**Student Declaration**

I confirm the following details:

|  |  |
| --- | --- |
| **Candidate Name:** | **Mr. Thant Pyae Shine** |
| **Candidate ID Number:** | **050423008** |
| **Qualification:** | **NCC Level-4 Diploma in Computing** |
| **Unit:** | **Computer Network** |
| **Centre:** | **NMA University** |
| **I have read and understood both NCC Education’s *Academic Misconduct Policy* and the *Referencing and Bibliographies* document. To the best of my knowledge my work has been accurately referenced and all sources cited correctly.**  I confirm that this is my own work and that I have not colluded or plagiarised any part of it. | |
| **Candidate Signature:** | A black background with a black background  Description automatically generated |
| **Date:** | **14.06.2024** |

**Contents**

[**Task 1 Planning a Network 3**](#_Toc181399076)

[**a) Logical Topology 3**](#_Toc181399077)

[**b) Redundant Network Topology 4**](#_Toc181399078)

[**Task 2 Network Operating Systems 7**](#_Toc181399079)

[**a) Network Operating Systems (NOS) 7**](#_Toc181399080)

[**b) Issues After End of Life on NOS 8**](#_Toc181399081)

[**Task 3 Design the Network 10**](#_Toc181399082)

[**Network Elements 10**](#_Toc181399083)

[**Calculating IP Addresses 11**](#_Toc181399084)

[**Logical Network Design 13**](#_Toc181399085)

[**Task 4 VPN 15**](#_Toc181399086)

[**Benefits 15**](#_Toc181399087)

[**Cons 15**](#_Toc181399088)

[**Task 5 Firewalls 17**](#_Toc181399089)

[**Software Firewall 17**](#_Toc181399090)

[**Hardware Firewall 17**](#_Toc181399091)

[**Task 6 Network Recommendation 19**](#_Toc181399092)

[**a) Scalability Recommendations 20**](#_Toc181399093)

[**b) Security Aspects 20**](#_Toc181399094)

[**References 22**](#_Toc181399095)

# Task 1 Planning a Network

## a) Logical Topology

Logical topology refers to theoretical design of a network system that illustrates how data flows between the network elements. It specifies how data is transferred regardless of detailed arrangement of the traffic. As contrast to physical topology, logical topology includes only the necessary connections between the network devices.

Logical Topology Diagrams show how data travels from one point to another within a system. The primary focus on a logical topology is the connection between the endpoints, but not the physical connections along the network.

In simplest form, logical typology clarifies logical relationships among devices and the paths that information takes to get to its intended location. Regardless of the physical media, these connections are illustrated with virtual channels to address systems and network protocols.

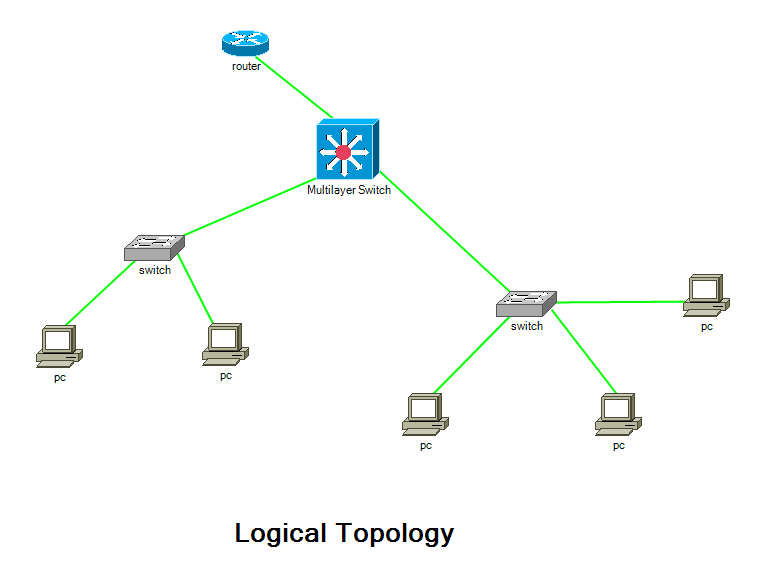


Figure 2.1 : Logical Topology Diagram

The diagram above illustrates a logical representation of a network, where devices are representatively linked through logical connections, Ethernet. This illustration showcases the logical pathways through which data flows for a conceptual understanding of a network communication.

