


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	
Abarca, Francis Roel L.	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: 7/26/24

Content

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

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

2. 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	Example
Wired	<ul style="list-style-type: none"> - Lower Latency - Faster Speeds - More Reliable 	<ul style="list-style-type: none"> - Requires careful planning and routing of cables - Use of Physical Cables 	<ul style="list-style-type: none"> - Ethernet (LAN) - Fiber-Optic Cables (SFP) - Copper
Wireless	<ul style="list-style-type: none"> - More Convenient - Less Cable Management - Quicker to Deploy 	<ul style="list-style-type: none"> - More Expensive - Susceptible to Interference - Less Secure - Higher Latency compared to Wired 	<ul style="list-style-type: none"> - Wi-Fi - Cellular - UWB
Hybrid	<ul style="list-style-type: none"> - Best of Both Worlds - Having the speed when you need it and the convenience when you don't. - Flexible 	<ul style="list-style-type: none"> - Complex Network Management - Costly to Deploy and Maintain - Requiring multiple hardware 	<ul style="list-style-type: none"> - Home Networks (Wired LAN for PC and Wireless for Phones) - Corporate Networks (Wired LAN for Office PCs and Wireless for Company Issued Laptops)

Network Standards	Benefits	Constraints	Purpose	List of Layers
OSI Model	<ul style="list-style-type: none"> - Standardized framework for interoperability and communication between different systems. - Helps in troubleshooting by segmenting functions into layers. 	<ul style="list-style-type: none"> - Theoretical model, not directly used in networking - Some layers are not strictly defined or overlap with TCP/IP 	Defines networking functions in a layered approach to help understand and design communication protocols.	<ul style="list-style-type: none"> - Physical - Data Link - Network - Transport - Session - Presentation - Application
TCP/IP Model	<ul style="list-style-type: none"> - Practical and simplified framework for real-world network communication - Maps directly to protocols widely used on the internet. 	<ul style="list-style-type: none"> - Less detailed compared to OSI. - Does not distinguish as many layers, making it less modular. 	Provides end-to-end communication specifying how data should be packetized, addressed, transmitted, routed, and received.	<ul style="list-style-type: none"> - Interface - Internet - Transport - Application
802.x	<ul style="list-style-type: none"> - Includes various networking standards (e.g., 	<ul style="list-style-type: none"> - Limited to LAN technologies - Focus is on hardware-level 	Specifies protocols for implementing Local Area	Common Standards: <ul style="list-style-type: none"> - 802.3 (Ethernet)

	802.3 is Ethernet and 802.11 for Wi-Fi) - Provides specifications for physical and data link control.	implementation.	Networks (LAN) and Wireless Networks (WLAN).	focuses on Physical and Data Link layers. - 802.11 (Wi-Fi) focuses on wireless communication.
--	--	-----------------	--	--

Impact of Network Topology, Communication, and Bandwidth Requirements

Network Topology

Network topology refers to the layout of connected devices in a network. The topology has a direct impact on performance, scalability, and reliability.

1. Bus Topology:

- **Definition:** In this topology, all devices are connected to a central cable then data is broadcasted to all devices but only the intended recipient processes it.
- **Advantages**
 - i. Simple to set up and cost-effective, requiring less cable compared to other topologies.
 - ii. Suitable for small networks with fewer devices.
- **Disadvantages:**
 - i. If the main cable fails, the entire network goes down.
 - ii. Performance degrades as more devices are added due to collisions.
 - iii. Difficult to troubleshoot because all devices share the same communication line.

2. Star Topology:

- **Definition:** In this topology, all devices are connected to a central hub or switch. This central device manages communication between nodes.
- **Advantages:**
 - i. Easy to add or remove devices without impacting the entire network.
 - ii. If one device fails, it doesn't affect others.
 - iii. Centralized management simplifies troubleshooting and monitoring.
- **Disadvantages:**
 - i. Requires more cabling than a bus topology.
 - ii. The central hub or switch is a single point of failure, and if it goes down, the entire network is affected.

3. Ring Topology:

- **Definition:** In this topology, devices are connected in a circular fashion where each device has exactly two neighbors. Data travels in one direction (or two in a dual ring).
- **Advantages:**
 - i. Predictable performance as data follows a predefined path.
 - ii. Collisions are reduced due to the unidirectional flow of data.
- **Disadvantages:**

- i. A failure in any device or connection can disrupt the entire network.
- ii. Troubleshooting and adding new devices can be challenging.
- iii. Data must travel through each device between the source and destination, increasing latency in larger networks.

