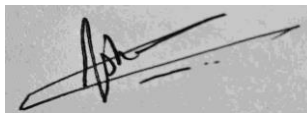


***A signed copy of this form must be submitted with every assignment.  
If the statement is missing your work may not be marked.  
For Level 7 assignments, please use the separate Level 7 Candidate  
Statement of Own Work form instead of this one.***

### **Student Declaration**

I confirm the following details:

<b>Candidate Name:</b>	ISHAN BAPARDEKAR
<b>Candidate ID Number:</b>	213062
<b>Qualification:</b>	L4DC
<b>Unit:</b>	COMPUTER NETWORKS
<b>Centre:</b>	FUT004
<b>Word Count:</b>	2939
<p>I have read and understood both NCC Education's <i>Academic Misconduct Policy</i> and the <i>Referencing and Bibliographies</i> document. To the best of my knowledge my work has been accurately referenced and all sources cited correctly.</p> <p>I confirm that I have not exceeded the stipulated word limit by more than 10%.</p> <p>I confirm that this is my own work and that I have not colluded or plagiarised any part of it.</p>	
<b>Candidate Signature:</b>	
<b>Date:</b>	April 20, 2025

## Table of Contents

<b>Task 1 project requirement analysis</b> .....	<b>1</b>
Key requirements for LAN design .....	2
Analysis of Growth Plans, Scalability Requirements, and Network Traffic .....	3
 <b>Task 2 - Network Topology Diagram</b> .....	<b>4</b>
Floor plan layout .....	5
Network topology .....	6
 <b>Task 3 selection and specification</b> .....	<b>7</b>
List of Required Networking Equipment and Specifications .....	8
Create a table which justifies your items based on RSP .....	9
 <b>Task 4 – IP Addressing and Subnetting</b> .....	<b>10</b>
IP Addressing Plan .....	11
Subnetting details .....	12
 <b>Task 5 security design</b> .....	<b>13</b>
Identify Potential Security Threats and Vulnerabilities .....	14
Design a Security Plan that includes Security Features, Tools, and Controls .....	15
 <b><u>Task 6 – Network Management and Monitoring</u></b> .....	<b>16</b>
Identify Tools and Software for Network Monitoring and Performance Analysis .....	17
Explain How You Will Ensure Network Reliability and Uptime .....	18
 <b>References</b> .....	<b>19</b>

### **Task 1 - Project Requirements Analysis – 10 marks**

Develop a detailed analysis of the project requirements based on the scenario provided.

- a) Identify key requirements for the LAN design, including the number of employees, types of devices and specific needs of different departments. (5 marks)
- b) Analyse the company's growth plans and scalability requirements and expected network traffic. Identify high-bandwidth applications and services used by the company and explain how this impacts the network design. (5 marks)

## **Task 1 project requirement analysis**

### **A) Key requirements for LAN design:**

#### **1. Number of employees and expected rise**

- The current workforce comprises 150 employees, with projected growth to 300 employees in future.
- Each employee will likely use one or more devices, including:
  - ❖ Desktops or laptops (for development and office work)
  - ❖ Mobile devices (smartphones, tablets)
  - ❖ VoIP phones (for internal and external communication)  
*Pearson, 2017.*

#### **2. Number of routers (wired /wireless)**

- Wired connections are needed for software development work place and server connections to ensure high-speed and low-latency connectivity.
- Wireless Access Points (WAPs) will be strategically placed to provide seamless Wi-Fi coverage throughout all three floors.
- Estimated equipment:
  - ❖ Core routers (x2) for redundancy
  - ❖ Layer 3 switches for network segmentation and routing
  - ❖ Access layer switches for user device connectivity
  - ❖ Minimum 10-12 enterprise-grade WAPs per floor to maintain coverage and support device density  
*McGraw-Hill, 2013.*

#### **3. Types of Cabling**

- Cat 6A Ethernet cables for internal wired network to support up to 10 Gbps bandwidth, suitable for high-speed data transfer and future upgrades.
- Fiber optic backbone cabling between floors and the server room to ensure high-speed interconnectivity and reduce bottlenecks.

