# Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

## Unit -3 Network Layer

| | |
|---|---|
| **III** | **Network Layer:** Point-to-point networks, Logical addressing, Basic internetworking (IP, CIDR, ARP, RARP, DHCP, ICMP), Routing, forwarding and delivery, Static and dynamic routing, Routing algorithms and protocols, Congestion control algorithms, IPv6. |

Edushine Classes

# Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

## ❖ Introduction to Network Layer (Layer 3)

### ✓ Real-Life Example:(Shuru karte hai example se)

- Soch lo aap ek **courier service** ho (like Blue Dart 🚚).
- Koi banda aapko ek **parcel** deta jisme address likha hota hai (👉 **IP address**).
- Aap decide karte ho **kaunsa rasta** best hoga parcel ko pahunchane ke liye (👉 **Routing**).
- Aap parcel ko har ek city se guzarte hue **sahi ghar tak deliver** kar dete ho (👉 **Delivery**).
- Bas yehi kaam karta hai **Network Layer** in computer networks.

Now,

**Network Layer** is the **3rd layer** in the OSI model.

It is responsible for:

- **Assigning logical addresses (IP)**
- **Routing packets across different networks**
- **Delivering data from one computer to another**, even if they are on **different networks**

# Computer Network (BCS603)

EduShine CLASSES
By:- ARMAN ALI

| 🔢 No. | 📌 Function | 📖 Easy Explanation |
|---|---|---|
| 1. | **Logical Addressing** | Har device ko ek **unique IP address** dena – jaise har ghar ka alag postal address hota hai. |
| 2. | **Routing** | Decide karna kaunsa **best path** hoga data ko ek network se dusre tak le jaane ke liye. |
| 3. | **Packet Forwarding** | Ek router se dusre router tak data packets ko bhejna. |
| 4. | **Packet Delivery** | Ensure karna ki data **destination computer** tak sahi se pahunch jaaye. |
| 5. | **Fragmentation & Reassembly** | Agar data bada hai, to usse chhote-chhote **packets** mein todna (fragment), aur destination pe fir se jodna (reassemble). |
| 6. | **Error Handling (via ICMP)** | Agar route available nahi ya koi galti ho, to error message bhejna – jaise "Destination Unreachable". |

# Computer Network (BCS603)

EduShine CLASSES By:- ARMAN ALI

## 💡 Remember:

- Network Layer = Delivery manager of the internet world 🌍
- IP address = Address on the parcel
- Routing = Deciding best road
- Forwarding = Giving parcel to next courier guy (router)

## 📄 What is Point-to-Point Network?

A **Point-to-Point network** is a **direct connection between two nodes or devices** in a network.

There are **no intermediate devices** (like switches or routers) between them.

💡 Devices could be:

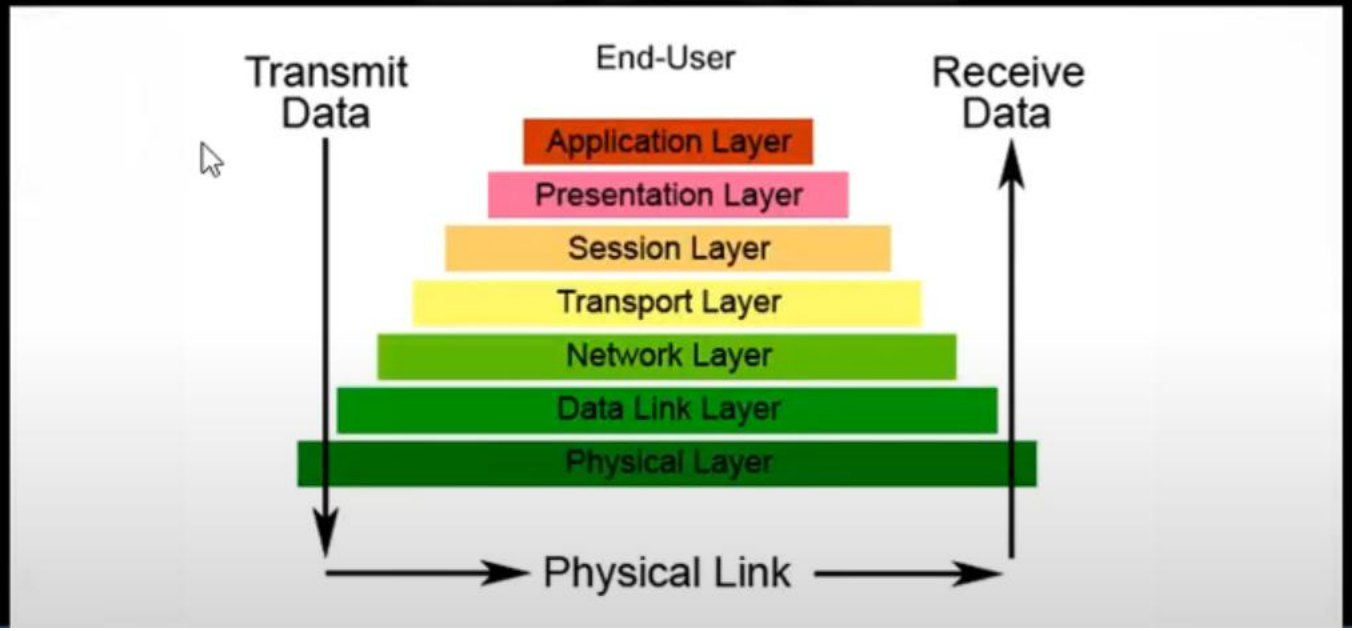
- Two computers
- Computer and printer
- Router and router
- Computer and server

# Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

## 📌 Characteristics:

- Only two endpoints (devices)
- Dedicated communication channel
- Mostly used in WANs or simple direct links



# Computer Network (BCS603)

EduShine CLASSES By:- ARMAN ALI

## ✅ Advantages of Point-to-Point Network

| 👍 Advantage | 📖 Easy Explanation |
|---|---|
| 1. Simple Design | Sirf 2 devices hote hain, isliye design aur setup easy hota hai. |
| 2. High Speed | Kyunki line dedicated hoti hai, speed fast hoti hai. |
| 3. Secure | Signal sirf do devices ke beech hota hai – no third-party device. |
| 4. Reliable | Kam chances of failure because only two devices are involved. |
| 5. Easy Troubleshooting | Agar kuch error ho toh sirf 2 devices check karne hain. |

# Computer Network (BCS603)

EduShine CLASSES
By:- ARMAN ALI

## ❌ Disadvantages of Point-to-Point Network

| 👎 Disadvantage | 📖 Easy Explanation |
|---|---|
| 1. Not Scalable | Sirf do hi devices connect ho sakte hain – bada network nahi bana sakte. |
| 2. Wastage of Resources | Agar dusri devices bhi connect karni ho, toh alag-alag lines chahiye hoti hain. |
| 3. Expensive for Large Networks | Agar har device ko doosre se connect karna ho, toh bahut saari cables lagenge |
| 4. Limited Use | Sirf small networks mein use hota hai, large networks mein nahi. |

# Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

## What is Logical Addressing?

A **Logical Address** is the **IP address** assigned to a device in a network to identify it uniquely at the network layer.

- Logical address is **not fixed** to hardware. It can **change**.
- It is assigned by software or a network admin.
- Example: **192.168.1.10** (IPv4 address)

**Real-Life Example**:

Soch ek **courier delivery system** hai.

- Har ghar ka **unique address** hota hai — city, street number, house number.
- Courier sirf address dekh ke **sahi jagah par deliver** hota hai.

**Computer networks** mein bhi aisa hi hota hai.

🔌 Har device (computer, mobile, server) ko network pe **ek unique address** diya jata hai — isse **Logical Address** kehte hain.

# Computer Network (BCS603)


## 🔍 Why is Logical Addressing Needed?

| 🧠 Reason | 💬 Explanation |
| --- | --- |
| Unique Identification | Har device ko pehchanne ke liye unique IP address chahiye. |
| Communication | Devices ek dusre ko address use karke locate karte hain. |
| Routing | Routers logical address dekh kar decide karte hain kis path se data bhejna hai. |

# Computer Network (BCS603)

EduShine CLASSES
By:- ARMAN ALI

## Logical Address vs Physical Address

| Feature | Logical Address (IP) | Physical Address (MAC) |
|---|---|---|
| Layer | Network Layer | Data Link Layer |
| Assigned by | Software (e.g. DHCP) | Hardware Manufacturer |
| Changeable? | Yes | No (mostly fixed) |
| Format | IPv4: 192.168.0.1 etc. | MAC: 00:1A:2B:3C:4D:5E |
| Scope | Globally Unique | Local Network Only |

# Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

## 🌐 What is Internetworking?

**Internetworking** means **connecting multiple different networks** together so that they can communicate with each other.

- **"Inter" = between**
- **"Networking" = connecting networks**

## 🏘️ Real-Life Example:

Imagine you live in a **society** with different **buildings**.
Each building is like a **network** (LAN).
Now, if you want to send a letter from one building to another, there needs to be a **system to connect all buildings** — like roads and delivery people.
That's what **internetworking** does — it connects different networks!

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

## Components Involved in Internetworking:

| Component | Role |
| --- | --- |
| Router | Connects different networks and forwards data using IP address |
| Gateway | Connects networks using different protocols |
| IP Addressing | Used to uniquely identify devices in different networks |
| Protocols | Rules that ensure communication is possible (like IP, TCP, etc.) |

# Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

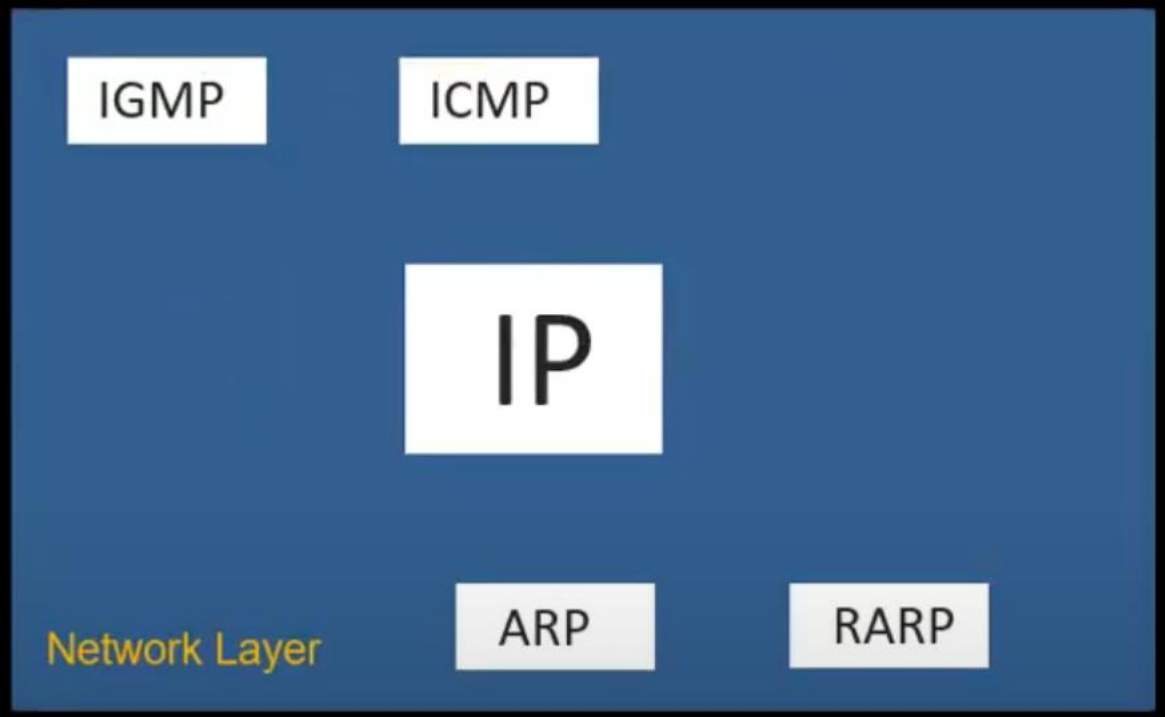
## Why Internetworking is Needed?

- To connect computers from different networks
- To form the **Internet** (a huge network of networks!)
- To share information globally
- To allow communication even if networks are built with different technologies

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

## ❖ Network Layer Protocol : (V.V.IMP)



# Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

❖ **IP Addressing :**

To understand IP Addressing, imagine this:

➢ You send a **parcel** to your friend who lives in another city.

You write the **address** on the box — house number, street, city, etc.

Without that address, the parcel would get lost, right?

📡 In the same way, when data (like a YouTube video, website, or message) travels across a network, it needs to know:

**Where it's coming from**

**Where it has to go**

☞ That's what **IP Addressing** does.

💡 **Definition:**

**IP Addressing** is the system used to **give a unique address to every device** (computer, phone, router, printer, etc.) on a network so that data can be sent and received properly.

