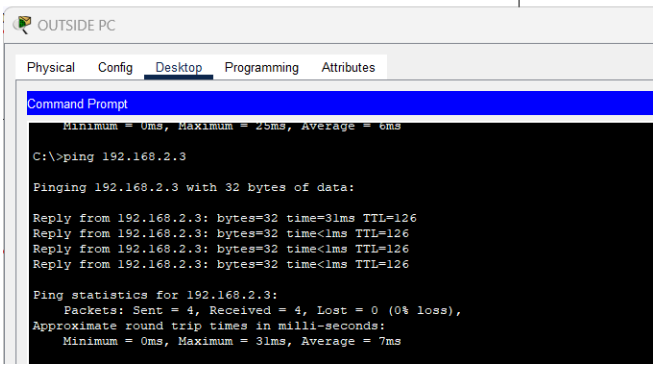
Internally

This is a successful exchange of email between Jemimah(sender) and Sameer(receiver) in the organization.



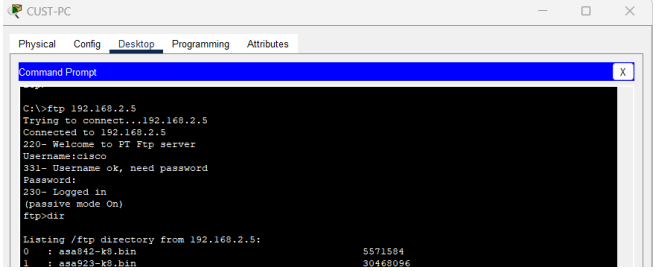
Externally

This shows that the PC outside the organization can successfully reach the email server and we verified this by using the ping command: ping 192.168.2.3



(g) The organization has a working file server.

This shows that the organization has a working file server as we can see that the PC in the customer care department successfully connected to the file server's IP address.



V. CONCLUSION

In summary, a good network should be able to possess certain attributes e.g. good performance, high scalability, better security, increased redundancy, integrated during its design and implementation. Our network meets all the above criteria and therefore, the organization would be very pleased with what we have been able to come up with. Subsequently, any maintenance and preventive measures can be taken into consideration later.