#### 4. Special needs of department and Segmentation

- The LAN must support segmentation (VLANs) for different departments:
  - ❖ **Software Development:** High bandwidth, access to internal development servers, Git repositories, and cloud services.
  - ❖ **Finance and HR:** Encrypted data transmission, restricted access to sensitive financial and employee records.
  - ❖ **Customer Support:** VoIP connectivity and access to CRM systems.
  - ❖ **Management Offices:** Secure remote access, video conferencing, and executive dashboards.

*Cisco Press, 2016.*

#### 5. Video Conferencing Capabilities

- Each of the four conference rooms will be equipped with:
    - ❖ High-end video conferencing systems
    - ❖ Support for 4K video quality and low-latency streaming
    - ❖ Dedicated bandwidth to ensure uninterrupted meetings
    - ❖ Integration with platforms like Zoom or Microsoft Teams
- Pearson, 2015.*

#### 6. CCTV Surveillance Systems

- CCTV cameras will be installed for security and monitoring:
  - ❖ Entry and exit points
  - ❖ Server room and IT storage areas
  - ❖ Common areas such as cafeteria and break rooms
- The network must provide PoE (Power over Ethernet) support for CCTV and remote monitoring capabilities.

*O'Reilly Media, 2017.*

## **B) Analysis of Growth Plans, Scalability Requirements, and Network Traffic:**

### **1. Scalability for Number of Employees**

- TechSavvy plans to scale from 150 to 300 employees, significantly increasing the demand on the network.
- To accommodate this:
  - ❖ The network must support high-speed connectivity, especially in open workspaces with many simultaneous users.
  - ❖ Backbone links and server room connections should be established using Fiber optics with 10 Gbps speeds, scalable to 40 Gbps as needed.
  - ❖ Access switches must support Gigabit ports per user and be stackable or modular to handle increased port requirements.
  - ❖ VLANs will be configured to reduce network congestion and ensure efficient traffic routing between departments.

### **2. Scalability for Number of Access Points (Wi-Fi Expansion)**

- With more employees and a bring-your-own-device (BYOD) culture, the number of connected devices will increase exponentially.
- The network must:
  - ❖ Support Wi-Fi 6 access points, capable of high device density and better throughput.
  - ❖ Be designed with future expansion of APs in mind—from 10–12 per floor now, expandable to 20+ per floor as needed.
  - ❖ Ensure centralized wireless controller support to manage access points and ensure seamless coverage and handoffs between floors.
  - ❖ Use Power over Ethernet (PoE+) switches to simplify deployment and support future hardware upgrades.

*Pearson, 2017.*

### **3. Scalability with Respect to Network Speed**

- As the company adopts more cloud-based services and handles larger data loads, bandwidth demands will increase.
- The network must be capable of:
  - ❖ Providing low-latency, high-throughput connections for services such as:
    - Video conferencing (Zoom, Teams)
    - VoIP communications
    - Cloud-hosted development environments
    - Large file transfers and backups

- ❖ Implementing Quality of Service (QoS) policies to prioritize time-sensitive traffic such as VoIP and video.
- ❖ Ensuring core network devices support multi-gigabit uplinks, with redundancy protocols like HSRP/VRRP for reliability.

