Here is a **clear and short summary** of the GeeksforGeeks article on:

🔹 Difference between Unicast, Broadcast, and Multicast in Computer Networks

---

✅ 1. Unicast (One-to-One)

- **Definition**: Data sent from one sender to one specific receiver.
- **Example**: Sending an email or file transfer.
- **Addressing**: Uses a unique destination IP.
- **Network Load**: Low.
- **Security**: High.

✅ 2. Broadcast (One-to-All)

- **Definition**: Data sent from one sender to all devices in a network.
- **Types**:
    - **Limited Broadcast**: Sent within the same local network using IP `255.255.255.255`.
    - **Direct Broadcast**: Sent to all hosts in a different network by setting host bits to 1.
- **Example**: DHCP requests, ARP.
- **Network Load**: High.
- **Security**: Low (reaches all devices).

✅ 3. Multicast (One-to-Many)

- **Definition**: Data sent from one sender to a selected group of receivers.
- **Example**: Live video streaming, online gaming.
- **Addressing**: Uses multicast IPs (Class D: 224.0.0.0 – 239.255.255.255).
- **Network Load**: Moderate.
- **Security**: Medium (only group members get data).

📊 Comparison Table

Feature	Unicast	Broadcast	Multicast
Transmission	One-to-One	One-to-All	One-to-Many
Address Used	Unique IP	Broadcast IP	Multicast IP (Class D)
Recipients	Single	All in network	Specific group
Bandwidth	Moderate	High	Moderate
Latency	Low	High	Moderate
Security	High	Low	Medium
Use Cases	Email, FTP	DHCP, ARP	IPTV, Online gaming

📝 Conclusion

Each type of “cast” serves different purposes:

- Use **Unicast** for personal communication,
- Use **Broadcast** for sending data to all,
- Use **Multicast** for efficient group communication.

Would you like this as a **PDF, table format, flashcards, or a one-page revision note**?

Thanks! Here's a **neatly formatted one-page revision note** based on the GeeksforGeeks article on **Unicast, Broadcast, and Multicast in Computer Networks**:

🧠 Unicast vs Broadcast vs Multicast – Quick Revision Sheet

✅ 1. Unicast (One-to-One)

- **Definition**: Communication from one sender to one specific receiver.
- **Used For**: Personal messaging, file transfers.
- **IP Addressing**: Unique destination IP address.
- **Pros**: Secure, low network load.
- **Example**: Sending an email.

✅ 2. Broadcast (One-to-All)

- **Definition**: Data is sent from one sender to **all** devices in the network.
- **Types**:
  - **Limited Broadcast**: Within the local network using IP `255.255.255.255`.
  - **Direct Broadcast**: Sent to all devices in another network by setting host bits to 1.
- **Used For**: Device discovery, address resolution.
- **Pros**: Reaches everyone.
- **Cons**: High network traffic, low security.
- **Example**: DHCP request, ARP.

✅ 3. Multicast (One-to-Many)

- **Definition**: Data is sent to a **specific group** of receivers.
- **Used For**: Efficient data delivery to multiple users.
- **IP Addressing**: Class D IPs (224.0.0.0 to 239.255.255.255).
- **Requires**: IGMP, multicast routing.
- **Example**: Video streaming, online gaming.

📊 Comparison Table

Feature	Unicast	Broadcast	Multicast
Communication	One-to-One	One-to-All	One-to-Many
IP Address	Unique IP	255.255.255.255 / Direct	Class D (224.x.x.x)
Target	Single device	All devices in network	Selected group
Bandwidth Usage	Moderate	High	Moderate
Security	High	Low	Medium
Latency	Low	High	Moderate
Network Load	Least	Most	Medium
Use Cases	Email, FTP	ARP, DHCP	IPTV, Gaming

📝 Key Takeaway

- **Unicast** → private, efficient, personal.
- **Broadcast** → universal but noisy.
- **Multicast** → balanced, for group-based services.

Let me know if you'd like this exported as a **PDF**, turned into **flashcards**, or included in your placement prep notes.

Here's a **clear, short summary** of the GeeksforGeeks article on:

🔹 TCP Connection Establishment – 3-Way Handshake

✅ What is TCP?

- **TCP (Transmission Control Protocol)** ensures reliable, ordered, and error-checked data transfer.
- Used in **web browsing, email, file transfer**.
- Works with **packets** and **retransmits** if lost.

