UNIT 4

COMPUTER NETWORK

MAC ADDRESSES

MAC Addresses are unique **48-bit** hardware numbers of a computer that are embedded into a network card (known as a **Network Interface Card**) during manufacturing. The MAC Address is also known as the **Physical Address** of a network device.

The data link layer is divided into two sub layers:

1. Logical Link Control (LLC) Sub layer.
2. Media Access Control (MAC) Sub layer.

The MAC address is used by the Media Access Control (MAC) sub layer of the Data-Link Layer. MAC Address is worldwide unique since millions of network devices exist and we need to uniquely identify each

FORMAT OF MAC ADDRESS

MAC Address is a 12-digit hexadecimal number (6-bit binary number), which is mostly represented by Colon-Hexadecimal notation.

The First 6 digits (say 00:40:96) of the MAC Address identify the manufacturer, called the OUI (**Organizational Unique Identifier**)

Examples:

CC:46:D6 – Cisco

00:9A:CD - HUAWEI TECHNOLOGIES CO.,LTD

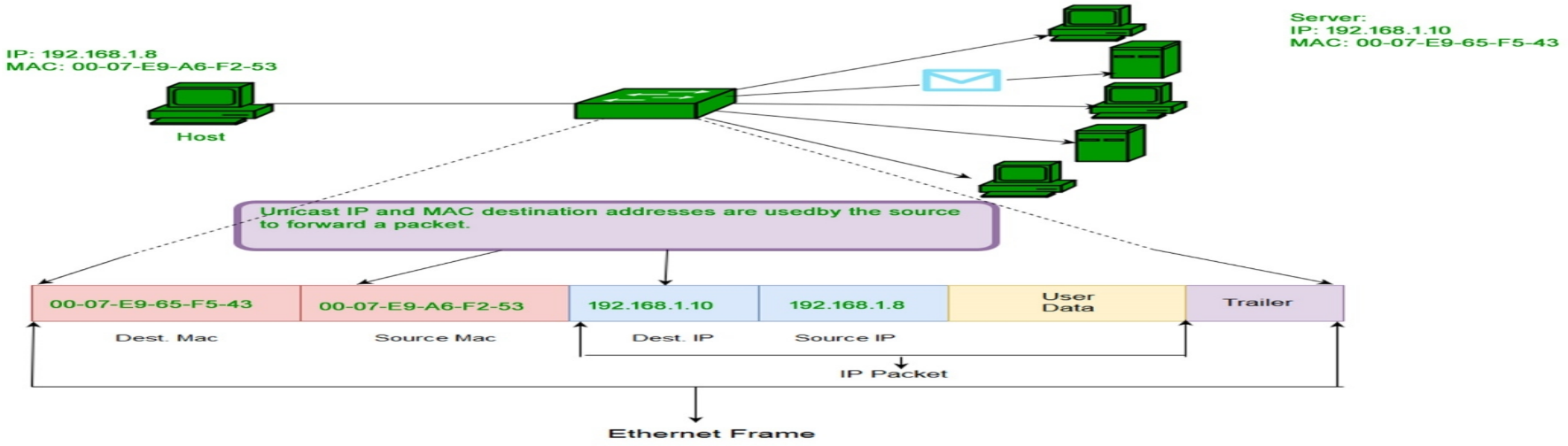
The rightmost six digits represent **Network Interface Controller**, which is assigned by the manufacturer.



