SLIIT UNI

THE KNOWLEDGE UNIVERSITY

Faculty of Computing

IE1030 – Data Communication Networks

Year 1 Semester 1 (2024)

Network Design Assignment

Group ID: P03-17
Batch Group No: Y1. S1. WD.03.17

Group members:

1. Udakara K W S	IT24101148
2. Tathsilu S.E.B	IT24101897
3. Vaishavi. I	IT24100086
4. Gamage T.G.R.N.	IT24101522
5. Mohammed M H S	IT24102308
6. Weerasinghe T. S.	IT24100719

30.09.2024
……………………..
Date of Submission

Content

1. **Physical & Logical Layout of Tech World**

1.1 Physical Layout Overview for Tech World

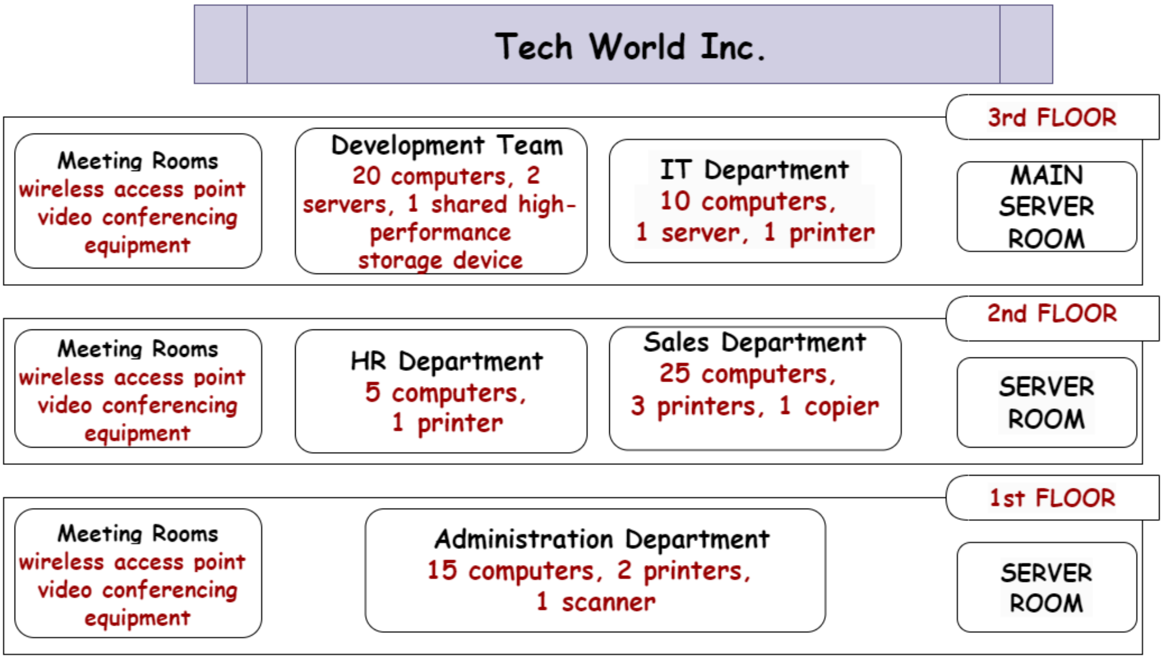

Figure 1.1: Physical Layout Overview for Tech World

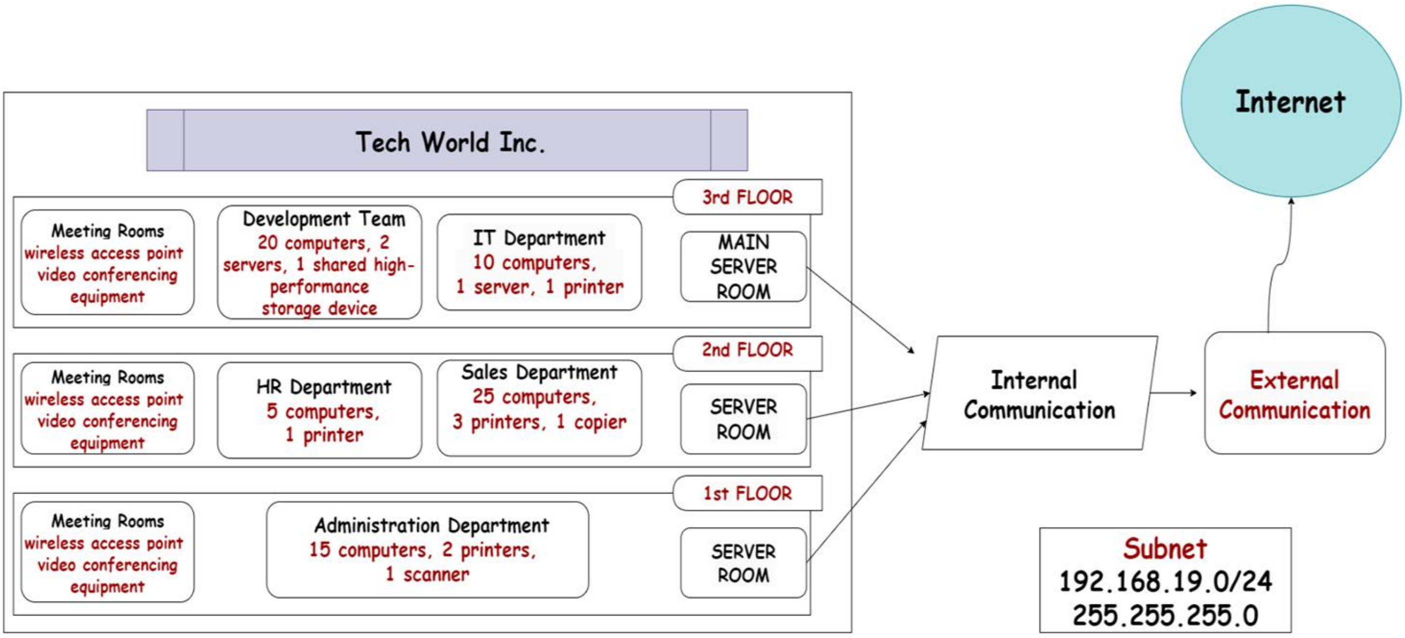

Figure 1.1: Physical Layout Overview for Tech World

1.2 Logical Layout Overview for Tech World

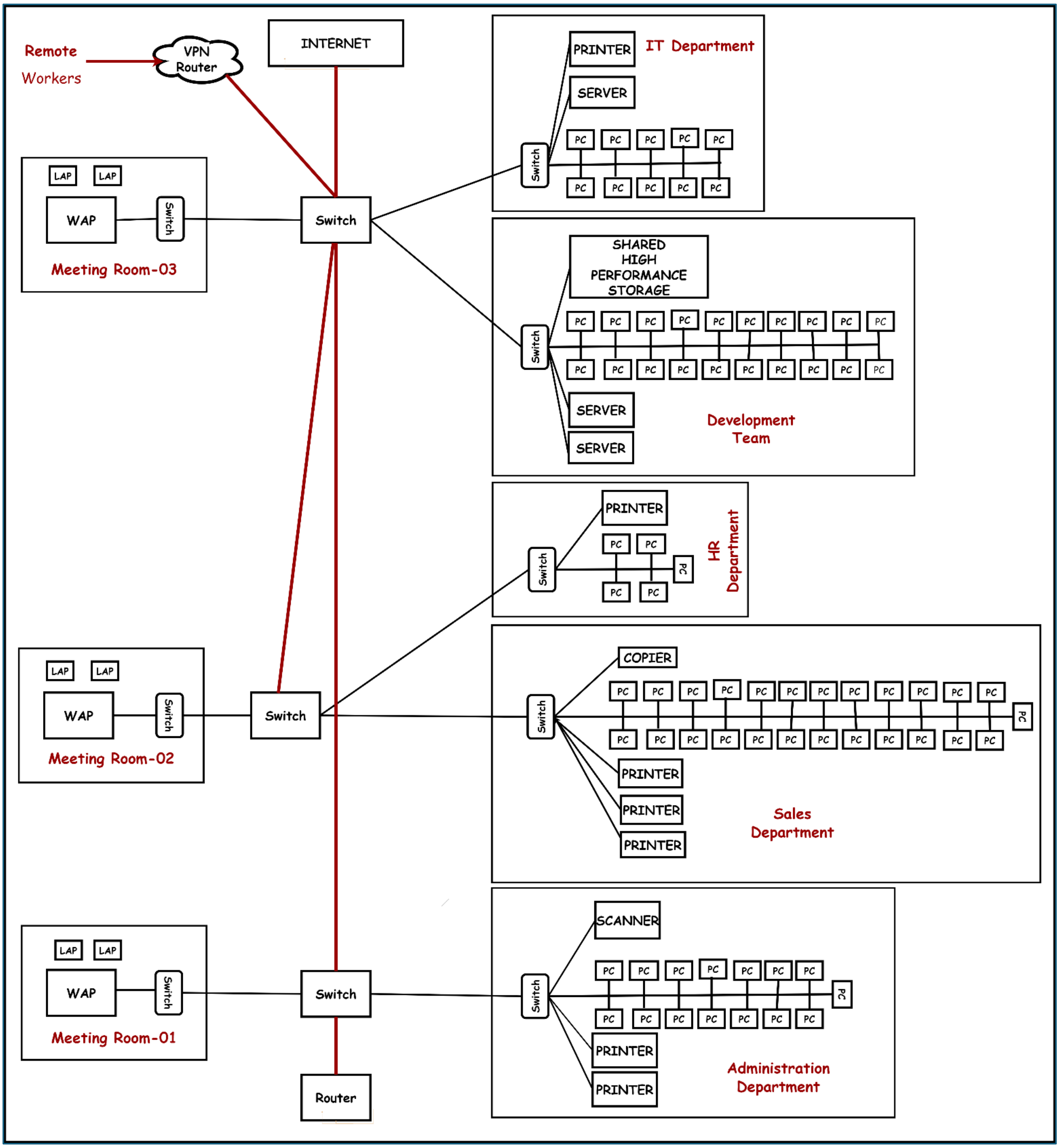

Figure 1.2: Logical Layout Overview for Tech World

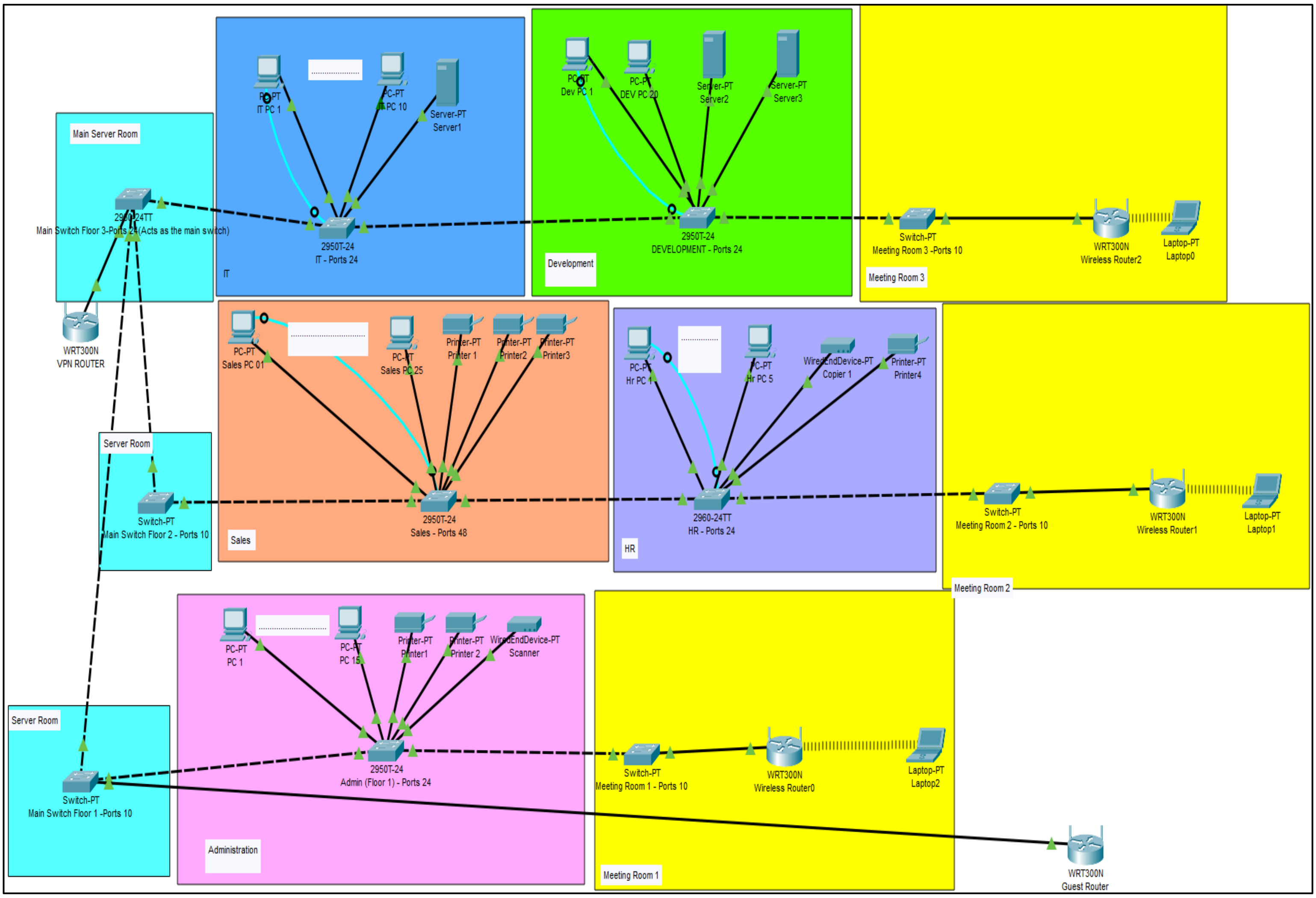