4. Mesh Topology:

- **Definition:** In this topology, each device is connected to multiple other devices. This creates numerous paths for data to travel between nodes.
- **Advantages:**
 - i. High redundancy and fault tolerance, as multiple paths exist between devices.
 - ii. The network is highly reliable, if one line fails, data can take an alternate route.
- **Disadvantages:**
 - i. Expensive and complex to install due to the large number of cables and ports required.
 - ii. Configuration and maintenance are challenging due to the complexity of interconnections.

5. Hybrid Topology:

- **Definition:** In this topology, it combines all of the different elements from the other topologies to create a network that leverages their strengths and minimizes weaknesses.
- **Advantages:**
 - i. Provides flexibility by combining benefits of multiple topologies, such as reliability and ease of management.
 - ii. Can be tailored to meet specific organizational needs.
- **Disadvantages:**
 - i. Complex design and configuration can be costly.
 - ii. Troubleshooting issues can be more challenging compared to simple topologies.

Impact of Network Topology on Network Design

- **Scalability**
 - i. Topologies like **star** or **tree** are easier to scale, as devices can be added with minimal impact.
- **Fault Tolerance**
 - i. **Mesh topology** provides excellent fault tolerance, ensuring multiple paths for communication, reducing downtime risks.
- **Cost**
 - i. **Bus topology** is cost-effective for small networks, but as the network grows, topologies like **star** or **mesh** may be required to support performance, increasing installation and maintenance costs.

Communication in Network Design

Communication between devices can be **wired** or **wireless**, and the choice significantly affects the network's performance, reliability, and scalability.

Wired Communication

- Twisted Pair Cables:

i. Definition:

- Twisted pair cables are a type of electrical cable consisting of pairs of insulated copper wires twisted together.
- The two main types:
 - a. **Unshielded Twisted Pair (UTP):** More commonly used for Ethernet cables in networks.
 - b. **Shielded Twisted Pair (STP):** Contains shielding to protect from EMI, used in environments with high interference.

ii. Advantages:

- **Cost-effective:** Twisted pair cables are relatively inexpensive compared to other cable types, making them an affordable choice for shorter distances.
- **Easy to Install:** Flexible and easy to install in a network setup.
- **Widely Available:** They are very common and come in different categories (Cat5e, Cat6, Cat7, etc.) which provide a range of options for different bandwidths.

iii. Disadvantages:

- **Limited Bandwidth and Distance:** Twisted pair cables are generally limited in data transfer speed (depending on the category) and have a short effective range for transmitting signals.
- **Susceptible to Interference:** Although twisting reduces interference, twisted pair cables can still be affected by EMI and cross-talk, particularly UTP cables without additional shielding.
- **Attenuation:** Signal quality diminishes over longer distances, making it unsuitable for very long data runs without signal boosters or repeaters.

- Fiber Optic Cables:

i. Definition:

- Fiber optic cables are network cables that contain one or more optical fibers, which are strands of glass or plastic designed to transmit data as light signals.

ii. Advantages:

- **High Bandwidth:** Fiber optic cables support extremely high data rates and bandwidths, making them ideal for fast internet connections and data transmissions.
- **Long Distance:** Fiber optics can transmit data over much greater distances without significant signal loss, compared to copper cables.
- **Immunity to Interference:** Fiber optic cables are immune to electromagnetic interferences, making them highly reliable in environment with electrical noise.

- **Security:** Since fiber optic cables do not emit signals, they are more secure and difficult to tap into without being detected.

iii. Disadvantages:

- **Cost:** Fiber optic cables and the associated equipment are more expensive compared to twisted pair solutions, especially for small-scale networks.
- **Installation Complexity:** Installing fiber optic cables requires specialized equipment and expertise, as they are more fragile and harder to splice.
- **Fragility:** The glass fibers are more delicate compared to copper, which makes them prone to damage during installation and handling.

Wireless Communication

- **Explanation:** Devices connect to the network using radio waves (Wi-Fi, Bluetooth).
- **Advantages:**
 - i. High flexibility and convenience for devices that need mobility.
 - ii. Quick and easy to set up, especially for large areas.
- **Disadvantages:**
 - i. Signal interference from obstacles or other devices may lead to reduced performance.
 - ii. Less secure than wired communication, requiring stronger security measures.

Impact of Communication on Network Design

- **Deployment Cost:** **Wired networks** often cost more initially but provide stable and high-speed connectivity. **Wireless networks** may be less expensive initially but require investment in maintaining performance and security.
- **Scalability and Flexibility:** **Wireless communication** is better for environments that need flexibility (e.g., offices or campuses). However, **wired communication** is preferred for environments with fixed, high-bandwidth requirements.
- **Security Considerations:** Wired networks are inherently more secure, while **wireless** networks require encryption and secure protocols to protect against data breaches.

Bandwidth Requirements in Network Design

Bandwidth refers to the capacity of a network link to transmit data. It is measured in bits per second (bps) and plays a vital role in the design of an efficient and effective network.