TYPES OF MAC ADDRESS

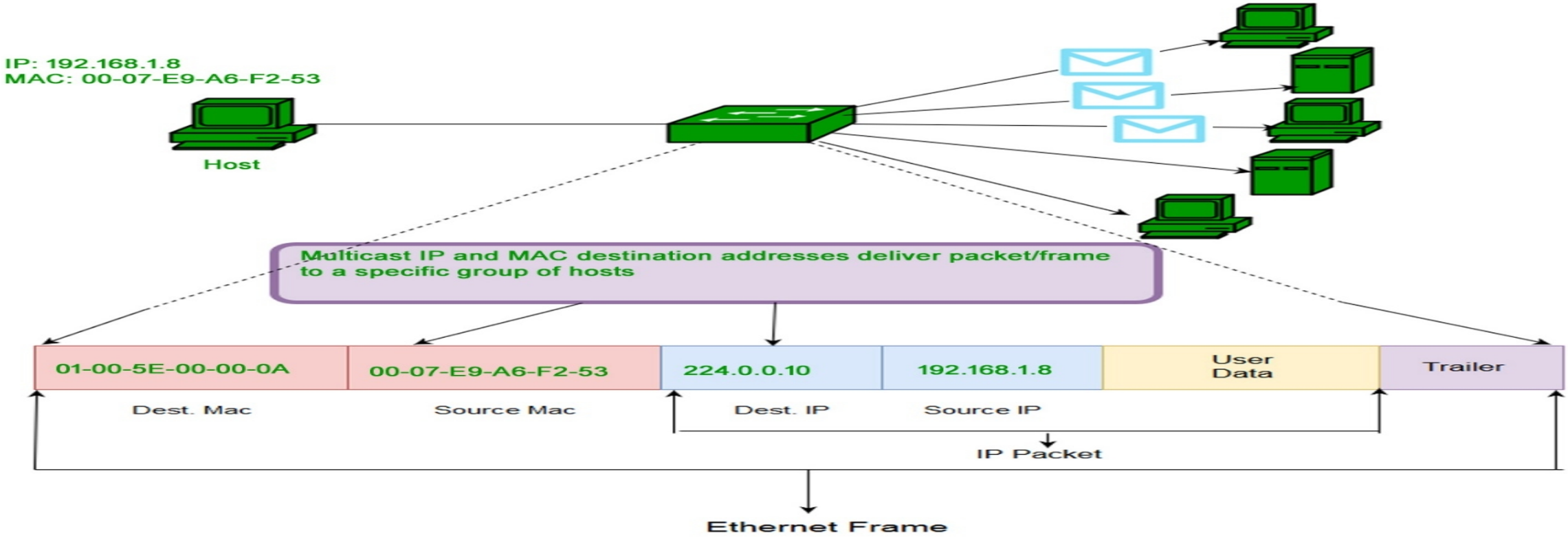
1. Unicast

- A Unicast-addressed frame is only sent out to the interface leading to a specific NIC. If the LSB (least significant bit) of the first octet of an address is set to zero, the frame is meant to reach only one receiving NIC. The MAC Address of the source machine is always Unicast.



2. Multicast

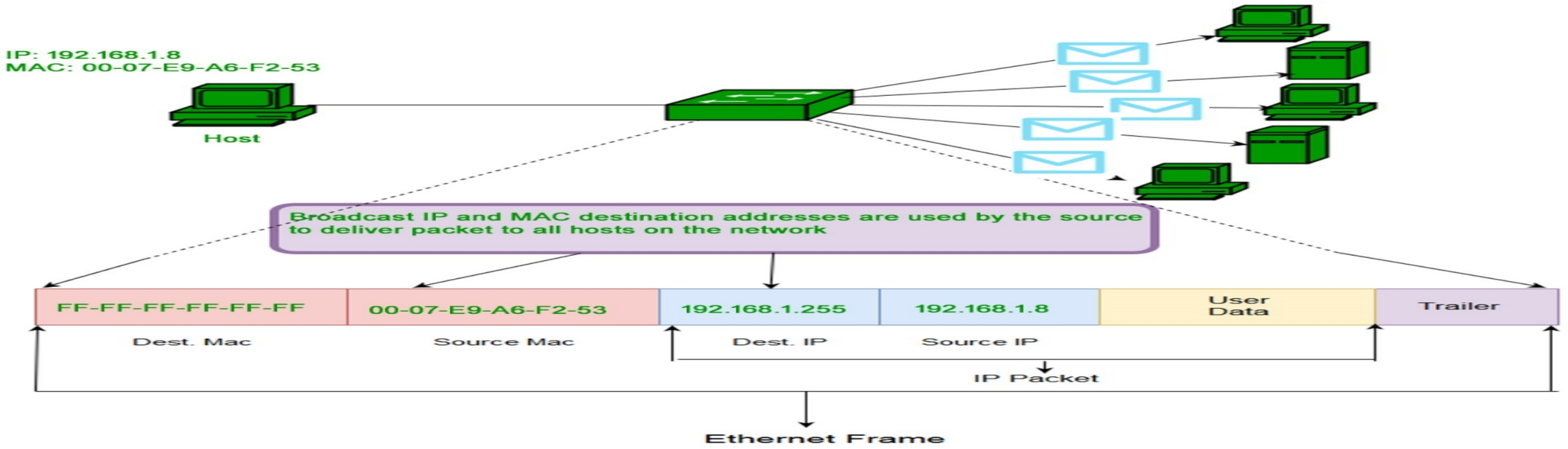
The multicast address allows the source to send a frame to a group of devices. In Layer-2 (Ethernet) Multicast address, the LSB (least significant bit) of the first octet of an address is set to one. IEEE has allocated the address block 01-80-C2-xx-xx-xx (01-80-C2-00-00-00 to 01-80-C2-FF-FF-FF) for group addresses for use by standard protocols.