Figure 1.2: Logical Layout Overview for Tech World using Cisco Packet Tracer

2. First Floor

2.1 Physical Layout of First Floor

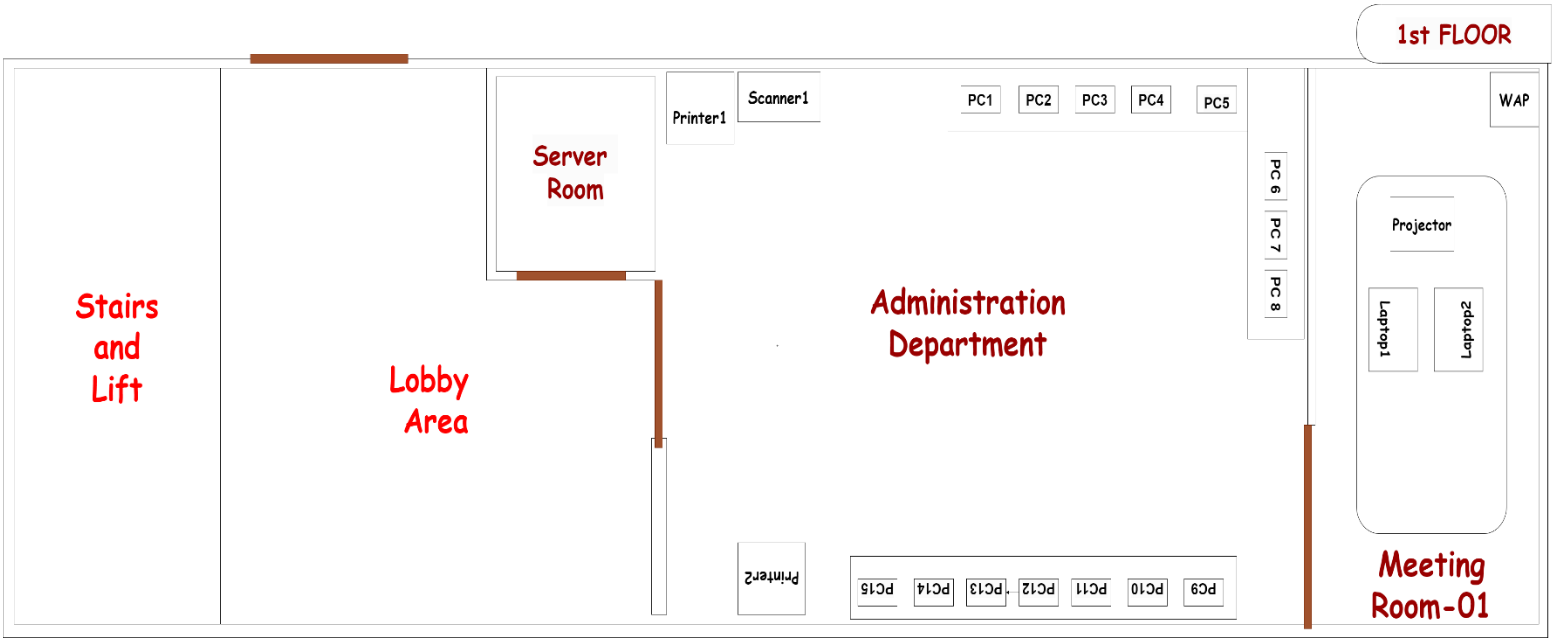

Figure 2.1: Physical Layout of First Floor

2.2 Logical Layout of First Floor

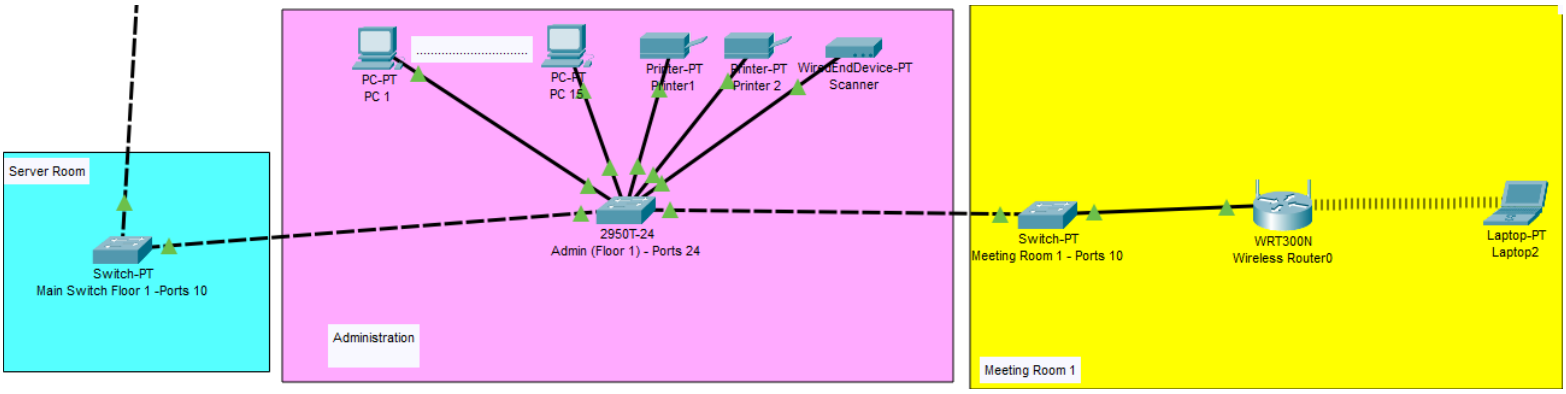

Figure 2.2: Logical Layout of First Floor

2.3 Configurations of First Floor

IP Configuration of First Floor

Department	Network Address	Broadcast Address	Subnet Mask	IP Range
Administration	192.168.19.120	192.168.19.151	255.255.255.224 (/27)	192.168.19.121 - 192.168.19.150
Meeting Room 1	192.168.19.152	192.168.19.167	255.255.255.240 (/28)	192.168.19.153 - 192.168.19.166

VLAN Segmentation of First Floor

Department	Devices	VLAN ID
Administration	15 computers, 2 printers, 1 scanner	VLAN 10
Meeting Rooms	1 room (WAP, video conferencing)	VLAN 60
Guest Wi-Fi	Secure guest network for visitors	VLAN 70

