**INTERNATIONAL SCHOOL OF   
MANAGEMENT AND TECHNOLOGY**



**FACULTY OF COMPUTING**

**ASSIGNMENT COVER SHEET**

*This form is to be completed by students submitting assignments of level 4 and level 5. Students are required to complete all sections and attach to your assignment.*

|  |  |
| --- | --- |
| STUDENT DETAILS | |
| STUDENT NAME | Sparsh Shrestha |
| STUDENT ID | PG77125 |

|  |  |  |  |
| --- | --- | --- | --- |
| UNIT AND ASSIGNMENT DETAILS | | | |
| UNIT TITLE | Unit 17: Network Security | | |
| UNIT NUMBER | L/615/1646 | | |
| ASSIGNMENT TITLE | London College Security | | |
| ISSUE DATE | 28th June, 2023 | DUE DATE | 27th June, 2023 |
| ASSESSOR NAME | Siddhant Bhattrai | | |
| ESTIMATED WORD LENGTH |  | | |

|  |  |
| --- | --- |
| SUBMISSION | |
| HAND IN DATE | 21th June, 2023 |

**DECLERATION AND ACKNOWLEDGEMENT**

***When submitting assignments, each student must sign a declaration confirming that the work is their own.***

Plagiarism and Collusion

**Plagiarism:** to use or pass off as one’s own, the writings or ideas of another without acknowledging or crediting the source from which the ideas are taken.

**Collusion:** submitting an assignment, project or report completed by another person and passing it off as one’s.

In accordance with the*Academic Integrity and Plagiarism Policy*:

1. **I declare that:**
2. this assignment is entirely my own work, except where I have included fully-documented references to the work of others,
3. the material contained in this assignment has not previously been submitted for any other subject at the University or any other educational institution, except as otherwise permitted,
4. no part of this assignment or product has been submitted by me in another (previous or current) assessment, except where appropriately referenced, and with prior permission from the Lecturer / Tutor / Unit Coordinator for this unit.
5. **I acknowledge that:**
6. if required to do so, I will provide an electronic copy of this assignment to the assessor;
7. the assessor of this assignment may, for the purpose of assessing this assignment:
8. reproduce this assignment and provide a copy to another member of academic staff;
9. communicate a copy of this assignment to a plagiarism checking service such as Plagiarism Check (which may then retain a copy of this assignment on its database for the purpose of future plagiarism checking).

|  |  |  |  |
| --- | --- | --- | --- |
| I am aware of and understand that any breaches to the Academic Code of Conduct will be investigated and sanctioned in accordance with the College Policy. | | | |
| SIGNATURE |  | DATE |  |

Table of Contents

[1.1. Introduction 1](#_Toc138256187)

[1.2. Network Security Device 1](#_Toc138256188)

[1.2.1. Types of Network Security Devices 1](#_Toc138256189)

[1.2.1.1. Firewall 2](#_Toc138256190)

[1.2.1.2. Intrusion Detection System (IDS) 2](#_Toc138256191)

[1.2.1.3. Intrusion Prevention System (IPS) 2](#_Toc138256192)

[1.2.1.4. Unified Treat Management (UTM) 3](#_Toc138256193)

[1.2.1.5. Network Access Control 3](#_Toc138256194)

[2.1. Network Security Protocol 4](#_Toc138256195)

[2.1.1. Types of Network Security Protocol 4](#_Toc138256196)

[2.1.1.1. Internet Protocol Security (IPsec) Protocol 4](#_Toc138256197)

[2.1.1.2. SSL and TLS 5](#_Toc138256198)

[2.1.1.3. Datagram Transport Layer Security (DTLS) 5](#_Toc138256199)

[2.1.1.4. Simple Network Management Protocol (SNMP) 6](#_Toc138256200)

[2.1.1.5. HTTP and HTTPS 6](#_Toc138256201)

[3.1. Purpose and Requirement for a Secured Network 7](#_Toc138256202)

[3.2. Purpose of Secured Network 7](#_Toc138256203)

[3.2.1. Protecting Sensitive Data 7](#_Toc138256204)

[3.2.2. Maintaining Data Integrity 7](#_Toc138256205)

[3.2.3. Preventing Unauthorized Access 7](#_Toc138256206)

[3.2.4. Mitigating Cyber Treats 7](#_Toc138256207)

[3.3. Requirement of Secured Network 7](#_Toc138256208)

[3.3.1. Network Segmentation 7](#_Toc138256209)

[3.3.2. Secure Network Architecture 8](#_Toc138256210)

[3.3.3. Access Control 8](#_Toc138256211)

[3.3.4. Encryption 8](#_Toc138256212)

[4.1. Network Hardware and Software 8](#_Toc138256213)

[4.1.1. Network Hardware 8](#_Toc138256214)

[4.1.2. Network Software 10](#_Toc138256215)

[5.1. Design of a Secured Network System for London College 11](#_Toc138256216)

[6.1. Importance of Network Security 12](#_Toc138256217)

[6.1.1. Protection of Confidential Information 12](#_Toc138256218)

[6.1.2. Prevention of Data Breaches and Losses 12](#_Toc138256219)

[6.1.3. Mitigation of Cyber Attacks and Malware Infections 12](#_Toc138256220)

[6.1.4. Maintenance of Business Continuity 13](#_Toc138256221)

[6.1.5. Compliance with Regulatory Requirement 13](#_Toc138256222)

[Conclusion 13](#_Toc138256223)

[7.1. Introduction 14](#_Toc138256224)

[7.1. Cryptography 14](#_Toc138256225)

[7.1.1. Cryptographic Types of Network Security 14](#_Toc138256226)

[7.1.1.1. Symmetric Cryptographic 14](#_Toc138256227)

[7.1.1.2. Asymmetric Cryptographic 15](#_Toc138256228)

[7.1.1.3. Hashing 15](#_Toc138256229)

[8.1. Network Security Configuration 16](#_Toc138256230)

[8.2. ACL 16](#_Toc138256231)

[8.2.1. Benefits of using ACL 16](#_Toc138256232)

[8.3. ACL Configuration 17](#_Toc138256233)

[8.4. VLANs 18](#_Toc138256234)

[8.4.1. VLANs Configuration 18](#_Toc138256235)

[8.5. Syslog 21](#_Toc138256236)

[8.6. Firewall 23](#_Toc138256237)

[8.6.1. Firewall Configuration 24](#_Toc138256238)

[9.1. Quality of Services (QoS) 26](#_Toc138256239)

[9.1.1. Importance of Prioritizing Security-Related Traffic 27](#_Toc138256240)

[9.1.2. Ensuring Reliable and Predictable Service 28](#_Toc138256241)

[Conclusion 30](#_Toc138256242)

[10.1. Introduction 31](#_Toc138256243)

[10.1.1. Sample Test table for the network of London College 31](#_Toc138256244)

[10.1.2. Testing firewall 32](#_Toc138256245)

[Conclusion 40](#_Toc138256246)

[References 41](#_Toc138256247)

# Introduction

My objective is to submit a thorough project report on network security as an aspiring professional trying to enroll in London College. Network security has grown to be a top issue for all enterprises in the linked world of today, including academic institutions like London College.

My project report will demonstrate my comfort speaking about various network security protocols, configuration settings, and security procedures. I'll list the drawbacks, advantages, and most frequent uses of security while also forecasting its future.

As the ISMT College's system and network security officer, my instructor will expect me to plan, develop, construct, and test a fully functional and secure network that satisfies his standards. My project will culminate in a thorough report on the network topologies, security-enhancement tools, and particular tools for maintaining contact with all partner universities and London Colleges branches in Nepal. I will also offer suggestions for strengthening and enhancing network security even more.

This task offers me a special chance to show off my network security expertise and experience while assisting in the safety and security of a learning environment.

# Network Security Device

Network security encompasses all the steps taken to protect the integrity of a computer network and the data within it. Network security is important because it keeps sensitive data safe from cyber-attacks and ensures the network is usable and trustworthy. Successful network security strategies employ multiple security solutions to protect users and organizations from malware and cyber-attacks, like distributed denial of service (Barney, 2022). Computer networks can be secured with the help of hardware or software tools that block unauthorised access, malicious assaults, and other security risks. These gadgets are made to keep an eye on and regulate network activity, spot and stop cyberattacks, and safeguard private data and information kept on the network.

## Types of Network Security Devices

There are several types of networks security devices some of them are discussed below:

### Firewall

A firewall is a piece of network security equipment that keeps an eye on and manages incoming and outgoing network traffic in accordance with pre-established security rules. A firewall's primary function is to block unauthorised access to or from a private network, such as the internal network of a business or a person's home. A firewall can be installed at multiple points in a network, such as the boundary between a private network and the Internet or between distinct sections of an organization's internal network. Firewalls can be hardware- or software-based.