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

## What is an IP Address?

IP = **Internet Protocol**

Address = **Location**

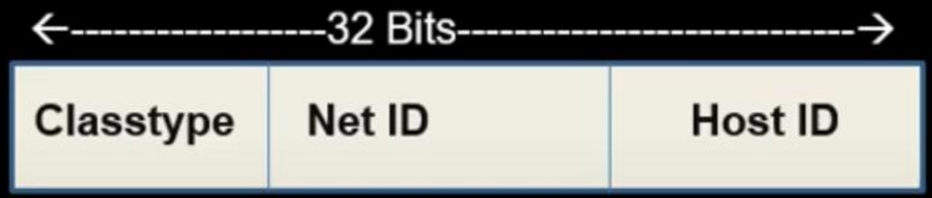
So, an IP address is the **digital address of your device** on a network or the internet.

## Example:

192.168.1.1 — This is a common format for an IP address.

It has **four parts** (called **octets**) separated by dots.

Each number ranges from 0 to 255.




## Why is IP Addressing Needed?

- To **identify devices** uniquely.
- To **send and receive data** correctly.
- To make **communication between devices possible**, like WhatsApp, YouTube, browsing, etc.

# Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

## ❖ Types of IP Addressing

There are **two major versions** of IP Addressing:

### i. ✓ IPv4 (Internet Protocol version 4)

- Format: 192.168.0.1
- Uses **32 bits**
- Has about **4.3 billion** unique addresses
- Most commonly used

### ii. ✓ IPv6 (Internet Protocol version 6)

- Format: 2400:cb00:2048:1::c629:d7a2
- Uses **128 bits**
- Has **trillions of addresses** (used as IPv4 is running out)

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

**Q1: Change the following IPv4 addresses from binary notation to dotted-decimal notation.**

**a.** 10000001 00001011 00001011 11101111

**b.** 11000001 10000011 00011011 11111111

**Q2: Change the following IPv4 addresses from dotted-decimal notation to binary notation.**

**a.** 111.56.45.78

Q: Find the error, if any, in the following IPv4 addresses.

a. 111.56.045.78

b. 221.34.7.8.20

c. 75.45.301.14

d. 11100010.23.14.67

# Computer Network (BCS603)


## Classification of IP Address :

To manage the huge number of devices, IPv4 addresses are **divided into 5 classes**: **Class A, B, C, D, and E**. These classes help in identifying how many devices (hosts) and networks can be handled by that address.

### i. ✓ Class A:

- Class A IP addresses start from **1 to 126** in the first part (octet).
- These are made for **very large organizations** like Internet Service Providers (ISPs).
- In Class A, **only the first part** of the IP address is used to identify the **network**, and the remaining **three parts** are used for **devices (hosts)**.
- Example of Class A IP address: 10.0.0.1

☞ It can support around **16 million hosts** in one network.

# Computer Network (BCS603)


### ii. ✓ Class B:

- Class B IP addresses range from **128 to 191** in the first octet.
- These are suitable for **medium-sized organizations**, such as universities.
- Here, the **first two parts** are for the **network**, and the **last two** are for **devices**.
- Example of Class B IP: 172.16.0.1

☞ It can support around **65,000 hosts** in each network.

### iii. ✓ Class C:

- Class C addresses range from **192 to 223** in the first octet.
- These are used for **small networks**, like small companies or home networks.
- In this class, the **first three parts** are used for **network** and only the **last part** is for **hosts**.
- Example: 192.168.1.1

☞ It supports only **254 devices** in one network.

# Computer Network (BCS603)


### iv. ✓ Class D:

- Class D addresses range from **224 to 239**.
- These are **not used for devices**.
- Class D is used for **multicasting**, where a message is sent to **multiple systems at once**.
- Example: 224.0.0.1

### v. ✓ Class E:

- Class E addresses range from **240 to 255**.
- These are **reserved for research and future use**.
- Not used in normal networks.

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

## ✓ Special Addresses:

- 127.0.0.1 → Called **loopback address**, used to test your own computer's network system.
- 0.0.0.0 → Means **unspecified address** or **this network**.
- 255.255.255.255 → Used for **broadcasting** to all devices in the network.

This classification helps divide IP addresses for different sizes of networks and purposes. It also helps routers and computers understand how to manage the network and communicate efficiently.

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

## 🌐 What is Subnetting?

**Subnetting** is the process of **dividing a large network (IP address block)** into **smaller, manageable pieces**, called **subnets**.

**Real-Life Example:**

Suppose you are the head of a big **college campus**. The whole campus has one big internet connection (one IP block), but you want:

- One network for **Admin Office**
- One for **Computer Labs**
- One for **Hostels**
- One for **Faculty Rooms**

Instead of giving the same network to all, you **break the main network into 4 parts (subnets)**. This is called **subnetting**.

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

## ❖ Default Subnet Mask :

| IP Class | Default Subnet | Network Bits | Host Bits | Total Hosts |
|---|---|---|---|---|
| A | 255.0.0.0 | First 8 bits | Last 24 bits | 16,777,216 |
| B | 255.255.0.0 | First 16 bits | Last 16 bits | 65,536 |
| C | 255.255.255.0 | First 24 bits | Last 8 bits | 256 |

**Q. You have given an IP Address Find Network Address ?**
**IP : 192.168.1.152**

**Hint : Network Address = IP Address(in Binary) AND Subnet Mask(in Binary)**

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

## Why is Subnetting important?

- ✓ Reduces networks traffic
- ✓ Increases security (each subnet is isolated)
- ✓ Helps organize big networks
- ✓ Efficient use of IP addresses

# Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

**Q. 1 Divide the network with IP Address 200.1.2.0 into two subnets.(V.IMP)**

**Step-by-step Solution:**

**1. Identify the class of the IP**

- 200.1.2.0 is a **Class C** IP address.
- Default subnet mask for Class C: 255.255.255.0 (i.e., /24)

**2. How many subnets?**

- We need **2 subnets**.
- To create subnets, we borrow bits from the host portion.

**Formula: 2^n >= Number of subnet.**

**Here, 2 Subnet Required →**

**2^1 =2**

**3. New subnet mask**

- Original subnet mask: /24
- After borrowing 1 bit: /25
- New subnet mask: 255.255.255.128

# Computer Network (BCS603)


## 4. Determine the subnets

With a /25 subnet mask, each subnet has:

$2^{32-25} = 128$ addresses (including network and broadcast)

✓ **Let's Divide the 256 IPs (0 to 255) into Two Subnets:**

### Subnet 1

- **Starts at**: 200.1.2.0
- **Has 128 IPs** → So it goes up to: 0 + 127 = 127
- **Network Address**: 200.1.2.0
- **First Usable IP**: 200.1.2.1
- **Last Usable IP**: 200.1.2.126
- **Broadcast Address**: 200.1.2.127

✓ **Broadcast Address = Network Address + (Total IPs - 1)**

## Subnet 2

- **Starts at**: 200.1.2.128 (right after Subnet 1 ends)
- **Has 128 IPs** → So it goes up to: 128 + 127 = 255
- **Network Address**: 200.1.2.128
- **First Usable IP**: 200.1.2.129
- **Last Usable IP**: 200.1.2.254
- **Broadcast Address**: 200.1.2.255

# Computer Network (BCS603)


## Q. 2 Divide the Network with IP address 200.1.2.0 into 5 subnets.(V.IMP)

**Step-by-step Solution:**

**1. Identify the class of the IP**

- 200.1.2.0 is a **Class C** IP address.
- Default subnet mask for Class C: 255.255.255.0 (i.e., /24)

**2. How many subnets?**

- We need **5 subnets**.
- To create subnets, we borrow bits from the host portion.

**Formula: 2^n >= Number of subnet.**

**Here, 5 Subnet Required →**

**2^3 >=8**

**3. New subnet mask**

- Original subnet mask: /24
- After borrowing 3 bit: /27 → Means 27 (ones) 5 (Zero)
- New subnet mask: 255.255.255.224

## 4. Determine the subnets

With a /27 subnet mask, each subnet has:

$2^{32-27}$ = 32 addresses (including network and broadcast)

But out of 32:

- 1 is for **network address**
- 1 is for **broadcast address**

So **30 usable IPs per subnet**

## Step 3: List the 5 subnets

| Subnet | Network Address | Usable IP Range | Broadcast Address |
|---|---|---|---|
| 1 | 200.1.2.0 | 200.1.2.1 – 200.1.2.30 | 200.1.2.31 |
| 2 | 200.1.2.32 | 200.1.2.33 – 200.1.2.62 | 200.1.2.63 |
| 3 | 200.1.2.64 | 200.1.2.65 – 200.1.2.94 | 200.1.2.95 |
| 4 | 200.1.2.96 | 200.1.2.97 – 200.1.2.126 | 200.1.2.127 |
| 5 | 200.1.2.128 | 200.1.2.129 – 200.1.2.158 | 200.1.2.159 |

# Computer Network (BCS603)

EduShine CLASSES
By:- ARMAN ALI

## ✅ Final Answer (Subnet Mask: /27 = 255.255.255.224):

| Subnet No. | Network | First IP | Last IP | Broadcast |
|---|---|---|---|---|
| 1 | 200.1.2.0 | 200.1.2.1 | 200.1.2.30 | 200.1.2.31 |
| 2 | 200.1.2.32 | 200.1.2.33 | 200.1.2.62 | 200.1.2.63 |
| 3 | 200.1.2.64 | 200.1.2.65 | 200.1.2.94 | 200.1.2.95 |
| 4 | 200.1.2.96 | 200.1.2.97 | 200.1.2.126 | 200.1.2.127 |
| 5 | 200.1.2.128 | 200.1.2.129 | 200.1.2.158 | 200.1.2.159 |

# Computer Network (BCS603)

EduShine CLASSES By:- ARMAN ALI

Q.3 The IP network **200.198.160.0** is using subnet mask **255.255.255.224** → i.e., **/27**

**Draw the subnets.**

**Sol : Try your self don't directly see the answer.**

| Subnet No. | Network Address | First Usable IP | Last Usable IP | Broadcast Address |
|---|---|---|---|---|
| 1 | 200.198.160.0 | 200.198.160.1 | 200.198.160.30 | 200.198.160.31 |
| 2 | 200.198.160.32 | 200.198.160.33 | 200.198.160.62 | 200.198.160.63 |
| 3 | 200.198.160.64 | 200.198.160.65 | 200.198.160.94 | 200.198.160.95 |
| 4 | 200.198.160.96 | 200.198.160.97 | 200.198.160.126 | 200.198.160.127 |
| 5 | 200.198.160.128 | 200.198.160.129 | 200.198.160.158 | 200.198.160.159 |
| 6 | 200.198.160.160 | 200.198.160.161 | 200.198.160.190 | 200.198.160.191 |
| 7 | 200.198.160.192 | 200.198.160.193 | 200.198.160.222 | 200.198.160.223 |
| 8 | 200.198.160.224 | 200.198.160.225 | 200.198.160.254 | 200.198.160.255 |

# Computer Network (BCS603)


## ❖ IPv4 Header Format : (V.V.VIMP)

The **IPv4 Header** is the **first part** of an IPv4 packet that contains all the **important information** required for delivering the packet from the **source to the destination**.

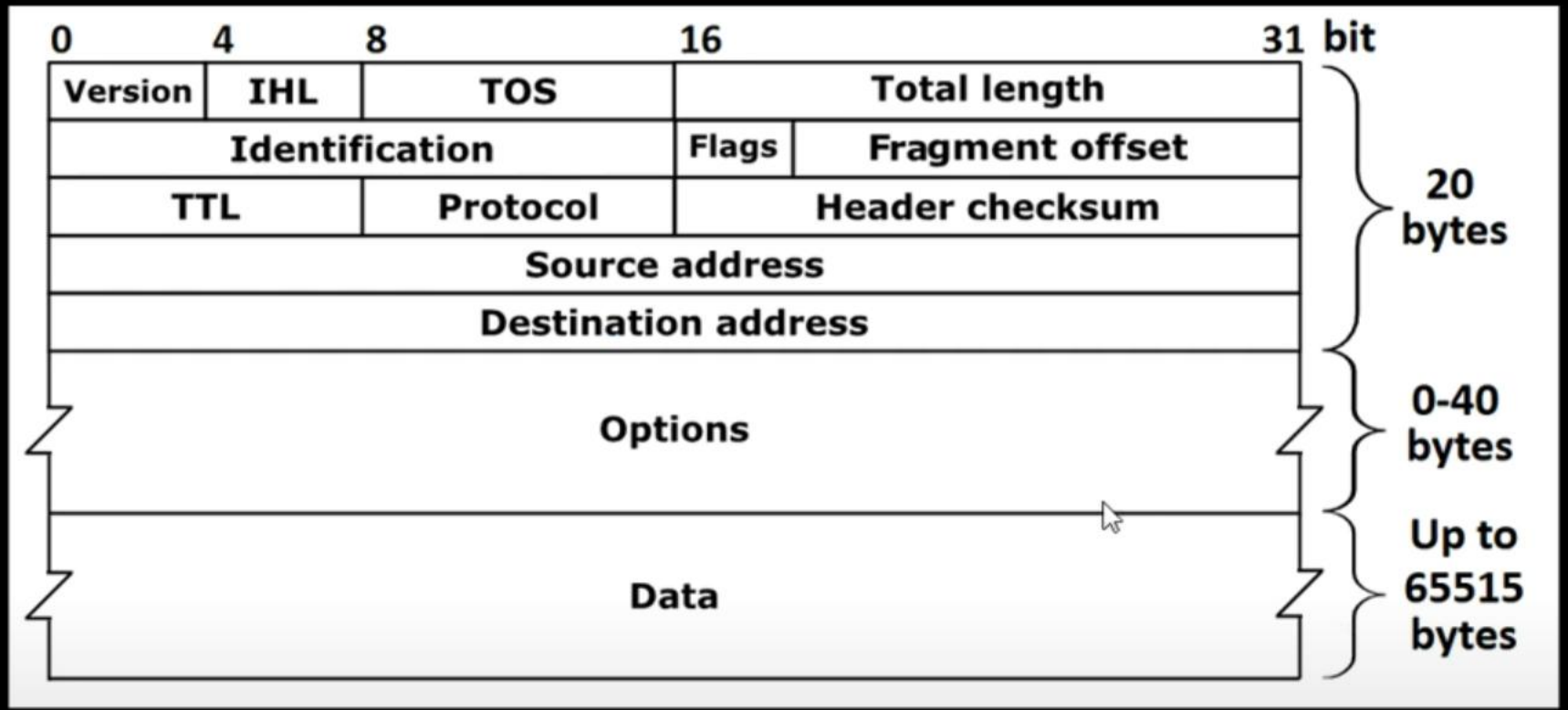
It tells routers and devices:

- Who sent the data?
- Who should receive it?
- How big is the packet?
- How long the packet can live on the network?
- What kind of data is inside?