✅ How TCP Establishes Connection? (3-Way Handshake)

🔸 Step 1: Client → Server (SYN)

- Sends a **SYN** (synchronize) packet with:
  - `Seq = 521` → Initial Sequence Number.
  - `MSS = 1460 B` → Max segment size.
  - `Window = 14600 B` → Client's buffer size.

🔸 Step 2: Server → Client (SYN + ACK)

- Responds with a **SYN + ACK** packet:
  - `Seq = 2000` → Its own sequence number.
  - `Ack = 522` → Acknowledges client's SYN.
  - `MSS = 500 B` → Smaller than client's, so both agree on **500 B**.
  - `Window = 10000 B` → Server's buffer size.

🔸 **Step 3: Client → Server (ACK)**

- Sends **ACK** packet:
  - `Seq = 522`, `Ack = 2001` (acknowledges server's SYN).
  - Connection is now **established**.

✅ TCP Flags Used

Flag	Meaning
SYN	Start a connection
ACK	Acknowledge received data
RST	Reset the connection
FIN	Finish/close the connection

📊 Window Size and MSS

- Sender can send: `10000 B / 500 B = 20 packets`
- Receiver can send: `14600 B / 500 B = 29 packets`

❌ Common Issues

- **SYN Flood Attack**: Sends repeated SYNs without completing the handshake.
- **Connection Timeout**: No reply from the other device.

- **Packet Loss**: Causes delays or failure.

⚡ Optimization Tips

- **TCP Fast Open**: Send data earlier in the handshake.
- **Keep-Alive**: Keeps connection open for longer.
- **Load Balancing**: Improves speed by using multiple servers.

💡 FAQ

- **“Established”** means 3-way handshake is done, and data can be exchanged.
- **Connection Limit**: Varies by system (can be thousands to millions).
- **Speed Limit**: No fixed limit—depends on bandwidth, congestion, etc.

Let me know if you'd like:

- Diagram of the 3-way handshake
- PDF revision sheet
- Flashcards
  or a quiz to test your understanding!

Here’s a concise summary of the **“Types of Routing”** article from GeeksforGeeks, including the key headings and one-line explanations:

🔁 Routing Overview

Routing is the process of determining the best path for data packets to travel across a network using Layer 3 devices like routers.

🧭 Types of Routing

There are **3 main types of routing**:

---

1. Static Routing

Routing paths are **manually configured** by a network administrator.

- **Advantages:**
  - No CPU overhead.
  - More secure.
  - No bandwidth usage for route updates.
- **Disadvantages:**
  - Tedious for large networks.
  - Requires deep knowledge of network topology.

Example Command:

```
ip route [destination network] [subnet mask] [next hop IP]
```

-

---

2. Default Routing

All unknown traffic is forwarded to a **default gateway**, typically used with **stub routers** (routers with only one path out).

- **Advantages:**
  - Acts as a last-resort path.
  - Simplifies routing table.
  - Improves reliability.
- **Disadvantages:**

    - Can cause inefficient routing.
    - May increase latency.

Example Command:

```
ip route 0.0.0.0 0.0.0.0 [next hop IP]
```

-

---

3. Dynamic Routing

Routers automatically discover and maintain routing tables using **protocols like RIP or OSPF**.

- **Advantages:**
    - Automatically adapts to network changes.
    - Suitable for large, complex networks.
- **Disadvantages:**
    - Consumes more bandwidth.
    - Less secure compared to static routing.
- **Key Points:**
    - Requires same protocol on all routers.
    - Shares updates on topology changes.

Would you like this in a **PDF**, **table format**, or as **flashcards for quick revision**?

Here's a **summarized version** of the **GeeksforGeeks article on "Introduction to Subnetting"**, with **main headings** and **one-line explanations** for each:

📌 Introduction to Subnetting

Subnetting is the process of dividing a large network into smaller parts (subnets) to **enhance manageability, security, and efficiency**.

🔍 Introduction to Subnet

A **subnet** is a smaller section of a larger network that allows localized communication among devices within that group.

❓ Why Subnetting is Important?

Subnetting helps:

- **Avoid IP address wastage**
- **Improve performance** by reducing traffic
- **Enhance security** through network isolation
  Example: Dividing a Class C network (192.168.1.0/24) into three efficient subnets for Sales, HR, and IT.

🧠 Key Concepts in Subnetting

✅ IP Addressing

IPv4 addresses are made of **network and host portions**, divided into classes (A, B, C).

✅ What is a Subnet Mask?

A 32-bit number that determines which portion of an IP is the network and which is the host.

✅ CIDR Notation

A simplified way to represent subnet masks using a slash (e.g., /24 for 255.255.255.0).

