# 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** | 2450 words, including headings. Excluding table of contents, figures, references, and glossary. | |
| **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: 14/12/2023** |

# Table of Contents

[ASSIGNMENT COVER SHEET 1](#_Toc153453379)

[Table of Contents 2](#_Toc153453380)

[Table of Figures 3](#_Toc153453381)

[Task 1 – OSI Model 4](#_Toc153453382)

[Physical Layer: 4](#_Toc153453383)

[Data Link Layer: 4](#_Toc153453384)

[Network Layer: 4](#_Toc153453385)

[Transport Layer: 5](#_Toc153453386)

[Session Layer: 5](#_Toc153453387)

[Presentation Layer: 5](#_Toc153453388)

[Application Layer: 5](#_Toc153453389)

[Summary and Criticisms: 5](#_Toc153453390)

[Task 2 – Physical Topologies 6](#_Toc153453391)

[Physical Network Topologies 6](#_Toc153453392)

[Bus Topology 6](#_Toc153453393)

[Star Topology: 6](#_Toc153453394)

[Ring Topology: 7](#_Toc153453395)

[Mesh Topology 7](#_Toc153453396)

[Connectivity Types between Remote Offices 7](#_Toc153453397)

[Leased Lines: 7](#_Toc153453398)

[Public Internet with VPN: 7](#_Toc153453399)

[Multi-Protocol Label Switching (MLPS): 7](#_Toc153453400)

[Network Protocol and Device 8](#_Toc153453401)

[Network Protocol: 8](#_Toc153453402)

[Network Device: 8](#_Toc153453403)

[Summary: 9](#_Toc153453404)

[Task 3 – IP Addressing Scheme 9](#_Toc153453405)

[Understanding IPv4 Addressing: 9](#_Toc153453406)

[Subnetting for Efficiency: 9](#_Toc153453407)

[Recommendation for New Network System: 9](#_Toc153453408)

[Technical Implementation 10](#_Toc153453409)

[Business Implications 10](#_Toc153453410)

[Summary: 10](#_Toc153453411)

[Task 4 Network Security 10](#_Toc153453412)

[The Transport Layer of OSI Model 10](#_Toc153453413)

[Encryption with SSL: 10](#_Toc153453414)

[Use of VPNs: 11](#_Toc153453415)

[Relevance to Software Consulting Environment 11](#_Toc153453416)

[Impact of Transport Layer Security 11](#_Toc153453417)

[Conclusion 11](#_Toc153453418)

[References 12](#_Toc153453419)

[Glossary 13](#_Toc153453420)

# Table of Figures

Figure 1 Internet Protocol stack & OSI Reference Model (Kurose, 2017). 3

Figure 2 - Common Network Topologies (Sayeed 2017) 6

Figure 3 Illustration of a B2B VPN Network Using MPLS (Stallings, 2015, ch.9.4) 7

# 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).

Introduced by the International Organization for Standardization (ISO) in 1983, the Open Systems Interconnection model (OSI) is a conceptual framework for understanding and designing computer network systems.

It extends the traditional Internet Protocol Stack[[1]](#endnote-1), forming a comprehensive seven layers, as shown in figure 1. Starting from the top level, it shows how human interactions with software applications can transfer data all the way down to physical cables.

This model breaks down the process of network communications by describing how a variety of network technologies and protocols are coupled together.

The aim of the model is to establish a universal standard set of protocols and technologies to allow open communication between devices through either hardware or software products (Imperva n.d.).

The following section aims to define and discuss related protocols & devices at each layer. It will cover their unique responsibilities and how they fit in with the bigger picture of safe and secure network communications.

The **Physical Layer** deals with the hardware elements of network communication, such as cables, switches (hardware that connects devices in networks), and network interface cards (NICs).

This acts as an exit for outgoing data and an entry point for incoming data. Ethernet cables, for example, are commonly used at this layer to physically transmit data (Davies, 2019).

The **Data Link Layer** is responsible for establishing and terminating connections between physically connected devices. Logical Link Controllers (LLC) enforce the format of data by performing error checking and reading Media Access Control (Obaidat, 2022) (MAC) policies of connected nodes to allow or disallow data transfer.

The Ethernet[[2]](#endnote-2) and historically Point-To-Point (P2P) protocols are found here to ensure efficient and error-free data transfer (Kurose, chapter 6, 2017).

The **Network Layer** manages packet delivery across multiple networks[[3]](#endnote-3). It is responsible for data routing, forwarding, and addressing, with the Internet Protocol[[4]](#endnote-4) (IP).

This layer ensures that data packets (formatted units of data)[[5]](#endnote-5) (Cisco, chapter 6, 2016) reach their intended destination using a physical device known as a Router[[6]](#endnote-6), regardless of the route they need to take.

