**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 |  | |  |
|  | | | |
| **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

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** | **Example** |
| **Wired** | - Lower Latency  - Faster Speeds  - More Reliable | - Requires careful planning and routing of cables  - Use of Physical Cables | - Ethernet (LAN)  - Fiber-Optic Cables (SFP)  - Copper |
| **Wireless** | - More Convenient  - Less Cable Management  - Quicker to Deploy | - More Expensive  - Susceptible to Interference  - Less Secure  - Higher Latency compared to Wired | - Wi-Fi  - Cellular  - UWB |
| **Hybrid** | - Best of Both Worlds  - Having the speed when you need it and the convenience when you don’t.  - Flexible | - Complex Network Management  - Costly to Deploy and Maintain  - Requiring multiple hardware | - 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** | - Standardized framework for interoperability and communication between different systems.  - Helps in troubleshooting by segmenting functions into layers. | - 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. | - Physical  - Data Link  - Network  - Transport  - Session  - Presentation  - Application |
| **TCP/IP Model** | - Practical and simplified framework for real-world network communication  - Maps directly to protocols widely used on the internet. | - 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. | - Interface  - Internet  - Transport  - Application |
| **802.x** | - Includes various networking standards (e.g., 802.3 is Ethernet and 802.11 for Wi-Fi)  - Provides specifications for physical and data link control. | - Limited to LAN technologies  - Focus is on hardware-level implementation. | Specifies protocols for implementing Local Area Networks (LAN) and Wireless Networks (WLAN). | Common Standards:  - 802.3 (Ethernet) 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**
     1. Simple to set up and cost-effective, requiring less cable compared to other topologies.
     2. Suitable for small networks with fewer devices.
   * **Disadvantages:**
     1. If the main cable fails, the entire network goes down.
     2. Performance degrades as more devices are added due to collisions.
     3. 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:**
     1. Easy to add or remove devices without impacting the entire network.
     2. If one device fails, it doesn’t affect others.
     3. Centralized management simplifies troubleshooting and monitoring.
   * **Disadvantages:**
     1. Requires more cabling than a bus topology.
     2. 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:**
     1. Predictable performance as data follows a predefined path.
     2. Collisions are reduced due to the unidirectional flow of data.
   * **Disadvantages:**
     1. A failure in any device or connection can disrupt the entire network.
     2. Troubleshooting and adding new devices can be challenging.
     3. 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:**
     1. High redundancy and fault tolerance, as multiple paths exist between devices.
     2. The network is highly reliable, if one line fails, data can take an alternate route.
   * **Disadvantages:**
     1. Expensive and complex to install due to the large number of cables and ports required.
     2. 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:**
     1. Provides flexibility by combining benefits of multiple topologies, such as reliability and ease of management.
     2. Can be tailored to meet specific organizational needs.
   * **Disadvantages:**
     1. Complex design and configuration can be costly.
     2. Troubleshooting issues can be more challenging compared to simple topologies.

**Impact of Network Topology on Network Design**

* + **Scalability**
    1. Topologies like **star** or **tree** are easier to scale, as devices can be added with minimal impact.
  + **Fault Tolerance**
    1. **Mesh topology** provides excellent fault tolerance, ensuring multiple paths for communication, reducing downtime risks.
  + **Cost**
    1. **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:** 
    1. **Definition:** 
       - Twisted pair cables are a type of electrical cable consisting of pairs of insulated copper wires twisted together.
       - The two main types:
         1. **Unshielded Twisted Pair (UTP):** More commonly used for Ethernet cables in networks.
         2. **Shielded Twisted Pair (STP):** Contains shielding to protect from EMI, used in environments with high interference.
    2. **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.
    3. **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:**
    1. **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.
    2. **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.
    3. **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:**
    1. High flexibility and convenience for devices that need mobility.
    2. Quick and easy to set up, especially for large areas.
  + **Disadvantages:**
    1. Signal interference from obstacles or other devices may lead to reduced performance.
    2. 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:**
    1. Supports bandwidth-intensive applications like video streaming, VoIP, and data backup.
    2. Improves overall network performance and reduces latency, especially for concurrent users.
  + **Disadvantages:**
    1. Higher costs for infrastructure, including cables, switches, and routers that can handle high-speed data.
    2. Increased power requirements to support high-speed networking hardware.

**Low Bandwidth:**

* + **Explanation:** Low bandwidth refers to limited data transmission capacity.
  + **Advantages:**
    1. Cost-effective solution for small networks or environments with limited data needs.
    2. Low maintenance and infrastructure costs.
  + **Disadvantages:**
    1. Network congestion and high latency when many devices are connected or when data-intensive applications are used.
    2. 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**

|  |  |  |  |
| --- | --- | --- | --- |
| **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
   1. **Dependency Overview**: Storage hardware and network software have a mutual dependency, especially in terms of shared resources and data transfer.
   2. **Hardware Dependency**: Storage on a workstation can be used to store cached data from network activities or temporary files form 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.
   3. **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
   1. **Dependency Overview**: The choice of network topology affects how workstations communicate with each other, and this impacts the hardware and software involved.
   2. **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.
   3. **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
   1. **Dependency Overview**: Bandwidth affects how efficiently a workstation can communicate over the network, depending on both the hardware capacity and networking software capabilities.
   2. **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.
   3. **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
   1. **Dependency Overview**: Latency refers to the delay in data communication across the network, influenced by both hardware and software factors.
   2. **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.
   3. **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**

Network Design

Task 3

**Task Statement :**

Task Solution :

# Task 4

Task Statement :

Task Solution :



# Bibliography