⚙️ How Subnetting Works

Subnetting modifies the **host portion** of an IP address to create subnets.
Example with Class C IP:

- Subnet 1 → 193.1.2.0 to 193.1.2.127
- Subnet 2 → 193.1.2.128 to 193.1.2.255
  Each with **126 usable host addresses**.

🔢 Example: Splitting a Class C Network

Using 255.255.255.192 (/26) divides a network into 4 subnets with **64 addresses each**, 62 usable.

🧮 Bitwise Subnetting Logic

- Dividing into 2 subnets → use 1 bit: `00`, `01`
- Dividing into 4 subnets → use 2 bits: `00`, `01`, `10`, `11`
- **More subnets = fewer hosts per subnet**

🧪 Example Questions

❓ Example 1

Given: `201.35.2.0/26`, find valid host IPs
✅ Valid: `201.35.2.129`
❌ Invalid: `201.35.2.191`, `201.35.2.255` (broadcast addresses)

❓ Example 2

Given: `201.32.64.0/29`, find invalid broadcast
❌ Not valid: `201.32.64.240`
✅ Valid broadcast: `201.32.64.135`, `207`, `231`

✅ Advantages of Subnetting

- **Security** between departments
- **Custom performance** for different subnets
- **Easier management** in small networks

❌ Disadvantages of Subnetting

- **Two IPs are wasted** per subnet (network ID & broadcast)
- **Higher infrastructure cost** (requires routers, switches)
- **More routing hops** than flat networks

Would you like this summary as a **cheat sheet**, **table**, or **downloadable PDF**?

Here’s a **clean summary with headings and concise explanations** of the article you provided on **Dynamic Host Configuration Protocol (DHCP)** from GeeksforGeeks:

✅ What is DHCP?

DHCP (Dynamic Host Configuration Protocol) is a **network protocol** that **automatically assigns IP addresses** and other network settings to devices on a network, eliminating the need for manual configuration.

🧩 Components of DHCP

- **DHCP Server**: Stores and assigns IP addresses and network info.
- **DHCP Client**: Device that requests configuration (PC, mobile, etc.).
- **DHCP Relay**: Passes DHCP messages between clients and servers across networks.

- **IP Address Pool**: Range of IP addresses the server can assign.
- **Subnets**: Divisions of the network to organize IP allocation.
- **Lease**: Duration a client can use the assigned IP.
- **DNS Servers**: Provided to clients for resolving domain names.
- **Default Gateway**: Router IP to communicate outside local network.
- **Options**: Extra settings like domain name, time servers, etc.
- **Renewal**: Clients renew lease before expiration.
- **Failover**: Redundant DHCP server setup for high availability.
- **Dynamic Updates**: DHCP server can update DNS records automatically.
- **Audit Logging**: Logs of all DHCP transactions for tracking.

📦 DHCP Packet Format

Key fields include:

- **Hardware Length** (e.g., 6 for Ethernet)
- **Hop Count**: Limits message hops.
- **Transaction ID**: Matches requests with replies.
- **Seconds Elapsed**: Since client started booting.
- **Flags**: Controls broadcast behavior.
- **IP Address Fields**: For client, server, and gateway.
- **Client MAC Address**
- **Server Name** (optional)
- **Boot Filename** (optional)
- **Options**: Vendor-specific or extended info.

🔁 Working of DHCP (DORA Process)

Uses **UDP**:

- **Server Port: 67**, **Client Port: 68**

🔄 The 4 Main Steps (DORA):

1. **Discover**: Client broadcasts to find DHCP servers.
2. **Offer**: Server offers IP and configuration.
3. **Request**: Client requests offered IP.
4. **Acknowledgment (ACK)**: Server confirms and leases IP.

✉️ All 8 DHCP Messages

1. **Discover** – Client asks for available servers.
2. **Offer** – Server offers IP and settings.
3. **Request** – Client requests the offered IP.
4. **ACK** – Server confirms the lease.
5. **NACK** – Server denies request (e.g., no IPs available).
6. **Decline** – Client rejects IP (e.g., duplicate found via ARP).
7. **Release** – Client releases IP back to server.
8. **Inform** – Client requests config info without IP allocation.

🛡️ Security Concerns

- **IP Pool Exhaustion**: Attackers flood requests (DHCP starvation).
- **Rogue DHCP Servers**: Unauthorized servers give false info.
- **DNS Exploitation**: Misuse of DNS info from DHCP.

🔐 Protection

- Detect and block starvation attacks.
- Validate DHCP servers in enterprise networks.

