SLIIT UNI
THE KNOWLEDGE UNIVERSITY

Faculty of Computing

IE1030 – Data Communication Networks
Year 1 Semester 1 (2024)

Network Design Assignment

Group ID: P5-13
Batch Group No: Y1.S1.WD.IT.05.02

Group members:

1. Wickramasinghe H.A.H.E IT24100886
2. Samarasekara S.O.A.N.N IT24102080
3. Jayaisuri L.B.A.H IT24100596
4. Disanayaka K.G.G.S IT24102031
5. Sathsarani M.B.N.K IT24102669

29th of September 2024
Date of Submission

Table of Contents

Index of Tables

Table of Figures

TechWorld Inc. Network Design Documentation

Prepared for: **Techworld Inc**
Prepared by: **P5-13**
Date: **27th of September 2024**

1. Overview

This document shows the proposed network design for TechWorld Inc's new office building. The design is made to provide a robust, secure, and scalable network infrastructure to support the company's current and future IT needs.

2. Network Requirements

Business Requirements

Scalability for Growth:

The network design needs to consider future growth based on the company's projections, such as hiring more employees, adding new departments, and offering additional services.

High Availability and Reliability:

Being a technology company, TechWorld Inc. depends on its IT infrastructure. High availability of network resources is critical to ensuring that business processes remain up and running with minimal downtime.

Remote Access Security:

The network will be required to have a safe method for the employees those who working from home. It has to be safe and they have to travel and connect them to the company resources as if they were on-site.

Inter-departmental Communication:

The network should facilitate easy communication and collaboration among employees within the departments and inter-departments.

Data Security:

The company's sensitive data, customer information, and intellectual property are very crucial and should be protected from unauthorized network access. The network design therefore should have appropriate security such that data breach and other security incidences are not encountered.

Technical Requirements:

Gigabit Ethernet:

All network connections, including connections to workstations, servers, and network devices, should use Gigabit Ethernet in order to provide the necessary bandwidth for both the current and future needs of.

Wireless Standard:

The wireless network should be deployed with the most recent generation Wi-Fi, such as 802.11ac to support high-speed wireless access for mobile devices like using AP – N.

VLAN Segmentation:

VLANs should be in place to segment the network into logical groups, either by department or function, in such a way that it enhances the security and improves network performance.

Firewall Protection:

Deploy firewalls at the network perimeters to control the flow of traffic, deny unauthorized access, and protect the network from external threats.

Virtual Private Network or VPN:

Establish a strong VPN solution to connect remote employees securely to the network.

DHCP and Static IP Addressing:

Use DHCP to automatically assign IP addresses to workstations and other devices, reserving static IP addresses for use with servers, printers, and other critical network devices.

Network Monitoring and Management:

Use appropriate network monitoring utilities along with techniques to proactively identify and address performance issues, security threats, and potential bottlenecks.

An IP-Based Intercom Solution:

This is and IP based PABS intercom connection to the voice only.

3. Network Topology Design

This section details the logical and physical topology of TechWorld Inc.'s new network infrastructure. The design employs a Star-Bus Hybrid topology to ensure scalability, security, and efficient network segmentation.

Logical Topology

As we got two layers, two different typologies will be used in each layer.

- **Access Layer:**

  Access layer contains the departments of HR, IT, Sales, Admin and Development. And also it got a server farm. So the designing team intents to add dedicated switches to each section, and all devices within a department connect directly to that switch. This centralized approach simplifies network management. And troubleshooting within each department. So, we intent to add a star topology to the access layer
- **Bus Topology:**

  The departmental switches are interconnected using a bus topology, creating a backbone. This backbone allows for high-speed data transfer between departments.
- **VLAN Segmentation:**

  Virtual LANs (VLANs) are implemented on top of the physical topology to further segment the network logically. Each department and the server farm are assigned to separate VLANs. This enhances security by isolating traffic between departments, preventing unauthorized access, and improving network performance by reducing broadcast domains.
- **VLAN**
  - VLAN 101: Sales Department
  - VLAN 102: HR Department
  - VLAN 103: Development Team
  - VLAN 104: Administration Department
  - VLAN 105: IT Department
  - VLAN 106: Servers
  - VLAN 107: Intercom

