Table of Contents

[Aim 1](#_Toc119277243)

[Case Problem 1](#_Toc119277244)

[Requirements 1](#_Toc119277245)

[Network Topology 3](#_Toc119277246)

[The Access Level 3](#_Toc119277247)

[The Distribution Level 3](#_Toc119277248)

[The Core Level 3](#_Toc119277249)

[ISPs 3](#_Toc119277250)

[Configuration 5](#_Toc119277251)

[Basic Configurations 5](#_Toc119277252)

[VLAN Setup and Access and Trunk Port Configuration 6](#_Toc119277253)

[IP addressing and Subnetting 8](#_Toc119277254)

[OSPF Configuration 11](#_Toc119277255)

[Static IP Allocation of Server Nodes 11](#_Toc119277256)

[DHCP Configuration 11](#_Toc119277257)

[DNS Configuration 13](#_Toc119277258)

[Inter-VLAN routing 13](#_Toc119277259)

[Access Point Configuration 13](#_Toc119277260)

[NAT Configuration 15](#_Toc119277261)

[Testing and Results 17](#_Toc119277262)

[Login Security 17](#_Toc119277263)

[Dynamic IP Acquisition via DHCP Server 17](#_Toc119277264)

[Intra-VLAN Communication 18](#_Toc119277265)

[Inter-VLAN Communication 18](#_Toc119277266)

[SSH 19](#_Toc119277267)

[NAT 19](#_Toc119277268)

[Conclusion 20](#_Toc119277269)

# Table of Figures

[Figure 1: Overall logical topology for the network 4](#_Toc119277469)

[Figure 2: Basic configurations (MOTD, concole password, vty password, password encryption) 5](#_Toc119277470)

[Figure 3: Setting up hostname and SSH 6](#_Toc119277471)

[Figure 4: Setting up VLAN, configuring trunk ports, and access mode ports 7](#_Toc119277472)

[Figure 5: Configuring L2 switch ports connected to routers not to be swithports 8](#_Toc119277473)

[Figure 6: Configuring IP addresses for the core-router-facing ports of a distribution-layer switch 10](#_Toc119277474)

[Figure 7: Assigning IP address on ISP 1 10](#_Toc119277475)

[Figure 8: OSPF configuration for a distribution-level switch 11](#_Toc119277476)

[Figure 9: Static IP allocation of the DHCP server 12](#_Toc119277477)

[Figure 10: DHCP configuration and address pools 12](#_Toc119277478)

[Figure 11: Configuring the DNS server 13](#_Toc119277479)

[Figure 12: Enabling inter-VLAN routing 14](#_Toc119277480)

[Figure 13: Setting up AP credentials 15](#_Toc119277481)

[Figure 14: NAT configuration 15](#_Toc119277482)

[Figure 15: Setting the default routes of the distribution-level switches 16](#_Toc119277483)

[Figure 16: Password request to access console and privileges 17](#_Toc119277484)

[Figure 17: Dynamic IP allocation of a PC on the Research & Development deparment 17](#_Toc119277485)

[Figure 18: Intra-VLAN communication (Devices within Finance & Accounts department) 18](#_Toc119277486)

[Figure 19: Inter-VLAN communication 18](#_Toc119277487)

[Figure 20: SSH into a core-level router from an Admin PC 19](#_Toc119277488)

[Figure 21: Pinging an ISP router from a Sales & Marketing PC 19](#_Toc119277489)

[Figure 22: NAT entries on core router 2 20](#_Toc119277490)

# List of Tables

[Table 1: Staff and department distribution in new premises 1](#_Toc119277292)

[Table 2: Allocation of VLANs to departments 6](#_Toc119277293)

[Table 3: IP addressing and subnetting design 9](#_Toc119277294)

[Table 4: Static IP address allocation of devices in the server room 11](#_Toc119277295)

# Aim

The aim of this project is to design, simulate and test a network. Cisco Packet Tracer shall be software used to simulate and test the network.

# Case Problem

Noble Pharma Solutions Ltd is a fictitious pharmaceutical company producing a wide range of drugs. The company is currently relocating to new a headquarters in Doha. The new premises is going to have the three buildings, with different departments located within as shown in table 1.

|  |  |  |
| --- | --- | --- |
| **Distribution of Departments** | | |
| **Building** | **Department** | **Staff Number** |
| **Building 1** | Manufacturing | 105 |
| Research & Development | 30 |
| Server Room | 12 |
| **Building 2** | Sales & Marketing | 100 |
| Human Resources & Logistics | 24 |
| **Building 3** | Finance & Accounts | 16 |
| Administration & PR | 24 |

Table 1: Staff and department distribution in new premises

Your team has been tasked to create the new network for Noble Pharma Solutions Ltd. It is expected that the current and future needs of the business shall be addressed in this new network.

# Requirements

The network is supposed to have the following requirements:

* The network is expected to use a hierarchical model
* The network should be connected to at least two ISPs for redundancy
* The company network is connected to the static public IP addresses: 78.142.100.0/30, 78.142.100.4/30, 78.142.100.8/30, and 78.142.100.12/30.
* The base network is supposed to have an IP address of 192.168.100.0
* Each department should be in a different subnet and different VLAN
* Each department should provide access to wireless networks for its users
* IP addresses should be allocated dynamically using DHCP
* Server room devices are to be allocated IP addresses statically
* OSPF routing should be configured on the routers and layer 3 switches
* Users in different departments should be able to communicate with each other using the multilayer switches configured for inter-VLAN routing
* NAT should be configured to use the relevant IPv4 router address. Necessary ACL rules should also be configured.

Besides these, the following basic configurations should be enabled:

* The hostname should be configured for the core routers
* The message of the day banner should be configured
* Console and vty passwords should be configured
* Password encryption services should be enabled
* Users should be able to remotely access the network using SSH

# Network Topology

The overall logical topology for the new network is as shown in figure 1. A hierarchical model was employed for this network. In this model, the network could be divided into access, distribution, and core levels.