Continue……

3. Broadcast

Similar to Network Layer, Broadcast is also possible on the underlying layer(Data Link Layer). Ethernet frames with ones in all bits of the destination address (FF-FF-FF-FF-FF-FF) are referred to as the broadcast addresses. Frames that are destined with MAC address FF-FF-FF-FF-FF-FF will reach every computer



MAC Cloning

- MAC Cloning is the way of fixing the connectivity in the network devices.
- Some ISPs use MAC addresses to assign an IP address to the gateway device. When a device connects to the ISP, the DHCP server records the MAC address and then assigns an IP address. Now the system will be identified through the MAC address. When the device gets disconnected, it loses the IP address.
- If the user wants to reconnect, the DHCP server checks if the device is connected before. If so, then the server tries to assign the same IP address (in case the lease period has not expired). In case the user changed the router, the user has to inform the ISP about the new MAC address because the new MAC address is unknown to ISP, so the connection cannot be established.
- Or the other option is **Cloning**, user can simply clone the registered MAC address with ISP. Now router keeps reporting the old MAC addresses to ISP and there will be no connection issue

CHARACTERISTICS OF MAC ADDRESS

- MAC addresses are used in LAN (Local Area Network) environments to identify devices and allow communication between them.
- MAC addresses are burned into the hardware of a network interface card (NIC) and cannot be changed, except in some rare cases where the manufacturer has provided a specific tool to do so.
- The first 3 bytes of a MAC address represent the manufacturer ID, while the last 3 bytes represent a unique identifier assigned by the manufacturer.
- MAC addresses are often used in conjunction with ARP (Address Resolution Protocol) to resolve IP addresses to MAC addresses for communication on a LAN.
- Some operating systems, such as Windows and Linux, allow you to view the MAC address of your network adapter through a command prompt or network settings.

ADVANTAGES OF MAC ADDRESS

- **Uniqueness:** Each MAC address is unique, which means that devices on the network can be easily identified and managed.
- **Simplicity:** MAC addresses are easy to configure and manage, and do not require any additional network infrastructure.
- **Compatibility:** MAC addresses are widely used and supported by a variety of networking technologies and protocols, making them compatible with many different systems.
- **Security:** MAC addresses can be used to restrict access to a network by only allowing devices with authorized MAC addresses to connect.
- **Fault-tolerance:** In case of hardware or software failure, a device can be easily replaced without affecting the network, as long as the new device has the same MAC address as the old one.

Continue……

- **Multicasting:** MAC addresses can be used for multicasting, allowing a single packet to be sent to multiple devices at once.
- **Efficiency:** MAC addresses allow for efficient communication on the network, as they enable devices to quickly and easily identify and communicate with each other.
- **Lower network overhead:** MAC addresses reduce network overhead by allowing devices to communicate directly with each other without the need for additional routing or addressing.
- **Ease of troubleshooting:** MAC addresses can be used to troubleshoot network issues by identifying the source of problems and tracking network activity.
- **Flexibility:** MAC addresses can be used to support a variety of network configurations and topologies, including peer-to-peer, client-server, and hybrid models

DISADVANTAGES OF MAC ADDRESS

- **Limited address space:** MAC addresses are 48-bit numbers, which means that there is a finite number of possible MAC addresses. This can lead to address conflicts if multiple devices have the same MAC address.
- **Spoofing:** MAC addresses can be easily spoofed, allowing unauthorized devices to gain access to the network.
- **Inefficiency:** MAC addresses are not hierarchical, which can make it difficult to efficiently manage large networks.
- **Static addressing:** MAC addresses are typically assigned at the time of manufacture and cannot be easily changed. This can be a disadvantage in situations where devices need to be reconfigured or replaced.
- **Limited scope:** MAC addresses are only used for identifying devices within a local network segment, and cannot be used to identify devices outside of this segment

Continue……

- **Hardware-dependent:** MAC addresses are tied to the network interface card (NIC) of a device, which means that if the NIC fails or is replaced, the MAC address also changes.
- **Lack of encryption:** MAC addresses are sent in plain text, which can make them vulnerable to interception and eavesdropping.
- **No inherent security:** While MAC filtering can be used to restrict access to a network, MAC addresses themselves do not provide any inherent security features.
- **MAC address collisions:** In rare cases, MAC addresses can collide, which can cause network disruptions and make it difficult to identify and manage devices on the network