Administration Department

VLAN ID -10
VLAN NAME- ADMINISTRATION

Meeting Room
VLAN ID -60
VLAN NAME- MEETINGROOM

Guest Wi-Fi
VLAN ID -70
VLAN NAME- GUESTWIFI

3. Second Floor

3.1 Physical Layout of Second Floor

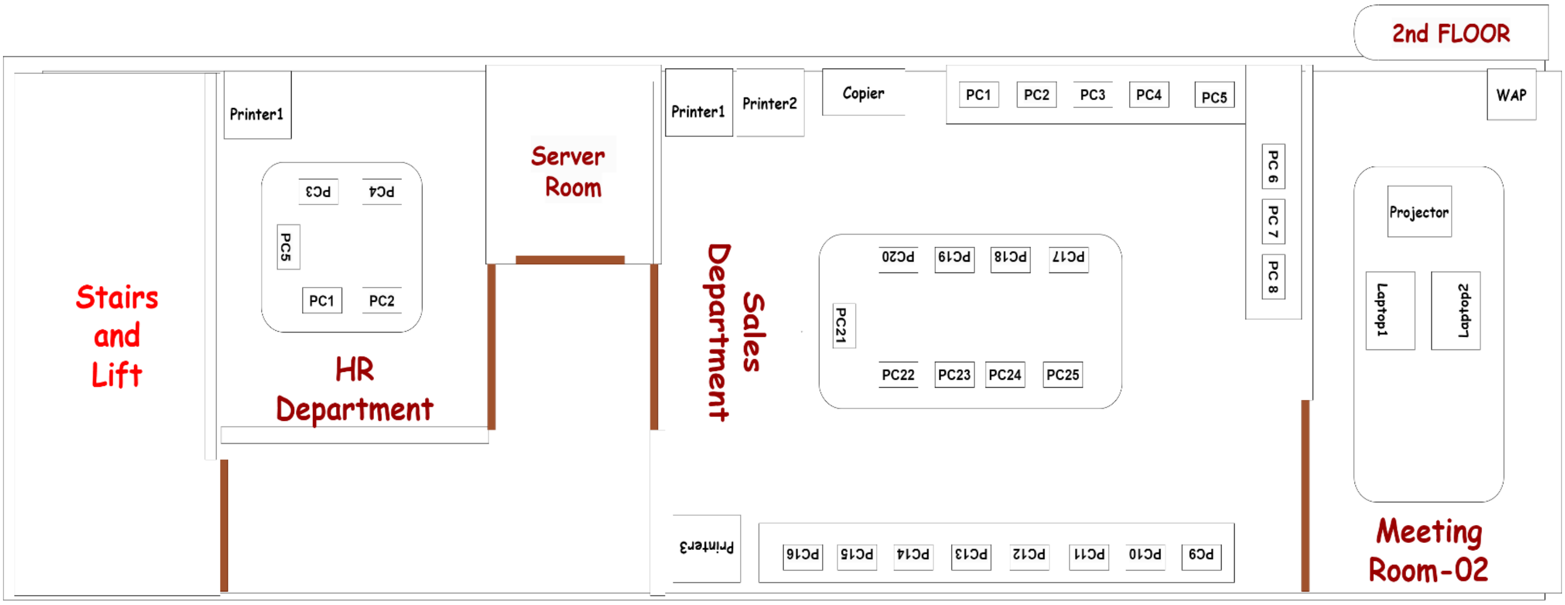

Figure 3.1: Physical Layout of Second Floor

3.2 Logical Layout of Second Floor

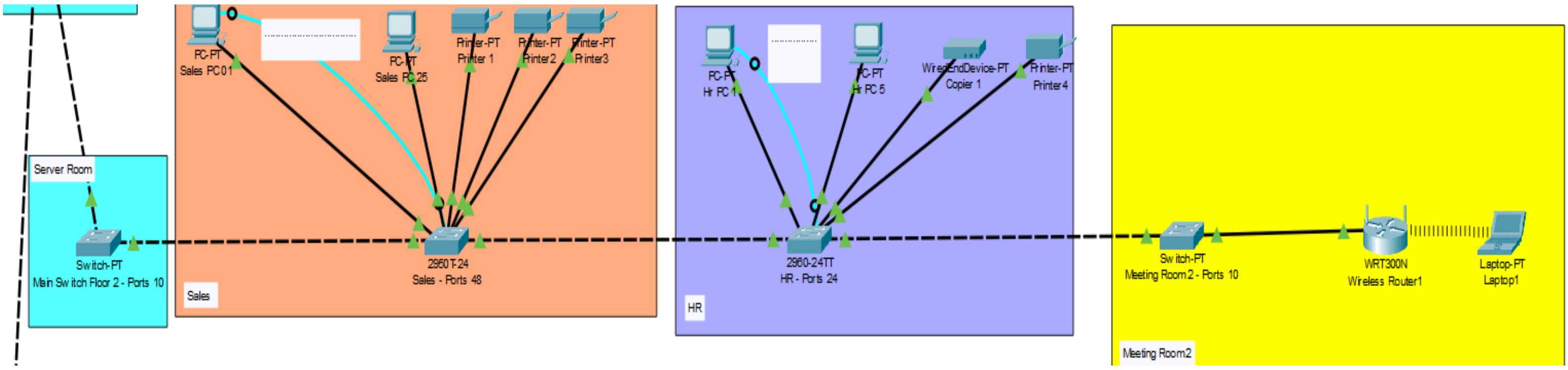

Figure 3.2: Logical Layout of Second Floor

3.3 Configurations of Second Floor

IP Configuration of Second Floor

Department	Network Address	Broadcast Address	Subnet Mask	IP Range
HR	192.168.19.48	192.168.19.55	255.255.255.248 (/29)	192.168.19.49 - 192.168.19.54
Sales	192.168.19.56	192.168.19.119	255.255.255.192 (/26)	192.168.19.57 - 192.168.19.118
Meeting Room 2	192.168.19.168	192.168.19.183	255.255.255.240 (/28)	192.168.19.169 - 192.168.19.182

VLAN Segmentation of Second Floor

Department	Devices	VLAN ID
HR	5 computers, 1 printer	VLAN 50
Sales	25 computers, 3 printers, 1 copier	VLAN 20
Meeting Rooms	1 room (WAP, video conferencing)	VLAN 60