## The Access Level

Each department was served by a single access-level switch (2960). Seven access-level switches serving the seven departments of the company were included. For simulation purposes, a department was taken to contain the following devices:

* Printer – served by the switch
* PC – served by the switch
* Access Point (AP-APT) – served by the switch
* Laptop – served by the access point
* Smartphone – served by the access point

## The Distribution Level

The distribution level was comprised of two switches (3650-24PS). Each distribution-level switch was connected to each access-level switch for a department. This way, each access-level switch had a connection to two distribution-level switches. This design was made so as to provide redundancy in case of link or switch failure.

## The Core Level

The core level was comprised of two routers (2911). Each core router was connected to each distribution-level switch. This way, each distribution-level switch had a connection to two core-level routers. This design was made to provide redundancy in case of link or router failure.

## ISPs

Two routers were chosen to simulate the ISP routers. A serial connection was chosen between the ISP routers and the core-level routers. Each core-level router was connected to two ISP routers. This way, redundancy was improved for the network in case of link or ISP router failure.

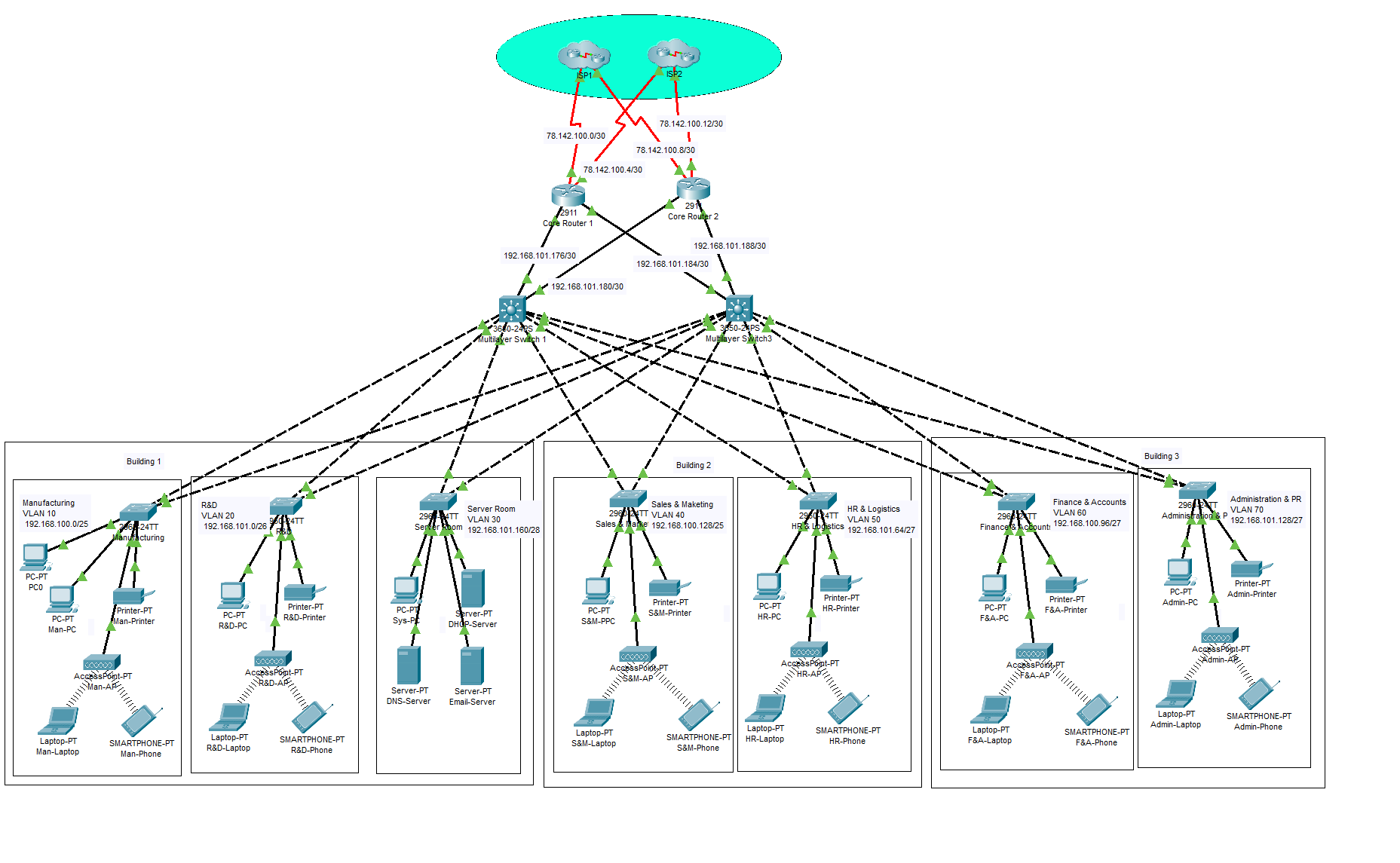


Figure 1: Overall logical topology for the network

# Configuration

## Basic Configurations

For each access-level switch, distribution-level switch, and core router, the following configurations were made:

1. **Message of the day (MOTD) banner –** The MOTD banner message “No Unauthorized Access” was set
2. **Console password –** the console password “cisco” was set
3. **Vty password** – the vty password “cisco” was set
4. **Password encryption** – password encryption was enabled.

A sample screenshot for such configuration in progress for the Manufacturing department switch is shown in figure 2.