*Cisco Press, 2016.*

## Task 2 - Network Topology Diagram

### a) Floor plan layout

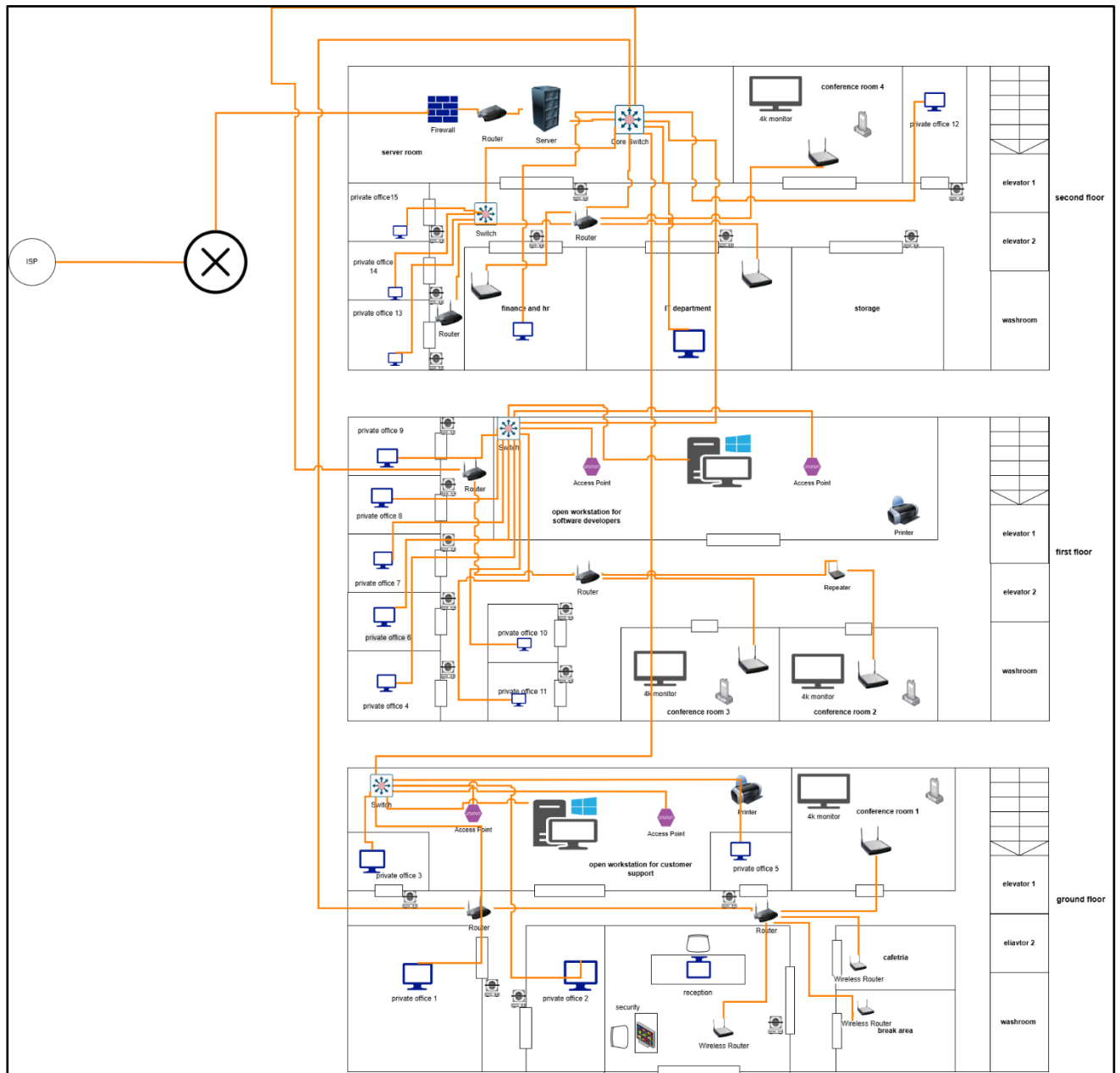


Fig 2.1 floor planning

**Justification for floor plan:**

Aspect	Justification
Core Networking Devices	Switches are placed centrally on each floor to minimize cable distance and improve performance. Router and firewall are located near the server room for secure, high-speed internet access.
Ground Floor Layout	Open workspace for customer support, reception with security systems, cafeteria, and break room. Wireless routers ensure strong Wi-Fi coverage for flexible work.
First Floor Layout	Open workspace for software developers. Private offices and two conference rooms are wired for high-speed access. Access Points provide seamless Wi-Fi for high device density.
Second Floor Layout	Server room, IT support, finance, HR, and senior management offices located for easy management of sensitive systems and better security.
Structured Cabling	Orange cabling for organized high-speed wired connections. Redundant cabling between core switches prevents single points of failure.
Wireless Coverage	Access Points are strategically placed across open areas and near conference rooms to ensure full building Wi-Fi coverage.
Security and Surveillance	Biometric scans are present at reception, server room, private offices and storage areas for monitoring and physical security.
High-Bandwidth Support	Conference rooms are wired for video conferencing and VoIP services. Server room directly connected for low-latency operations.
Scalability	Switches and Access Points have capacity for additional users and devices, supporting future growth to 300 employees without major redesign.

