What is Networking?

Networking is like building roads that connect houses (computers) so they can send messages (data) to each other. Imagine two friends living in different neighborhoods want to send letters. They need a system of streets, addresses, and rules for how to send and receive mail. That's what a network does for computers.

How Networks are Built

Networks can be built in different **shapes (topologies)**:

- **Star:** Like a mall where all shops are connected to a central hall.
- **Mesh:** Like a spiderweb where every point connects to others.
- **Tree:** Like branches of a tree with one main trunk and smaller branches.

They also use different **tools to connect (mediums):**

- **Ethernet cables:** Like roads.
- **Fiber optics:** Like high-speed highways.
- **Wireless (Wi-Fi):** Like sending letters using drones.

And they follow different **rules (protocols):**

- **TCP:** Like making sure a package is delivered safely and signed for.
- **UDP:** Like shouting a message without caring if someone heard it.

Why Security in Networking Matters

Think of your network as your house:

- A **flat network** is like living in a house with just one lock on the door. It's easy for someone to break in and roam around without restrictions.
- A **segmented network** is like having separate rooms with locks, alarms, and cameras. Even if someone gets in, they can't access everything.

Examples for Better Security

1. **Access Control Lists (ACLs):**

   Imagine putting a **fence** around your yard with gates for entry and exit. If someone tries to jump over the fence, it's suspicious and easier to notice.

   - Example: Why is the printer talking to the server over HTTP (an unsecure method)?

2. **Documentation and Monitoring:**

   Think of **putting lights** around your yard to see what's happening.

   - Example: Why is the printer talking to the internet at all?

3. **Intrusion Detection Systems:**

   Like having **bushes** near your windows. They make it harder for someone to sneak in and easier to detect unusual activity.

   - Example: Why did a port scan come from the printer network?

Common Mistakes

Many people make their networks too simple and **flat** (one big space with no divisions). This is like letting every visitor in your house go to any room without checking where they belong.

For example:

- You give your printer an address (IP) on a flat network. Now the printer can talk to your servers, computers, and even the internet without restriction. That's risky!

Story Time: A Pentester's Mistake

A penetration tester (like a burglar hired to test your locks) made this mistake:

- The company had split its network into two halves:
  - One for servers: **10.20.0.1–10.20.0.126**
  - One for client devices: **10.20.0.129–10.20.0.254**

The tester's computer was set to **talk to everyone** (flat network) but could only communicate with client devices. They missed the fact that the **servers** were on a different "room" (network segment).

How the Internet Works (Simple Analogy)

- **Your home network (Wi-Fi):** Like your house with its own mailbox (router).
- **The internet:** Like a massive delivery system with post offices (ISPs) everywhere.
- **Sending a request:**
  - When you type a website like "www.hackthebox.eu," it's like writing a letter with an address.
  - Your router sends the letter to the ISP, which finds the actual "geographical" address (IP address).
  - The website responds, and the packet (data) is delivered back to you.

Making Networks More Secure

1. **Separate Networks (Segmentation):**

   Divide devices into smaller networks based on their purpose:

   - **Web servers in a DMZ (Demilitarized Zone):** Like keeping visitors in a guest room instead of the living room.
   - **Workstations isolated:** Prevents employees' computers from talking to each other unnecessarily.

2. **Admin Network:**

   Protect routers and switches by keeping them on their own private network.

   - Example: This stops hackers from sending fake instructions (man-in-the-middle attacks).

3. **Dedicated Networks for Phones/Printers:**

   - Phones need special treatment to avoid delays (like giving ambulances priority on roads).
   - Printers are hard to secure and can be used to steal passwords. Keep them on their own network.

Takeaway

Think of your network as a neighborhood:

- A flat network is like having one giant open field with no fences or walls—risky!

- A segmented network is like having houses, fences, and security cameras. Each part has its purpose, making it harder for intruders to roam freely.

When you design or manage a network, always think about:

- Who should talk to whom?
- How can you make it hard for attackers to move around?
- What tools can help detect suspicious activity?

Networking connects devices so they can talk to each other, like roads connecting towns or neighborhoods. Depending on how far the network stretches or how it is set up, we give them different names.

There are two main categories to know:

- **Common Terms:** These are practical terms you'll hear often.
- **Book Terms:** These are terms that are good to know for exams or rare cases.