Virtual Private Network[[7]](#endnote-7) Devices (VPNs) operate here to encapsulate and encrypt the payload of IP Packets. VPNs are very commonly used commercially to ensure data safety and integrity over the public internet.

The **Transport Layer** is responsible for delivering and checking packets for errors, regulating their size & sequencing and the transfer of data between systems and hosts.

Kurose (2017, p.216) states that “Application processes use the logical communication provided by the transport layer to send messages to each other”.

Protocols like the Transmission Control Protocol (TCP) (A10 Networking, 2021) operate at this level, enabling applications and devices to exchange messages over networks.

The **Session Layer** controls conversations, called sessions, between devices (Imperva, n.d) within a network. It establishes and manages connects between applications.

Network Basic Input/Output System (NetBIOS) is used at the session layer to allow applications to communicate over a local area network (Froehlich, 2021).

Additionally, Singla (2022) states that this layer is responsible for token management, which prevents two users from simultaneously accessing or attempting the same critical operation.

The **Presentation Layer** prepares data to be passed to the application layer. It defines how devices should encrypt (the process of converting data into a coded form)[[8]](#endnote-8) and decrypt (reverting coded data into a human readable form) data, as well as reducing the size of the data, known as compressing, and converting data from a user-dependent format to the common binary format (Javatpoint, 2021).

The Secure Sockets Layer[[9]](#endnote-9) (SSL) protocol operates at this layer, commonly used for establishing secure links between servers and clients by encrypting data to make it impossible to be read if intercepted (Kaspersky, n.d).

Finally, the **Application Layer**, directly interacts with software applications to provide network services (Cisco, chapter 10, 2016), allowing applications to send and receive information while presenting meaningful data to users (Imperva, n.d).

The Hypertext Transfer Protocol (HTTP), operates at this layer, managing the transfer of web content. Additionally, protocols like Simple Mail Transfer Protocol (SMTP)[[10]](#endnote-10) for email and File Transfer Protocol (FTP)[[11]](#endnote-11) for file transfers function at this layer.

## Summary:

Each layer of the OSI model interacts with the layers directly above and below it, creating an easily understandable framework for network communications.

It not only simplifies the complex process of data transmission across networks but also aids in troubleshooting network issues by splitting different network functions into distinct layers.

The historical IP Stack cemented how layered architectures shape the field of network communication.

The OSI model extended this model to add the necessary session & presentation layers that software applications required to enforce security and the readability of data to humans.

It serves as a guide for designing network systems and for understanding the complexities of data transmission across diverse network infrastructures.

Not all networks strictly conform to this model, but its importance remains for network 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 (logical topologies), describe the paths for data transfer within the network (Pcmag, n.d.).

Individual topologies offer varying advantages and disadvantages depending on the requirements of the business and the network. The section below evaluates a few common topologies and aims to justify a recommended topology for a business with remote offices.

## Physical Network Topologies

Several computer network connections

Description automatically generated with medium confidence

Figure - Common Network Topologies (Sayeed 2017)

### Bus Topology

In this layout, all nodes are connected to a single central cable, the bus. It’s simple and easy to install but limited in scalability and robustness as performance degrades with additional devices and a single failure topples the entire network.

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

Each node connects to a central hub or switch. It can add complexity as each node requires a dedicated physical connection, however it is 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, meaning data can be sent directly to any node in the network without complicated routing. 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) and it simplifies the process of setting up an on-premises VPN. 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[[12]](#endnote-12) rather than long network addresses avoiding complex lookups in a routing table.

A diagram of a network connection

Description automatically generated

Figure Illustration of a B2B VPN Network Using MPLS (Stallings, 2015, ch.9.4)

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 (Kurose, chapter 8.7.1, 2017).

## Network Protocol and Device

### Network Protocol:

IPsec (Internet Protocol Security) is a protocol suite for securing Internet Protocol communications. It authenticates and encrypts each IP packet in a communication session, providing data integrity, authentication[[13]](#endnote-13), 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, allowing private and protected data to be transmitted over an unsecured network like the internet (Suh, n.d.). For remote office connectivity, Tunnel mode is preferred, as it encapsulates[[14]](#endnote-14) 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. 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. Combining the use of IPsec and a VPN router can ensure safe transmission of data, allowing secure and remote communication.

# Task 3 – IP Addressing Scheme

IPv4’s[[15]](#endnote-15) 32-bit[[16]](#endnote-16) addressing provides approximately 4.3 billion unique addresses (Ripe, n.d).

This was previously thought to be enough, however given that the world population is now over 8 billion, with almost 6.6 billion of those own smart phones (Statista, 2022), it is no longer enough.