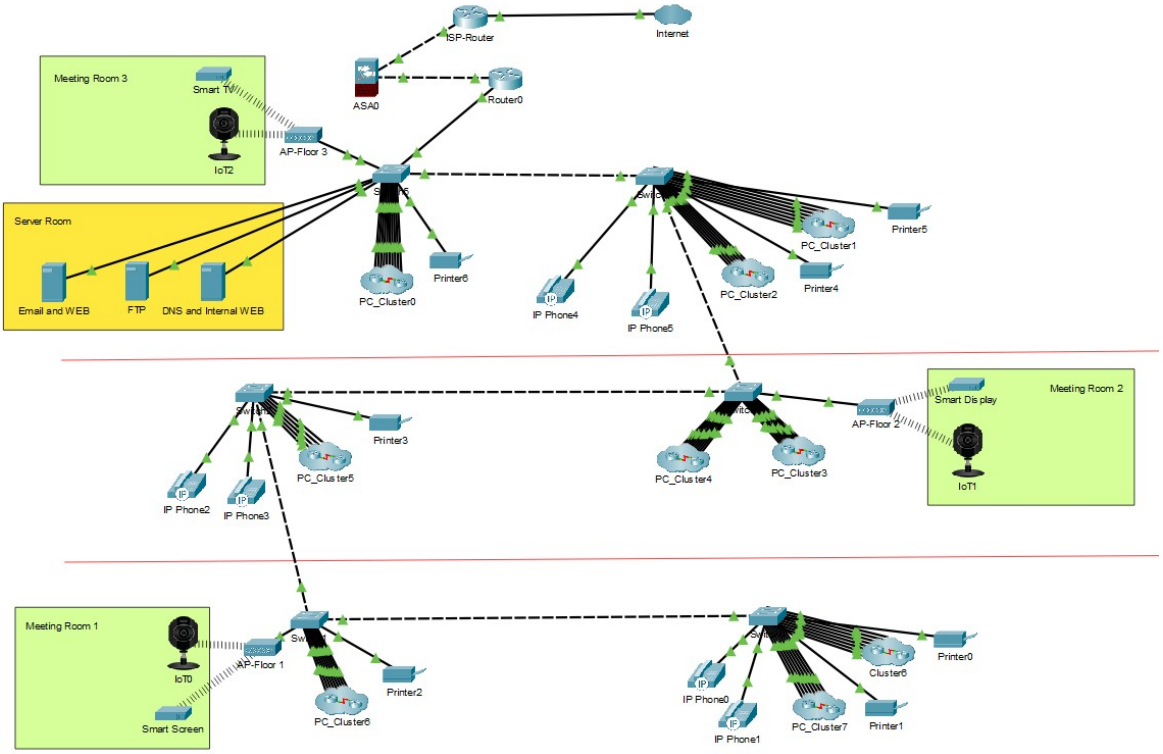


Figure 1: Logical Topology - Simplified Diagram

Physical Topology

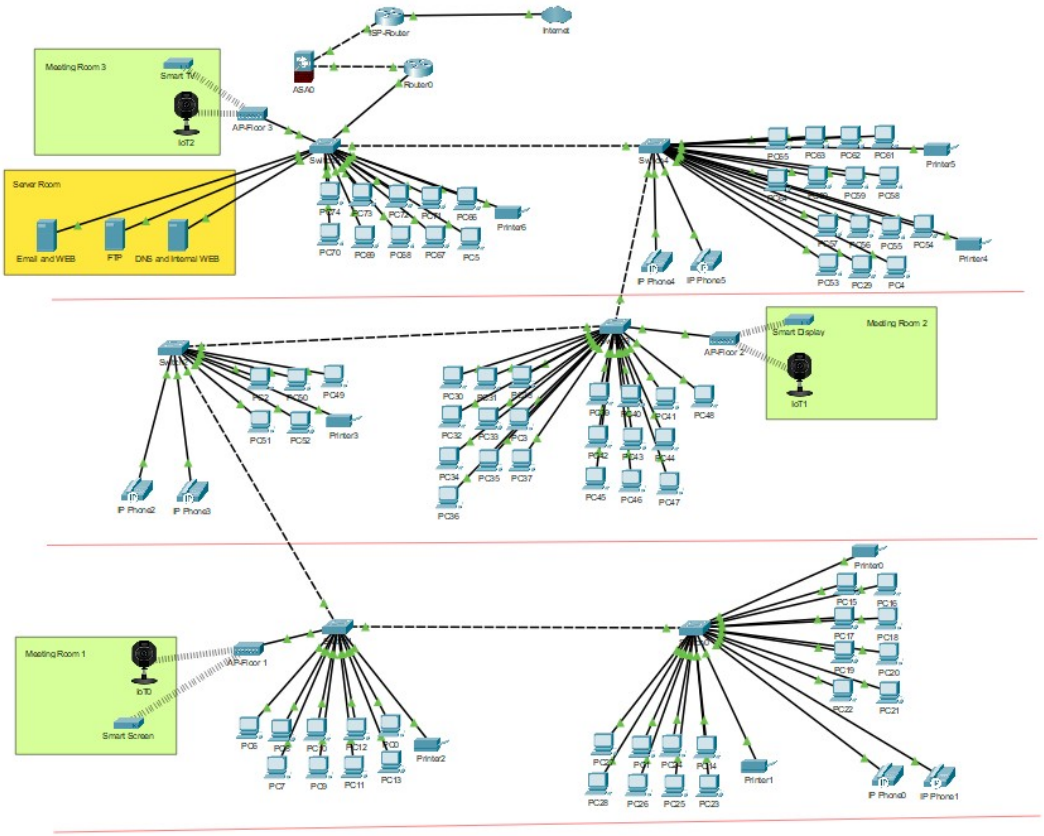


Figure 2: Physical Topology With All the Devices

1. Diagram key:

- **Switches (2960-24TT):** Represented by the rectangular boxes labeled Switch1, Switch2 etc.
- **Access Points (AP-N):** Represented by the icons labeled Access Point1, Access Point2, and Access Point3
- **Router (2911):** Represented by the router icon, labeled Router1 and ISP router
- **Workstations:** Represented by the computer icons (PC1, PC2, ……, etc.).
- **Servers:** Represented by the server icons (Server1, Server2, Server3).
- **Intercom:** Represented by the IP Phone icons (IP Phone1, IP Phone2 etc)

2. Physical Layout:

- **Three Floors:** The network spans three floors in the office building.
- **Switch and AP Placement:** Each floor has two switches and one access point strategically placed to provide optimal coverage and connectivity.
- **Router Location:** The router, which provides the internet connection and the network traffic managements, is located on the 3rd floor and is connected to one of the switches on that floor.
- **Servers:** The three servers are grouped together in a server room or rack, likely on the same floor (3rd floor) as the router, and connected to their dedicated switch.