Common Terminology

Network Type	Definition
Wide Area Network (WAN)	The Internet or any large network that connects smaller networks together. Example: Government networks.
Local Area Network (LAN)	A small network, like your home or office network.
Wireless Local Area Network (WLAN)	A LAN that works over Wi-Fi instead of cables. Example: Your home Wi-Fi.
Virtual Private Network (VPN)	A secure tunnel to connect devices or networks over the internet. Example: Remote work networks.

Breakdown of Common Terms

WAN (Wide Area Network)

A WAN connects multiple LANs together. The Internet is the most common example of a WAN.

- **Think of it as:** Highways connecting different cities (LANs).
- **Example:** Your home network is connected to the Internet (WAN) through your Internet Service Provider (ISP).
- **Other WANs:** Large companies and governments often have private WANs (e.g., Intranets).

LAN/WLAN (Local Area Network/Wireless Local Area Network)

A LAN connects devices within a small area, like your home or office. If it's wireless, it's called a WLAN.

- **Think of it as:** Streets in your neighborhood.
- **Example:** Your laptop, phone, and smart TV all connected to your Wi-Fi.
- **Key Fact:** LANs typically use private IP addresses like 192.168.x.x or 10.x.x.x, which cannot be accessed directly from the Internet.

VPN (Virtual Private Network)

A VPN creates a secure connection between devices or networks over the Internet. It makes you feel like you're connected to a private network even if you're far away.

- **Think of it as:** A secret tunnel between two places.
- **Types of VPNs:**
  1. **Site-to-Site VPN:** Connects two networks, like linking two offices in different cities.
     - **Example:** Two company branches in New York and London sharing files securely.
  2. **Remote Access VPN:** Lets individual devices connect to a network.
     - **Example:** Hack The Box's VPN lets you connect to its labs from anywhere.
  3. **SSL VPN:** Works in your browser, streaming applications or desktops securely.
     - **Example:** Hack The Box Pwnbox.
- **Split-Tunnel VPNs:** Only some traffic goes through the VPN (like Hack The Box labs), while the rest uses your regular Internet.
- **Full-Tunnel VPNs:** All your traffic goes through the VPN, which is better for security.

Book Terms

Network Type	Definition
Global Area Network (GAN)	A worldwide network. Example: The Internet or private networks of global companies.
Metropolitan Area Network (MAN)	Connects multiple LANs in a city or region. Example: A city's government network.
Personal Area Network (PAN)	A very small network for personal devices. Example: Your phone connected to your smartwatch.
Wireless Personal Area Network (WPAN)	A wireless version of a PAN. Example: Devices connected via Bluetooth.

Breakdown of Book Terms

GAN (Global Area Network)

A GAN connects devices and networks globally.

- **Think of it as:** The entire world connected by undersea cables, satellites, and data centers.
- **Example:** The Internet or a global company's private network.

MAN (Metropolitan Area Network)

A MAN connects multiple LANs in a city or region.

- **Think of it as:** Express trains connecting stations (LANs) in a city.
- **Example:** A city government's network connecting schools, libraries, and offices.

PAN/WPAN (Personal Area Network/Wireless Personal Area Network)

A PAN connects devices around one person, like a phone and smartwatch. A WPAN is the wireless version, often using Bluetooth.

- **Think of it as:** A tiny bubble around you for your devices.
- **Example:** Your wireless headphones connected to your phone via Bluetooth.

Real-Life Example: Smart Homes with IoT

In smart homes, WPANs are used to connect low-power devices like smart bulbs, thermostats, and doorbells. They use protocols like ZigBee or Z-Wave to communicate with each other.

- **Think of it as:** A mini-network in your house for controlling devices.
- **Example:** Turning off the lights or locking the door from your phone.

Conclusion

Networking comes in all shapes and sizes, from small personal networks (PAN) to global ones (GAN). Here's the summary:

- WAN = Internet or large networks connecting LANs.
- LAN/WLAN = Small networks at home or office (wired or wireless).
- VPN = Secure tunnels to connect devices or networks.
- GAN/MAN = Large-scale networks for cities or globally.
- PAN/WPAN = Tiny networks for personal devices like Bluetooth headphones.

Each type serves a different purpose, but together, they make up the world of networking!

What is Network Topology?

Network topology describes how devices (like computers and routers) are connected and interact within a network. It can be **physical** (how devices are physically linked with cables or wireless signals) or **logical** (how data flows across the network).