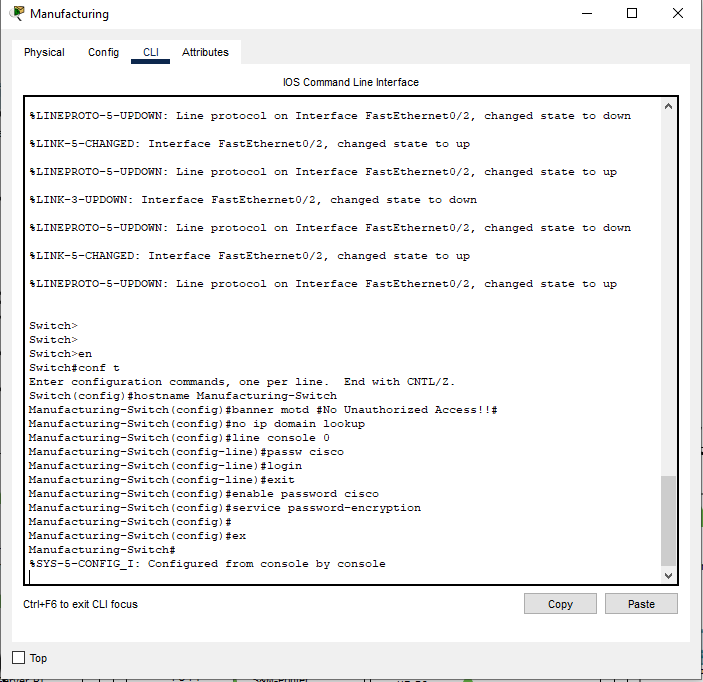


Figure 2: Basic configurations (MOTD, concole password, vty password, password encryption)

The hostname on the switches and routers were configure to be “noblepharma.com”. Crypto keys were generated for the RSA algorithm, and SSH correspondingly enabled as shown in figure 3.

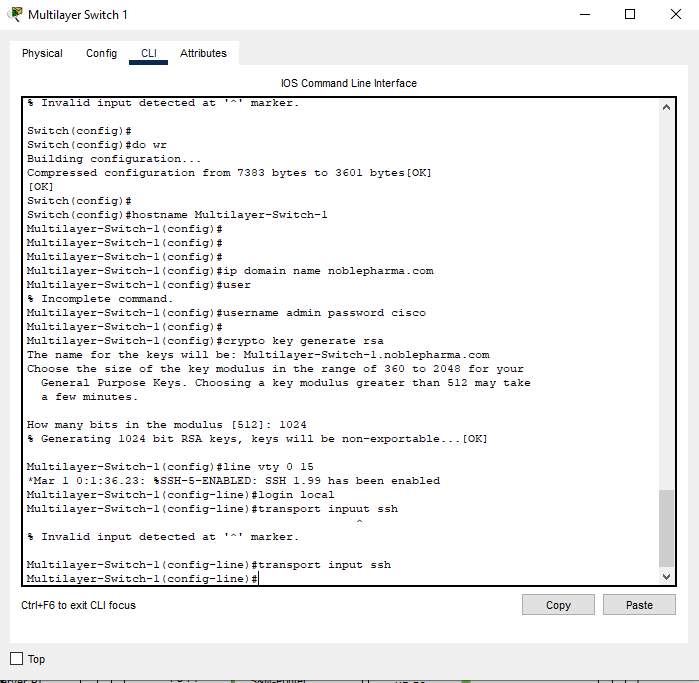


Figure 3: Setting up hostname and SSH

## VLAN Setup and Access and Trunk Port Configuration

It was desired that the departments on the network be on separate VLANs. The VLAN assignment to the departments was allocated as shown in table 2.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Dept** | Manufacturing | Research & Development | Server | Sales & Marketing | HR & Logistics | Finance & Accounts | Admin & PR |
| **VLAN** | VLAN 10 | VLAN 20 | VLAN 30 | VLAN 40 | VLAN 50 | VLAN 60 | VLAN 70 |

Table 2: Allocation of VLANs to departments

For access-level switches, the two interfaces connected to the distribution-level (fa0/1-2) switches were configured to be trunks. The remaining interfaces connected to the end nodes (fa0/3-24) were configured to operate in the access mode. A VLAN (named TrapVLAN) was configured to cater to the interfaces that were not to be in operation for the access level switches (gig0/1-2). A sample of these steps in operation for the access-level switch of the manufacturing department is shown in figure 4.

