Network Layer in Computer Networks

Lecture (Theory)

Department of Computer Science and Engineering,
Chitkara University, Punjab

Index

CHITKARA UNIVERSITY

1. Concept of IP Packet and Addresses
2. IPV4 Protocol Format
3. Routing Algorithm- Distance Vector Routing
4. Link State Routing

Introduction to Network Layer

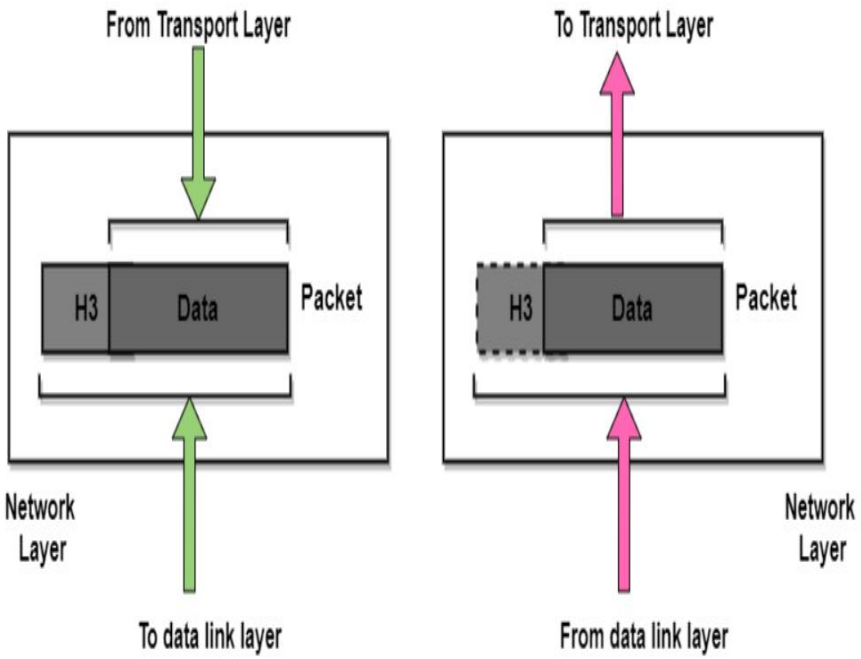
CHITKARA UNIVERSITY

- Network Layer is layer 3 of the OSI reference model. The network layer controls the operation of the subnet. The main aim of this layer is to deliver packets from source to destination across multiple links (networks). It routes the signal through different channels to the other end and acts as a network controller.
- As the data link layer oversees the delivery of the packets between two systems on the same network; the network layer mainly ensures that each packet gets from its point of origin to the final destination.

Introduction to Network Layer

CHITKARA UNIVERSITY

- The main responsibility of the network layer is to deliver individual packets from the source host to the destination host.



IP Packets

CHITKARA UNIVERSITY

- The main function of the internet protocol is to provide addressing to the hosts, encapsulating the data into a packet structure, and routing the data from source to the destination across one or more IP networks. In order to achieve these functionalities, internet protocol provides two major things which are given below.
- **An internet protocol defines two things:**

  -Format of IP packet

  -IP Addressing system

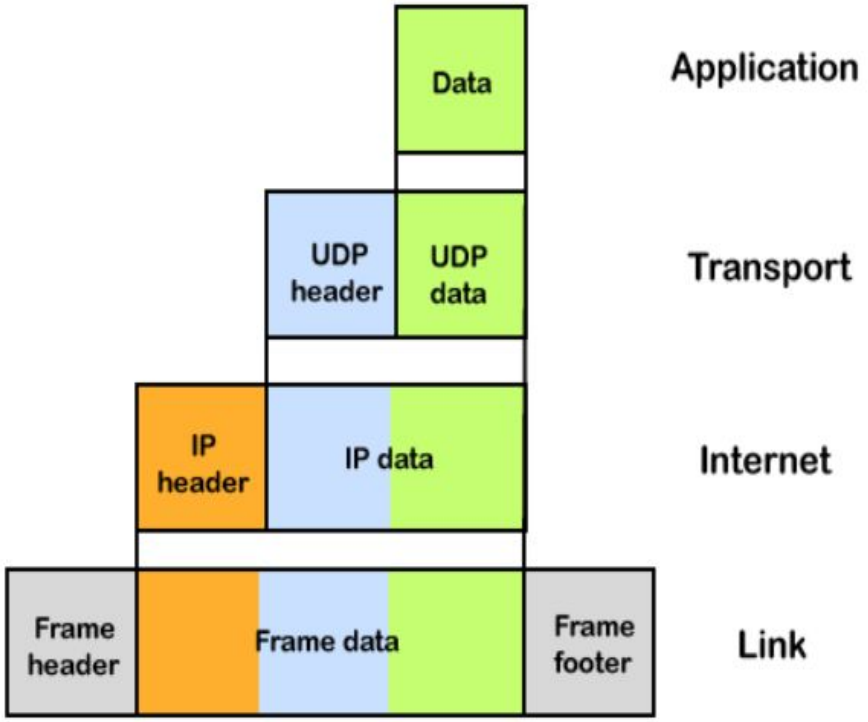
- What is an IP packet?