Think of it as:

- **Physical topology:** The map of roads connecting cities.
- **Logical topology:** The rules for how traffic moves on those roads.

Key Parts of Network Topology

Network topology has three main aspects:

1. **Connections**
2. **Nodes (Devices)**
3. **Classifications (Types)**

---

1. Connections

This describes the method used to link devices in a network.

Wired Connections	Wireless Connections
Coaxial cabling	Wi-Fi
Glass fiber cabling	Cellular (4G, 5G)
Twisted-pair cabling (Ethernet)	Satellite

Example:

- A wired Ethernet connection at home uses twisted-pair cables.
- Wi-Fi or cellular networks are wireless connections.

---

2. Nodes (Devices)

Nodes are the points where devices connect to the network. They send, receive, or forward data.

Examples of Network Nodes	Functions
Repeaters	Boost weak signals to travel longer distances.
Hubs	Broadcast data to all devices in a network.
Switches	Direct data to the correct device.
Routers/Modems	Manage traffic between different networks.
Gateways	Connect different network types.
Firewalls	Protect networks from unauthorized access.

Example:

- Your router at home is a node that connects your devices to the Internet.
- A switch in an office connects many computers in a LAN.

---

3. Classifications (Types of Topology)

Network topology can be physical (how devices are connected) or logical (how data flows).

Here are the **8 basic types** of topologies:

Type	Description
Point-to-Point	Direct connection between two devices.
Bus	All devices share a single cable.
Star	All devices connect to a central hub, switch, or router.
Ring	Devices are connected in a circle; data flows in one direction.
Mesh	Devices connect directly to multiple others; can be fully or partially connected.
Tree	Like a hierarchical structure; combines multiple star topologies.
Hybrid	Mix of different topologies (e.g., star and bus).
Daisy Chain	Devices are connected one after another in a line.

Detailed Explanation of Topologies

1. Point-to-Point Topology

- **What it is:** A simple connection between two devices.
- **Think of it as:** A direct phone line between two people.
- **Example:** A computer connected directly to a printer.

---

2. Bus Topology

- **What it is:** All devices share the same cable. Data travels along this single path.
- **Think of it as:** A shared microphone where only one person can talk at a time.
- **Example:** Early Ethernet networks using coaxial cables.

---

3. Star Topology

- **What it is:** All devices connect to a central device (like a switch or router).
- **Think of it as:** A wheel with spokes connecting to a central hub.
- **Example:** Most home networks where all devices connect to a Wi-Fi router.
- **Advantage:** Easy to add or remove devices.

- **Disadvantage:** If the central device fails, the network stops working.

---

4. Ring Topology

- **What it is:** Devices are connected in a circle, and data travels in one direction.
- **Think of it as:** A relay race where the baton (data) passes around in a loop.
- **Example:** Token Ring networks used in the past.
- **Advantage:** Easy to predict data flow.
- **Disadvantage:** If one connection breaks, the entire network fails.

---

5. Mesh Topology

- **What it is:** Devices connect to multiple others for redundancy. Can be fully connected (every device links to every other) or partially connected.
- **Think of it as:** A web where multiple paths exist between points.
- **Example:** The Internet or a WAN with backup links.
- **Advantage:** High reliability; if one connection fails, data can take another path.
- **Disadvantage:** Complex and expensive to set up.

---

6. Tree Topology

- **What it is:** Combines multiple star networks into a hierarchical structure.
- **Think of it as:** A family tree with branches.
- **Example:** A company network where departments are star networks connected to a central backbone.
- **Advantage:** Scalable for large networks.
- **Disadvantage:** A single failure in the backbone can affect the entire network.

---

7. Hybrid Topology

- **What it is:** A mix of two or more topologies.
- **Think of it as:** Combining different building blocks into one system.
- **Example:** A tree topology connecting star networks over a bus.
- **Advantage:** Flexible to meet specific needs.
- **Disadvantage:** Can be complex and expensive to manage.

---

8. Daisy Chain Topology

- **What it is:** Devices are linked in a straight line.
- **Think of it as:** Christmas lights, where one bulb connects to the next.
- **Example:** Automation networks like CAN in manufacturing.
- **Advantage:** Simple to set up for small networks.
- **Disadvantage:** If one device fails, it can disrupt the entire chain.