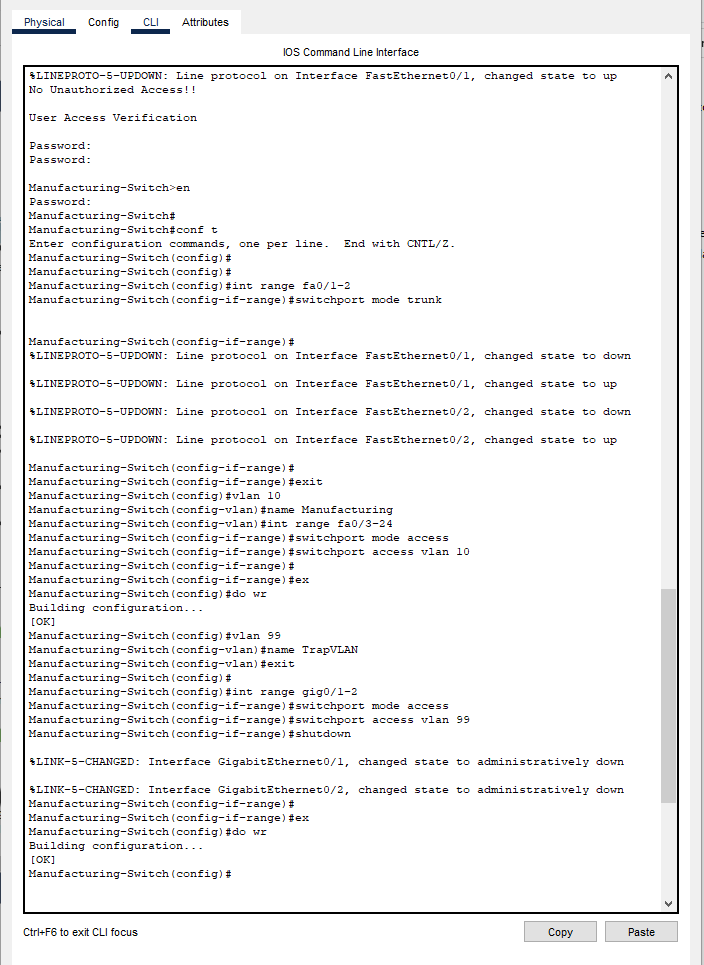


Figure 4: Setting up VLAN, configuring trunk ports, and access mode ports

The ports of the distribution-layer switches (gig1/0/1-2) connected to the core-level switches were configured not to be switchports as shown in figure 5.

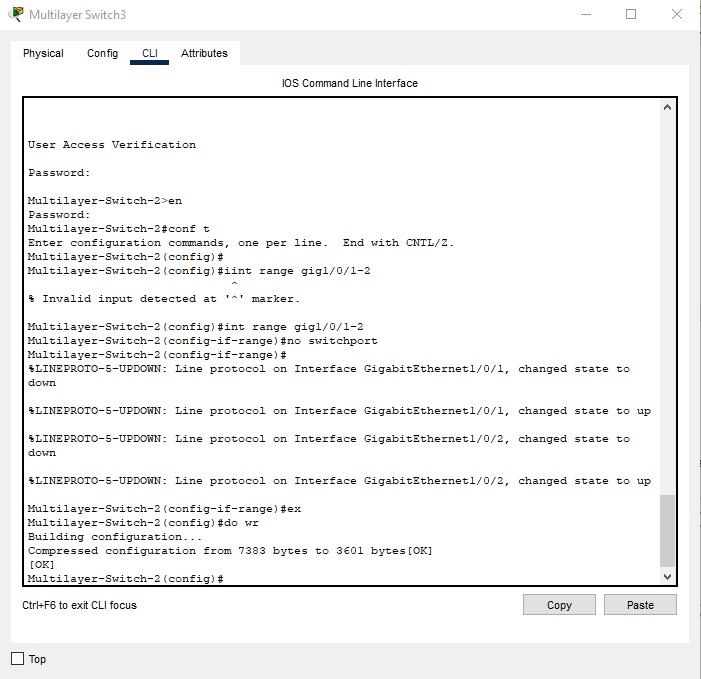


Figure 5: Configuring L2 switch ports connected to routers not to be swithports

## IP addressing and Subnetting

A base IP address of 192.168.100.0 was desired for this network as specified in the specifications. Based on the staffing requirements of each department that was provided in table 1, IP addressing and subnetting were to be designed as per the design provided in table 3.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Department/ Device Ports** | **Network Address** | **Subnet Mask** | **Host Address Range** | **Broadcast Address** |
| **Building 1** | | | | |
| Manufacturing | 192.168.100.0 | 255.255.255.128 | 192.168.100.1 –  192.168.100.126 | 192.168.100.127 |
| R&D | 192.168.101.0 | 255.255.255.192 | 192.168.101.1-  192.168.101.62 | 192.168.101.63 |
| Server room | 192.168.101.160 | 255.255.255.240 | 192.168.101.161 –  192.168.101.174 | 192.168.101.175 |
| **Building 2** | | | | |
| Sales & Marketing | 192.168.100.128 | 255.255.255.128 | 192.168.100.129 –  192.168.100.254 | 192.168.100.255 |
| Human Resource & logistics | 192.168.101.64 | 255.255.255.224 | 192.168.101.65 –  192.168.101.94 | 192.168.101.95 |
| **Building 3** | | | | |
| Finance & Accounts | 192.168.101.96 | 255.255.255.224 | 192.168.101.97 –  192.168.101.126 | 192.168.101.127 |
| Administration & PR | 192.168.101.128 | 255.255.255.224 | 192.168.101.129 –  192.168.101.158 | 192.168.101.159 |
| **Interfaces** | | | | |
| R1 – MLSW1 | 192.168.101.176 | 255.255.255.252 | 192.168.101.177 –  192.168.101.178 | 192.168.101.179 |
| R1-MLSW2 | 192.168.101.180 | 255.255.255.252 | 192.168.101.181 –  192.168.101.182 | 192.168.101.183 |
| R2-MLSW1 | 192.168.101.184 | 255.255.255.252 | 192.168.101.185 –  192.168.101.186 | 192.168.101.187 |
| R2-MLSW2 | 192.168.101.188 | 255.255.255.252 | 192.168.101.189 –  192.168.101.190 | 192.168.101.191 |

Table 3: IP addressing and subnetting design

The manufacturing department had an address of 192.168.100.0/25. This allowed for 126 usable hosts to support the 105 staff. The Human Resource & Logistics department had an address of 192.168.100.128/25. This allowed for 126 usable hosts to support the 100 staff.

The Research & Development department had an address of 192.168.101.0/26. This allowed for 62 usable hosts to support the 30 staff members, with a provision of expansion seeing as this department was expected to grow. The Human Resources & Logistics, Finance & Accounts, and Administration & PR departments addresses of 192.168.101.64/27, 192.168.101.96/27, and 192.168.101.128/27 respectively. These allowed for 30 usable hosts each to support the staffing requirements in each department.

The subnet 255.255.255.252 was used when assigning IP addresses to the ports of the core-level switches to the distribution-layer switches. With this subnetting, 2 usable hosts were available, catering the IP of the particular interface of interest.

A sample of the assignment of IP addresses on the ports of the distribution-layer switches facing the core-level switches is shown in figure 6.