Before an IP packet is sent over the network, two major components are added in an IP packet, i.e., **header** and a **payload**.

IP Packet

IP Packet

- An IP header contains lots of information the IP packet which includes:
- Source IP address: The source is the one w sending the data.
- Destination IP address: The destination is a that receives the data from the sender.
- Header length
- Packet length
- TTL (Time to Live): The number of hops c before the packet gets discarded.
- Transport protocol: The transport protocol by the internet protocol, either it can be T UDP.
- There is a total of 14 fields exist in th header, and one of them is optional.
- **Payload:** Payload is the data that is to be transported.



How does the IP routing perform?

CHITKARA UNIVERSITY

- IP routing is a process of determining the path for data so that it can travel from the source to the destination. As we know that the data is divided into multiple packets, and each packet will pass through a web of the router until it reaches the final destination. The path that the data packet follows is determined by the routing algorithm. The routing algorithm considers various factors like the size of the packet and its header to determine the efficient route for the data from the source to the destination. When the data packet reaches some router, then the source address and destination address are used with a routing table to determine the next hop's address. This process goes on until it reaches the destination. The data is divided into multiple packets so all the packets will travel individually to reach the destination.
- **For example**, when an email is sent from the email server, then the TCP layer in this email server divides the data into multiple packets, provides numbering to these packets and transmits them to the IP layer. This IP layer further transmits the packet to the destination email server. On the side of the destination server, the IP layer transmits these data packets to the TCP layer, and the TCP layer recombines these data packets into the message. The message is sent to the email application.

What is IP Addressing?

CHITKARA UNIVERSITY

- An IP address is a unique identifier assigned to the computer which is connected to the internet. Each IP address consists of a series of characters like 192.168.1.2. Users cannot access the domain name of each website with the help of these characters, so DNS resolvers are used that convert the human-readable domain names into a series of characters. Each IP packet contains two addresses, i.e., the IP address of the device, which is sending the packet, and the IP address of the device which is receiving the packet.
- **Types of IP addresses**

IPv4 addresses are divided into two categories:

- **Public address**
- **Private address**
- Public address

The public address is also known as an external address as they are grouped under the WAN addresses. We can also define the public address as a way to communicate outside the network. This address is used to access the internet. The public address available on our computer provides the remote access to our computer. With the help of a public address, we can set up the home server to access the internet. This address is generally assigned by the ISP (Internet Service Provider).