Table 2.1 aspects



## b) Network topology

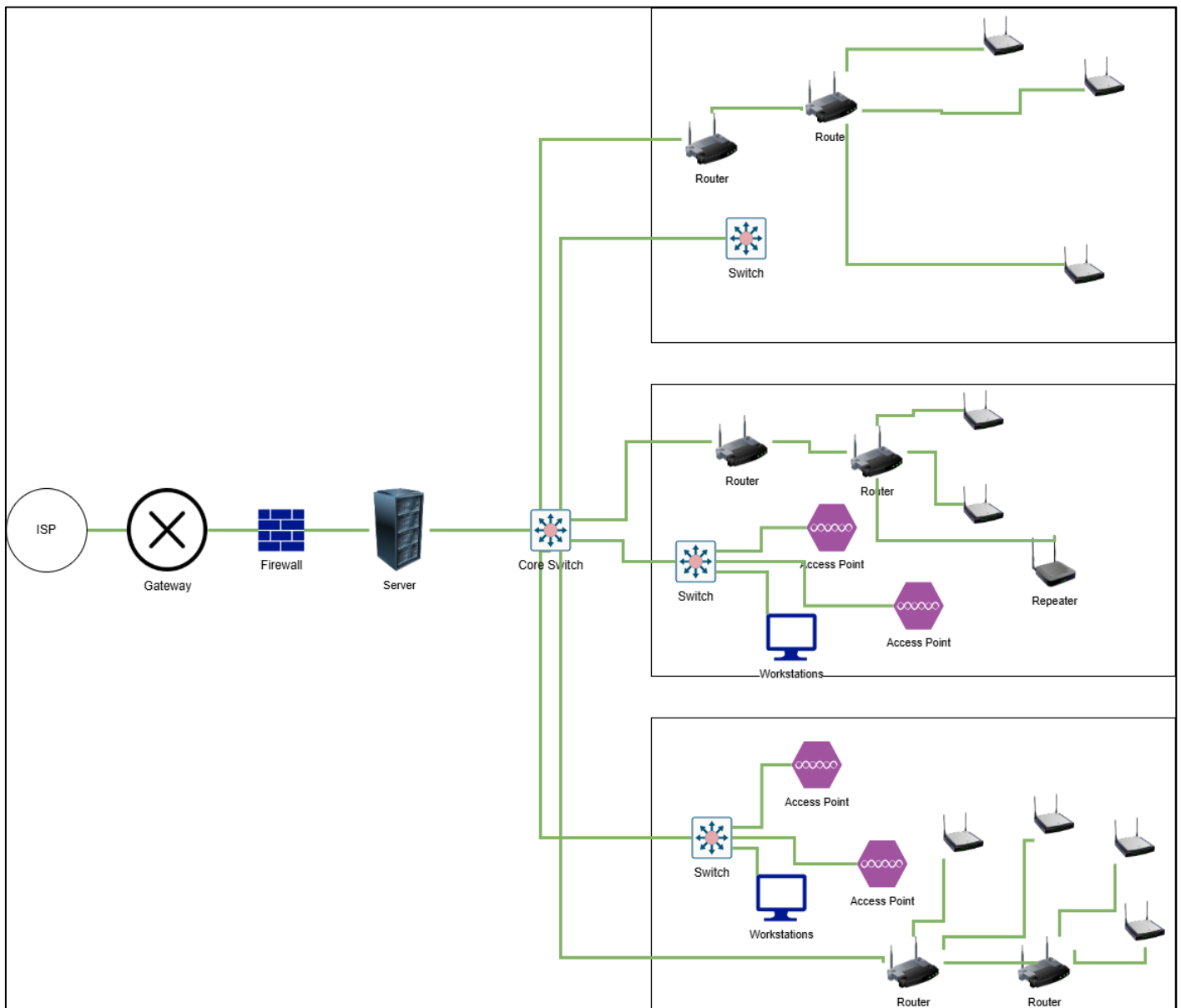


Fig 2.2: network topology diagram

## Network Topology Discussion

### ❖ Star Topology (Based on Layout)

In the above network diagram, a star topology is used. In a star topology, all devices are connected to a central device (like a switch or hub).

In this case:

- The main switch acts as the central point.

- Routers, access points, servers, and workstations are all linked back to this main switch.
- The switch connects upstream to the gateway and server for internet access and data services.

➤ **Advantages of Star Topology:**

- Easy to manage and troubleshoot: If one device fails, it does not affect the rest of the network.
- Scalability: New devices can be easily added without disrupting the network.
- Performance: Centralized management improves overall performance.