For simulation purposes, the IP addresses of the ISP were assigned as shown in figure 7. The IP address of ISP 1 was taken to be 78.142.100.2 while the IP of ISP 2 was taken to be 78.142.100.14.

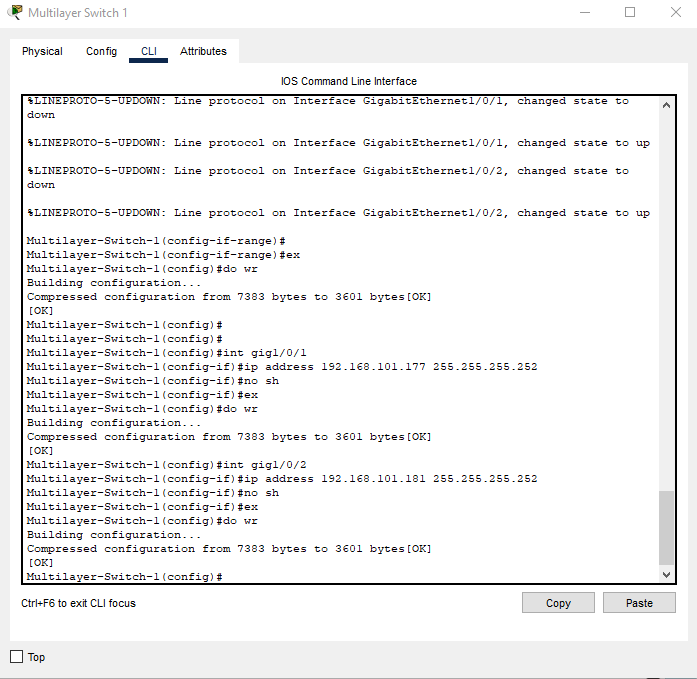


Figure 6: Configuring IP addresses for the core-router-facing ports of a distribution-layer switch

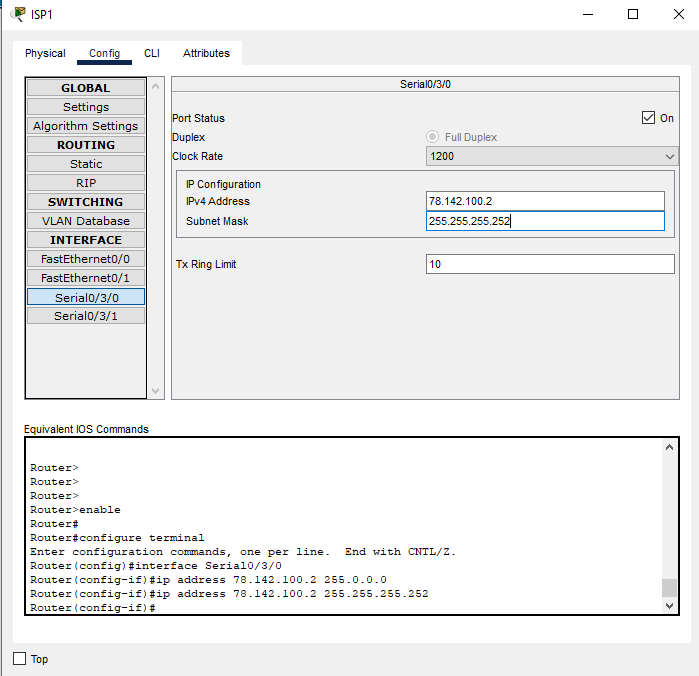


Figure 7: Assigning IP address on ISP 1

## OSPF Configuration

The OSPF protocol was configured for the distribution-level switches and core-level routers. The networks accessible by each switch and router were specified. A sample of this process for a distribution-layer switch is shown in figure 8.

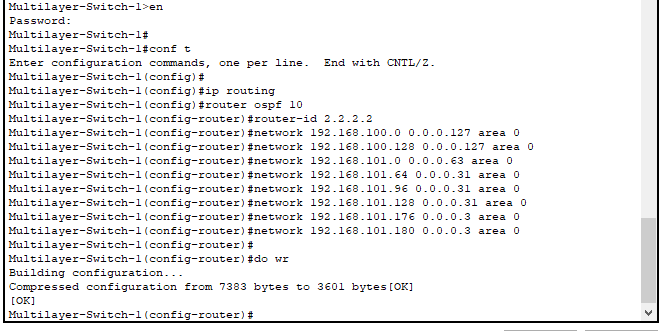


Figure 8: OSPF configuration for a distribution-level switch

In the sample shown in figure 9, the networks for each department, together with the network of the interfaces to the routers were configured to be published.

## Static IP Allocation of Server Nodes

The server nodes were allocated IP addresses statically as shown in table 4.

|  |  |  |  |
| --- | --- | --- | --- |
| Device | DHCP Server | DNS Server | PC |
| IP | 192.168.101.162 | 192.168.101.163 | 192.168.101.164 |

Table 4: Static IP address allocation of devices in the server room

A sample of the configuration of the IP address of the DHCP server is shown in figure 9.

## DHCP Configuration

It was desired that the access-level devices, save for the server end nodes, obtain IP addresses dynamically using the DHCP protocol. To achieve this, the DHCP service was enabled for the DHCP server. Address pools were then added for each department corresponding with the network’s IP and subnet masks. The address pools of the DHCP server are shown in figure 10.