Imagine you're **sending a WhatsApp message** from your phone to a friend over the internet. This message goes through routers, cables, and many networks. It is broken into **packets**, and **each packet has a header** — like an envelope has sender, receiver, and instructions.

Let's now look at **each field** of the IPv4 header, like we are opening this envelope:

# Computer Network (BCS603)




✓ **Size of IPv4 Header:**

**Minimum size:** 20 bytes (when there are no options)

**Maximum size:** 60 bytes (when options are included)

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

### ✓ 1. Version (4 bits)

**Kya hai?** Ye batata hai ki IP kaunsa version use ho raha hai.
**IPv4 ke liye hamesha 4 hota hai.**
**Example:** If it's IPv6, this value would be 6.
**Think like:** "Which format is the envelope written in?" — Answer: Version 4 format.

### ✓ 2. IHL (Internet Header Length) (4 bits)

**Kya hai?** Ye batata hai ki header kitne words ka hai.
1 word = 4 bytes. Minimum value is **5** → 5 × 4 = **20 bytes** (default IPv4 header size).
Agar options add ho, toh header size badh sakta hai.
**Example:** If IHL = 6, then header = 6×4 = 24 bytes.
💡 **Think like:** "Kitna space envelope ke upar likhne me lag gaya?"

# Computer Network (BCS603)


## ✓ 3. Type of Service (TOS) or Differentiated Services (8 bits)

**Kya hai?** Ye batata hai ki packet kitna important hai — priority.

Example: Voice call packets should get faster delivery than a file download.

**Example:**

Video call → High priority (TOS set to high)

Email → Normal priority

💡 **Think like:** "Is this urgent mail or normal mail?"

## ✓ 4. Total Length (16 bits)

**Kya hai?** Ye pura packet ka size batata hai — header + data.

Maximum = 65,535 bytes (2^16 - 1)

**Example:**

Header = 20 bytes

Data = 980 bytes

Total = 1000 bytes

💡 **Think like:** "Kitna bada envelope + letter mila?"

## ✓ 5. Identification (16 bits)

**Kya hai?** Agar ek bada message chhoti packets me divide kiya gaya hai, toh sab packets ka **same ID** hota hai.

Router is ID se samajhta hai ki ye pieces ek hi message ke hain.

**Example:**

Suppose 1 video file is broken into 4 packets. All 4 will have the same ID = 12345.

💡 **Think like:** "All parts of the same courier have same tracking ID.“

## ✓ 6. Flags (3 bits)

**Kya hai?** Ye batata hai ki packet ko todna hai ya nahi.

3 bits:

Bit 0: Reserved (always 0)

Bit 1: DF (Don't Fragment)

Bit 2: MF (More Fragments)

**Example:**

DF = 1 → Don’t break this packet

MF = 1 → More parts are coming

💡 **Think like:** "Courier ko tod ke bhejna allowed hai ya nahi?"

# Computer Network (BCS603)


## ✓ 7. Fragment Offset (13 bits)

- **Kya hai?** Jab packet break hota hai, to har part kis order me hai, wo yahan likha hota hai.
- Helps in **reassembling** the original data.

**Example:**

- 1st packet: Offset = 0
- 2nd packet: Offset = 1480 (assuming 1480 bytes/piece)
- 3rd: Offset = 2960, and so on.

💡 **Think like:** "Is piece ki original jagah kaun si hai?"

## ✓ 8. Time to Live (TTL) (8 bits)

**Kya hai?** Ye batata hai ki packet kitni der tak zinda rahe.

Har router se pass hone par TTL -1 hota hai.

Agar TTL = 0 → Packet is dropped.

**Example:**

- TTL = 64
- After 10 routers → TTL = 54
- If reaches 0 → Discarded

💡 **Think like:** "Kitni der tak courier zinda rahega, warna expire."

### ✓ 9. Protocol (8 bits)

**Kya hai?** Ye batata hai ki data kis protocol ke liye hai — TCP, UDP, ICMP etc.

- Most common values:
- TCP → 6
- UDP → 17

**Example:**

- WhatsApp call → UDP
- Webpage loading → TCP

💡 **Think like:** "Ye envelope kiske liye hai — chat, call ya email?"

### ✅ 10. Header Checksum (16 bits)

- **Kya hai?** Ye ek error checking value hoti hai — sirf header ke liye.
- Agar header me koi galti ho gayi, toh packet discard ho jata hai.

**Example:** Router checks the checksum and finds a mismatch → Drops the packet.

💡 **Think like:** "Envelope par likha address galat hai ya sahi?"

### ✅ 11. Source IP Address (32 bits)

- **Kya hai?** Jo IP address ne packet bheja, uska address.
- Format: 192.168.1.1

**Example:** You send the message from your device → Source IP: 192.168.0.101

💡 **Think like:** "Courier kisne bheja?"

### ✅ 12. Destination IP Address (32 bits)

- **Kya hai?** Jis IP ko packet milna hai — receiver.
- Format: 192.168.1.2

**Example:** Your friend's device IP: 192.168.0.102

💡 **Think like:** "Courier kisko bhejna hai?"

### ✓ 13. Options (0 to 40 bytes)

**Kya hai?** Optional field — rarely used. Extra instructions de sakte ho jaise route record, timestamp etc.

**Example:** You want packet to pass through a specific path → write option.

💡 **Think like:** "Special note likhna hai toh yahan likh."

### ✓ 14. Padding

**Kya hai?** Options field ke baad agar extra space bacha ho, toh usme zero add karte hain so that header is multiple of 4 bytes.

💡 **Think like:** "Blank space fill karna envelope me so that size fix ho."

## ❖ IPv6 Header Format : (V.V.VIMP)

IPv6 is the latest version of Internet Protocol used for communication over the internet.

When data is sent from one device to another, it travels in small pieces called **packets**.

Each IPv6 packet has a **header** — a section that contains important information about the packet.

IPv6 header is **simpler and more efficient** than IPv4.

It has **8 fixed fields** and the size is always **40 bytes**.

### Let's Understand Each Field in Detail:

### 1. Version (4 bits)

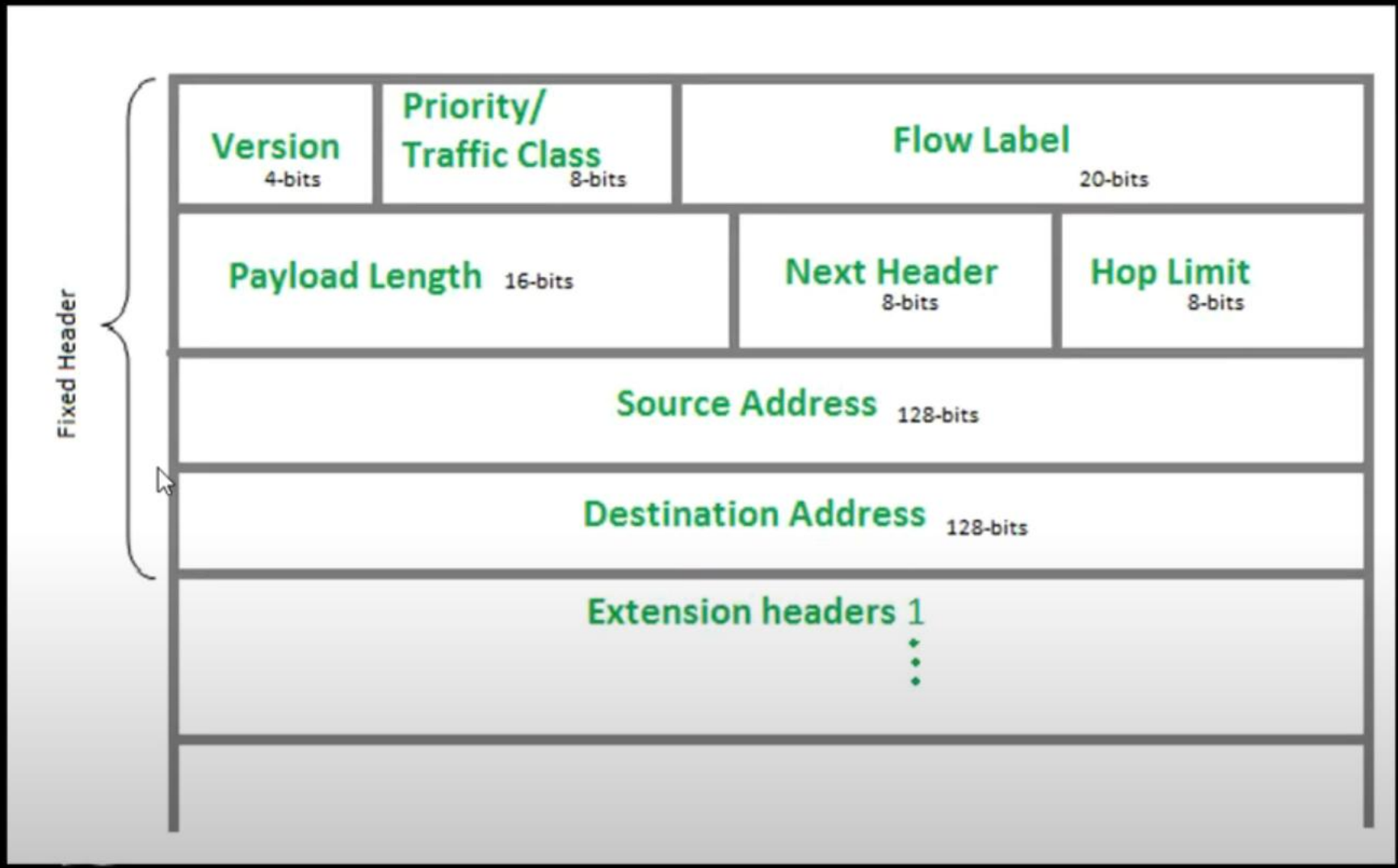
This field tells which IP version is being used.

In IPv6, the version value is always 6.

📄 **Example**:

Think of it like a tag on a letter that says "This is Version 6 message".

# Computer Network (BCS603)



**2. Traffic Class (8 bits)**

It is used to define the priority of the packet — which packet should be handled first.
Important data like voice or video can be given higher priority.

📘 **Example:**

If you're doing a video call and downloading a file at the same time, the video call gets higher priority through this field.

**3. Flow Label (20 bits)**

This field is used to group related packets.
All packets of a video stream or a game can be given the same flow label to help routers identify them quickly.

📘 **Example:**

Imagine you're watching a movie. All packets of that movie get a tag (e.g., Flow 12345), so routers treat them as a single group.

### 4. Payload Length (16 bits)

It tells how much actual data is being sent **(excluding the header)**.

Maximum payload size is 65,535 bytes.

📄 **Example:**

If you're sending a document of 1000 bytes, this field will have the value 1000.

### 5. Next Header (8 bits)

This tells what comes **after** the IPv6 header.

It indicates which transport layer protocol is used — like TCP (6), UDP (17), etc.

📄 **Example:**

If the data inside is a web page, TCP might be used. So, this field will have 6 (for TCP).

### 6. Hop Limit (8 bits)

This field defines how many routers the packet can pass through before it is discarded.

Each router decreases this value by 1. If it becomes 0, the packet is dropped.

📄 **Example:**

Think of it like a packet has 10 lives. After each router, it loses one life. If it hits zero, the packet dies.

### 7. Source Address (128 bits)

This is the IP address of the sender – where the packet is coming from.

📄 **Example:**

If you are sending a message, your device's IPv6 address will be written here, like 2001:abcd::1.

### 8. Destination Address (128 bits)

This is the IP address of the receiver – where the packet should go.