High Bandwidth:

- **Explanation:** High bandwidth means the network can handle a greater volume of data at faster speeds.
- **Advantages:**
 - i. Supports bandwidth-intensive applications like video streaming, VoIP, and data backup.
 - ii. Improves overall network performance and reduces latency, especially for concurrent users.
- **Disadvantages:**
 - i. Higher costs for infrastructure, including cables, switches, and routers that can handle high-speed data.

- ii. Increased power requirements to support high-speed networking hardware.

Low Bandwidth:

- **Explanation:** Low bandwidth refers to limited data transmission capacity.
- **Advantages:**
 - i. Cost-effective solution for small networks or environments with limited data needs.
 - ii. Low maintenance and infrastructure costs.
- **Disadvantages:**
 - i. Network congestion and high latency when many devices are connected or when data-intensive applications are used.
 - ii. Poor performance in applications requiring real-time data transmission or large file transfers.

Impact of Bandwidth Requirements on Network Design

- **Application Requirements:** High-bandwidth networks are essential for data centers, video streaming, and applications with real-time data needs. Low-bandwidth networks are suitable for basic functions like email or web browsing.
- **Network Size:** Large networks, such as corporate or educational institutions, require
- **User Experience:** Sufficient bandwidth is necessary to ensure that end-users have a positive experience, with minimal lag and quick response times. Network congestion due to limited bandwidth can lead to high latency, causing disruptions in performance.

Common Networking Principles

- **OSI Model**

Description: The Open Systems Interconnection (OSI) model is a conceptual framework that standardizes the functions of a telecommunication or computing system into seven distinct layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application. Each layer serves specific roles, allowing for standardized network communication.

- **TCP/IP Model**

Description: The Transmission Control Protocol/Internet Protocol (TCP/IP) model is a simplified framework with four layers: Link, Internet, Transport, and Application. It is used to ensure reliable data transmission across networks, and serves as the foundation for the internet.

- **IP Addressing**

Description: Internet Protocol (IP) addressing assigns unique identifiers (IP addresses) to devices on a network, allowing them to communicate. IPv4 and IPv6 are the two versions, with IPv6 introduced to expand address space due to IPv4 limitations.

- **Subnetting**

Description: Subnetting is a method of dividing a larger network into smaller, manageable segments or subnets. It optimizes network traffic, improves performance, and increases security by limiting broadcast domains.

- **Routing**

Description: Routing is the process of selecting paths in a network along which to send data packets. Routers use protocols like RIP, OSPF, and BGP to determine the best path, ensuring efficient data delivery across networks.

- **Switching**

Description: Switching involves transferring data packets within a local network. Switches operate primarily at the Data Link layer, and can direct data to specific devices, increasing network efficiency and reducing collisions.

- **DHCP (Dynamic Host Configuration Protocol)**

Description: DHCP dynamically assigns IP addresses to devices on a network. This simplifies network management by automatically managing IP assignments, rather than requiring manual configurations.

- **DNS (Domain Name System)**

Description: DNS translates human-readable domain names into IP addresses. This makes it easier for users to access websites without needing to memorize complex IP addresses.

- **NAT (Network Address Translation)**

Description: NAT is a method of modifying IP address information in packet headers while in transit, often used to enable multiple devices on a local network to share a single public IP address.

- **Firewall**

Description: A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules, helping to protect a network from unauthorized access.

- **VPN (Virtual Private Network)**

Description: VPNs create secure, encrypted connections over public networks, allowing users to access remote networks securely as if they were on the local network.

- **QoS (Quality of Service)**

Description: QoS is a mechanism to prioritize specific types of network traffic. It's used to ensure that critical applications (like VoIP or video conferencing) have sufficient bandwidth and low latency.

Network Server Types

Network Server Types	Operating Principle	Function	Impact
Domain Server	Manages a centralized database that stores information about users and devices within a domain using protocols like LDAP.	Provides authentication, authorization, and management of domain resources, enabling centralized control over users and devices.	Centralizes network security and simplifies user/device management, but can become a single point of failure if not replicated.
Web Server	Listens for HTTP/HTTPS requests and serves web pages and applications to clients based on those requests.	Hosts and delivers websites and web applications over the internet.	Allows organizations to establish an online presence but can be vulnerable to cyber-attacks, such as DDoS, if not secured properly.
File Server	Uses network file-sharing protocols (e.g., SMB, NFS) to store, manage, and share files among users.	Centralizes file storage, backup, and sharing to enable easy data access for network users.	Facilitates collaboration and centralized backups but can create network bottlenecks when many users access large files simultaneously.

