SLIIT UNI

THE KNOWLEDGE UNIVERSITY

Faculty of Computing

IE1030 – Data Communication Networks

Year 1 Semester 1 (2024)

Network Design Assignment

Group ID: P11-14
Batch Group No: Y1.S1.WD.IT.11.02

Group members:

1. Pinthu D.I.U.	IT24100139
2. Vithanage M.M.	IT24100288
3. Liyanage N.R.W.	IT24100536
4. Gangodawila G.P.I.C.	IT24100020
5. Abeyweera G.I.J.	IT24100524
6. Weerasinghe M.P.H.N.	IT24101217

29.09.2024
……………………..
Date of Submission

Contents

1. Floor Plan

The floor plan of the building of tech world is provided as below

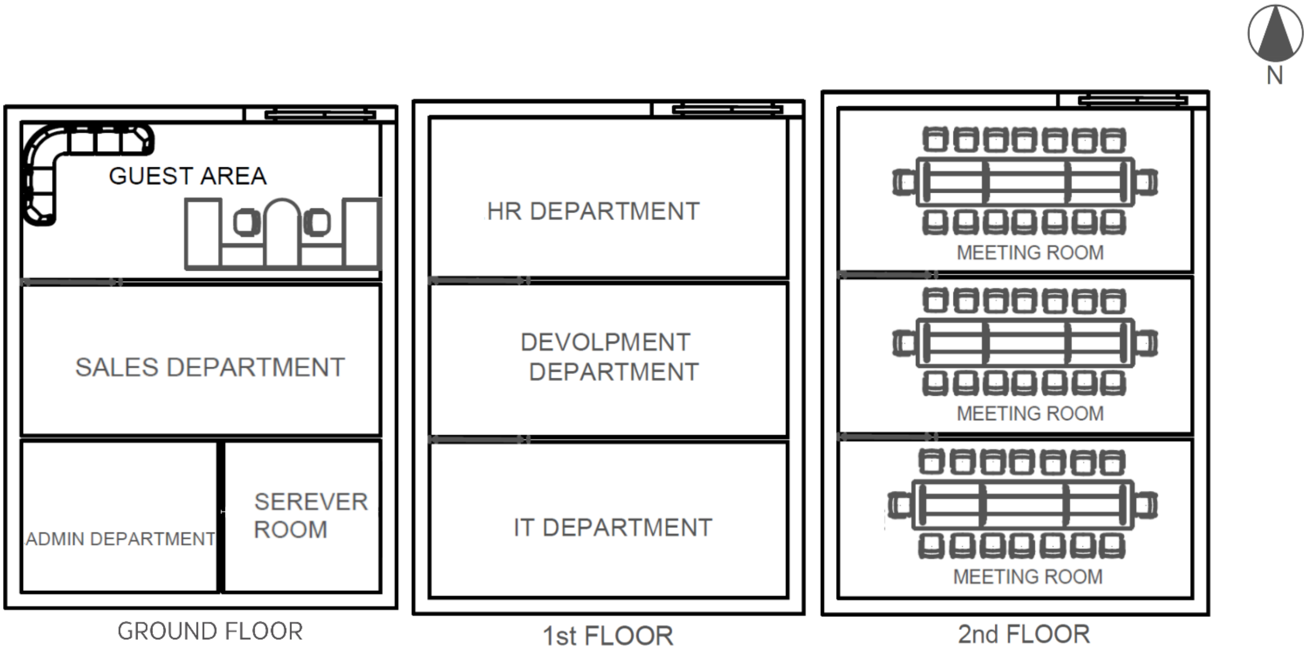

Figure 2.1: Floor Plan

- ✓ The first floor accommodates the Guest Area, Sales Department, Administration Department, and the Demilitarized Zone (DMZ).
- ✓ The second floor houses the IT Department, Development Team, and HR Department.
- ✓ The third floor is dedicated to three Meeting Rooms.

2. Network Topology Design

2.1 Server Room (Central) Network Topology

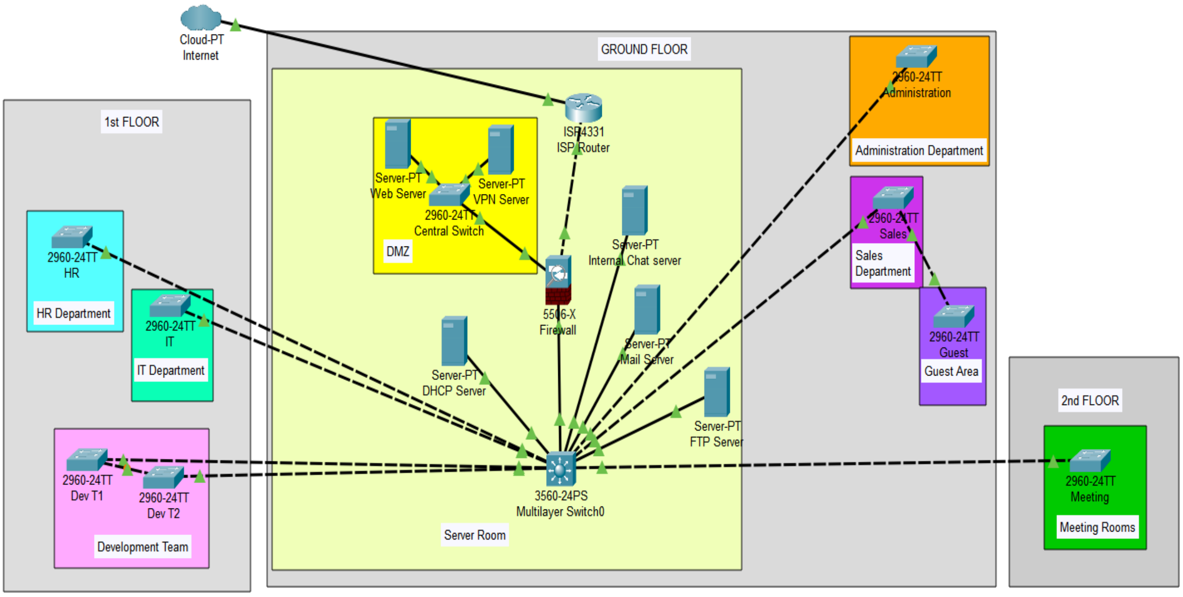

Figure 2.1: Network Topologies

The ISP Router connects to a Firewall, which connects to a central Switch in the Demilitarized Zone. The central Switch houses VPN Servers and Web Servers for external communication. The Firewall connects to a Multilayer Switch, acting as the Main Router for the office network. The Main Router connects DHCP Servers, Mail Servers, FTP Servers, and Internal Chat Servers for internal communication. Eight switches belong to different departments, such as Sales, Guest Area, Administration, IT, Development Team, HR, and Meeting Rooms, not within the DMZ.