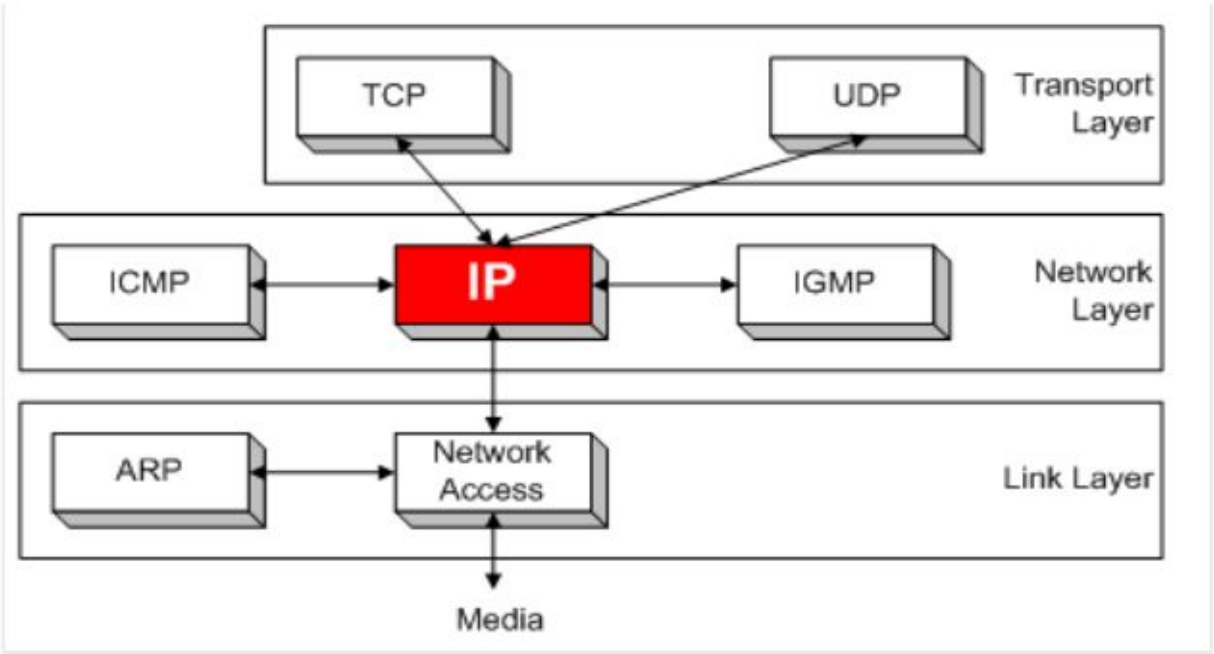
Private Addresses

CHITKARA UNIVERSITY

- A private address is also known as an internal address, as it is grouped under the LAN addresses. It is used to communicate within the network. These addresses are not routed on the internet so that no traffic can come from the internet to this private address. The address space for the private address is allocated using **InterNIC** to create our own network. The private addresses are assigned to mainly those computers, printers, smartphones, which are kept inside the home or the computers that are kept within the organization. For example, a private address is assigned to the printer, which is kept inside our home, so that our family member can take out the print from the printer.
- If the computer is assigned with a private address, then the devices available within the local network can view the computer through the private ip address. However, the devices available outside the local network cannot view the computer through the private IP address, but they can access the computer if they know the router's public address. To access the computer directly, NAT (Network Address Translator) is to be used.

IPv4

- IP (Internet Protocol) is a Network Layer Protocol.



- There are currently two version in use: IPv4 (version 4) and IPv6 (Version 6)
- Here we discuss IPv4