Database Server	Uses a Database Management System (DBMS) to handle data queries from client devices.	Stores, retrieves, and manages structured data, enabling applications to function effectively.	Enhances application efficiency, but if not optimized, can become a bottleneck, impacting system performance.
DNS Server	Resolves domain names to IP addresses using DNS protocols, allowing devices to access resources using human-friendly URLs.	Provides domain name resolution, translating web addresses to IP addresses.	Simplifies internet navigation but DNS server failure or misconfigurations can lead to service unavailability.
Email Server	Uses SMTP to send, and POP3/IMAP to receive and store emails between users.	Manages email communications, including sending, receiving, and storing messages.	Enables efficient business communication but is vulnerable to spam and phishing if not well secured.
Firewall Server	Uses packet inspection and filtering techniques to control network traffic based on predefined security rules.	Protects the network by filtering incoming and outgoing traffic to prevent unauthorized access.	Provides enhanced network security but can add latency and become a bottleneck if filtering rules are extensive.
IoT Gateway Server	Acts as a bridge between IoT devices and the main network, converting different communication protocols as needed.	Facilitates communication between IoT devices and central systems by aggregating data and converting protocols.	Enables IoT device integration but increases network complexity and opens potential security vulnerabilities.
Routers	Routes data packets between different networks based on IP addresses. Uses routing protocols like RIP, OSPF, or BGP.	Connects different networks and forwards data between them, enabling internetwork communication.	Critical for connecting networks, but incorrect routing configuration can lead to network downtime or data leakage.
Switches	Connects devices within the same network and uses MAC addresses to forward data frames to the appropriate device.	Manages and directs data between devices in a LAN to ensure efficient communication.	Increases network efficiency and reduces collisions but requires proper VLAN configuration for security in larger networks.
Firewall	Monitors and filters incoming and outgoing network packets using security rules to determine if the packet should be allowed.	Protects the internal network from external threats by monitoring traffic and blocking unauthorized access.	Crucial for security but can become a bottleneck if poorly managed, potentially affecting performance.
Repeaters	Amplifies weak signals to extend the reach of a network. Typically operates at the physical layer.	Extends the range of a network by boosting signals that weaken over long distances.	Enhances network coverage, especially in large areas, but doesn't filter traffic, so data collisions might still happen if there is too much traffic.
Bridges	Connects two separate network segments and forwards data based on MAC addresses, operating at the data link layer.	Extends a network by connecting different segments to make them act as a single segment.	Reduces network traffic by dividing collision domains but can introduce slight latency and requires careful configuration.

Workstation Hardware and Networking Software Dependencies

Workstation hardware and networking software are interdependent to ensure seamless connectivity, performance, and stability within a network.

1. Network Interface Card (NIC)

- **Dependency Overview:** The Network Interface Card is a critical hardware component in a workstation that connects it to the network. Networking software, such as drivers and configuration tools, is essential for the proper functioning of the NIC.
- **Hardware Dependency:** The NIC hardware requires networking software drivers to communicate with the workstation's operating system. These drivers enable the NIC to translate data packets between the physical network and the system's memory.
- **Software Dependency:** Networking software, like protocol (e.g., TCP/IP), relies on the NIC to physically transmit data to the network. Without a functional NIC, software that relies on data communication would fail, leading to connectivity loss.

2. Storage

- a. **Dependency Overview:** Storage hardware and network software have a mutual dependency, especially in terms of shared resources and data transfer.
- b. **Hardware Dependency:** Storage on a workstation can be used to store cached data from network activities or temporary files from network communications. Efficient storage devices (e.g., SSDs) are required to keep up with high-speed network transfers and ensure minimal delay in accessing shared resources.
- c. **Software Dependency:** Networking software that facilitates shared storage, such as **Network Attached Storage (NAS)** protocols or **cloud storage clients**, relies on the speed and reliability of the local storage hardware. A slower storage device would increase latency when accessing or saving data, affecting network-based operations, especially in large file transfers.

3. Network Topology and Infrastructure

- a. **Dependency Overview:** The choice of network topology affects how workstations communicate with each other, and this impacts the hardware and software involved.
- b. **Hardware Dependency:** In a **star topology**, for instance, workstations depend on networking hardware, such as switches, to connect effectively. Each workstation must have an appropriate NIC to support the required technology.
- c. **Software Dependency:** Networking software must be configured to work within the specific network topology. In complex **hybrid topologies**, routing protocols and network configuration software become essential in ensuring efficient communication between different workstations. Without appropriate software configuration, network hardware would not be able to optimize traffic flow or manage data efficiently.