2.2 Administration Department Network Topology

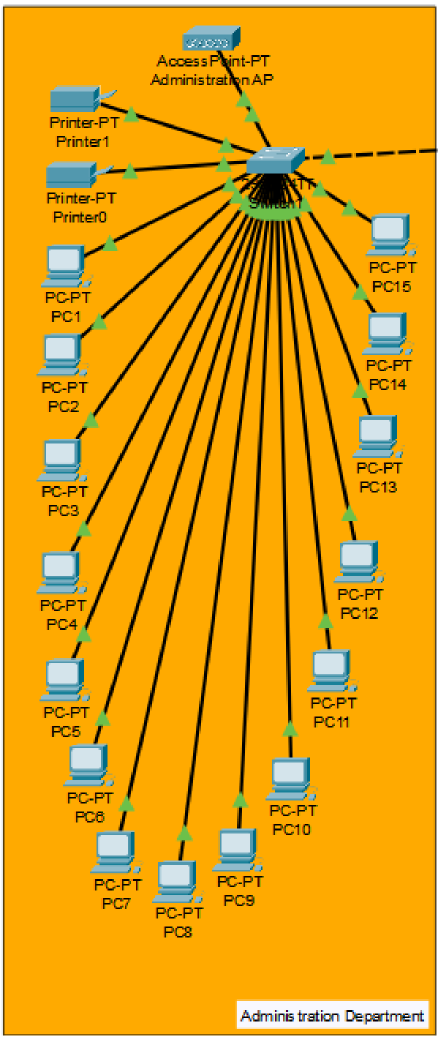

Figure 2.2.1: Administration Department Logical layout

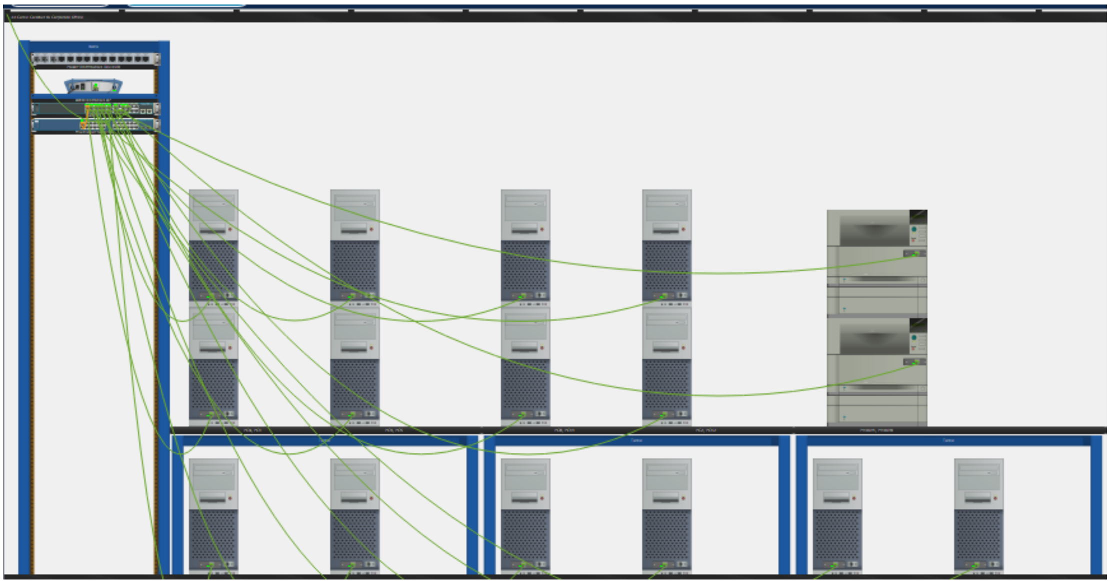

Figure 2.2.2: Administration Department physical layout

2.3 Sales Department Network Topology

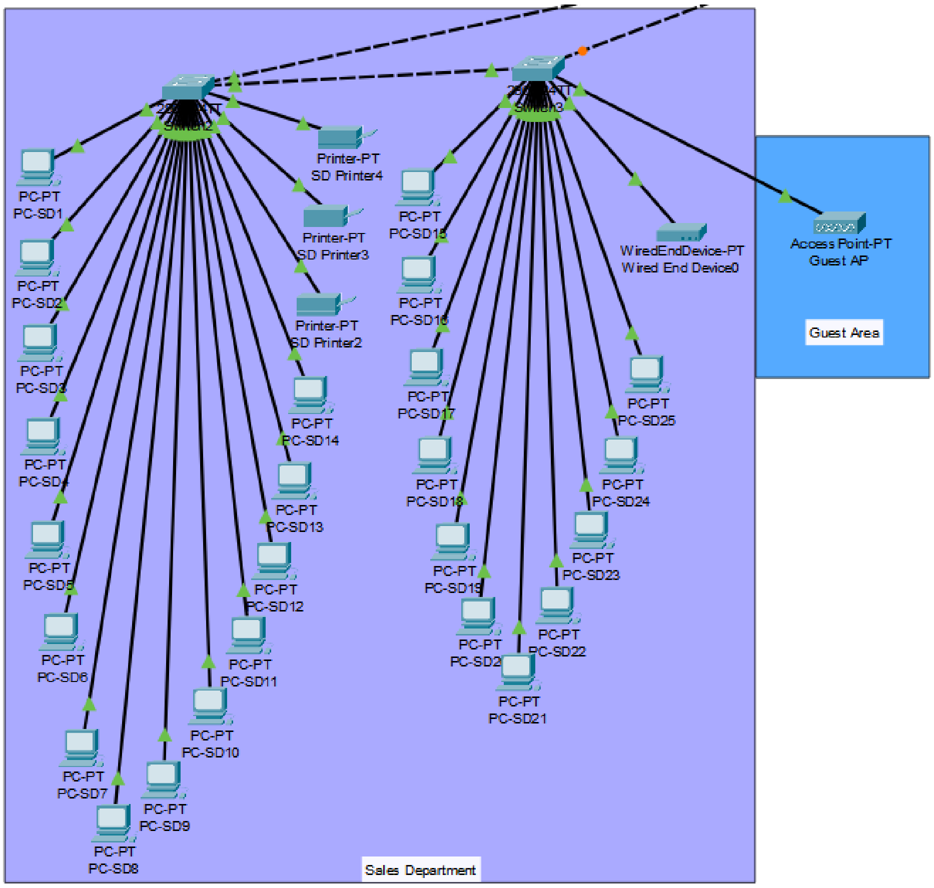

