**Project Report**



|  |  |
| --- | --- |
| **Product Name** | Higher Diploma in Software Engineering (HDSE) |
| **Qualification Name** | Higher Diploma in Software Engineering |
| **Project title** | **Principles and Design of Networked Systems** |
| **Module Name (HDSE)** | IT Systems & Networks |

|  |  |  |  |
| --- | --- | --- | --- |
| **Student name** | | **Assessor name** | |
| Escarro, Sebastian Seth R. | | Grace Bee Cho Tok | |
| **Date issued** | **Completion date** | | **Submitted on** |
| 7/20/2024 | 11/9/2024 | | 11/11/2024 |
|  | | | |
| **Project title** | **Principles and Design of Networked Systems** | | |

|  |
| --- |
| **Learner declaration** |
| I certify that the work submitted for this assignment is my own and research sources are fully acknowledged.  Student signature:  Date:7/20/24 |

**Content**



1. Project background
2. Project Objectives
3. Requirement Specifications
4. Task 1
5. Task 2
6. Task 3
7. Task 4



# Project Background

Swift & Bacon Publishers (SBP) Ltd is a medium-sized company specializing in the publication of scientific and technical books and journals. SBP operates from two office buildings and supports a hybrid working model, allowing employees to work both remotely and on-site. The organization consists of four subject-specific Publishing Teams, each managed by a Publishing Team Leader (PTL) and supported by up to 20 Publishing Editors (PEs). SBP's network infrastructure includes secure servers for managing manuscripts and publishing content, with a need to maintain high security and efficient data handling.

Given the company's recent shift towards hybrid working, SBP plans to close one office building and reconfigure the remaining building to support both on-site and remote work. This reconfiguration involves setting up a secure, efficient, and robust network infrastructure that caters to the needs of employees working from home and those who choose to work from the office.

1. **Project Objective**

* Improve Remote Working
* Reconfigure Infrastructure
* Upgrade Network
* Better Security
* Networking Solutions

1. **Requirement Specification**

* **Network Infrastructure (Top Floor, Middle Floor, Ground Floor)**
* **Remote Work Capabilities: Company Issued Laptop and VPN Server**
* **Security**
* **Connectivity**
* **Data Management**
* **Employee Management**

# Task 1

|  |  |  |  |
| --- | --- | --- | --- |
| Network Types | Benefits | Constraints | Examples |
| Wired | -Stable and reliable connection  -High speeds with low latency  -Less susceptible to interference | -Limited mobility  -Requires physical cables  -Higer costs in a complex environment | -Ethernet (LAN)  -Fiber Optic Networks |
| Wireless | -Great mobility and flexibility  -Quicker to deploy  -No cables | -Might be affected by interference  -Slower compared to wired  -Possible security concerns | -Wi-fi  -Cellular Networks |
| Hybrid | -Combines advantages of wireless and wired  -More scalable and flexible design | -Complex network management  -Expensive to deploy and maintain  -Integration issues | -Corporate Networks (wired LAN and wireless access)  -Home networks (Ethernet and Wi-fi) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Network Standards | Benefits | Constraints | Purpose | List of Layers |
| OSI Model | - Provides a comprehensive framework for network architecture  - Helps in troubleshooting and standardizing protocols  - Easy to understand and teaches network fundamentals | |  | | --- | | - The model is theoretical and not always practical  -Implementation can vary | | |  | | --- | | - To standardize network functions and facilitate interoperability between different systems | | |  | | --- | | 1. Physical  2. Data Link  3. Network  4. Transport  5. Session  6. Presentation  7. Application | |
| TCP/IP Model | - Practical and widely used for real-world networks  - Simplified compared to OSI  - Focuses on protocols that are in use today | - Less granular than OSI  - Can be less helpful for detailed network troubleshooting | - To define the protocol suite used for communication over the internet | 1. Link  2, Internet  3. Transport  4. Application |
| 802.x | - Defines various aspects of local area network (LAN) standards  - Ensures compatibility and interoperability  - Supports high-speed networking | - Each standard has different applications and may not be compatible with each other  - Implementation complexity | - To provide standards for different types of network interfaces and technologies | - Specific layers vary by standard, but commonly include physical and data link layers.  Examples:  - **802.3** (Ethernet)  - **802.11** (Wi-Fi)  - **802.15** (Bluetooth) |

