NETWORKING

INTRODUCTION

# In today's interconnected world, networking plays a pivotal role in facilitating communication and data exchange across various devices and systems. As technology continues to evolve, the importance of robust and efficient networking solutions becomes increasingly evident. This report aims to explore key concepts, challenges, and advancements in the field of networking, offering insights into its fundamental principles and practical applications.

# The primary objective of this report is to provide a comprehensive overview of networking, covering topics ranging from basic networking concepts to advanced protocols and technologies.

FOUNDATION OF NETWORKING

TYPES OF NETWORKS

1. LAN = local area network: comprised of interconnected computers that cover small geographical are, like an organisations building.
2. WAN = wide area network: comprised of interconnected computers that cover a very wide are, its the entire internet
3. MAN = metropolitan area network: comprised of interconnected computers that cover a city.
4. WLAN = wireless local area network: uses wireless communication technology to connect devices.
5. PAN = personal area network: It's a network that interconnects devices within the immediate surroundings of an individual.
6. VPN = virtual private network: they make users feel as if they were plugged into a different network.

NETWORK TOPOLOGIES

# this is the physical or logical of devices in a network.

We can divide the entire network topology area into three areas:

1. Connections

Wired connections	**Wireless connections**
Coaxial cabling	Wi-Fi
Glass fiber cabling	Cellular
Twisted-pair cabling	Satellite
and others	and others

2. Nodes - Network Interface Controller (NICs)

Repeaters	Hubs	Bridges	Switches
Router/ Modem	Gateways	Firewalls	

Network nodes are the `transmission medium's connection points` to transmitters and receivers of electrical, optical, or radio signals in the medium.

3. Classifications

Therefore these topologies can be either `physical` or `logical`.
Network topologies are divided into the following eight basic types:

Point-to-Point	Bus
Star	Ring
Mesh	Tree
Hybrid	Daisy Chain

# Bus topology: All hosts are connected via a transmission medium in the bus topology. Every host has access to the transmission medium and the signals that are transmitted over i
# Star topology: Each host is connected to the `central network component` via a separate link. This is usually a router, a hub, or a switch, which directs packet to the destination.
# Ring topology: each host or node is connected to the ring with two cables:
# Tree topology: is an extended star topology that more extensive local networks have in this structure
# Mesh topology: it does not have a basic structure but rather it is a combination of other topologies combined together.

NETWORK PROTOCOLS AND STANDARDS
# There are two netorking models that descirbe communicatino and transfer of data between connected devices; The OSI Model and TCP/IP model.

OSI MODEL
# is a reference model that can be used to describe and define the communication between systems. The reference model has `seven` individual layers, each with clearly separated tasks.
# It has got seven layer;

1. PHYSICAL LAYER: The Physical layer is responsible for the physical transmission of data.
Security considerations at this layer involve protecting against physical layer attacks, such as unauthorized access to network devices or tampering with physical connections.
2. DATA LINK LAYER: The Data Link layer ensures reliable and error-free data transmission across a physical network by providing mechanisms for framing, error detection and
flow control.
data link layer attacks;MAC address spoofing or man-in-the-middle attacks.
3. NETWORK LAYER: The Network layer handles logical addressing and routing of data packets across multiple networks.
network layer attacks;IP spoofing or denial-of-service (DoS) attacks.
4. TRANSPORT LAYER: The Transport layer ensures reliable delivery of data between hosts, by establishing end-to-end connections, performs segmentation and reassembly of
data, and provides error recovery mechanisms.
5. SESSION LAYER: It establishes, maintains, and terminates connections between applications.
Security considerations at this layer involve authentication and access control to prevent unauthorized session hijacking.
6. PRESENTATION LAYER: The Presentation layer deals with data formatting, encryption, and compression.
Security considerations include protecting against presentation layer attacks, such as data injection or format string vulnerabilities
7. APPLICATION LAYER: • The Application layer provides services directly to end-users. It includes protocols for

email, web browsing, file transfer, and more.

- Security considerations at this layer involve secure coding practices and implementing application layer security measures to prevent attacks like cross-site scripting or SQL injection.