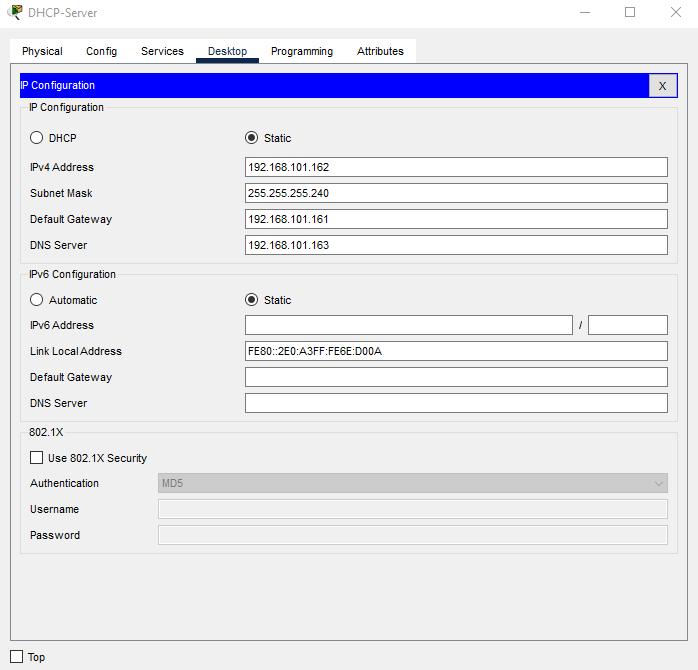


Figure 9: Static IP allocation of the DHCP server

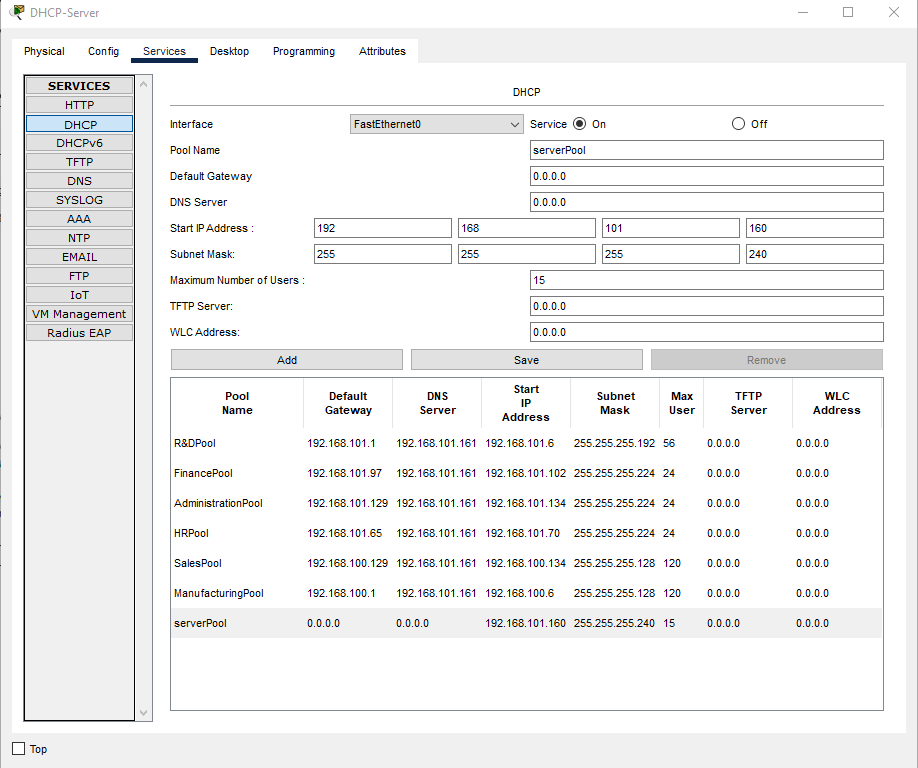


Figure 10: DHCP configuration and address pools

## DNS Configuration

To configure the DNS service, the service was simply turned on on the DNS server and an A record for [www.noblepharma.com](http://www.noblepharma.com) added as shown in figure 11.

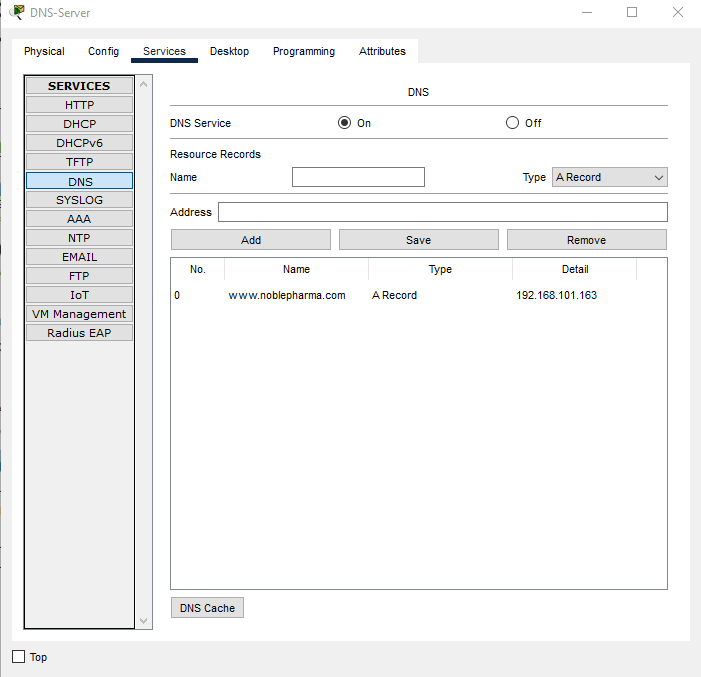


Figure 11: Configuring the DNS server

## Inter-VLAN routing

Inter-VLAN routing was enabled on the switches as shown in figure 12. The IP addresses and helper addresses of each VLAN were specified to achieve this.

## Access Point Configuration

The SSID of each AP was set, and the corresponding WPA2-PSK password was setup. A sample of the setup of the manufacturing AP is shown in figure 13.

The laptops and smartphones on each department were connected to their corresponding access points.