Typically, firewalls filter network traffic using a set of rules that include source and destination IP addresses, port numbers, and protocols to decide whether to allow or restrict particular types of data. For instance, a firewall may be set up to let incoming communication only on particular ports used by authorised applications and to restrict traffic from IP addresses known to be malicious.

Network security is not complete without firewalls, which provide defence against a variety of online dangers like malware, phishing, and hacking.

### Intrusion Detection System (IDS)

Network security is not complete without firewalls, which provide defense against a variety of online dangers like malware, phishing, and hacking (pp\_pankaj, 2020). A network security tool known as an intrusion detection system (IDS) watches network traffic for indications of malicious activity and issues alarms when it does. An IDS's main objective is to immediately identify and respond to security occurrences like unauthorised access attempts and other security breaches.

IDS can be set up as hardware or software devices and installed at different points in a network, such as the boundary between a private network and the Internet, inside a local network, or at crucial locations inside a company's internal network.

An IDS often employs a set of established rules and signatures to spot unexpected traffic patterns or attempts to exploit known vulnerabilities among other suspicious patterns of network activity. Some IDS can also utilise machine learning techniques to find network traffic irregularities that might point to a security risk.

### Intrusion Prevention System (IPS)

An intrusion prevention system (IPS) is a cybersecurity tool that examines [network traffic](https://www.techtarget.com/searchnetworking/definition/network-traffic) to identify potential threats and automatically take action against them. An IPS might, for example, recognize and block [malicious software](https://www.techtarget.com/searchsecurity/definition/malware) or vulnerability [exploits](https://www.techtarget.com/searchsecurity/definition/exploit) before they can move further into the network and cause damage. IPS tools continually monitor and log network activity in real time (Gillis, 2023). A network security tool known as an intrusion prevention system (IPS) not only recognises malicious activity but also actively works to stop it by blocking traffic from known malicious sources or by dropping packets that go against established security regulations.

A hardware or software IPS device is often installed at a network's edge or within a local network. It functions through real-time monitoring of network traffic and comparison with a database of known risks and predefined security policies. The IPS acts to stop the attack by blocking or dropping the offending traffic when a threat or policy violation is discovered.

### Unified Treat Management (UTM)

Several security elements are combined into a single platform as part of the network security strategy known as "Unified Threat Management" (UTM), which offers a complete and integrated method to safeguarding computer networks from online attacks.

A firewall, intrusion detection and prevention system (IDS/IPS), antivirus and anti-malware software, support for virtual private networks (VPNs), web content filtering, and other security technologies are frequently found in UTM appliances. UTM offers a more effective and efficient method of network protection by combining these functionalities into a single device, making it easier to manage and administer security rules and lowering the cost of ownership.

Small and medium-sized enterprises frequently utilise UTM since they do not have the capacity to administer complex security rules or deploy numerous security devices. UTM offers a practical means of defending against a variety of cyberthreats and aids in maintaining the privacy, accuracy, and accessibility of network resources and data.

### Network Access Control

Network access control, also called network admission control, is a method to bolster the security, [visibility](https://www.techtarget.com/searchnetworking/definition/network-visibility) and [access management](https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system)  of a proprietary [network](https://www.techtarget.com/searchnetworking/definition/network). It restricts the availability of network resources to endpoint devices and users that comply with a defined [security policy](https://www.techtarget.com/searchsecurity/definition/security-policy) (Awati, 2021). Network access control (NAC) is a network security technique that restricts who may access a network, what resources they can access, and how they can access those resources by enforcing policies that specify these criteria.

A software or hardware system called NAC is often used to authenticate and authorise devices before allowing them access to the network. The first thing that happens when a device tries to join to the network is that it is assessed to see if it complies with the organization's security standards and rules, such as having the most recent antivirus software installed or adhering to particular network security protocols. The device is given access to the network if it complies with the requirements; otherwise, it may be quarantined or denied access.

In order to provide a complete network security solution, NAC can be combined with other security technologies like firewalls, intrusion detection and prevention systems, and virtual private networks. NAC can be installed in a range of network contexts, including wired and wireless networks.

# Network Security Protocol

The integrity and security of data exchanged through network connections are guaranteed by network security protocols. The type of protected data and network connection determine the precise network security protocol that is employed. Each protocol outlines the methods and steps necessary to safeguard network data from nefarious or unauthorised efforts to read or exfiltrate information.

There are different kinds of network security protocols that are available, and each one performs a certain task, such as access control, authentication, or encryption. These protocols are used to protect against various network security threats, secure network traffic and communications, stop unauthorised access to network resources, and more.

For a network and its resources to be secure, network security protocols must be implemented. Businesses must carefully assess their needs for network security and choose the right protocols to satisfy those needs. In order for network security procedures to be successful against new and developing security threats, they must also be kept current.

## Types of Network Security Protocol

Following are the some of the most common network security protocol:

### Internet Protocol Security (IPsec) Protocol

IPsec is a set of protocols and algorithms designed to ensure data transmission across public networks, such as the Internet. In the 1990s, IPsec protocols were made available by a task force on Internet Engineering called IETF. They provide a layer of protection for IP packets by encrypting and authenticating them.

ESP and AH protocols have been included in IPsec from the beginning. Encapsulating Security Payload (ESP) encrypts data and provides authentication, while Authentication Header (AH) offers anti-replay capabilities and protects data integrity. The suite has since expanded to include the Internet Key Exchange (IKE) protocol, which provides shared keys establishing security associations (SAs). They'll allow the use of a firewall or router for encryption and decryption.

### SSL and TLS

The encrypted protocols that make the Internet secure are HTTP Secure Transport Layer and HTTPS Secure Transport Layer. In order to provide a secure connection for web browsers and Internet servers, SSL has been an initial protocol that was followed by TLS.

In order to secure data transactions between a client and server from eavesdropping, tampering, and other types of cyber-attacks, SSL and TLS both employ encryption. To establish a secure connection and verify the server's identity, they also utilise digital certificates.

The more used protocol right now is TLS, which has a number of versions available with progressively greater performance and security features. SSL is no longer advised because it is regarded as insecure.

TLS is frequently used to offer secure communication over the Internet, including for online transactions like e-commerce, online banking, and other secure web-based applications. Additionally, it is utilised for virtual private networks (VPNs), secure email, and other network applications.

### Datagram Transport Layer Security (DTLS)

The UDPD protocol provides secure communications over unreliable datagram TLS based networks such as User Datagram Protocols. It is a variant of the Transport Layer Security Protocol, designed to work in conjunction with Datagram protocols that do not have an established data delivery service.

DTLS is used in applications where real-time communication and low latency are critical, such as voice and video conferencing, online gaming, and IoT (Internet of Things) devices. It provides encryption, message integrity, and authentication to ensure that data is protected during transmission.

In order to verify a server's identity and create secure connections, DTLS shall use the Digital Certificate as an alternative to TLS. In order to ensure the protection of data transmission, it also uses a combination of two types of encryption: Simplification and Unsymmetrical Encryption.

### Simple Network Management Protocol (SNMP)

SNMP is an application-layer protocol for managing and monitoring network devices. It may protect LAN or WAN-connected devices. Through the use of a network management system, SNMP offers a common language for servers and routers. SNMP is a founding member of the family of Internet protocols outlined by the IETF.

SNMP architecture is composed of the Manager, Agent and Management Information Base. The manager is the client, the agent is the server, and the MIB is the database. SNMP agent can use the MIB protocol to reply to manager's requests. As SNMP is available at a large extent, administrators need to change their default configuration in order to allow communication between agents and the network management system so that they can implement this protocol.

The SNMP protocol gained three crucial security features with the introduction of SNMPv3 in 2004: packet encryption to prevent eavesdropping, integrity checks to guarantee packets were not altered with in transit, and authentication to confirm that communications come from a known source.

### HTTP and HTTPS

Full form of HTTP is Hypertext Transfer Protocol. HTTP offers set of rules and standards which govern how any information can be transmitted on the World Wide Web. HTTP provides standard rules for web browsers & servers to communicate (Williams, 2023).

HTTPS stands for Hyper Text Transfer Protocol Secure. It is highly advanced and secure version of HTTP. It uses the port no. 443 for Data Communication. It allows the secure transactions by encrypting the entire communication with SSL. It is a combination of SSL/TLS protocol and HTTP. It provides encrypted and secure identification of a network server (Williams, 2023).

# Purpose and Requirement for a Secured Network

The purpose and requirement for a Secured Network is given below:

## Purpose of Secured Network

The purpose is given below:

### Protecting Sensitive Data

A secure network is designed to ensure the confidentiality of sensitive information, preventing unauthorised access, interception or eavesdropping. It is aimed at ensuring that sensitive information, such as customer data, financial records, IPR and commercial secrets are protected from damage or theft.

