Computer Network (BCS603)

EduShine CLASSES By:- ARMAN ALI

Unit – 5 Application Layer

V	**Application Layer:** Domain Name System, World Wide Web and Hyper Text Transfer Protocol, Electronic mail, File Transfer Protocol, Remote login, Network management, Data compression, Cryptography – basic concepts.

Edushine Classes

Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

❖ Introduction to Application Layer :

The **Application Layer** is the **top-most layer** of the **OSI model** (7th layer) and also in the **TCP/IP model**.

- ◆ It is **closest to the user** — meaning the apps you use (like browsers, Gmail, WhatsApp) all work at this layer.
- ◆ It provides **services** to users and apps so they can communicate over a network.
- The application layer provides the functionality to send and receive data from users. It acts as the interface between the user and the application.
- The Application Layer is the “face” of the network that the user interacts with. It helps applications talk over the internet using services like browsing, email, file sharing, and more.

Computer Network (BCS603)

EduShine CLASSES By:- ARMAN ALI

✓ Functions of the Application Layer (Explained Simply)

Here are the main **functions** of the Application Layer:

Functions of Application Layer

1. Data Representation
2. Network Service Access
3. Application Protocols
4. Session Management

Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

1. Data Representation

It ensures that data is in a readable format for both the sender and receiver, including data translation, compression, and encryption.

2. Network Service Access

It provides applications with access to network services, enabling communication over a network.

Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

3. Application Protocols

It supports protocols like HTTP, FTP, SMTP, and DNS that enable communication between applications.

4. Session Management

It manage establishment, maintenance, and termination of communication sessions between applications.

Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

✓ Protocols in Application Layer (With Uses)

Protocol	Full Form	Use / Function
HTTP	HyperText Transfer Protocol	Used to browse websites (web pages)
HTTPS	Secure HTTP	Same as HTTP but with encryption (secure)
FTP	File Transfer Protocol	To upload/download files between computers
SFTP	Secure File Transfer Protocol	Same as FTP, but secure (uses SSH)
SMTP	Simple Mail Transfer Protocol	Used to **send emails**
POP3	Post Office Protocol version 3	Used to **receive emails** (downloads to device)
IMAP	Internet Message Access Protocol	Used to **receive emails** (keeps mail on server)
DNS	Domain Name System	Converts website names to IP addresses
DHCP	Dynamic Host Configuration Protocol	Assigns IP addresses to devices automatically
Telnet	Terminal Emulation Protocol	For remote login (not secure)
SSH	Secure Shell	Secure remote login and command execution
SNMP	Simple Network Management Protocol	Used for network monitoring and management
NTP	Network Time Protocol	Synchronizes clocks of computers over network

Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

🌐 What is Domain Name System (DNS)?

DNS stands for **Domain Name System**.

- It is like the **phonebook of the internet**.
  It helps to convert **website names** (like www.google.com) into **IP addresses** (like 142.250.190.78), which computers use to identify each other.

✓ Why DNS is Needed (Requirements):

1.Humans remember names, not numbers

→ Easier to remember www.facebook.com than 157.240.22.35.

2.IP addresses can change

→ Even if IP changes, name stays same (DNS maps new IP).

3.Reduces Complexity

→ No need to update every time IP changes.

4.Helps Routing and Access

→ Helps find websites fast and globally.

Computer Network (BCS603)

☆ Features of DNS:

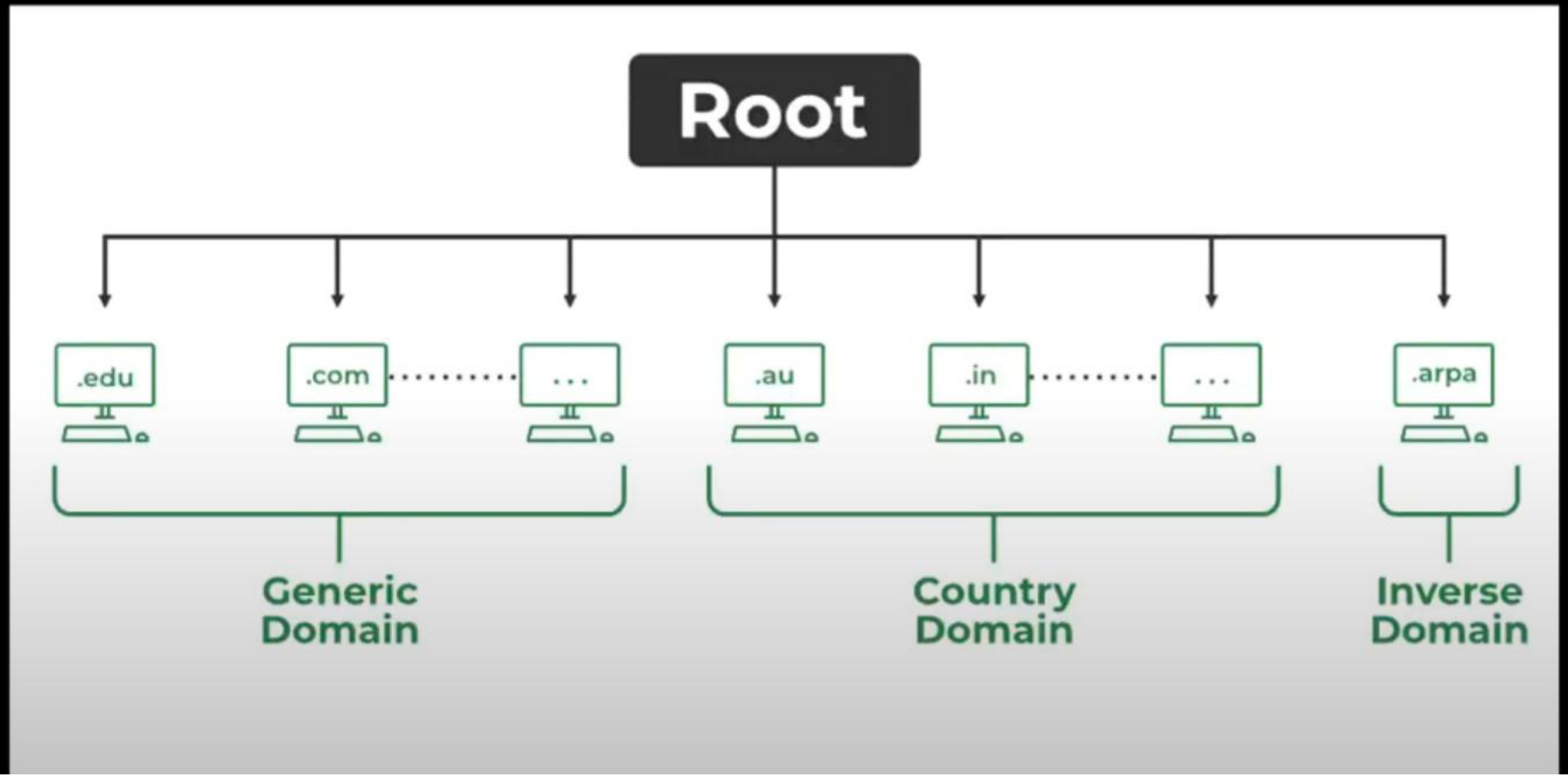
Feature	Explanation
Distributed system	Data is spread across many servers worldwide
Hierarchical	Works in levels (root → TLD → subdomain)
Reliable and Fast	Caches previous results for quick access
Easy to use	You use domain names instead of IPs
Scalable	Supports billions of domain names

