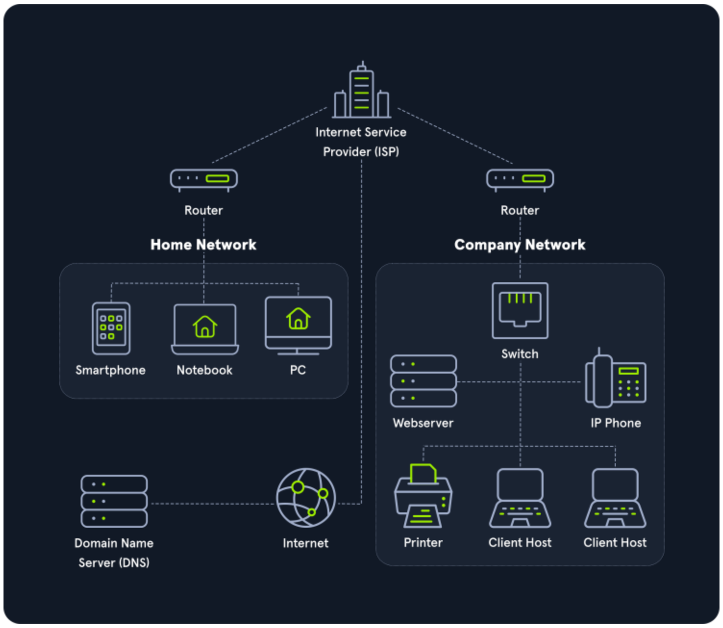
Introduction to Networking

Introduction

https://academy.hackthebox.com/achievement/949661/34

This report aims to provide a foundational understanding of various aspects of networking. Designed for both beginners and intermediate learners, it covers key concepts, technologies, and protocols that form the backbone of the networking world. From the basics of cryptography and TCP/UDP connections to more advanced topics like network security and VLANs, this guide presents an accessible yet comprehensive overview.



Networking Basics and Network Security

- Understanding basic networking concepts, such as network topologies and protocols, is foundational for any networking student.
- Network security involves protecting data during transmission and includes measures like firewalls, antivirus software, and intrusion detection systems.

Network Types

- Different network types serve different purposes. LANs (Local Area Networks) are used in small geographical areas like an office, while WANs (Wide Area Networks) cover broader areas, like cities or regions.
- Wireless LANs (WLANs) use radio waves for connectivity, offering mobility and flexibility compared to wired LANs.

Networking Topologies

- Network topology refers to the arrangement of different elements (links, nodes, etc.) in a computer network. Nodes serve as connection points for transmission mediums, transferring signals across the network. Network topologies can be physical or logical, independent of the actual placement of devices. The eight basic types are Point-to-Point, Bus, Star, Ring, Mesh, Tree, Hybrid, and Daisy Chain. - Each topology has its advantages and disadvantages. For example, a star topology is easy to manage but requires more cable than a bus topology.

Proxies

- A proxy server acts as an intermediary between a user's computer and the internet. It can be used for anonymity, caching data, or bypassing content filters.

Types of proxies include: Dedicated Proxy / Forward Proxy, Reverse Proxy, Transparent Proxy, Non-Transparent Proxy

Proxies are employed for security, traffic control, and to bypass network restrictions or monitoring. They play a critical role in corporate network security, penetration testing, and web application protection.

Malware needs to be proxy-aware to effectively bypass network security measures. Different browsers and applications handle proxy settings differently, impacting how malware might interact with them.