DIFFERENT BETWEEN MAC ADDRESS AND IP ADDESS

MAC Address	IP Address
MAC Address stands for Media Access Control Address.	IP Address stands for Internet Protocol Address.
MAC Address is a six byte hexadecimal address.	IP Address is either a four-byte (IPv4) or a sixteen-byte (IPv6) address.
A device attached with MAC Address can retrieve by ARP protocol.	A device attached with IP Address can retrieve by RARP protocol.
NIC Card's Manufacturer provides the MAC Address.	Internet Service Provider provides IP Address.

ROUTER

The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks.

A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets.

There are some popular companies that develop routers; such are **Cisco**, **3Com**, **HP**, **Juniper**, **D-Link**, **Nortel**

HOW DOES ROUTER WORK?

- A router determines a packet's future path by examining the destination IP address of the header and comparing it to the routing database. The list of routing tables outlines how to send the data to a specific network location. They use a set of rules to determine the most effective way to transmit the data to the specified IP address.
- To enable communication between other devices and the internet, routers utilize a modem, such as a cable, fiber, or DSL modem. Most routers include many ports that can connect a variety of devices to the internet simultaneously. In order to decide where to deliver data and where traffic is coming from, it needs routing tables.
- A routing table primarily specifies the router's default path. As a result, it might not determine the optimum path to forward the data for a particular packet. For instance, the office router directs all networks to its internet service provider through a single default channel.
- Static and dynamic tables come in two varieties in the router. The dynamic routing tables are automatically updated by dynamic routers based on network activity, whereas the static routing tables are configured manually.

TYPES OF ROUTER

- **Broadband Routers:** These are one of the important kinds of routers. It is used to do different types of things. it is used to connect computers or it is also used to connect to the internet.
- **Wireless routers:** These routers are used to create a wireless signal in your office or home.
- **Wired Routers:** Wired Router is used to connects multiple wired devices using a Ethernet cable, It takes the transmission data from the modem and distribute it to a further network, it is widely used in schools and small offices.
- **Edge Routers**: As the name indicates, these are located at the edges usually connected to an Internet Service Provider, and distribute packets across multiple packets.

Continue….

- **Core Routers:** Core routers distribute packets within the same network. The main task is to carry heavy data transfers.
- **Virtual Router:** They are implemented using a software on the virtual machine , and they are more flexible and scalable.
- **Portable Routers:** They are used to create private Wi-Fi and hence designed for easy portability.

FUNCTIONS OF ROUTER

- **Forwarding:** The router receives the packets from its input ports, checks its header, performs some basic functions like checking checksum, and then looks up to the routing table to find the appropriate output port to dump the packets onto, and forwards the packets onto that output port.
- **Routing:** Routing is the process by which the router ascertains what is the best path for the packet to reach the destination, It maintains a routing table that is made using different algorithms by the router only.
- **Network Address Translation (NAT):** Routers use NAT to translate between different IP address ranges. This allows devices on a private network to access the internet using a single public IP address.
- **Security:** Routers can be configured with firewalls and other security features to protect the network from unauthorized access, malware, and other threats.