One of the main components of logical topology is the establishment of logical links or paths between devices that are independent of physical constraints. Typically, these links are defined by addressing schemes, routing algorithms, and network protocols. To ensure effective and reliable communication, logical topology controls how data packets are routed from the source to the destination across the network.

In computer network design and management, logical topology is essential because it establishes the network's ability for efficient data transmission and its resilience to failures. Overall network stability can be improved, guaranteed and performance can be maximized by knowing fundamentals of logical topology.

## b) Redundant Network Topology

A mesh network topology would be most suitable to reduce the risks of communication failures due to access point failures. Every node or access point in a mesh network connects to several other nodes to form a decentralized network architecture. When there is a disruption at an access point, the network can actively redirect traffic to alternative paths to minimize any delays. This redundancy is crucial for maintaining uninterrupted communication.

This redundancy is crucial for maintaining constant communication, especially in environments where reliability is critical. Applications such as emergency response systems, military communications, and smart city infrastructure greatly benefit from this robustness provided by mesh networks.

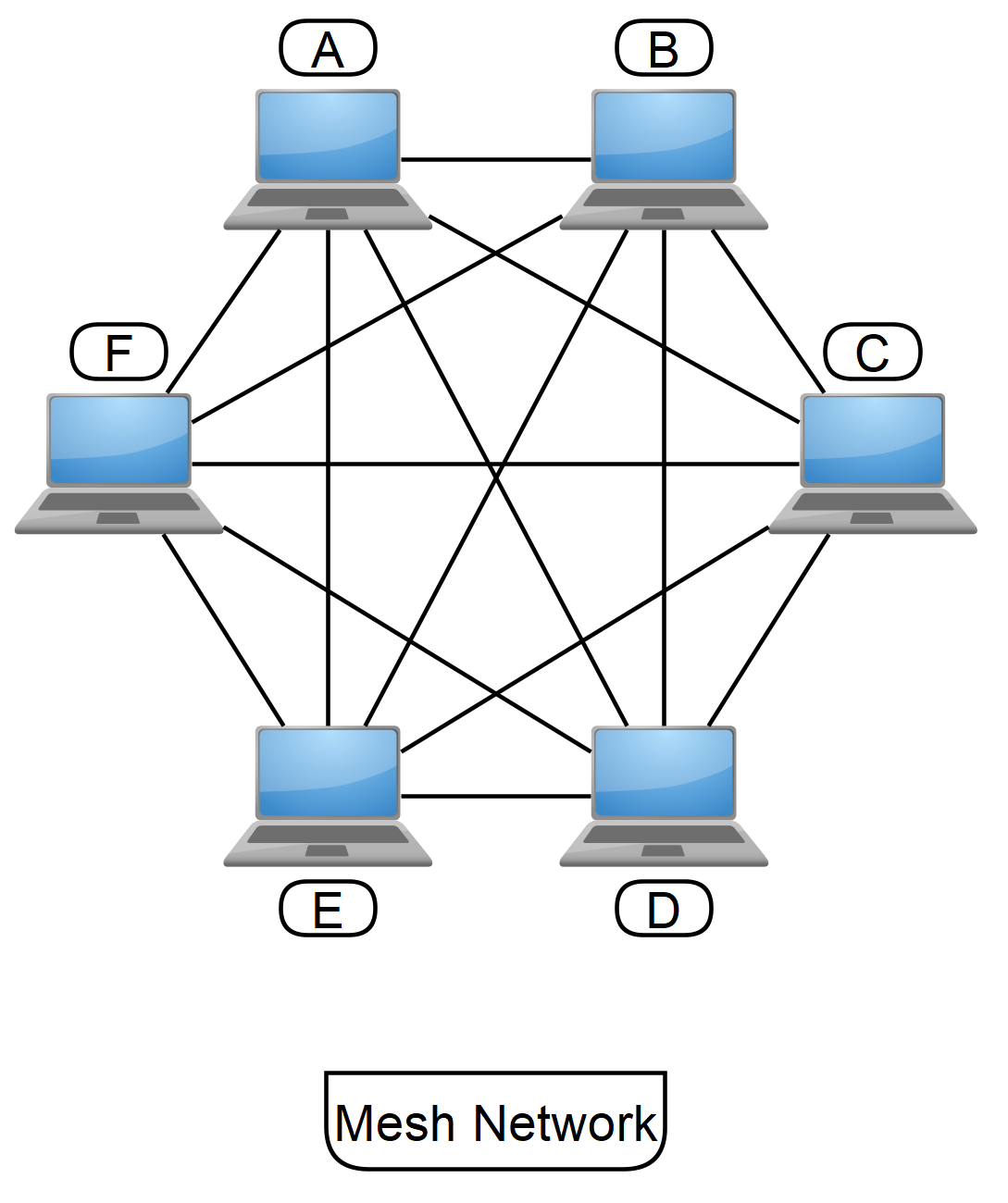


Figure 1.2: Mesh Topology Diagram

Each access point in this diagram is connected to other access points in the locality to create a structure that resembles a mesh. Devices connected to access points B and C can continue to communicate in the event of a malfunction by rerouting data flows through operational access points A, D, E, and F.