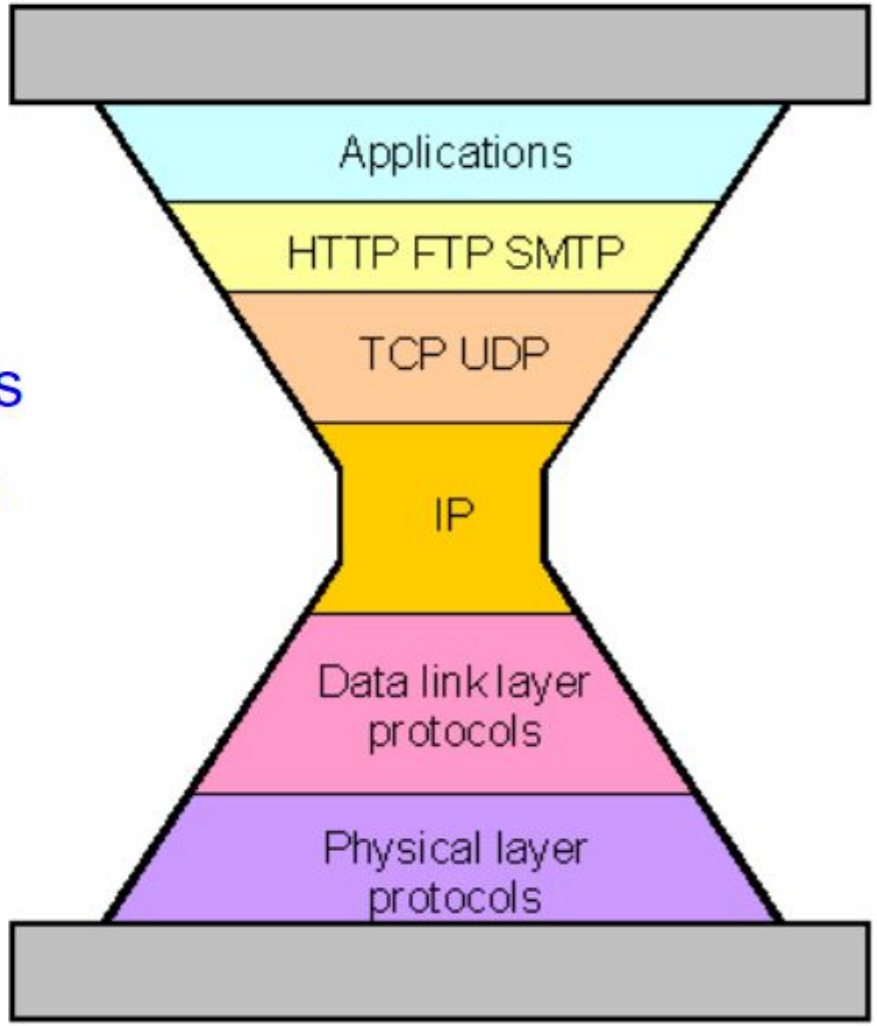
IPv4

CHITKARA UNIVERSITY

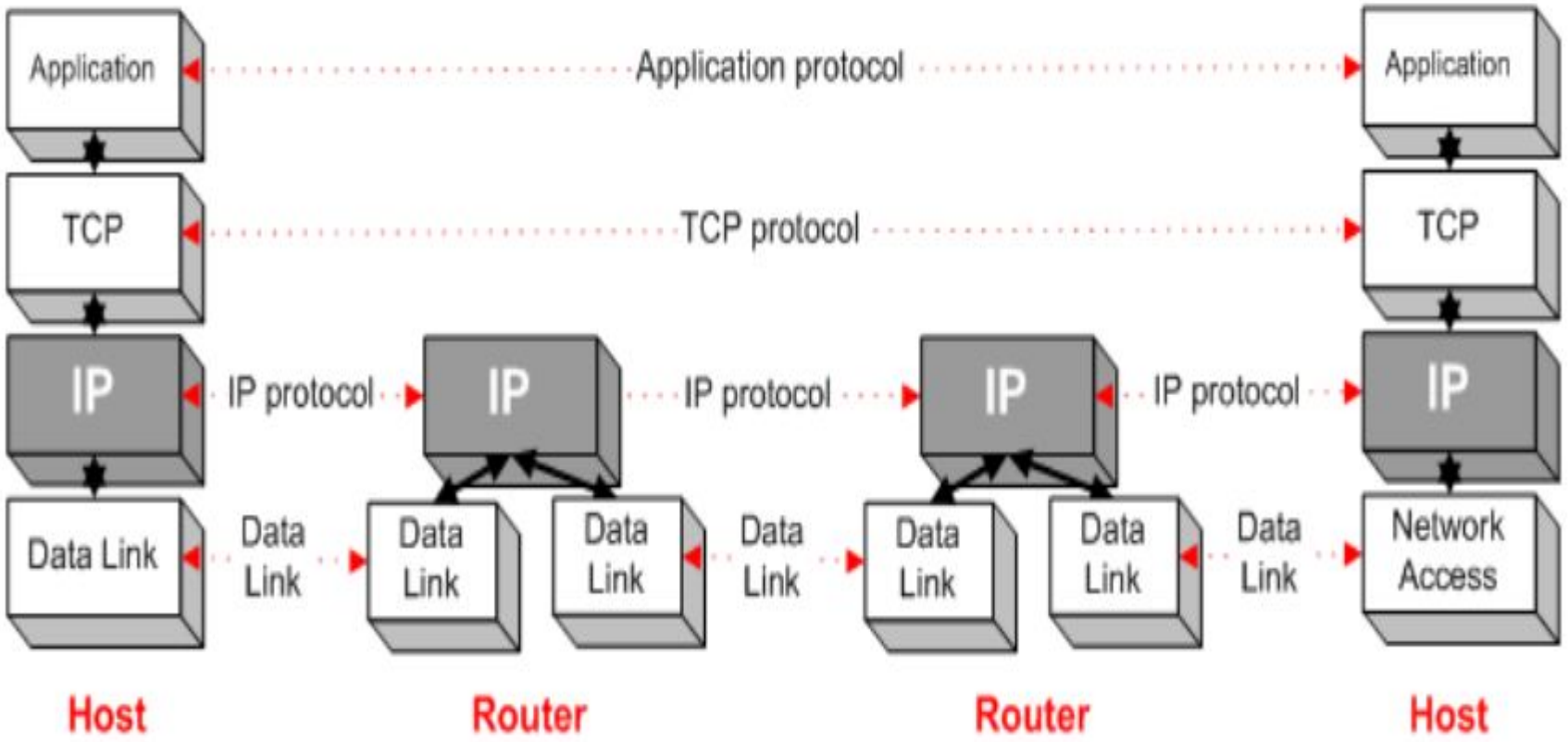
- **IP is the waist of the hourglass of the Internet protocol architecture**

- Multiple higher-layer protocols
- Multiple lower-layer protocols

- Only one protocol at the network layer.



Application Protocol



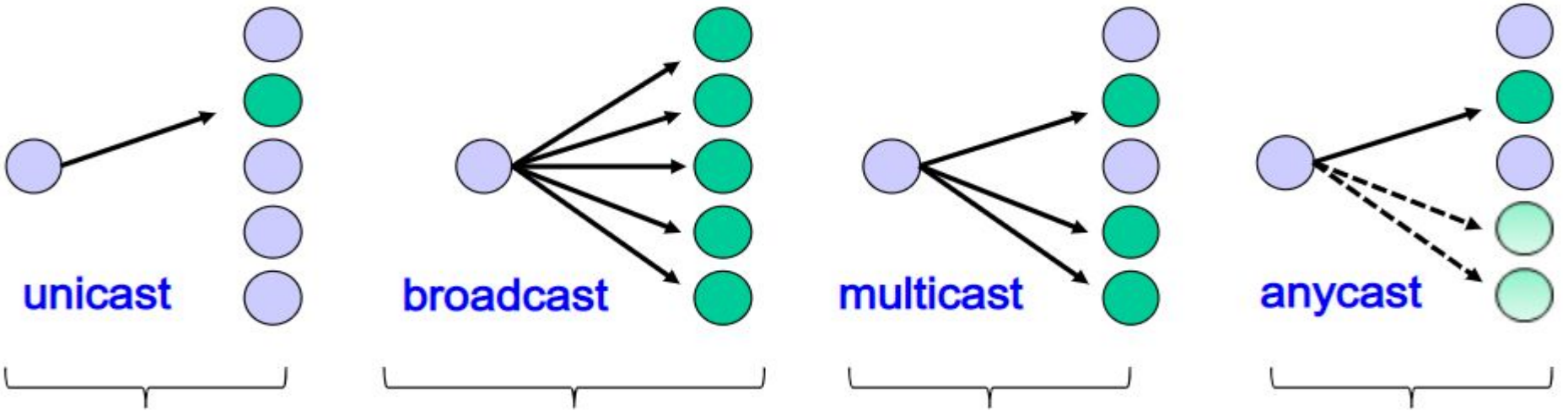
Delivery Modes

Supported by IPv4

- one-to-one (unicast)
- one-to-all (broadcast)
- one-to-many (multicast)