4. Bandwidth

- a. **Dependency Overview:** Bandwidth affects how efficiently a workstation can communicate over the network, depending on both the hardware capacity and networking software capabilities.
- b. **Hardware Dependency:** Workstations require a NIC capable of handling the available bandwidth. For instance, a gigabit-capable NIC is necessary if the network infrastructure provides high-speed connections, like **1 Gbps, 10 Gbps or 40 Gbps** links.
- c. **Software Dependency:** Networking software, such as load balancers or Quality of

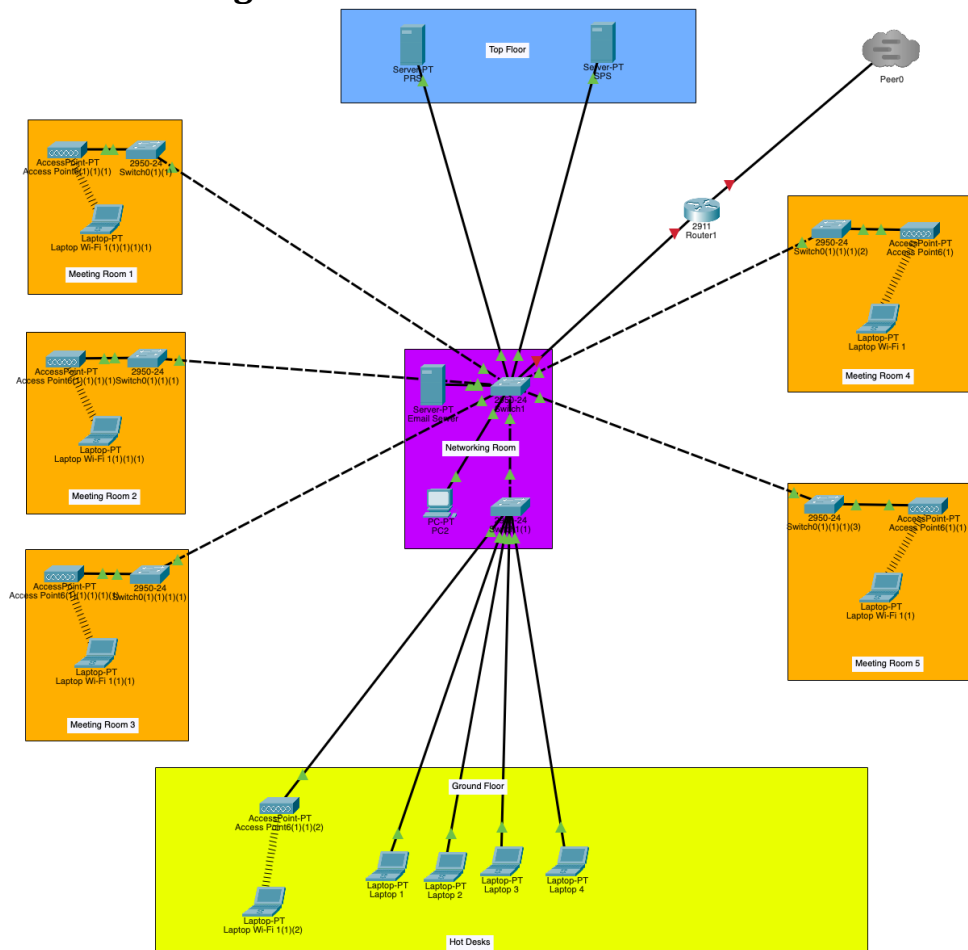
Service (QoS) protocols, relies on adequate hardware to control and allocate bandwidth effectively. If the NIC or other hardware cannot handle high-speed connections, software settings to optimize bandwidth became irrelevant, resulting in network performance bottlenecks.

5. Latency

- Dependency Overview:** Latency refers to the delay in data communication across the network, influenced by both hardware and software factors.
- Hardware Dependency:** Lower latency in data transmission is dependent on high-performance NICs, quality cables, and switches. Workstation hardware must be capable of quickly processing and transmitting data to minimize latency.
- Software Dependency:** Networking software protocols and settings also play a crucial role in reducing latency. Software like **TCP optimization**, error-checking algorithms, and network stack configurations depend on hardware that supports fast data transfers. If the hardware does not support the intended speed, software adjustments to reduce latency would be ineffective.

Task 2

Network Design



Device Configuration and Security Considerations

- Device Configuration
Each networked device will be configured according to SBP's security policies to maintain secure data access control and privacy. Key configurations include:
 - i. File Server
 - ii. Public Repository Server (PRS)
 - iii. Secure Publishing Server (SPS)
 - iv. Email Server
 - v. Company-issued Laptops
 - vi. Network Administrator's PC
- Security Considerations
To enhance security across SBP's network, the following measures are planned:
 - i. Hardware Firewalls
 - ii. VPN Access

Maintenance Schedule

No.	Equipment Description	Condition	Maintenance Frequency (Days)	Description of Maintenance Activity	Assignee	Last Maintenance Date	Next Maintenance Date
1	File Server	Good	30	Inspection, Access Logs, Firmware Updates, Backup Check	Network Admin	2024-09-11	
2	Public Repository Server	Good	15	Security Check, Data Encryption Audit	Network Admin	2024-09-11	
3	Secure Publishing Server	Good	30	Content Review, Backup Check, System Updates	Network Admin	2024-09-11	
4	Email Server	Good	15	Security Check, Check System Updates, Backup Check	Network Admin	2024-09-11	
5	Company-issued Laptops	Fair	90	Inspection, Access Logs, Virus Check	Senior IT	2024-09-11	
6	Network Administrator's PC	Good	60	Inspection, Firmware Updates	Senior IT	2024-09-11	

Test Plan

Test Item	Test Action	Test Data	Expected Results
Topology	Test if the topology is up and running.	Routing tables, Ping test outputs	All networking devices are connected.