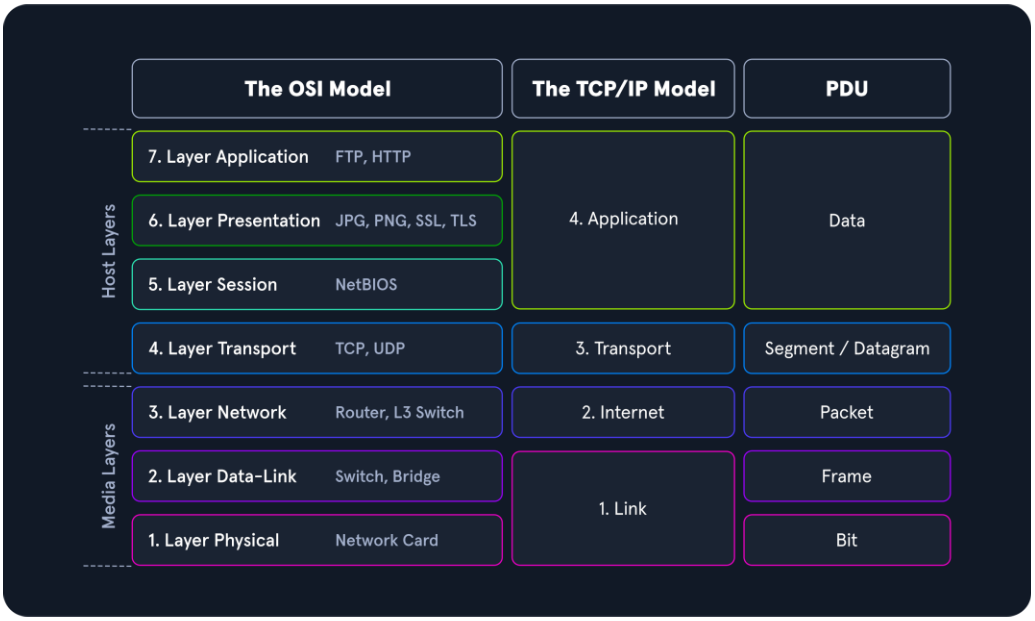
Networking Models

- The OSI model is a conceptual framework used to understand network interactions in seven layers, from physical hardware to application software.

- - The TCP/IP model is more streamlined with four layers and is used to understand internet-based communications.

TCP/IP focuses on internet connectivity, offering more flexibility within its guidelines compared to the OSI model.

OSI serves as a comprehensive reference model, known for its structured approach and strict adherence to protocols.



	The OSI Model		The TCP/IP Model	PDU
Host Layers	7. Layer Application	FTP, HTTP	4. Application	Data
	6. Layer Presentation	JPG, PNG, SSL, TLS		
	5. Layer Session	NetBIOS		
	4. Layer Transport	TCP, UDP	3. Transport	Segment / Datagram
Media Layers	3. Layer Network	Router, L3 Switch	2. Internet	Packet
	2. Layer Data-Link	Switch, Bridge	1. Link	Frame
	1. Layer Physical	Network Card		Bit

The OSI Model

- The OSI (Open Systems Interconnection) Model, developed as the ISO/OSI standard, aims to enable communication between diverse technical systems using various devices and technologies. It ensures compatibility across different network implementations**.**

Layer Functions:

- **Layer 7** - Application: Controls data input/output and provides application functions.
- **Layer 6 -** Presentation: Converts system-dependent data presentation into a format independent of the application**.**
- **Layer 5 -** Session: Manages logical connections between systems and addresses connection issues.
- **Layer 4 -** Transport: Responsible for end-to-end control and management of data transfer, including congestion avoidance and data segmentation**.**
- **Layer 3 -** Network: Establishes connections in circuit-switched networks and forwards packets in packet-switched networks, handling data transmission across the entire network**.**

- **Layer 2 -** Data Link: Ensures reliable, error-free transmission over the medium by organizing bitstreams into blocks or frames.
- **Layer 1** - Physical: Involves the actual transmission techniques (electrical, optical, electromagnetic) over wired or wireless media**.**

The OSI model is crucial for understanding and ensuring the security, reliability, and efficiency of communications in networking. It provides a standardized framework for different network tasks and interactions.

The TCP/IP Model

The TCP/IP model, also known as the Internet Protocol Suite, is a layered reference model primarily used for internet-based communications. It is named after two of its most significant protocols: the Transmission Control Protocol (TCP) and the Internet Protocol (IP).

Layer Structure and Functions:

- **Layer 4 - Application**: Allows applications to access network services and defines protocols for data exchange.
- **Layer 3 - Transport**: Responsible for providing session (TCP) and datagram (UDP) services to the Application Layer.
- **Layer 2 - Internet**: Handles host addressing, packaging, and routing functions.
- **Layer 1 - Link**: Manages the placement and reception of TCP/IP packets on the network medium, working independently of the network access method, frame format, and medium.