Not supported by IPv4:

- one-to-any (anycast)



Class A, B, C addresses

Broadcast addresses (e.g.,255.255.255.255, 128.100.255.255)

Class D addresses

There are no anycast addresses

IPv4 Address classes

CHITKARA UNIVERSITY

IPv4 class is a way of division of addresses in the IPv4 based routing. Separate IP classes are used for different types of networks. They can be explained as follows

CLASSES	Range
Class A	1.0.0.0 to 127.255.255.255
Class B	128.0.0.0 to 191.255.255.255
Class C	192.0.0.0 to 223.255.255.255
Class D	224.0.0.0 to 239.255.255.255
Class E	240.0.0.0 to 255.255.255.255

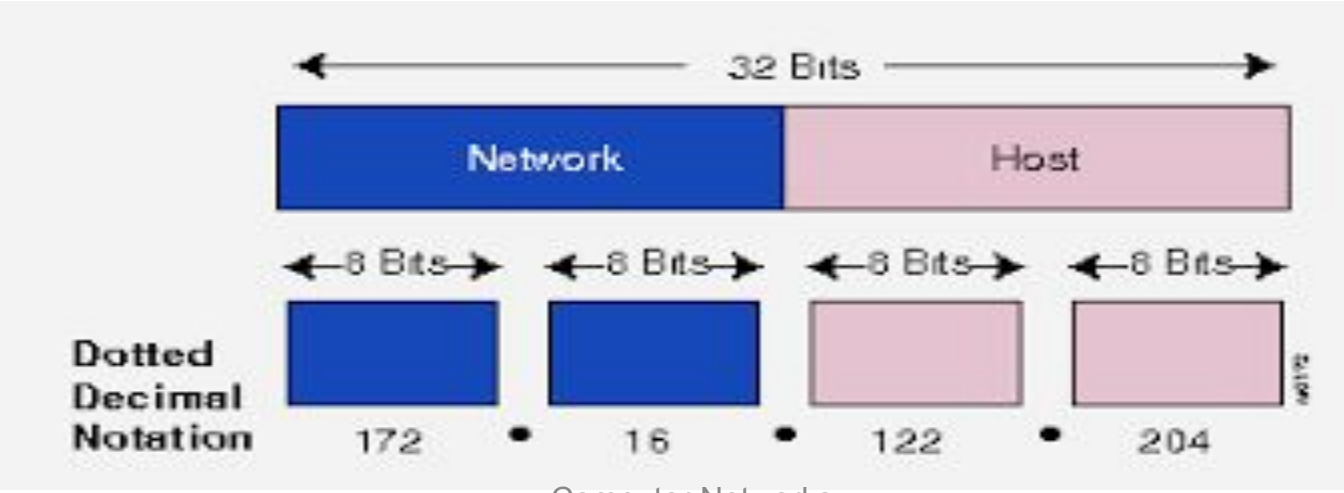
a Router has more than one IP address because router connects two or more different networks. But A computer or host can only have one and a unique ip address. A routers function is to inspect incoming packet and determine whether it belongs to local network or to a Remote Network, if a local packet is determined then there is no need of routing and if a Remote packet is determined then it will route that packet according to the routing table other wise the packet will be discarded.

In the virtual hosting environment, a single machine can act like multiple machines (with multiple domain names and IP addresses.

