**IT2652 Assignment 2**

**Name:** Olfsen Valones

**Admin No:** 220274X

**Case Study Set A**

Table of Contents

**Introduction1**

**About the Network2**

VLSM3-4

VLAN Tables5-7

Network Topology8

Routing8-9

**Features9**

Printers10

ACL10

Servers11

SSH11

**Introduction**

In this, the task was to design a network of a HQ office with 7 floors, and a warehouse at another physical location. Each had their own departments with varying number of employees and needs.

Method of addressing involved VLSM was used to prevent waste of IP addresses.

**About the Network**

VLSM:

**VLSM: (network address =172.18.0.0/16)**

**255.255.0.0**

**(HQ Office)**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| LAN/WAN | No. of hosts | Host bits required | Resultant CIDR prefix | Subnet Mask that will be configured | Size of subnet (Magic Number) | subnet address allocated | First IP address that can be assigned | Last IP address that can be assigned | Broadcast IP for the subnet |
| **4th Floor Ops Support** | **140** | 8 | /24 | 255.255.255.0 | 256 | 172.18.0.0 | 172.18.0.1 | 172.18.0.254 | 172.18.0.255 |
| **5th Floor Sales & Marketing** | **110** | 7 | /25 | 255.255.255.128 | 128 | 172.18.1.0 | 172.18.1.1 | 172.18.1.126 | 172.18.1.127 |
| **2nd Floor Warehouse** | **90** | 7 | /25 | 255.255.255.128 | 128 | 172.18.1.128 | 172.18.1.129 | 172.18.1.254 | 172.18.1.255 |
| **3rd Floor IT Department** | **60** | 6 | /26 | 255.255.255.192 | 64 | 172.18.2.0 | 172.18.2.1 | 172.18.2.62 | 172.18.2.63 |
| **6th Floor Management & HR** | **50** | 6 | /26 | 255.255.255.192 | 64 | 172.18.2.64 | 172.18.2.65 | 172.18.2.126 | 172.18.2.127 |
| **7th Floor Cafeteria** | **6** | 3 | /29 | 255.255.255.248 | 8 | 172.18.2.128 | 172.18.2.129 | 172.18.2.134 | 172.18.2.135 |
| **Ground Level Reception** | **4** | 3 | /29 | 255.255.255.248 | 8 | 172.18.2.136 | 172.18.2.137 | 172.18.2.142 | 172.18.2.143 |

**VLSM (network address =172.25.0.0/16)**

**(Warehouse)**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| LAN/WAN | No. of hosts | Host bits required | Resultant CIDR prefix | Subnet Mask that will be configured | Size of subnet (Magic Number) | subnet address allocated | First IP address that can be assigned | Last IP address that can be assigned | Broadcast IP for the subnet |
| **Ops Support Department** | **65** | 7 | /25 | 255.255.255.128 | 128 | 172.25.0.0 | 172.25.0.1 | 172.25.0.126 | 172.25.0.127 |
| **Warehouse Department** | **40** | 6 | /26 | 255.255.255.192 | 64 | 172.25.0.128 | 172.25.0.129 | 172.25.0.190 | 172.25.0.191 |
| **IT Department** | **5** | 3 | /29 | 255.255.255.248 | 8 | 172.25.0.192 | 172.25.0.193 | 172.25.0.198 | 172.25.0.199 |
| **WAN LINK** | **2** | 2 | /30 | 255.255.255.252 | 4 | 10.0.0.0 | 10.0.0.0 | 10.0.0.1 | 10.0.0.2 |