TCP/IP is essential for understanding how data is transmitted over the internet, including addressing, routing, and application-level communications. It forms the backbone of modern internet communication and network infrastructure.

Network Layer

The Network Layer, as the third layer of the OSI model, is primarily responsible for the exchange of data packets across a network. It plays a crucial role in managing and directing data from the source to the destination.

Core Responsibilities:

- **Logical Addressing**: Assigns addresses to each data packet to facilitate their routing through the network.
- **Routing**: Determines the best path for data packets to travel from the source to the destination.
- **Flow Control**: Manages the rate of data transmission to prevent network

PROTOCOLS: IPv4/IPv6, IPsec, ICMP, IGMP (Internet Group Management Protocol), RIP (Routing Information Protocol), OSPF (Open Shortest Path First)

IPv4 Addresses

IP addresses are used for identifying hosts within a network. While MAC addresses work within a single network, IP addresses (IPv4 and IPv6) are required for communication across different networks.

Subnetting

Subnetting is dividing a range of IPv4 addresses into smaller groups or subnets. It allows logical segmentation of a network, where each subnet has a unique network address.

Helps in efficient management of IP address space, improving network performance and security. It's like dividing a large building into smaller, manageable departments.

Key Components in Subnetting:

- **Network Address**: Identifies the subnet and is essential for routing within and between subnets.
- **Broadcast Address**: Used for sending messages to all devices in a subnet.
- **First and Last Hosts**: Defines the range of usable IP addresses within a subnet.
- **Number of Hosts**: Total count of assignable addresses in a subnet.

Understanding which octet changes based on the CIDR notation helps in quickly identifying the network's scope.

Using the remainder of the subnet mask's CIDR notation divided by 8 helps in determining the size of each subnet.

Remembering powers of two or dividing 256 by two repeatedly helps in calculating the number of addresses in each subnet.

Questions and answers

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

A /27 subnet mask means that the first 27 bits of the IP address are reserved for the network part. This translates to a subnet mask of **255.255.255.224** in decimal notation.

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

The subnet 10.200.20.0/27 covers addresses from 10.200.20.0 to 10.200.20.31. The broadcast address is always the last address in the subnet, which is **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.**

Splitting a /27 subnet into 4 subnets means adding 2 more bits to the subnet mask (since 2^2 = 4), resulting in a /29 subnet mask. Each /29 subnet has 8 addresses.

The 1st subnet: 10.200.20.0/29 (10.200.20.0 to 10.200.20.7)

The 2nd subnet: 10.200.20.8/29 (10.200.20.8 to 10.200.20.15)

The 3rd subnet: 10.200.20.16/29 (10.200.20.16 to 10.200.20.23)

The network address of the 3rd subnet is **10.200.20.16.**

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

From the previous calculation, the 2nd subnet ranges from 10.200.20.8 to 10.200.20.15. The broadcast address for this subnet (10.200.20.8/29) is **10.200.20.15**.

MAC Addresses

MAC (Media Access Control) addresses are unique 48-bit (6 octets) identifiers for network interfaces, represented in hexadecimal format. They are essential for the physical addressing of devices in a network.

MAC addresses are used across various technologies, including Ethernet (IEEE 802.3), Bluetooth (IEEE 802.15), and WLAN (IEEE 802.11).

MAC addresses facilitate data delivery at Layer 2 (Data Link Layer) to either a physical address within the same subnet or to a router for different subnets.

ARP maps IP addresses to MAC addresses, enabling communication within a LAN. It uses broadcast messages to resolve a device's MAC address based on its IP address.

MAC addresses can be spoofed or manipulated, posing security risks such as MAC spoofing or ARP spoofing attacks.

Network security measures, including firewalls and secure protocols, are essential to mitigate these risks.

IPv6 Addresses

IPv6 is the successor to IPv4, designed to address the limitations of the IPv4 protocol, primarily the shortage of available IP addresses. It uses 128-bit addresses, significantly expanding the address space.