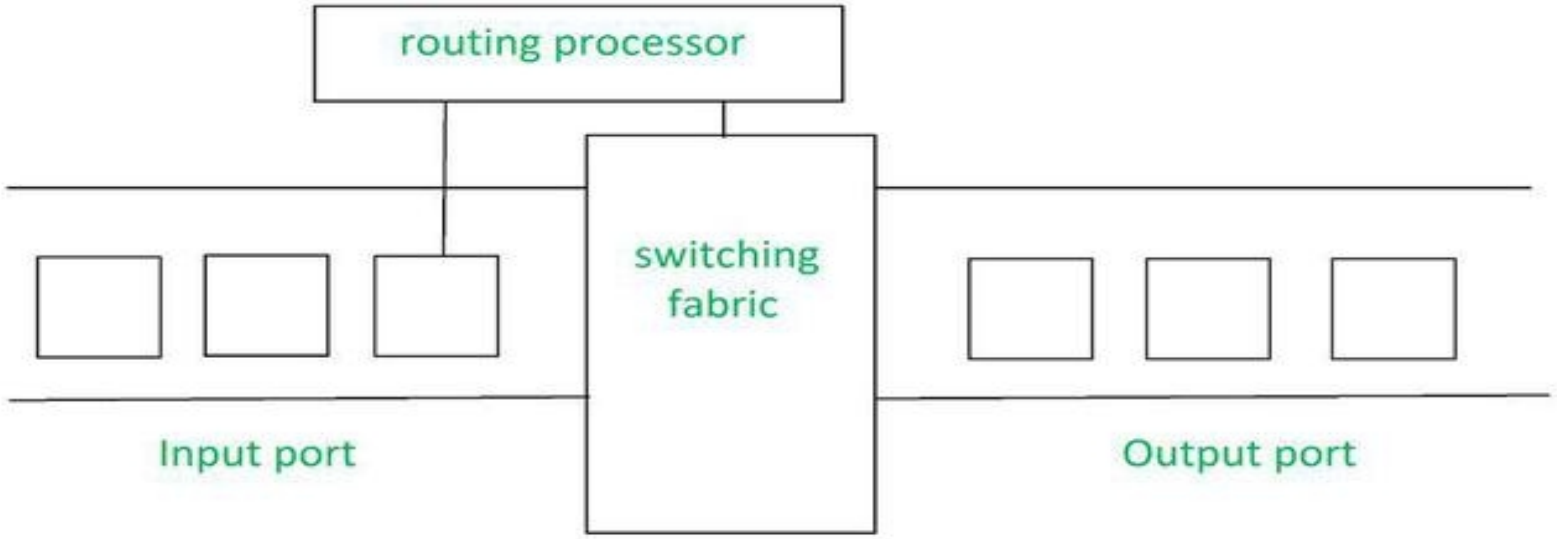
Continue…….

- **Quality of Service (QoS):** Routers can prioritize network traffic based on the type of data being transmitted. This ensures that critical applications and services receive adequate bandwidth and are not affected by lower-priority traffic.
- **Virtual Private Network (VPN) connectivity:** Routers can be configured to allow remote users to connect securely to the network using a VPN.
- **Bandwidth management:** Routers can be used to manage network bandwidth by controlling the amount of data that is allowed to flow through the network. This can prevent network congestion and ensure that critical applications and services receive adequate bandwidth.
- **Monitoring and diagnostics**: Routers can be configured to monitor network traffic and provide diagnostics information in the event of network failures or other issues. This allows network administrators to quickly identify and resolve problems

ARCHITECTURE OF ROUTER

A generic router consists of the following components:

- **Input Port:** This is the interface by which packets are admitted into the router, it performs several key functions as terminating the physical link at the router, this is done by the leftmost part in the below diagram, and the middle part does the work of interoperating with the link-layer like decapsulation, in the last part of the input port the forwarding table is looked up and is used to determine the appropriate output port based on the destination address.
- **Switching Fabric:** This is the heart of the Router, It connects the input ports with the output ports. It is kind of a network inside a networking device. The switching fabric can be implemented in several ways some of the prominent ones are:
  - **Switching via memory:** In this, we have a processor which copies the packet from input ports and sends it to the appropriate output port. It works as a traditional CPU with input and output ports acting as input and output devices.
  - **Switching via bus:** In this implementation, we have a bus that connects all the input ports to all the output ports. On receiving a packet and determining which output port it must be delivered to, the input port puts a particular token on the packet and transfers it to the bus. All output ports can see the packets but they will be delivered to the output port whose token has been put in, the token is then scraped off by that output port and the packet is forwarded
  - **Switching via interconnection network:** This is a more sophisticated network, here instead of a single bus we use a 2N bus to connect n input ports to n output ports.



Architecture of Router

- **Output Port:** This is the segment from which packets are transmitted out of the router. The output port looks at its queuing buffers (when more than one packets have to be transmitted through the same output port queuing buffers are formed) and takes packets, does link layer functions, and finally transmits the packets to an outgoing link.
- **Routing Processor:** It executes the routing protocols, and it works like a traditional CPU. It employs various routing algorithms like the link-state algorithm, distance-vector algorithm, etc. to prepare the forwarding table, which is looked up to determine the route and the output port.

SECURITY CHALLENGES IN ROUTER

Here below are some security challenges in router:

1. Vulnerability Exploits

- Firmware is automatically installed on all hardware-based routers to assist the operation of the router. Like any other programme, router firmware frequently has flaws that hackers could use against it. Vendors of routers usually release updates to fix these flaws. Router firmware needs to be updated on a frequent basis as a result. Attackers have the ability to monitor traffic on unpatched routers and utilise them as part of a botnet.