**VLAN Tables**

A screenshot of a computer

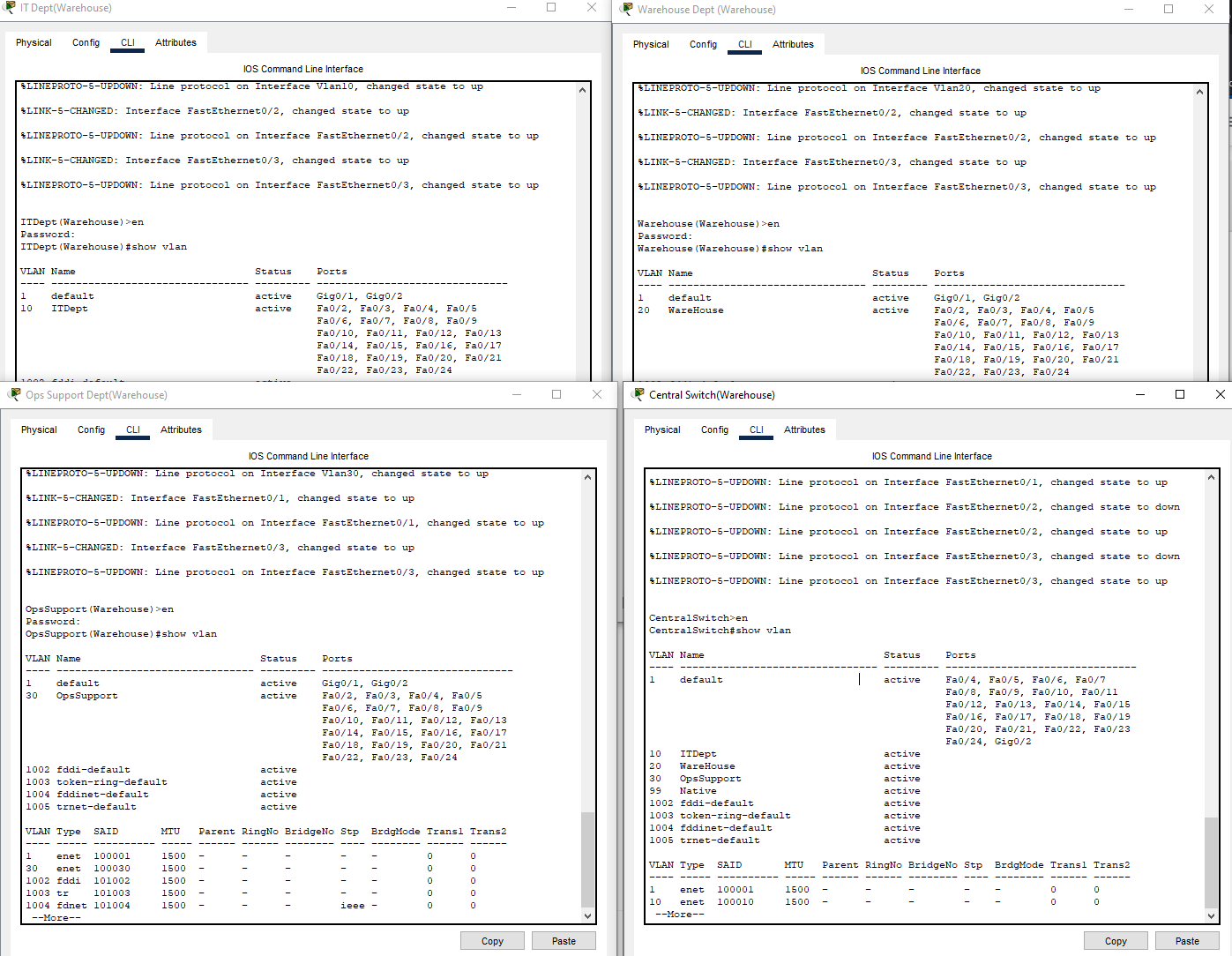
Description automatically generatedHQ VLANs:

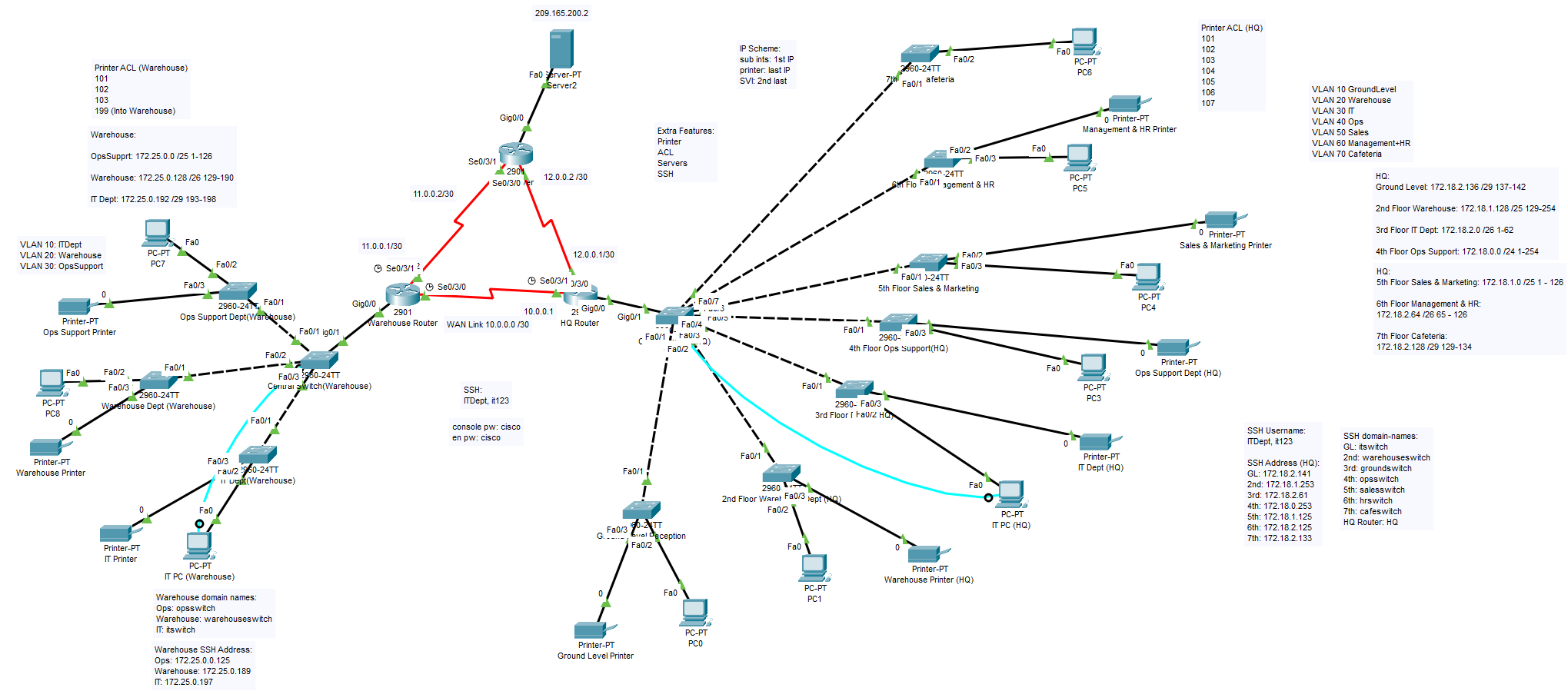
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Warehouse VLANs:

**Network Topology**

*Reason behind choosing a router-on-a-stick configuration*

The router on a stick configuration was selected for the network topology as it still allowed for scaling should the company expand in departments and the need for more VLANs. Another benefit of it was being the use of a single physical cable and interface, with multiple logical sub-interfaces created for the respective VLANs and to also enable inter-VLAN routing.

**Routing**

In the case study, two types of routing protocols were used:

1. OSPF (Dynamic routing)
2. Static route (Default route)

*OSPF (Dynamic Routing)*

OSPF (Open Shortest Path First) is a dynamic routing protocol where routers in the network learn about each other through sending messages and building their respective databases of the network.

For OSPF to work, one of the main requirements is that the routers involved need to have the same router ID (if configured manually). In this assignment, the router IDs for OSPF were done manually using the ‘router ospf 1’ command after doing the ‘configure terminal’ command in the privileged EXEC mode.

As for how OSPF works and learns, it does the following in order:

* Link State Request (LSR)
* Link State Update (LSU)
* Link State Acknowledge (LSAck)

Example: Warehouse router learns of HQ router using OSPF

* Both routers are using ospf ID 1
* Warehouse router sends the LSR to HQ router to learn about its tables
* The HQ router sends a LSU to respond to the request, updating the Warehouse router’s table to also have the HQ router’s information
* After the update, the Warehouse router sends an LSUAck to acknowledge it received and has been updated

Benefits of dynamic routing:

* Can be easily scaled by just updating the router with the new network
  + Other routers can learn and be updated as well to be in sync with their neighbor(s)
* Independent of network size
* Automatically adapts to topology changes
  + OSPF is based on choosing the shortest path to its destination

*Static Routing*

In static routing, it was about configuring a default route where any traffic that didn’t match those in the OSPF routing table would be routed towards. This was mainly for traffic from the respective networks to the servers and vice versa.

Benefits of static routing:

* Administrator intervention required
* Good for simple topologies
* No additional resources like CPU and memory needed
* Paths are *explicitly* defined by the administrator

**Features**

In this case study, the following features were implemented:

1. Printers
2. ACL (Access Control List)
3. Servers
4. SSH (Secure Shell)

*Printers*

In an office setting, each department usually has its own printer. So for the implementation, each department has their own printer that is associated with the respective VLAN. The addressing on them are static unlike other end devices like PCs, so for DHCP configuration, these addresses are excluded in the pool when leasing address.

*ACL (Access Control List)*

An ACL is implemented to allow/deny specific traffic to and from a specific interface. With inter-VLAN routing, all PCs were able to ping one another, but this also meant that PCs from another department could contact other printers, which shouldn’t happen in an office setting.

So to prevent it, ACL was implemented by deny any traffic to the printer’s IP address while allowing other traffic to go through.

*Servers*

In the case study, servers were implemented to emulate access to websites on the internet. This was where the default route from both HQ and Warehouse router would be directed towards.

*SSH (Secure Shell)*

As there is an IT Department, it is important for them for have access to remote configure resources in the network after the initial configuration. For this, SSH was enabled on the switches for the respective VLANs, central switches, and the routers that are part of the network.

As SSH itself is encrypted over Telnet, information is secured and prevents man in the middle attacks where the packets could be sniffed and intercepted during its transmission, preventing unauthorized access to those who doesn’t know the username and password.