Networking Key Terminology

1. **WEP (Wired Equivalent Privacy):**
    - An outdated security protocol for wireless networks.
2. **SSH (Secure Shell):**
    - A secure protocol for remote system access and command execution**.**
3. **FTP (File Transfer Protocol):**
    - Used for transferring files between systems**.**
4. **SMTP (Simple Mail Transfer Protocol):**
    - Protocol for sending and receiving emails.
5. **HTTP (Hypertext Transfer Protocol):**
    - Client-server protocol for data transfer over the internet.
6. **SMB (Server Message Block):**
    - Protocol for sharing files, printers, and other resources in a network.
7. **NFS (Network File System):**
    - **Protocol for accessing files over a network.**
8. **SNMP (Simple Network Management Protocol):**
    - Manages network devices.
9. **WPA (Wi-Fi Protected Access):**
    - A security protocol for wireless networks.
10. **TKIP (Temporal Key Integrity Protocol):**
    - A less secure wireless network security protocol.
11. **NTP (Network Time Protocol):**
    - Synchronizes the timing of computers on a network.
12. **VLAN (Virtual Local Area Network):**
    - Segments a network into multiple logical networks.
13. **VTP (VLAN Trunking Protocol):**
    - Layer 2 protocol for managing VLANs across multiple switches**.**
14. **RIP (Routing Information Protocol):**
    - A distance-vector routing protocol for LANs/WANs**.**
15. **OSPF (Open Shortest Path First):**
    - Interior gateway protocol for routing within a single Autonomous System.
16. **IGRP (Interior Gateway Routing Protocol):**
    - Cisco proprietary protocol for routing within autonomous systems**.**
17. **EIGRP (Enhanced Interior Gateway Routing Protocol):**
    - Advanced distance-vector routing protocol for IP traffic routing**.**
18. **PGP (Pretty Good Privacy):**
    - Encryption program for securing emails, files, and data.
19. **NNTP (Network News Transfer Protocol):**
    - Protocol for distributing messages in newsgroups.
20. **CDP (Cisco Discovery Protocol):**

- **Proprietary protocol for managing Cisco devices.**
- Cisco proprietary wireless authentication protocol.

Common Protocols

1. **TCP (Transmission Control Protocol):**
    - A reliable, connection-oriented protocol ensuring data integrity and delivery.
2. **UDP (User Datagram Protocol):**
    - A connectionless protocol, faster than TCP but less reliable.
3. **Telnet:**
    - A remote login service using unencrypted text communication.
4. **SSH (Secure Shell):**
    - Secure protocol for remote login and command execution.
5. **SNMP (Simple Network Management Protocol):**
    - Manages network devices, typically on port 161-162.
6. **HTTP/HTTPS (Hypertext Transfer Protocol/Secure):**
    - Protocol for transferring web pages; HTTPS adds encryption.
7. **DNS (Domain Name System):**
    - Resolves domain names to IP addresses, typically on port 53.
8. **FTP/TFTP (File Transfer Protocol/Trivial File Transfer Protocol):**
    - FTP (port 20-21) and TFTP (port 69) are used for file transfer.
9. **NTP (Network Time Protocol):**
    - Synchronizes clocks of networked devices.
10. **SMTP/POP3/IMAP (Simple Mail Transfer Protocol/Post Office Protocol/Internet Message Access Protocol):**
    - Protocols for email transfer and retrieval.