CONCLUSION: The OSI model provides a structured approach to understanding and securing network communications.

By comprehending the functions, protocols, and security considerations at each layer, organizations and cyber security professionals can implement robust security measures that encompass the entire network infrastructure.

THE TCP/IP MODEL

1. Application Layer:

At the topmost layer, the Application layer facilitates access to services and defines the protocols used for data exchange between applications. It acts as an interface between the underlying layers and the end-user applications, ensuring smooth communication.

2. Transport Layer:

Sitting above the network layer, the Transport layer caters to session services (TCP) and datagram services (UDP) for the application layer. It ensures reliable data transfer and establishes connections between the data stream and the application.

3. Internet Layer:

The Internet layer takes charge of addressing, packaging, and routing of hosts. It enables end-to-end connectivity, handling the intricacies of network addressing and routing packets across different networks.

4. Link Layer:

The Link layer plays a crucial role in transmitting TCP/IP packets over the network medium and receiving corresponding packets from it. Irrespective of the network access method or frame format, the Link layer ensures seamless communication between devices.

CONCLUSION

Understanding the TCP/IP model empowers us to grasp the intricacies of internet communication and appreciate the technological marvel that drives our connected world.

NETWORK ADDRESSING

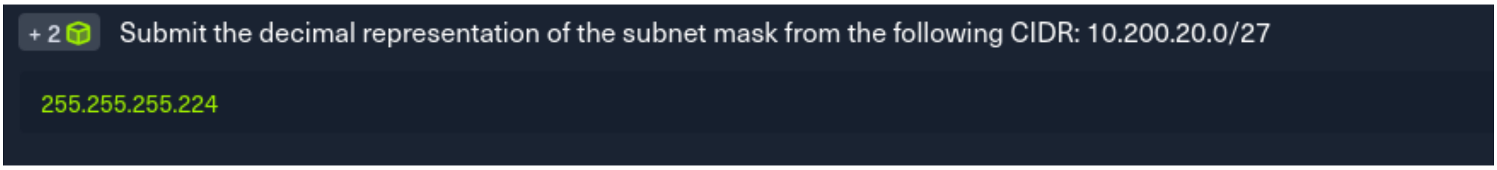
# Addressing on the Internet is done via the `IPv4` and/or `IPv6` address, which is made up of the `network address` and the `host address`.

# The most common method of assigning IP addresses is `IPv4`, which consists of a `32`-bit binary number combined into `4 bytes` consisting of `8`-bit groups (`octets`) ranging from `0-255`.

# A further separation of these classes into small networks is done with the help of `subnetting`. This separation is done using the `netmasks`, which is as long as an IPv4 address.

SUBNETTING~

A subnet is a logical segment of a network that uses IP addresses with the same network address.



Submit the decimal representation of the subnet mask from the following CIDR: 10.200.20.0/27

255.255.255.224

10.200.20.0/27

→ '/27' = first 27 bits are set to 1, and the remaining are 0.

∴ 11111111.11111111.11111111.11100000.

~~ver~~ verify conversion

11111111

$= 1 \times 2^0 = 1$

$1 \times 2^1 = 2$

$1 \times 2^2 = 4$

$1 \times 2^3 = 8$

$1 \times 2^4 = 16$

$1 \times 2^5 = 32$

$1 \times 2^6 = 64$ +

$1 \times 2^7 = 128$

~~1×2^8~~ = 255

11100000

$1 \times 2^5 = 32$

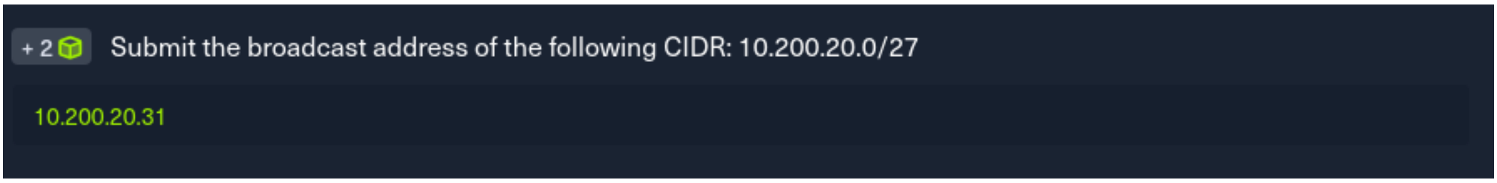
$1 \times 2^6 = 64$ +

$1 \times 2^7 = 128$

224.

