# ASSIGNMENT COVER SHEET

|  |  |  |
| --- | --- | --- |
| **Student’s name** | Joshua | Morton |
| **Module name** | Data Communications & Network Security | |
| **Title of assignment** | Joshua Morton DCNS Assesssment | |
| **Complete Word Count in my assignment** |  | |
| **Date submitted** |  | |

All work must be submitted by the due date. If an extension of time to submit work is required, a [Mitigating Circumstances Extension Form](https://canvas.qa.com/courses/1041/files/660514?module_item_id=143660) must be submitted.

X

**Has an extension been approved? Yes No If yes, please give the new submission date ….…/..…./…….**

|  |
| --- |
| IMPORTANT: THIS STATEMENT MUST BE READ & SIGNED  **Academic Integrity Statement**  Academic integrity and honesty are fundamental to the academic work you produce at the University of Roehampton. You are expected to complete coursework which is your own and which is referenced appropriately. The university has in place measures to detect academic dishonesty in all its forms. If you are found to be cheating or attempting to gain an unfair advantage over other students in any way, this is considered academic misconduct, and you will be penalised accordingly.   ​  **I declare that the work I am submitting is my own work, is properly referenced and has not been submitted elsewhere.** |
| **Student Signature (Full Name):**  **Date: 13/12/2023** |

# Table of Contents

[ASSIGNMENT COVER SHEET 1](#_Toc150610324)

[Table of Contents 1](#_Toc150610325)

[Table of Figures 1](#_Toc150610326)

[Task 1 – OSI Model 1](#_Toc150610327)

[Task 2 – Physical Topologies 2](#_Toc150610328)

[Task 3 – Network Security 2](#_Toc150610329)

[Task 4 Reflections 2](#_Toc150610330)

[Appendices 2](#_Toc150610331)

[References 2](#_Toc150610332)

[Glossary 2](#_Toc150610333)

# Table of Figures

[Figure 1 Internal Protocol stack & OSI Reference Model (Kurose, 2017). 2](#_Toc150612528)

# Task 1 – OSI Model

A table of different types of software

Description automatically generated with medium confidence

Figure Internet Protocol stack & OSI Reference Model (Kurose, 2017).

## Brief:

Introduced by the International Organization for Standardization (ISO) in 1983, the OSI (Open Systems Interconnection) model is a fundamental conceptual framework for understanding and designing network systems. It extends the traditional Internet Protocol Stack with two additional layers, resulting in a comprehensive seven-layer architecture. This model is crucial for explaining the complex process of network communication, though it's important to note that not all networks strictly adhere to this model in practice.

## Physical Layer:

The foundation of the OSI model, the Physical Layer, deals with the hardware elements of network communication, such as cables, switches, and network interface cards (NICs). Ethernet cables, for example, are commonly used at this layer to physically transmit data.

## Data Link Layer:

Responsible for node-to-node transfer, the Data Link Layer provides error detection and correction. It also defines protocols for establishing and terminating connections between physically connected devices. The Ethernet Protocol is a key protocol at this layer, ensuring efficient and error-free data transfer.

## Network Layer:

This layer manages packet delivery across multiple networks. It is responsible for data routing, forwarding, and addressing, with the Internet Protocol (IP) being pivotal in performing these functions. The Network Layer ensures that data packets reach their intended destination, regardless of the route they need to take.

## Transport Layer:

The Transport Layer provides a reliable and transparent transfer of data between end systems. Protocols like the Transmission Control Protocol (TCP) offer error recovery, flow control, and complete data transfer, ensuring data integrity.

## Session Layer:

Establishing, managing, and terminating connections between applications, the Session Layer uses protocols like NetBIOS. This layer is essential for setting up and coordinating communication between applications, facilitating data exchange in an organized manner.

## Presentation Layer:

Acting as a translator, the Presentation Layer converts data between the network and application layers. It is responsible for crucial functions like data encryption and decryption, compression, and translation. The Secure Sockets Layer (SSL) protocol, commonly used for establishing secure links between servers and clients, operates at this layer.

## Application Layer:

The topmost layer, the Application Layer, directly interacts with software applications to provide network services. The Hypertext Transfer Protocol (HTTP), fundamental to the World Wide Web, operates at this layer, managing the transfer of web content.

## Summary and Criticisms:

Each layer of the OSI model interacts seamlessly with the layers directly above and below it, creating a cohesive and comprehensive framework for understanding network communications. This model not only simplifies the complex process of data transmission across networks but also aids in troubleshooting network issues by segmenting different network functions into distinct layers.

However, the OSI model is not without its limitations. Its strict layering can sometimes be too rigid for practical implementations, and some modern protocols operate across multiple layers, blurring the distinctions outlined by the model. Despite this, the OSI model remains a cornerstone in the field of network communication, providing a clear and structured approach to understanding how different network technologies and protocols interact.

In conclusion, the OSI model, with its layered architecture, plays a pivotal role in the field of network communication. It serves as a guide for designing network systems and for understanding the complexities of data transmission across diverse network infrastructures. While not all networks strictly conform to this model, its theoretical framework continues to be crucial for students, engineers, and IT professionals in grasping the fundamentals of network communication.

# Task 2 – Physical Topologies

In an increasingly interconnected business environment, the ability to efficiently connect multiple office locations is paramount. This essay delves into the various aspects of network topologies, types of connectivity for remote offices, and the technicalities of a specific network protocol and device. Each section not only discusses the available options but also recommends the most suitable choice for connecting two remote offices.

## Physical Network Topologies

### Bus Topology

In this layout, all nodes are connected to a single central cable, the bus. It’s simple but limited in scalability and robustness.

### ****Star Topology****:

Each node connects to a central hub or switch. It’s highly scalable and reliable; if one link fails, it doesn’t affect others.

### Ring Topology:

Each node connects to exactly two other nodes, forming a ring. While it can efficiently handle data in one direction, its redundancy is limited.

### Mesh Topology

Every node is connected to every other node. This offers high redundancy and reliability but is complex and expensive to implement.

For connecting remote offices, the Star Topology is recommended. Its simplicity, scalability, and reliability are key advantages. In a business context, these attributes ensure minimal downtime and ease of network management.

## Connectivity Types between Remote Offices

Connecting remote offices requires consideration of various connectivity types, each with its strengths and challenges:

### Leased Lines:

Dedicated telephone lines for continuous use. They offer security and consistent quality but are expensive.

### Public Internet with VPN:

The public internet with a Virtual Private Network (VPN) provides secure and cost-effective connectivity.

### Multi-Protocol Label Switching (MLPS):

A routing technique in telecommunications networks that directs data from one node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table.

Considering cost-effectiveness and security, using the Public Internet with a VPN is recommended. It provides a balance of security, reliability, and affordability, crucial for small to medium-sized businesses.

## Network Protocol and Device

### Network Protocol:

IPsec (Internet Protocol Security) is a protocol suite for securing Internet Protocol (IP) communications. It authenticates and encrypts each IP packet in a communication session, providing data integrity, authentication, and confidentiality. IPsec operates in two modes: Transport and Tunnel. Transport mode encrypts only the message within the data packet, while Tunnel mode encrypts the entire packet. For remote office connectivity, Tunnel mode is preferred, as it encapsulates the entire IP packet for transmission over unsecured networks like the internet.

### Network Device:

A VPN router is a networking device that enables the creation of a secure connection over a public network. In our scenario, it allows remote offices to connect securely to the head office network. The router encrypts data from the sending network and decrypts it at the receiving end, creating a 'tunnel' for safe data transmission. It integrates well with IPsec, enhancing the security of data transmission across the internet.

## Summary:

For effective connectivity between remote offices, the Star Topology is the most suitable physical layout due to its balance of reliability and simplicity. The use of the public internet with a VPN offers a cost-effective and secure way to connect these offices. The combination of IPsec and a VPN router ensures that sensitive data remains secure during transmission. This integrated approach provides a robust solution for modern businesses, ensuring efficient and secure communication across multiple locations.

# Task 3 – Network Security

**NOTES: 555 words**

# Task 4 Reflections

**NOTES: 555 words**

# Appendices

# References

ISO/IEC, 1994. Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. Multiple, America. [Accessed 11/11/2023]

Kurose, James, 16/02/2018. Computer Networking: A Top-Down Approach, Global Edition. Pearson Education, Rotherham, England. [Accessed 11/11/2023]

# Glossary