2. DDoS Attacks

- Distributed Denial-Of-Service (DDoS) attacks against network infrastructure frequently target both large and small organizations. Network outages can be caused by unmitigated network layer DDoS attacks, which can overload routers or bring them down. Using Cloud flare Magic Transit is one way to defend networks and routers against DDoS attacks of this nature.

3. Administration Credentials

- To carry out administration tasks, a set of admin credentials is included with every router. The default values for these credentials are “admin” for the username and “admin” for the password. As soon as possible, change the username and password to something more secure since, if they are not changed, attackers can use them to remotely take over the router. They are aware of the typical default values for these credentials.

ADVANTAGES OF ROUTER

- **Easier Connection:** Sharing a single network connection among numerous machines is the main advantage of router. This enables numerous people to connect to the internet, boosting total productivity. In addition, routers have connections between various media and network designs.
- **Security:** Undoubtedly, installing a router is the first step in securing a network connection. Because using a modem to connect directly to the internet exposes your computer to several security risks. So that the environment is somewhat secure, routers can be utilized as an intermediary between two networks. While not a firewall or antivirus replacement.
- **NAT Usage:** Routers use Network Address Translation (NAT) to map multiple private IP addresses into one public IP address. This allows for a better Internet connection and information flow between all devices connected to the network.

Continue……

- **Supports Dynamic Routing:** The router employs dynamic routing strategies to aid in network communication. The internet work's optimum path is chosen through dynamic routing. Additionally, it creates collision and broadcast domains. Overall, this can lessen network traffic.
- **Filtering of Packets:** Switching between packets and filtering packets are two more router services. A collection of filtering rules are used by routers to filter the network. The packets are either allowed or passed through.

DISADVANTAGES OF ROUTER

- **Slower:** Routers analyze multiple layers of information, from the physical layer to the network layer, which slows down connections. The same issue can also be encountered when multiple devices are connected to these network devices, causing “connection waiting”.
- **High Cost:** They are more expensive than some other tools for systems administration. This includes security, extension, and the focal point. As a result, routers are typically not the greatest option for issues.
- **Need for configuration:** The router must be properly configured to work properly. In general, the more complex the intended use, the more configuration is required. This requires professional installation, which can add to the cost of buying a router

Continue……..

- **Quality Issues:** The time transitions are not always accurate. Even yet, some modern devices use the 2.4GHz band, which is frequently deactivated. These kinds of separations are frequently possible for those who live in apartments and condominiums.
- **Bandwidth shortages:** Dynamic routing techniques used by routers to support connections tend to cause network overhead, consuming a lot of bandwidth. This leads to a bandwidth shortage that significantly slows down the internet connection between connected devices

APPLICATIONS OF ROUTER

There are several applications of router because nowadays routers are widely used in most of the networking communication for better communication:

- Hardware equipment, such as servers from BSC, MGW, IN, SGSN, and other remote location networks, is connected to these networks via routers.
- It is utilized in both wired and wireless communication since it supports a high speed of data transmission due to its utilization of STM connections for connectivity.
- Routers are frequently used by internet service providers to transfer data, such as audio, video, image, and email, from one location to another. Additionally, it can transmit data globally by utilizing the destination’s IP address.
- Routers provide access control. It can be set up so that some users can access all of the data while others can access just a subset of it.

ROUTING PROTOCOL

The router can recognize other routers on the network and decide on a dynamic basis where to deliver all network messages through the routing protocol. Several protocols exist, some of which are listed below:

- **Open Shortest Path First:** As packets travel across several networks, it is utilized to determine the optimal path for them to take in order to arrive at their destination.
- **Border Gateway Protocol (BGP):** It facilitates information sharing between edge routers to control internet packet routing. For routers, it offers network stability. It can easily switch to another network connection to transfer the packets.

Continue….

- **Interior Gateway Routing Protocol (IGRP) :** IGRP outlines the protocol for exchanging routing data between gateways inside the separate networks. The routing information can then be used by the other network protocols to decide how data packets should be routed.
- **Enhanced Interior Gateway Routing Protocol (EIGRP):** This protocol requests a router to route its neighbours if it cannot find a path to a destination from the routing tables. The neighbours then forward the request to further neighbours until a router finds the path.
- **Exterior Gateway Protocol (EGP):** It is also frequently used for the communication of routing table data between internet hosts.