Access Speed	Test file transfer performance for all employees.	Event Simulation	Sustained performance.
File Access	Test access restrictions for Publishing Teams.	Access logs	Each PE has access only to their content.

Analysis of User Feedback for Design Optimization

Summary of Feedback Gathered:

Feedback from 3 users highlighted occasional network lag during remote access and FTP transfers and there was also a request for a more robust backup schedule to prevent data unavailability.

Analysis for Efficiency Improvement

To improve network efficiency and address the feedback:

- Bandwidth Allocation: Improve load balancing for remote access during peak hours can help minimize delays and improve overall user experience.
- Adding Access Points per room: Improve network speed significantly and allows more users to be connected per room.

Network Design Optimization and Improvements

Implemented Changes Based on Analysis

- Bandwidth Optimization: Dedicated load balancers for remote access were implemented to reduce lag and ensure smoother performance for remote users.
- Revised Backup Schedule: Backups are now scheduled to occur during off-peak-hours, ensuring uninterrupted access to shared resources during business hours.
- Firewall Addition: Added a firewall between the main server and the switch to increase network security.
- Individual Switches and Access Points: Installed dedicated switches and wireless access points per room and floor for enhanced performance and supporting more users.
- Fiber Optic Cables for Server Connections: Fiber optic cables were utilized for server connections, providing high-speed and lower latency data transfer.

Network Server Types and Recommended Selection

Here are a range of Server Types and Recommended Selection:

1. File Server

- a. Recommended Model: Custom SuperMicro Server
- b. Specifications:
 - i. 24-core AMD EPYC 9255 CPU
 - ii. SuperMicro MBD-H13SSL-NT Motherboard
 - iii. 128GB DDR5-4800 ECC memory
 - iv. 40TB worth of Seagate EXOS HDDs in RAID Z
 - v. 8TB Samsung PM1725b NVME SSD
 - vi. Mellanox SFP NIC
- c. Cost: \$9,000
- d. Description: This custom File Server is designed for the utmost speeds and has the highest upgradability for the requirements of SBP Publishing. The AMD EPYC CPU is also known for its great performance and efficiency that it also saves them power with this server.

2. File and Data Storage Servers

- a. Recommended Model: Custom Gigabyte Server

- b. Specifications:
 - c. Cost: \$6,000
 - d. Description:
3. Backup Server
- a. Recommended Model: 45Drives Storinator 32 Bay 4U
 - b. Specifications:
 - i. 16-core AMD EPYC 9135 CPU
 - ii. SuperMicro MBD-H13SSL-NT Motherboard
 - iii. 64GB DDR5-4800 ECC RAM
 - iv. 250TB worth of Seagate EXOS HDDs in RAID Z
 - v. 960GB Intel Optane 900P SSD
 - vi. Intel 40 Gigabit NIC
 - c. Cost: \$6,000
 - d. Description:
4. Email + DHCP Server
- a. Recommended Model:
 - b. Specifications:
 - c. Cost:
 - d. Description:

Justification of Recommended Server Selection

Cost and Performance Optimization:

- **Cost Efficiency**
By selecting custom-built servers with AMD EPYC processors, we maximize performance while staying within a \$20,000 budget. SuperMicro, Gigabyte, and Storinator options are cost-effective compared to brands like HP ProLiant and Dell PowerEdge, which tend to be more expensive due to bundled support contracts.
- **Performance Optimization**
AMD EPYC processors offer high core counts and powerful multi-threading capabilities, allowing these servers to handle multiple simultaneous tasks, ideal for file sharing, VPN, and DHCP roles. The inclusion of Mellanox SFP connections for the main file servers ensures minimal network bottlenecks and high-speed access.
- **Storage Reliability and Scalability**
The file server's 40TB of Seagate EXOS HDD storage with 8TB NVMe SSD caching supports fast data retrieval and ample storage capacity for SBP's publishing needs. The backup server's 250TB of RAID Z storage ensures robust, long-term data retention, with ZFS caching provided by a 1TB SSD and 64GB RAM.
- **Customization and In-House Maintenance**
These server configurations provide SBP's IT team with flexibility in maintenance and upgrades. With skilled IT staff, SBP can avoid the high costs of relying on vendor support and instead perform custom troubleshooting and scaling as needed. This approach aligns well with SBP's preferences for self-sufficient infrastructure, where cloud services like Azure, AWS, or GCP are preferable for managed solutions rather than daily operational needs.