**Impact of Network Topology, Communication, and Bandwidth Requirements**

**Network Topology**

* Network topology defines the arrangement of devices and connections within a network. It directly influences data flow, performance, and security. There many types of topologies, which include:
* **Star Topology:** In a star topology, all nodes are connected via a central hub or switch

**Advantages:**

* + - * Easy to set up and understand
      * One device failure won’t affect others
      * New devices are easily added

**Disadvantages:**

* + - * If the hub fails, entire network is affected
      * Require a lot of cabling
* **Bus Topology:** Devices are connected via a single central cable. Like a bus going from point a to point b

**Advantages:**

* + - * Simple and Cost Effective
      * Suitable for small networks

**Disadvantages:**

* + - * If the single cable breaks, entire network is down
      * Degradation of performance with more devices
* **Tree Topology:** Structured like a tree where a root node branches out into multiple nodes

**Advantages:**

* + - * Clear parent child relationships
      * One device failure won’t affect others
      * New devices are easily added

**Disadvantages:**

* + - * If the root node fails, entire network is affected
      * Complex cabling
      * Expensive
* **Ring Topology:** Devices form a loop making a circle

**Advantages:**

* + - * Simple and predictable
      * Only one device can transmit at a time

**Disadvantages:**

* + - * If one device fails, entire network is affected
      * Difficult to remove and add devices

**Communication**

* Communication ensures seamless data exchange between devices and users within a network. It’s like the network’s “language” that allows devices to talk to each other effectively. Some methods include:
* **Twisted Pair Cables:** Twisted pair cables consist of wires twisted together in pairs. They are cost-effective, easy to install, and suitable for short distances. However, they have limited bandwidth and are susceptible to interference from other electrical equipment.

**Advantages:**

* + - * Affordable and widely available
      * Easy to set up and disassemble
      * Suitable for short distances

**Disadvantages:**

* + - * Limited bandwidth
      * Susceptible to interference
* **Fiber Optic Cables:** Fiber optic cables use light signals for data transmission. They offer high performance, immunity to electromagnetic interference, and long-distance connectivity. Their bandwidth is excellent, making them ideal for high-speed applications.

**Advantages:**

* + - * Immunity to electromagnetic interference (EMI)
      * Exceptional data transmission speeds
      * Suitable for long distances

**Disadvantages:**

* + - * Complex to terminate
      * Delicate cables, quite fragile
      * Expensive
* **Wireless Networks:** Wireless networks provide mobility and ubiquitous access. They allow devices to connect without physical cables, making them versatile for various scenarios. However, wireless networks trade off bandwidth and security considerations.

**Advantages:**

* + - * Doesn’t require physical cables
      * Accessible network within area of coverage
      * Relatively easy to add new devices to

**Disadvantages:**

* + - * Lower bandwidth compared to wired connections
      * Easily intercepted signals
      * Susceptible to interference from other devices and physical obstacles

**Bandwidth Requirements**

* Bandwidth refers to how much data can be sent or received through a network link in a given time. It’s like the network’s “highway capacity”—enough bandwidth ensures smooth data flow, while insufficient bandwidth leads to congestion. Its impact to network design include:
* **Capacity:** Determines network’s ability to support activities.
* **Design Principles:** Structured cabling system design.
* **Data Rates:** Higher data rates require more bandwidth.
* **Considerations:** NEXT (near-end crosstalk) and external noise.

Higher bandwidths are usually sought after but lower bandwidths are more cost effective.

**Common Network Principles**

**Scalability:** A network must be able to handle growth like if new devices are added or if new users are using it. An effective system must allow for expansion without degrading performance

**Security:** Protecting the network from cyber threats is essential. Security measure like encryptions, firewalls or protocols must be used in order to ensure safe data travel.