Mesh networks are very flexible and fault-tolerant for the fact that they have a large number of redundant channels. They perform exceptionally well in environments like large corporate buildings or college campuses where dependability and continuous connectivity is essential.

Mesh networks offer high flexibility and fault tolerance because of their multitude of redundant paths. This also makes them ideal for scenarios where reliability and continuous connectivity are essential, such as in large office buildings or campuses.

It is important to understand that a mesh network's real-world application could vary significantly based on a variety of factors, such as device capabilities, network size, and specific operating requirements. Because of this, careful design and modification are essential to ensuring that the mesh network architecture is customized to the specific requirements of the environment or organization it serves.

# Task 2 Network Operating Systems

## a) Network Operating Systems (NOS)

Network operating system or ‘NOS’ is a kind of operating system designed for network services and protocols for network devices like routers or servers. It consists of typical functions for file sharing, remote access, security services as well as network protocols.

The role of an operating system is to serve as midway between hardware device and user. Users interact with operating systems on their devices through graphical user interface (GUI) to access and manipulate the software or information on the device. Similarly, a network operating system (NOS) links user devices and servers within a network for smooth sharing of resources among them.

Examples of Proprietary Network Operating Systems are Microsoft Windows Server, Novell NetWare.

Examples of Open-Source NOS are Ubuntu Server, FreeBSD.

Advantages of Open-Source NOS

**Flexibility:** Open-source software usually grants public access to their source code. It enables users to modify the software according to individual needs.

**Community Support:** Being open source, large developer community can join the ongoing development to improve productivity.

**Affordability:** Open-source Network Operating Systems are mostly free to use, reducing not only initial investment but also long-term expenses for license fees.

Disadvantages of Open-Source NOS

**Limited Vendor Support:** Despite community support, open-source systems often lack vendor support. It slows down the improvement of fundamental functions on the system.

**Integration Difficulties:** Open-source system software sometimes encounters compatibility issues with licensed hardware or software.

**Security Risks:** Although the community can help with development, there’s no guarantee that open-source operating systems are vulnerable to specific security attacks if not properly maintained.

## b) Issues After End of Life on NOS

Security Vulnerabilities

After EOL products no longer receive software updates, they tend to have unpatched vulnerabilities that can be benefited by hackers or ransomware. Without updates patches, expired operating systems become more vulnerable to security abuses and sensitive data and network infrastructure are at risk. This can have severe consequences such as potential harm to victims, financial losses, legal implications, and most importantly reputational damage.

Compliance Violations

Organizations must sometimes deal with conflicting rules and requirements from different authorities. EOL products may not meet regulatory standards or industry-specific requirements. For example, financial institutions have a rather complex and diverse regulatory environment than a productive industry. Financial institutions require very strict data protection and privacy policies. As such, failure to follow industry regulations and standards by running expired NOS can result in serious compliance violations, exposing organizations to legal consequences and financial penalties.

Incompatibility with New Technologies

Expired NOS may not support newer network technologies, or protocols, limiting the organizations’ ability to adopt new technologies and innovations. With EOL operating systems, organizations are forced to continue running older applications. These applications themselves are probably facing their end-of-support too.

Reduced Performance and Reliability

Outdated NOS also lacks compatibility for modern hardware and software, leading to decreased network performance and efficiency. These products may become slower over time as they must encounter more data or tasks than they were initially designed for. Not only that but end-of-Life products can become less stable or reliable since they may encounter more malfunctions, or bugs that are no longer resolved by the manufacturer.

Added Expense

The operation costs required to maintain and fix an OS without vendor support can be quite high. This added expense includes not only the budgets for maintaining system issues but also the indirect costs correlated with potential system downtime and deficiency of productivity.

# Task 3 Design the Network

According to the requirements of WeBuyAnyVehicle’s network structure, the design for new network space must prioritize scalability, security enhancement, and wireless connectivity. With a workspace of 200 minimum employees, the network must accommodate seamless connectivity while ensuring flexibility and adaptability to future growth.