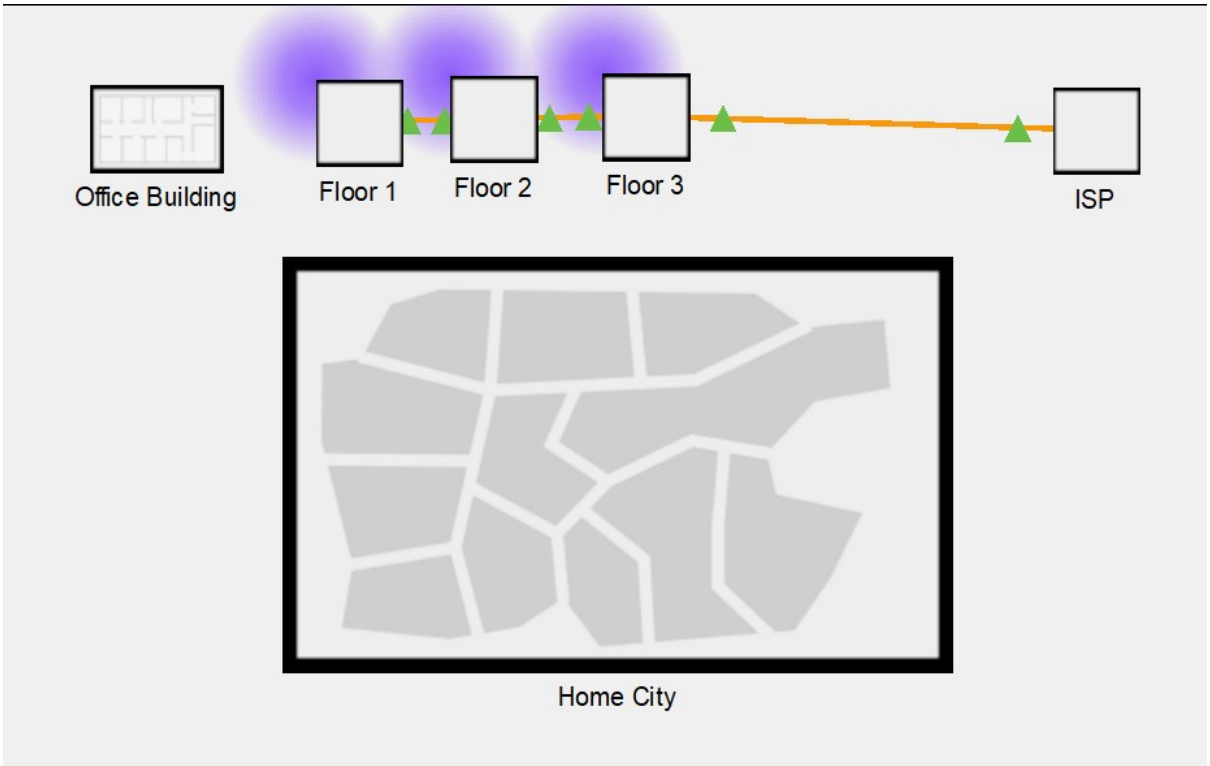


Figure 3: Physical Structure

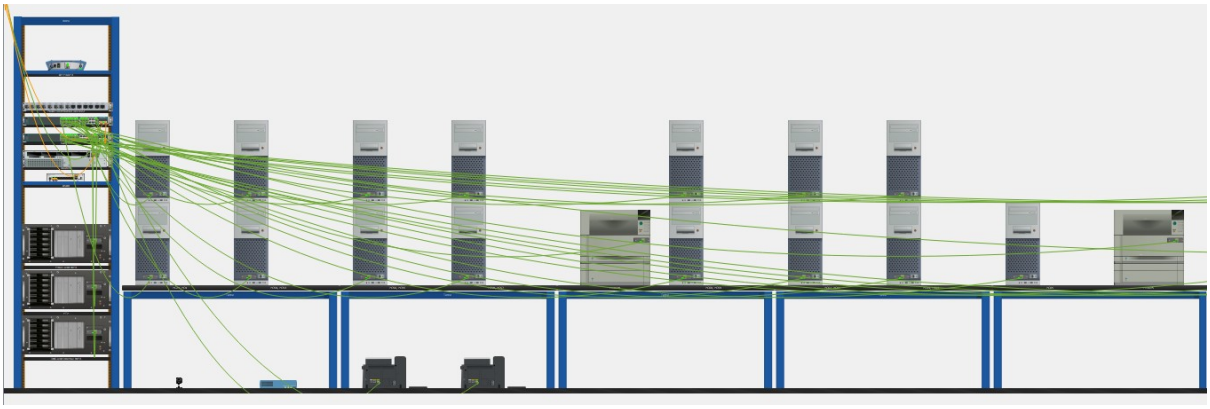


Figure 4: Floor_3 in the Physical mode

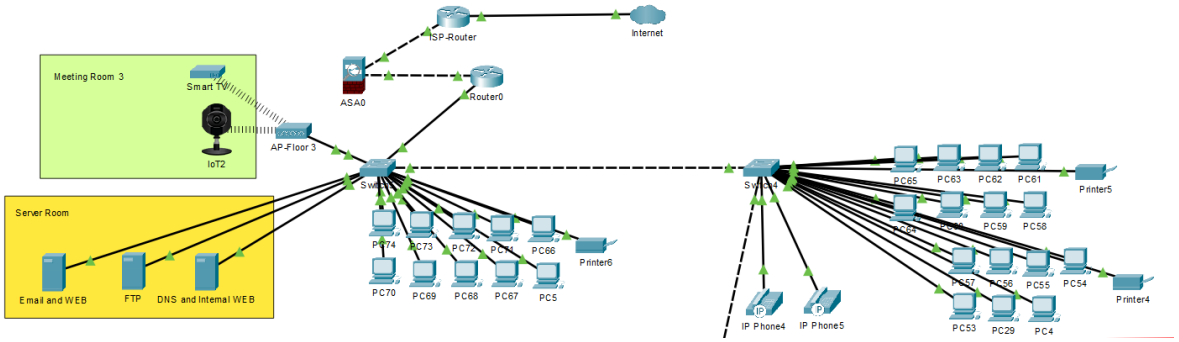


Figure 5: Floor_3 in Logical Mode

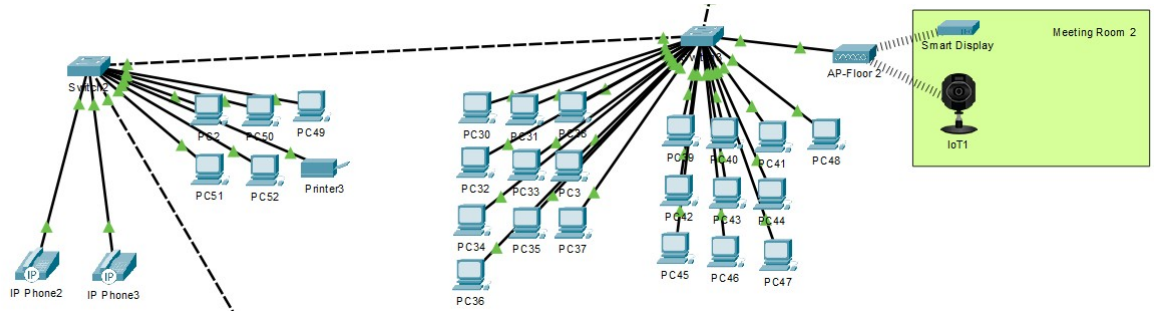


Figure 6: Floor_2 in Logical Mode

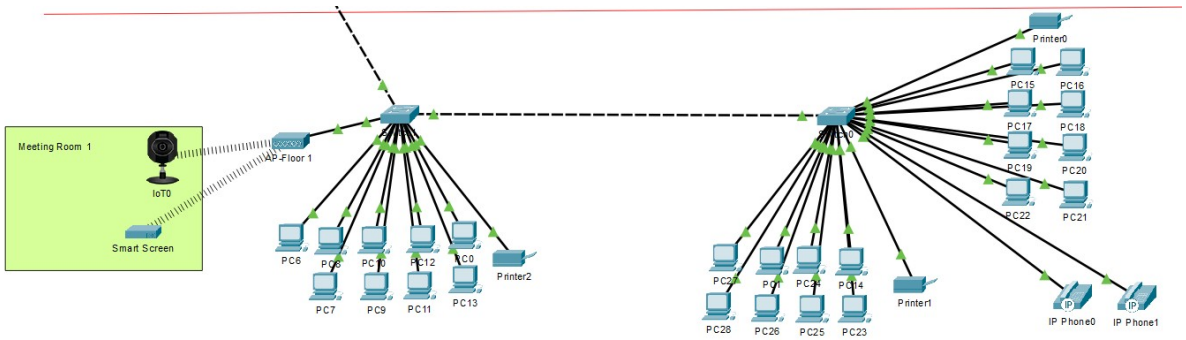


Figure 7: Floor_1 in Logical Mode

4. Why to choose?

Cisco Catalyst 2960-X 24-Port Gigabit Ethernet Switch

The Cisco Catalyst 2960X 24-port Gigabit Ethernet switch is a good choise for TechWorld Inc.'s network infrastructure, by considering scalability, performance, security, scalability, and manageability.