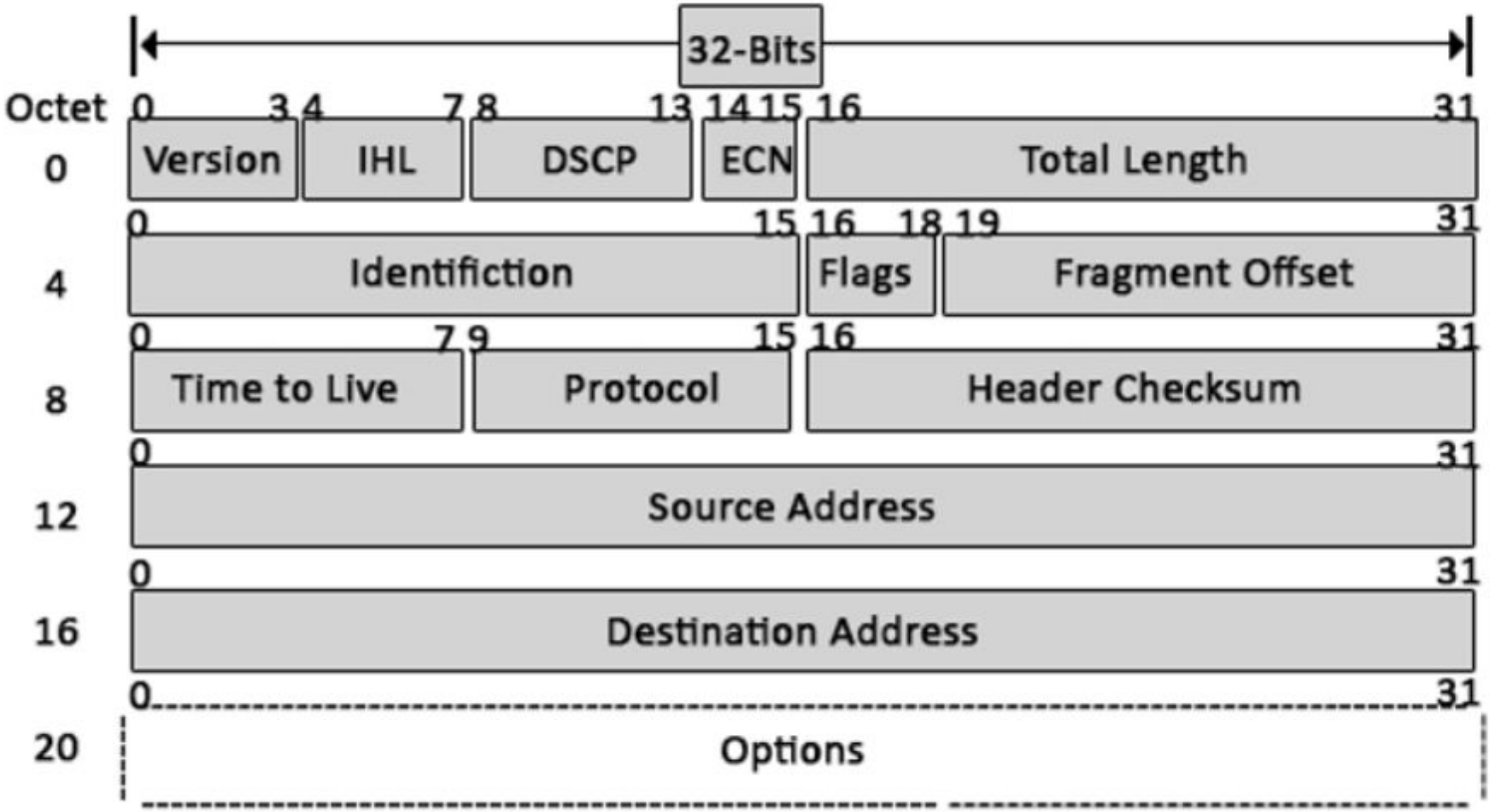
IP Address Format

CHITKARA UNIVERSITY

- The 32-bit IP address is grouped eight bits at a time, separated by dots and represented in decimal format. This is known as dotted decimal notation as shown in fig.
- Each bit in the octet has a binary weight (128,64,32, 16,8,4,2, 1).
- The minimum value for an octet is 0, and the maximum value for an octet is 255.



IPv4 Protocol Format



IPv4 Components

CHITKARA UNIVERSITY

Below is the list mentioned.

1. Version.
2. Internet Header Length.
3. Type of Service.
4. Explicit Congestion Notification.
5. Total Length.
6. Identification.
7. Flags.
8. Fragment Offset
9. Time to live.
10. Protocol.
11. A checksum of header.
12. Source Address.
13. Destination Address.
14. Options.

IPv4 Components

CHITKARA UNIVERSITY

- **Version**: The first header field is a 4-bit version indicator. In the case of IPv4, the value of its four bits is set to 0100, which indicates 4 in binary.
- **Internet Header Length:** IHL is the 2nd field of an IPv4 header, and it is of 4 bits in size. This header component is used to show how many 32-bit words are present in the header. As we know, IPv4 headers have a variable size, so this is used to specify the size of the header to avoid any errors. This size can be between 20 bytes to 60 bytes.
- **Type of Service:** ToS is also called Differentiated Services Code Point or DSCP. This field is used to provide features related to service quality, such as for data streaming or Voice over IP (VoIP) calls. It is used to specific how a datagram will be handled.
- **Explicit Congestion Notification:** ECN is used to send notifications to the sender or receive in situations where network congestion happens. This is an optional feature of IPv4 can; if one of the endpoints don't support it, it is not used.
- **Total Length:** This field's size is 16 bit, and it is used to denote the size of the entire datagram. The minimum size of an IP datagram is 20 bytes, and at the maximum, it can be 65,535 bytes. Practically, all hosts are required to be able to read 576-byte datagrams. If a datagram is too large for the hosts in the network, fragmentation is used, which is handled in the host or packet switch.