**Redundancy:** Networks must have a backup system in place just in case some unfortunate circumstances happen. It helps contribute to the network’s resilience

**Reliability:** The network must provide a consistent and stable connection with minimal outages. This includes protocols that are resilient to errors and are fault-tolerant

**Bandwidth Management:** Ensuring proper bandwidth for all data demand is crucial. Proper bandwidth management ensures smooth data flow and reduced network congestion

**Latency and Throughput:** Latency refers to delay while throughput refer to successfully transmitted data. Having low latency and high throughput are critical for network performance.

**Network Protocols**

**IPv4 (Internet Protocol Version 4):**

* IPv4 is the fourth version of the Internet Protocol, responsible for assigning unique IP addresses to devices on a network and routing data between them.
* **Advantages**:
  + Widely deployed and understood.
  + Simpler structure with shorter addresses (32-bit).
  + Supported by most devices and software.
* **Disadvantages:**
  + Limited address space (around 4.3 billion addresses), leading to the need for network address translation (NAT).
  + Less efficient for routing than IPv6.

**IPv6 (Internet Protocol Version 6):**

* IPv6 is the successor to IPv4, designed to address the limitations of IPv4, most notably its limited address space.
* **Advantages:**
  + Virtually unlimited address space (128-bit addresses), solving the address exhaustion issue.
  + Improved routing efficiency and security features like mandatory support for IPSec (Internet Protocol Security).
  + Better performance for real-time traffic, especially in peer-to-peer applications.
* **Disadvantages:**
  + More complex to implement and requires new hardware/software configurations.
  + Not as widely adopted yet, so dual-stack configurations are often required (supporting both IPv4 and IPv6).

**HTTPS (Hypertext Transfer Protocol Secure):**

* HTTPS is the secure version of HTTP (the protocol used for web traffic), which encrypts data between a client (like a web browser) and a server using SSL/TLS.
* **Advantages:**
  + Provides encrypted communication, ensuring data integrity and confidentiality.
  + Protects against man-in-the-middle attacks and eavesdropping.
  + Boosts user trust and is increasingly required for websites, especially **with** modern browsers marking HTTP as "not secure."
* **Disadvantages:**
  + More resource-intensive than HTTP, requiring more processing power for encryption/decryption.
  + Slightly slower due to encryption overhead.

**Operating Principles of Network Devices**

|  |  |  |  |
| --- | --- | --- | --- |
| **Network Server Types** | **Operating Principle** | **Function** | **Impact** |
| Routers | Operate at network layer | - Connect different networks  - Route data packets between networks  - Choose optimal paths for data transmission | - Enables communication between networks  - Manages data traffic efficiently  - Enhance connectivity to network |
| Switches | Operate at the data link layer | - Connect devices within a local LAN  - Forward data based on MAC addresses  - Improve network efficiency | - Facilitate device communication  - Reduce unnecessary traffic  - Enhance LAN performance |
| Firewalls | Operate based on predefined rules | - Control access for networks  - Inspect packet headers and manage traffic  - Blocks threats | - Protection from unauthorized access  - Safeguard sensitive data  - Prevent malicious traffic |
| Repeaters | Operate at physical layer | - Amplify weak signals within the same network  - Extends signal transmission distance | - Extend network coverage  - Prevent signal degradation |
| Bridges | Operate at the data link layer | - Connect two LANs on the same protocol  - Filter content based on MAC addresses | - Efficiently segment LANs  - Enhance network performance |
| IoT Gateways | Serve as intermediaries between IoT devices and networks. | -Aggregate data from IoT devices  - Convert protocols for seamless communication  - Provide security | - Enable IoT device integration  - Ensure data interoperability  - Enhance IoT system security |
| Domain Servers | Manage domain names an IP addresses | - Resolve domain names to IP addresses  - User authentication | - Facilitate user-friendly web browsing  - Enable centralized authentication |
| Web Servers | Serve web content to clients | - Respond to HTTP requests  - Host websites and web applications | - Efficient web page delivery  - Enable online presence for businesses |
| File Servers | Store and manage files for network users | - Centralize file storage  - Provide access control and permissions | - Facilitate collaboration  - Ensure data consistency  - Improve data security |
| Database Servers | Manage databases and handle queries | - Create, read, update, and delete data.  - Handle transactions | - Optimize query performance  - Ensure data integrity |