Conclusion

Network topologies determine how devices are connected and communicate. Here's a quick summary:

- **Point-to-Point:** Simple and direct.
- **Bus:** Shared single cable; easy but outdated.
- **Star:** Common for home and office networks.
- **Ring:** Sequential but prone to failure.
- **Mesh:** Reliable with multiple paths but costly.
- **Tree:** Hierarchical for large setups.
- **Hybrid:** Flexible for complex needs.
- **Daisy Chain:** Linear connections, simple but fragile.

Choosing the right topology depends on the size, purpose, and budget of your network.

What is a Proxy? (Simplified Version)

A **proxy** is like a middleman that sits between two parties—like you and the internet. Its job is to pass messages back and forth while possibly inspecting, filtering, or changing them along the way.

Think of it as a receptionist in an office. You tell the receptionist what you need, and they communicate your request to the right department. Similarly, a proxy handles your request to access something online and decides how to process it.

Different Types of Proxies (with Real-Life Examples)

1. Forward Proxy

- **What it does**: Acts on behalf of the user (you) to connect to something online.
- **Example**: You want to visit a website, but you're on a school or work network that uses a proxy. The proxy fetches the website for you but might block certain sites based on rules, like banning social media.
- **Analogy**: Imagine sending a letter to someone. Instead of mailing it directly, you give it to a friend who mails it for you.
- **Real-Life Use Case**:
  - Companies use forward proxies to prevent employees from accessing harmful or unproductive websites.
  - Tools like **Burp Suite** act as a forward proxy to help cybersecurity professionals test websites by intercepting and analyzing web traffic.

---

2. Reverse Proxy

- **What it does**: Acts on behalf of the service (like a website or server) to protect it or manage traffic.
- **Example**: When you visit a popular site like Amazon, you’re not connecting directly to Amazon’s servers. Instead, a **reverse proxy** (like Cloudflare) handles your request, checks for security threats, and forwards it to Amazon’s server if it’s safe.
- **Analogy**: Imagine calling a famous celebrity’s office. You don’t speak directly to them; their assistant answers and forwards your message to the celebrity if appropriate.
- **Real-Life Use Case**:

- Organizations use **Cloudflare** as a reverse proxy to block malicious traffic (e.g., bots or hackers) and handle Distributed Denial of Service (DDoS) attacks.

---

3. Transparent Proxy

- **What it does**: Works without you knowing it's there. It doesn't require special settings on your device.
- **Example**: When you use free Wi-Fi at a coffee shop, a **transparent proxy** might filter or monitor the sites you visit to block inappropriate content.
- **Analogy**: It's like a security guard at a mall quietly observing shoppers to ensure they're following the rules.
- **Real-Life Use Case**:
  - Hotels and schools often use transparent proxies to enforce their internet usage policies.

---

4. Non-Transparent Proxy

- **What it does**: Requires you to configure your device or software to use it.
- **Example**: If your office network requires you to set up proxy settings in your browser to access the internet, that's a **non-transparent proxy**.
- **Analogy**: This is like having to knock on a specific door and announce yourself before entering a building.
- **Real-Life Use Case**:
  - Developers configure non-transparent proxies to debug network traffic or simulate different internet conditions.

Common Misconceptions About Proxies

1. **"Proxies = VPNs"**
   - A **VPN** changes your location and encrypts your data but doesn't act as a mediator for inspecting traffic. Most people confuse the two because both can hide your IP address.
2. **"Proxies are only for hackers or illegal activities"**
   - While hackers use proxies to hide their identity, proxies are widely used for legal purposes, like speeding up website performance or improving network security.

Everyday Examples to Understand Proxies Better

- **Netflix**:
  - If Netflix isn't available in your country, you might think a "proxy" lets you watch shows from another country. Technically, that's usually a VPN, not a proxy, but the idea of rerouting your connection applies to both.
- **School Networks**:
  - When a school blocks YouTube, it's likely using a forward proxy to filter web traffic.
- **Customer Support Call Centers**:
  - If you call a support hotline, the person who answers is like a reverse proxy—they listen to your request and forward it to the right department.

The Key Idea

A proxy sits in the middle of your connection to do something useful—filter, inspect, or protect. Whether it’s helping you access a website, securing a server, or monitoring your network, it’s like a middleman that makes communication smoother (or safer) depending on its type.

Understanding the OSI and TCP/IP Models in Simple Terms

The OSI (Open Systems Interconnection) and TCP/IP (Transmission Control Protocol/Internet Protocol) models describe how data moves from one computer to another. They break the communication process into **layers**, with each layer responsible for specific tasks. Think of them like a factory assembly line: each station (layer) has its job to ensure the product (data) reaches its destination in perfect condition.