## Network Elements

Network devices to be included are listed below.

Router: The router acts as a gateway between its internal network and external Internet. It enables data transmission and routing traffic between different network segments.

Switches: To facilitate effective communication and data exchange between devices, switches are used to link multiple devices within a network.

Wireless Access Points (APs): Also known as wireless routers, APs offers wireless connectivity to mobile devices such as laptops, smartphones, so that staff members can access the network wirelessly from any location in the office.

Firewall: By monitoring and regulating incoming and outgoing network traffic to avoid unauthorized access and potential security breaches, the firewall serves as a barrier between the internal network and external threats.

File Server: Crucial company data is managed and stored on the file server. Its goal is to make file sharing between network devices easier.

## Calculating IP Addresses

Utilizing appropriate IPv4 address schemes, IP addresses and subnet masks will now be assigned to each network segment based on the specified accommodation for staff members in HR and Finance, Management, IT, and shared presence.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rooms | Slash Notation | Network Address | Broadcast Address | Host Address Range | Subnet Mask |
| Shared presence | /24 | 192.168.10.0 | 192.168.10.255 | 192.168.10.1  to  192.168.10.254 | 255.255.255.0 |
| IT | /26 | 192.168.11.0 | 192.168.11.63 | 192.168.11.1  to  192.168.11.62 | 255.255.255.192 |
| HR & Finance | /27 | 192.168.11.64 | 192.168.11.95 | 192.168.11.65  to  192.168.11.94 | 255.255.255.224 |
| Management | /28 | 192.168.11.96 | 192.168.11.111 | 192.168.11.97  to  192.168.11.110 | 255.255.255.240 |

This satisfies the initial device allocation from each room. However, future development was not considered in this calculation. For instance, the usable address for HR & Finance is 30, which is the exact number the company asked for. This satisfies the immediate requirements of the company. However, it is important to recognize that future development and growth need to be considered to ensure the scalability and longevity of the network infrastructure.

To accommodate future growth, IP address allocation for each network segment will be adjusted to allow for at least a 10% increase in staff numbers.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rooms | Slash Notation | Network Address | Broadcast Address | Host Address Range | Subnet Mask |
| Shared presence | /24 | 192.168.10.0 | 192.168.10.255 | 192.168.10.1  to  192.168.10.254 | 255.255.255.0 |
| IT | /26 | 192.168.11.0 | 192.168.11.63 | 192.168.11.1  to  192.168.11.62 | 255.255.255.192 |
| HR & Finance | /26 | 192.168.11.64 | 192.168.11.127 | 192.168.11.65  to  192.168.11.126 | 255.255.255.192 |
| Management | /28 | 192.168.11.128 | 192.168.11.143 | 192.168.11.128  to  192.168.11.142 | 255.255.255.240 |

## Logical Network Design

A diagram of a network

Description automatically generated

Figure 3.1 : Logical Diagram for WeBuyAnyVehicle

**Network Layout Description**

This suggested network configuration for WeBuyAnyVehicles's new office is designed to offer a scalable, secure, and effective infrastructure to accommodate a wide range of demands of the company. A firewall is the main component of the network and hence positioned ahead of the main router to prevent outside threats. By ensuring examined and filtered traffic, this firewall protects the internal network from potential cyberattacks and unauthorized accesses.

A Layer 3 switch connected to the primary router serves as network's central hub for traffic routing. Maintaining smooth and effective communication, this Layer 3 switch can improve network performance and lower latency.

Many Layer 2 switched, extending from that of Layer 3, are positioned properly in each office room. These Layer 2 switches facilitate seamless communication between devices in the same room and offer localized control over network connectivity within each department, making network management easier.

A Wireless Access Point (AP) is additionally linked to the highest-level switch. This Wireless AP promotes flexibility and mobility in the workplace by enabling users to safely access the network from anywhere in the building.

Additionally, the IT department has a server that is linked to its local switch. With permission to access it from any room, this server can act as a central repository for vital business information and resources. The network design can make it possible for devices in various departments, like Management or HR & Finance, to communicate directly with the IT department server, which promotes effective workflow and smooth teamwork.

In conclusion, the proposed network architecture emphasizes security, effectiveness, and smooth communication while providing a solid and scalable infrastructure. Applying Layer 3 switching and carefully placing network devices, it provides WeBuyAnyVehicle a strong platform upon which to run its business and grow in the future.