IPv4 Components

CHITKARA UNIVERSITY

- **Identification:** The identification or ID field in a packet can identify an IP datagram's fragments uniquely. Some have suggested using this field for other things such as adding information for packet tracing etc.
- **Flags:** flag in an IPv4 header is a three-bit field that is used to control and identify fragments. The following can be their possible configuration:
  - Bit 0: this is reserved and has to be set to zero
  - Bit 1: DF or do not fragment
  - Bit 2: MF or more fragments.
- **Fragment Offset:** This field is 13 bit long in length, and it is measured by blocks that units of 8-byte blocks. These are used to specify the offset of a fragment relative to the start of the IP datagram, which when it was not fragmented. As you can expect, the first offset of a fragment is always set to zero. The maximum possible offset is $(2^{13}-1) * 8 = 65528$, but it is more than the maximum possible IP Packet length, which is 65,535 bytes long with the length of a header added in.
- **Time to live:** Time to live (or TTL in short) is an 8-bit field to indicate the maximum time the datagram will be live in the internet system. The time here is measured in seconds, and in case the value of TTL is zero, the datagram is erased. Every time a datagram is processed, it's Time to live is decreased by one second. These are used so that datagrams that are not delivered are discarded automatically. TTL can be between 0 – 255.

IPv4 Components

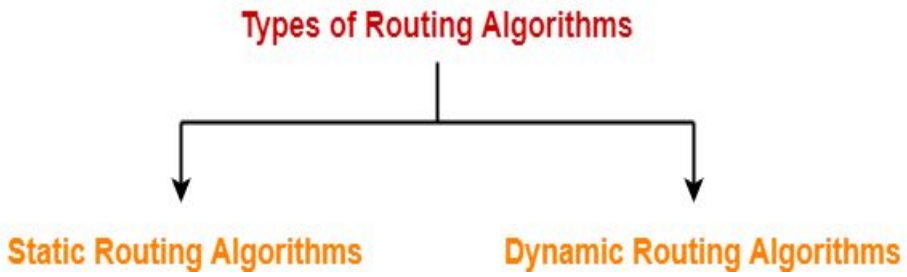
CHITKARA UNIVERSITY

- **Protocol:** This is a filed in the IPv4 header reserved to denote which protocol is used in the later (data) portion of the datagram. For Example, number 6 is used to denote TCP and 17 is used to denote UDP protocol.
- **The header's checksum:** The checksum field is of 16-bit length, and it is used to check the header for any errors. The header is compared to the value of its checksum at each hop, and in case the header checksum is not matching, the packet is discarded. Keep in mind that this is only for the header, and its protocol handles the data field. UDP and TCP, for example, have their own checksum fields.
- **Source Address:** It is a 32-bit address of the source of the IPv4 packet.
- **Destination Address:** the destination address is also 32 bit in size, and it contains the receiver's address.
- **Options**: This is an optional field of the IPv4 header. It is used only when the value of IHL is set to more than 5. These options contain values and settings for things related to security. Record route and time stamp etc. You will find that the list of options component ends with an End of Options or EOL in many cases.