**Workstation Hardware and Network Software**

**Network Interface Card (NIC)**

* **Hardware:**
  + The NIC is a critical piece of hardware that connects a workstation to the network. It converts data into signals that can be transmitted over wired (Ethernet) or wireless (Wi-Fi) networks.
* **Software:**
  + Network drivers are needed to control the NIC and allow it to communicate with the operating system and the network.
  + Networking software relies on the NIC’s drivers to send and receive data packets. Without properly functioning drivers, the NIC cannot operate.
* **Dependency:**
  + Hardware-software synchronization is crucial. If the NIC hardware does not match the capabilities of the network software, performance can degrade. For example, a high-speed NIC (Gigabit Ethernet) will need compatible software to utilize its full capacity, or else bottlenecks can occur.
  + Compatibility: The NIC’s hardware must support the network protocol (IPv4, IPv6) that the software is using. If a network requires IPv6 but the NIC or drivers only support IPv4, it creates a compatibility issue.

**Storage**

* **Hardware:**
  + Workstation storage (hard drives, SSDs) stores network configurations, software, and data files.
  + In modern networks, cloud storage or network-attached storage (NAS) is often used to extend local storage.
* **Software:**
  + Network software (such as network protocols and client software) accesses this storage to retrieve files, log network activities, and handle backups.
  + Network-attached applications (like file-sharing services) need the storage system to be compatible with the network protocols and systems.
* **Dependency:**
  + Speed and Access: Fast storage (SSDs) enables faster access to networked files, which improves overall network performance.
  + File Syncing: If a workstation uses cloud storage, the local storage and network software must work together to sync files between the local machine and remote servers. If the storage is too slow, it can cause latency in accessing network resources.

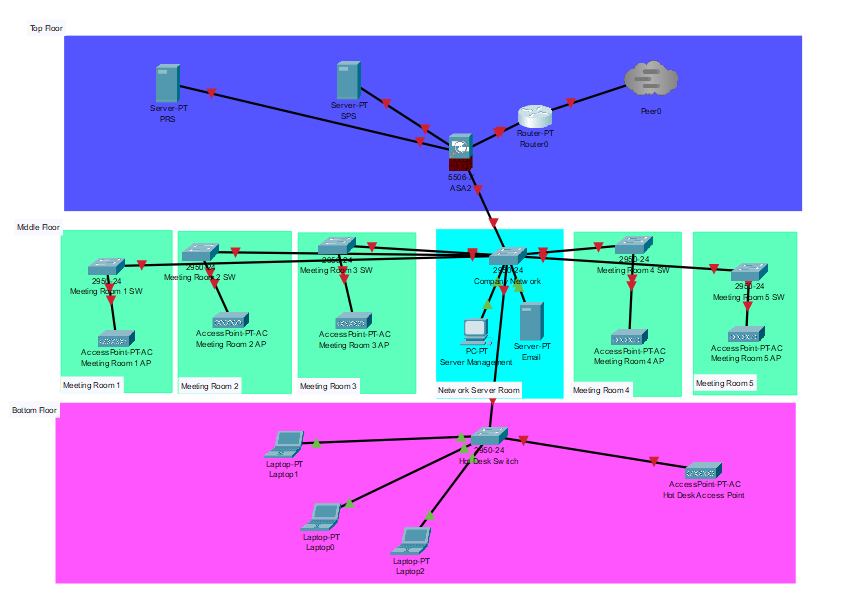
**Network Topology and Infrastructure**

* **Hardware:**
  + The network's physical topology (star, bus, ring, etc.) defines how workstations connect to the network infrastructure (routers, switches, access points).
  + The cabling (Ethernet, fiber optics) and wireless hardware (Wi-Fi routers) are part of the infrastructure that supports communication between the workstation and the network.
* **Software:**
  + Network management software (such as network monitoring tools) ensures that the topology is efficiently used and data is routed correctly.
  + Software protocols (TCP/IP) manage data transmission over the chosen topology, handlinghow data is packetized, addressed, and sent over the network.
* **Dependency:**
  + Topology-Software Efficiency: If the workstation hardware is in a wired star topology but the software is configured for a wireless mesh topology, network performance will suffer. The software needs to match the network infrastructure for optimal performance.
  + Infrastructure Compatibility: Workstation NICs, routers, and switches need to support the same protocols and bandwidth capabilities that the network software requires to minimize data loss or collisions in the network.