➤ **Disadvantages of Star Topology:**

- Single point of failure: If the main switch or central node fails, the entire network is disrupted.
- Cable intensive: Requires more cabling compared to simpler topologies like bus networks.

❖ **Mesh Topology (An Alternative)**

An alternative to star topology is the mesh topology.

In a mesh network, each device connects directly to multiple other devices, creating multiple paths for data transmission.

➤ **Advantages of Mesh Topology:**

- High reliability and redundancy: If one connection fails, data can be rerouted through another path.
- High performance: Mesh networks handle heavy traffic well because multiple paths reduce congestion.
- Fault tolerance: Mesh design minimizes downtime.

➤ **Disadvantages of Mesh Topology:**

- Complex setup: Installing and configuring a mesh network is complicated.
- High cost: Requires more cabling, more network interfaces, and more complex routing.
- Maintenance difficulty: Managing many connections becomes difficult as the network grows.

*McGraw-Hill, 2013.*

**Final Thoughts:**

While a mesh topology would offer better reliability and fault tolerance, it would significantly increase the cost and complexity of the network.

Given the size and structure of the current design, a star topology is more cost-effective, easier to manage, and suitable for the current needs. However, for future critical upgrades, especially where zero downtime is required, implementing elements of a partial mesh topology could be considered.

### Task 3 - Equipment Selection and Specification - 20 marks

Select the necessary network equipment and provide detailed specifications.

- List all required networking equipment, including switches, routers, access points, cables and connectors. (10 marks)
- Justify your equipment choices based on performance, reliability and scalability. (10 marks)

### Task 3 selection and specification

#### a) List of Required Networking Equipment and Specifications

Equipment	Model Example	Specification/Configuration Details	Purpose
Core Switch	Cisco Catalyst 9300 Series	<ul style="list-style-type: none"> <li>- 48 Gigabit Ethernet ports</li> <li>- 4 x 10G SFP+ uplink ports</li> <li>- Layer 3 capable</li> <li>- Support for VLANs, QoS, redundancy protocols (like HSRP)</li> </ul>	Acts as the main switch distributing traffic to floor switches and servers
Floor Switches (per floor)	Cisco Catalyst 9200 Series	<ul style="list-style-type: none"> <li>- 24 Gigabit Ethernet ports</li> <li>- 2 x 10G uplink ports</li> <li>- Layer 2 managed switch</li> <li>- VLAN and trunking support</li> </ul>	Connects workstations, routers, and access points per floor
Routers (Floor level)	Cisco ISR 1000 Series	<ul style="list-style-type: none"> <li>- Dual WAN ports</li> <li>- 1 Gbps throughput</li> <li>- VPN support</li> <li>- Integrated security features (firewall, IPS)</li> </ul>	Manage traffic routing between different floors and provide secure internet access
Access Points	Cisco Aironet 2800 Series	<ul style="list-style-type: none"> <li>- Dual-band (2.4GHz and 5GHz) support</li> <li>- 802.11ac Wave 2 (Wi-Fi 5)</li> <li>- MU-MIMO for multiple device connections</li> <li>- 5.2 Gbps maximum throughput</li> </ul>	Provide wireless connectivity to mobile users and devices
Repeaters	TP-Link AC1750 Wi-Fi Range Extender	<ul style="list-style-type: none"> <li>- Dual-band Wi-Fi support</li> <li>- Gigabit Ethernet port</li> <li>- 1750 Mbps wireless speed</li> </ul>	Extend wireless coverage in large open areas or blind spots
Firewall/Gateway	Fortinet FortiGate 100F	<ul style="list-style-type: none"> <li>- 10 Gbps firewall throughput</li> <li>- Intrusion prevention system (IPS)</li> <li>- Application control, anti-</li> </ul>	Protect network from external threats and

		malware - Site-to-site VPN support	manage secure traffic flow
Server	Dell PowerEdge R740	- Dual Intel Xeon processors - 256GB RAM - 10Gb Ethernet NIC - Redundant power supply	Hosts internal services, databases, and applications
Fiber Optic Cable (ISP to Gateway)	OM4 Multimode Fiber	- 10 Gbps up to 550 meters - LC/LC connectors - Armored option for better protection	High-speed backbone from ISP to building gateway and server room
Ethernet Cables (Internal Networking)	Cat 6A Ethernet Cable	- Supports 10Gbps over 100 meters - Shielded Twisted Pair (STP) for minimal interference - RJ45 connectors	Connect desktops, printers, access points, and other devices internally
Patch Panels	48-Port Cat6 Patch Panel	- Organized cable management - Labeling for easier troubleshooting	Termination point for network cables in server and floor rooms
Network Racks	42U Enclosed Server Rack	- Cooling fans and cable management trays - Lockable for physical security	Houses core switches, servers, firewalls, patch panels neatly