Wireless Networks

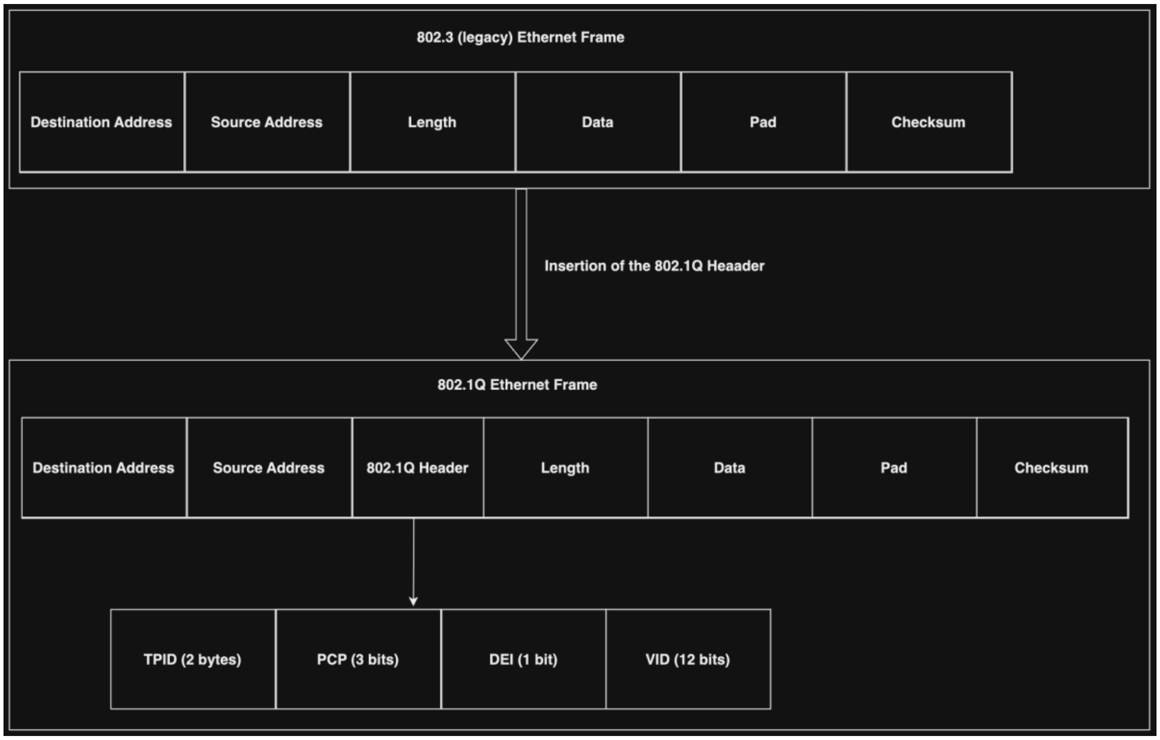
Wireless networks use wireless data connections between network nodes, allowing devices like laptops, smartphones, and tablets to communicate without physical cables.

They utilize radio frequency (RF) technology, with devices equipped with wireless adapters to send and receive RF signals.

Virtual Private Networks

VPNs create secure, encrypted connections over the internet, allowing remote access to private networks. They enable remote management of servers and provide employees access to internal services from outside the local network

VPNs use encryption and authentication to secure data transmission. The remote user connects to a VPN server, which then grants access to the private network. This connection is encrypted, making it secure against eavesdropping.



Components and Requirements of a VPN:

VPN Client: Installed on the remote device to establish a connection.

VPN Server: Accepts connections and routes traffic between the VPN client and the network.

Encryption: Secures the connection using algorithms like AES and protocols like IPsec.

Authentication: Ensures that the client and server can trust each other, using shared secrets or certificates.

Security and Limitations:

While VPNs provide security for data transmission, they depend on the strength of the chosen protocols and encryption methods. Newer protocols like OpenVPN and WireGuard offer more security and efficiency compared to older ones like PPTP.

Cisco Networking and VLANs

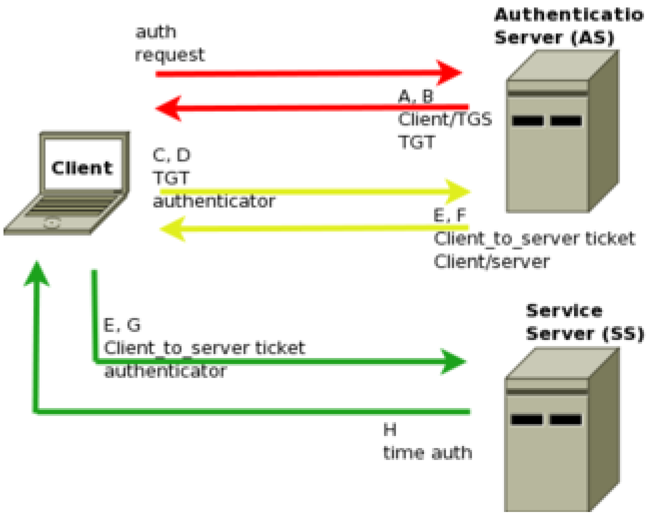
- Cisco is a leading manufacturer of networking equipment. Cisco IOS is their software used on routers and switches, known for its robustness and features.
- VLANs (Virtual Local Area Networks) in Cisco networks help in logically dividing a network into different segments for improved management and security.