Administration Department

VLAN ID -50
VLAN NAME- HR

Sales Department
VLAN ID -20
VLAN NAME- SALES

Meeting Room
VLAN ID -60
VLAN NAME- MEETINGROOM

4. Third Floor

4.1 Physical Layout of Third Floor

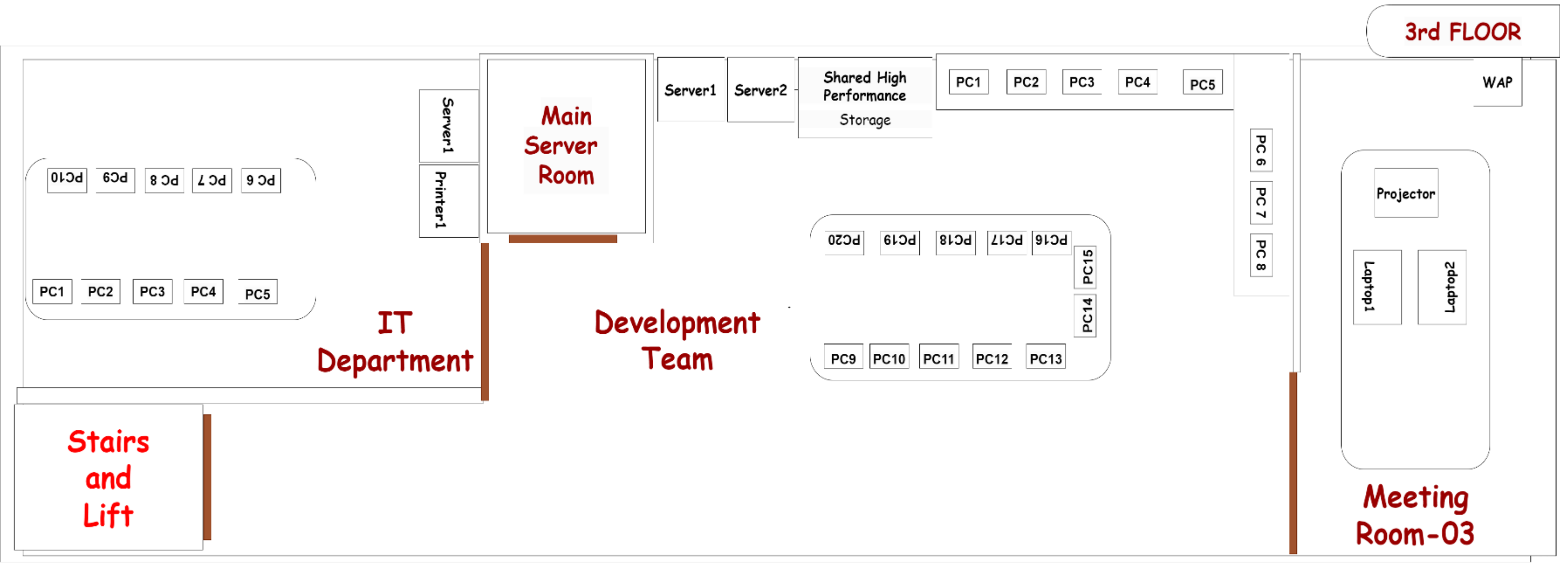

Figure4.1: Physical Layout of Third Floor

4.2 Logical Layout of Third Floor

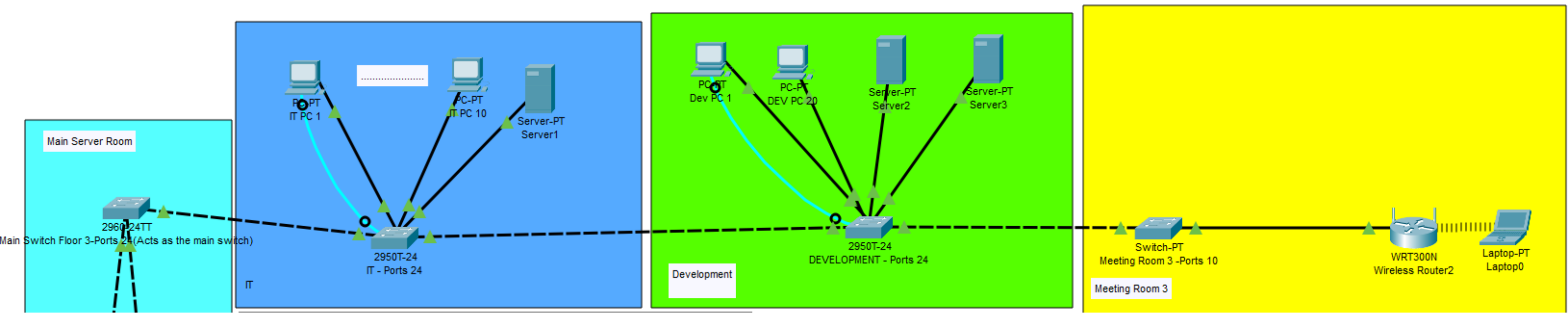

Figure 4.2: Logical Layout of Third Floor

4.3 Configurations of Third Floor

IP Configuration of Third Floor

Department	Network Address	Broadcast Address	Subnet Mask	IP Range
IT	192.168.19.0	192.168.19.15	255.255.255.240 (/28)	192.168.19.1 - 192.168.19.14
Development	192.168.19.16	192.168.19.47	255.255.255.224 (/27)	192.168.19.17 - 192.168.19.46
Meeting Room 3	192.168.19.184	192.168.19.199	255.255.255.240 (/28)	192.168.19.185 - 192.168.19.198

VLAN Segmentation of Third Floor

Department	Devices	VLAN ID
IT	10 computers, 1 server, 1 printer	VLAN 30
Development Team	20 computers, 2 servers, 1 high-performance storage	VLAN 40
Meeting Rooms	1 room (WAP, video conferencing)	VLAN 60