✅ Advantages of DHCP

- Centralized IP management.
- Automatic configuration.
- Easy to add new clients.
- IP reuse and dynamic assignment.
- Simplifies mobile device IP handling.
- Supports easy network changes.

⚠️ Disadvantages of DHCP

- **IP Conflicts** can occur.
- **Clients accept any server**, including malicious ones.
- **No DHCP = No network access**.
- **Machine name doesn't update** automatically with IP.

Let me know if you'd like:

- A PDF or Word summary
- Flashcards
- A diagram of the DHCP message flow
- A quiz to test understanding

Here’s a **structured summary** of the **GeeksforGeeks article on "Types of Network Firewall"**:

🔐 What is a Network Firewall?

A **firewall** is a hardware or software solution that monitors and controls network traffic to protect private networks from unauthorized access.

🧱 Main Purpose

To separate **internal (trusted)** networks from **external (untrusted)** networks and prevent malicious access or data leaks.

🔎 Types of Network Firewalls (Grouped by Criteria)

1. Based on Network Placement

Type	Function	Analogy
Packet Filtering Firewall	Filters packets based on header info (IP, port, protocol)	Checking ID at a gate
Stateful Inspection Firewall	Remembers active connections and makes decisions contextually	Hotel that remembers you checked in

Proxy Firewall	Intercepts traffic, inspects, and forwards it	Assistant fetching things for you
Circuit-Level Gateway	Verifies TCP handshakes without inspecting content	Confirming a call is from a known number
Web Application Firewall (WAF)	Protects websites/web apps from specific attacks (e.g., SQL injection)	Form guard checking input before it reaches your site
Next-Generation Firewall (NGFW)	Combines traditional firewall + IDS/IPS, malware filtering, etc.	A security team with all kinds of advanced tools

---

2. Based on Scope

Type	Description	Analogy
Network Firewall	Protects the entire network (at entry/exit points)	Guard at building entrance
Host-Based Firewall	Installed on individual devices (e.g., laptops)	App guarding just your phone

---

3. Based on Data Filtering Method

Type	Description	Analogy
Perimeter Firewall	Positioned at the network boundary	Fence gate guarding the property

Internal Firewall	Positioned between internal network segments	Door locks for each department
Distributed Firewall	Applied across multiple endpoints	Alarm systems in every room

4. Based on Form Factor

Type	Description	Analogy
Hardware Firewall	Physical device connected to the network	Security gate at the entrance
Software Firewall	Software installed on individual machines	Security app on your device

⚙️ Working of Firewalls

- Inspects **data packets** for harmful content.
- Blocks **spam, viruses, and malware**.
- Controls both **inbound and outbound** traffic.

🚀 Modern Firewall Capabilities

- **Application-level filtering**
- **Intrusion prevention**
- **Encrypted traffic inspection**

- A **single firewall solution** may include multiple types for layered defense.

⚠️ Limitations of Firewalls

Issue	Description
Cost	Hardware-based solutions can be expensive
Restrictions	May prevent legitimate user actions in large organizations
Speed Issues	Can slow down the network due to traffic inspection
Maintenance	Requires constant updates to defend against evolving threats

---

If you'd like, I can convert this summary into a **PDF, Word doc, or flashcards**—just let me know!

Here’s a **structured and simplified summary** of the **GeeksforGeeks article on "Types of Cyber Attacks"**, updated as of **15 July 2025**:

🔐 What is a Cyber Attack?

A **cyberattack** is a deliberate attempt to exploit systems, networks, or devices to:

- Steal data
- Cause damage or disruption

- Gain unauthorized access

Cybercriminals exploit vulnerabilities in software or human behavior to achieve their goals.

💣 Common Types of Cyber Attacks

1. Phishing

- **What it is**: Fake emails or messages impersonating legitimate sources.
- **Goal**: Trick users into clicking malicious links or giving personal info.
- **Example**: Email that looks like it's from a bank asking you to "verify your account."

---

2. Social Engineering

- **What it is**: Psychological manipulation to trick people into revealing sensitive information.
- **Example**: Leaving infected USB drives labeled “Payroll Info” in public places to lure users into plugging them in.

---

3. Ransomware

- **What it is**: Malware that encrypts your files and demands payment (usually in cryptocurrency) to unlock them.
- **Famous examples**: WannaCry, Maze.
- **Impact**: Business operations freeze until ransom is paid.

---

4. Cryptocurrency Hijacking (Cryptojacking)

- **What it is**: Secretly using someone else's device to mine cryptocurrency.