Figure 2.3.1: Sales Development Logical layout

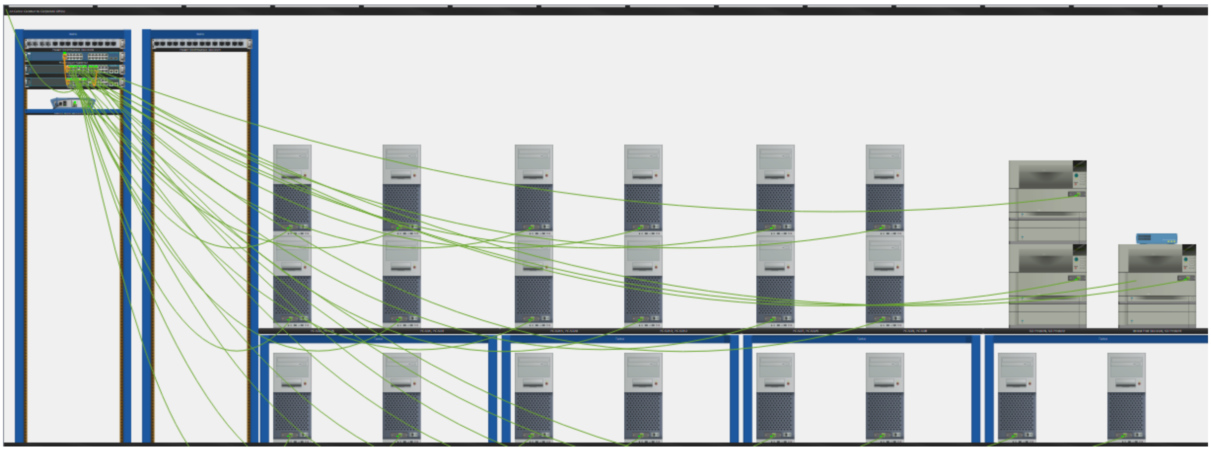

Figure 2.3.2: Sales Development physical layout

2.4 IT Department Network Topology

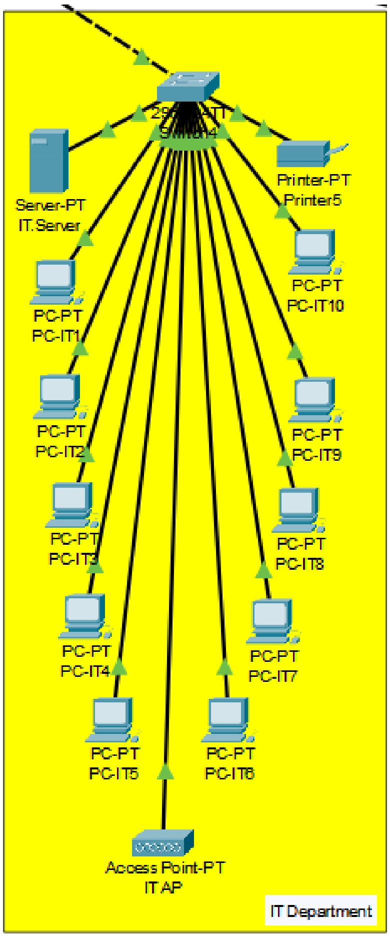

Figure 2.4.1: IT Development
Logical layout

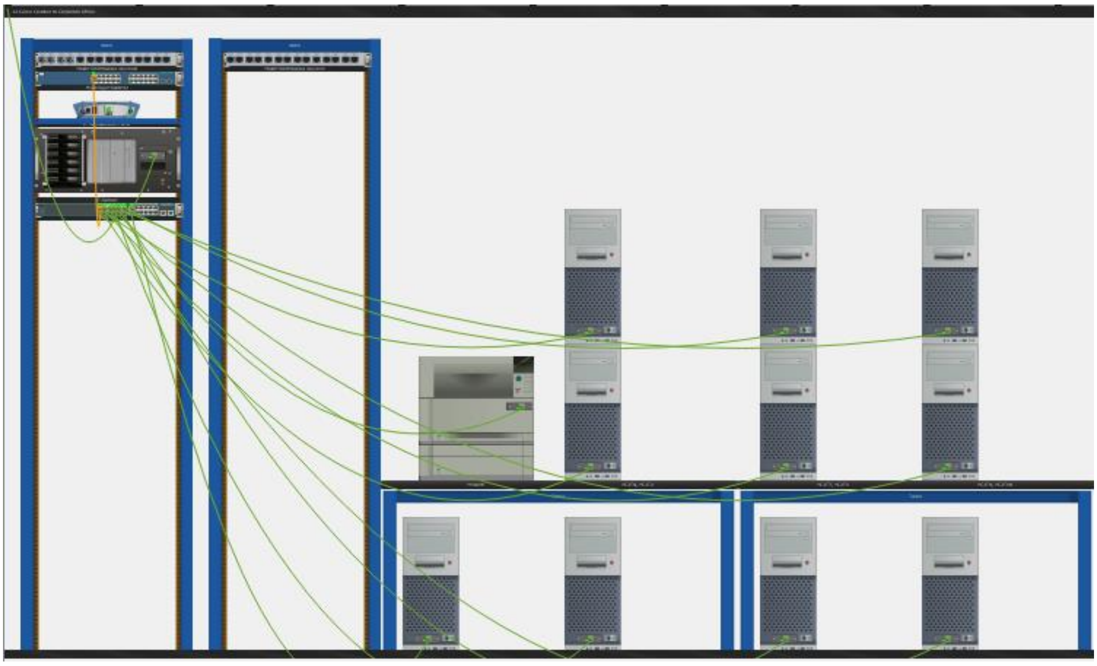

Figure 2.4.2: IT Development
physical layout

2.5 Development Team Network Topology