IT Department
VLAN ID -30
VLAN NAME- IT

Development Team
VLAN ID -40
VLAN NAME- DEVELOPMENT

Meeting Room
VLAN ID -60
VLAN NAME- MEETINGROOM

5. IP Address Allocation for Overall Company

Department	Network Address	Broadcast Address	Subnet Mask	IP Range
IT	192.168.19.0	192.168.19.15	255.255.255.240 (/28)	192.168.19.1 - 192.168.19.14
Development	192.168.19.16	192.168.19.47	255.255.255.224 (/27)	192.168.19.17 - 192.168.19.46
HR	192.168.19.48	192.168.19.55	255.255.255.248 (/29)	192.168.19.49 - 192.168.19.54
Sales	192.168.19.56	192.168.19.119	255.255.255.192 (/26)	192.168.19.57 - 192.168.19.118
Administration	192.168.19.120	192.168.19.151	255.255.255.224 (/27)	192.168.19.121 - 192.168.19.150
Meeting Room 1	192.168.19.152	192.168.19.167	255.255.255.240 (/28)	192.168.19.153 - 192.168.19.166
Meeting Room 2	192.168.19.168	192.168.19.183	255.255.255.240 (/28)	192.168.19.169 - 192.168.19.182
Meeting Room 3	192.168.19.184	192.168.19.199	255.255.255.240 (/28)	192.168.19.185 - 192.168.19.198
Server	192.168.19.200	192.168.19.231	255.255.255.224 (/27)	192.168.19.201 - 192.168.19.230

6. VLAN Segmentation of Overall Company

Department	Devices	VLAN ID
Administration	15 computers, 2 printers, 1 scanner	VLAN 10
Sales	25 computers, 3 printers, 1 copier	VLAN 20
IT	10 computers, 1 server, 1 printer	VLAN 30
Development Team	20 computers, 2 servers, 1 high-performance storage	VLAN 40
HR	5 computers, 1 printer	VLAN 50
Meeting Rooms	3 rooms (WAP, video conferencing)	VLAN 60
Guest Wi-Fi	Secure guest network for visitors	VLAN 70

7. Security Considerations

As a Network Consultants team, we have prioritized our client's network security considerations to ensure it is the best and most secure. We have specifically designed the network with security measures to maintain a high level of protection and scalability.
To make this level of protection, we have categorized security measures as follows:

7.1 Security plans for VLAN s

7.2 Security Plans for Firewalls

7.3 Physical Security

7.1 Security plans for VLAN s

1. VLAN Isolation and Segmentation

Purpose:

Reduce the effects of possible attacks on security and stop unauthorized access between departments.

Implementation:

- ✓ Create separate VLANs for every department and functional area.
- ✓ To control and limit traffic between VLANs,
  use Layer 3 switches or routers equipped with access controls.
- ✓ Keep important VLANs like server apart from VLANs used for regular user access.

2. Lists of access controls

Purpose:

Control and restrict traffic flow between VLANs according with previously determined security guidelines.

Implementation:

- ✓ Allow only necessary traffic between VLANs by defining access controls on routers or Layer 3 switches.
- ✓ Prevent unnecessary traffic from entering sensitive VLANs (for as by preventing access from general user VLANs to the Finance VLAN).
- ✓ To stop loss of data, implement access controls to limit incoming traffic from VLANs.

3. Private VLANs

Purpose:

Offer more isolation inside a VLAN; this is particularly helpful in setups where devices or servers must be kept apart from one another while still being able to connect to a main router or firewall.

Implementation:

- ✓ To provide restricted communication among a collection of devices, use community VLANs.
- ✓ To make sure that devices are unable to connect directly with one another, use isolated VLANs.

4. Port Security

Purpose:
Stop illegal devices from using VLAN access ports to connect to the network.

Implementation:

- ✓ To restrict the amount of MAC addresses per port, enable port security on switches.
- ✓ Set up ports such that, if an unauthorized MAC address is discovered, traffic is automatically disabled or restricted.
- ✓ Use sticky MAC addresses to identify and link authorized devices to ports.

5. VLAN Trunking Protocol (VTP) Security

Purpose:
VLAN Trunking Protocol security is preventing unauthorized VLAN changes

Implementation:

- ✓ As an additional security, use VTP password.

6. Regular VLAN Security Audits

Purpose:
To ensure effectiveness of security systems and measures.

Implementation:

- ✓ Conducting regular security checking to check, port security settings, and VLAN segmentation policies.
- ✓ Update VLAN configurations to detect security threats.

7.2 Security Plans for Firewalls

1. Define Security Policies and Rulesets

Purpose:
Clearly define the types of traffic that the firewall will permit or prevent.

Implementation:

- ✓ Make a default deny rule that by default blocks all traffic; only services and ports that are specifically needed are then allowed.
- ✓ Based on business needs, define inbound and outbound rules, making sure that only necessary traffic is allowed.
- ✓ Adopt a least privilege strategy, permitting only the minimum amount of access required to do tasks.

2. Firewall Placement and Zoning

Purpose:
Place firewalls strategically to safeguard important network segments and impose security guidelines.

Implementation:

- ✓ Install firewalls in front of important servers between VLANs, and at other strategic locations.
- ✓ Establish security zones (External and Internal) and use the relevant rules to control traffic flowing between them.

3. Deploy Stateful Inspection

Purpose:
Keep track of the status of running connections and take actions according to the protocol, port, and state.

Implementation:

- ✓ Track active sessions with stateful inspection to make sure that only reliable, established connections are permitted.
- ✓ To end idle sessions and lessen sensitivity to possible attacks, enable session timeouts.

4. Application Layer Filtering

Purpose:
Analyses and filter communications according to certain application protocols to defend against attacks at the application layer.

Implementation:

- ✓ To analyze and filter traffic based on application signatures, enable deep packet inspection (DPI).
- ✓ Disable or prohibit dangerous programs and protocols (such as unapproved, peer-to-peer VPNs).