Key Exchange Mechanisms

- Key exchange mechanisms are crucial for secure communication. They enable the sharing of cryptographic keys over an insecure channel.
- Popular key exchange algorithms include Diffie-Hellman, RSA, and ECDH (Elliptic Curve Diffie-Hellman), each with its strengths and use cases.

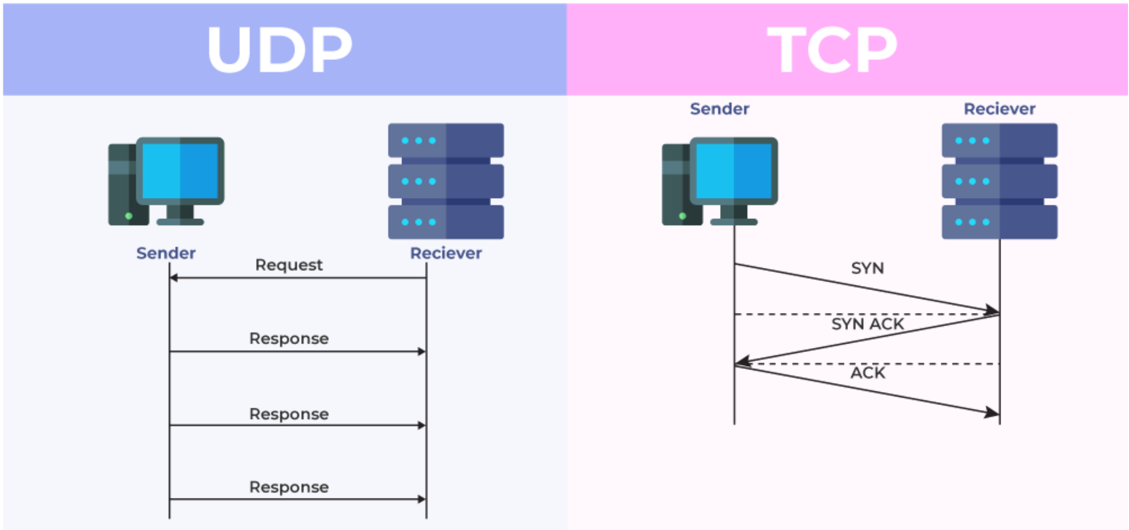
Authentication Protocols

- Authentication protocols verify the identity of users and devices in a network. Protocols like Kerberos, SSL/TLS, and OAuth are fundamental for secure network access.
- Each protocol has its specific use case, like OAuth for web authorization and SSL/TLS for secure web browsing.



TCP/UDP Connections and IP Packets

- TCP (Transmission Control Protocol) is a reliable protocol ensuring ordered and error-free transmission of data. It's essential for applications where data integrity is crucial, like file transfers.
- UDP (User Datagram Protocol) is faster but less reliable than TCP. It’s used in applications like video streaming where speed is more important than perfect accuracy.
- IP packets are the basic units of data transmitted over the internet. They contain both the data being sent and the necessary routing information.