# Task 4 VPN

VPN represents "Virtual Private Network”. It is a utility which establishes a secure network. It hides the user’s true IP address and generates a virtual address, allowing security and anonymity. Users can also use this to remotely access services that are beyond public access.

To implement a VPN, we first require a VPN server between our organizational network and the computer which administrates IPs. The server serves as medium to encrypt the data before it is transmitted on the internet. Through VPN software, users can connect on it to the VPN server in a secure manner. Upon connection, the VPN client software and VPN server would make an encrypted tunnel, established a secure and anonymity.

## Benefits

**Extra protection:** It reduces the chance of a data breach because it encrypts data therefore eavesdropping and information interception cannot happen. This makes VPNs efficient.

**Convenience:** VPN users can access the private network from anywhere since it is connected over the Internet.

**Cost-effective:** They cut down the cost required to set up an office Virtual private network as one does not have to rent physical space for their employees to occupy hence reduce commuting money.

**Helps employees access resources:** Limited geo-access companies do not have to worry anymore. Employees will be able to connect to the company’s website as if they were outside their private network.

## Cons

**Complicated setup and maintenance:** VPN communication is hard to set up and keep up. Once the network is up and running, it will require ongoing maintenance to stay that way.

**Performance Impact: Network performance may be decreased while data undergoes encryption and decryption inside a VPN tunnel.**

**Dependent on Internet Connectivity:** Internet service providers’ poor connectivity or network bottleneck will result in a bad internet connection, which will cause connectivity issues worse, and affect user experience.

**Security problems:** The VPN creates a secure connection and secures your connection from any internet point. However, if the VPN server is poorly managed or configured, data is more vulnerable and other security hazards may emerge.

# Task 5 Firewalls

## Software Firewall

A software firewall is a program or application installed on a device within the host’s operating system. It functions by logically controlling network traffic on the device it is installed on. Software firewalls are installed on individual devices, such as computers or mobile devices. They filter traffic only at their device level.

Advantages

**Cost-effective:** due to the lack of hardware units, software firewalls are undoubtedly more affordable than hardware firewalls.

**Customizability:** software firewalls are also known for better customizability, allowing each user to modify individual devices’ security policies according to their preferences.

Disadvantages

**Limited Protection:** software firewalls only protect the device on which they are installed.

**Dependence on Host System:** software firewalls mainly rely on the host’s operating system, making them more vulnerable when host devices were to fail.

**Resource Consumption:** software firewalls can consume resources from the host such as processors and memory, possibly reducing device’s performance.

## Hardware Firewall

A hardware firewall is typically a standalone physical device. It operates independently with the devices it protects. Hardware firewalls are placed at the network perimeter, between internal and external network. They filter any incoming and outgoing traffic through the whole network system, providing security for all devices within the network.

Advantages

**Network-wide Defense:** A hardware firewall can actively protect every device on the network.

**Centralized Management:** Administrators can apply security policies throughout the network from a single access point thanks to their central management capability.

**Specialized Appliance:** Hardware firewalls are specifically designed for the intention of handling the most security-related tasks without sacrificing network performance.

Disadvantages

**Complex Configuration:** Maintaining or configuring a hardware firewall is difficult and requires special expertise.

**Costly:** Compared to software firewalls, they are usually more expensive to install and maintain.

# Task 6 Network Recommendation

The network design presented offers the following advantages:

**Enhanced Security:** By filtering incoming and outgoing traffic before it reaches the internal network, placing the firewall in front of the main router adds an additional level of protection. It defends against external threats like malware and cyberattacks as well as helps prevent unauthorized access.

**Efficient Routing:** If the Layer 3 switch is connected to the router directly, traffic within the network can be routed effectively. The general efficiency of the network is enhanced and the load on the primary router is reduced by handling inter-VLAN routing at the switch level.

**Simplified Network Management:** Layer 2 switches installed in every room facilitate a simpler network infrastructure. This makes maintenance and troubleshooting duties easier for every department.

**Scalability and Flexibility:** As the business expands, the modular design makes it simple to grow and scale. To support more users, more switches and access points can be added without affecting the current network infrastructure.

**Improved Communication:** Internal communication between devices in various departments becomes seamless when all rooms are linked to the Layer 3 switch. Without the main router, users in any room, including Management and HR & Finance, can communicate directly with the server housed in the IT department. By doing this, latency is decreased, and intercommunication effectiveness is improved.