### Maintaining Data Integrity

In transmitting and storing data, a secure network shall ensure that the data are not distorted, incomplete or unremarkable. This ensures that data are not modified, deleted or corrupted without authorisation and thus maintains their integrity and reliability.

### Preventing Unauthorized Access

In order to ensure that users and devices are identified when accessing network resources, a secure network is equipped with access controls and authentication mechanisms. It is designed to prevent unauthorised persons or bad actors from accessing sensitive data and system resources through the enforcement of robust user authentication and authorization policies.

### Mitigating Cyber Treats

For the purpose of defending against cyber threats, a secured network consists of various security measures including firewalls, intrusion detection systems and encryption. It reduces the risks for financial losses, reputation damage or legal consequences by detecting and preventing infection of malicious software, attempts to hack into sensitive data as well as another type of cyber-crime.

## Requirement of Secured Network

### Network Segmentation

In London College network segmentation is necessary because, A separation of the network into groups or areas according to security requirements and separate critical assets from a lower risk area. This will help to minimise the risk of security breach and limit access by unauthorised persons.

### Secure Network Architecture

Implementing a well-designed network architecture integrating security controls at multiple levels, e.g. firewalls, intrusion prevention systems, virtual private networks and secure remote access mechanisms.

### Access Control

To provide authentication and authorization of network users, devices and systems by means of robust access control mechanisms. To limit access rights based on job role and responsibilities, this applies to the use of user specific authentication credentials, Multifactor Authentication via a combination of Multiple Factors WFA; Roles Based Access Control RBAC.

### Encryption

To protect the data in transit and at rest using encryption protocols. The use of strong encryption algorithms and a secure key management method are also used to encrypt sensitive data, e.g. passwords, credit card numbers or customer information.

# Network Hardware and Software

In computer network infrastructure network Hardware and Software are essential components. Together, they support data transfer, resource sharing, and network communication. An overview of network gear and software is provided below:

## Network Hardware

In a computer network, the physical hardware that is used to set up, run, and connect devices is referred to as network hardware. These physical elements allow for the management, routing, and transmission of data through a network. Here are a few typical illustrations of network hardware:

* **Network Interface Cards (NICs):** A network interface card (NIC) is a hardware component, typically a circuit board or chip, which is installed on a computer so it can connect to a network. Modern NICs provide functionality to computers, such as support for [I/O](https://www.techtarget.com/whatis/definition/input-output-I-O) interrupt, direct memory access ([DMA](https://www.techtarget.com/whatis/definition/Direct-Memory-Access-DMA)) interfaces, data transmission, network traffic engineering and partitioning (Contributor, 2021).
* **Switches:** A switch, in the context of networking, is a high-speed device that receives incoming data packets and redirects them to their destination on a local area network (LAN) (Rouse, 2020).

A switch is a network device that connects various devices on a local area network (LAN) in the context of computer networking. It is in charge of forwarding data packets between connected devices based on their distinct Media Access Control (MAC) addresses and operates at the data connection layer (Layer 2) of the OSI model.

* **Routers:** A router is a physical or [virtual appliance](https://searchservervirtualization.techtarget.com/definition/virtual-appliance) that passes information between two or more packet-switched computer networks. A router inspects a given data [packet](https://www.techtarget.com/searchnetworking/definition/packet-loss)'s destination Internet Protocol address (IP address), calculates the best way for it to reach its destination and then forwards it accordingly (Irei, 2021).

A router is a network device that joins different computer networks and makes it easier for data packets to move back and forth. It operates at Layer 3 of the OSI model's network layer, where routing tables and protocols are used to find the best path for data transfer.

* **Firewalls:** A firewall is a piece of hardware or software for network security that serves as a wall between a computer network and other networks, like the internet. On the basis of preset security rules and policies, it is intended to monitor and regulate both incoming and outgoing network traffic. A firewall's main function is to safeguard the network and the devices connected to it from unauthorised access, malicious activity, and other security risks.
* **Wireless Access Point (WAPs):** A wireless access point (WAP) is a hardware device or configured node on a local area network (LAN) that allows wireless capable devices and wired networks to connect through a wireless standard, including Wi-Fi or Bluetooth. WAPs feature radio transmitters and antennae, which facilitate connectivity between devices and the Internet or a network (Rouse, 2013).
* **Network Cables and Connectors:** In order to make physical connections between network devices and enable the transfer of data signals within a computer network, network cables and connectors are crucial components. They give devices the tools they need to speak with one another and share data via the network infrastructure.
* Network Server: A network server is a computer designed to act as central repository and help in providing various resources like hardware access, disk space, printer access, etc,. to other computers in the network (Rouse, 2014).

A computer or other device that serves as a network server is one that offers resources and services to other clients—or devices—in the network. In order to facilitate effective communication and collaboration among network users, it is in charge of managing and allocating network resources, including files, programmes, databases, and network connections.

## Network Software

Network software is a collective term for the set of applications, protocols, and programmes that make it easier for computers to operate, administer, and communicate with one another. It includes a broad range of software parts that make it possible for networks to function, move data, be secure, and be administered. Here are a few typical illustrations of network software:

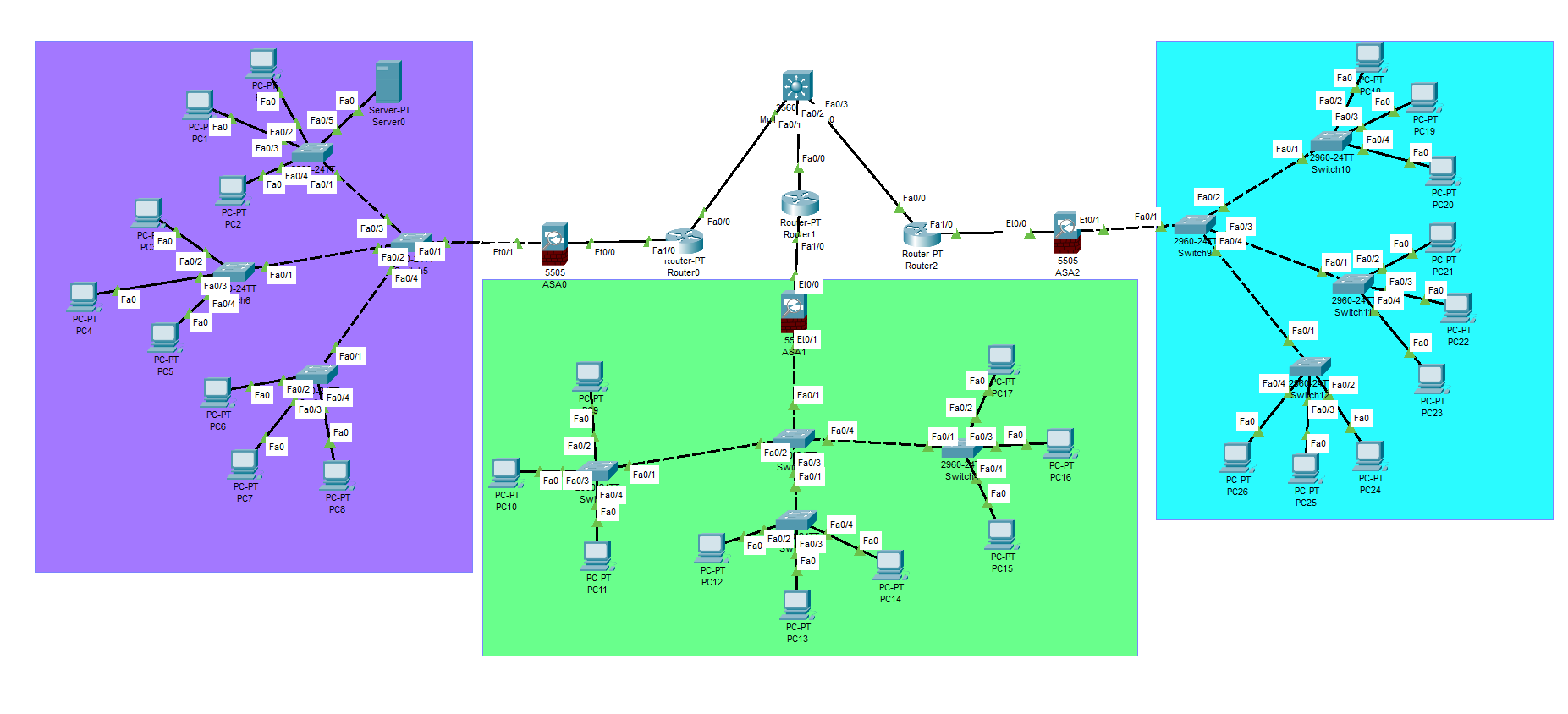
* **Network Operating Systems (NOS):** An operating system specifically created to manage and coordinate network resources and services within a computer network is known as a network operating system, or NOS. It offers the features and services required for several computers or devices to interact, share information, and use network resources.