This custom-built solution not only meets SBP's operational requirements but also offers high performance and adaptability for future growth, delivering significant long-term value without exceeding the budget.

Task 3

Areas Improved in the Company Network

- **Quality of Service (QoS):** Implemented to improve network transfer locally and VPN connectivity too for remote access.
- **Network Bandwidth:** Improved the network access and distribution across the building with Gigabit speeds and multiple switches.
- **Wi-Fi Coverage:** Added multiple access points per Meeting Room instead of 1 for the whole floor to increase performance and coverage.

Impact of Enhancements

1. Quality of Service (QoS) Implementation

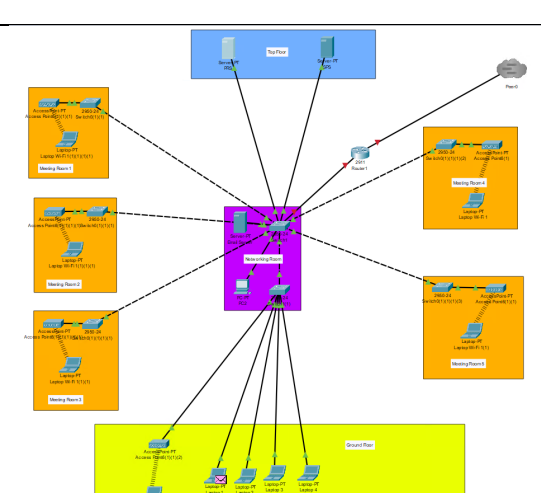
By implementing QoS, network performance has been optimized for both local transfers and remote VPN access. This prioritization of critical traffic helps prevent congestion, especially during peak usage times, ensuring that essential operations like file sharing, video conferencing, and remote access proceed smoothly. As a result, employees working remotely or accessing resources from outside the office experience reduced lag, faster data access, and improved overall connectivity.

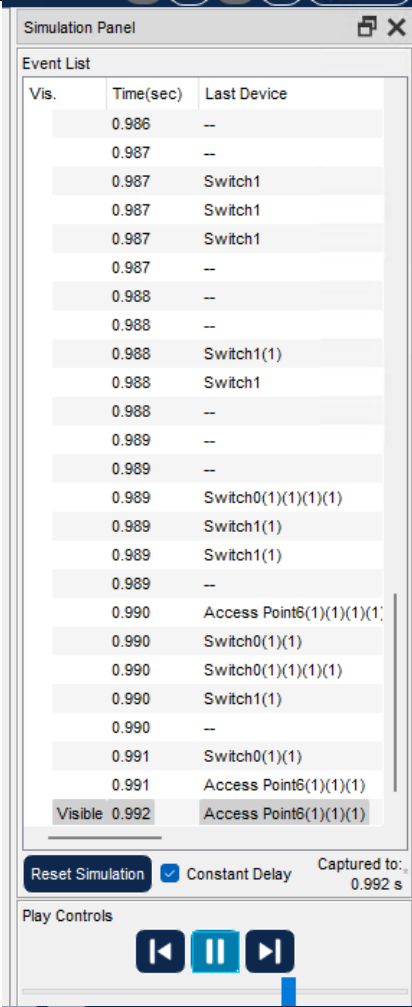
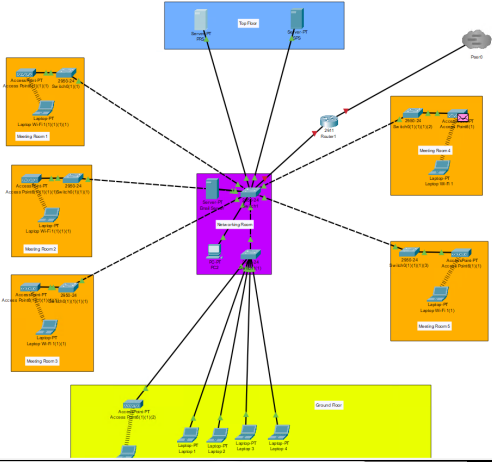
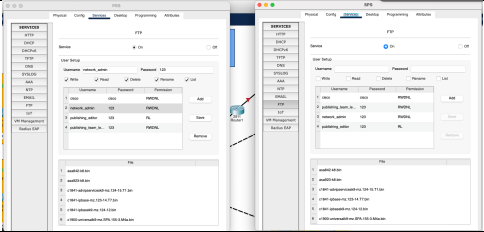
2. Improved Network Bandwidth

Upgrading the network to support Gigabit speeds and deploying additional switches throughout the building have enhanced data transfer rates, ensuring high-speed connectivity for all users. This increased bandwidth availability supports data-intensive applications, minimizes delays when transferring large files, and provides a more responsive experience when accessing shared resources. The deployment of multiple switches also improves load distribution, reducing the risk of network bottlenecks and creating a more scalable and resilient network infrastructure to accommodate future growth.