📄 **Example:**

If your friend is receiving the data, his/her device's IPv6 address will be here, like 2001:abcd::2.

## Real-Life Example:

Let's say you are watching a YouTube video:

- Your device's IP: 2001:abcd::1
- YouTube server's IP: 2404:6800:4001::200e
- Data size: 2000 bytes
- Protocol used: TCP

So the IPv6 header would be:

- **Version**: 6
- **Traffic Class**: High (for video)
- **Flow Label**: 4321
- **Payload Length**: 2000
- **Next Header**: 6 (TCP)
- **Hop Limit**: 64
- **Source Address**: 2001:abcd::1
- **Destination Address**: 2404:6800:4001::200e

# Computer Network (BCS603)


## ❖ Advantages of IPv6 over IPv4:

The next generation of the Internet Protocol is **IPv6**, and it solves many problems that existed in **IPv4**. Here are the main benefits:

### 1. ✓ Larger Address Space

**IPv4** has only **4.3 billion IP addresses**, and most of them are already used.
**IPv6** supports around **340 trillion trillion trillion (2^128) addresses**.

**Easy Example**:

Imagine IPv4 is like having 4 billion phone numbers, but the world has more people now. IPv6 gives *unlimited numbers*, so every device can have its own IP.

### 2. ✓ No Need for NAT (Network Address Translation)

In IPv4, we use **NAT** because there aren't enough IPs, so many devices share one.
In IPv6, each device can have a **unique IP address**.

**Easy Example:**

With IPv6, your phone, laptop, smart TV – all can have their own public IP. No need to share.

### 3. ✓ Simpler and Faster Routing

IPv6 uses a **simpler header**, which makes packet processing **faster**.
Helps routers work more efficiently.

**Easy Example:**

It's like giving a bus a shorter route and fewer signals – it reaches faster

### 4. ✓ Built-in Security (IPSec)

IPv6 was designed with **security in mind**.

It supports **encryption and authentication** by default using IPSec.

**Easy Example**:

IPv6 adds a lock and ID card to every message for safe delivery.

### 5. ✓ Better Support for Mobile Devices

IPv6 handles **mobile communication** better with features like **Mobile IPv6**.

Helps in seamless connection when devices move between networks.

**Easy Example**:

When your phone switches from WiFi to mobile data, IPv6 keeps the connection smooth.

# Computer Network (BCS603)


### 6. ✓ Improved Quality of Service (QoS)

IPv6 supports better handling of important traffic like voice or video.

**Easy Example:**

Important deliveries (like video calls) are prioritized like an ambulance on the road.

### 7. ✓ No Broadcast, Uses Multicast Instead

IPv6 avoids network congestion by using multicast, not broadcast.

**Easy Example:**

Instead of shouting to everyone (broadcast), it quietly sends data only to those who need it (multicast).

# Computer Network (BCS603)

EduShine CLASSES By:- ARMAN ALI

| Feature | IPv4 | IPv6 |
|---|---|---|
| Full Form | Internet Protocol version 4 | Internet Protocol version 6 |
| Address Size | 32 bits | 128 bits |
| Total IP Addresses | Around 4.3 billion | 340 undecillion (almost unlimited) |
| IP Address Format | Decimal (e.g., 192.168.1.1) | Hexadecimal (e.g., 2001:0db8:85a3::8a2e:0370:7334) |
| Header Size | 20–60 bytes (variable) | 40 bytes (fixed) |
| Configuration | Manual or DHCP | Auto-configuration supported |
| Security | Not built-in (optional IPSec) | Built-in security (IPSec mandatory) |
| NAT Needed? | Yes (due to less IPs) | No (enough addresses for everyone) |
| Broadcast Support | Uses Broadcast | Doesn't use Broadcast, uses Multicast instead |
| Routing | Complex | Simplified and faster |
| Mobile Support | Limited support | Better support for mobile devices |

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

❖ **What is CIDR (Classless inter domain routing) –**

**Chalo ek mast example se samjhte hai**

💡 **Imagine This First:**

Tere paas ek packet of 100 chocolates hai (jaise IP addresses).

Tere 3 dost hain:

i. Arman: Use chahiye 2 chocolates

ii. Salim: Use chahiye 30 chocolates

iii. Riya: Use chahiye 70 chocolates

Ab tu kya karega?

Tu 33-33-33 karke sabko de dega? ✗ Waste hoga chocolates ka.

Ya fir sirf jitna unhe chahiye, utna dega? ✓ Sahi way.

# Computer Network (BCS603)


➢ **Same Problem Internet mein bhi tha!**

Pehle internet ke IP addresses ko **Class A, B, C** mein divide kiya tha.

Jise hum **Classful addressing** bolte hain.

- Class A: 1 crore se zyada IPs
- Class B: 65,000+ IPs
- Class C: 256 IPs

But socho, agar kisi ko sirf 50 IP chahiye aur usse Class C mil gaya = 256 IPs ka **waste** ho gaya.

**Solution kya tha?**

➞ **CIDR** (Classless Inter-Domain Routing)

- CIDR is a method to **efficiently allocate IP addresses** and **reduce wastage**.
  It removes the **fixed class system (A, B, C)** and allows **flexible subnetting**.

# Computer Network (BCS603)


CIDR ek aisa system hai jo IP addresses ko **flexible way mein divide karta hai** — bina Class A, B, C ke.

CIDR bolta hai:

"Main tumhe utne IP address dunga jitne tumhe chahiye. Na zyada, na kam."

❖ ◈ **What is ARP (Address Resolution Protocol)? —**

ARP ka kaam hota hai:

**IP address se MAC address dhoondhna**.

Imagine :

- Tu kisi society mein rehta hai (Network).
- Tu jaanta hai kisi ka **naam (IP address)**, par tu uske **ghar ka exact address (MAC address)** nahi jaanta.
- To tu chowkidar (ARP) se puchhta hai:

"Bhai, 192.168.1.3 ka ghar kaun sa hai?"

•Chowkidar de deta hai: “Iska MAC address: AB-CD-EF-12-34-56”

➞ Yehi kaam **ARP** karta hai computer network mein.

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

**ARP** stands for **Address Resolution Protocol**.

It is used to **find the MAC (Media Access Control) address** of a device **when its IP address is known**.

→ **In simple terms**:

When a computer wants to send data to another computer on the same network, it knows the IP address, but it needs the MAC address to send the data.

**ARP helps to find that MAC address.**

**Now let understand its Working how it works means let see an example →**

✓ **Example:**

Suppose:

- Your computer has IP: 192.168.1.2
- You want to send data to IP: 192.168.1.3
- But you don't know the MAC address of 192.168.1.3

**Step-by-step:**

**1. ARP Request:**

Your computer sends a message to the network saying:
"Who has IP address 192.168.1.3? Tell me your MAC address."
This request is **broadcasted** to all devices on the network.

## 2. ARP Reply:

The device with IP 192.168.1.3 replies:

"Yes, I have this IP. My MAC address is AA:BB:CC:DD:EE:FF."

Now your computer stores this information and sends the data to that MAC address.

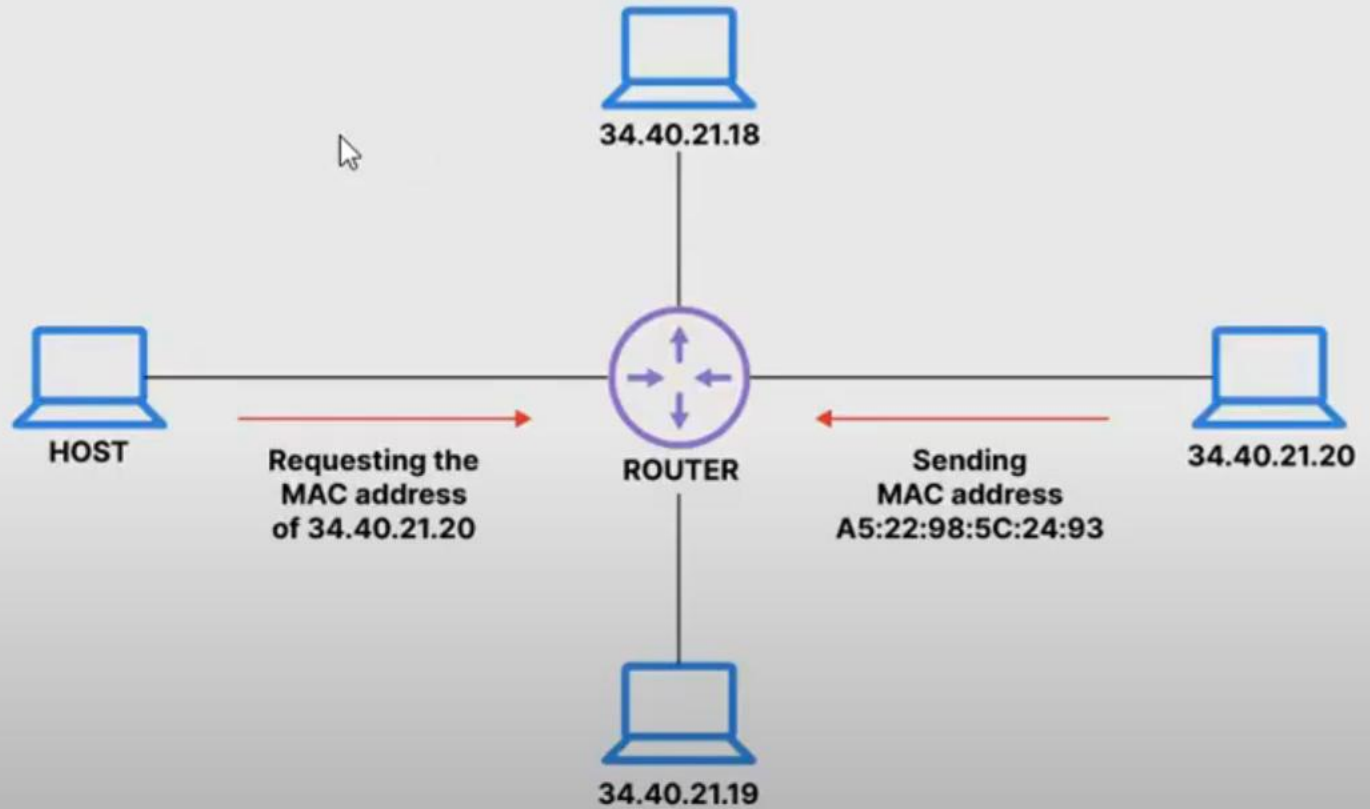
## ✓ ARP Table:

Every computer keeps a **small table** called the **ARP Cache**, which stores:

- IP address
- Corresponding MAC address

This avoids sending ARP requests every time.

# How Address Resolution Protocol (ARP) Works



# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

## 🔁 What is RARP?

**Full Form**: Reverse Address Resolution Protocol

**Purpose**:

While ARP finds the MAC address from an IP address,

**RARP does the opposite** – it finds the **IP address** when the **MAC address** is known.

## 🔧 Why do we need RARP?

Imagine a device (like an old computer or printer) that **only knows its MAC address**, but doesn't know what its **IP address** is.

It needs an IP address to communicate on a network.

So it uses **RARP** to ask:

"Hey! My MAC address is AA:BB:CC:DD:EE:FF. Can someone please tell me my IP address?"

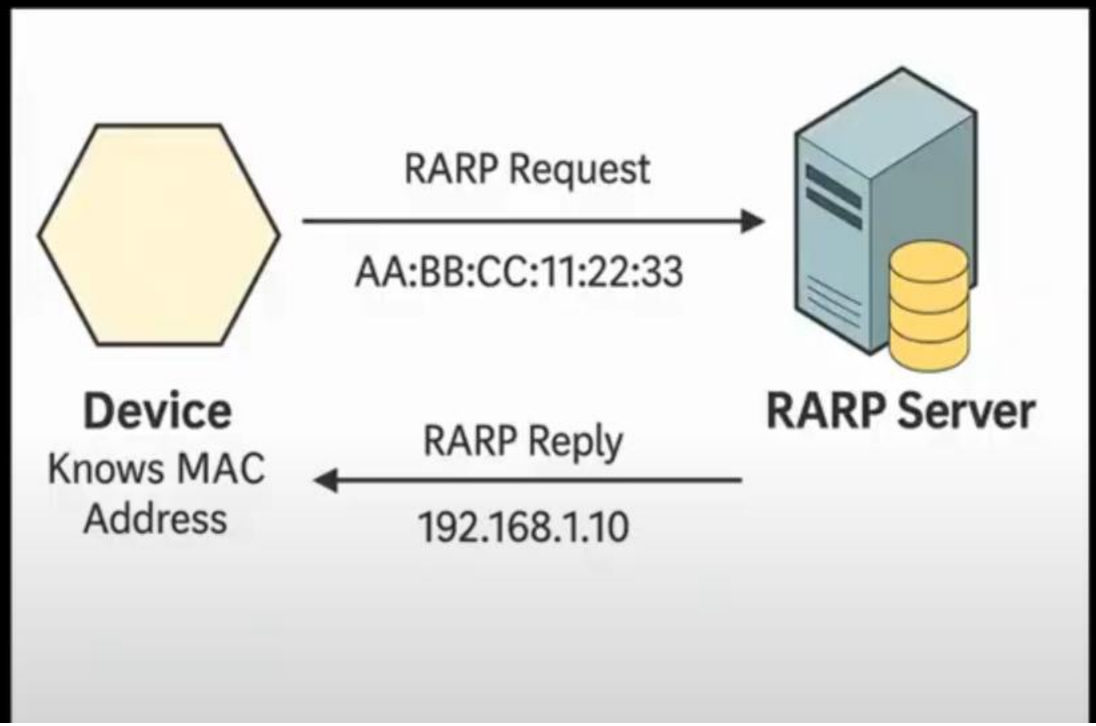
# Computer Network (BCS603)

EduShine CLASSES
By:- ARMAN ALI

**Example:**

Let's say a computer has this MAC address:
AA:BB:CC:11:22:33
It sends a RARP request to the network.
The RARP server replies:
"Your IP address is **192.168.1.10**"
Now the computer knows both:

- Its MAC: AA:BB:CC:11:22:33
- And its IP: 192.168.1.10 ✓



## What is DHCP?(V.IMP)

**DHCP (Dynamic Host Configuration Protocol)** is like an **automatic address giver** in a network.

☞ Imagine you enter a hotel (network), and instead of you choosing your room number (IP address) yourself, the receptionist (DHCP server) gives you one automatically.