Table 3.1: networking equipment

**Cable Choices Justification:**

Connection	Cable Type	Reason
ISP to Gateway and Gateway to Server Room	Fiber Optic (OM4)	Fiber optics support extremely high speeds (10 Gbps+), low latency, and long-distance transmissions without signal loss, critical for external and backbone connections.
Internal Networking (Workstations, Access Points, Printers)	Cat 6A Ethernet Cable	Cat 6A supports 10 Gbps over standard office distances (up to 100 meters), is shielded for interference protection, and is cost-effective for internal cabling compared to fiber.

Table 3.2: cable type

**b) Create a table which justifies your items based on RSP**

Device	Performance	Reliability	Scalability
--------	-------------	-------------	-------------

Core Switch (Cisco Catalyst 9300)	High-speed switching with 10G uplinks, low latency	Enterprise-grade hardware with redundancy features (stacking, dual power)	Supports future expansion with additional switches and 10G backbones
Floor Switch (Cisco Catalyst 9200)	Gigabit speeds, VLAN and QoS capabilities	Stable operation with professional support and long MTBF (Mean Time Between Failures)	Can add more ports or stack switches as employee count grows
Router (Cisco ISR 1000)	Secure high-speed routing, optimized for WAN and VPN traffic	Integrated firewall, software updates for consistent protection	Supports modular upgrades and increased branch connections
Access Points (Cisco Aironet 2800)	High throughput (up to 5.2Gbps), excellent device handling with MU-MIMO	Business-grade wireless hardware with strong security and lifetime support options	Easy to add more APs as user/device density increases
Repeater (TP-Link AC1750)	Boosts Wi-Fi coverage without major cabling	Stable consumer-grade extender, suitable for low-traffic areas	Can add additional repeaters if blind spots appear
Firewall/Gateway (Fortinet FortiGate 100F)	10Gbps throughput, advanced threat protection, IPS, VPN support	High-availability (HA) options, regular firmware updates for security	Scales with network needs through licensing and clustering options
Server (Dell PowerEdge R740)	Dual processors, high memory and storage bandwidth	Enterprise reliability, RAID storage, redundant power for uptime	Modular upgrades for RAM, CPU, storage expansion
Fiber Optic Cables (OM4)	10Gbps+ speeds, immune to EMI (electromagnetic interference)	Very low signal loss, highly durable	Future-ready for even 40Gbps or 100Gbps upgrades if needed
Ethernet Cables (Cat 6A)	10Gbps speeds over 100m distance	Shielded cabling reduces cross-talk and network errors	Future-proof for 10G networking, beyond standard gigabit needs
Patch Panel	Keeps data center cabling organized and neat	Reduces wear on ports and simplifies maintenance	Easy to expand by adding more panels if needed
Network Racks	Efficient airflow and cooling improves performance	Physical security against unauthorized	Racks allow modular addition of more hardware

		access, protects equipment	(servers, switches)
--	--	-------------------------------	------------------------

Table 3.3: items based on RSP

## Task 4 - IP Addressing and Subnetting - 15 marks

Develop an IPv4 addressing scheme for the network.

- Create an IP addressing plan that supports efficient routing and management. (7 marks)
- Subnet the network to accommodate different departments and functions. (6 marks)
- Ensure the addressing scheme allows for future growth and scalability. (2 marks)

## Task 4 – IP Addressing and Subnetting

### a) IP Addressing Plan

Department/Function	Subnet	IP Range	Purpose
Management	192.168.130.0/25	192.168.130.1 – 192.168.130.126	Reserved for directors, managers, and admin team
IT Department	192.168.130.128/25	192.168.130.129 – 192.168.130.254	IT team, network admins, servers
Sales Department	192.168.131.0/25	192.168.131.1 – 192.168.131.126	Sales reps, CRM tools
HR Department	192.168.131.128/26	192.168.131.129 – 192.168.131.190	HR users and employee portal
Finance Department	192.168.131.192/26	192.168.131.193 – 192.168.131.254	Payroll servers and finance users
Guest WiFi / Visitors	192.168.132.0/24	192.168.132.1 – 192.168.132.254	Visitors and guest devices
Backup and Storage	192.168.133.0/25	192.168.133.1 – 192.168.133.126	Backup servers and storage systems
Future Expansion	192.168.133.128/25	192.168.133.129 – 192.168.133.254	Reserved for future departments