**Bandwidth and Latency**

* **Hardware:**
  + The NIC, processor, and memory affect how much data a workstation can process at any given time.
  + Bandwidth is the capacity of the hardware to handle data transmission. High-speed connections (Gigabit Ethernet) allow for more data to be transferred, reducing congestion.
  + Latency is the time taken for data to travel between two points. Hardware (like NICs and routers) with low latency improves network response times.
* **Software:**
  + Network software manages the flow of data and determines bandwidth usage through protocols like TCP/IP. Software also monitors for packet loss and retransmissions that can increase latency.
  + Quality of Service (QoS) software can prioritize certain types of traffic (e.g., video conferencing) to ensure low latency.
* **Dependency:**
  + Bandwidth Utilization: If the workstation hardware (e.g., NIC) supports Gigabit Ethernet but the software limits the bandwidth (due to traffic shaping or misconfigurations), performance will not be optimized. The software needs to be configured to fully utilize the hardware bandwidth.
  + Latency Minimization: Latency-sensitive applications (like VoIP or online gaming) rely on low-latency hardware and software configurations. High-quality hardware combined with optimized software ensures minimal delay in communications.

# Task 2



* Device Configuration:
  + Configure IP addresses for servers, routers, and switches, possibly using a DHCP server for dynamic allocation.
  + Set up VPN and firewall settings on laptops for secure remote access.
  + Configure access controls for the PRS and SPS servers to limit access based on user roles.
* Security Considerations:
  + Firewall settings for network perimeter defense.
  + Data encryption for storage and transmission, especially for PRS.
  + Role-based access control (RBAC) to enforce the security model.

Maintenance Schedule

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| No. | Equipment Description | Condition | Maintenance Frequency (days) | Description of Maintenance Activity | Assignee | Last Maintenance Date | Next Maintenance Date |
| 1 | Public Repository Server | Good | 30 | Inspection, Security Check | Network Admin | 11/02/2024 | 11/09/2024 |
| 2 | Secure Publishing Server | Good | 30 | Content Review,  Check Backup | Network Admin | 11/02/2024 | 11/09/2024 |
| 3 | Email Server | Good | 15 | Security Check, System Updates | Network Admin | 11/02/2024 | 11/09/2024 |
| 4 | Laptops | Fair | 90 | Inspection, Virus Check | Senior IT | 11/02/2024 | 11/09/2024 |
| 5 | Network Admin’s Pc | Good | 60 | Inspection, Check Updates | Senior IT | 11/02/2024 | 11/09/2024 |

Test Plan

|  |  |  |  |
| --- | --- | --- | --- |
| Test Item | Test Data | Test Action | Expected Result |
| Topology | Test if topology is up and running | Routing tables ping requests | All devices are connected |
| Access Control Test | Test if users have the proper roles and permissions | Attempt to access files with different roles | - Network Administrator should have full access to all server resources.  -Publishing Editor and Publishing Team Leader should have limited or read-only access, depending on their roles.  -Unauthorized access attempts should be denied, maintaining security policies. |
| Bandwidth Test | Test if multiple files load properly | Measure upload/download speeds between floors | Network should handle the file transfers smoothly with minimal speed drop. |

Analysis of User Feedback

High file transfer loads affect network speed, especially when multiple users are transferring large files. This indicates a need for higher bandwidth connections between servers and switches to improve file transfer performance.

Wi-Fi coverage in some meeting rooms is weak, impacting wireless collaboration during presentations. This highlights the need to enhance Wi-Fi coverage in specific areas, ensuring reliable connectivity throughout all meeting rooms.

Use crossover for the switches

Network Design Optimization

Based on the user feedback, several optimizations to the network design are recommended:

* Quality of Service (QoS) Implementation:

Configure QoS settings on the router to prioritize VPN traffic. This will ensure remote access remains stable even during peak hours, improving remote user productivity.