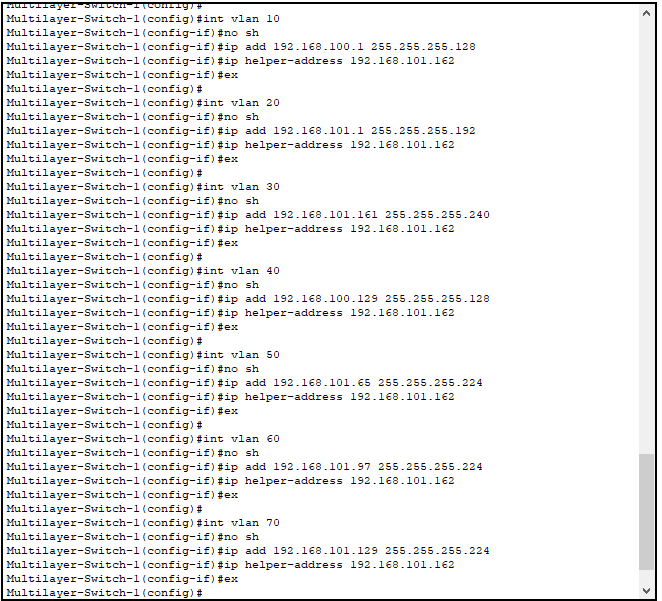


Figure 12: Enabling inter-VLAN routing

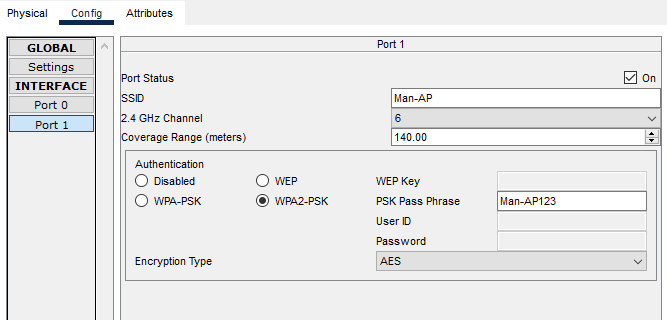


Figure 13: Setting up AP credentials

## NAT Configuration

NAT was to be used in the network to translate the IP addresses of the internal network to public forms and vice versa. A sample of this is shown in figure 14.

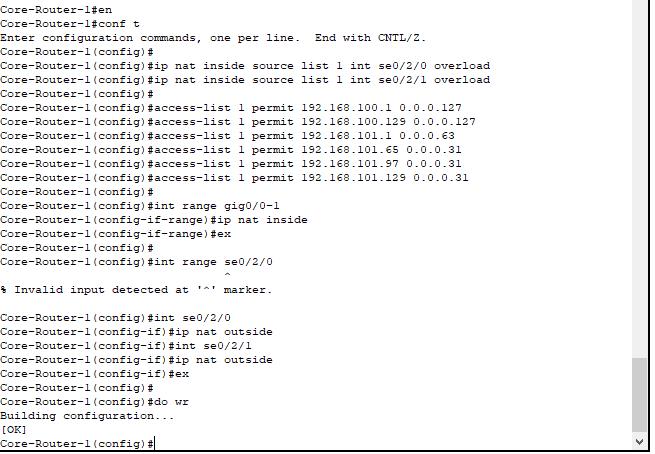


Figure 14: NAT configuration

The default routes where also specified for the distribution-layer switches to forward traffic to the core level switches.

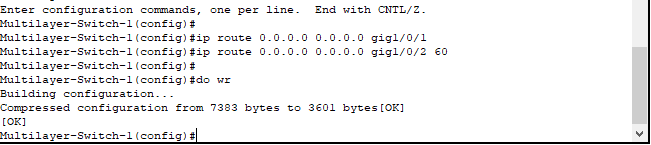


Figure 15: Setting the default routes of the distribution-level switches

# Testing and Results

## Login Security

A console password was requested when accessing a switch or router on the network. Access was rejected when an incorrect password was entered. Likewise, a vty password was requested to access the privileged mode of a switch or router. Access was rejected when the wrong password was provided. This request of passwords is as shown in figure 16.

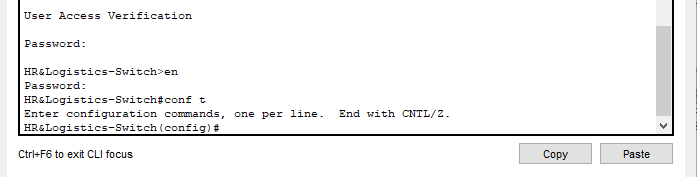


Figure 16: Password request to access console and privileges

## Dynamic IP Acquisition via DHCP Server

To request a for an IP address using DHCP, thee DHCP option was toggled for the IP Configuration section of the desktop tab on an end node. It was observed that an IP address within the devices network was availed from the IP addresses on the VLAN’s address pool. A sample acquisition for a PC on the Research & Development department is shown in figure 17. In this case, the IP 192.168.101.6 was assigned to the PC.

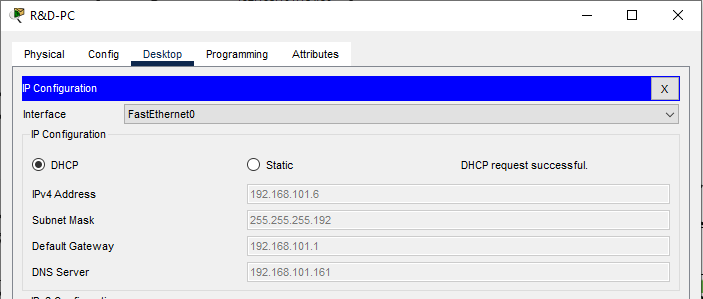


Figure 17: Dynamic IP allocation of a PC on the Research & Development deparment

## Intra-VLAN Communication

Intra-VLAN communication was noted to have been achieved in this network. A sample of a PC on the Finance & Accounts department pinging a Laptop IP 192.168.101.106 on the same network is shown in figure 18.