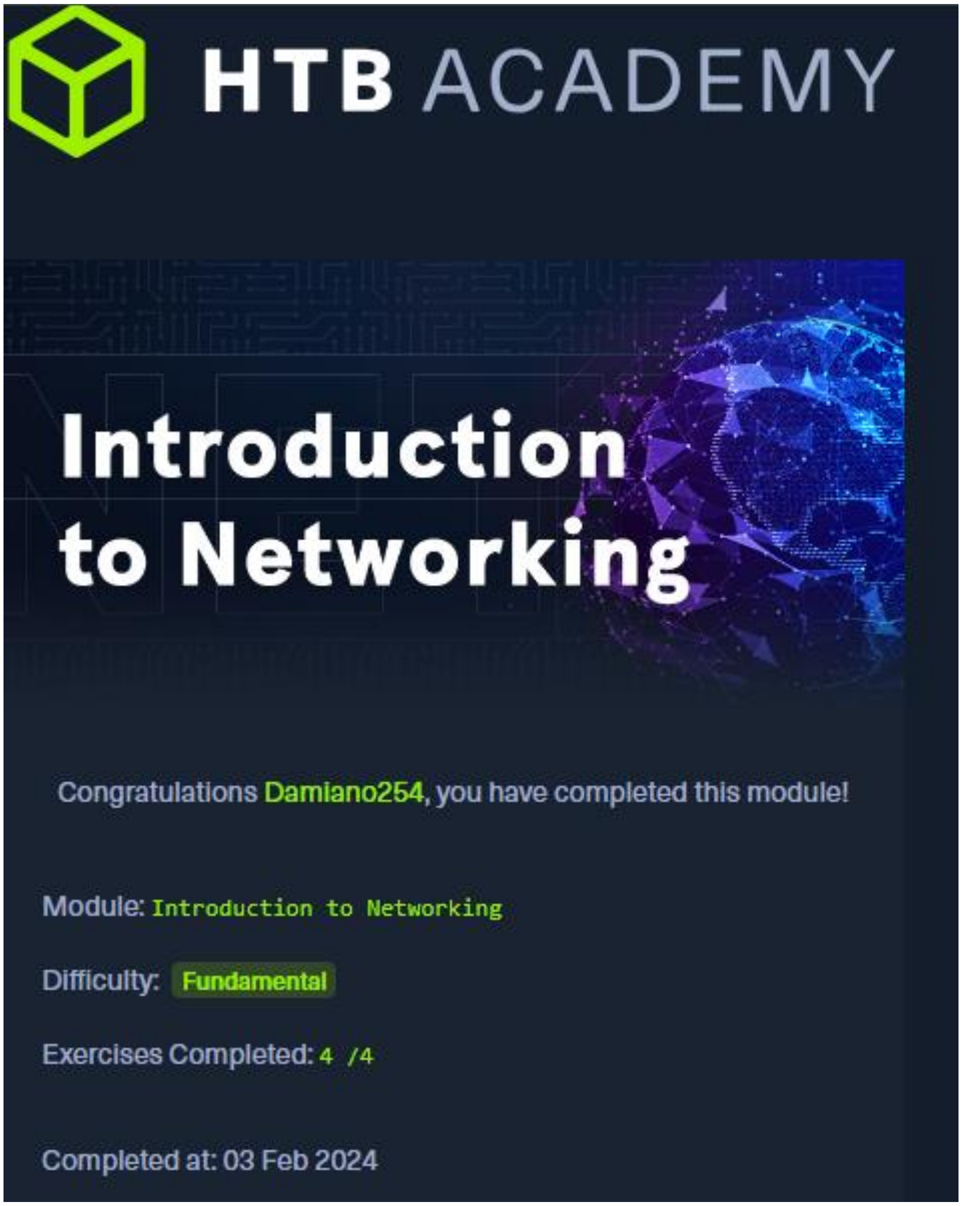


Cryptography in Networking

- Cryptography is vital for securing data transmitted over networks. It involves techniques like encryption to convert data into a secure format.
- Encryption uses algorithms, like AES and DES, to transform readable data (plaintext) into an unreadable format (ciphertext).
- Symmetric encryption uses the same key for both encryption and decryption, while asymmetric encryption uses a public key for encryption and a private key for decryption.
- Cipher modes, like CBC and GCM, define how blocks of data are encrypted, ensuring data security and integrity.

Conclusion

In conclusion, networking is a vast and dynamic field that is fundamental to the modern digital world. Understanding these key concepts and protocols is crucial for anyone looking to delve deeper into the field of networking or seeking to enhance their technical skill set. This guide serves as a starting point for further exploration and learning in the ever-evolving landscape of network technologies.



HTB ACADEMY

Introduction to Networking

Congratulations Damiano254, you have completed this module!

Module: Introduction to Networking

Difficulty: Fundamental

Exercises Completed: 4 /4

Completed at: 03 Feb 2024