A network operating system's main objective is to make resource sharing and communication between computers and other connected devices easier. It oversees security, user authentication, and network management duties while enabling users to access files, printers, databases, and other shared resources.

* **Network Protocols:** Network protocols are a set of guidelines and standards that control how devices in a computer network communicate with one another. Devices can share information effectively and dependably because to their definition of the format, timing, sequencing, and error management of data transmission. Data is properly packaged, addressed, transferred, received, and understood over the network thanks to network protocols.
* **Network Management Software:** A class of tools and programmes known as network management software is used to monitor, manage, configure, and operate computer networks. It gives network managers a centralised platform to manage and troubleshoot network resources, services, and equipment efficiently. A variety of features and functionalities are normally available in network management software to optimise network performance and streamline network operations.
* **Network Security Software:** Software particularly created to safeguard computer networks from unauthorised access, data breaches, and other security risks is referred to as network security software. It focuses on protecting the network's hardware, connected devices, and sent data. Network security software aids businesses in protecting the privacy, availability, and integrity of their network resources.
* **Network Applications:** Software that is intended to run across a number of devices or computers connected via a network is referred to as a network application, also known as a networked application or distributed application. In order to exchange information, carry out activities, and communicate with other systems or devices, network applications make use of the network infrastructure.
* **Network Configuration Tools:** Network administrators can manage and configure network devices and settings with the use of software programmes known as network configuration tools. By automating and streamlining the configuration of network equipment, these technologies save time and lower the possibility of mistakes. They give administrators centralised control and insight over network configurations, enabling effective management of network resources.

# Design of a Secured Network System for London College

1. To ensure network security, the installation of firewalls, intrusion detection and avoidance systems, Virtual Private Networks, access control lists, Syslog, VLANs and DMZ are included in the development of a secure network system for London College. In addition, in order to assure that networks remain available at all times, the network needs to be configured for efficient traffic management and should have redundant components.
2. Example:



# Importance of Network Security

In today's linked world, network security is of the utmost significance. The following are some major arguments in favour of network security:

## Protection of Confidential Information

Sensitive and confidential data is protected from unauthorised access, interception, and theft through network security protocols, access controls, and encryption. This covers safeguarding client information, financial data, intellectual property, and trade secrets.

## Prevention of Data Breaches and Losses

Network security aids in preventing data breaches, which can result in large financial losses, damage to one's reputation, and legal repercussions. Organisations can lower their risk of data breaches brought on by hackers, malware, insider threats, or other cyberattacks by putting strong security measures in place.

## Mitigation of Cyber Attacks and Malware Infections

Firewalls, intrusion detection systems (IDS), and antivirus software are examples of network security technologies that can identify and counteract cyberattacks, malware infections, and other nefarious actions. These precautions assist in spotting risks and counteracting them, guarding against unauthorised access, data loss, and interruption of network services.

## Maintenance of Business Continuity

Network security is essential for ensuring business continuity because it safeguards crucial network resources and infrastructure from disruptions. Organisations may promptly identify and manage security problems, minimising the impact on operations and maintaining continuous service availability, by deploying security controls and incident response plans.

## Compliance with Regulatory Requirement

Network security and data protection are subject to a wide range of legislation and compliance standards in many different sectors and jurisdictions. Maintaining confidence and credibility with clients and business partners, as well as avoiding negative legal and financial repercussions, depends on adhering to these rules.

# Conclusion

Over all in this session, I write so many things like what are the types of network security devices and also, I explained about it also. After finishing the explanation of network security devices, I jumped in the network security protocol.

In purpose and requirements for secured network there are various thing like preventing unauthorized access, maintaining data integrity, protecting sensitive data and many more. And there is short explanation of this things.

In network hardware and software there are many things like firewall, router, switch, and many more and also there is network protocol network, configuration tools, network application, network management application, this are the software that I had explained on this part.

This is the last part, in here I had created the design of the secured network which is based on scenario, they include many more devices. It is the designed for London college which should include Syslog, VLAN, ACL. To handle network traffic efficiently and should have redundancy built-on to ensures the network.

7.1. Introduction

As I had already finish previous session. In this part I am going to explain about the cryptographic and it’s type of network security. I also explain in its types in briefly. After explaining cryptographic I will write about network security for network which is given in scenario. And also, I will write about ACL, VLAN, Syslog, and Firewall. After describing them I had paste their configuration screenshot of ACL, VLAN, Syslog and firewall.

After finishing this part there is short explanation of Quality of services relation to network security in configuration.

# Cryptography

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it (Richards, 2021).

In computer science, the term "cryptography" refers to safe information and communication methods that use mathematical principles and a system of calculations based on rules, or "algorithms," to change messages in ways that are challenging to read. These deterministic algorithms are employed in the creation of cryptographic keys, digital signature, online browsing on the internet, and private communications like email and credit card transactions.

## Cryptographic Types of Network Security

The types of cryptographic are given below:

### Symmetric Cryptographic

A cryptographic method known as symmetric cryptography, also referred to as secret-key cryptography or conventional cryptography, encrypts and decrypts data using the same key. In other words, the original information is converted into ciphertext and then back into its original form using a secret key that is shared by the sender and the recipient.

With symmetric cryptography, the plaintext (original message) is encrypted by using a particular technique, called a symmetric encryption algorithm, and a shared secret key. This results in the ciphertext, which to someone without the key seems as random and incomprehensible data.

### Asymmetric Cryptographic

Asymmetric cryptography, commonly referred to as public-key cryptography, is a cryptographic method that employs a set of two keys—a public key and a private key—that are mathematically related for encryption and decryption. Asymmetric cryptography uses distinct keys for encryption and decryption as opposed to symmetric cryptography, which uses the same key for both operations.

While the private key is kept private and only known to the owner, the public key is widely dispersed and available to everyone. Data is encrypted using the public key, and it is decrypted using the corresponding private key.

The recipient's public key is obtained and used to encrypt the message when someone wishes to send them a private message. The recipient's private key is required to decrypt a communication once it has been encrypted. With the private key in their possession, this makes sure that only the intended receiver can access and read the message.

Asymmetric cryptography has features beyond confidentiality as well. For example, it makes key exchange and digital signatures possible.

### Hashing

In computer science and information security, the method of hashing is used to convert data into a fixed-size representation known as a hash value or hash code. It entails applying a mathematical procedure known as a hash function to the input data in order to produce an original output that is distinct from all other outputs. Using the input, the hash function executes calculations to produce a hash value, which is often a string of alphanumeric characters.

Hashing is useful for many uses. Verifying data integrity is a crucial application. One can determine if data has been changed or corrupted by computing the hash value of a file, message, or other piece of data and comparing it to a hash value that was previously computed. It is helpful for spotting tampering or inadvertent modifications because even a slight change in the input data may cause a completely different hash value.

Hashing is frequently used to store passwords. The hash value of the password is kept instead of the actual password itself. For authentication purposes, a user's password is hashed and compared to a value that has been previously stored. This method improves security since even if the password database is hacked, the actual passwords are hidden and would require a lot of work to deduce from the hash values the original passwords.

Data retrieval structures like hash tables and hash maps also depend on hashing. Hash values are used as keys in these structures to identify and retrieve data fast. Information may be accessed and retrieved quickly thanks to the hash value's function as an index to locate the storage place.

# Network Security Configuration

The process of setting up and configuring different security controls and safeguards to safeguard a computer network from unauthorised access, data breaches, and other security risks is known as network security configuration. To create a strong security posture, a mix of hardware, software, and network settings must be implemented.