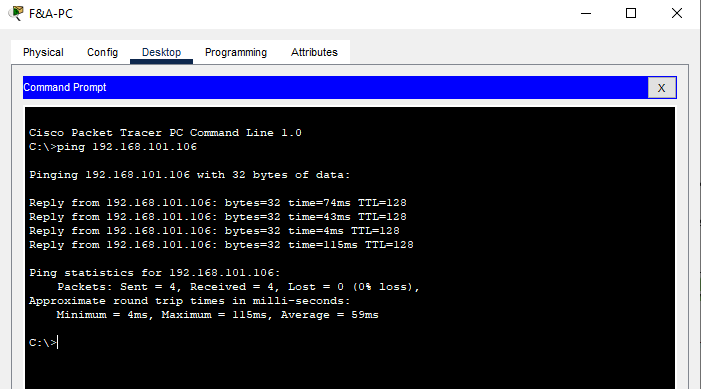


Figure 18: Intra-VLAN communication (Devices within Finance & Accounts department)

## Inter-VLAN Communication

Inter-VLAN communication was noted to have been achieved in this network. A sample of a PC on the Finance & Accounts department pinging a PC on the Sales & Marketing department of IP 192.168.100.139 is shown in figure 19.

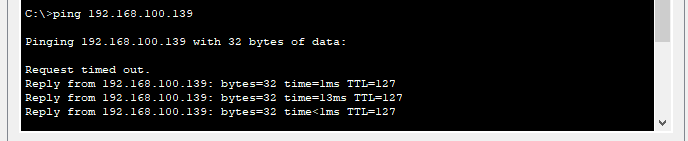


Figure 19: Inter-VLAN communication

## SSH

SSH was noted to have been achieved in this network. A sample of a PC on the Administration & PR department SSHing into the core router 1 is shown in figure 20. After successful authentication, normal operations could be remotely performed on the router. The MOTD banner was also displayed.

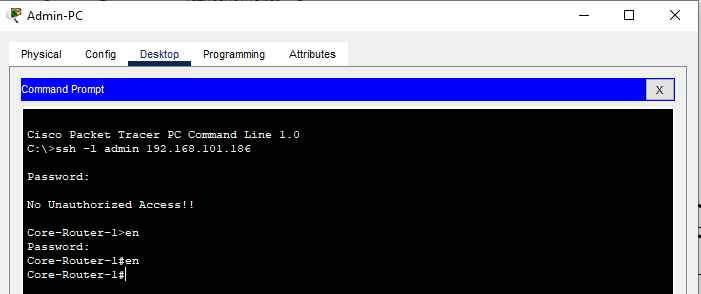


Figure 20: SSH into a core-level router from an Admin PC

## NAT

To test NAT, an ISP was pinged from a PC on the Sales & Marketing department. The ping was a success as shown in figure 21.

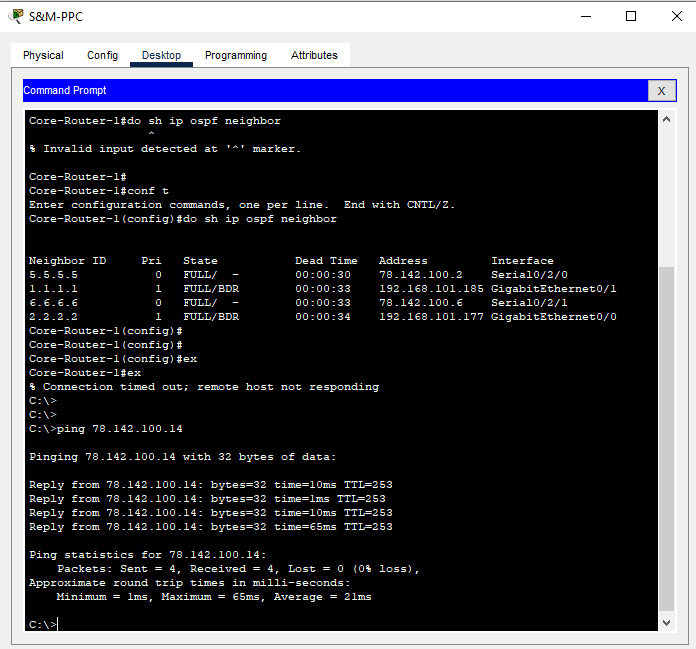


Figure 21: Pinging an ISP router from a Sales & Marketing PC

The NAT table of a core router was inspected. As expected, NAT entries were present on the router, showing the translations that took place as shown in figure 22.

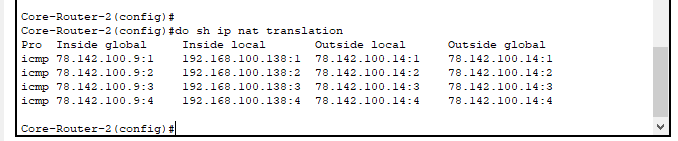


Figure 22: NAT entries on core router 2

# Conclusion

In this project, a case of a fictitious pharmaceutical company needing a network design was investigated. Cisco Packet Tracer was chosen to be the software for simulating the network. A hierarchical model was used in this network. Basic configurations such as console and vty passwords, password encryption, and MOTD were implemented. Each department was allocated a VLAN. The IP addresses of each VLAN, and L1 and L2 were mapped. The OSPF protocol was selected for the network. Static IP addresses were successfully assigned to the devices on the server room. DHCP was enabled successfully, allowing devices on the access layer to dynamically acquire IP addresses. DNS services were configured on a DNS server. Inter-VLAN routing was enabled allowing devices on different networks to communicate. Access points were setup to allow devices on a VLAN to be served by their AP. Finally, NAT was enabled on the core routers to enable communication with the outside world.