So, **DHCP is a protocol that gives IP addresses to devices automatically** when they join the network.

## ✓ Why do we need DHCP?

Without DHCP:

- You have to manually enter IP address, subnet mask, gateway, DNS, etc.
- It's slow, confusing, and prone to errors.

With DHCP:

- Everything is automatic!
- Fast and error-free.

# Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

## 🔄 How does DHCP Work? (Step-by-step with example)

Let's say your **laptop** wants to connect to the internet using **Wi-Fi** at college.

### ✅ Step 1: DHCP Discover

Your laptop says:

"Hey! Is there any DHCP server here? I need an IP address."

(This is a **broadcast message** sent to everyone.)

### ✅ Step 2: DHCP Offer

The DHCP server replies:

"Yes! I'm here. I can offer you IP address 192.168.1.10. Do you want it?"

### ✅ Step 3: DHCP Request

Your laptop says:

"Yes, please! I would like to use that IP address."

## ✓ Step 4: DHCP Acknowledgement

The DHCP server says:

"Done! IP 192.168.1.10 is now yours. You can use it for 24 hours."

This whole process is called **DORA**:

D-> Discover

O -> Offer

R-> Request

A-> Acknowledge

# Computer Network (BCS603)


## Q. 1 How is the BOOTP different from DHCP

### First, What is BOOTP?

**BOOTP (Bootstrap Protocol)** is an older protocol used to assign IP addresses to computers automatically in a network.
It was mainly designed for diskless computers (computers without hard drives) that needed to **download their OS from the network**.

### What is DHCP?

**DHCP (Dynamic Host Configuration Protocol)** is like the **modern version** of BOOTP.
It does the same job — assigning IP addresses — but **automatically and more efficiently**, with many more features.

# Computer Network (BCS603)

| Feature | BOOTP ⁇⁇ (Old) | DHCP ⁇⁇💻 (New/Modern) |
|---|---|---|
| **Developed By** | BOOTP came before DHCP | DHCP was developed later as an upgrade |
| **IP Assignment** | Static (manual entry by admin) | Dynamic (auto-assign by server) |
| **Configuration** | Hard to configure | Easy to configure |
| **Lease Time** | No lease (permanent IP) | Has lease (temporary IP) |
| **Supports Mobility** | No (devices get fixed IP) | Yes (devices can move & reconnect) |
| **Extra Info Provided** | Only IP address | IP, Gateway, Subnet Mask, DNS, etc. |
| **Uses DORA?** | No | Yes (Discover, Offer, Request, Ack) |
| **Common Today?** | Rarely used now | Widely used everywhere |

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

## Q.2 What Is the Purpose of domain name system. Discuss three main division of the domain name space.(V.IMP)

### 🌐 What is the Domain Name System (DNS)?

Imagine the internet is like a phonebook.
When you want to visit a website like www.google.com, your computer doesn't understand names — it only understands **IP addresses** (like 142.250.182.132).
So, DNS is like a **translator**.

### ✅ Purpose of DNS:

**DNS translates domain names into IP addresses**, so computers can find each other on the internet.

Example:

```
You type → www.google.com
DNS says → "Oh! That means 142.250.182.132"
Then your browser opens Google.
```

# Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

## ❖ Three Main Divisions of the Domain Name Space:

### 1. Top-Level Domain (TLD)

These are the endings of websites.

Examples:

- .com → for commercial sites
- .org → for organizations
- .edu → for education
- .in, .uk, .us → for countries

📝 TLD is the **last part** of a domain name.

### 2. Second-Level Domain (SLD)

This is the **main name** of the website, chosen by the owner.

Example:

- In google.com → google is the second-level domain
- In harvard.edu → harvard is the second-level domain

### 3. Subdomain

These are **optional parts** before the second-level domain.

Examples:

- www.google.com → www is a subdomain
- mail.yahoo.com → mail is a subdomain

It helps organize sections of a website.

# Computer Network (BCS603)

EduShine CLASSES
By:- ARMAN ALI

## What is ICMP?

**ICMP (Internet Control Message Protocol)** is like the **messenger** of the internet.

☞ It is used by **network devices (like routers, computers)** to **send error messages** or **status information**.

It doesn't carry user data like emails or webpages. Instead, it helps in **diagnosing network problems**.

**Think of ICMP like this:**

You're on a road trip and ask someone, “Is the road to Delhi open?” — if someone replies **“No, road blocked!”**, that’s ICMP.

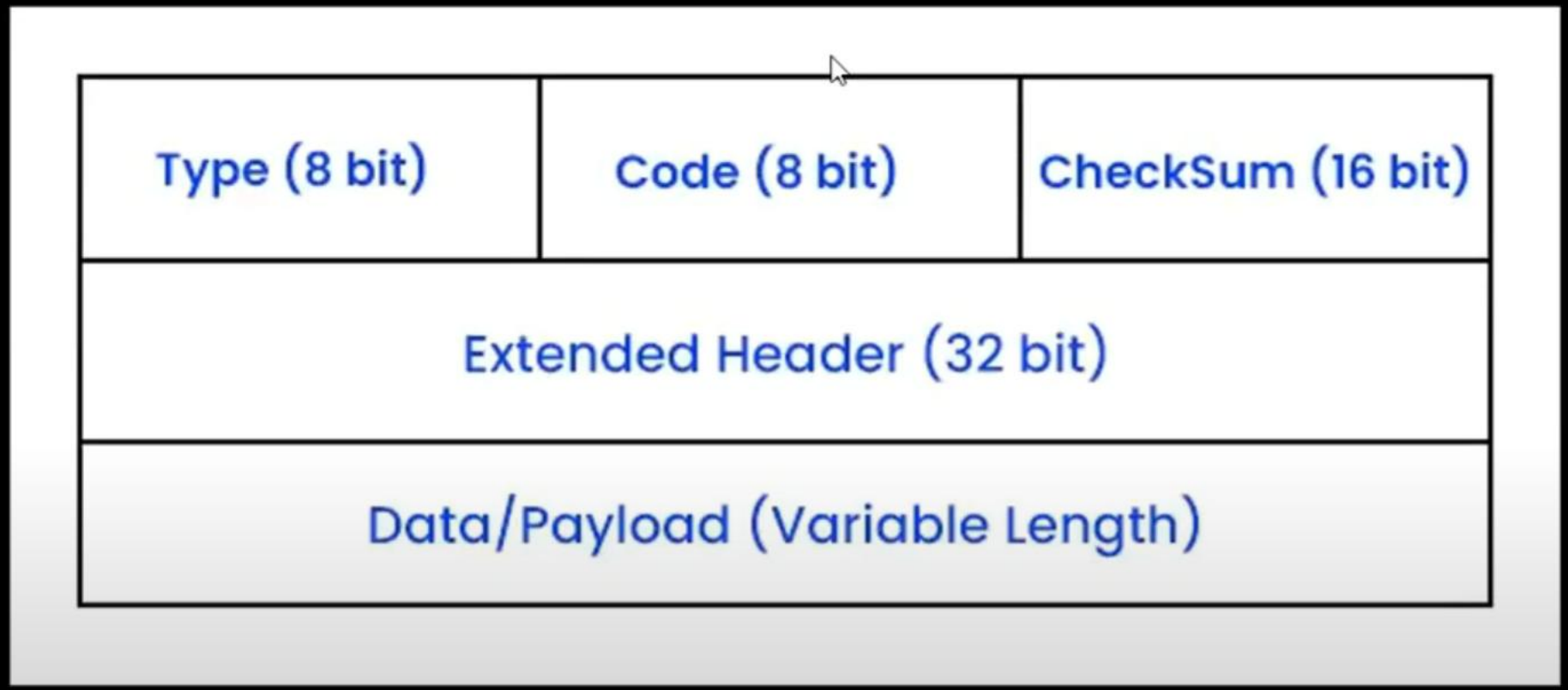
So, ICMP is used to send messages like:

- “Hey, destination not reachable!”
- “Time’s up, packet expired!”
- “Ping received!”

# Computer Network (BCS603)

EduShine CLASSES By:- ARMAN ALI

## ICMP Message Format (Structure) :



## 1. Type (8 bits)

This is the **first field** in an ICMP message.

You can think of this as the **category of the message** — it tells what kind of message ICMP is sending.

**For example:**

- If **Type = 8**, it's a "Ping Request" (called Echo Request)
- If **Type = 0**, it's a "Ping Reply" (called Echo Reply)
- If **Type = 3**, it means "Destination is unreachable"

This is just like when someone starts a sentence with, "Hey, I have an issue!" or "Everything's okay!" — it sets the **intention** of the message.

## 2. Code (8 bits)

This field gives **more details** about the Type.

**Example:**

If Type = 3 (Destination unreachable), the Code will tell **why** the destination was unreachable:

- Code = 0 → Network unreachable
- Code = 1 → Host unreachable
- Code = 3 → Port unreachable

So think of **Code** as the "sub-reason" or **specific explanation** related to the Type.
It helps give **more context** about the problem.

### 3. Checksum (16 bits)

This field is for **error checking**.

What does that mean?

Well, when a message is sent, sometimes due to network noise or issues, the data can get changed or corrupted.

The **Checksum** is a calculated value based on the content of the message.

When the receiver gets the message, it also calculates a checksum and compares it.

- If both match ✓ → message is fine
- If they don't ✗ → message has an error

It's like sending a parcel and putting a seal — if the seal is broken when received, it means something went wrong.

### 4. Rest of Header (varies by Type and Code)

This part of the ICMP message **changes depending on what kind of message it is** (depends on Type and Code).

For example:

- In Echo Request/Reply (Ping), it contains:
- **Identifier** (like a process ID or a number to match requests and replies)
- **Sequence Number** (used to keep track of message order — like Ping 1, Ping 2, etc.)

So this part works like **extra information specific to the purpose** of the message.

### 5. Data (Variable Length)

This is the **payload** — the actual message content.

In Echo Request/Reply, this field can carry some data like:

- Timestamps
- Sequence numbers
- Or a simple text message like “Hello!”

This data is **usually used to test if the message went and came back correctly**.
For example:

- If you send a Ping with message "TEST" and get back the same message → means it traveled properly.

**Q. Discuss each command in detail used in networking –**

i. Ipconfig
ii. Netstat
iii. Ping
iv. Hostname
v. tracert

# Computer Network (BCS603)

EduShine CLASSES By:- ARMAN ALI

## ✓ 1. ipconfig

- Shows IP address, subnet mask, and default gateway.
- Used to troubleshoot internet or network issues.
- Example: ipconfig(run in cmd)

## ✓ 2. netstat (Network Statistics)

- Shows all the **current connections** and **open ports** on your system.
- Helps you check if any **programs or viruses** are using the network without your knowle

**Example:** netstat(run in CMD)

Want to check if your browser is connected to Google? Run netstat and look for connections on port **443** (HTTPS).

## ✓ 3. ping (Packet Internet Groper)

- Sends a small message to another computer/server and waits for a reply.
- To check if a server or device is **reachable** (online) or not.

**Example: ping google.com**

**Real-life use:**

If your internet is slow or not working, use ping to test if websites are responding.

- If replies come = Internet is working
- If "Request Timed Out" = Problem with your connection

# Computer Network (BCS603)


### ✓ 4. hostname

- Displays the **name of your computer** in the network.
- To know how your system is identified in a local network.

◈ **Example:** hostname

### ✓ 5. tracert (Trace Route)

- Shows the **path taken by packets** to reach a destination — all the routers it travels through.
- To **see where network delays or problems** are happening.

◈ **Example: tracert google.com**

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

## What is Routing?

**Routing** is the process of **finding the best path** for data to travel from one computer (or device) to another across a network.

- Think of it like Google Maps for data packets.
- When you send data (like opening a website), it needs to **travel through many routers** to reach its destination.
- The job of finding the best path is called **routing**, and the devices doing this job are called **routers**.