* Upgrade Core Network Links:

Upgrade connections between core switches and servers from 1 Gbps to 10 Gbps to handle high file transfer loads efficiently. This will improve network performance for users transferring large files, reducing lag.

* Wi-Fi Coverage Enhancement:

Adjust access points in meeting rooms and add range extenders as needed to improve signal strength. This will ensure consistent Wi-Fi coverage across meeting rooms, facilitating better wireless collaboration during presentations.

* VPN Server Configuration:

Consider enhancing the VPN server’s capabilities by increasing its processing power or bandwidth allocation, ensuring stable remote access for users.

Network Server Types and Recommended Selection

* Primary Server (PRS):

Type: File Server

Purpose: To store and manage large volumes of data required by the publishing team for editing and production.

Recommended Specifications: High storage capacity (e.g., RAID setup for data redundancy), 10 Gbps network interface card (NIC), and robust processing power to handle concurrent file access.

* Secondary Server (SPS):

Type: Backup Server

Purpose: To provide backup and redundancy for the file server, ensuring data availability in case of primary server failure.

Recommended Specifications: Similar storage capacity as PRS with RAID, but configured as a secondary storage device with backup management software.

* VPN Server:

Type: Remote Access Server

Purpose: To facilitate secure remote access for users working off-site.

Recommended Specifications: Moderate storage, 10 Gbps NIC, and sufficient RAM to manage VPN connections. It should have robust encryption capabilities to ensure secure connections.

* Email Server:

Type: Mail Server

Purpose: To handle internal and external email communication for the organization.

Recommended Specifications: Sufficient storage for emails, antivirus and spam filtering software, and a 1 Gbps NIC.

Justification of Recommended Server Selection

* File and Backup Servers:
* A File Server with high storage capacity is essential for storing large volumes of data. The Backup Server ensures data redundancy and prevents data loss in case of hardware failure. Together, they support high-demand tasks, such as data storage and transfer for the publishing team, which was highlighted as a priority in the feedback.
* VPN Server:
* The VPN Server is necessary for secure remote access, supporting the Network Administrator’s request for stable remote connectivity. The selected VPN server specifications ensure that remote access remains reliable and secure, even during peak usage.
* Email Server:
* An Email Server with spam and antivirus filtering is recommended to manage internal and external communications. The Publishing Editor’s feedback on accessibility to internal resources supports the need for this dedicated server, allowing efficient communication within the organization.

Task 3

Areas Enhanced in the Networked System:

* Quality of Service (QoS): Implemented to prioritize VPN traffic, improving remote work connectivity.
* Network Bandwidth: Upgraded links between core switches and servers to 10 Gbps, addressing file transfer speeds.
* Wi-Fi Coverage: Adjusted access points and added range extenders in meeting rooms to enhance signal strength.
* VPN Server Performance: Configured to handle high-throughput, reducing connection lags for remote employees.

Impact of Enhancements:

* Remote Connectivity: QoS ensures stable VPN performance, allowing employees to work remotely without interruptions.
* Data Transfer Efficiency: Upgraded bandwidth enables faster file access, especially beneficial for high-volume file transfers by publishing teams.
* Improved Collaboration: Enhanced Wi-Fi coverage ensures reliable connectivity in meeting rooms, facilitating collaboration.
* Data Security and Backup: The optimized setup, including the VPN server and backup server configurations, ensures secure and reliable data access and storage.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test Item | Test Data | Test Action | Expected Result | Actual Results |
| Topology | Test if topology is up and running | Routing tables ping requests | All devices are connected |  |
| Access Control Test | Test if users have the proper roles and permissions | Check the FTP of servers | - Network Administrator should have full access to all server resources.  -Publishing Editor and Publishing Team Leader should have limited or read-only access, depending on their roles.  -Unauthorized access attempts should be denied, maintaining security policies. |  |
| Bandwidth Test | Test if multiple files load properly | Measure upload/download speeds between floors simulation | Network should handle the file transfers smoothly with minimal speed drop. |  |

# Task 4

**Evaluation of Network Topology and Protocols**

**Network Topology:** The network employs a hybrid Star and Tree topology. The core of the network consists of a central router that connects to various network segments, including floors with individual switches that further connect to devices like laptops, servers, and access points.