1. High-Performance Connectivity:

- **Gigabit Ethernet throughout:** This switch supports Gigabit Ethernet speeds on all 24 ports, providing higher bandwidth.
- **Power over Ethernet Options:** Many models in the 2960-X series offer Power over Ethernet, a feature that supplies both power and data over a single cable. This reduces cabling costs and minimizes extra cabling clutter.

2. Advanced Security Features:

- Access Control Lists Managing (ACLs)
- Port Security for preventing unauthorized devices from accessing the network.
- DHCP Snooping

3. Cost Effectiveness:

- **Right-Sized for Needs:** The 2960-X series offers the right mix of a plethora of features and real-world affordability to provide enterprise-class functionality without the corresponding enterprise-class price seen on more advanced models.
- **Reduced Downtime:** The robustness of the feature set, in terms of reliability and management capability, tends to minimize network downtime to directly affect productivity and the bottom line of TechWorld Incorporated.

Figure 8: Cisco Catalyst 2960-X 24-Port Gigabit Ethernet Switch

Cisco 2911 Router

Here's why the Cisco 2911 is a good choice, and why it does not make much of a difference to have an exact sub-model in Packet Tracer:

- Enough features for a medium-sized network:
  The 2911 has been endowed with adequate routing, switching, security, and WAN connectivity for a network for a medium-sized company like TechWorld Inc., such as:

- Supporting More Functions:
  - Such as for VLANs ACL's, NAT, VPN (Software based VPN capabilities)
  - WAN Connectivity
  - PoE

- Scalability :
  This model had 3 Gigabit Ethernet ports named Gig0/0, Gig0/1, Gig0/2 for a high speed connectivity

- Memory and Traffic Load:
  This model Have a higher processing speed and a large memory.

Figure 9: Cisco 2911 Router

5. IP addressing scheme

The IP addressing system describes how devices in a network are given distinct IP addresses so they may interact with one other. In order to arrange devices logically, this includes establishing the IP range, subnet mask, and gateway. By dividing traffic using subnets or virtual local area networks (VLANs), a well-organized plan prevents conflicts and increases network security.

HR Department

This is the Human resource department of Techworld InC. It uses 6 devices. Considering the future growth of the company, its subnet usable for 16 hosts. And also we design a DHCP pool PC allocation for this subnetwork which have showed in the below table which includes 10 IP's for the pool and 4 excluded IP addresses for Printers copiers.

Devices	5 computers, 1 printer (6 hosts)
Network Address	192.168.86.240/28
Broadcast Address	192.168.86.255/28
Wildcard Address	0.0.0.15
Subnet Mask	255.255.255.240
Usable Range	192.168.86.241/28 – 192.168.86.254/28 (16 hosts)
Default Geatway	192.168.86.254/28
DHCP Pool	192.168.86.241/28 – 192.168.86.250/28 (10 hosts)
DHCP excluded-address	192.168.86.251/28 - 192.168.86.254/ 28 (4 hosts)
Vlan ID	102

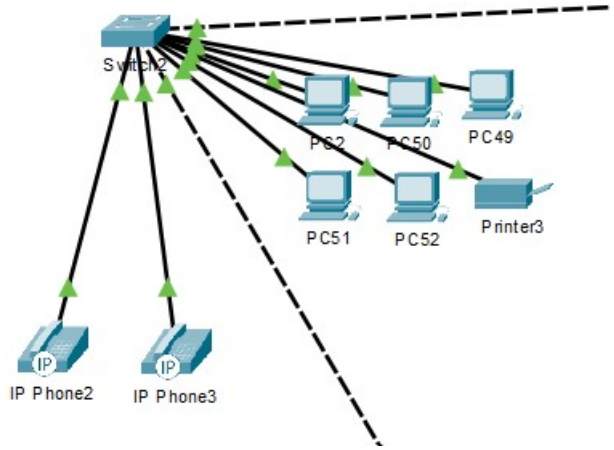


Figure 10: HR Department Logical Structure

IT Department

The IT department of Tecworld InC. It handles all the IT related connections and rectifies issues inside the company. It uses 11 hosts. By considering the future growth of the company this subnet can be expandable up-to 30 hosts. DHCP pool was also provided for the PC allocations in the Subnetwork. Including 20 IP's for the pool and excluding 10 IP addresses for Printers copiers and other.

Devices	10 computers, 1 printer (11 hosts)
Network Address	192.168.86.160/27
Broadcast Address	192.168.86.191
Wildcard Address	0.0.0.31
Subnet Mask	255.255.255.224
Usable Range	192.168.86.161/27 – 192.168.86.190/27 (30 hosts)
Default Geatway	192.168.86.190/27
DHCP Pool	192.168.86.161/27 – 192.168.86.180/27 (20 hosts)
DHCP excluded-address	192.168.86.181/27 – 192.168.86.190/27 (10 hosts)
Vlan ID	105

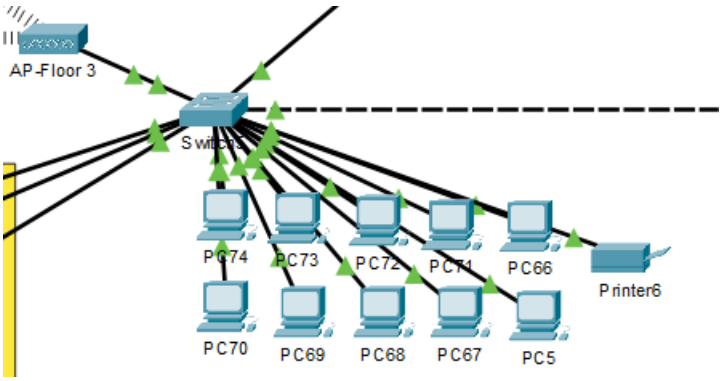


Figure 11: IT Department Logical Structure

Sales Department

Sales department of Techworld Inc. is responsible for managing the buissness related works and looking after the buissness statistics. This department uses 29 hosts, considering the future growth of the company. This can be expandable up to 62 hosts. We intend to provide DHCP pool for the PC allocation for this subnetwork and extended DHCP for the printers and the copier.