- **How it happens**:
  - Through phishing emails with hidden mining code.
  - Via websites or ads with embedded mining scripts.
- **Result**: Slower computers, higher electricity usage, and resource abuse.

---

5. Botnet Attacks

- **What it is**: A network of infected devices (called “zombies”) controlled by an attacker.
- **Used for**:
  - DDoS attacks (taking down servers by overwhelming them)
  - Credential stuffing (using stolen usernames/passwords)
  - Data theft
  - Spamming

💥 Impact of Cyber Attacks

Type of Impact	Description
💸 Financial Losses	Theft of money, card details, or ransom demands.
📉 Reputation Damage	Loss of trust from customers or partners.
📂 Data Loss	Loss of critical data (personal, business, legal).

🚫 Service Disruption	Crashing of vital services (e.g., healthcare).

🛡️ How to Prevent Cyber Attacks

✅ Best Practices

1. **Antivirus + Firewalls** – Regularly update and use security software.
2. **Security Training** – Teach employees to recognize scams and phishing.
3. **Strong Passwords** – Use complex, unique passwords + password managers.
4. **Two-Factor Authentication (2FA)** – Adds an extra layer of protection.
5. **Regular Backups** – Ensure recovery if data is lost or encrypted.
6. **Avoid Public Wi-Fi** – Use VPNs for safe connections.
7. **Patch Systems** – Always update software to fix security holes.
8. **Implement Security Policies** – Define data access, device usage, and incident response protocols.
9. **Monitor Systems** – Use threat detection tools and logs.

⚠️ Most Common Cyber Attacks (Recap List)

Type	Description
Phishing	Deceptive emails tricking users into revealing data
Ransomware	Encrypts data and demands ransom

Malware	General malicious software like viruses or worms
DoS / DDoS	Overload systems to shut them down
Man-in-the-Middle	Intercepting and altering communication
SQL Injection	Exploiting database vulnerabilities
Zero-Day Exploits	Attacks on undiscovered software flaws

🧠 Conclusion

Cybersecurity requires **proactive protection**:

- Combine **technical tools** (firewalls, antivirus, VPNs)
- Maintain **user awareness**
- Enforce **policies and monitoring**
- Prepare an **incident response plan**

Staying informed and vigilant is essential for individuals and organizations to defend against modern cyber threats.

Would you like this as:

- A **PDF summary**
- A **PowerPoint deck**
- A **Word document**

- Or **flashcards**?

Just let me know your preferred format!

Here’s a **concise, clear, and student-friendly summary** of the **GeeksforGeeks article on “Virtualization in Cloud Computing and Its Types”** (Updated: **31 July 2025**):

☁️ What is Virtualization in Cloud Computing?

Virtualization is the process of creating multiple **virtual versions** of computers, servers, or other resources on a **single physical machine**.

💡 Instead of using four physical servers, virtualization allows you to run **4 virtual machines (VMs)** on one server—saving cost, space, and energy.

⚙️ How Does Virtualization Work?

- **Software Used**: **Hypervisor**
  - Controls how virtual machines (VMs) access the physical computer's resources.
- **Components**:
  - **Host**: The real physical machine.
  - **Guest**: The virtual machine.

🔧 Types of Hypervisors:

Type	Description
Type 1 (Bare-Metal)	Installed directly on hardware (no OS). Fast & efficient.
Type 2	Installed on top of an OS (like Windows). More flexible.

🧱 Types of Virtualization

1. Application Virtualization

- **What it is**: Run apps on any device **without installing** them locally.
- **Example**: Microsoft Azure lets employees run apps via the cloud from any device.

---

2. Network Virtualization

- **What it is**: Run **multiple virtual networks** on a single physical network.
- **Example**: Google Cloud enables companies to create flexible cloud-based networks (with firewalls, VPNs, etc.).

---

3. Desktop Virtualization

- **What it is**: Create virtual desktops accessible from any device.
- **Example**: Amazon WorkSpaces lets GeeksforGeeks team members access coding environments from anywhere.

---

4. Storage Virtualization

- **What it is**: Combine storage from different devices into one virtual system.
- **Example**: Amazon S3 lets companies store and access large data securely from anywhere.

---

5. Server Virtualization

- **What it is**: Split a physical server into multiple **independent virtual servers**.

- **Example**: Using VMware to run a web server, a database, and a file server on one physical server.

---

6. Data Virtualization

- **What it is**: Access and manage data from multiple sources **without moving or copying it**.
- **Example**: IBM and Oracle tools allow combining data from various platforms into a unified view.