**Strengths of the Topology:**

* Scalability: The Tree topology allows for easy expansion as additional floors or rooms can be added by connecting new switches to the central backbone.
* Fault Isolation: The Star elements in the topology mean that if a device or segment of the network fails (like a floor switch), it won’t disrupt the rest of the network, maintaining service continuity.
* Centralized Management: The central router acts as a control point, making it easier to monitor, manage, and secure the network from a single location.

**Protocols Used:**

* + Dynamic Host Configuration Protocol (DHCP): This protocol simplifies IP address management by automatically assigning IPs to laptops, desktops, and other devices on the network, ensuring that devices can connect seamlessly without manual IP configuration.
    - Strength: DHCP minimizes administrative effort, reduces IP conflicts, and ensures efficient use of available IP addresses, which is essential for a network with many users and devices.
  + Transmission Control Protocol/Internet Protocol (TCP/IP): This suite of protocols forms the backbone of network communication, enabling reliable data transmission between devices.
    - Strength: TCP/IP provides robust, reliable connectivity for the company's internal and external communications, supporting both local file sharing and internet access.
  + VPN Protocol (e.g., IPsec or OpenVPN): Used for remote access, VPN protocols ensure that employees can securely access the network from external locations.
    - Strength: VPN enhances security by encrypting data between remote employees and the network, protecting sensitive information and allowing for secure remote work.

**Efficiency of the Topology and Protocols**

The combination of the hybrid topology and selected protocols demonstrates efficient network usage by:

* Allowing centralized control and fault isolation, enhancing performance and manageability.
* Supporting seamless device onboarding with DHCP, reducing downtime and human errors.
* Ensuring reliable data communication with TCP/IP, which is critical for daily operations.
* Providing secure remote access through VPN, which accommodates flexible work arrangements.

**Reflection of Final Design**

Overview of the Network Design: The implemented network is designed to support a large, segmented office environment, with a clear separation of floors and departments. Each floor has a dedicated switch connected to a centralized router, which facilitates efficient data flow across the network and enables secure connections to essential services such as the PRS, SPS, and Email servers.

**Strengths of the Network Design:**

* Modularity: The Tree structure allows easy scalability; additional switches or devices can be added without major reconfiguration.
* Reliability: By using dedicated switches for each floor and meeting room, the network is resilient to individual device failures, reducing the risk of widespread downtime.
* Security: The ASA firewall and VPN setup enhance security, particularly for remote access, protecting sensitive company data.

**Areas for Improvement:**

* Load Balancing: If network traffic increases significantly, some links might become bottlenecks. Implementing load balancing on high-traffic areas could help mitigate congestion.
* Redundancy: The design could benefit from additional redundancy, such as backup links or redundant paths between key switches and servers, to enhance fault tolerance further.
* Network Monitoring and Management Tools: Adding network monitoring software would provide real-time visibility, allowing administrators to identify and resolve potential issues before they affect users.

**Reflection on Enhancements**

**Enhancement Areas:**

* VPN Implementation: The VPN setup has improved remote accessibility, allowing employees to securely access the network from external locations, which supports flexible working arrangements and ensures secure remote access to critical resources.
* Firewall Configuration: The addition of an ASA firewall has increased the network’s security posture by protecting internal resources from external threats, which is essential for safeguarding company data and maintaining compliance with security standards.
* DHCP Deployment: Implementing DHCP across the network has streamlined device management, enabling automatic IP assignment. This reduces administrative overhead and simplifies device setup, ensuring that employees can quickly connect their devices.

**Impact of Enhancements on the Company:**

* Improved Security: With VPN and firewall enhancements, the company can ensure data protection and compliance, which is especially important if sensitive client or internal data is handled.
* Operational Efficiency: The automation provided by DHCP reduces the time IT staff spend on network configuration, allowing them to focus on other critical tasks.
* Remote Access Capability: The VPN implementation supports remote work, increasing flexibility and employee satisfaction while maintaining secure access to network resources.