Devices	25 computers, 3 printers, 1 copier (29)
Network Address	192.168.86.0/26
Broadcast Address	192.168.86.63/26
Wildcard Address	0.0.0.63
Subnet Mask	255.255.255.192
Usable Range	192.168.86.1/26 – 192.168.86.62/26 (62 hosts)
Default Geatway	192.168.86.62/26
DHCP Pool	192.168.86.1/26 – 192.168.86.49/26 (49 hosts)
DHCP excluded-address	192.168.86.50/26 – 192.168.86.62/26 (13 hosts)
Vlan ID	101

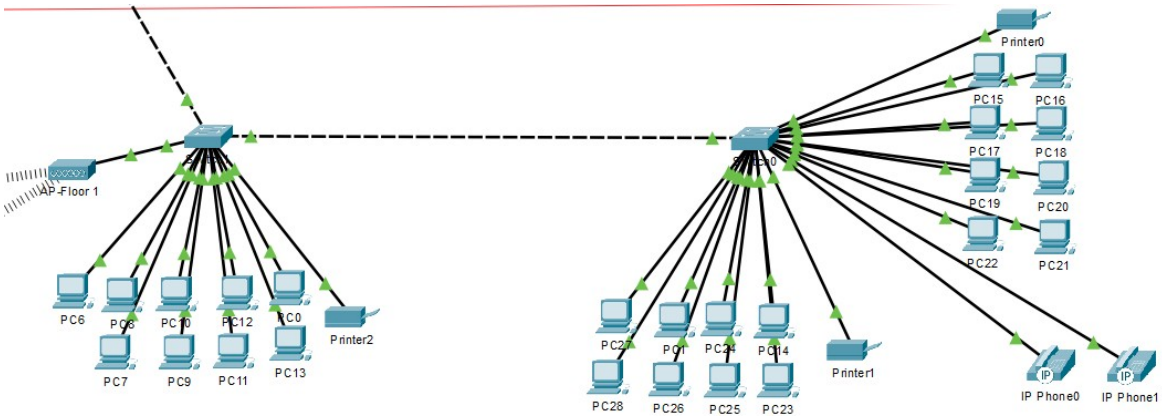


Figure 12: Sales Department Logical Structure

Administration Department

Administration department is the in charge sub organization which looks after the governing of the Techworld Inc. For this department, tend to uses 18 hosts. By considering the future growth of the company this subnet can be expandable upto 30 hosts. DHCP pool was also provided for the PC allocations in the Subnetwork. Including 21 IP's for the pool and excluding 9 IP addresses for Printers copiers and other.

Devices	15 computers, 2 printers, 1 scanner (18)
Network Address	192.168.86.128/27
Broadcast Address	192.168.86.159/27
Wildcard Address	0.0.0.31
Subnet Mask	255.255.255.224
Usable Range	192.168.86.129/27 – 192.168.86.158/27 (30 hosts)
Default Geatway	192.168.86.158/27
DHCP Pool	192.168.86.129/27 – 192.168.86.149/27 (21 hosts)
DHCP excluded-address	192.168.86.150/27 – 192.168.86.158/27 (9 hosts)
Vlan ID	104

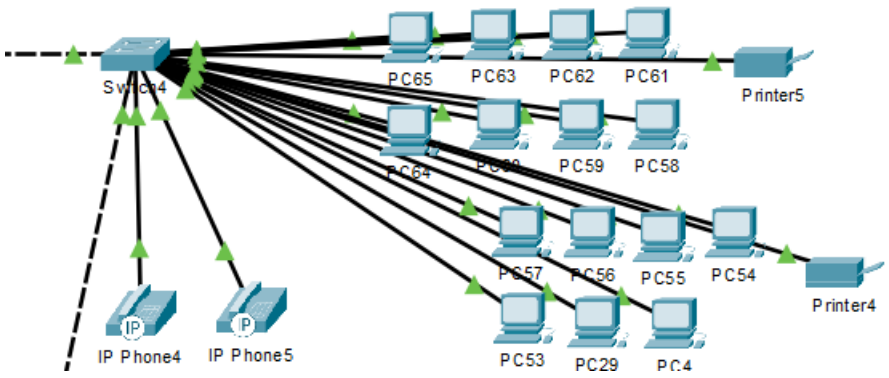


Figure 13: Administration Department Logical Structure

Development Team

As an IT related company Techworld Inc uses a team to provide solutions for its customers' problems. So, for this development team uses 20 hosts. Considering the future growth of the company, this can be expandable up to 62 hosts. We intend to provide DHCP pool for the PC allocation for this subnetwork and excluded addresses for printers or other devices.

Devices	20 computers
Network Address	192.168.86.64/26
Broadcast Address	192.168.86.127/26
Wildcard Address	0.0.0.63
Subnet Mask	255.255.255.192
Usable Range	192.168.86.65/26 – 192.168.86.126/26 (62 hosts)
Default Geatway	192.168.86.126/26
DHCP Pool	192.168.86.65/26 – 192.168.86.115/26 (52 hosts)
DHCP excluded-address	192.168.86.116/26 – 192.168.86.126/26 (10 hosts)
Vlan ID	103

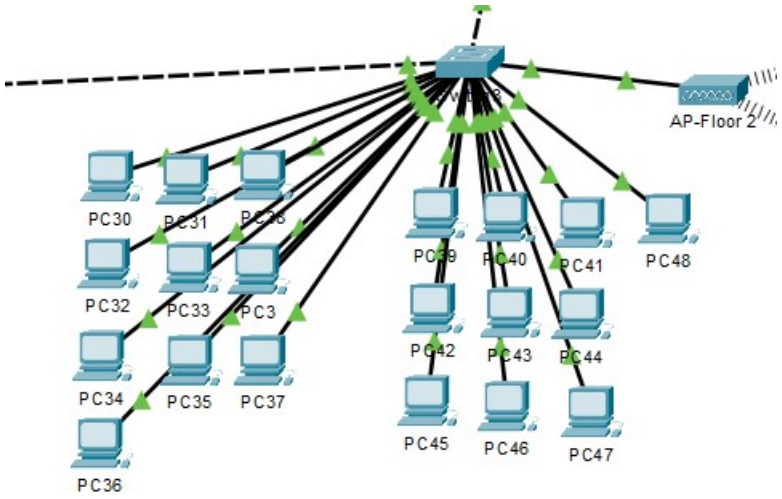


Figure 14: Development Team Logical Structure

Servers

In the TechWorld Inc., There have to be a server room for DNS and Internal Web Services, External Web Services and Email Service for the company, and FTP for high speed sheared memory… In here The Development have only access to the FTP server and the DNS & Internal Wb server, While the IT department having access for the External Web and the Email server. The Access Level control rules are given below….