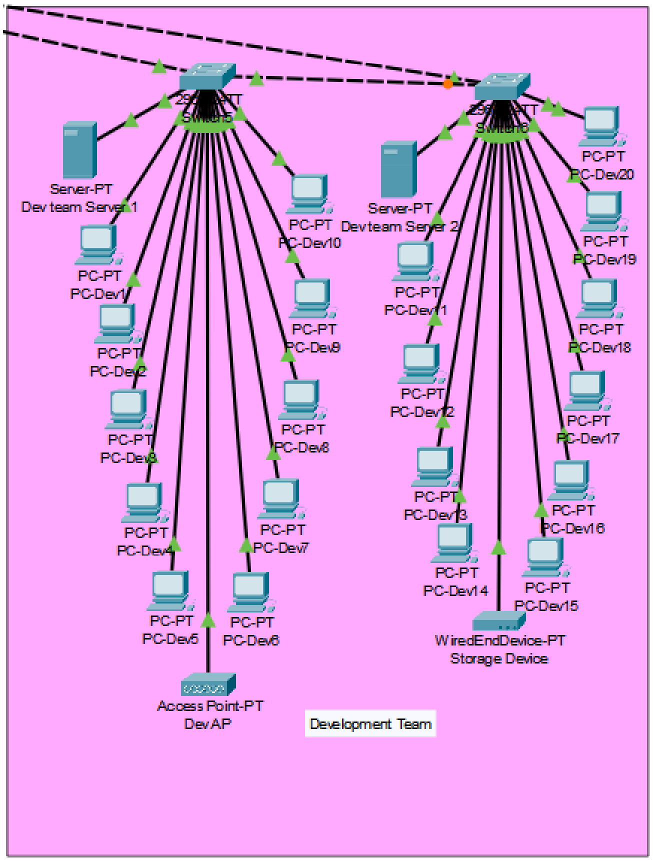

Figure 2.5.1: Development Team Logical layout

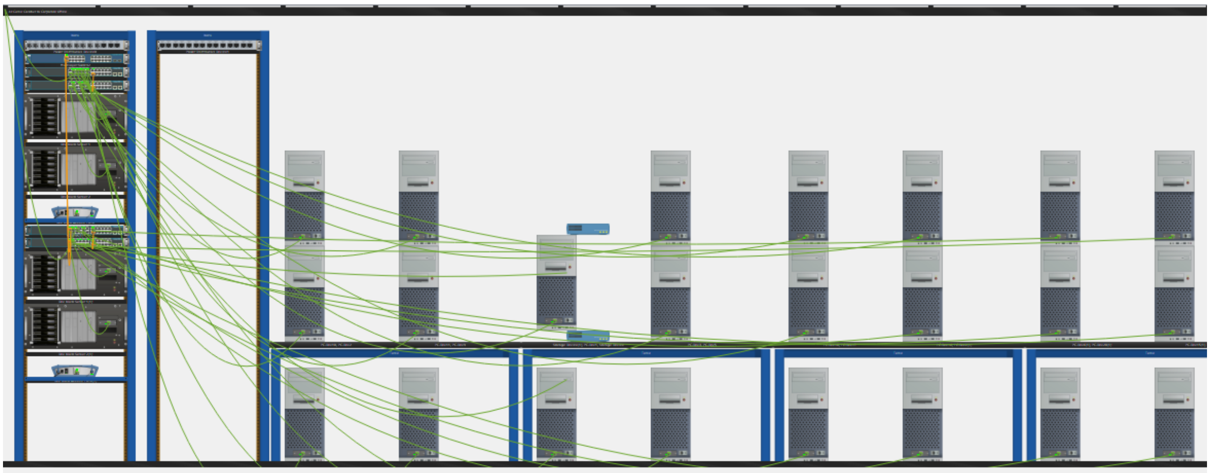

Figure 2.5.2: Development Team physical layout

2.6 Meeting Rooms Network Topology

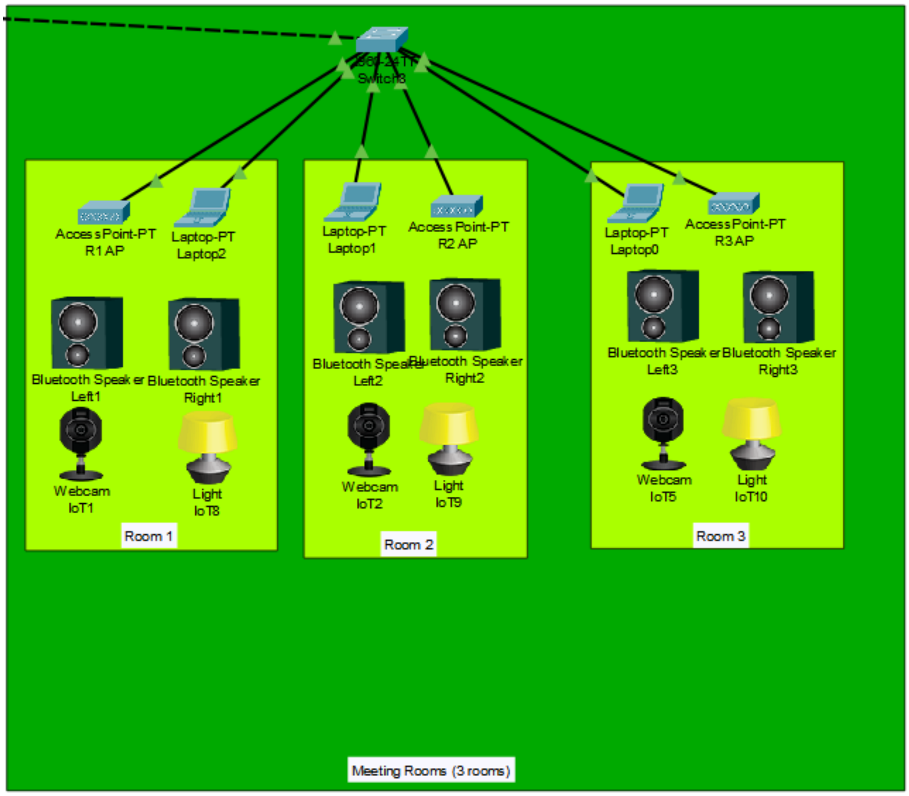

Figure 2.6.1: Meeting Rooms Logical layout

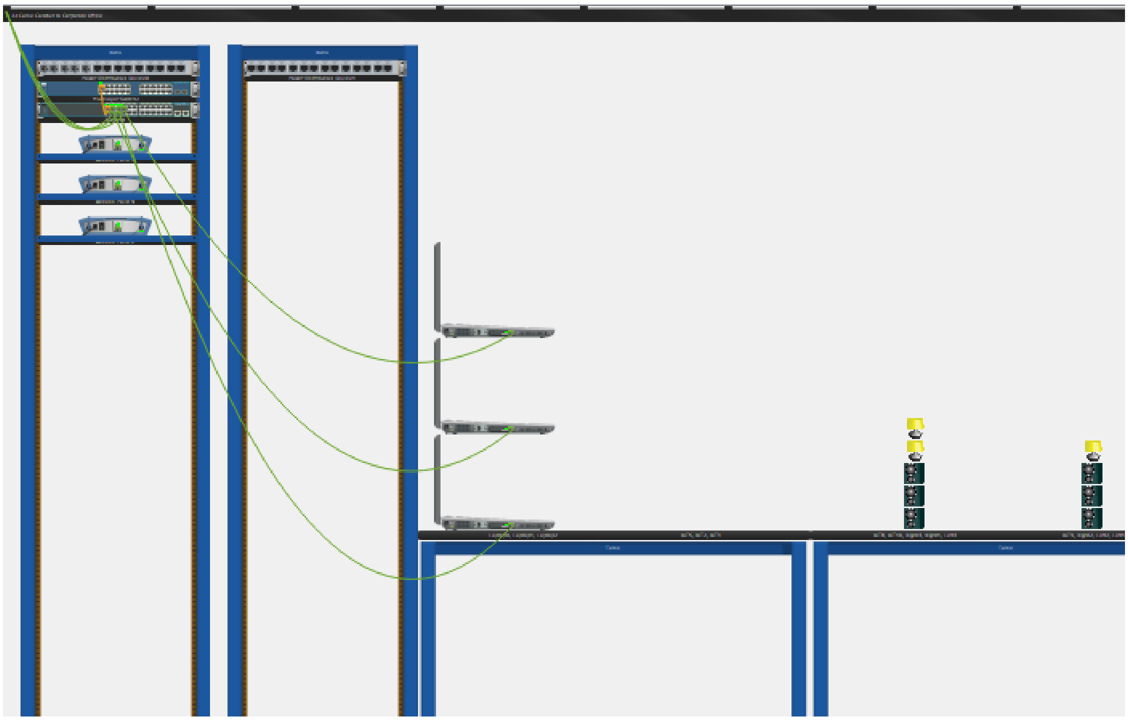