The OSI Model: 7 Layers of Communication

The OSI model divides the process into **seven layers**, from the physical transfer of data (electric signals, light, etc.) to the meaningful messages humans understand. Here's a simple breakdown:

1. **Physical Layer**
   - **What it does**: Transfers raw bits (0s and 1s) over cables, Wi-Fi, or other media.
   - **Example**: The actual Ethernet cable or Wi-Fi signal you use.
   - **Analogy**: It's like the roads and vehicles used to deliver goods.
2. **Data Link Layer**
   - **What it does**: Organizes raw data into frames for transmission and ensures error-free delivery.
   - **Example**: A switch or MAC address managing your connection.
   - **Analogy**: Think of this as traffic rules ensuring cars (data) don’t crash.
3. **Network Layer**
   - **What it does**: Handles addressing and routing so data knows where to go.
   - **Example**: An IP address directing packets to the right device.
   - **Analogy**: It’s like GPS guiding a car to its destination.
4. **Transport Layer**
   - **What it does**: Manages data delivery, ensuring it’s complete and in order.
   - **Example**: TCP and UDP protocols controlling the flow.
   - **Analogy**: This is like packaging goods in boxes to ensure nothing gets lost.
5. **Session Layer**
   - **What it does**: Manages and maintains connections between devices.
   - **Example**: Logging into a website and staying connected.
   - **Analogy**: Think of this as scheduling a meeting room for a conversation.
6. **Presentation Layer**
   - **What it does**: Translates data formats so devices understand each other.
   - **Example**: Converting video formats or encrypting data.
   - **Analogy**: This is like translating languages for two people to communicate.
7. **Application Layer**
   - **What it does**: Where humans interact with the network.
   - **Example**: Web browsers (HTTP), email (SMTP), or file transfers (FTP).

- **Analogy**: This is like the customer receiving their package.

The TCP/IP Model: 4 Simplified Layers

The TCP/IP model is a **practical approach** used on the Internet today. It combines some OSI layers to simplify the process. It's like a shortcut map:

1. **Network Interface** (Similar to OSI's Physical + Data Link Layers)
   - Handles physical connections and data framing.
   - Example: Ethernet or Wi-Fi protocols.
2. **Internet** (Similar to OSI's Network Layer)
   - Manages IP addresses and routing data.
   - Example: IPv4, IPv6.
   - Analogy: Ensures the package gets to the correct address.
3. **Transport** (Same as OSI's Transport Layer)
   - Ensures data delivery and order.
   - Example: TCP (reliable) or UDP (fast but less reliable).
4. **Application** (Combines OSI's Application, Presentation, and Session Layers)
   - Where humans interact with the network services.
   - Example: HTTP, FTP, DNS.

How Data Travels (Encapsulation and Decapsulation)

When data moves from your computer to another device:

1. It starts at the **Application Layer**, where you send a message (e.g., a web request).
2. As the message moves down the layers, each adds its own **header** (extra information) to guide it, like adding labels to a package. This is called **encapsulation**.
3. At the receiving device, the process reverses. Each layer reads and removes its header, like unwrapping a gift, in a process called **decapsulation**.

Real-Life Analogy: Ordering a Pizza

Let's compare this process to ordering a pizza:

1. **Application Layer**: You place an order with the pizza shop (e.g., by calling or using an app).
2. **Transport Layer**: The shop confirms your order and prepares the pizza, ensuring it's complete.
3. **Network Layer**: The delivery driver gets your address and plans the route.
4. **Data Link Layer**: The driver follows the traffic rules to reach your house.
5. **Physical Layer**: The pizza is handed to you.

Why Both Models Matter to Penetration Testers

- **TCP/IP Model**: Gives a high-level overview of how devices communicate. Useful for quickly understanding network setups and spotting weak points.
- **OSI Model**: Allows for detailed analysis of each step, helping to identify specific vulnerabilities, like issues in encryption or routing.

For example:

- A penetration tester might capture network traffic using tools like Wireshark. The OSI model helps them dissect the data, layer by layer, to identify problems like unencrypted passwords (Application Layer issue) or incorrect routing (Network Layer issue).

By understanding these models, penetration testers can better secure networks or find vulnerabilities to exploit during tests.