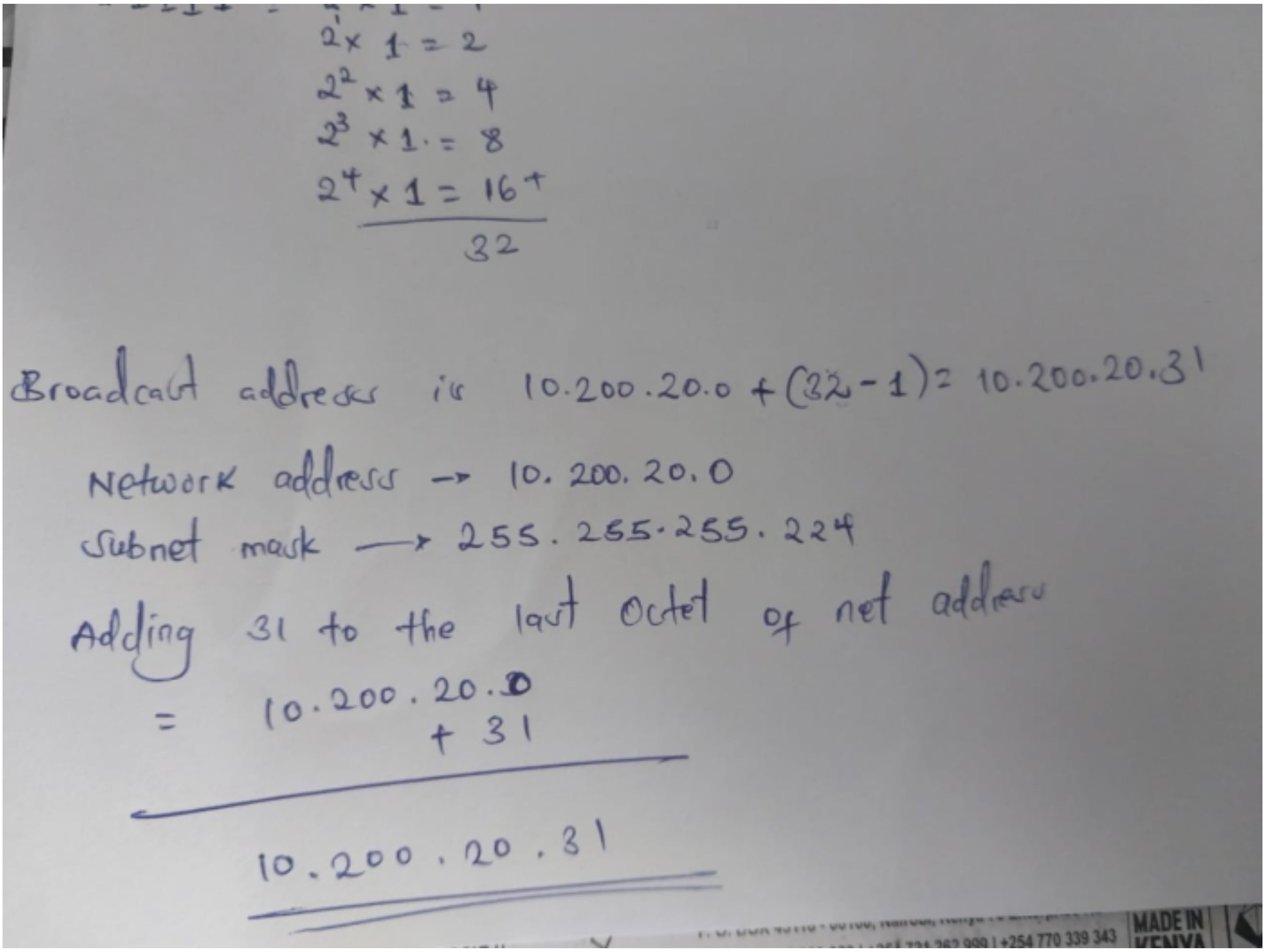
255.255.255.224

= 255.255.255.224



+2 Submit the broadcast address of the following CIDR: 10.200.20.0/27

10.200.20.31



$2^1 \times 1 = 2$

$2^2 \times 1 = 4$

$2^3 \times 1 = 8$

$2^4 \times 1 = 16 +$

32

Broadcast address is 10.200.20.0 + (32 - 1) = 10.200.20.31