Figure 2.6.2: Meeting Rooms physical layout

2.7 HR Department Network Topology

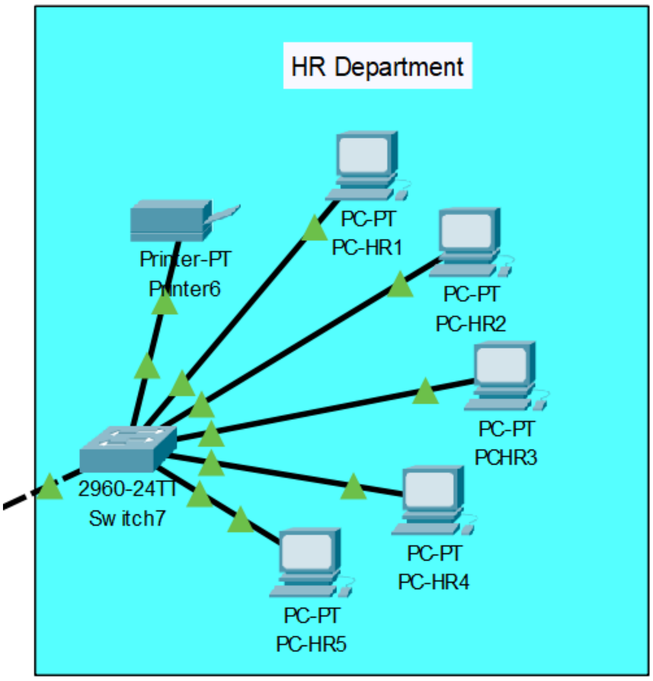

Figure 2.7.1: HR Department Logical layout

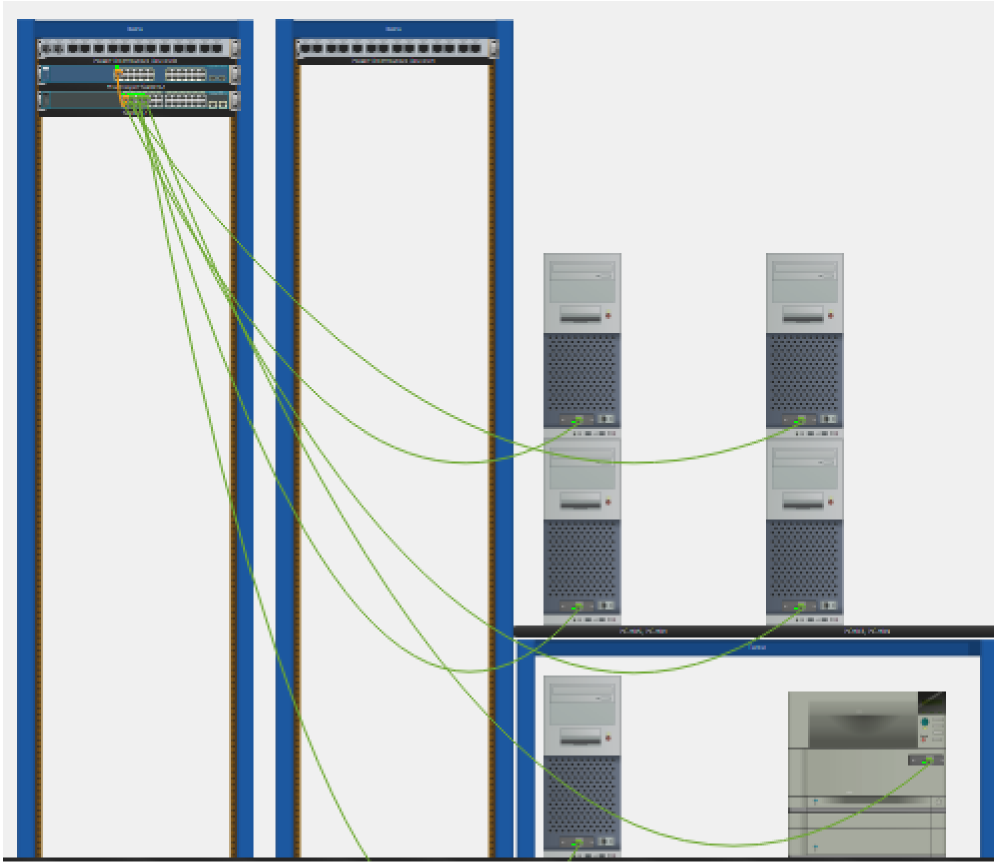

Figure 2.7.2: HR Department Physical layout

2.8 Full Network Diagram

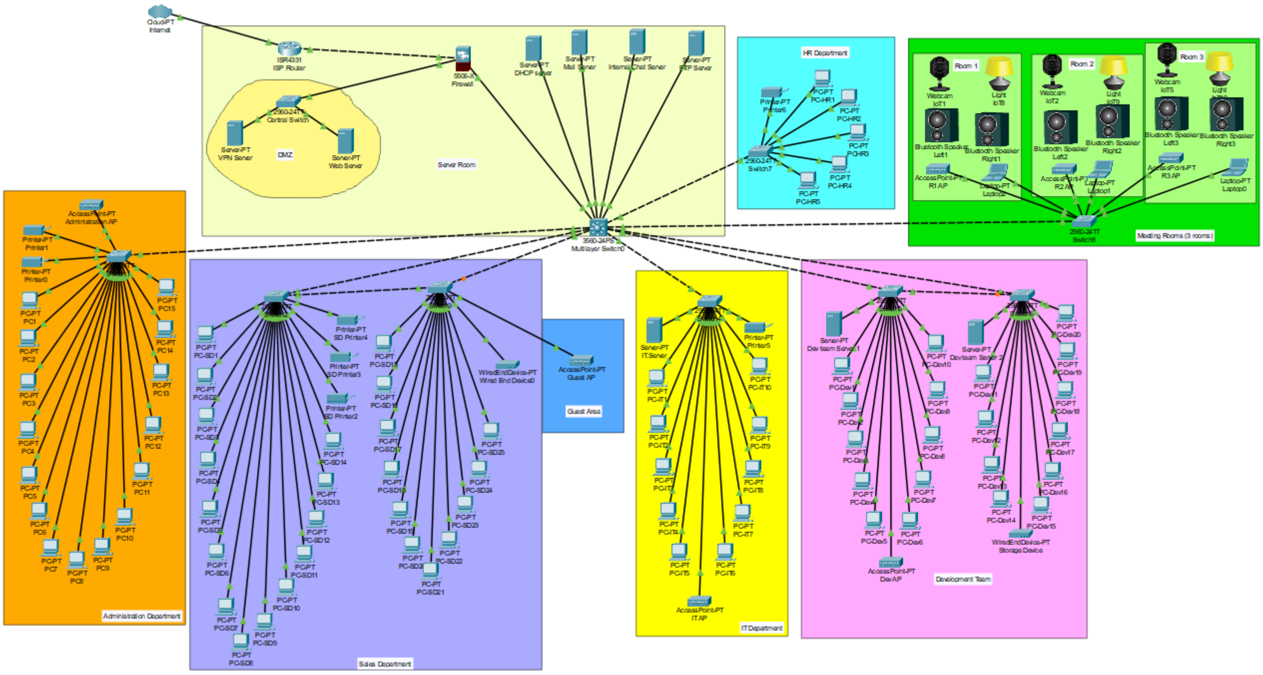

Figure 2.8.: Full Network Diagram

3. IP Addressing Scheme

Our leader’s student number is IT24100020 So, the company's IP address is **192.168.20.0/24.** To accommodate the 9 different sections of the office, including Server Room, DMZ, Sales Department, Manage Network, Administration, IT, Development Team, HR, and Meeting Rooms, 9 subnetworks will be created.