**Enhanced Wireless Connectivity:** Consistent and dependable wireless connectivity across the office space is ensured by mounting the Wireless AP on the Layer 3 switch. Users can safely access the network from anywhere in the building, which encourages mobility and flexibility at work.

All things considered, this network architecture provides a strong and expandable framework that puts security, effectiveness, and smooth internal communication before anything else. It enhances network performance and promotes collaborative work environments by utilizing Layer 3 switching while carefully setting network devices.

## a) Scalability Recommendations

Implement Network Segmentation: Divide the network into smaller, manageable segments using VLANs (Virtual Local Area Networks) to accommodate future growth. This allows for better control over network traffic and facilitates easier expansion as the organization expands.

Invest in High-Performance Hardware: Install enterprise-grade networking equipment capable of handling increased bandwidth demands and supporting advanced features. This may include switches with higher port densities to meet the growing needs of the organization.

Accept Cloud Technologies: To improve scalability and flexibility, move some network services and resources to cloud-based platforms. Cloud solutions offer adaptable scalability, allowing the organization to dynamically adjust resources based on demand without the need for significant upfront investment in infrastructure.

## b) Security Aspects

**Implement Access Control Policies:** To prevent unwanted access to confidential network resources, implement access control policies. This includes Role-based Access Control (RBAC) mechanisms to ensure that users only have access to the resources necessary for their roles.

**Install Next-Generation Firewalls (NGFWs):** Upgrade to NGFWs with Deep Packet Inspection (DPI) and Intrusion Detection & Prevention Systems (IDPS), which can detect and prevent advanced threats. NGFWs provide enhanced protection from complex threats like malware and zero-day exploits.

**Enforce Strong Authentication Mechanisms:** To avoid unwanted access, use Multifactor Authentication (MFA) when gaining access to important network resources. This includes requiring users to authenticate using multiple factors such as passwords, biometrics, and one-time passcodes.

**Frequent updates and audits of security:** Perform routine security audits to find holes and weak points in the network architecture. Apply security patches and updates to network hardware and software frequently to fix known vulnerabilities and reduce the chance that attackers will take advantage of them.

**Employee Training and Awareness**: Inform staff members about cybersecurity practices as well as alert them to potential dangers like social engineering and phishing attacks. Topics like identifying doubtful emails, staying off suspicious hyperlinks, and quickly informing the IT department of security incidents should all be included in training programs. Having staff awareness is essential for stopping security breaches and safeguarding the network from insider threats.

**Total Words: 2973**

# References

* GeeksforGeeks (2021). *What is a Network Operating System?* [online]
  + Available at: <https://www.geeksforgeeks.org/what-is-a-network-operating-system>
* Java Point (n.d.). Open-Source Operating System - javatpoint. [online]
  + Available at: <https://www.javatpoint.com/open-source-operating-system>
* Vinogradov, A. (2020). 5 Risks of Using End-of-Life Operating System. [online]
  + Available at: <https://blog.cloudlinux.com/5-risks-of-using-end-of-life-operating-system>
* nordvpn.com. (2023). *Logical topology definition – Glossary | NordVPN*. [online]
  + Available at: <https://nordvpn.com/cybersecurity/glossary/logical-topology>
* Venngage. (n.d.). *Logical Topology Diagram*. [online]
  + Available at: <https://venngage.com/templates/diagrams/logical-topology-diagram-ff9fa292-5c57-499b-af41-4c48c3b758c3>
* Kaspersky (2020). *What is a VPN and how does it work?* [online] Kaspersky.
  + Available at: <https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn>
* Cisco (2023). *What Is a Firewall?* [online] Cisco.
  + Available at: <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>
* “Deep Packet Inspection.” Wikipedia, Wikimedia Foundation [online]
  + Available at: <https://en.wikipedia.org/wiki/Deep_packet_inspection>
* What Is a Next-Generation Firewall (NGFW)? | Cloudflare
  + Available at: [www.cloudflare.com/learning/security/what-is-next-generation-firewall-ngfw](http://www.cloudflare.com/learning/security/what-is-next-generation-firewall-ngfw)
* “Intrusion Detection System (IDS).” GeeksforGeeks [online]
  + Available at: [www.geeksforgeeks.org/intrusion-detection-system-ids](http://www.geeksforgeeks.org/intrusion-detection-system-ids)
* Yasar, Kinza, and Mary E. Shacklett. “What Is Multifactor Authentication? Definition from TechTarget.” Security, TechTarget, 2 Oct. 2023, [online]
  + Available at: [www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA](http://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA)