# 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](#_Toc150627954)

[Table of Contents 2](#_Toc150627955)

[Table of Figures 3](#_Toc150627956)

[Task 1 – OSI Model 3](#_Toc150627957)

[Brief: 3](#_Toc150627958)

[Physical Layer: 4](#_Toc150627959)

[Data Link Layer: 4](#_Toc150627960)

[Network Layer: 4](#_Toc150627961)

[Transport Layer: 4](#_Toc150627962)

[Session Layer: 4](#_Toc150627963)

[Presentation Layer: 4](#_Toc150627964)

[Application Layer: 4](#_Toc150627965)

[Summary and Criticisms: 5](#_Toc150627966)

[Task 2 – Physical Topologies 5](#_Toc150627967)

[Physical Network Topologies 5](#_Toc150627968)

[Bus Topology 6](#_Toc150627969)

[Star Topology: 6](#_Toc150627970)

[Ring Topology: 6](#_Toc150627971)

[Mesh Topology 6](#_Toc150627972)

[Connectivity Types between Remote Offices 6](#_Toc150627973)

[Leased Lines: 6](#_Toc150627974)

[Public Internet with VPN: 6](#_Toc150627975)

[Multi-Protocol Label Switching (MLPS): 7](#_Toc150627976)

[Network Protocol and Device 7](#_Toc150627977)

[Network Protocol: 7](#_Toc150627978)

[Network Device: 7](#_Toc150627979)

[Summary: 7](#_Toc150627980)

[Task 3 – IP Addressing Scheme 7](#_Toc150627981)

[Brief: 7](#_Toc150627982)

[Understanding IPv4 Addressing: 8](#_Toc150627983)

[Subnetting for Efficiency: 8](#_Toc150627984)

[Recommendation for New Network System: 8](#_Toc150627985)

[Summary: 8](#_Toc150627986)

[Task 4 Network Security 9](#_Toc150627987)

[The Transport Layer of OSI Model 9](#_Toc150627988)

[Encryption with SSL: 9](#_Toc150627989)

[Use of VPNs: 9](#_Toc150627990)

[Relevance to Software Consulting Environment 9](#_Toc150627991)

[Impact of Transport Layer Security 9](#_Toc150627992)

[Summary 10](#_Toc150627993)

[Appendices 10](#_Toc150627994)

[References 10](#_Toc150627995)

[Glossary 11](#_Toc150627996)

# 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 1 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 today’s increasingly interconnected business world, efficient network connections across multiple office locations are essential. Network topology refers to the arrangement of elements in a network. Physical topology is the actual layout of these elements, while non-physical, also referred to as logical topology, describes the paths for data transfer within the network (Pcmag). Individual topologies offer varying advantages and disadvantages depending on the requirements of the business and the network.

## Physical Network Topologies

Several computer network connections

Description automatically generated with medium confidence

Figure 2 - Common Network Topologies (Sayeed 2017)

### 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 (Rouse, 2023).

### 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 (Stewart, 2015). In a business, 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 (Kurose, pg. 666, 2017).

### 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 (Stewart, chapter 11, 2020).

## 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 – IP Addressing Scheme

## Brief:

Despite the advent of IPv6, IPv4’s 32-bit addressing provides approximately 4.3 billion unique addresses, historically thought to be sufficient. However, with the exponential growth of internet-connected devices, efficient utilization of these addresses is crucial. Businesses aiming to adopt new network segments must consider their addressing schemes & subnetting for minimal wastage of addresses.

## Understanding IPv4 Addressing:

IPv4 addresses utilize 32-bit numbers, expressed in decimal formats as four octets separated by periods, for example: 192.168.1.1. Each octet ranges from 0 to 255. The 4.3 billion number of unique addresses comes from multiplying 256 to the exponent of 4. This format not only facilitates address readability but also helps in network segmentation, commonly known as subnetting. Subnetting divides a larger network into smaller, manageable segments, improving network performance security.

## Subnetting for Efficiency:

Subnetting is key to utilizing IPv4 addresses efficiently. It involves using a subnet mask to determine the division of network and host components within an IP address. The subnet mask reveals how many addresses are available for a network and its devices. For example, a subnet mask of 255.255.255.0 (/24) allows for 256 addresses, but if a network only needs to support 50 devices, this results in significant wastage.

## Recommendation for New Network System:

Assuming the need is to accommodate approximately 200 devices, a /24 network (255.255.255.0) provides 256 addresses, which exceeds the requirement and leads to wastage. A more fitting choice would be to use a /25 subnet (255.255.255.128), which offers 128 addresses. However, this wouldn’t suffice for 200 devices. Thus, the recommendation is to use two /25 subnets or a single /24 subnet but segmented into smaller subnets as needed.

For minimal wastage, using two /25 subnets is optimal. This scheme allows for 256 addresses in total (128 per subnet), closely matching the requirement of 200 addresses. This way, the network can accommodate all necessary devices with minimal address space left unused.