Table 4.1: IP address plans

### b) Subnetting Details

Subnet	CIDR	Subnet Mask	Hosts per Subnet	Department/Use
192.168.130.0/25	/25	255.255.255.128	126 hosts	Management
192.168.130.128/25	/25	255.255.255.128	126 hosts	IT Department

192.168.131.0/25	/25	255.255.255.128	126 hosts	Sales Department
192.168.131.128/26	/26	255.255.255.192	62 hosts	HR Department
192.168.131.192/26	/26	255.255.255.192	62 hosts	Finance Department
192.168.132.0/24	/24	255.255.255.0	254 hosts	Guest WiFi
192.168.133.0/25	/25	255.255.255.128	126 hosts	Backup and Storage
192.168.133.128/25	/25	255.255.255.128	126 hosts	Reserved for future growth

Table 4.2 subnetting

### c) Future Growth and Scalability

- **Reserved Subnet:** 192.168.133.128/25 is kept fully free for adding new departments, servers, or additional users.
- **Large Guest WiFi Subnet:** 192.168.132.0/24 can accommodate many visitors without exhausting the IP pool.
- **Flexible Subnetting:** Departments with fewer users (like HR and Finance) use /26 subnets (smaller subnets) to avoid wastage of IP addresses.



## Task 5 - Network Security Design - 15 marks

Design the security infrastructure for the network.

- Identify potential security threats and vulnerabilities. (7 marks)
- Design a security plan that includes security features, tools and controls as appropriate. Provide a justification for your controls. (8 marks)

### Task 5 security design

#### a) Identify Potential Security Threats and Vulnerabilities

##### I. . What is a Threat?

A **threat** is any **potential danger** that can exploit a weakness (vulnerability) in a system to cause harm — such as **data theft, disruption, or unauthorized access**.

##### II. What is a Vulnerability?

A **vulnerability** is a **weakness** or **gap** in a system's defenses that could be exploited by a threat to gain unauthorized access or cause damage.

Example: Weak passwords, outdated firewalls, unsecured WiFi.

##### III. Goals of Network Security

The three main goals of network security are:

Goal	Purpose
<b>Confidentiality</b>	Keep data private and accessible only to authorized users.
<b>Integrity</b>	Ensure data is not altered or tampered with.
<b>Availability</b>	Keep network and resources available to legitimate users when needed.

Table 5.1: network security goals

##### IV. Types of threats

Type	Example	Explanation
<b>Unauthorized Access</b>	Employees accessing confidential files without permission	Insider threats or weak access control measures.
<b>Malware and Viruses</b>	Virus infections via email or USB	Malware can corrupt files, steal data, or crash systems.
<b>Denial of Service (DoS)</b>	Server flooding with fake traffic	Causes services to be unavailable for real users.
<b>Data Breaches</b>	Data packets intercepted or leaked	Due to weak network encryption or firewall misconfigurations.
<b>Phishing and Social Engineering</b>	Fake emails to steal passwords	Exploits human error rather than system flaws.

<b>Unsecured Endpoints</b>	BYOD (Bring Your Own Device)	Devices without security measures can introduce vulnerabilities.
<b>Weak Network Monitoring</b>	Lack of logging/alerts	Leads to delayed detection of attacks.