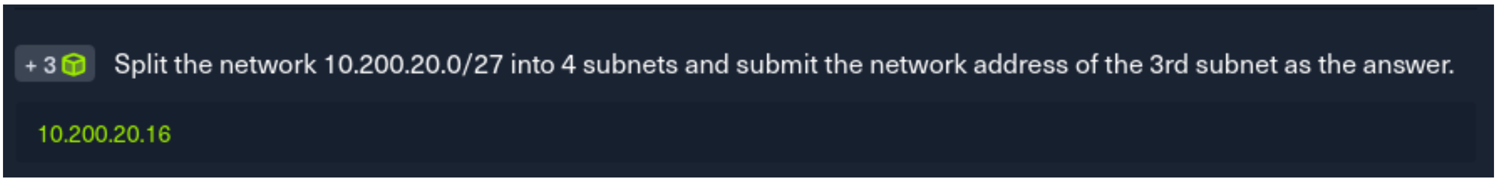
Network address → 10.200.20.0

Subnet mask → 255.255.255.224

Adding 31 to the last Octet of net address

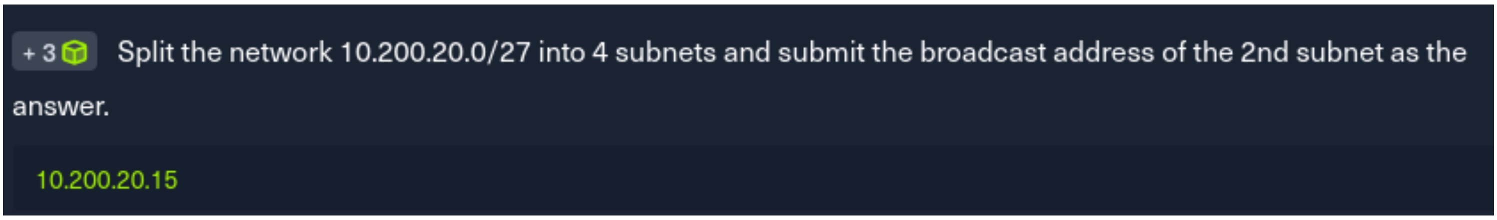
= 10.200.20.0
+ 31

10.200.20.31



+3 Split the network 10.200.20.0/27 into 4 subnets and submit the network address of the 3rd subnet as the answer.