Technical Implementation

In a practical scenario, the two /25 subnets can be allocated based on departmental needs or geographical location. For instance, one subnet can be designated for administrative use, and another for operational departments. This not only conserves address space but also enhances network organization, management, and security.

Business Implications

From a business perspective, efficient IP address utilization leads to cost savings, as purchasing additional IP addresses can be expensive. It also prepares the business for future scalability and possible integration with IPv6. Additionally, well-planned subnetting enhances network performance and security, which are critical for business operations.

## Summary:

An effective IPv4 addressing scheme for a network segment requiring around 200 addresses would be to use two /25 subnets. This approach minimizes wastage while ensuring sufficient addresses for all devices. It exemplifies efficient network planning, balancing the need for adequate address space with the conservation of limited IPv4 resources, a practice crucial in today's network-driven business environments.

# Task 4 Network Security

In a software consulting firm, particularly one that operates behind an office VPN and interfaces with client networks, network security is paramount. This essay focuses on the Transport Layer of the Open Systems Interconnection (OSI) model, discussing how security can be effectively implemented at this layer to protect sensitive data and communications in a consulting environment.

## The Transport Layer of OSI Model

Discussed earlier, the transport layer of the OSI model, plays a critical role in providing communication services directly to the application processes running on different hosts. The Transport Layer ensures that data is transferred reliably and without errors, making it a focal point for implementing security measures in network communications.

## Encryption with SSL:

* Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols that provide secure communication over a computer network at the Transport Layer.
* They encrypt the data transmitted between the client and server, ensuring that sensitive information remains confidential and secure from potential eavesdropping or tampering.
* In the context of a software consulting firm, SSL/TLS can be used to secure communications with client networks, particularly when accessing sensitive data or transferring proprietary information.

## Use of VPNs:

* While VPNs operate across multiple layers, their use of SSL/TLS protocols ties them closely to the Transport Layer.
* A VPN encrypts all data that passes through it, ensuring that all information moving between the consulting firm and external networks remains secure.
* This is particularly important when consultants access client systems remotely, as it prevents unauthorized access and data breaches.

## Relevance to Software Consulting Environment

Data and network security are crucial for maintaining client trust and protecting intellectual property, the importance of Transport Layer security cannot be overstated:

* SSL/TLS protocols ensure that data is not altered or intercepted during transmission, enhancing data integrity and confidentiality. This is crucial when handling client data, especially for projects involving sensitive information.
* Consultants often need to access client networks and resources remotely. Secure VPN connections, leveraging Transport Layer protocols, ensure that remote access is as secure as if the consultants were on-site.
* Many industries have strict data protection and privacy regulations. Software Consultancy firms often seek an ISO/IEC 27001 certificate, which is an international standard to manage information security. Implementing robust Transport Layer security helps in complying with these standards, avoiding potential legal and financial repercussions.

## Impact of Transport Layer Security

The implementation of security measures at the Transport Layer has a significant impact on a software consulting firm:

* Demonstrating a commitment to security through robust Transport Layer protocols enhances client confidence and trust, a key asset in the consulting business.
* By encrypting data transmissions, the risk of data breaches and cyber-attacks is significantly lowered, protecting both the firm and its clients.
* Secure and reliable data transfer ensures that projects run smoothly without interruptions caused by security breaches or data loss.

## Summary

In conclusion, focusing on security at the Transport Layer of the OSI model is crucial for a software consulting firm. Utilizing SSL/TLS protocols and VPNs to secure data transmission at this layer is not only a technical necessity but also a business imperative. It ensures the protection of sensitive data, maintains client trust, and aligns with industry standards for data security and privacy.

# Appendices

# References

Bidgoli, Hossein, 06/08/2002. Encyclopedia of Information Systems. 1st Edition. Academic Press, Cambridge, Massachusetts, United States of America. [16/11/2023]

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]

Pcmag, N.D. Definition of logical vs physical topology. [online] Available at: [Accessed 16/11/2023]

Rouse, Margaret, 28/06/2023. Star Topology [online] Available at: https://www.techopedia.com/definition/13335/star-topology [Accessed 16/11/2023]

Sayeed, Abu. 12/09/2023. Computer Network Topology Outline. [article] Available At: <https://systemzone.net/computer-network-topology-outline/> [Accessed 13/11/2023]

Stallings, William. 13/10/2023. Foundations of Modern Networking: SDN, NFV, QoE, IoT and Cloud. 1st Edition, Addision-Wesley Professional. Boston, United States of America. [Accessed 12/11/2023]

Stewart, James Michael. 23/10/2015. CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide. 7th Edition. Sybex, Alameda, California, United States of America. [Accessed 14/11/2023]

Stewart, James Michael. 15/10/2020. Network Security, Firewalls and VPNs. 3rd Edition. Jones & Bartlett Learning. Burlington, Massachusetts, United States of America. [Accessed 17/11/2023]

Wilson, Engr Kurt. 05/12/2019. Network Topology: The Physical and Logical Structure of a Network connection Between Model and nodes. N/A. [Accessed 13/11/2023]

# Glossary