🆚 Virtualization vs Cloud Computing

Aspect	Virtualization	Cloud Computing
What it is	Creating virtual versions of physical resources	Using computing services over the internet
Where it runs	On physical servers	On cloud provider’s remote infrastructure
Focus	Efficient use of hardware	On-demand access to resources
Example	Running multiple VMs on one PC	Storing files on Google Drive or AWS
Control	You manage the entire setup	You manage only what you use; provider handles rest

---

🧠 Real-World Benefits of Virtualization

- ✅ Saves money on hardware
- ✅ Easy scaling and resource management
- ✅ Boosts performance and availability
- ✅ Supports cloud-based flexibility and mobility

Would you like this as:

- 📄 A **PDF summary**
- 📊 A **PowerPoint presentation**
- 📚 Flashcards for revision
- 📘 A Word document?

Let me know how you'd like it formatted!

Here's a **well-structured summary** of the GeeksforGeeks article on **Wired and Wireless Networking** and related topics, tailored for Class 9 or beginner-level understanding:

🌐 Internet and Networking Summary

1. 🚀 Origin of the Internet

- **Created in the 1960s** for government research and communication.
- **ARPANET** was the first form, built for communication even after a nuclear attack.
- **TCP/IP** became the universal communication protocol in 1983, enabling the modern internet.

---

2. 🕸 World Wide Web (WWW)

- A **service on the Internet** used to access documents via protocols.
- Uses **hypertext links** and **browsers** to navigate between web pages.
- A **URL** (Uniform Resource Locator) identifies each web page.
- A **website** is a collection of web pages under a single domain (e.g., www.google.com).

---

3. 💻 Computer Network

- A **network** is a group of connected computers that share resources.
- Nodes in a network can include PCs, servers, and networking devices.
- Connections can be **wired** (cables) or **wireless** (radio waves, infrared).

---

4. 🔌 Wired vs Wireless Networking

📶 Types:

- **Wired Network**: Uses cables (e.g., Ethernet).
- **Wireless Network**: Uses electromagnetic waves (e.g., Wi-Fi, Bluetooth).

🔁 Comparison:

S.No	Wired Network	Wireless Network
1	Uses cables for connection	Uses EM waves (radio, infrared)
2	Faster transmission speed	Slower transmission speed
3	Low propagation delay	High propagation delay

4	More secure	Less secure
5	Devices need wiring	Easy installation
6	Less expensive hardware	More expensive devices
7	High installation/maintenance cost	Low installation/maintenance cost
8	Uses hubs, switches	Uses routers, access points

---

5. 📡 Wi-Fi

- **Wi-Fi = Wireless Fidelity**
- Allows wireless Internet access via **routers** using **radio frequencies**.
- Defined by the **IEEE 802.11 standard**.

---

6. 🔄 Bluetooth

- Wireless technology for **short-range** communication.
- Uses **2.4 GHz radio frequency**.
- Works through **walls/objects**, unlike older **infrared** systems.
- Limited range (~30 feet), but **energy efficient** and low cost.

---

7. ☁️ Cloud Computing

✅ **Definition:**

- A method to **access computing resources online** (e.g., storage, servers).
- Enables **on-demand** service with **minimal management effort**.

☁️ **Types of Clouds:**

Type	Description	Example
Public Cloud	Available to the general public; less secure	Microsoft Azure, GAE
Private Cloud	Exclusive to one organization	E-bay
Hybrid Cloud	Mix of public, private, and community clouds	—
Community Cloud	Shared by organizations with similar requirements	—

🌟 **Benefits of Cloud Computing:**

1. Available 24x7
2. Strong security (data backup & recovery)
3. Cost-effective & scalable
4. Pay-per-use model
5. Resource pooling & shared infrastructure
6. Easy disaster recovery

---

8. 📄 Basic Definitions

Term	Definition
Web Page	A document written in HTML, can contain text, images, and hyperlinks.
Website	A group of related web pages accessed via a common URL.
Browser	Software used to access and display websites (e.g., Chrome, Firefox).
URL	The address of a web page (e.g., https://www.geeksforgeeks.org).

---

9. 🌐 Wi-Fi vs Internet

Wi-Fi	Internet
Wireless method to access local networks	Global network that connects devices worldwide
Needs router but not always internet	Needs ISP and modem to access globally
May exist without Internet	Cannot access websites without Internet

---

Would you like this as a **PDF**, **flashcards**, or **revision notes**?