5. Network Address Translation (NAT)

Purpose:
Maintain IP address space and hide internal network addresses from outside parties.

Implementation:

- ✓ One public IP address can be shared by several devices by using PAT (Port Address Translation).
- ✓ For servers that must be reachable from the outside while protecting other internal addresses, use Static NAT.

6. Management of Virtual Private Networks (VPNs)

Purpose:
Safely link external sites and users to the internal network.

Implementation:

- ✓ Construct VPN tunnels (such as IPsec or SSL VPNs) for site-to-site communications and remote access.
- ✓ Encrypt all VPN connections and use solid verification, such as multi-factor authentication.
- ✓ To guarantee that all traffic goes via the firewall for inspection, use divide tunneling wisely or turn it off.

7. Logging and Monitoring

Purpose:
Constantly keep an eye on firewall activity to identify and address security incidents.

Implementation:

- ✓ Turn on logging for all firewall actions and rules, including traffic that is permitted and prohibited.
- ✓ For centralized monitoring and analysis, connect firewall logs with a SIEM (Security Information and Event Management) system.
- ✓ Set notifications for important situations, such repeated unsuccessful login attempts or breaking the rules.

8. Authentication and Access Control

Purpose:

Restrict unauthorized personnel's access to firewall control interfaces.

Implementation:

- ✓ To gain access to firewall administration, create strong, one-of-a-kind passwords and enable two-factor authentication (2FA).
- ✓ Limit access to management to IP addresses or ranges
- ✓ To grant various levels of access based on user roles

7.3 Physical Security

24/7 Monitoring:

As the Easiest way to hack into a network is to use a physical connection, it is paramount that all sever rooms are monitored using Cameras and have at least fingerprint & and id scanning to restrict entry into server rooms

8.Budget

Hardware and Software	Quantity	Unit Price (LKR)	Total cost (LKR)
1. Hardware			
Wi-Fi router -TP-link TL-MR100	5	21,200	106,000
Synology DS920+ (NAS) (Shared High Performance Storage)	1	1,50,000	150,000
Dell EMC PowerEdge T140 Server	3	1,500,000	4,500,000
StarTech 12U Open Frame Server Rack	3	300,000	900,000
Serial to RJ45 Console Cables	11	3,500	38,500
Cisco SG350-10-K9-EU 10 port switch	6	210,000	1,260,000
Aruba Instant On 1930 24-Port JL684B PoE+ managed Network Switch	4	515,000	2,060,000
Netgear GS752TP 48 Port Gigabit Ethernet Smart Managed Pro Switch	1	725,000	725,000
Patch Cord RJ45 Cat6 Network Cable	2000m	1m=350	700,000
Optical Fiber cable	200m	1m=900	180,000
Ethernet Connectors	200	45	9,000
Fiber Optic Connectors	200	100	20,000
Total Cost			10,648,500

Category	Software	Price (Dollar)	Total cost (LKR)
2. Software			
Network Monitoring	SolarWinds Network Performance	$2,995	Paid
Firewall and Security	Cisco ASA or Firepower	$1,000 (basic model)	Paid
VPN Solutions	Cisco AnyConnect	$8,000 (for 80 users annually)	Paid
Email and Collaboration	Microsoft Exchange Online	$4,800 annually	Paid
File Sharing and Storage	Microsoft SharePoint	$4,800 annually	Paid
Virtualization	VMware vSphere	$995 (base license)	Paid
Total (Paid Solutions To maintain secure)		Approximately $18000 annually	5,400,000

Category	Paid Solution	Cost	Free Alternative	Cost (Free Version)
Network Monitoring	SolarWinds Network Performance	$2,995	Nagios Core	Free
Firewall and Security	Cisco ASA or Firepower	$1,000 (basic model)	pfSense	Free
VPN Solutions	Cisco AnyConnect	$8,000 (for 80 users annually)	OpenVPN	Free
Email and Collaboration	Microsoft Exchange Online	$4,800 annually	Zimbra Collaboration Suite (Open-Source Edition)	Free
File Sharing and Storage	Microsoft SharePoint	$4,800 annually	Nextcloud	Free
Virtualization	VMware vSphere	$995 (base license)	Proxmox VE	Free

Total Cost

1.Hardware and Paid Software

Note:

Paid versions offer more advanced features, better performance, dedicated support, and enhanced security compared to free versions

Hardware Total Cost	10,648,500
Software Total Cost	5,400,000 (annually)
Installation Cost (Hardware +Software) 10percent of Hardware and Software Total Cost	1,064,850
Total Cost	17,113,350

2.Hardware and Free Software

Note:

Free solutions are often not preferable because they may lack dedicated support, advanced features, regular updates, and robust security.

Hardware Total Cost	10,648,500
Software Total Cost	~~5,400,000 (annually)~~ (If we are using free, we can cutdown cost)
Installation Cost (Hardware +Software) 10percent of Hardware and Software Total Cost	1,064,850
Total Cost	11,713,350

As network consultants for Tech World Inc.,

we have designed a robust and scalable network infrastructure to support the company's growth and IT service demands. Our approach includes VLAN segmentation for enhanced security and traffic management, efficient IP address allocation, and strategic deployment of firewalls. We've also integrated essential hardware, such as high-performance servers and managed switches, to ensure reliable and fast communication. In terms of software, we proposed both paid and free alternatives, with a recommendation for paid solutions due to their advanced features, security, and dedicated support, ensuring a highly secure and resilient network. We are confident that this design will meet your current needs and support your future growth effectively.