Assignment on Networking Fundamentals

Submitted by:

Name: Nobojit Majumder
Contact: 01997041499
Course: 100 Days Cyber Security Bootcamp
Submission Date: 7 November 2025

1. TCP/IP Model

The TCP/IP model (Transmission Control Protocol/Internet Protocol) is the foundation of modern computer networking. It defines how data should be transmitted over a network and ensures reliable communication between devices. The model is divided into four layers, each responsible for specific functions.

- Application Layer:
  This layer provides services directly to users or applications. Protocols like HTTP, FTP, SMTP, and DNS work here. For example, when you browse a website, HTTP operates at this layer to request and deliver web pages.

- Transport Layer:
  The transport layer handles end-to-end communication between devices. It ensures data is delivered accurately and in order. The two main protocols are TCP (connection-oriented, reliable) and UDP (connectionless, faster but less reliable).

- Internet Layer:
  This layer determines the best path for data packets to travel through the network. The IP (Internet Protocol) operates here, assigning unique IP addresses to devices. It also includes ICMP for error handling and diagnostics (like when you use the ping command).

- Network Access Layer:
  Also known as the Link Layer, it manages how data is physically sent through network hardware such as Ethernet or Wi-Fi. It handles MAC addresses, framing, and error detection.

In short, TCP/IP allows computers worldwide to communicate efficiently — from browsing a website to sending an email.

2. OSI Seven Layer Model

The OSI (Open Systems Interconnection) model is a theoretical framework developed by ISO to standardize how network systems communicate. It divides the process into seven layers, each performing a unique role.

1. **Physical Layer:** Handles the physical transmission of data through cables, switches, or wireless signals.

2. **Data Link Layer:** Ensures error-free transfer between directly connected devices using MAC addresses.

3. **Network Layer:** Determines the routing and addressing of data packets.

4. **Transport Layer:** Provides reliable data delivery through segmentation, acknowledgment, and error control.

5. **Session Layer:** Manages sessions or connections between applications.

6. **Presentation Layer:** Translates, encrypts, or compresses data for the application layer.

7. **Application Layer:** The user-facing layer, enabling services like email, web browsing, and file transfer.

Difference between OSI and TCP/IP:

- OSI has **7 layers**, while TCP/IP has **4**.

- OSI is a **theoretical reference model**, TCP/IP is **practical and implemented**.

- OSI separates presentation and session layers; TCP/IP merges them into the application layer.

The OSI model helps students and engineers understand networking systematically, while TCP/IP powers the actual internet.

3. IP Address

An **IP address** (Internet Protocol address) identifies a device on a network. It acts like a digital address, allowing data to find its correct destination.

There are **two main versions**:

1. **IPv4 (Internet Protocol version 4):**

- Uses **32-bit** addresses (e.g., 192.168.1.1).
- Supports around 4.3 billion unique addresses.
- Example: 192.168.0.10

1. **IPv6 (Internet Protocol version 6):**

- Uses **128-bit** addresses (e.g., 2400:cb00:2048:1::c629:d7a2).
- Provides a much larger address space.
- Designed to overcome IPv4 exhaustion.
- Supports better security and efficiency.

Feature	IPv4	IPv6
Address	32-bit	128-bit
Total Address	Dotted Decimal	Hexadecimal
Format	~4.3 billion	Almost unlimited
Security	Optional (IPSec)	Mandatory (IPSec built-in)

4. Subnet Mask

A **Subnet Mask** is used to divide an IP address into **network** and **host** portions. It helps identify which part of the IP belongs to the network and which identifies a specific device.

For example:

- IP: 192.168.1.10
- Subnet Mask: 255.255.255.0

Here, the first three octets (192.168.1) represent the **network**, and the last octet (.10) represents the **host**.

Subnetting is the process of breaking a large network into smaller sub-networks to improve efficiency and security. It reduces congestion and allows better management of IP addresses.

For example, a Class C network (255.255.255.0) can be subnetted into four smaller subnets using the mask 255.255.255.192.

5. Public and Private IP Addresses

Public IP Address:
These are globally unique IPs assigned by ISPs. They can be accessed over the internet.

- Example: 8.8.8.8 (Google DNS)
- Used for: Servers, websites, routers connected to the internet.

Private IP Address:
Used inside local networks and cannot be accessed directly from the internet.

- Examples: 192.168.x.x, 10.x.x.x, 172.16.x.x – 172.31.x.x
- Used for: Home networks, offices, schools.

Main Differences:

Type	Access	Example	Assigned By
Public	Internet-wide	8.8.8.8	ISP
Private	Local network only	192.168.1.1	Network Admin

In simple terms, public IPs face the world; private IPs stay inside your walls.

6. Networking Protocols

Networking protocols are the rules that define how data is transmitted, received, and interpreted across networks. Here are some key ones:

- **HTTP (Hypertext Transfer Protocol):** The foundation of web communication. It transfers web pages from servers to browsers.
- **HTTPS (HTTP Secure):** An encrypted version of HTTP using SSL/TLS, ensuring data privacy and security.
- **FTP (File Transfer Protocol):** Used to transfer files between computers over a network.
- **DNS (Domain Name System):** Converts domain names (like google.com) into IP addresses.
- **SMTP (Simple Mail Transfer Protocol):** Handles the sending of emails.
- **TCP (Transmission Control Protocol):** Ensures reliable data delivery by establishing a connection before transmitting.
- **UDP (User Datagram Protocol):** Sends data faster but without error checking — often used in streaming or gaming.

These protocols keep the internet running smoothly — every click, email, and video depends on them working together.

Conclusion

Networking is the backbone of cyber security. Understanding models like TCP/IP and OSI, IP addressing, subnetting, and communication protocols builds the foundation for securing systems and preventing cyber threats. Without mastering these basics, no advanced cybersecurity concept can stand strong.