1) Sales: 29 hosts → 62 Usable IPs → /26
2) Dev.: 23 hosts → 62 Usable IPs → /26
3) Admin.:18hosts → 30 Usable IPs → /27
4) IT:12 hosts → 14 Usable IPs → /27
5) Manage.: 10 hosts → 14 Usable IPs → /28
6) HR: 6 hosts → 14 Usable IPs → /28
7) Server R.: 4 servers → 6 Usable IPs → /29
8) Meeting R.: 3 hosts → 6 Usable IPs → /29
9) DMZ: 2 servers → 6 Usable IPs → /29

1) Sales Department IP Addressing

IP Addresses (29 hosts)	25 Computers
	3 Printers
	1 Copier
Network ID	192.168.20.0/26
Subnet Mask	255.255.255.192
1st Usable IP	192.168.20.1
Last Usable IP (Default Gateway)	192.168.20.62
Broadcast Address	192.168.20.63
Computers (25)	192.168.20.1 - 192.168.20.24
Printers (3)	192.168.20.25 - 192.168.20.27
Copier (1)	192.168.20.28
Unused IP Addresses (34)	192.168.20.29 -192.168.20.62

Table 3.1.: Sales Department IP Addressing Scheme

2) Development Team IP Addressing

IP Addresses (23 hosts)	20 Computers
	2 Servers
	1 Storage Device
Network ID	192.168.20.64/26
Subnet Mask	255.255.255.192
1st Usable IP	192.168.20.65
Last Usable IP (Default Gateway)	192.168.20.126
Broadcast Address	192.168.20.127
Computers (20)	192.168.20.65 - 192.168.20.84
Servers (2)	192.168.20.85 & 192.168.20.86
Storage Device (1)	192.168.20.87
Unused IP Addresses (39)	192.168.20.88 - 192.168.20.126

Table 3.2.: Development Team IP Addressing Scheme

3) Administration Department IP Addressing

IP Addresses (18 hosts)	15 Computers
	2 Printers
	1 Scanner
Network ID	192.168.20.128/27
Subnet Mask	255.255.255.224
1st Usable IP	192.168.20.129
Last Usable IP (Default Gateway)	192.168.20.158
Broadcast Address	192.168.20.159
Computers (15)	192.168.20.129 - 192.168.20.143
Printers (2)	192.168.20.144 & 192.168.20.145
Scanner (1)	192.168.20.146
Unused IP Addresses (12)	192.168.20.147 - 192.168.20.158

Table 3.3.: Administration Department IP Addressing Scheme

4) IT Department IP Addressing

IP Addresses (12 hosts)	10 Computers
	1 Printers
	1 Servers
Network ID	192.168.20.160/27
Subnet Mask	255.255.255.224
1st Usable IP	192.168.20.161
Last Usable IP (Default Gateway)	192.168.20.174
Broadcast Address	192.168.20.175
Computers (10)	192.168.20.161 - 192.168.20.169
Printers (1)	192.168.20.170
Server (1)	192.168.20.171
Unused IP Addresses (3)	192.168.20.172 - 192.168.20.174

Table 3.4.: IT Department IP Addressing Scheme

5) Manage Network IP Addressing

Management Network

- The management network of a network system is a separate network dedicated to managing that network, and it is a logical network. This allows network administrators to monitor, control, and troubleshoot the network without disrupting the operation of the main network.
- For the manage network, the switches and APs belonging to the existing topologies of the network are used, and the IP addresses of the devices used like that in the network we have created can be shown as follows.

IP Addresses (10 hosts)	Ground Floor	2 Switches
		2 APs (Access Point)
	1st Floor	1 Switches
		2 APs
	2nd Floor	3 APs
Network ID	192.168.20.176/28	
Subnet Mask	255.255.255.240	
1st Usable IP	192.168.20.177	
Last Usable IP (Default Gateway)	192.168.20.190	
Broadcast Address	192.168.20.191	
Switches (3)	192.168.20.177 - 192.168.20.179	
APs (Access Point) (7)	192.168.20.180 - 192.168.20.186	
Unused IP Addresses (4)	192.168.20.187 - 192.168.20.190	

Table 3.5.: Manage Network IP Addressing Scheme

6) HR Department IP Addressing

IP Addresses (6 hosts)	5 Computers
	1 Printer
Network ID	192.168.20.192/28
Subnet Mask	255.255.255.240
1st Usable IP	192.168.20.193
Last Usable IP (Default Gateway)	192.168.20.206
Broadcast Address	192.168.20.207
Computers (5)	192.168.20.193 - 192.168.20.197
Printer (1)	192.168.20.198
Unused IP Addresses (7)	192.168.20.199 - 192.168.20.206

Table 3.6.: HR Department IP Addressing Scheme

7) Server Room IP Addressing

IP Addresses (5 hosts)	4 Servers
	1 Firewall
Network ID	192.168.20.208/29
Subnet Mask	255.255.255.248
1st Usable IP	192.168.20.209
Last Usable IP (Default Gateway)	192.168.20.214
Broadcast Address	192.168.20.215
Servers (4)	192.168.20.209 - 192.168.20.212
Firewall (1)	192.168.20.213
Unused IP Addresses (1)	192.168.20.214

Table 3.7.: Server Room IP Addressing Scheme

8) Meeting Room IP Addressing

IP Addresses (3 hosts)	3 Laptops
Network ID	192.168.20.216/29
Subnet Mask	255.255.255.248
1st Usable IP	192.168.20.217
Last Usable IP (Default Gateway)	192.168.20.222
Broadcast Address	192.168.20.223
Laptop (3)	192.168.20.217 - 192.168.20.220
Unused IP Address (2)	192.168.20.221 & 192.168.20.222

Table 3.8.: Meeting Room IP Addressing Scheme

9) Demilitarized (DMZ) IP Addressing

IP Addresses (2 hosts)	2 Servers
Network ID	192.168.20.224/29
Subnet Mask	255.255.255.248
1st Usable IP	192.168.20.225
Last Usable IP (Default Gateway)	192.168.20.230
Broadcast Address	192.168.20.231
Servers (2)	192.168.20.225 & 192.168.20.226
Unused IP Addresses (4)	192.168.20.227 - 192.168.20.230

Table 3.9.: DMZ IP Addressing Scheme

- **Note:** Unused IP addresses provide a pool of available addresses for future network expansion and device allocation.