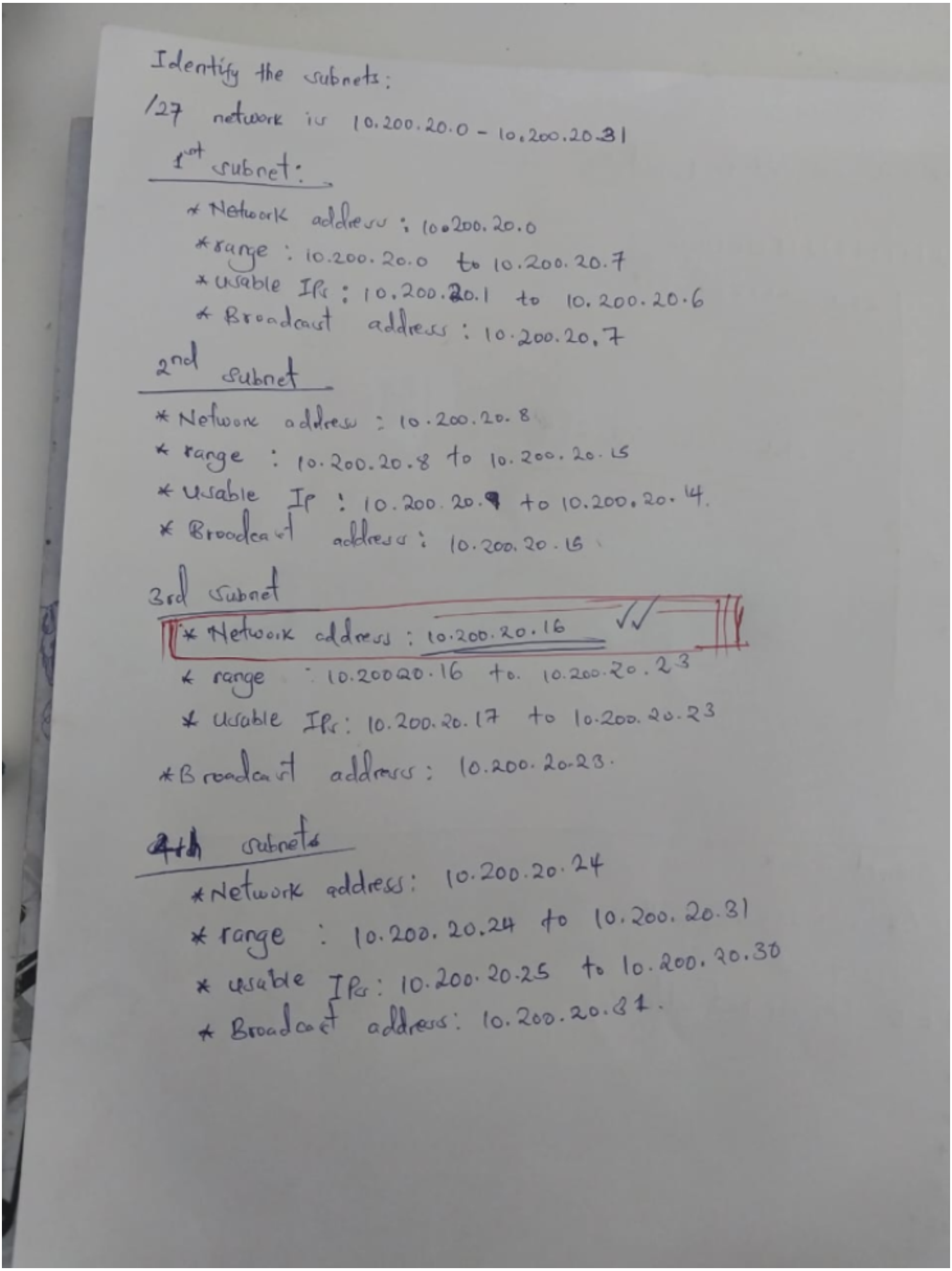
10.200.20.16



+3 Split the network 10.200.20.0/27 into 4 subnets and submit the broadcast address of the 2nd subnet as the answer.

10.200.20.15

#the image below explains how i calculated the answers for the two questions above.



Identify the subnets:

/27 network is 10.200.20.0 - 10.200.20.31

1st subnet:

- * Network address : 10.200.20.0
- *range : 10.200.20.0 to 10.200.20.7
- * usable IPs : 10.200.20.1 to 10.200.20.6
- * Broadcast address : 10.200.20.7

2nd subnet

- * Network address : 10.200.20.8
- * range : 10.200.20.8 to 10.200.20.15
- * Usable Ip : 10.200.20.9 to 10.200.20.14.
- * Broadcast address : 10.200.20.15

3rd subnet

- * Network address : 10.200.20.16 ✓✓
- * range : 10.20020.16 to. 10.200.20.23
- * usable IPs : 10.200.20.17 to 10.200.20.23
- *Broadcast address : 10.200.20.23.

4th subnets

- *Network address: 10.200.20.24
- * range : 10.200.20.24 to 10.200.20.31
- * usable IPs: 10.200.20.25 to 10.200.20.30
- * Broadcast address: 10.200.20.31.