Understanding the OSI Model in Simple Terms

The **OSI Model (Open Systems Interconnection)** is a framework that explains how data travels between two systems, step by step. It organizes the communication process into **seven layers**, each with a specific job. Think of it as a relay race where each layer hands off the baton (data) to the next layer, ensuring the message reaches its destination safely and reliably.

The 7 Layers of the OSI Model with Real-Life Examples

1. **Application Layer (Layer 7)**
   - **What it does**: Interfaces directly with the user or application. It handles the input and output of data.
   - **Example**: When you open a browser and type a URL, this layer handles your request. Protocols like HTTP (web browsing) and SMTP (email) operate here.
   - **Analogy**: It's like ordering a pizza through an app—this is where you interact with the service.
2. **Presentation Layer (Layer 6)**
   - **What it does**: Translates data into a format the application understands. It also handles encryption, compression, and decryption.
   - **Example**: SSL/TLS encrypting your web connection or converting images from .png to .jpg for compatibility.
   - **Analogy**: Think of this as the pizza kitchen preparing the food in a format everyone can eat (e.g., slices for sharing).
3. **Session Layer (Layer 5)**
   - **What it does**: Manages the session or connection between two systems, ensuring communication remains active. It also handles reconnections if needed.
   - **Example**: Keeping your login session alive on a website without needing to re-login repeatedly.
   - **Analogy**: It's like reserving a table at a restaurant, ensuring you have a place to dine.
4. **Transport Layer (Layer 4)**
   - **What it does**: Ensures the data is delivered reliably and in order. It segments data streams and manages congestion.
   - **Example**: TCP (reliable delivery) or UDP (faster but less reliable delivery).
   - **Analogy**: This is like packaging the pizza in a box to ensure it arrives intact.
5. **Network Layer (Layer 3)**
   - **What it does**: Routes data across networks, finding the best path to the destination using IP addresses.
   - **Example**: Routers use this layer to direct data to the right device using IPv4 or IPv6.
   - **Analogy**: It's like the delivery driver using GPS to find your house.

6. **Data Link Layer (Layer 2)**
    - **What it does**: Handles communication between devices on the same network and ensures error-free transmission.
    - **Example**: MAC addresses or switches directing traffic within a local network.
    - **Analogy**: This is like ensuring the delivery driver uses the correct apartment buzzer code to enter your building.
7. **Physical Layer (Layer 1)**
    - **What it does**: Transmits raw bits (0s and 1s) over cables, fiber optics, or Wi-Fi signals.
    - **Example**: Ethernet cables, radio waves, or Bluetooth signals.
    - **Analogy**: It's the physical road or path the delivery driver uses to bring your pizza.

The Layers at Work: Sending and Receiving Data

When you send data (e.g., visiting a website):

1. The process starts at **Layer 7 (Application)**, where you type a URL.
2. Each layer below adds its specific functionality (like routing, error checking, or encryption) until the data is converted into electrical signals at **Layer 1 (Physical)** and sent over the network.

When the data reaches the receiver:

1. It travels in reverse, starting at **Layer 1**, where the physical signals are picked up.
2. Each layer processes its part, removes unnecessary headers, and passes the data upward until it reaches **Layer 7**, where it's displayed as a readable webpage.

Real-Life Example: Sending a Text Message

Imagine sending a text message through a chat app:

1. **Application Layer (Layer 7)**: You type and send the message.
2. **Presentation Layer (Layer 6)**: The message is converted into a readable format for the recipient.
3. **Session Layer (Layer 5)**: The app maintains a connection with the recipient's app.
4. **Transport Layer (Layer 4)**: The message is divided into small packets and sent reliably.
5. **Network Layer (Layer 3)**: The packets are routed across the Internet to the recipient.
6. **Data Link Layer (Layer 2)**: The packets are organized into frames for error-free transmission.
7. **Physical Layer (Layer 1)**: The message travels as electrical signals or radio waves to the recipient's device.

The recipient's device then unpacks and processes the message, reversing the layers, so they see it in their chat window.

Key Points to Remember

- **Layers 1-4**: Focus on reliable delivery (transport-oriented).
- **Layers 5-7**: Focus on user interaction and applications (application-oriented).
- Every layer performs specific tasks and uses the services of the layer below it.

Understanding this structure helps troubleshoot issues, analyze traffic, and secure communications, which is why penetration testers and network engineers use it extensively.