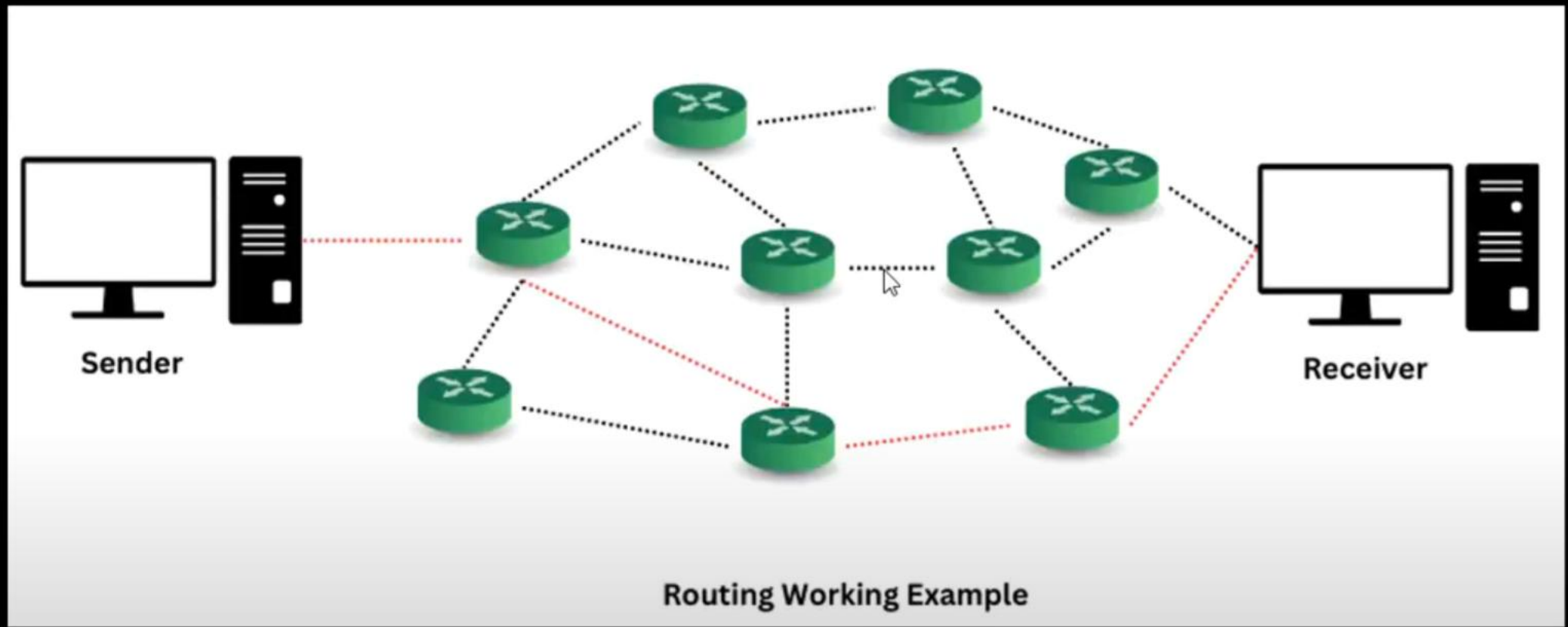
## Types of Routing

Routing is mainly of **two types**:

i. Static Routing
ii. Dynamic Routing

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI




Routing Working Example

## ✓ 1. Static Routing

In static routing, routes are manually set by the network administrator.

📌 Key Points:

- Routes don’t change automatically.
- Good for small or simple networks.
- Admin must update the routes manually if there’s any change.
- Easy to configure but not flexible.

**Example:**

You tell your GPS to always take Route A to your office. Even if there's traffic, it won’t change the route unless you update it.

# Computer Network (BCS603)


## ✓ 2. Dynamic Routing

In dynamic routing, routers automatically learn and update routes using routing protocols.

### 📌 Key Points:

- Routes are updated automatically if network changes.
- Used in large and complex networks.
- More flexible and fault-tolerant.
- Uses routing protocols like RIP, OSPF, EIGRP, BGP, etc.

**Example:**

Your GPS automatically changes the route if it finds traffic or a roadblock.

# Computer Network (BCS603)


## ✓ Static Routing

### ◆ Advantages:

- **Easy to configure in small networks**
  → Best for home or small office use.
- **No extra CPU or memory usage**
  → Router doesn't need to run any routing protocol.
- **More secure**
  → Only manually set routes are used, so fewer chances of wrong paths.
- **No bandwidth usage**
  → No updates or messages are shared between routers.

## Disadvantages:

- **Manual changes required**
  → If network changes, admin must update routes by hand.
- **Not scalable**
  → Becomes very difficult in large networks with many routers.
- **No automatic backup path**
  → If one path fails, data can't switch to another route on its own.

# Computer Network (BCS603)


## ✓ Dynamic Routing

### ◆ Advantages:

- **Automatic updates**
  → Routers adjust paths automatically if network changes.
- **Scalable**
  → Best for large and complex networks like in companies or ISPs.
- **Supports backup paths**
  → If one path fails, router automatically chooses another route.
- **Less manual work**
  → Admin does not need to configure each route.

# Computer Network (BCS603)


## Disadvantages:

- **More resource usage**
  → Router uses CPU, RAM, and bandwidth to run protocols.
- **Can be less secure**
  → Since routers learn routes automatically, they may be tricked if not secured.
- **Slower initial setup**
  → Routers need time to learn all paths in a big network.

# Computer Network (BCS603)

EduShine CLASSES
By:- ARMAN ALI

❖ **Difference between Static and Dynamic routing :**

| Feature | Static Routing | Dynamic Routing |
|---|---|---|
| Set by | Manual (admin) | Automatically (protocols) |
| Suitable for | Small networks | Large networks |
| Changes with network | No (manual update needed) | Yes (auto update) |
| Complexity | Simple | Complex but flexible |
| Examples | Home network | Company or internet routing |

# Computer Network (BCS603)

EduShine CLASSES
By:- ARMAN ALI

## 🌐 What is Delivery in Network Layer?

In networking, delivery means how a message (or data packet) is transferred from one device (computer) to another. This work is managed by the network layer (like IP protocol).
There are **two types** of delivery:

### ✅ 1. Direct Delivery

When the sender and receiver are in the same network, the data is sent directly — no need for any router in between.

**🔑Example:**

- You have two computers connected to the same Wi-Fi network at home.
- One computer sends a file to the other.
- This is direct delivery — no middle router is needed.

❖ **Key Points:**

- Same network
- Uses MAC address for delivery
- Faster and simpler

✓ **2. Indirect Delivery**

When the sender and receiver are in different networks, the data is sent indirectly through one or more routers.

🔑**Example:**

- You send a WhatsApp message from your phone (home Wi-Fi) to your friend who is in another city on a different network.
- Your message travels through many routers on the internet to reach your friend.
- This is indirect delivery.

# Computer Network (BCS603)

EduShine CLASSES
By:- ARMAN ALI

**Key Points:**

- Different networks
- Routers are used
- Uses IP addresses to route the packet

## 🌐 What is Forwarding?

Forwarding means deciding where to send a data packet next on its way to the final destination.

💡 Think of it like a post office: When a letter comes in, the post office checks the address and decides which route or truck to send it on next. Similarly, a router checks the packet's destination IP address and decides the next stop (next router or destination).

## ✅ Why is Forwarding Important?

It helps data reach the correct destination by making smart decisions at every router or device in the path.

# Computer Network (BCS603)


## 🔀 Forwarding Techniques (Methods)

Routers use different ways to decide where to send a packet. These are the three common techniques:

### 1. Next Hop Method

Instead of storing the entire path, the router just stores the IP address of the next hop (the next router) where the packet should go.

### 🔑 Example:

Imagine you want to go to Delhi, and someone tells you, “First go to Lucknow, from there you’ll find the way.”

Here, Lucknow is the next hop.

**Key Point:** Saves memory by only storing the next step, not the full route

## 2. Network-Specific Method

Instead of remembering individual IP addresses, the router stores routes based on **entire networks**.

🔑 **Example:**

If a packet's destination is 192.168.10.5, the router checks for a route to **network 192.168.10.0** and forwards the packet that way.

**Key Point:** Makes routing faster by grouping similar IP addresses.

## 3. Default Method

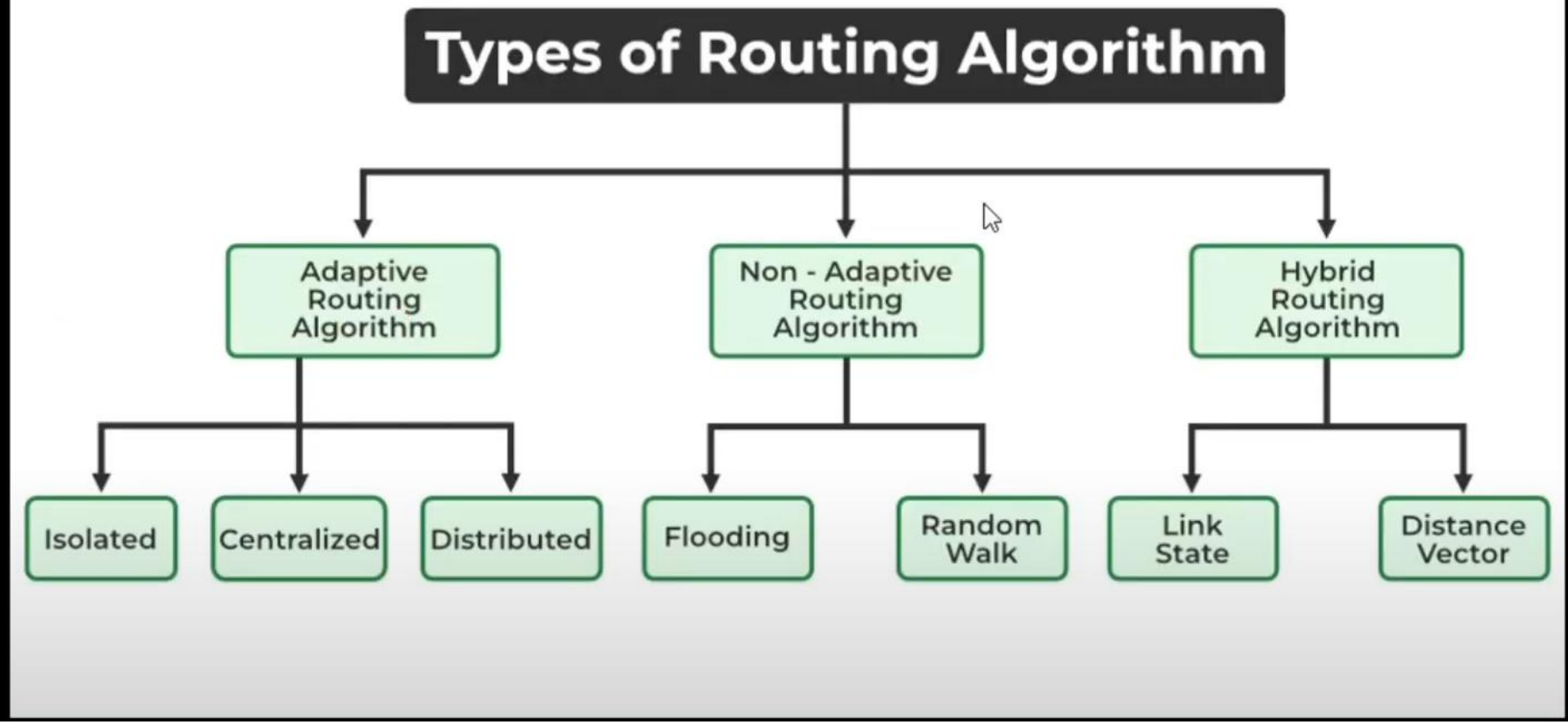
When there is no specific route in the routing table for a packet, the router sends the packet to a default route (like a backup path).

🔑 **Example:**

You don't know which bus goes to a small town, so you take a general bus to the main city bus station, and from there they handle it.

# Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI



# Computer Network (BCS603)


## ❖ Adaptive Routing Algorithm (Dynamic Routing):

- It **changes path** automatically if the network condition changes (like traffic, errors, etc.).
- It's smart and **adjusts routes**.
- These are the algorithms that change their routing decisions whenever network topology or traffic load changes. The changes in routing decisions are reflected in the topology as well as the traffic of the network. Also known as dynamic routing, these make use of dynamic information such as current topology, load, delay, etc. to select routes. Optimization parameters are distance, number of hops, and estimated transit time.

Further, these are classified as follows:

### i. Isolated :

Isolated Routing is a method in which a router makes its own routing decisions based only on its own local information. It does not exchange routing updates with its neighbors or use information from other routers.

### 🎯 Example (Real-life):

Imagine you are going to a friend's house in a city you've never been to before.
You don’t ask anyone for help, and you don’t use Google Maps.
You just take turns randomly and hope you reach the destination.
That's exactly how isolated routing works!

### ii. Centralized :

Centralized Routing means there is one central controller (or server) that knows everything about the whole network.
This central system makes all the routing decisions and tells the routers what path to follow.