Table 5.2: types of threats

### **b) Design a Security Plan that includes Security Features, Tools, and Controls**

Here's a strong, realistic plan you can use:

<b>Security Feature / Tool</b>	<b>Description</b>	<b>Justification</b>
<b>Firewall</b>	Blocks unauthorized traffic between internal network and external networks.	Protects against external attacks by filtering network traffic.
<b>Intrusion Detection and Prevention System (IDPS)</b>	Monitors traffic for suspicious activities and blocks them.	Early detection and stopping of potential breaches.
<b>Antivirus and Antimalware Software</b>	Protects devices from viruses, trojans, ransomware, and spyware.	Ensures all endpoints are secure from malicious software.
<b>Virtual Private Network (VPN)</b>	Secure, encrypted connection for remote users.	Protects data transmission over untrusted networks.
<b>Multi-Factor Authentication (MFA)</b>	Requires two or more verification steps (password + OTP, fingerprint).	Stronger access control, reduces risk of account compromise.
<b>Network Segmentation</b>	Divides network into sections (e.g., Admin, HR, Guest WiFi).	Limits spread of an attack; better traffic control and monitoring.
<b>Regular Security Updates and Patches</b>	Systematic updating of OS, software, and firmware.	Fixes known vulnerabilities quickly, reducing attack surface.
<b>Security Policies and Employee Training</b>	Guidelines for safe password use, email handling, etc.	Reduces human errors, the most common cause of breaches.

Table 5.3: security tools

## Task 6 - Network Management and Monitoring - 10 marks

Outline the management and monitoring strategies for the network.

- Identify tools and software for network monitoring and performance analysis. (6 marks)
- Explain how you will ensure network reliability and uptime. (4 marks)

## **Task 6 – Network Management and Monitoring**

### **a) Identify Tools and Software for Network Monitoring and Performance Analysis**

Here's a list of important tools you can mention:

Tool / Software	Purpose	Why it's Important
SolarWinds Network Performance Monitor (NPM)	Monitors network devices, bandwidth usage, and alerts for issues.	Provides real-time visibility and quick issue detection.
Paessler PRTG Network Monitor	Monitors uptime, traffic, and network health with sensors.	Easy to set up and gives detailed monitoring of all devices.
Wireshark	Analyzes network packets to detect problems and security issues.	Useful for deep packet analysis to troubleshoot faults.
Nagios	Monitors servers, switches, applications, and services.	Highly customizable and scalable monitoring system.
ManageEngine OpManager	Monitors server health, network bandwidth, and traffic patterns.	Good for medium-large networks needing visual insights.
Zabbix	Open-source tool for monitoring networks, systems, and apps.	Cost-effective solution with strong alerting capabilities.

Table 6.1: software and its purpose

### **b) Explain How You Will Ensure Network Reliability and Uptime**

Here's how you can answer this clearly:

Strategy	Description	Justification
Fault Tolerance Features	Use of redundant network paths, redundant switches/routers (failover systems).	Ensures the network keeps running even if one device fails.

Regular Backups of Networking Devices	Configuration backups for routers, switches, firewalls saved periodically.	Enables quick recovery in case of device failure or corruption.
Safeguarding Against Unauthorized Access	Implement strong authentication, firewalls, access control lists (ACLs), encryption (SSL/TLS).	Protects the network from internal and external attacks that could cause downtime.
Monitoring and Proactive Maintenance	Regular health checks using monitoring tools and predictive maintenance schedules.	Detects issues early to prevent unexpected network outages.

Table 6.2 strategy

## References:

1. Kurose, James F., and Keith W. Ross. *Computer Networking: A Top-Down Approach*. 7th ed., Pearson, 2017.
2. Forouzan, Behrouz A. *Data Communications and Networking*. 5th ed., McGraw-Hill, 2013.
3. Cisco Systems, Inc. *Cisco Networking Academy: Introduction to Networks*. Cisco Press, 2016.
4. Stallings, William. *Data and Computer Communications*. 10th ed., Pearson, 2015.
5. Wright, Jeremy. *Networking for Systems Administrators*. O'Reilly Media, 2017.
6. Kurose, James F., and Keith W. Ross. *Computer Networking: A Top-Down Approach*. 7th ed., Pearson, 2017.
7. Cisco Systems, Inc. *Cisco Networking Academy: Introduction to Networks*. Cisco Press, 2016.
8. Forouzan, Behrouz A. *Data Communications and Networking*. 5th ed., McGraw-Hill, 2013.

## Candidate checklist

Please use the following checklist to ensure that your work is ready for submission.

Have you read the NCC Education document *Academic Misconduct Policy* and ensured that you have acknowledged all the sources that you have used in your work? ☐

Have you completed the *Statement and Confirmation of Own Work* form and attached it to your assignment? **You must do this.** ☐

Have you ensured that your work has not gone over or under the recommended word count by more than 10%? ☐

Have you ensured that your work does not contain viruses and can be run directly? ☐