Computer Network (BCS603)

EduShine CLASSES By:- ARMAN ALI

Types of Domains in DNS :

DNS divides domain names into **3 main types**:



Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

1. Generic Domain (gTLD)

- Used for general/global websites.
- Examples:
  - ✓ .com → Commercial (e.g., amazon.com)
  - ✓ .org → Organizations (e.g., wikipedia.org)
  - ✓ .net → Networks (e.g., slideshare.net)
  - ✓ .edu → Educational institutions (e.g., mit.edu)
  - ✓ .gov → Government (e.g., usa.gov)

✓ **Used worldwide, not country-specific.**

2. Country Domain (ccTLD)

- Based on **country codes** (2 letters).
- Examples:
  - ✓ .in → India (e.g., google.co.in)
  - ✓ .uk → United Kingdom
  - ✓ .us → United States
  - ✓ .jp → Japan
  - ✓ .au → Australia

✓ **Used for region-specific websites.**

3. Inverse Domain

- Used to **map IP address back to domain name**.
- Works **opposite** of normal DNS.
- Example:
  - IP → 157.240.22.35
  - Reverse DNS might map it to → facebook.com

✓ **Used in network troubleshooting, email servers (spam check), etc.**

Domain Type	Example	Used For
Generic Domain	.com, .org, .edu	General/global use
Country Domain	.in, .us, .uk	Country-specific websites
Inverse Domain	IP → Domain	Reverse IP lookup

Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

🔄 How DNS Works (Step-by-Step)

Let's say you want to visit a website like www.edushineclasses.in👇

Step 1: Your Computer Checks Cache

First, your **browser**, **computer**, or **router** checks:

- "Do I already know the IP address of this website?"
- If **yes**, it uses that — ✅ Done.
- If **no**, it continues to the next step.

📞 Step 2: Ask the DNS Resolver

- Your computer sends a query to a **DNS Resolver** (usually from your ISP or Google like 8.8.8.8).
- The resolver's job is to **find the IP address** for the domain.

Computer Network (BCS603)

Step 3: Go to the Root Server

DNS Resolver asks the **Root DNS Server**:

- "Hey, do you know the IP of www.edushineclasses.in?"

- Root server says:

"I don't know the full address, but I know who handles .in domains — go ask the **TLD server**."

Step 4: Go to TLD Server

- Resolver goes to the **TLD (Top Level Domain) server** for .org.
- Asks: "Do you know edushineclasses.in?"
- TLD says:

"Ask the **Authoritative Name Server** for edushineclasses.in."

Computer Network (BCS603)

🏠 Step 5: Go to Authoritative Name Server

- Resolver goes to **Authoritative Name Server** of edushineclasses.in
- This server says:

"Yes! The IP address of www.edushineclasses.in is **52.25.139.210**"

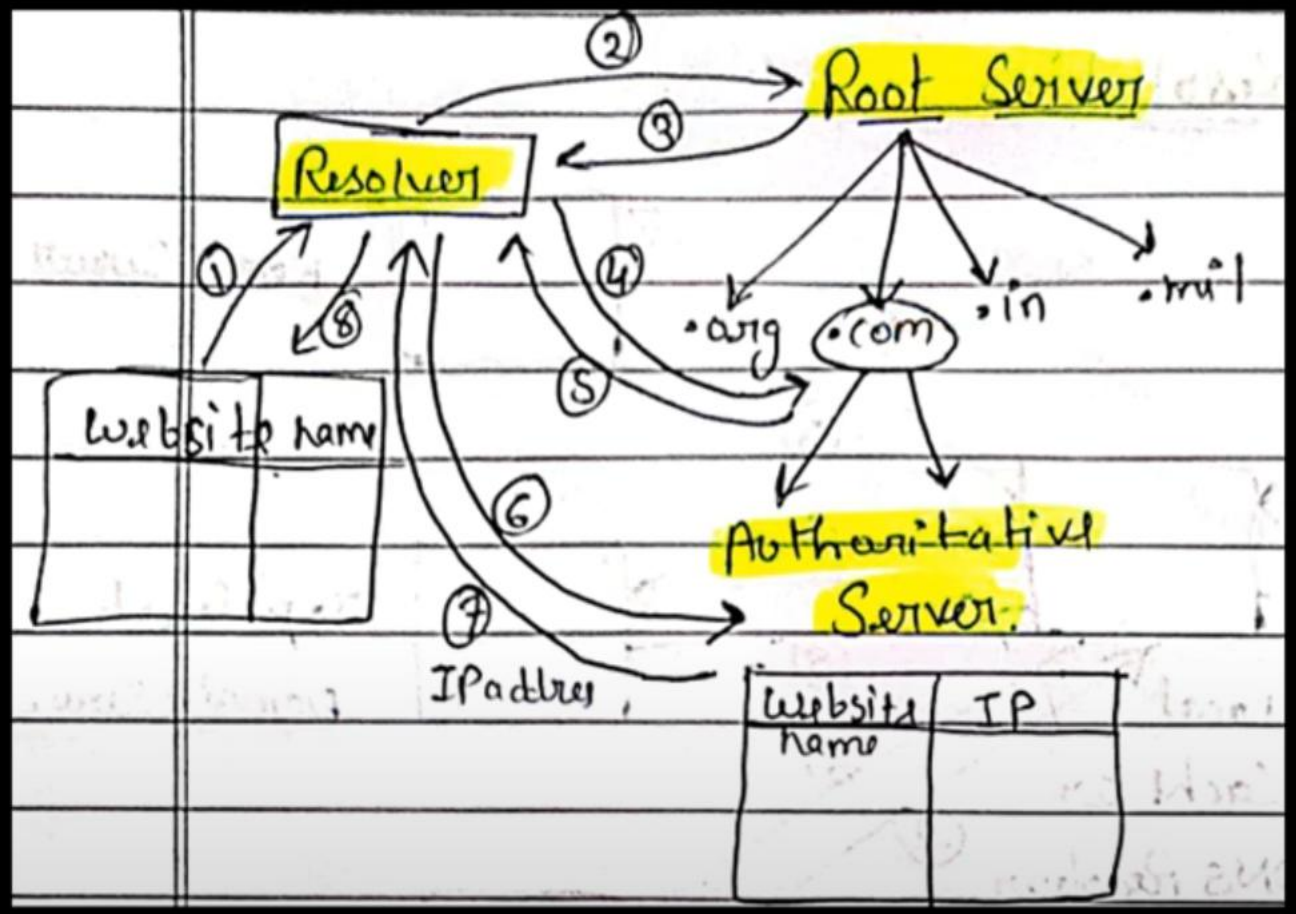
💻 Step 6: Send the IP Back

- DNS Resolver sends the IP address **back to your computer**.
- Now your browser knows where to go.

🌐 Step 7: Load the Website

- Your browser uses the IP 52.25.139.210 to contact the actual server.
- The website opens on your screen ✓

Computer Network (BCS603)



Computer Network (BCS603)

What is DNS Resolution?

DNS resolution means: **"Finding the IP address of a domain name."**

There are **two ways** your system can resolve a domain:

i. **Recursive Resolution**
ii. **Iterative Resolution**

1. Recursive Resolution (Your computer says: "Please do everything for me")

Your system tells the DNS Resolver:

- "I don't know anything. Please go and find the IP for me and come back with the answer."

The resolver takes the full responsibility to go through:

- Root Server
- TLD Server
- Authoritative Server

Then it returns the final IP address to your system.

Computer Network (BCS603)

💡 **Example:**

You (Client):

- "Hey Resolver, give me the IP of www.geeksforgeeks.org."

Resolver:

- Asks Root Server → Gets TLD
- Asks TLD Server → Gets Authoritative Server
- Asks Authoritative Server → Gets IP: 52.25.139.210

Resolver gives this final answer back to you.

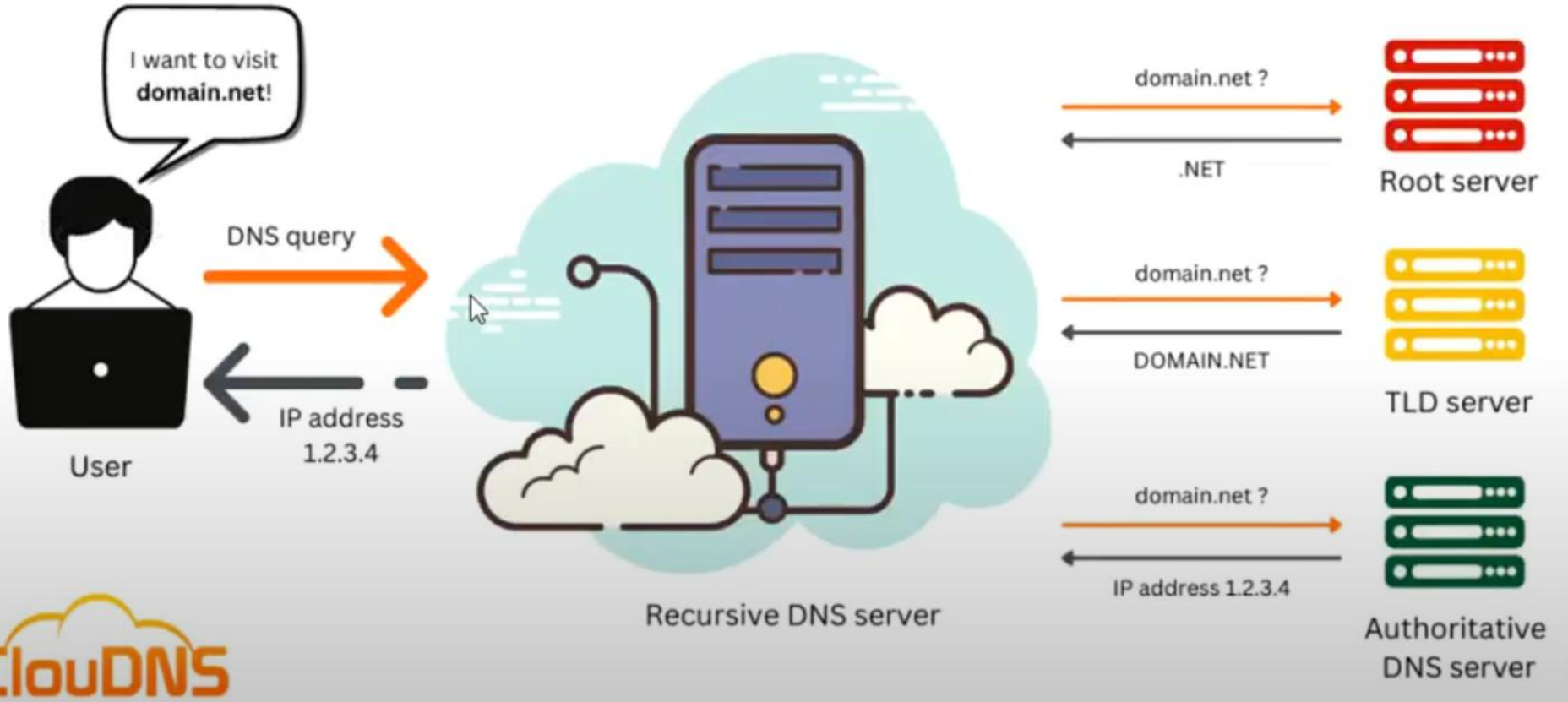
✅ **You don't talk to any other server.**

✅ **You just get the final answer.**

📌 **Features:**

- Easy for the client (no extra work)
- More work for the resolver
- Takes more memory at resolver side

Recursive DNS server



Computer Network (BCS603)

2. Iterative Resolution (Client does the step-by-step job)

Your system tells the DNS Resolver:

- "Tell me the next place I should ask."

And then your computer **goes to each server one-by-one** to find the final answer.

💡 **Example:**

➢ **You (Client):**

"Hey Root Server, what's the IP of www.geeksforgeeks.org?"

➢ **Root Server:**

"I don't know, but ask the .org TLD server."

➢ **You ask TLD Server:**

"Do you know geeksforgeeks.org?"

➢ **TLD Server:**

"No, but ask the authoritative server."

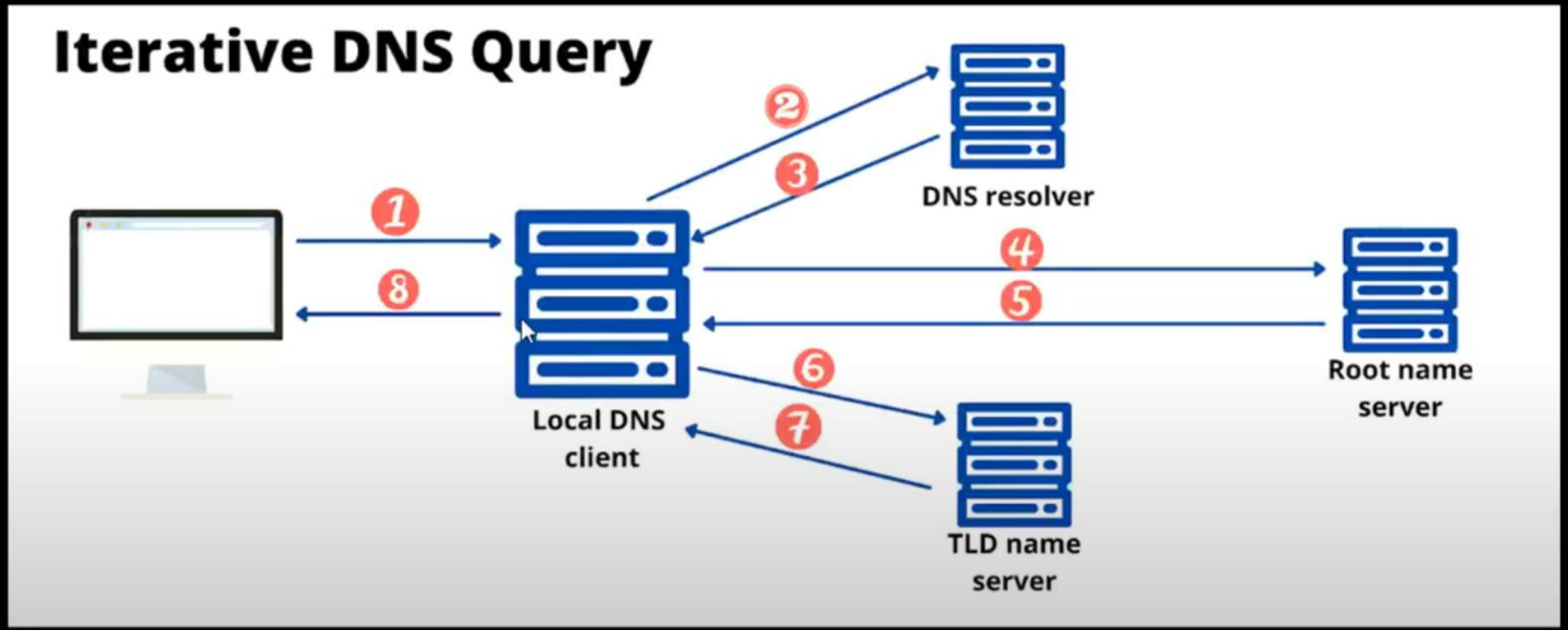
➢ **You ask Authoritative Server:**

"Do you know the IP?"**directly.**

➢ **Authoritative Server:**

"Yes! It is 52.25.139.210."

✓ **You (the client) talk to every server**



Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

Feature	Recursive Resolution	Iterative Resolution
Who finds the IP?	Resolver does full work	Client finds IP by asking step-by-step
Client effort	Very low	High
Resolver effort	High	Low
Time taken	Slightly more	Usually less (but depends)
Example	Google DNS (8.8.8.8) uses this	DNS root servers use this

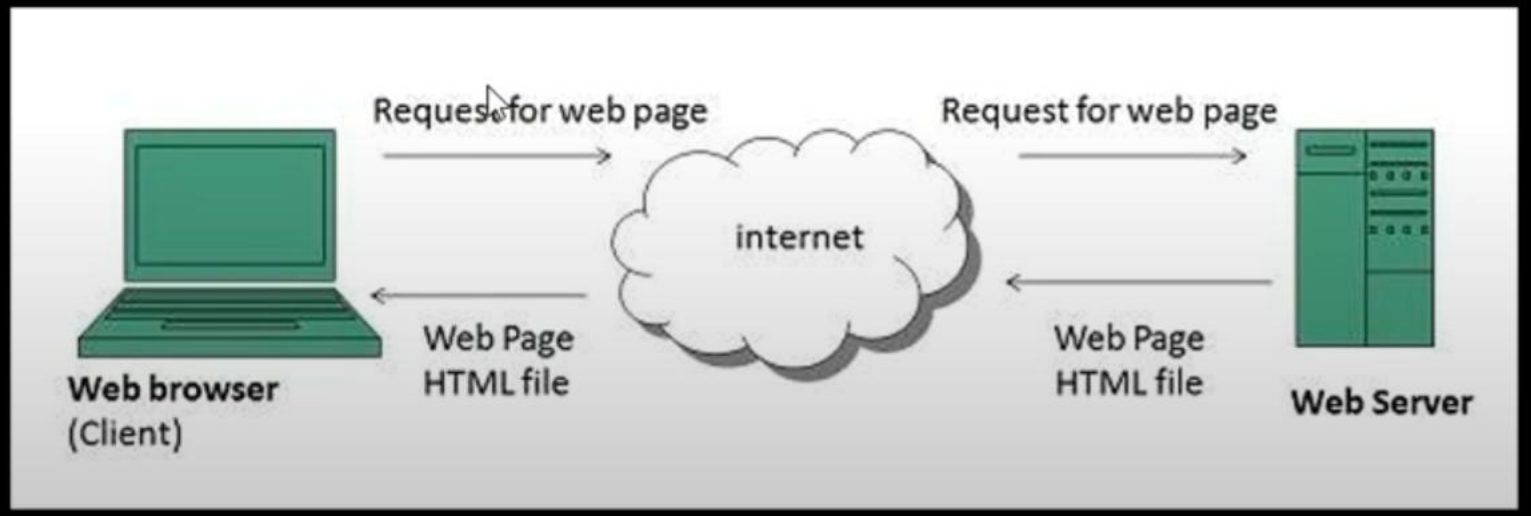
Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

🌐 What is the World Wide Web (WWW)?

The **World Wide Web** is a **system of web pages** that you can **access using the internet**. It allows us to see websites, watch videos, read blogs, shop online, learn from websites, and more.

- When you open a browser like **Chrome or Firefox** and type in a website address (like www.google.com), you are using the **World Wide Web**.



Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

❖ **Key Points :**

Term	Easy Meaning
Web	A collection of websites you can visit.
Website	A group of related web pages (like YouTube, Facebook, etc.).
Web Page	A single page of a website (like the homepage or about page).
Web Browser	Software like Chrome, Firefox, or Safari that lets you open websites.
Web Server	A special computer that stores websites and gives them to you when you request.

Computer Network (BCS603)

EduShine CLASSES By:- ARMAN ALI

How does WWW work?

1. **You type a website address** (like www.rrsimt.ac.in) in your browser.
2. The browser sends a request to the **web server**.
3. The **server finds the web page** you asked for.
4. It **sends the page back to your browser**.
5. You **see the page** (text, images, videos, etc.).

The **World Wide Web (WWW)** is a collection of websites and web pages that can be accessed using the Internet. It works through web browsers and uses protocols like **HTTP** to display content such as text, images, and

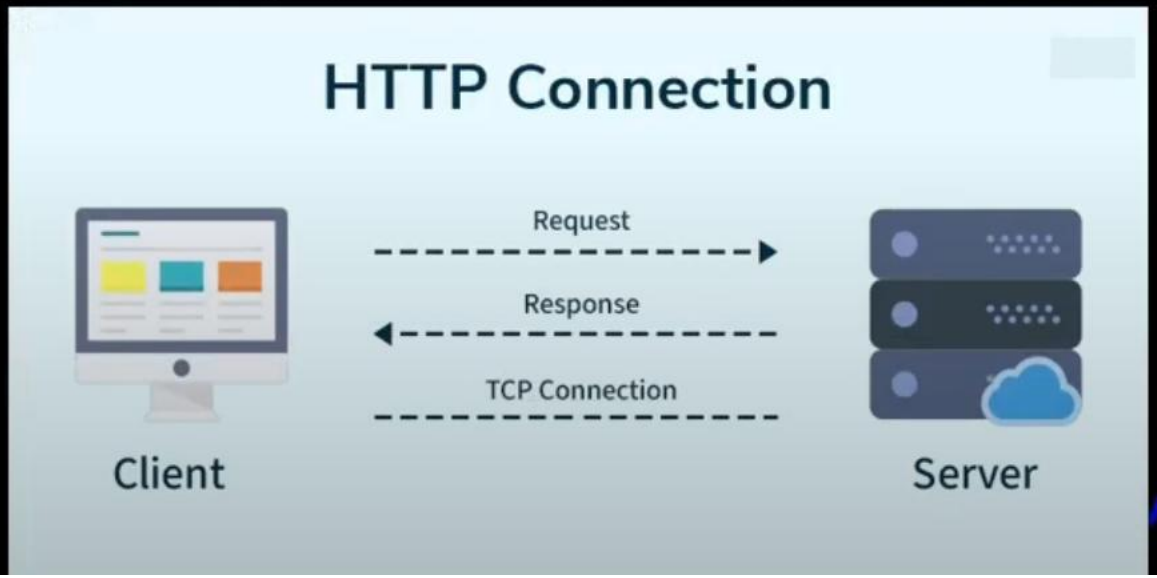
Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

❖ HTTP(Hyper text transfer Protocol) :

- **HTTP** stands for **HyperText Transfer Protocol**.
- It is the **main protocol** used on the **World Wide Web**.
  Whenever you **open a website**, your browser uses **HTTP** to **talk to the server** and get the page.