**Example :**

Imagine you're in a delivery company. Instead of each delivery boy deciding their own route, they call the main office, and the office tells them the best route to deliver the package. The office knows all the roads, traffic, and shortcuts this is how centralized routing works.

**iii. Distributed :**

In distributed routing, each router makes its own routing decisions using information it gets from nearby routers.

There is no central controller. All routers work together, like a team.

**Example :**

Imagine a group of friends trying to find the shortest path to a destination in a big city.

Each friend talks to the friend next to them and shares road updates like:

“Hey, this road is blocked” or

“This way is faster now.”

Everyone **shares updates**, and together they find the **best route**.

That’s **distributed routing**!

## ❖ Non-Adaptive Routing Algorithm(Static Routing) : (V.VIMP)

- Routing path is **fixed** and doesn't change automatically.
- Even if the network is busy or broken, it follows the same route.
- These are the algorithms that do not change their routing decisions once they have been selected. This is also known as static routing as a route to be taken is computed in advance and downloaded to routers when a router is booted.

Further, these are classified as follows:

### i. Flooding Routing?

**Flooding** means sending the data to **all possible paths** in the network, whether they are useful or not.

Imagine you want to invite your friends to a party, but you don't know who's available.

So, you send the **same message** to **every contact** in your phone. They also forward it to their contacts, and so on.

Eventually, **everyone gets your message**!

That's exactly how **flooding routing** works.

# Computer Network (BCS603)


## How It Works:

- A router receives a packet (data).
- Instead of choosing one path, it sends the same packet to all its neighbors.
- Then those neighbors send it to their neighbors.
- This continues until the packet reaches its destination.

## Example:

Let's say Router A wants to send a message to Router D.

- A sends it to B and C.
- B sends it to C and D.
- C sends it to B and D.
- D receives the message from both B and C.

**Mission complete!** D got the message, even if some paths were extra.

# Computer Network (BCS603)


### ⚙ To Avoid Problems:

Because packets can **go in circles**, we use these methods:

1. **Hop Count Limit** – Each packet has a limit (like max 5 routers).
2. **Sequence Number** – To ignore duplicate packets.
3. **Visited List** – Packet remembers where it has already gone.

### 👍 Advantages:

- ✓ **Very simple** method.
- ✓ **Guaranteed delivery** – message will definitely reach.
- ✓ Good for **finding unknown routes**.

### 👎 Disadvantages:

- ✓ **Wastes bandwidth** – sends too many copies.
- ✓ Causes **congestion** in the network.
- ✓ Creates **duplicate packets**.

## ii. Random Walk Routing?

Random Walk Routing means sending the data to only one randomly chosen neighbor instead of all neighbors like in flooding.

**Example :**

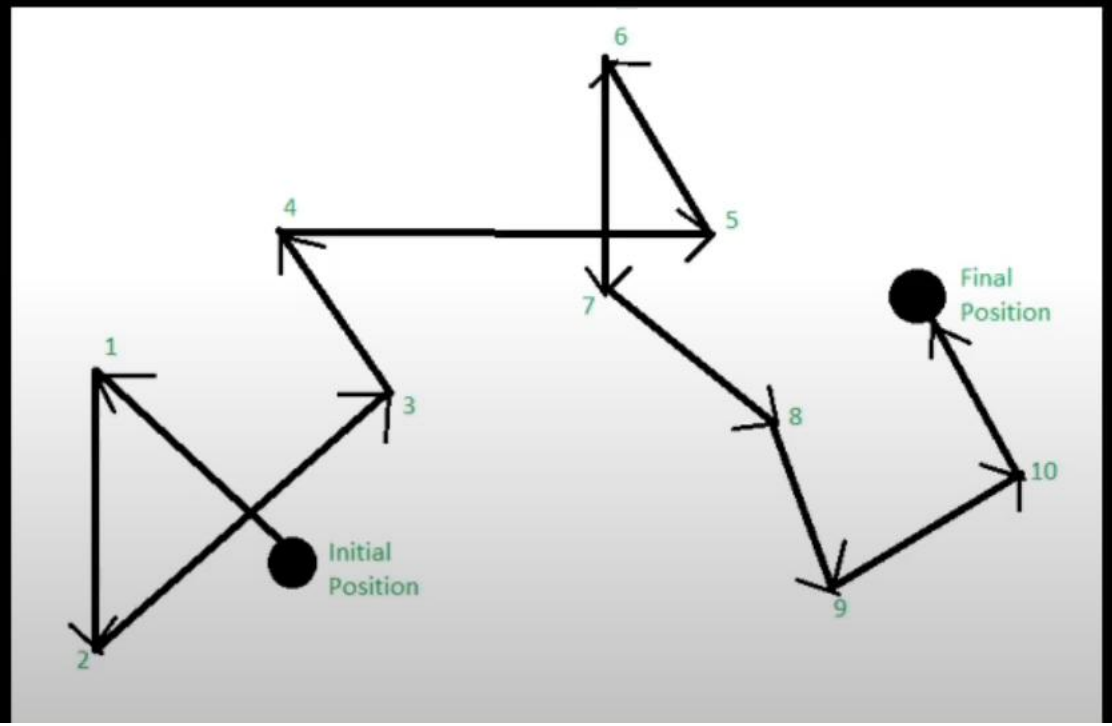
Imagine you are in a big building and you want to find Room 101, but you don't know the way.
Instead of asking everyone or going in all directions (like flooding),
you just ask one random person, then follow their direction,
then ask another random person… and so on.
Eventually, you may reach Room 101.
That's Random Walk Routing.

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

## How It Works:

- A router receives a packet.
- It randomly selects one of its neighbors and sends the packet there.
- The next router also does the same — chooses one neighbor randomly.
- This process continues until the packet reaches the destination.



## ❖ Hybrid Routing Algorithm :

- It uses both static and dynamic methods.
- Tries to balance between speed and accuracy.
- As the name suggests, these algorithms are a combination of both adaptive and non-adaptive algorithms. In this approach, the network is divided into several regions, and each region uses a different algorithm.
  Further, these are classified as follows:

### i. Link State Routing :

- Link State Routing is a routing method where every router in the network knows the complete map of the network — like Google Maps for routers!
- In this method, each router creates a detailed and complete map of the network which is then shared with all other routers. This allows for more accurate and efficient routing

# Computer Network (BCS603)

EduShine CLASSES By- ARMAN ALI

## 💡 Easy Explanation:

Soch le tu ek delivery boy hai, aur tujhe har gali, har road, har shortcut ka map mil gaya hai.
Ab tu khud best shortest route decide kar sakta hai.
Same way, in Link State Routing:

- Har router khud ka map banata hai.
- Sab routers apna map ek dusre se share karte hain.
- Har router khud shortest path calculate karta hai.

## 🛠️ Steps of Link State Routing:

**1.Discover Neighbors**

Router finds out which other routers are directly connected to it.

**2.Measure Link Cost**

It checks the "distance" or "cost" to each neighbor (e.g. speed, delay).

**3. Send Link-State Advertisement (SLA)**

Router sends info about itself and its neighbors to **all other routers**.

**4. Build the Link-State Database**

Using all info from all routers, each router makes a **full network map**.

**5. Run Dijkstra Algorithm**

Router calculates the **shortest path** to every other router using this map.

👍 **Advantages:**

- Very **accurate** (since each router has full info).
- Finds the **best path**.
- Adapts quickly if any path fails

👎 **Disadvantages:**

- Needs **more memory** (to store full map).
- More **complex** than distance vector.
- If network is very large, sharing info takes time.

## ii. Distance Vector Routing?(V.V.VIMP)

Distance Vector Routing is a method where each router only knows:

- How far (distance) the destination is
- And which direction (next router) to go

It doesn't know full network map, just info from its neighbors.

✓ In this method, each router maintains a table that contains information about the distance and direction to every other node in the network. This table is then shared with other routers in the network. The disadvantage of this method is that it may lead to routing loops.

### 👍 Advantages:

- Simple to implement
- Routers don't need full map

## 🛠️ How It Works (Steps):

**1. Each router keeps a table**

That table tells:

- Which destination
- How far (number of hops)
- And which neighbor to send to

**2. Routers share their tables with neighbors**

They exchange this info regularly.

**3. Update tables**

After getting neighbor info, routers update their own tables.

**4. Best path is chosen**

If neighbor gives a shorter path, router updates its route.

Example : In Video

# Computer Network (BCS603)


## ✓ What is Path Vector Routing?

Path Vector Routing is a type of routing protocol used mostly between different networks (AS – Autonomous Systems).

It tells not just the distance — but also the full path (route) that data should take.

**Autonomous System** is like a **large network** or **group of networks** that are all controlled by **one organization** or **one internet provider**.

## ⛓ Path Vector Protocol Example:

Let's say you have 4 Autonomous Systems (AS):

- AS1
- AS2
- AS3
- AS4

If **AS1 wants to reach AS4**, and the path is:

➡ AS1 → AS2 → AS3 → AS4

Then the routing table in AS1 will store:

- Destination: AS4
- Path: AS1 → AS2 → AS3 → AS4

If there's a loop (like AS4 trying to come back to AS1), routers can check and avoid it — because they see the full path.

👍 **Advantages:**

- Avoids loops easily (because it tracks full path)
- Good for big, interconnected networks like the Internet
- Each AS (network) can make its own policies

👎 **Disadvantages:**

- Needs more memory (because of full path info)
- Slower updates compared to other routing types

**Path Vector Routing** is a routing technique where each router stores the complete path (sequence of networks) to a destination, not just distance or next hop. It is mainly used in inter-domain routing like BGP.

# Computer Network (BCS603)


**Q. Explain all interdomain and intradomain routings algorithms.(AKTU 2023-24)**

**Ans :**

❖ **Intradomain Routing algorithm :**

i. Distance Vector Routing (pichhe ho gya hai)
ii. Link state routing(" " )

❖ **Interdomain Routing algorithms :**

i. Path vector routing (" ")

**Q. What is Unicast Routing ? Discuss unicast routing protocols.(AKTU 2018-19)**

Unicast routing means sending data from one device to one specific device — one-to-one communication.

i. Distance Vector routing
ii. Link state routing
iii. Path vector routing

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

## ❖ Difference between Adaptive and non adaptive routing algorithms :

| Feature | Adaptive Routing | Non-Adaptive Routing |
|---|---|---|
| 🔄 Changes based on network? | ✔ Yes | ✖ No |
| ❓❓ Based on current conditions | ✔ Uses real-time info (like traffic, failures) | ✖ Uses fixed info set at start |
| 📈 Performance | Better in changing networks | Not flexible if network changes |
| 🕒 Routing updates | Happens regularly | Rare or never |
| 🚦 Handles traffic/load | Can avoid congestion | May cause delays if network is busy |
| 🔁 Example protocols | OSPF, RIP, EIGRP | Static routing, Flooding, Shortest Path First |

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

| Feature | Distance Vector Routing | Link State Routing |
|---|---|---|
| Information Shared | Only with **neighbors** | Shared with **all routers** in the network |
| Network Knowledge | Router knows info only about neighbors | Router knows **full map** of network |
| Update Method | **Periodically** sends full routing table | Sends **link-state packets** only when needed |
| Path Calculation | Based on neighbor's info (Bellman-Ford algorithm) | Uses **Dijkstra's algorithm** |
| Convergence Speed | **Slow** (takes time to update network changes) | **Fast** (quick updates and convergence) |
| Loop Chances | Higher chance of **routing loops** | Less chance of loops |
| Memory/CPU Use | **Less memory and CPU** needed | Needs **more memory and CPU power** |
| Example Protocols | **RIP (Routing Information Protocol)** | **OSPF (Open Shortest Path First)** |
| Configuration | **Simple** to configure | **More complex** to configure |

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

## 📡 What is Multicast Routing?

Multicast routing means sending one copy of data to multiple specific devices — one-to-many communication.

But not to everyone — only to a selected group.

## 💡 Easy Example:

Imagine a teacher wants to send notes 📝 to only the students in the science club, not the whole class.

- She sends one message
- But only science club members receive it

That's Multicast!

# Computer Network (BCS603)

EduShine CLASSES
By:- ARMAN ALI

## What is Congestion in a Network?

Congestion happens when too much data is trying to travel through the network at the same time — and the network gets overloaded.

**Think of it like:**

A road with too many cars = traffic jam

A network with too many data packets = network congestion

## Why is Congestion Bad?

- Data gets delayed
- Packets may get lost
- Network slows down
- Applications like video calls or gaming lag or freeze

# Computer Network (BCS603)


## 🛡️❓ What is Congestion Control?

Congestion control means using techniques to avoid or fix the traffic jam in the network.

Its goal is to:

- Keep data flowing smoothly
- Prevent overload
- Ensure fair usage for all users

## 🔧 Techniques to Prevent or Control Congestion:

### 🔓 1. Open Loop Congestion Control

Think of it as: “Plan Ahead”

In Open Loop, we try to prevent congestion before it happens.