Here are the some configuration of the network:

## ACL

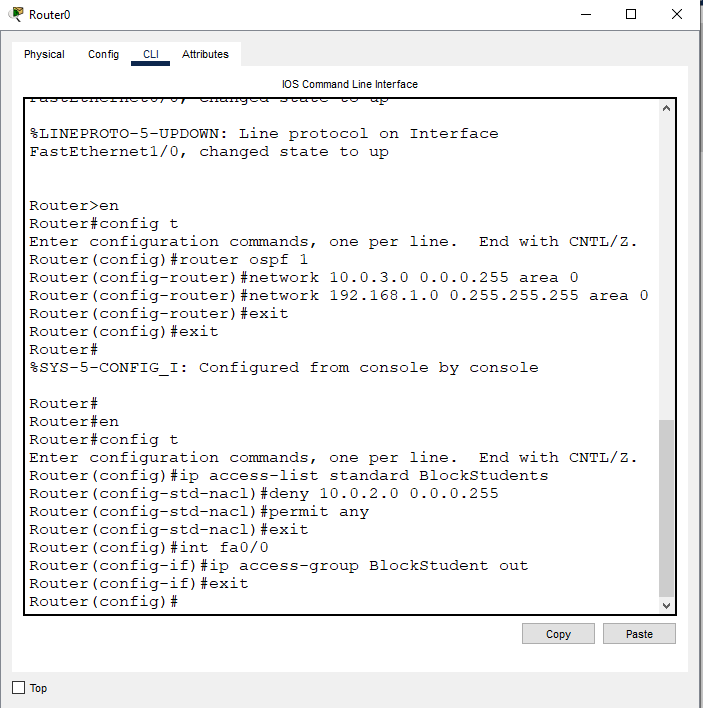
An access control list (ACL) is a list of rules that specifies which users or systems are granted or denied access to a particular object or system resource. Access control lists are also installed in routers or switches, where they act as filters, managing which traffic can access the network (Lutkevich, 2022).

### Benefits of using ACL

There are several benefits of using ACL which includes the following:

* **Simplified User Identification:** User identification is made easier with the aid of an access control list. ACLs guarantee that a system can only be accessed by authorised users and traffic.
* **Performance:** Compared to alternative technologies that provide the same purpose, ACLs offer performance advantages. Access control lists don't affect routing device performance because they are configured directly on the forwarding hardware of the device. In contrast, a stateful inspection firewall is a different piece of software that might result in performance reduction. Additionally, managing network traffic makes networks more effective.
* **Control:** Administrators can have more precise control over user and traffic permissions on a network at numerous points along the network by using ACLs. They assist in regulating traffic moving between internal networks and access to network endpoints.

# ACL Configuration

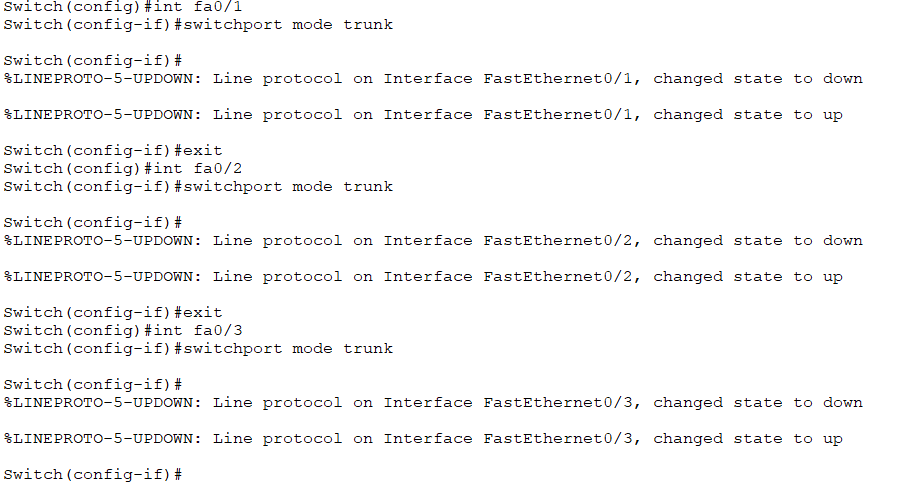


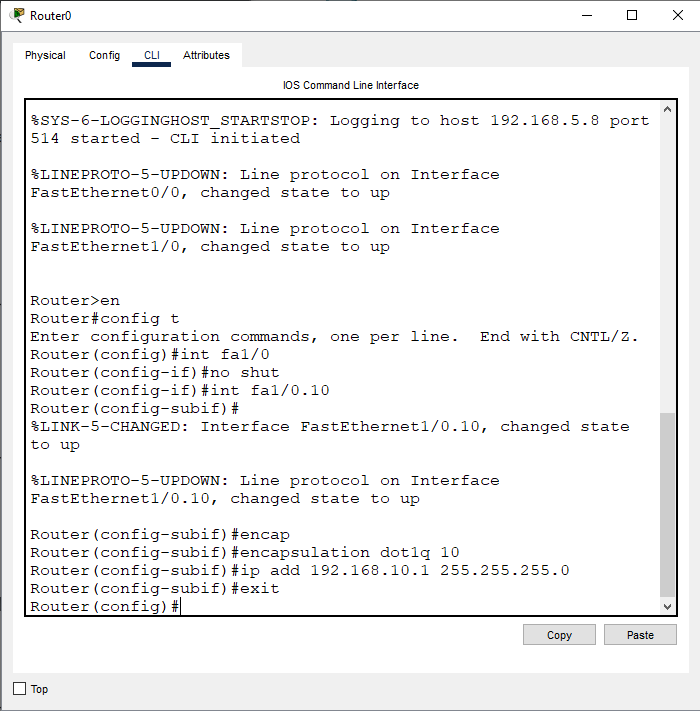
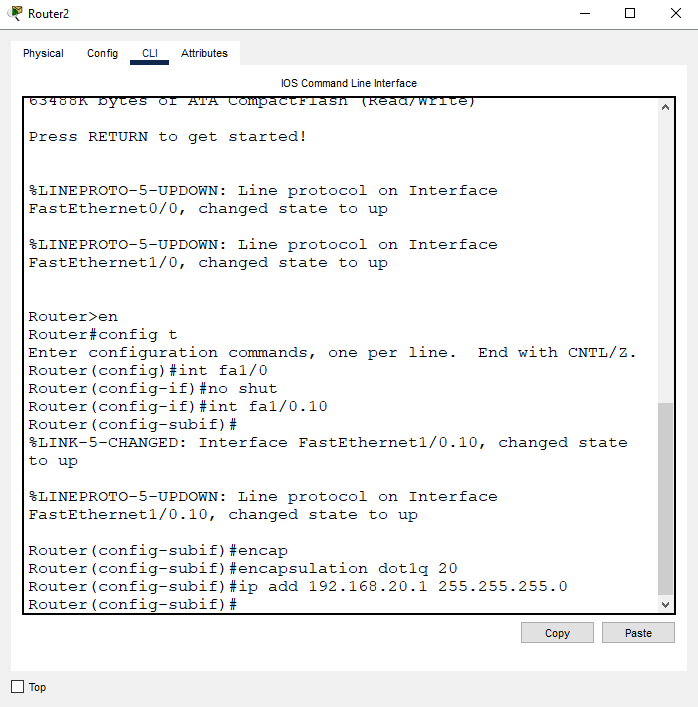
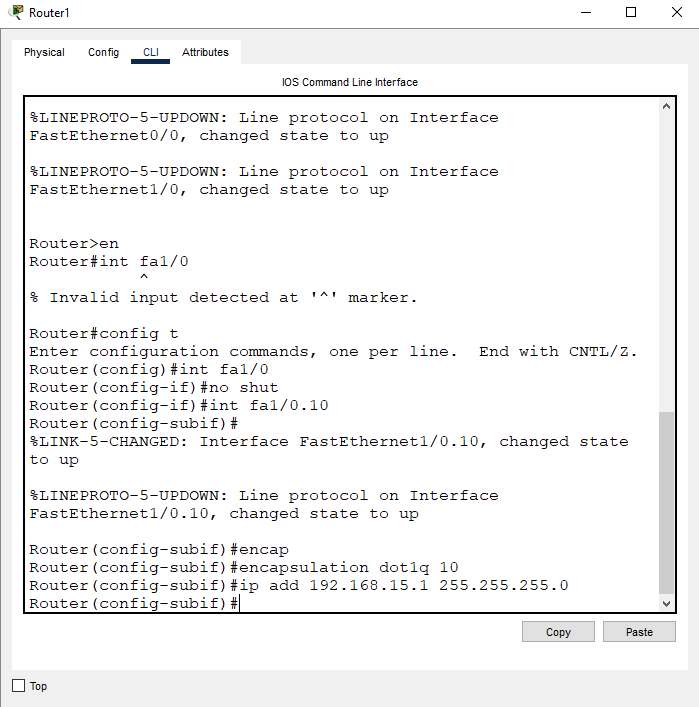
# VLANs

VLAN is a custom network which is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN. The full form of VLAN is defined as Virtual Local Area Network (Williams, 2023).

A logical collection of devices within a physical network infrastructure is called a VLAN (Virtual Local Area Network). Network administrators can divide a network into various virtual networks, regardless of where they are physically located or connected. By dividing network traffic based on logical criteria rather than physical topology, VLANs offer flexibility, security, and better network administration.

## VLANs Configuration



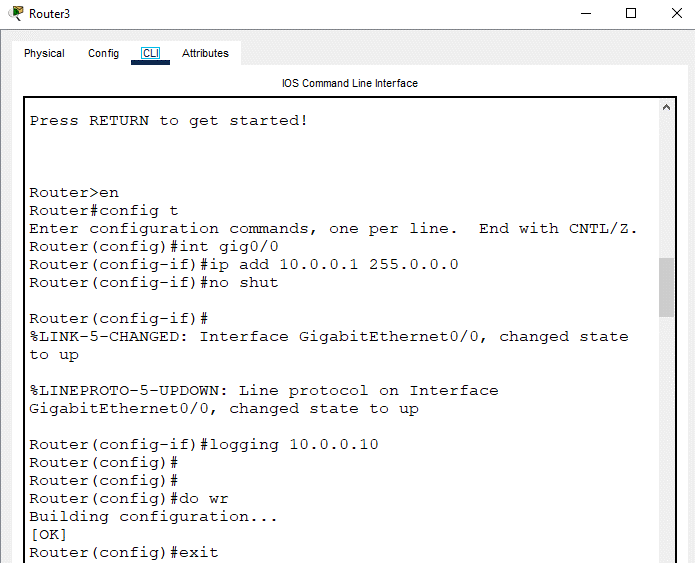


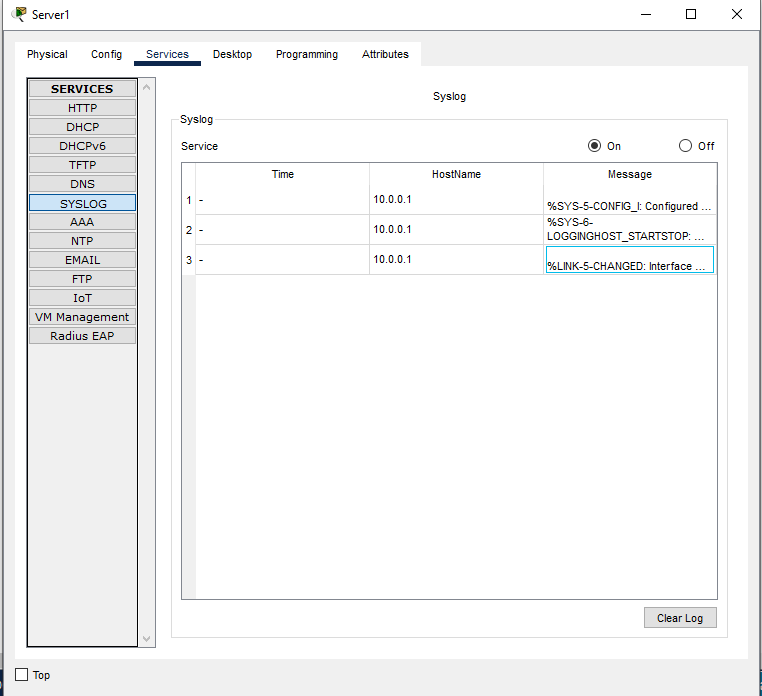
# Syslog

To gather, transmit, and store log messages from diverse hardware and software applications, computer networks employ the standard protocol and message logging system known as Syslog. System administrators and security staff can monitor and analyse system behaviour, troubleshoot problems, and carry out auditing thanks to the standardised format it provides for logging events and actions.

The syslog protocol has a client-server architecture, in which syslog client’s devices or programs send log messages to a central server called the syslog server or syslog daemon. The actual log content which may include information about system events, faults, warnings, or informational messages as well as timestamp and the source of the log message (such as the device or application that generated it) are all included in the syslog message.

Configuration





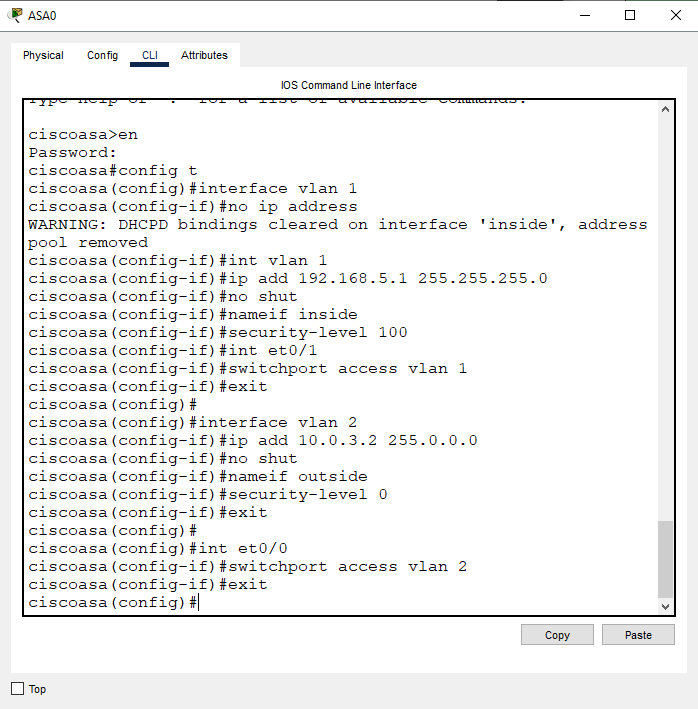
# Firewall

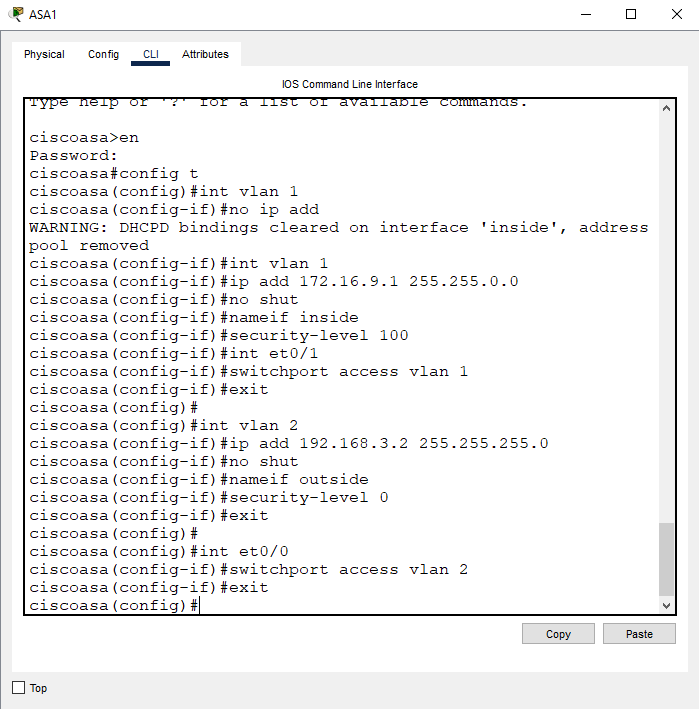
A firewall is a network security device that prevents unauthorized access to a network. It inspects incoming and outgoing traffic using a set of security rules to identify and block threats (Yasar, 2023).

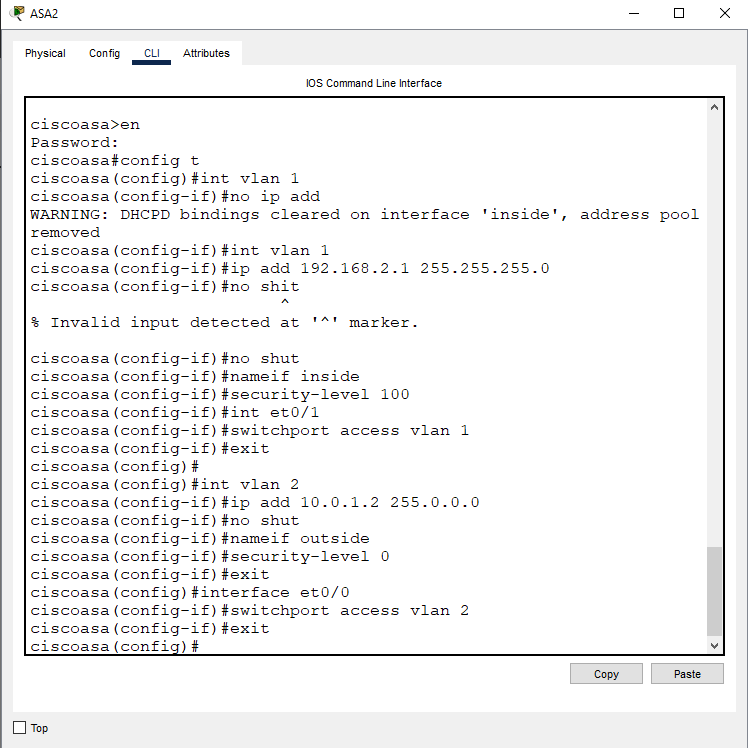
An internal network, like a company's private network, and an external network, like the Internet, are separated by a firewall, a network security device or piece of software. Its main objective is to watch over and manage incoming and outgoing network traffic in accordance with predefined security policies.

Based on the configured rules, firewalls examine network packets and decide whether to allow or prohibit them. Based on factors including source and destination IP addresses, port numbers, protocols, and other properties, these rules specify what kinds of communication are approved or disapproved. Firewalls assist in defending networks against unauthorised access, harmful activity, and other security risks by enforcing these rules.

## Firewall Configuration







# Quality of Services (QoS)

Quality of service (QoS) refers to any technology that manages data traffic to reduce [packet loss](https://www.techtarget.com/searchnetworking/definition/packet-loss), latency and [jitter](https://www.techtarget.com/searchunifiedcommunications/definition/jitter) on a network. QoS controls and manages network resources by setting priorities for specific types of data on the network (Luthkevich, 2021).

Enterprise networks must offer dependable and quantifiable services to enable the transmission of delay-sensitive data, voice, and video. Businesses employ QoS to fulfil the traffic demands of sensitive applications, such real-time voice and video, and to stop the quality from degrading as a result of packet loss, delay, and jitter.

Utilising specific tools and methods, such as jitter buffer and traffic shaping, organisations can achieve a QoS. To ensure a specific degree of network performance, many organisations incorporate QoS in their service-level agreements (SLAs) with their network service providers.

Delivering dependable and predictable network performance for vital applications and services that demand constant and high-quality communication is the main objective of QoS. It aids in maximising network usage, reducing congestion, and ensuring that network resources are effectively used in accordance with the requirements of various applications or users.

## Importance of Prioritizing Security-Related Traffic

In today's digital world, giving security-related traffic top priority is crucial. The importance of giving security-related traffic priority can be seen in the following main reasons:

* **Protection against cyber threats:** Networks, systems, and sensitive data are protected from different cyber threats such as malware, ransomware, phishing assaults, and data breaches by giving security-related traffic priority. Organisations can give enough network resources and attention to crucial security measures, such as intrusion detection and prevention systems, firewalls, and antivirus software, by giving security-related traffic priority.
* **Mitigation of Distrusted Denial of Services (DDoS) attacks:** DDoS assaults can saturate networks with so much traffic that they become unresponsive and disrupted. Organisations are able to put in place systems that efficiently identify and mitigate DDoS attacks by giving security-related traffic priority. Organisations can recognise and filter out fraudulent traffic, allowing legitimate traffic to flow freely, by giving priority to traffic from trusted sources and deploying traffic analysis technologies.
* **Real-time threats detection and response:** The ability to monitor network traffic in real-time and give security-related traffic priority makes it possible to quickly identify security issues and potential threats. Organisations can deploy intrusion detection systems (IDS) and intrusion prevention systems (IPS) that examine network traffic patterns and spot suspicious activity by allocating resources to security-related traffic. Security teams can quickly respond to threats and reduce potential damage thanks to this prioritisation.
* **Compliance with regulatory requirements:** Organisations must abide by numerous industry-specific security and privacy rules, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). Organisations can comply with these legal requirements by putting in place security-related measures including data encryption, access controls, and secure communication channels.
* **Protection of Critical Services:** Some services, such financial transactions, healthcare systems, or emergency services, need to be available constantly and without interruption. Organisations can guarantee the dependability and accessibility of crucial services by giving security-related traffic priority, avoiding any disruptions or unauthorised access that might endanger public safety, economic stability, or privacy.
* **Enhanced user experience:** By lowering latency and enhancing network speed, prioritising security-related data can enhance user experience. Organisations can avoid bottlenecks and dedicate enough bandwidth and resources to security measures by optimising the flow of security-related traffic. This strategy aids in preserving the reliability of network connections, guards against malicious activity, and offers consumers a simple and safe interface.

## Ensuring Reliable and Predictable Service

For companies and organisations to maintain a high level of customer satisfaction, operational efficiency, and competitiveness, reliable and predictable service is crucial. Here are a few important elements that go into providing dependable and predictable service:

* **Network Stability:** Network stability is an issue of load on the hardware of the network. The goal of network stability is to get all packets traveling from source to destination at a regular speed. Don’t confuse the goals of network stability and high network speeds (Zelleke, 2023). For reliable service delivery, a robust and well-maintained network infrastructure is essential. This entails using failover mechanisms, monitoring systems for early issue detection, and having redundant components. Organisations can reduce downtime, service interruptions, and the resulting harm to customers and operations by maintaining network stability.
* **Quality of Services (QoS):** Any solution that controls data flow to lower packet loss, latency, and jitter on a network is known as a quality of service (QoS). By assigning priorities to particular types of network traffic, Quality of Service (QoS) regulates and maintains network resources. Organisations can prioritise and allocate network resources depending on the particular needs of various services or applications by implementing QoS systems. Organisations can make sure that crucial services like VoIP, video conferencing, or real-time data transmission receive the necessary bandwidth, latency, and dependability to operate at their best by giving them a higher priority.
* **Traffic Management:** Effective traffic management promotes network performance optimisation and guarantees consistent service delivery. Organisations can manage network congestion, avoid bottlenecks, and allocate resources depending on service requirements by using traffic shaping, traffic prioritisation, and bandwidth management strategies. This method minimises the negative effects of bandwidth-intensive applications on other services while ensuring a consistent user experience.
* **Service-level agreements (SLAs):** The agreed-upon service level between a provider and a customer is specified by SLAs. They provide information about performance indicators, response times, uptime assurances, and sanctions for not upholding the established criteria. Organisations commit to provide dependable and predictable service by establishing SLAs with consumers, and they have procedures in place to address any issues that may develop.
* **Monitoring and Proactive Maintenance:** For the purpose of discovering possible problems or performance degradation before they have an influence on service quality, it is essential to continuously monitor network infrastructure, systems, and services. Regular updates, patches, and hardware/software upgrades are all examples of proactive maintenance that assist avoid vulnerabilities, security lapses, and unplanned service interruptions. Organisations may guarantee dependable and predictable service delivery by monitoring and maintaining the network environment.
* **Capacity Planning:** A thorough analysis of the present and foreseeable demands for network resources and services is necessary for capacity planning. Organisations can prevent resource exhaustion, a decline in service quality, and unscheduled downtime by forecasting growth and matching network capacity with anticipated needs. By allowing for scalability and flexibility, capacity planning makes sure that services can handle rising traffic and demand without jeopardising dependability.
* **Disaster recovery and Business Continuity:** Effective business continuity and disaster recovery plans are essential for reducing service interruptions in the case of unanticipated incidents. This consists of consistent backups, redundant systems, additional connectivity alternatives, and established processes for an immediate service restoration in the event of an interruption. Organisations may sustain dependable and predictable service even in difficult conditions by proactively preparing for future disasters.

# Conclusion

For real-time and latency-sensitive applications like VoIP (Voice over Internet Protocol), video conferencing, online gaming, and video streaming, QoS is especially crucial. A better user experience is achieved by prioritising and assigning resources to these key services, ensuring that they get the required bandwidth, low latency, and minimal packet loss.

Overall, QoS is essential for managing network congestion, maximising network performance, and providing dependable and predictable service for various types of traffic.

In conclusion, giving security-related traffic priority is essential for safeguarding networks, systems, and sensitive information, reducing cyber threats, adhering to regulations, and assuring the availability of vital services. It helps maintain a strong security posture, improve user experience, and increase resilience to changing cybersecurity issues.

In conclusion, a stable network infrastructure, QoS mechanisms, efficient traffic management, SLAs, proactive monitoring and maintenance, capacity planning, and disaster recovery procedures are all necessary to ensure reliable and predictable service. Organisations may exceed consumer expectations, deliver dependable, high-quality services, and acquire a competitive edge in the market by concentrating on these elements.