4. Budgeting

Device	Quantity	Unit Price	Total
End device (PC – Dell Vostro 3020 i7)	75	308,000	23,100,000
Monitor (Lenovo G24-20 23.8`` FHD Monitor)	75	54,000	4,050,000
Laptops (MSI Modern 15 B12M-i5)	3	284,000	852,000
Mouse and Keyboard (Logitech MK120 Combo)	78	5,000	390,000
Printer (Canon PIXMA TS207)	7	15,000	105,000
Scanner (EPSON PERFECTION V39)	1	35,200	35,200
Copier (Canon MF235)	1	56,000	56,000
Backup Power (PROLINK 910Es 10KVA ONLLINE UPS)	1	628,200	628,200
Projector (EPSON H971C EB-E01)	3	146,000	438,000
Web Cam (DAHUA HTI-UC325 1080P FHD)	3	18,200	54,600
NAS System (Synology DiskStation)	1	115,000	115,000
Switch (N/W Switch D-Link 24 Port Des-1024d)	9	16,250	146,250
Multilayer Switch (Cisco Catalyst 3560-X Core 24 Port Switch)	1	180,000	180,000
Routers (ISR400 Branch Router)	1	319,150	319,150
WAPs (TP Link 300mbps Wireless N Ceiling Mount Access Point-Eap110)	9	23,500	211,500
Firewall (Cisco ASA5506-K9)	1	337,620	337,620
Server (Dell PowerEdge R440 Xeon Rack Server)	9	465,000	4,185,000
Windows 11 (Operating System)	75	26,500	1,987,500
Speakers (Sonance Mariner 54)	3	77,300	231,900
Cat6 Ethernet Cables 100m	25	10,400	260,000
Installation			750,000
Total Cost (**LKR**)			38,432,920

5. Security Consideration

According to the Network Diagram we created the network of TechWorld Pvt is made up of three layers, Internet, DMZ and Internal Network. This Segmentation Helps to Isolate Critical Systems from External Threats.

a. VLAN Segmentation

- **Purpose**: Further isolate network segments within the internal network to limit the spread of malware and unauthorized access.
- **Implementation**: VLANs are essential for isolating traffic between different departments and ensuring that sensitive resources are only accessible to authorized users.
  - **Departmental VLANs**: Each department (Administration, Sales, IT, HR, Development, and Meeting Rooms) is assigned its own VLAN:
    - ✓ Administration VLAN
    - ✓ Sales VLAN
    - ✓ IT VLAN
    - ✓ HR VLAN
    - ✓ Development VLAN
    - ✓ Guest VLAN for visitors and unmanaged devices

    This segmentation ensures that traffic from one department cannot access another's resources unless explicitly permitted by security policies.

  - **DMZ VLAN**: Servers like the Web Server and VPN Server located in the DMZ (Demilitarized Zone) are isolated from the internal network to minimize exposure to external threats. Only the required services and ports should be accessible from the internet.

  - **Inter-VLAN Communication**: Traffic between VLANs (e.g., from the IT Department to the Server Room) should be strictly controlled using the Layer 3 multilayer switch (Cisco 2960-24RS) and the firewall. Access control lists (ACLs) should be used to ensure that only necessary traffic between VLANs is permitted.

b. Create Manage Network

- Management network is a logical network used to monitor and control network performance, to increase the efficiency of network topologies in a network. (That is the management network cannot be represented physically).

- This network is very important in managing network systems to protect against network threats.

c. Firewall Configuration

- **Purpose**: Strengthen the network perimeter and control traffic flow.
- **Implementation**: Firewalls play a crucial role in controlling both inbound and outbound traffic and enforcing security policies.
    - **Firewall**: The **Cisco 5506-X Firewall** acts as the primary defense for the network, protecting the internal network from external threats coming from the internet.
        - Network Topology(3VLAN):
            - ✓ VLAN 1 (Inside): Connected to Gig1/3
            - ✓ VLAN 2 (Outside): Connected to Gig1/1
            - ✓ VLAN 3 (DMZ): Connected to Gig1/2

    - **Traffic Flow**
        - Outside to DMZ: Traffic from VLAN 2 (Outside) can only access VLAN 3 (DMZ).
        - Inside to DMZ and Outside: Traffic from VLAN 1 (Inside) can access both VLAN 3 (DMZ) and VLAN 2 (Outside).
        - Outside to Inside: Replies from VLAN 2 (Outside) to VLAN 1 (Inside) are allowed, subject to security policies.
        - VPN Access: Only VPN-connected users from VLAN 2 (Outside) can access VLAN 1 (Inside).

  - **Security**:
    - SSH: Remote access via SSH is allowed only for VLAN 1 (Inside) and VPN-connected users.

d. Secure Wireless Networks

- **Purpose:** Protect wireless communications from unauthorized access and eavesdropping.
- **Implementation**: Given the presence of a **Guest VLAN** in the network, wireless security is crucial to preventing unauthorized access.
  - **Segregated Wireless Networks**:
    - ✓ A dedicated wireless network for internal staff connected to the **IT VLAN** should use WPA3 encryption to ensure secure communication.
    - ✓ A separate SSID for guests (linked to the **Guest VLAN**) should be isolated from the internal network to prevent guest devices from accessing sensitive resources. The Guest VLAN should only allow internet access.

  - **Wireless Access Points (WAPs):**
    - ✓ Wireless access points should be secured with strong passwords, and SSID broadcasting for internal networks should be disabled to reduce the risk of casual attempts to connect.
    - ✓ WAPs should also be configured with MAC filtering to only allow authorized devices.