Overview of Networking Protocols

Networking protocols are standardized rules and procedures that define how data is transmitted and received over a network. They ensure interoperability between different devices and systems, allowing seamless communication. Protocols operate at various layers of the OSI (Open Systems Interconnection) and TCP/IP (Transmission Control Protocol/Internet Protocol) models, each with specific roles and functionalities.

Types of Networking Protocols

Networking protocols can be broadly categorized into several types based on their functions and the OSI layer they operate in:

1. **Application Layer Protocols:**

- **HTTP/HTTPS (Hypertext Transfer Protocol / Secure):** Used for transmitting web pages over the internet.
- **FTP (File Transfer Protocol):** Facilitates the transfer of files between client and server.
- **SMTP (Simple Mail Transfer Protocol):** Manages the sending of emails.
- **DNS (Domain Name System):** Translates domain names into IP addresses.

- **Transport Layer Protocols:**

◇ **TCP (Transmission Control Protocol):** Ensures reliable, ordered, and error-checked delivery of data.
◇ **UDP (User Datagram Protocol):** Provides a faster, connectionless service with no guarantee of delivery, useful for real-time applications.

- **Network Layer Protocols:**

◇ **IP (Internet Protocol):** Responsible for addressing and routing packets across networks.
◇ **ICMP (Internet Control Message Protocol):** Used for error reporting and diagnostic functions like ping.

- **Data Link Layer Protocols:**

◇ **Ethernet:** A common protocol for wired local area networks (LANs).
◇ **Wi-Fi (Wireless Fidelity):** Enables wireless networking and internet access.

- **Physical Layer Protocols:**

◇ These protocols define the hardware connections, electrical signals, and data transmission mediums (e.g., cables, radio waves).

Functions of Key Networking Protocols

1. **TCP/IP Protocol Suite:**

◇ The TCP/IP suite is the foundation of the internet and most modern networks. It includes several protocols that work together to ensure data can travel from its source to its destination across diverse networks.
◇ **IP:** Handles addressing and routing of packets.
◇ **TCP:** Provides connection-oriented services, ensuring data integrity and delivery.
◇ **UDP:** Offers a lightweight, connectionless service for applications where speed is critical.

- **HTTP/HTTPS:**

◇ **HTTP:** Facilitates the transfer of web content between servers and browsers.
◇ **HTTPS:** Adds a layer of security by encrypting data using SSL/TLS, ensuring secure communication.