Example :**HTTP is a set of rules** that help your browser and a web server **talk to each other** and **exchange web pages, images, videos, etc.**



Computer Network (BCS603)

⊘ Why is HTTP called a Stateless Protocol?

This is important!

HTTP is called **stateless** because:

✓ 💡 **It does not remember anything from the previous request.**

Every time you send a new request to the server, the server **doesn't know who you are or what you did before**.

🎁 Example of Stateless:

Let's say:

- You first open page1.html → Server gives you page1.
- Then you open page2.html → Server gives you page2.

But the server **doesn't remember** that you had opened page1 before.

It **treats each request as new**.

Computer Network (BCS603)

❖ Electronic Mail :

- **Electronic mail, commonly known as email, is a method of exchanging messages over the internet.**
- **Email (Electronic Mail)** is a way to **send messages** using the Internet.
  Just like sending a letter, but **digitally and instantly!**

✓ Here are the basics of email:

- An email address: This is a unique identifier for each user, typically in the format of name@domain.com.
- An email client: This is a software program used to send, receive and manage emails, such as Gmail, Outlook, or Apple Mail.
- An email server: This is a computer system responsible for storing and forwarding emails to their intended recipients.

Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

❖ Email Architecture – How Email Works (Simple Structure)

There are **3 main components** in email architecture:

1. User Agent (UA) – You, the user!

This is the **email app or software** like:

- Gmail
- Outlook
- Thunderbird

You use it to **write, read, and send emails.**

2. Mail Transfer Agent (MTA) – The post office

- It is the **software that sends your email to another computer.**
- Think of it as a **delivery van** that picks up your mail and finds the best route to deliver it.

Computer Network (BCS603)

3. Mail Delivery Agent (MDA) – The local postman

- It **receives the email** and **puts it into the receiver's inbox.**

Example Flow:

You send an email to your friend:

1.You write and send it via **User Agent** (like Gmail).
2.The message goes to the **MTA** (server like smtp.gmail.com).
3.The MTA sends it across the internet to your friend's **MTA**.
4.It reaches the **MDA** and then goes to your friend's inbox.
5.Your friend uses their **User Agent** to read the email.

Email Protocols :

- **SMTP**: Sends the email from your computer to the server (like a postman).
- **POP3**: Downloads the email to your computer, then deletes it from the server.
- **IMAP**: Lets you view emails without deleting from the server (used in mobile, Gmail).

1. SMTP (Simple Mail Transfer Protocol)

- **Used for sending emails**.
- Sends your email from your **email app to the mail server** or from **one server to another server**.

Example:

- When you send an email from Gmail, SMTP helps deliver it to the receiver's server.

Works only in one direction:

- You → Server → Receiver
- **Can't be used to receive or read emails.**

Port Number:

- Port **25** (standard)
- Port **587** (with encryption)

2. POP3 (Post Office Protocol version 3)

- **Used to receive emails.**
- It **downloads emails from the server to your device** and then **deletes them from the server**.

Example:

- You open your email app (like Outlook). It connects to the server, downloads all emails, and then the emails are gone from the server.

Good for:

- People who use **only one device** (like a personal laptop).

Not good for:

- Accessing the same email account on **multiple devices** (like mobile + PC), because once emails are downloaded, they are **not available anywhere else.**

Port Number:

- Port **110**

🌐 3. IMAP (Internet Message Access Protocol)

- **Used to receive emails**.
- But instead of downloading and deleting, it **lets you view emails directly from the server**.

🔹 Example:

- You open Gmail on your mobile, laptop, or tablet. You see the same inbox everywhere.
- Because emails **stay on the server** until **you delete them manually**.

🔹 Good for:

- People who use **multiple devices**.
- You can **sync, organize folders**, and even **search emails on the server**.

🔹 Port Number:

- Port **143** (non-secure)
- Port **993** (with encryption)

Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

📎 MIME (Multipurpose Internet Mail Extensions)

It extends the basic email format

MIME is a **standard** that allows **emails** to send:

- 🖼️ Images
- 📄 Documents (like PDF, Word)
- 🎵 Audio files
- 📹 Videos
- 💻 HTML content (fancy formatted text)

Originally, email could only send **plain text**, but thanks to MIME, you can now attach files and send rich content!

🌐 What is FTP?

FTP (File Transfer Protocol) is a **standard way to send or receive files** between two computers over the internet or a network.

- Imagine you want to **upload your website files** to your hosting server — FTP is the tool used for that.

💻 Example:

You made a website and now want to upload it to the internet.

You open an FTP client (like FileZilla), connect to the hosting server using your login, and **upload files** using drag and drop. Simple! ✅

Computer Network (BCS603)

⚙TFTP (Trivial File Transfer Protocol) :

- TFTP is a **very simple** way to **send and receive files** between computers on a network.
- Think of it like a very basic version of a courier that can **only deliver or pick up small files**, without asking too many questions.

🔸 Key Points:

✓ Used in **small networks** (like a computer lab or office).
✓ **No login or password** needed.
✓ **No fancy features**, just basic file transfer.
✓ Uses **UDP** (not TCP), so it's **fast but less reliable**.

🔸 Port Number:

- **69** (UDP)

Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

❖ 📡 FTP Connection Modes: Active vs Passive

When you use **FTP** to transfer files, the **way the connection is made** between your computer (Client) and the server can be either:

🟢 Active Mode 🟢 Passive Mode

Feature	⁉️ Active FTP	🟢 Passive FTP
📞 Who opens data connection	**Server** connects back to the client	**Client** connects to the server for data
🔐 Firewalls/NAT friendly	❌ Not friendly (because server tries to connect back)	✅ Better with firewalls and NAT
🔑 Port used by server	Server uses **port 20** for data	Server uses a **random port above 1024**
🔑 Port used by client	Client listens on a random port	Client initiates both control and data connections
🔧 Control connection port	Port **21** (same in both)	Port **21** (same in both)
👀 Use case	Older systems, trusted networks	Modern systems, secure environments with firewalls

Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

Ques : Explain the following terms : (AKTU 2022-23)

i.FTP ii. SMTP

iii. DNS iv. ARP

Ques. Difference between FTP and HTTP (AKTU 2023-24)

Ques : Write a short note on : (AKTU2021-22)

i. **FTP**
ii. **SMTP**
iii. **DNS**

Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

✓ What is SNMP?

SNMP (Simple Network Management Protocol) is a **protocol used to manage and monitor devices** like:

- Routers
- Switches
- Servers
- Printers
- Modems

Think of it like a **watchman** that keeps an eye on devices in a network and helps collect or change their information.

❖ Why SNMP is used?

- To **check device health** (Is it working properly?)
- To **monitor traffic or errors**
- To **get alerts** when something goes wrong (like a device goes offline)
- To **configure settings** on devices remotely

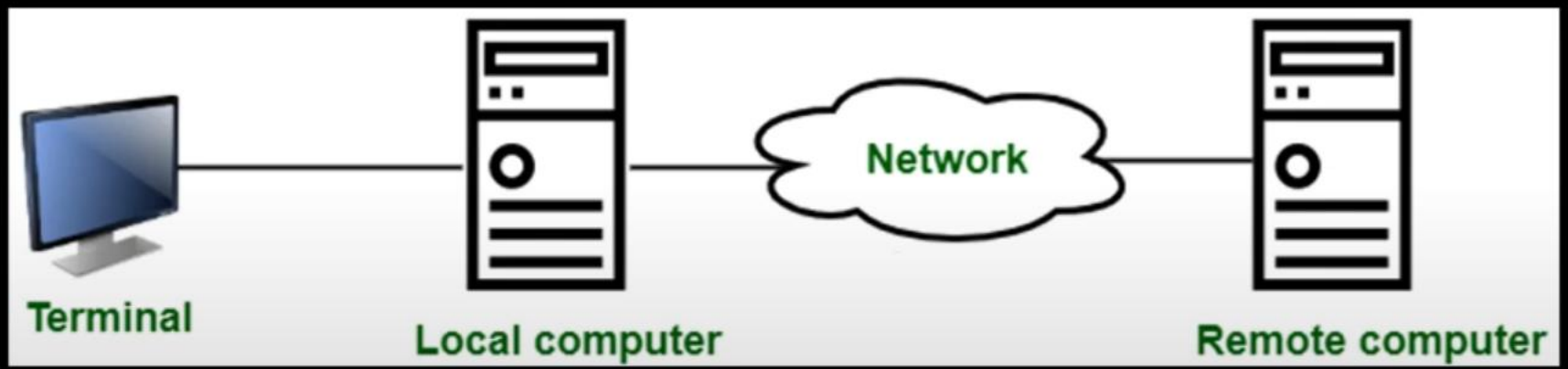
Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

What is Remote Login?

Remote login means **accessing another computer from far away** (remotely) over a network or the internet.

Imagine sitting at your home and using a computer that's in your office — as if you're sitting right in front of it. That's remote login!



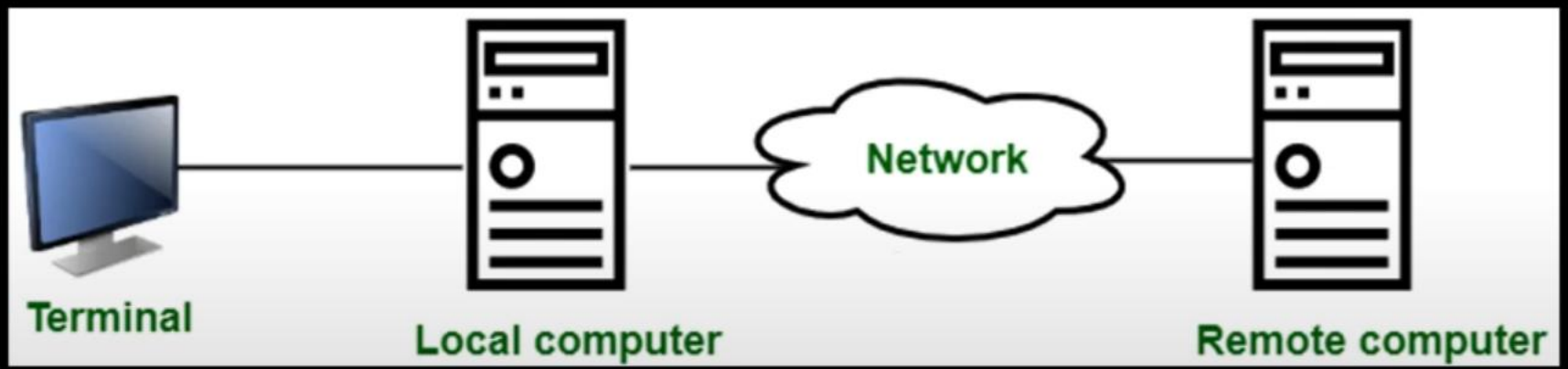
Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

What is Remote Login?

Remote login means **accessing another computer from far away** (remotely) over a network or the internet.

Imagine sitting at your home and using a computer that's in your office — as if you're sitting right in front of it. That's remote login!



Computer Network (BCS603)

🔐 TELNET is NOT Secure

- TELNET sends data (including usernames and passwords) as plain text.
- Anyone who intercepts the data can read it easily.
- That’s why it's mostly replaced by SSH (Secure Shell) now.

🛠️❓ How TELNET Works (Simple Steps):

- Client starts a TELNET session using a TELNET application or terminal.
- Client sends a connection request to the server's TELNET port (usually port 23).
- Server accepts the connection.
- User is prompted to enter a username and password.
- After login, user can type and execute commands on the remote server.
- When done, the user logs out and closes the session.

Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

🛡️❓ What is SSH?

SSH (Secure Shell) is a **secure network protocol** used to **remotely access and control** another computer or server **over a network or the internet**.

📌 You can think of SSH like a **secure version of TELNET** that keeps your login info and data safe with encryption.

SSH is mainly used by **network administrators, developers, and IT professionals** to:

- Remotely log in to servers
- Manage files
- Run commands
- Transfer files securely
- Set up secure tunnels between systems

Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

🔐 Why is SSH "Secure"?

- SSH **encrypts all data** you send and receive.
- Your **password, commands, files**—everything is safe and unreadable to hackers.
- Even if someone captures the data, they **can't understand it** without the encryption key.

🛠️ How SSH Works (Simple Steps):

1. **You open SSH client software** (like PuTTY or Terminal).
2. You type the command like:

```
ssh username@server-address
```

3. SSH connects to the **server's port 22** (default SSH port).
4. Server asks for your **password or key**.
5. Once verified, you're **logged into the server** and can start working securely.
6. You can now run commands as if you're using that computer locally.

Computer Network (BCS603)

EduShine CLASSES
By:- ARMAN ALI

❖ 📡 Network Management :

Network Management means taking care of a computer network so that it works smoothly, safely, and without any problems.
It includes **monitoring**, **maintaining**, **troubleshooting**, and **controlling** the devices and systems connected to a network—like computers, routers, switches, and servers.

🛠️❓ Main Goals of Network Management:

✓ Make sure the **network is working properly**.
✓ **Find and fix problems** quickly.
✓ **Protect** the network from hackers or data loss.
✓ **Improve performance** and avoid slow internet or crashing.

Computer Network (BCS603)

❖ Function of Network Management :

Area	What it Means (Easy Word)
1. Fault Management	Finding and fixing network problems (like broken links or down devices).
2. Configuration Management	Setting up and updating devices like routers and switches.
3. Performance Management	Checking speed, traffic, and ensuring everything runs fast.
4. Security Management	Protecting the network from viruses, hackers, and attacks.
5. Accounting Management	Tracking who is using how much data or bandwidth.

Computer Network (BCS603)

EduShine CLASSES By:- ARMAN ALI

Ques : Write Short note on : (AKTU 2018-19)

i. SMTP ii. TELNET

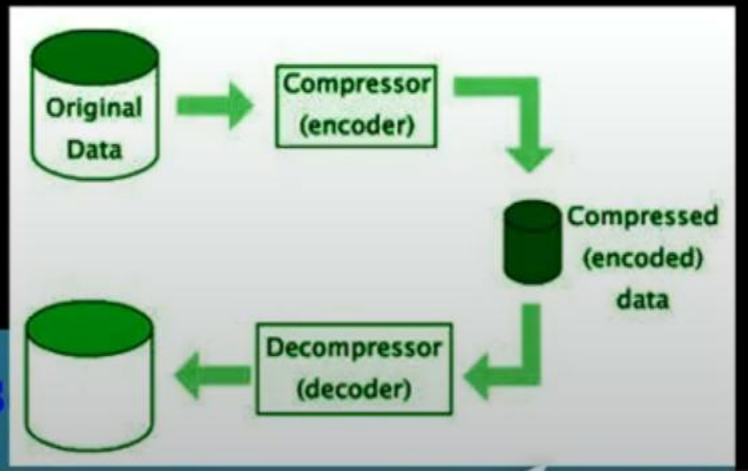
iii. HTTP

What is Data Compression?

Data Compression means **reducing the size of files or data** so that it takes **less storage space** or **less time to send over a network**.

It helps in:

- Saving space (e.g., smaller file size on your computer or phone).
- Faster upload/download on the internet.
- Sending files more easily via email or messaging.



Download Notes : https://rzp.io/rzp/dOh3

Why is it useful?

- To save memory or disk space.
- To reduce transmission time.
- To improve speed and efficiency in data communication.

Types of Data Compression:

1. Lossless Compression

No data is lost. You get back the **exact original file** after decompressing.

Features:

- Perfect for text, documents, or code (where every bit matters).
- Common formats: **ZIP**, **PNG**, **GIF**, **FLAC**.

Example:

If you compress a **text file or ZIP a folder**, after unzipping, you get exactly the same file—nothing is missing.

How it works:

It finds **repeating patterns** or **common characters** and replaces them with **shorter codes**.

🔸 2. Lossy Compression

☞ Some data is **lost during compression**, but it's done in a way you **don't usually notice** (especially for media like images, audio, or video).

✓ Features:

- Good for media files like **photos**, **music**, and **videos**.
- Smaller size but slightly reduced quality.
- Common formats: **JPEG**, **MP3**, **MP4**, **WEBP**.

Example:

If you save a photo in JPEG format, it may lose tiny details or colors—but it still looks good, and the file size becomes smaller.

🎁 How it works:

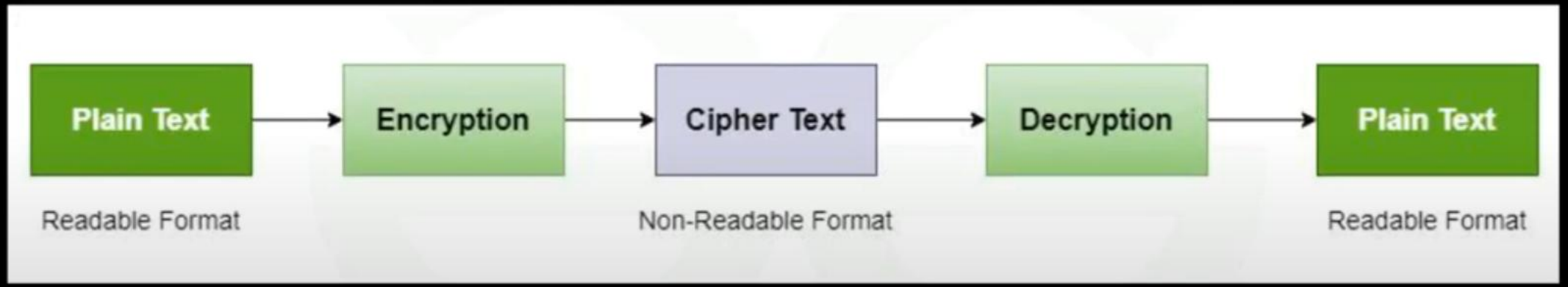
It removes **less important parts** of the data (like sounds you can't hear or colors you can't see clearly).

Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

What is Cryptography?

- **Cryptography** is a method of **protecting information** by turning it into a **secret code** so that only **authorized people** can understand it.
- It keeps your **messages, emails, passwords, and data safe** from hackers or others.
- It is widely used in **banking, chatting apps (like WhatsApp), websites, etc.**



Computer Network (BCS603)

EduShine CLASSES By:- ARMAN ALI

❖ **Basic Cryptography Process :**

- **Plain Text**: Original message in readable form. (e.g., "Hello Arman")
- **Encryption**: Process of converting plain text into unreadable text.
- **Cipher Text**: The scrambled or encoded message (not understandable).
- **Decryption**: Turning cipher text back into plain text.
- **Plain Text**: You get the original message back.

🗝️ **Types of Cryptography :**

There are **two main types**:

🔐 **1. Symmetric Key Cryptography (Same key used)**

- **Only ONE key** is used for both encryption and decryption.
- This key must be **shared secretly** between sender and receiver.
- Fast and simple method.

✅ **Example:**

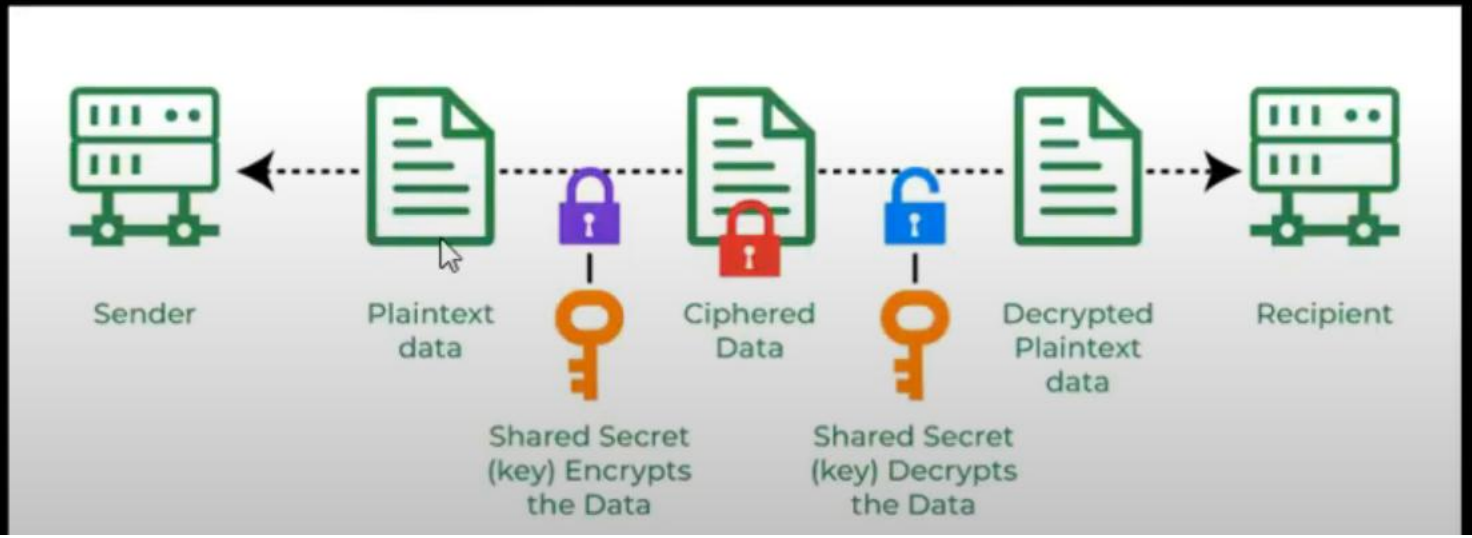
If Arman and Rohan share the same key, Arman encrypts a message with it, and Rohan uses the **same key** to decrypt it.

🔑 **Used In:**

AES, DES, Blowfish

📌 **Problem:**

Key distribution is risky—if someone steals the key, they can read the message.



Computer Network (BCS603)

🔐 2. Asymmetric Key Cryptography (Different keys used)

Uses **two keys**:

- **Public Key** (shared with everyone)
- **Private Key** (kept secret)

The sender encrypts using the **receiver's public key**, and only the receiver can decrypt it using their **private key**.

✅ Example:

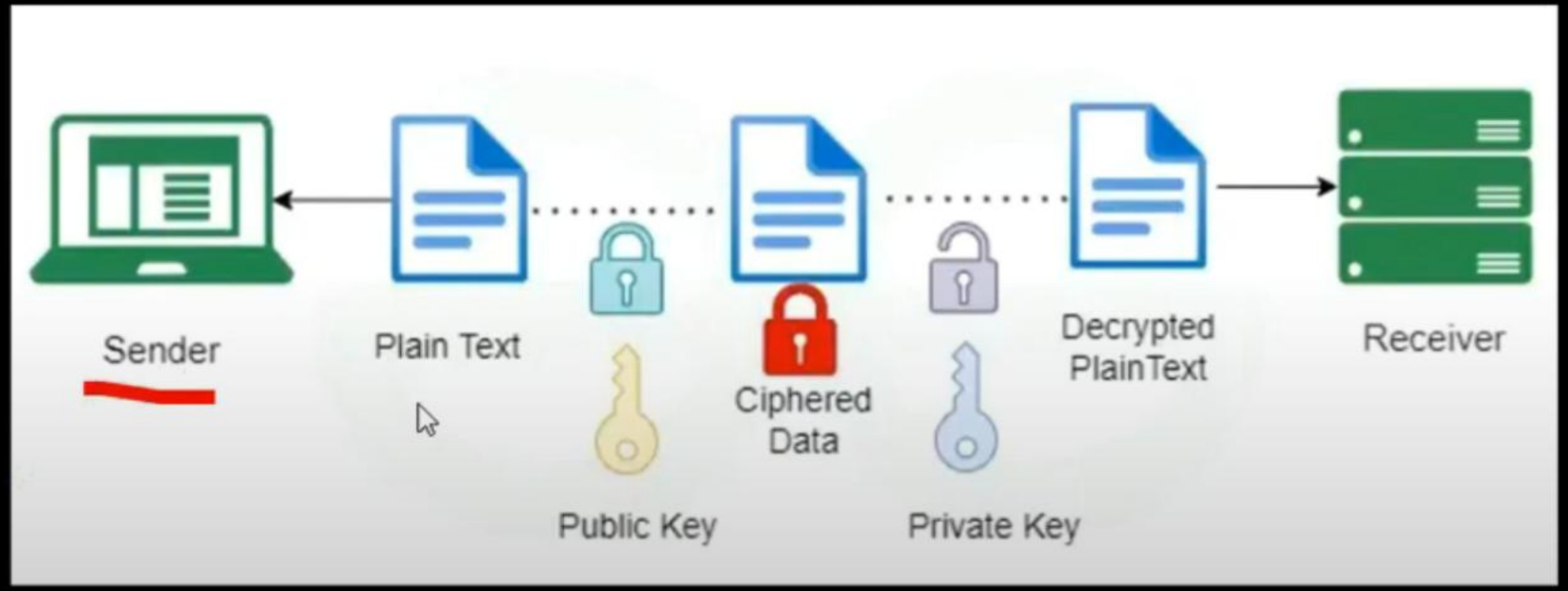
- Arman wants to send a message to Rohan.
- Arman encrypts using **Rohan's public key**.
- Rohan decrypts using his **own private key**.
- Even Arman cannot decrypt the message!

Used In:

RSA, ECC

Advantage:

More secure—no need to share a secret key.



Computer Network (BCS603)

EduShine CLASSES By:- ARMAN ALI

❖ Difference Between Symmetric key & Asymmetric Cryptography

Feature	Symmetric Key	Asymmetric Key
Keys Used	One key (same for both)	Two keys (public + private)
Speed	Fast	Slower
Security	Less secure (key sharing)	More secure (private key safe)
Examples	AES, DES	RSA, ECC
Used In	File encryption	Secure email, websites (HTTPS)

Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

🔐 What is RSA Algorithm?(V.V.V.IMP)

RSA (Rivest-Shamir-Adleman) is one of the most used **asymmetric encryption algorithms**.

- It uses **two keys**:
  - 🔑 **Public Key** → used to encrypt the data
  - 🔐 **Private Key** → used to decrypt the data
- It's mainly used in secure data transmission (like **HTTPS**, **email security**, **digital signatures**, etc.)
- It is an Asymmetric Cryptography algorithm.

Encryption : $C = P^e \bmod n$

Decryption : $P = C^d \bmod n$

❖ 📄 Simple Steps in RSA

Step 1: Choose Two Prime Numbers

Let's call them p and q

Example:

p = 3, q = 11

Step 2: Calculate n and ϕ(n)

- $n = p \times q = 3 \times 11 = 33$
- $\phi(n) = (p - 1) \times (q - 1) = (3 - 1) \times (11 - 1) = 2 \times 10 = 20$

Step 3: Choose Public Key e

- e must be a number such that:
  - $1 < e < \phi(n)$
  - e and ϕ(n) are **coprime** (no common factor other than 1)

Let's choose e = 7

Step 4: Calculate Private Key d

- d is such that $(d \times e) \bmod \phi(n) = 1$

We need:

$d \times 7 \bmod 20 = 1$

Try d = 3 → $3 \times 7 = 21$, and $21 \bmod 20 = 1$ ✓

So, d = 3

🔑 Keys are:

- **Public Key (e, n)** = (7, 33)
- **Private Key (d, n)** = (3, 33)

Let Data(P) = 8 (Plain text)

Now let first encrypt→

Encryption :

$C = P^e \bmod n$

$C = 8^7 \bmod 33 = 2$ (Cipher Text)

Now ,

Decryption :

$P = C^d \bmod n$

$P = 2^3 \bmod 33 = 8$ (Plain text)

Thank You...