CHITKARA UNIVERSITY

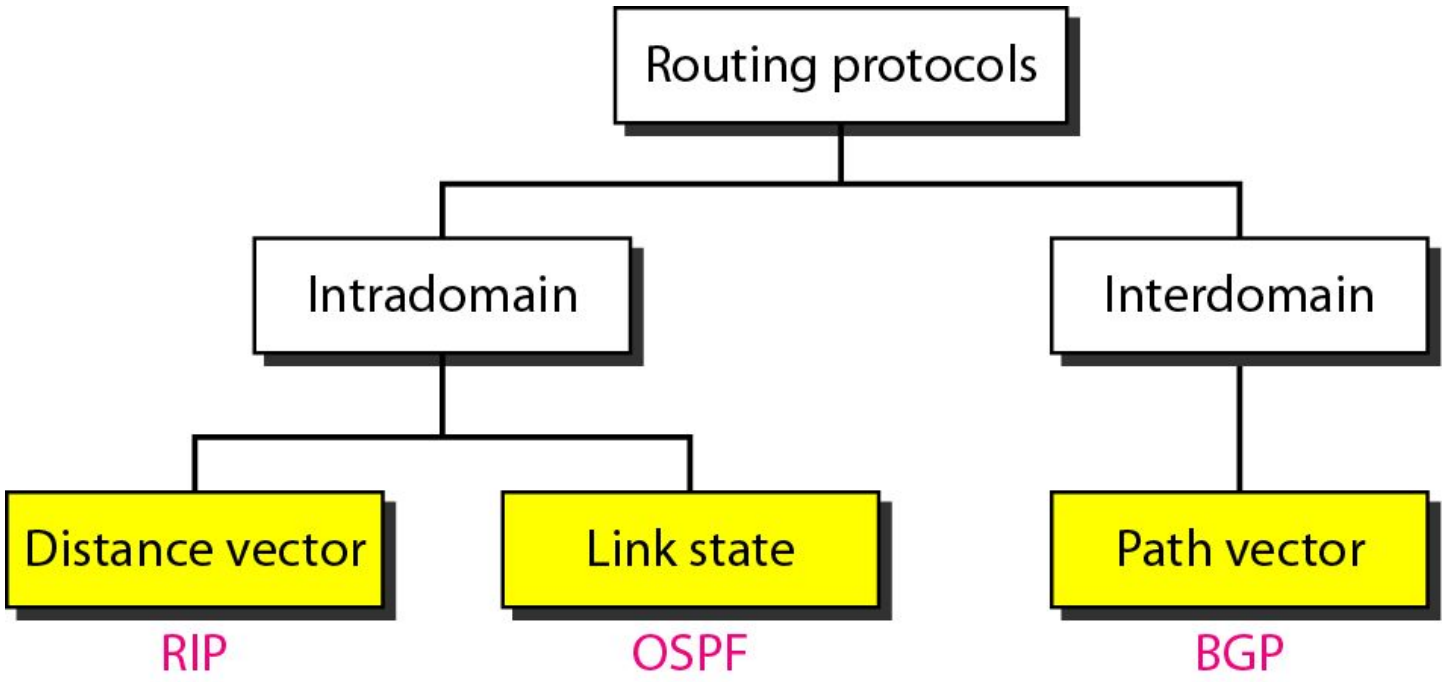
Routing Algorithms-

- Routing algorithms are meant for determining the routing of packets in a node.
- Routing algorithms are classified as-



1. Static Routing Algorithms
2. Dynamic Routing Algorithms

Popular routing protocols



Distance Vector Routing:

CHITKARA UNIVERSITY

- So far we have studied Static Routing Algorithms. But practically dynamic Routing Algorithms are used. Following two are Dynamic Routing Algorithms:
  - 1. Distance Vector Routing Algorithm.
  - 2. Link State Routing Algorithm.
- **Distance Vector Routing Algorithm:**
- At each step within a router:
  - Get routing tables from neighbours
  - Compute distance to neighbours
  - Compute new routing table

1. Router transmits its *distance vector* to each of its neighbors.
2. Each router receives and saves the most recently received *distance vector* from each of its neighbors.
3. A router **recalculates** its distance vector when:
   a. It receives a *distance vector* from a neighbor containing different information than before.
   b. It discovers that a link to a neighbor has gone down (i.e., a topology change).

The DV calculation is based on minimizing the cost to each destination.

The distance vector routing algorithm is sometimes called by other names, the **distributed Bellman-Ford** routing algorithm and the **Ford-Fulkerson algorithm.**

Note

CHITKARA UNIVERSITY

In distance vector routing, each node shares its routing table with its immediate neighbors periodically and when there is a change.

Difference between Link State and Distance Vector

CHITKARA UNIVERSITY

Link State	Distance Vector
link states algorithm is an algorithm **using global information**	the distance vector algorithm is **iterative, asynchronous, and distributed**
each node **talks with all other nodes**, but tell them only the cost of it's directly comparison of some of their attribute	each node **talks to only its directly connected neighbors**, but provides its neighbor with least cost estimates from itself to all the nodes.
Message complexity: With link state, every node has to keep the information about the cost of each link within the network.	**Message complexity**: with distance vector algorithm, message is exchanged between two hosts which are directly connected to each other.
very times, if any of the link cost is changed, all the nodes are **updated.**	change of cost in the link which is belong to the least cost path for one of the nodes, the DV algorithm will update the new value. But if the change doesn't belong to the least cost part between 2 hosts, there will **no updating**.
Speed of convergence: can converge faster in comparison of later.	**Speed of convergence**: can converge slowly and have routing loops while the algorithm is converging.
Such probability is less.	DV algorithm also suffers from the **count to infinity** problem.
Robustness: For LS, when a router is down, it can broadcast a wrong cost for the closest one. LS node is computing for its own forwarding table and other node do the calculation for themselves. **Better than DV.**	**Robustness:** DV, the wrong least cost path can be passed to more than one or all of the node so the wrong calculation will be process in the entire net work. This problem of DV is much **worse than LS algorithm**.

Link State Routing

CHITKARA UNIVERSITY

Each router must do the following:

1. Discover its neighbors, learn their network address.
2. Measure the delay or cost to each of its neighbors.
3. Construct a packet telling all it has just learned.
4. Send this packet to all other routers.
5. Compute the shortest path to every other router.

A complete topology is developed. Then Dijkstra's Algorithm can be used to compute the shortest path.

Following 5 steps are followed to implement it.

1. Learning about the Neighbors
2. Measuring Line Cost.
3. Building Link State Packets.
4. Distributing the Link State Packets.
5. Computing the New Routes.

happy

LEARNING