IPv4 addresses utilize 32-bit numbers, expressed in decimal points separating four octets[[17]](#endnote-17), for example: 192.168.1.1.

As octets are 8-bit numbers, they range from 0 to 255. The 4.3 billion number of unique addresses comes from multiplying 256 to the exponent[[18]](#endnote-18) of 4. This format facilitates address readability and network segmentation, commonly known as subnetting.

Subnetting[[19]](#endnote-19) divides a larger network into smaller, manageable segments, allowing you to minimise the IP addresses in a network & logically divide networks.

## Subnetting for Efficiency:

Subnetting is key to utilizing IPv4 addresses efficiently. It involves using a subnet mask[[20]](#endnote-20) 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 (Class C Network[[21]](#endnote-21)) allows 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 Class C 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 (This notation indicates the number of bits used for the network portion of the address) subnet (255.255.255.128) (Cisco, chapter 8, 2016), which divides addresses into two subnets offering 128 addresses each.

One address is required for the network identifier[[22]](#endnote-22), and one is required for a broadcast address[[23]](#endnote-23) (Kurose, p.369), leaving 126 hosts that can be allocated to employee devices.

For minimal wastage, it is recommended to use two /25 subnets. This scheme allows for 256 addresses in total (128 per subnet), meeting the requirement of 200 addresses.

## Technical Implementation

Practically, the two /25 subnets can be allocated based on departmental needs or geographical location. For example, one subnet can be designated for administrative use, and another for operational departments (Cloudflare, N.D). This can enhance network organization, management, and security.

## Business Implications

Financially, efficient IP address utilization save the cost of purchasing additional IP addresses, which can be expensive (Rogers, N.D).

It also prepares the business for future scalability and possible integration with IPv6, additionally, well-planned subnetting enhances network performance and security.

## 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 represents efficient network planning, balancing the need for IP address space with conservation of limited IPv4 resources in mind.

# Task 4 Network Security

In, for example, a software consulting firm, particularly one that operates behind an office VPN and interfaces with client networks, network security is paramount. This section focuses on the Transport Layer of the 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 (Stallings, 2015, ch.9.3).

## 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.

## 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.

# References

A10 Networks, 06/12/2021. What is Layer 4 of the OSI Model? [online] Available at: <https://www.a10networks.com/glossary/what-is-layer-4-of-the-osi-model/> [Accessed 13/12/2023]

Cisco Networking Academy, 14/12/2016. Introduction to Networks v6 Companion Guide. 1st edition. Cisco Press. Indianapolis, Indiana, United States. [Accessed 23/11/2023]

Cloudflare, N.D. What is a Subnet. [Article] Available at: <https://www.cloudflare.com/en-gb/learning/network-layer/what-is-a-subnet/> [Accessed 11/02/2024]

Hammad, Madhuri, 24/08/2020. GeeksForGeeks – Critique of OSI Model and Protocols. [online] Available at: <https://www.geeksforgeeks.org/critique-of-the-osi-model-and-protocols/> [Accessed 22/11/2023]

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

Davies, Gordon, 01/12/2019. Networking Fundamentals. 1st Edition. Packt Publishing, Birmingham, England. [Accessed 13/12/2023]

Froehlich, Andrew, 15/06/2021. NetBIOS (Network Basic Input/Output System) [article] Available at: <https://www.techtarget.com/searchnetworking/definition/NetBIOS> [Accessed 13/12/2023]

Imperva, N.D. OSI Model. [article] Available at: <https://www.imperva.com/learn/application-security/osi-model/> [Accessed 04/02/2024]

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

Javatpoint, 2021. Presentation Layer in OSI Model. [article] Available at: <https://www.javatpoint.com/presentation-layer-in-osi-model> [Accessed 13/12/2023]

Kaspersky, N.d. What is an SSL certificate – Definition and Explanation. [Article] Available at: <https://www.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate> [Accessed 09/02/2024]

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

Obaidat, Muath A, 14/04/2022. The Rise of Smart Cities: Advanced Structural Sensing and Monitoring Systems. 1st Edition, Butterworth-Heinemann, Digital Press, Oxford, England.