Devices	3 Servers (2 - from Development, 1 - from IT)
Network Address	192.168.86.224/28
Broadcast Address	192.168.86.239/28
Wildcard Address	0.0.0.15
Subnet Mask	255.255.255.240
Usable Range	192.168.86.225/28 – 192.168.86.238/28 (14 hosts)
Default Geatway	192.168.86.238/28
Vlan ID	106

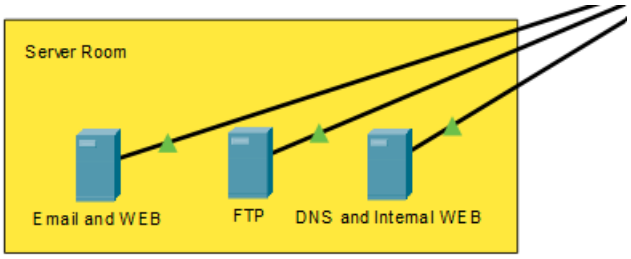


Figure 15: Server Room Logical Structure

Meeting rooms

In each floor of the Techworld Inc. Have a meeting room for the conferences and discussions. It is not necessary to have another subnetwork for the meeting room devices. All the meeting room devices such as wireless web camera and a smart wireless screen has connected to the access point of the each floor. If there is another device to connect it can use the WPA2-PSK encryption to connect...

- 1st Floor Meeting room – Sales Department
- 2nd Floor Meeting room – Development Department
- 3rd floor Meeting room – Administration Department

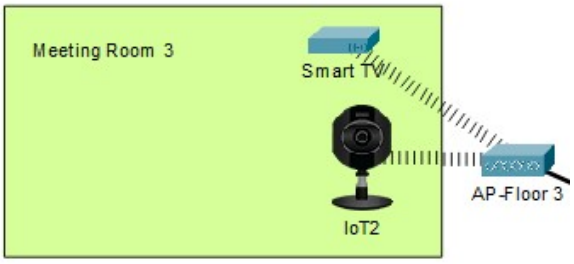


Figure 16: Meeting Room_3 Logical Structure

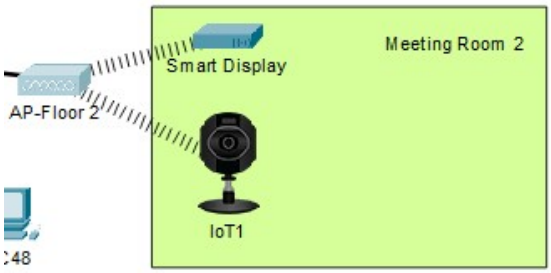


Figure 17: Meeting Room_2 Logical Structure

IP-Intercoms

In Each floor there is an IP based PABS intercom voice connection represented by the IP phone and The IP-Intercom has separated to another VLAN which allows to add 14 hosts. In this subnetworks there is no DHCP configuration because It have to be Static IP's.

- Reception – 192.168.86.209/28
- Sales Department – 192.168.86.210/28
- HR Department – 192.168.86.211/28
- Development team – 192.168.86.212/28
- Administration Department – 192.168.86.213/28
- IT Department – 192.168.86.214/28

Devices	IP Phone
Network Address	192.168.86.208/28
Broadcast Address	192.168.86.223/28
Wildcard Address	0.0.0.15
Subnet Mask	255.255.255.240
Usable Range	192.168.86.209/28 – 192.168.86.222/28 (14 hosts)
Default Geatway	192.168.86.222/28
Vlan ID	107

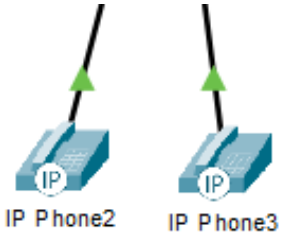


Figure 18: Voice Intercom

VLAN Table

VLAN ID	Department/Purpose	Usable IP Address Range
101	Sales	192.168.86.1/26 – 192.168.86.62/26
102	HR	192.168.86.241/28 – 192.168.86.254/28
103	Development	192.168.86.65/26 – 192.168.86.126/26
104	Admin	192.168.86.129/27 – 192.168.86.158/27
105	IT	192.168.86.161/27 – 192.168.86.190/27
106	Servers	192.168.86.225/28 – 192.168.86.238/28
107	Intercom Voice	192.168.86.209/28 – 192.168.86.223/28

Trunk ports

- Every Switch Gigabit Ethernet Ports (Gig0/1, Gig0/2) has configured trunked and allowed all VLANS.

Fiber Connectivity:

To this network we planned to use Multi-mode Fiber cable connection between switches to switch and switch to routers. Because it gives a higher bandwidth and can operate with a small distance. For this network, we planned to use Dual link LC-LC Multimode cables.

Figure 19: D-Link- LC-LC Multimode fiber cable

LC SFP:

To connect the fiber cable to the Cisco router 2911 and the Cisco Catalyst 2960-X 24-Port Gigabit Ethernet Switch we choose GLC-SX-MM SFP connector.

Figure 20: LC SFP

6. Security considerations

VLAN Segmentation

We disconnected inter vlan routing from the router. So it won't allow communicating through the vlans. It's a security step to take in this project. Only from the access control levels (ACL) can permit for want resources for each host. Access control levels (ACLs) determine the permissions for each host regarding the resources they can access.

ACL (Access Control Lists)

ACLs are used to filter traffic and ensure the implementation of security policies in an environment by denying or permitting certain types of traffic based on the source and destination IP addresses, protocols, and ports. Below are all the key rules associated with extended ACLs.

Rule 1

```
ip access-list extended BLOCK_DEVELOPMENT_TO_OTHERS_N_ALLOW_SERVER
 permit ip 192.168.86.64 0.0.0.63 host 192.168.86.225
 permit ip 192.168.86.64 0.0.0.63 host 192.168.86.226
 deny ip 192.168.86.64 0.0.0.63 192.168.86.240 0.0.0.15
 deny ip 192.168.86.64 0.0.0.63 192.168.86.160 0.0.0.31
 deny ip 192.168.86.64 0.0.0.63 192.168.86.0 0.0.0.63
 deny ip 192.168.86.64 0.0.0.63 192.168.86.128 0.0.0.31
deny ip 192.168.86.64 0.0.0.63 192.168.86.224 0.0.0.15
 permit ip any any
```

Objective: Deny access to the Development Department to the other Vlans and Only allow to access to the internal web server, DNS server and the File Transfer Server

Rule 2:

```
ip access-list extended BLOCK_HR_TO_OTHERS
 deny ip 192.168.86.240 0.0.0.15 192.168.86.64 0.0.0.63
 deny ip 192.168.86.240 0.0.0.15 192.168.86.160 0.0.0.31
 deny ip 192.168.86.240 0.0.0.15 192.168.86.0 0.0.0.686
 deny ip 192.168.86.240 0.0.0.15 192.168.86.128 0.0.0.31
deny ip 192.168.86.240 0.0.0.15 192.168.86.224 0.0.0.15
 permit ip any any
```

Objectives: Block HR department traffic to Others, but if there are any other IP permitting is allowed to go on.