3. Enhanced Wi-Fi Coverage

By adding dedicated access points to each meeting room rather than relying on a single access point per floor, Wi-Fi performance and coverage have greatly improved. This enhancement provides stronger, more stable wireless connectivity, allowing employees to collaborate seamlessly in meetings and access network resources without interruption. The targeted placement of access points also reduces network interference and enhances signal strength, ensuring that users in high-traffic areas receive reliable, high-quality wireless service.

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 Speed	Test file transfer performance for all employees.	Event Simulation	Sustained performance .	 
File Access	Test access restrictions for Publishing Teams.	Access logs	Each PE has access only to their content.	

Task 4

Evaluation of Network Topology and Protocols

Network Topology:

The network design utilizes a hybrid Star and Tree topology. At the core of the setup is a central router, which connects to various network segments across floors, each of which has its own switch. These switches then connect to devices such as laptops, servers, and wireless access points.

Strengths of the Topology:

- **Scalability:** The Tree topology allows the network to grow easily, as new floors or rooms can be connected by simply adding switches to the central backbone.
- **Fault Isolation:** The Star components in the topology ensure that if a single device or segment (like a floor's switch) encounters an issue, the rest of the network remains unaffected, providing greater continuity.
- **Centralized Management:** The central router acts as a focal point for network control, simplifying monitoring, management, and security from a single location.

Protocols in Use:

- **Dynamic Host Configuration Protocol (DHCP):** DHCP automates IP address assignments, enabling seamless connectivity for laptops, desktops, and other network devices without manual IP configuration.
 - **Strength:** DHCP reduces administrative workload, minimizes IP conflicts, and optimizes IP address usage, which is essential given the number of devices and users on the network.
- **Transmission Control Protocol/Internet Protocol (TCP/IP):** TCP/IP forms the foundation of the network's communication framework, ensuring reliable data transfer across devices.
 - **Strength:** TCP/IP provides reliable and robust connectivity for internal and external communication, supporting critical functions like local file sharing and internet access.

Network Efficiency through Topology and Protocols

The hybrid topology combined with these protocols enables efficient network operation by:

- Enabling centralized control and fault isolation, which improves performance and manageability.
- Allowing streamlined device connectivity with DHCP, reducing downtime and configuration errors.
- Ensuring stable data communication via TCP/IP, essential for daily workflows.

Reflection on Final Network Design

Overview of the Network Structure:

The network is structured to support a segmented office environment, with each floor and department operating independently but securely interconnected. Each floor has its own switch connected to a central router, which maintains efficient data flow and allows access to essential services such as the PRS, SPS, and Email servers.

- **Modularity:** The Tree topology supports modular expansion, allowing new devices or floors to be added with minimal reconfiguration.
- **Reliability:** Dedicated switches per floor and per room enhance network reliability, isolating potential failures to specific areas and minimizing downtime.
- **Security:** The integration of an ASA firewall strengthens security by protecting internal resources from external threats, safeguarding sensitive data and supporting compliance.

Areas for Potential Improvement:

- **Load Balancing:** As network traffic grows, some links may become congested. Implementing load balancing in high-traffic areas would help distribute data more evenly and reduce bottlenecks.
- **Redundancy:** Adding backup links or redundant paths between key switches and servers would further enhance fault tolerance and network resilience.
- **Network Monitoring Tools:** Incorporating real-time network monitoring software would allow proactive identification and resolution of issues, enhancing overall reliability.

Reflection on Recent Network Enhancements

Enhancement Focus Areas:

- **DHCP Deployment:** DHCP implementation across the network simplifies device management, enabling automatic IP address assignment. This reduces administrative effort and allows employees to connect quickly.
- **Network Quality Improvements:** Enhancements like Quality of Service (QoS) and the addition of SFP connections for critical servers have optimized data transfer speeds and provided high-speed access for essential services.

Impact of Enhancements on Company Operations:

- **Enhanced Security:** With the firewall in place, the company can better protect its data and meet security compliance requirements, crucial for safeguarding client and internal data.
- **Increased Operational Efficiency:** DHCP automation frees up IT resources by simplifying network configuration, allowing staff to focus on other critical tasks.
- **Improved Network Performance and Accessibility:** QoS and optimized connections facilitate smoother network operations, improving both local and remote access, leading to higher employee productivity and satisfaction.