Pcmag, N.D. Definition of logical vs physical topology. [online] Available at: <https://www.pcmag.com/encyclopedia/term/logical-vs-physical> [Accessed 16/11/2023]

Ripe, N.D. Understanding IP Addressing and CIDR Charts. [article] Available at: <https://www.ripe.net/about-us/press-centre/understanding-ip-addressing/> [Accessed 11/02/2024]

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

Rogers, Andrew. N.D. How much do IPV4 addresses cost. [blog] Available at: <https://www.prefixbroker.com/news/how-much-do-ipv4-addresses-cost/> [Accessed 11/02/2024]

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

Singla, Aman. 12/01/2022. Session Layer in OSI Model. [article] Available at: <https://www.geeksforgeeks.org/session-layer-in-osi-model/> [Accessed 09/02/2024]

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]

Statista, 2022. Bank My Cell – How many phones are in the world. [Article] Available at: <https://www.bankmycell.com/blog/how-many-phones-are-in-the-world#sources> [Accessed 11/02/2024]

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]

Suh, Jonathan et al, n.d. Cloudflare: What is IPsec? How IPsec VPNs work. [article] Available at: <https://www.cloudflare.com/en-gb/learning/network-layer/what-is-ipsec/> [Accessed 13/12/2023]

William Stallings. 19/11/2015. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. 1st Edition. Addison-Wesley Professional. Boston, United States Of America. [Accessed 20/11/2023]

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

1. The **Internet** **Protocol** **Stack** is a hierarchical framework of protocols enabling data communication across diverse interconnected networks, supporting various applications and services. Later replaced with the OSI Model. [↑](#endnote-ref-1)
2. **Ethernet** is a widely used LAN technology, facilitating data transmission within a network segment based on MAC addressing and using frames to encapsulate and transfer data packets. [↑](#endnote-ref-2)
3. A **Network** is a system where multiple nodes, such as computers, devices or individuals are interconnected. Allowing for communication, data exchange and resource sharing. They facilitate collaborate tasks over varying distances. [↑](#endnote-ref-3)
4. The **Internet Protocol** is a set of rules governing the format, addressing, routing and delivery of packets of data across networks, forming the basis of internet communication. [↑](#endnote-ref-4)
5. **Data Packets** are formatted units of data carried by a packet-switched network, containing source and destination information, along with the payload being transmitted. [↑](#endnote-ref-5)
6. **Routers** connect multiple networks, directing data packets based on IP Addresses, ensuring efficient pathfinding and traffic management across diverse interconnected network segments. [↑](#endnote-ref-6)
7. **Virtual Private Networks** securely extend a private network across a public network, enabling remote access and data encryption for privacy and security in online communications. [↑](#endnote-ref-7)
8. **Encryption/Decryption** is the process of converting data into a coded form to secure it during transmission or storage, requiring a cipher to revert it back to it’s original, readable format. [↑](#endnote-ref-8)
9. The **Secure Sockets Layer** is a cryptographic protocol providing secure communication over a computer network, often used for secure web browsing, email and data transfers. [↑](#endnote-ref-9)
10. **Simple Mail Transfer Protocol (SMTP)** is a protocol used for sending email messages between servers. [↑](#endnote-ref-10)
11. **File Transfer Protocol** is a standard network protocol used for transferring files between a client and server on computer networks. It supports both upload and download functions. [↑](#endnote-ref-11)
12. **Short Path Labels** are identifiers used to direct data packets across predefined network paths enhancing efficiency and speed within large & complex networks. [↑](#endnote-ref-12)
13. **Authentication** in networking is the practice of proving the identity of a user or process. [↑](#endnote-ref-13)
14. **Encapsulation** in networking is the process of wrapping a data with protocol information before transmission over a network, ensuring reliable and structured communication. [↑](#endnote-ref-14)
15. **IPv4** and **IPv6** are Internet Protocol versions. [↑](#endnote-ref-15)
16. **32-bit** numbers in computing represent data using 32 binary digits, offering a range of values from 0 to 4,294,967,295, commonly used in IP addressing and system architectures. [↑](#endnote-ref-16)
17. **Octets,** in networking, are eight-bit number (representing at max 256 values), fundamental in IP addressing. They represent the range of 0 to 255. [↑](#endnote-ref-17)
18. An **exponent** is a mathematical operation indicating how many times a number has been multiplied by itself. [↑](#endnote-ref-18)
19. **Subnetting** divides a network into smaller subnetworks improving security and performance by reducing network congestion. It can also be used to extend a limited range of addresses within a network. [↑](#endnote-ref-19)
20. **Subnet Masks** are 32-bit numbers that divide the IP addresses into network and host portions, defining a networks size and facilitating the efficient IP address allocation and network organization. [↑](#endnote-ref-20)
21. A **Class C Network** in the context of IP Addressing, ranges from 192.0.0.0 to 255.255.255.0, primarily used for small networks, supporting up to 254 addresses per network segment. [↑](#endnote-ref-21)
22. A **Network Identifier** is the first address in an IP Subnet, used to identify the network itself and is not assignable to individual devices. [↑](#endnote-ref-22)
23. A **Broadcast Address** is the last address in an IP Subnet, used to send data to all devices on that network simultaneously. [↑](#endnote-ref-23)