Rule 3:

```
ip access-list extended BLOCK_SALES_TO_OTHERS
 deny ip 192.168.86.0 0.0.0.63 192.168.86.64 0.0.0.63
 deny ip 192.168.86.0 0.0.0.63 192.168.86.160 0.0.0.31
 deny ip 192.168.86.0 0.0.0.63 192.168.86.240 0.0.0.15
 deny ip 192.168.86.0 0.0.0.63 192.168.86.128 0.0.0.31
deny ip 192.168.86.0 0.0.0.63 192.168.86.224 0.0.0.15
 permit ip any any
```

Objectives: Block Sales department traffic to Others, but if there are any other IP permitting is allowed to go on.

Rule 4:

```
ip access-list extended BLOCK_ADMIN_TO_OTHERS
 deny ip 192.168.86.128 0.0.0.31 192.168.86.64 0.0.0.63
 deny ip 192.168.86.128 0.0.0.31 192.168.86.160 0.0.0.31
 deny ip 192.168.86.128 0.0.0.31 192.168.86.240 0.0.0.15
 deny ip 192.168.86.128 0.0.0.31 192.168.86.0 0.0.0.63
deny ip 192.168.86.128 0.0.0.31 192.168.86.224 0.0.0.15
 permit ip any any
```

Objectives: Block Admin department traffic to Others, but if there are any other IP permitting is allowed to go on.

Rule 5:

```
ip access-list extended BLOCK_IT_TO_OTHERS_N_ALLOW_SERVER
 permit ip 192.168.86.160 0.0.0.31 host 192.168.86.237
 deny ip 192.168.86.160 0.0.0.31 192.168.86.240 0.0.0.15
 deny ip 192.168.86.160 0.0.0.31 192.168.86.0 0.0.0.63
 deny ip 192.168.86.160 0.0.0.31 192.168.86.64 0.0.0.63
 deny ip 192.168.86.160 0.0.0.31 192.168.86.128 0.0.0.31
 deny ip 192.168.86.160 0.0.0.31 192.168.86.224 0.0.0.15
```

Objectives: Block IT department traffic to Others, but if there are any other IP permitting is allowed to go on.

Rule 6:

```
ip access-list extended BLOCK_INTERCOM_TO_OTHERS
 deny ip 192.168.86.208 0.0.0.15 192.168.86.240 0.0.0.15
 deny ip 192.168.86.208 0.0.0.15 192.168.86.0 0.0.0.63
 deny ip 192.168.86.208 0.0.0.15 192.168.86.64 0.0.0.63
 deny ip 192.168.86.208 0.0.0.15 192.168.86.128 0.0.0.31
 deny ip 192.168.86.208 0.0.0.15 192.168.86.224 0.0.0.15
 deny ip 192.168.86.208 0.0.0.15 192.168.86.160 0.0.0.31
```

Objectives: Block Intercom voice to the other departments and only allow traffic for inter connections IP PABS intercom voice connection

Then these ACLs are applied to the router interfaces to control the flow of traffic between VLANs and between the internal network and the internet. These rules make the traffic reduced and keep them separated. This greatly limits the ability to access the system via unauthorized use.

Internal Access:

Access to IT

- Server 1 – Email, External Web hosting like https://techworld.com/

Access to Development

- Server 2- File Shearing
- Server 3- DNS and Internal web server for the development team and records.

External Access:

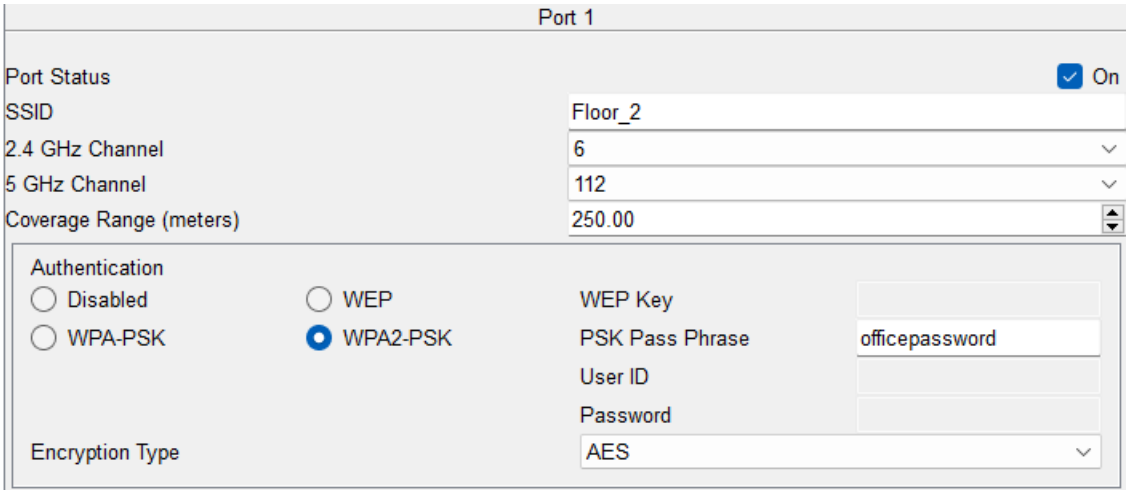
VPN from the Email server and if it is a development team use he has special access to the DNS server, FTP Server and the Internal WEB server

Wireless Security:

The wireless network shall utilize WPA2-PSK encryption, which is considered state-of-the-art in wireless security, to send and receive data wirelessly. WPA2-PSK is highly recommended due to its robust encryption, as unauthorized devices cannot penetrate the network, let alone transmit data wirelessly.

Password Policy:

- **Strong Passwords:** We will provide a better security by giving strong passwords like 12 characters length, Symbols, Numbers etc.
- **Regular Change:** Passwords are changed on a regular basis, such that every 90 days the risk of password compromise decreases. Besides, if multiple SSIDs are configured, then each department may have its separate password for wireless network use, thus providing better control and compartmentalization.



Firewall:

A Cisco ASA 5506-X firewall is applied to protect the network against external threats. Basic access control and NAT rules are configured on the firewall to ensure safe and efficient internet access.

- permit ip any any eq 443 ! For SSL VPN traffic (port 443)
- permit udp any any eq 500 ! For IPsec VPN (IKE - port 500)
- permit udp any any eq 4500 ! For IPsec VPN (NAT-T - port 4500)

NAT:

Through the firewall, we employ NAT filtering. Because internal devices can use a public IP address to spoof their location and access the internet. The network is further secured since external systems are unaware of the internal IP addresses.

- Router0(config)# interface GigabitEthernet0/1 // WAN interface
- Router0(config-if)# ip nat outside
- Router0(config-if)# exit

- Router0(config)# interface GigabitEthernet0/0 // LAN interface
- Router0(config-if)# ip nat inside
- Router0(config-if)# exit

Extended ACL for NAT traffic

```
ip access-list standard NAT-TRAFFIC
 permit 192.168.86.240 0.0.0.15
 permit 192.168.86.160 0.0.0.31
 permit 192.168.86.0 0.0.0.63
 permit 192.168.86.128 0.0.0.31
 permit 192.168.86.64 0.0.0.63
 permit 192.168.86.224 0.0.0.15
 deny 192.168.86.208 0.0.0.15
```

7. Scalability and Flexibility

Future Growth:

We consider a major attention on scalability. So the infrastructure is able to support growth over a period of time without major revamps. Some of the important features that mark this design include:

Modular Switches:

We have chosen the Cisco 2960 switches, which can easily be expand the network by adding more switches by connecting Gigabit Ethernet ports which gives a higher bandwidth. This enables the network to grow without the need to replace the core infrastructure.

Expansion with larger subnets:

The IP addressing scheme 192.168.86.0/24 is utilized for larger subnetting by selecting the appropriate device count and considering future growth. For example, using /26 or /27 subnets allows for a host range of up to 64 addresses, which is suitable for departments that require support for at least 20 devices. The advantage of this approach is that it enables the addition of more devices without necessitating changes to the IP schema.

Reserved IP address Space:

We reserve IP address ranges on the subnetwork for potential future use, such as for additional servers, printers, and other network devices. We have also created a DHCP pool for employee computers and established excluded DHCP pools for printers, copiers, and similar devices to ensure easy access for employees. This approach ensures effective address management and facilitates future expansion with minimal hassle.

Rack Space and Cable Management:

The physical infrastructure includes extra rack space for additional devices, such as new servers, routers, and switches. These devices are organized on well-managed patch panels, which facilitate ease of access and minimize the need for reorganization. As the organization grows and incorporates more IoT devices, the network has been structured to accommodate these devices securely and efficiently.

Scalability and flexibility have been brought into our network in order to meet immediate expansion and long-term expansion requirements, whether it is to support the ever-increasing numbers of IoT devices or other emerging technologies.

8. Budgeting

Pricing for basic Components

Below is a preliminary cost breakdown of key components for the network and office setup. Please note that the pricing is subjective and based on an analysis of current market conditions, which may change over time. Final prices may be adjusted based on market fluctuations and specific vendor offerings.

1. Network Equipment

Table 1: Table of Network Equipment Budget

Component	Model	Unit Price	Qty	Estimated Price (LKR)
Switch	Cisco 2960	258,000.00	6	1,548,000.00
Routers	Cisco 2911	550,200.00	2	1,100,400.00
Access Points	Cisco AP-N	125,000.00	3	375,000.00
Firewall	Cisco Firewall 5506-X	384,000.00	1	384,000.00
Server Controllers		715,000.00	3	2,145,000.00
Fiber Cabling (m)		950.00	500	475,000.00
Copper Straight-Through Cables (m)		535.00	1000	535,000.00
Total Estimated cost for Network Equipment				**6,562,400.00**

The Unit Prices Can Be Change due to the **Dollar rate and +tax

2. Installation and Configuration

Table 2: Table of Installation and Configuration Budget

Service	Estimated Price (LKR)
Installation & Configuration	1,568,000.00
Rack Mounting & Accessories	386,000.00
Patch Panels (Fiber & Copper)	480,000.00
Total Estimated Cost for I&C	**2,434,000.00**

The Unit Prices Can Be Change due to the **Dollar rate and +tax

3. Office Equipment

Table 3: Table of Office Equipment Budget

Item	Model	Unit Price	Qty	Estimated Price (LKR)
PC	High Speed(i7/Ryzen7)	330,000.00	32	10,560,000.00
	Average(i5/Ryzen5)	210,000.00	48	10,080,000.00
Meeting Cameras	Integrated Web Cam	7,500.00	3	22,500.00
Projectors	Hitachi	158,700.00	3	476,100.00
Printers	Canon	78,900.00	10	789,000.00
Copier	Canon	56,000.00	3	168,000.00
Domain and Web Services (monthly)	HostGator(Business Plan)	9,000.00	1	9,000.00
Total Estimated Cost for Office Equipment				**22,104,600.00**

The Unit Prices Can Be Change due to the **Dollar rate and +tax

Table 4: Table of Total Estimation

Purpose	Final Estimated Cost (LKR)
Network Equipment	6,562,400.00
Installation and Configuration	2,434,000.00
Office Equipment	22,104,600.00
Total Estimation for the Project	**31,101,000.00**

The Unit Prices Can Be Change due to the **Dollar rate and +tax

Key Point End

- **Market Variability:** All prices quoted in the following discussion are market and vendor prices prevailing at the time of this publication. These are liable to change with any fluctuation in the cost of components, exchange rates, or special promotions by vendors.
- **Final Pricing:** The final prices depend upon the time of actual purchase, choice of vendor, and any additional services or customization required.
- **Customizations:** Any additional items or services not listed above such as ongoing support, license software or specific installation requirements would add to the overall cost.

9. Conclusion

The subsequent design offers a robust, scalable, and secure IT infrastructure for TechWorld Inc., considering both present needs and future growth: A design based on Cisco networking technologies has the following key strengths:

- **Scalability and Flexibility:**

  The implementation of VLANs, a structured IP addressing scheme, and scalable routing and switching equipment will facilitate network expansion as TechWorld Inc. grows, enabling the unlimited addition of new users, departments, and services.

- **Improved Security:**

  Connections with the company network get secured and encrypted with the remote access. And also ACLs and firewalls will be serving as gatekeepers to regulate traffic flow between department and further restricting access to critical resources.

- **Improved Network Performance:**

  Segmentations that use VLANs enhance performance by limiting traffic towards particular departments and reducing unessential broadcasts across the network. Because of that, the security status of the network is improved

- **Centralized Management:**

  The overall infrastructure features centralized control through Cisco devices and network management tools. This facilitates configuration, monitoring, and troubleshooting, simplifying network administration. The design has been carefully crafted to future-proof the network by supporting wireless connectivity and integrating IoT devices, among other features. This approach ensures that the network can adapt to evolving technologies and business requirements.

TechWorld Inc.'s holistic approach to network infrastructure establishes a strong foundation for continued success by providing the necessary connected environment, ensuring data security, and offering the flexibility to meet the challenges posed by future technological advancements.

10. References

Cisco
https://www.cisco.com/c/en/us/support/index.html
https://www.netacad.com/

Routers, Switches, Access Points, Firewall

https://www.cisco.com/c/en/us/support/routers/2900-series-integrated-services-routers-isr/series.html

https://www.cisco.com/c/en/us/support/switches/catalyst-2960-x-series-switches/series.html

https://www.cisco.com/site/us/en/products/networking/wireless/access-points/index.html

https://www.cisco.com/c/en/us/support/security/asa-firepower-services/series.html

Budgeting

https://www.ubuy.com.lk/en/search/?q=Cisco

https://www.amazon.com/stores/Cisco/Cisco/page/475E0681-58B9-47D7-A2DB-467DE0F3B852