# Introduction

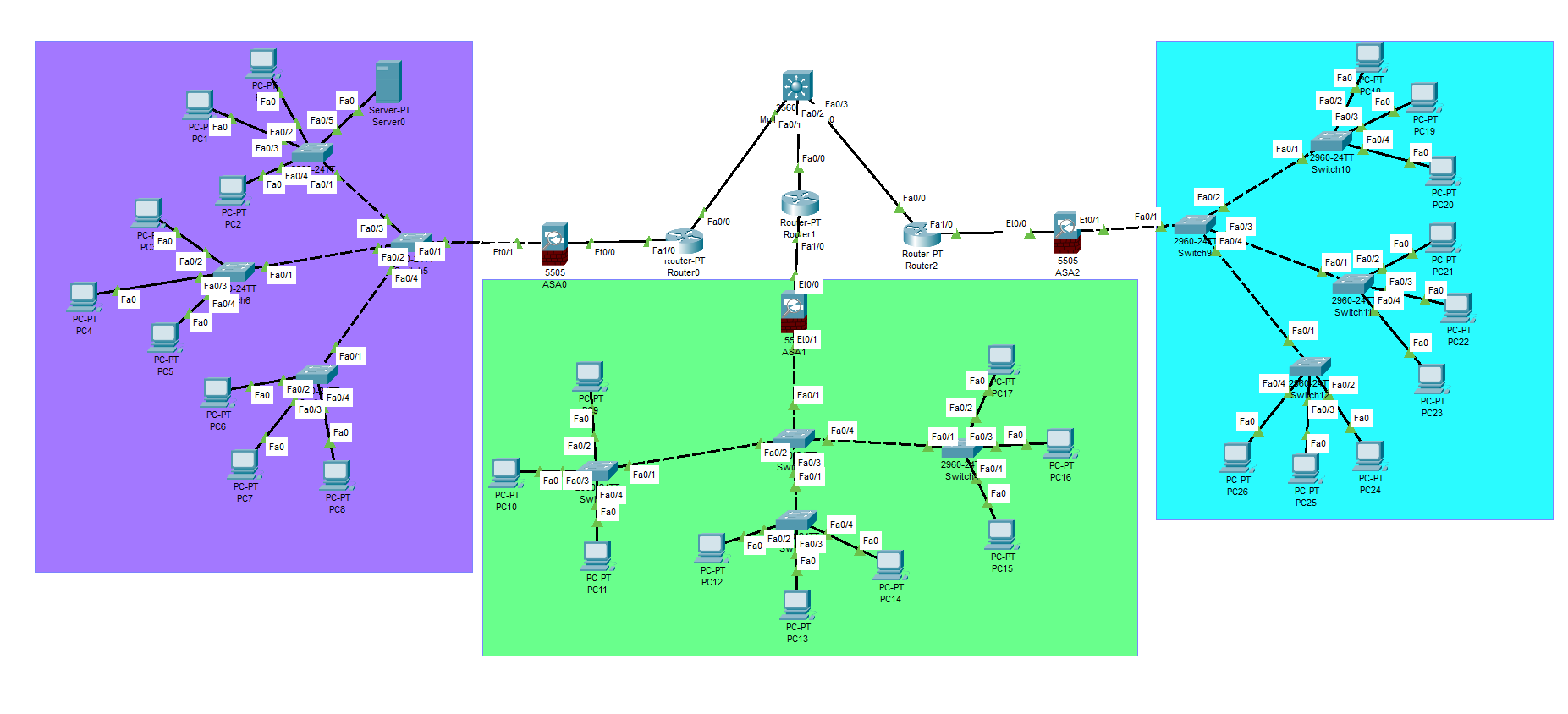
In this part I am going to do network testing which is given on the scenario. The act of analysing and evaluating your network using a network performance test to find faults and performance issues, assess significant network modifications, and measure network performance is known as network testing (or network performance testing), which is comparable to software testing. I will be test plan development in this part as well as I am going to write test plan explanation, identification of test object and many more.

## Sample Test table for the network of London College

|  |  |
| --- | --- |
| Title | To-Dos. |
| Test Title | * What is being tested? |
| Test Scenario | * Background of the scenario where we are testing. * What pre-configurations have been done in which devices? * What are the results before the configuration? |
| Test Steps | * What steps have been taken to fulfil the test? |
| Expected Result | * What are the criteria for the test to be successful? |
| Test Data | * Screenshots and scripts of the testing. |
| Actual Result | * What is the outcome of the test? |
| Analysis | * Have the criteria for the test to be successful been met? * Write down additional comments if necessary. |

**Network Testing**

Logical workspace of the London College Network:



## Testing firewall

|  |  |
| --- | --- |
| Test Title | Testing firewall configuration. |
| Test Scenario | VLANs 1 and 2 have been set up; VLAN 1 is for the internal interface and VLAN 2 is for the external interface. Because it is the internal network and a more secure area behind the firewall, the inside interface has been given a security-level of 100. As the least trusted zone, the outside interface has been given a security-level of 0. Here, we'll test whether or not the firewall will prevent incoming traffic into the LAN. |
| Test Steps | First, let me confirm the VLANs and Security-level setup for firewall.        From now on, ICMP traffic will be sent from the local area network. We should observe the ping failing since firewalls frequently block ICMP Echo Request and Echo Reply signals. |
| Expected Result | Blocks ICMP Traffic |
| Test  Data |  |
| Actual Result | Blocks ICMP Traffic |
| Analysis | The criteria for the test to be successful has been fulfilled. The ICMP traffic has been blocked. |

**Testing ACL**

|  |  |
| --- | --- |
| Test Title | Testing ACL |
| Test Scenario | The firewalls had not previously been configured with an ACL.  I configured the firewalls with an interior security level of 100 and an outside security level of 0. As a result, it previously refused all inbound traffic. The next screenshot depicts a PC in Block A pinging the successful inside interface of the firewall and the unsuccessful outside interface of the firewall. |
| Test Steps | Configuration of ACL to allow ICMP and TCP traffics |
| Expected Result | Ping should be success |
| Test Data |  |
| Actual Result | Ping Sucessfull |
| Analysis | The test has met the requirements necessary for it to be successful. According to how the ACL is set up, ICMP traffic is permitted to flow through. |

# Conclusion

In this part I had test various testing like testing ACL, Testing firewall. And also created testing table for the London college. The act of analysing and evaluating your network using a network performance test to find faults and performance issues, assess significant network modifications, and measure network performance is known as network testing (or network performance testing), which is comparable to software testing. I will be test plan development in this part as well as I am going to write test plan explanation, identification of test object and many more.

# References

Awati, R., 2021. *TechTarget.* [Online]   
Available at: https://www.techtarget.com/searchnetworking/definition/network-access-control  
[Accessed 8 May 2023].

Barney, N., 2022. *TechTarget.* [Online]   
Available at: https://www.techtarget.com/searchnetworking/definition/network-security  
[Accessed 8 May 2023].

Contributor, T., 2021. *TechTarget.* [Online]   
Available at: https://www.techtarget.com/searchnetworking/definition/network-interface-card  
[Accessed 19 June 2023].

Gillis, A. S., 2023. *TechTarget.* [Online]   
Available at: https://www.techtarget.com/searchsecurity/definition/intrusion-prevention  
[Accessed 8 May 2023].

Irei, A., 2021. *TechTarget.* [Online]   
Available at: https://www.techtarget.com/searchnetworking/definition/router  
[Accessed 19 June 2023].

Luthkevich, B., 2021. *TechTarget.* [Online]   
Available at: https://www.techtarget.com/searchunifiedcommunications/definition/QoS-Quality-of-Service  
[Accessed 19 June 2023].

Lutkevich, B., 2022. *TechTarget.* [Online]   
Available at: https://www.techtarget.com/searchnetworking/definition/access-control-list-ACL  
[Accessed 12 May 2023].

pp\_pankaj, 2020. *GeeksforGeeks.* [Online]   
Available at: https://www.geeksforgeeks.org/intrusion-detection-system-ids/  
[Accessed 8 May 2023].

Richards, K., 2021. *TechTarget.* [Online]   
Available at: https://www.techtarget.com/searchsecurity/definition/cryptography  
[Accessed 12 May 2022].

Rouse, M., 2013. *Techopedia.* [Online]   
Available at: https://www.techopedia.com/definition/13538/wireless-access-point-wap  
[Accessed 19 June 2023].

Rouse, M., 2014. *Techopedia.* [Online]   
Available at: https://www.techopedia.com/definition/8558/network-server  
[Accessed 19 June 2023].

Rouse, M., 2020. *Techopedia.* [Online]   
Available at: https://www.techopedia.com/definition/2306/switch-networking  
[Accessed 19 June 2023].

Williams, L., 2023. *GURU99.* [Online]   
Available at: https://www.guru99.com/difference-http-vs-https.html  
[Accessed 8 May 2023].

Williams, L., 2023. *GURU99.* [Online]   
Available at: https://www.guru99.com/vlan-definition-types-advantages.html  
[Accessed 12 May 2023].

Yasar, K., 2023. *TechTarget.* [Online]   
Available at: https://www.techtarget.com/searchsecurity/definition/firewall  
[Accessed 19 June 2023].

Zelleke, L., 2023. *Comparitech.* [Online]   
Available at: https://www.comparitech.com/net-admin/how-to-network-stability-test/#:~:text=Network%20stability%20is%20an%20issue,stability%20and%20high%20network%20speeds.  
[Accessed 20 June 2023].