- **DNS:**

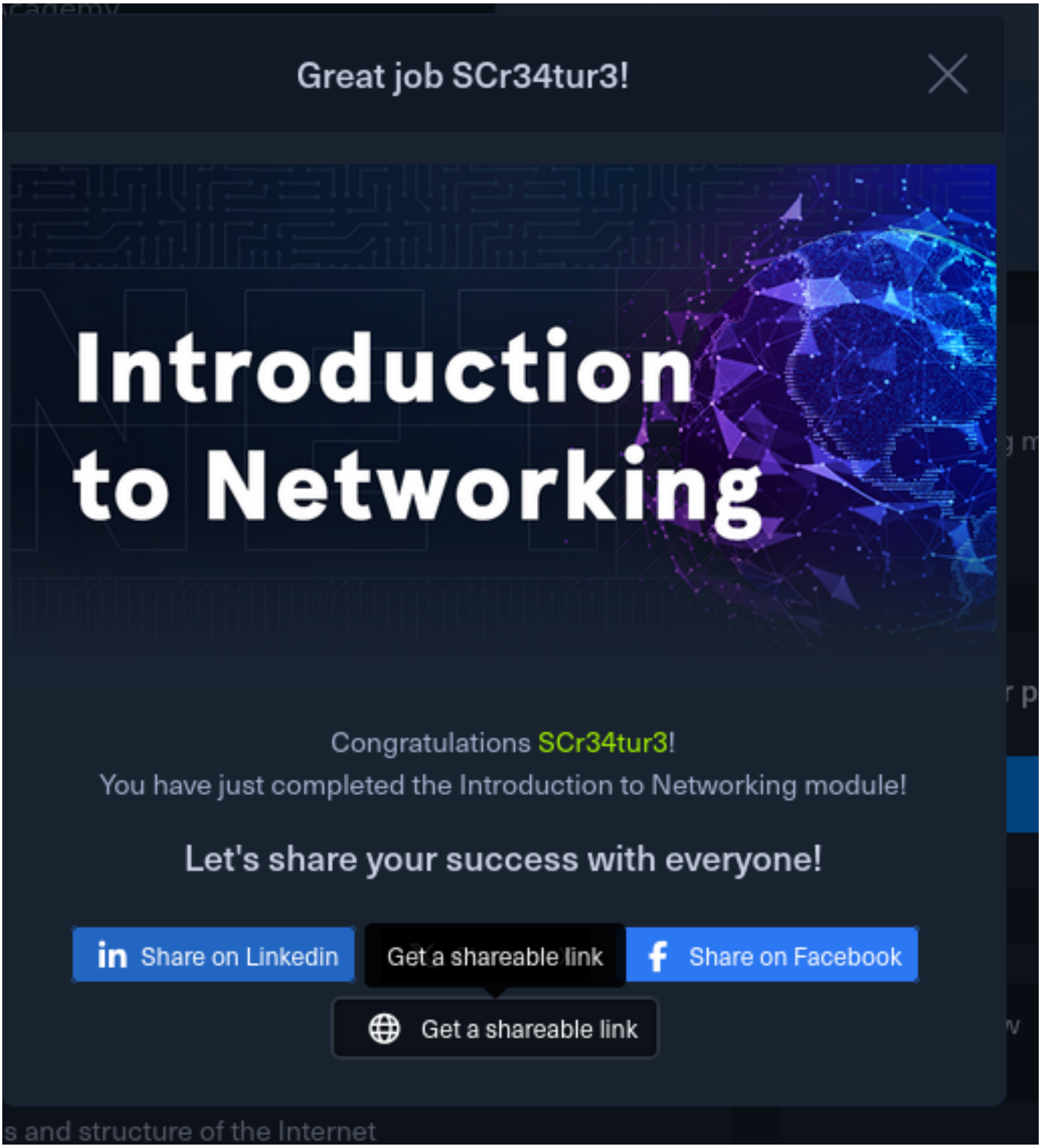
◇ DNS translates human-readable domain names (e.g., www.example.com) into IP addresses that computers use to identify each other on the network.

- **SMTP:**

◇SMTP is used to send emails, typically working in conjunction with protocols like POP3 or IMAP that handle email retrieval.

The two main types of connections used on networks are Transmission Control Protocol (`TCP`) and User Datagram Protocol (`UDP`).

AUTHENTICATION PROTOCOLS
# Many different authentication protocols are used in networking to verify the identity of devices and users.
# Here are examples of authentication protocols: https,ssh,LEAP,PEAP,MFA,2FA,SSL,TLS
This ensures that the client can verify the server's identity and helps to prevent MITM attacks.



Great job SCr34tur3!

Introduction to Networking

Congratulations SCr34tur3!
You have just completed the Introduction to Networking module!

Let's share your success with everyone!

https://academy.hackthebox.com/achievement/1287818/34

CONCLUSION

In this report, we have explored the critical role of networking protocols in modern communication systems. Networking protocols serve as the foundational elements that facilitate data exchange, ensure interoperability, and maintain the integrity and security of information transmitted across networks.

We began by examining the various types of networking protocols, categorized by the OSI model layers, from application layer protocols like HTTP/HTTPS and DNS, to transport layer protocols such as TCP and UDP, down to the network and data link layer protocols like IP and Ethernet

In conclusion, understanding and implementing networking protocols are vital for the efficient operation and growth of modern networks. As technology continues to advance, the evolution of these protocols will be essential in addressing new challenges and opportunities in the realm of digital communication. For network administrators, engineers, and IT professionals, staying abreast of these developments will be crucial in ensuring robust, secure, and high-performing networks.

Future research and development in networking protocols should focus on improving security measures, enhancing efficiency, and supporting the growing number of connected devices.