- It’s like planning your journey before you leave to avoid traffic
- Once the data is sent, we don’t change anything — no feedback or correction

### 🔧 Techniques Used in Open Loop:

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

## 1. ✅ Retransmission Policy

📨 This decides **how and when to resend lost packets**.

- **Why it matters**: Too many retransmissions can **increase congestion**!
- So in open loop, we avoid resending too much or too quickly.

🤔 Think of it like:

"If your friend doesn't reply to your message, don't keep sending it again and again instantly — wait a bit!"

## 2. ✅ Window Policy

🎁 A **window** is how many packets can be sent before needing an acknowledgment (ACK).

- **A good window policy** avoids sending too much data at once.
- If the window is too big → network may get overloaded.
- **Fixed-size windows** are often used in open loop (no change based on feedback).

🤔 Think of it like:

"Send only 5 messages before waiting for a reply, instead of flooding the chat with 50!"

### 3. ✅ Acknowledgment Policy

📨 This controls **how often receivers send acknowledgments** (ACKs).

- If ACKs are sent too frequently → adds traffic
- If delayed or combined (called **delayed ACKs**) → reduces congestion

🤔 Think of it like:

"Instead of saying 'thanks' after every sentence, wait and say 'thanks for all' at the end."

### 🔁 2. Closed Loop Congestion Control

🤔 Think of it as: "React & Adjust"

In Closed Loop, we monitor the network, detect congestion, and fix it on the fly.

**Like using Google Maps while driving — it warns you of traffic ahead and reroutes you**

🔧 **Techniques Used in Closed Loop:**

# Computer Network (BCS603)

EduShine CLASSES
By- ARMAN ALI

## 1. 🔄 Backpressure

🚧 This is used **between routers**.

- If one router is full, it tells the one before it:
  "Don't send me more packets yet!"
- This **stops traffic from entering the busy area**.

👮 Like traffic police saying:
"The next road is jammed — wait here!"

## 2. 🚨 Choke Packet

📨 A special control packet sent by the router to the **sender** saying:
"Slow down! I'm overloaded."

- This is a direct message
- It helps reduce traffic from the sender

👩‍🏫 Like a teacher telling a student:
"You're writing too fast — slow down!"

### 3. 🕵️‍♂️ Implicit Signaling

There's no special packet, but the sender guesses there's congestion based on things like:

- Packet loss
- Delays
- Missing ACKs

Like figuring out someone is angry — not because they said it, but because of their behavior 😂

### 4. 📣 Explicit Signaling

📨 Here, the network **clearly tells** the sender there's congestion.

- Special bits are set in the packet headers to warn the sender
- Much more **direct and clear** than implicit

🗣️ Like someone saying:

"Hey, I'm overloaded. Please slow down your messages."

## ❖ Congestion Control Algorithms :

### 1. Leaky bucket algorithm :

The Leaky Bucket Algorithm is used to control the flow of data in a network.

It helps prevent congestion by making sure data is sent at a steady, smooth rate, even if it arrives in bursts.

### 💡 Simple Real-Life Example:

Imagine a bucket with a small hole at the bottom.

- You can pour water (data) into the bucket at any speed.
- But the water will only drip out at a fixed, steady rate.

If you pour in too much water too quickly, the bucket overflows, and some water is lost.

💧 = Data Packets

🪣 = Buffer (bucket)

➖ = Fixed rate at which data is sent

# Computer Network (BCS603)


## In Networking Terms:

- The bucket is like a buffer (a place to hold packets).
- Packets arrive at any speed — fast or slow.
- But they are sent out at a fixed rate.
- If the buffer (bucket) gets full → new incoming packets are discarded (data loss).

## Why Use It?

✓ Smoothens traffic (avoids sudden bursts)
✓ Prevents congestion in routers and networks
✓ Maintains a constant data flow

# Computer Network (BCS603)

EduShine CLASSES By:- ARMAN ALI

### 🔁 Step 1: Initialize the Bucket

- Define the bucket size (how many packets it can hold)
- Set the leak rate (how fast packets are sent out)
  e.g., 1 packet per second

### 🚀 Step 2: Receive Incoming Packets

When data (packets) comes in:

- If the bucket is not full → accept the packet and put it in the bucket
- If the bucket is full → discard the packet (overflow)

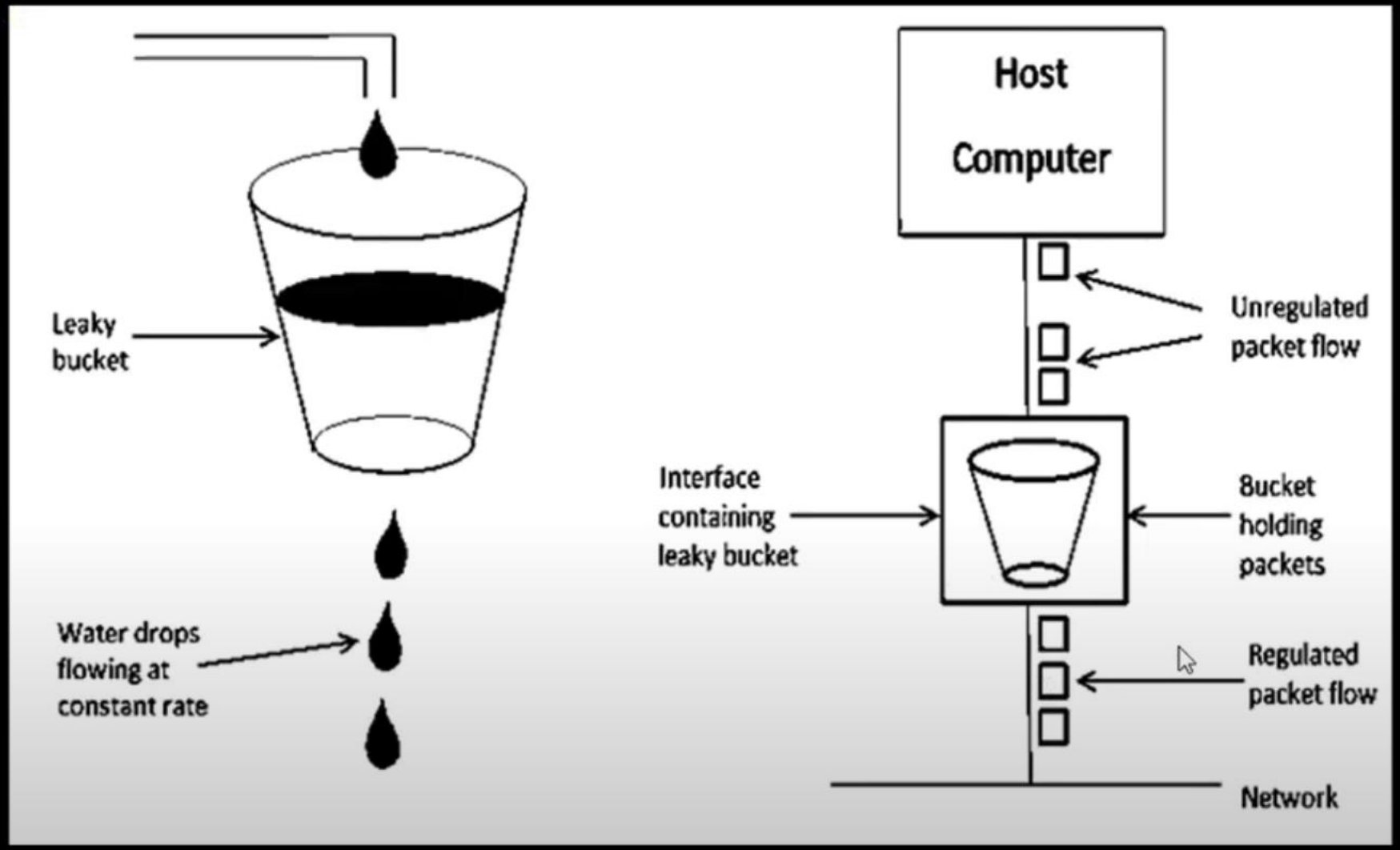
### ⏳ Step 3: Leak Packets Out

- At a fixed interval, leak out (send) one packet from the bucket to the network
- This happens no matter how fast the data comes in

### 🔄 Step 4: Repeat Continuously

- Keep accepting new packets to (if there's space)
- Keep leaking packets out at the fixed rate
- If incoming traffic is too fast → bucket fills up → excess packets get dropped

# Computer Network (BCS603)



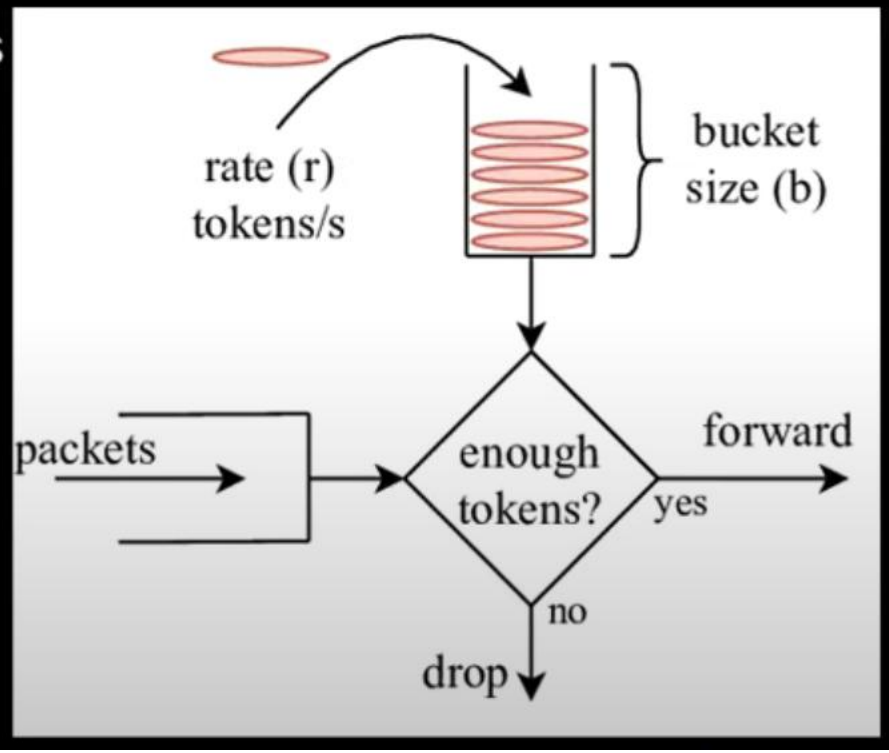
## ✓ 2. Token Bucket Algorithm :

Now imagine a bucket that holds tokens, not water.

- Tokens are added to the bucket at a fixed rate.
- To send 1 packet, you need 1 token.
- If you have enough tokens, you can send many packets at once (a burst).

If there are no tokens, you must wait until tokens are added.

☞ So, this allows controlled bursts of data when needed and still keeps the traffic under control.



# Computer Network (BCS603)


## ✕ Limitations of Leaky Bucket Algorithm

i. **No flexibility:** It always sends at a fixed rate, even if the network can handle more. This wastes bandwidth.

ii. **Bursty traffic is not allowed:** If there's a sudden need to send more data (a burst), it will drop the extra packets.

iii. **Not suitable for real-time traffic**: Applications like video or voice calls need flexibility, which this algorithm doesn't support.

iv. **No priority handling:** It treats all data equally. It can't handle urgent data differently.

# Computer Network (BCS603)

EduShine CLASSES
By:- ARMAN ALI

## ✅ What is QoS (Quality of Service)?

QoS (Quality of Service) is a way to control the quality of network service.
It helps to make sure that important data like videos, voice calls, or online games get good speed, less delay, and better performance over the internet.

### ❓❓ Example to Understand:

Imagine you're on a **video call**, and your little brother is **downloading a movie** at the same time.
Without QoS, your video call might **lag or freeze**.
But with QoS, the network will say:
"Okay! This video call is more important, so I'll give it better speed and low delay."

### ❖ 🎯 QoS Parameters (4 Main Things QoS Checks)

# Computer Network (BCS603)

EduShine CLASSES
By:- ARMAN ALI

## 1. ✓ Reliability

- Meaning: How dependable the network is to deliver data without losing it.
- Simple Words: Data should not be lost or corrupted while sending.
- Example: When you send an email, it should arrive complete, not missing some parts.

## 2. 🕒 Delay (Latency)

- Meaning: The time taken for data to reach from sender to receiver.
- Simple Words: How long it takes for your message or data to travel.
- Example: In a voice call, if you say “Hello” and the other person hears it after 3 seconds — that's high delay.

## 3. 🔁 Jitter

- Meaning: The variation or change in delay of data packets.
- Simple Words: When some packets arrive fast and some arrive slow.
- Example: In a video, if some parts load quickly and some parts load late, the video may lag or shake — this is due to jitter.

## 4. Bandwidth

- Meaning: Maximum amount of data that can be sent in one second.
- Simple Words: Think of it like the size of the road – the bigger the road (more bandwidth), the more vehicles (data) can pass at the same time.
- Example: Downloading a big file will be faster if you have more bandwidth.

## What is Traffic Shaping?(2 Marks)

Traffic Shaping is a technique used in QoS to control and manage the flow of data in a network.





# Thank You...