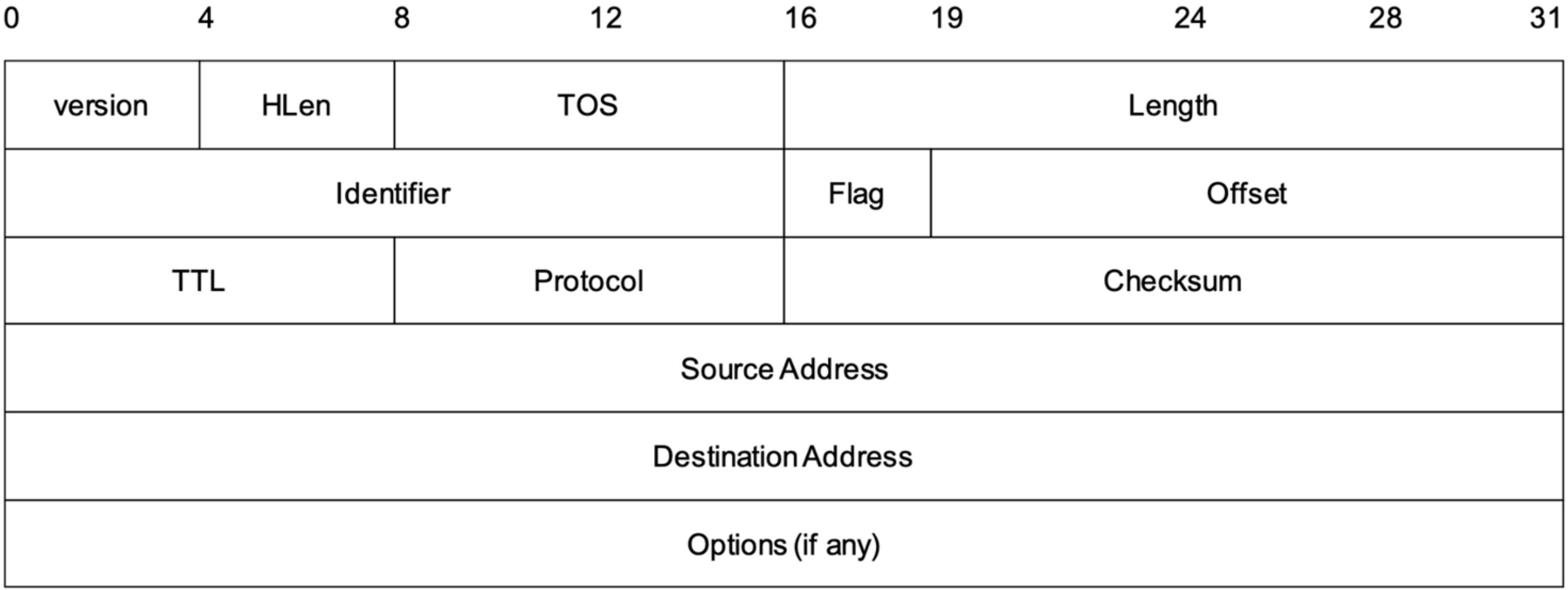
CHAPTER 4
NETWORK LAYER

PREPARED BY: Asst. Prof. Sanjivan Satyal

IPV4 Header



<table>
<tr><th>0</th><th>4</th><th>8</th><th>12</th><th>16</th><th>19</th><th>24</th><th>28</th><th>31</th></tr>
<tr><td>version</td><td>HLen</td><td colspan="2">TOS</td><td colspan="5">Length</td></tr>
<tr><td colspan="4">Identifier</td><td>Flag</td><td colspan="4">Offset</td></tr>
<tr><td colspan="2">TTL</td><td colspan="2">Protocol</td><td colspan="5">Checksum</td></tr>
<tr><td colspan="9">Source Address</td></tr>
<tr><td colspan="9">Destination Address</td></tr>
<tr><td colspan="9">Options (if any)</td></tr>
</table>

IPv4 Header Format

- **Version (4 bits):** Indicates the version number, In this case 4

- **HLEN (Header Length ,4 bits):** Length of headeris 4 bit in 32 bit words. The minimum value is five for a minimum header length of 20 octets

- **TOS (Type-of-Service , 8 bit):** The Type-of-Service field contains an 8- bit binary value that is used to determine the priority of each packet

- **Length (8 bits)**: Total datagram/ packet length ,in bytes (octets)

- **Identifier (16 bits):** A sequence number that, together with the source address, destination address, and user protocol, is intended to uniquely identify a packet

- Flags(3 bits): Only two of the bits are currently defined

1. MF(More Fragments) bit
2. DF(Don't Fragment) bit
3. Future use bit

- Fragment Offset : A router may have to fragment a packet when forwarding it from one medium to another medium that has a smaller MTU *. When fragmentation occurs, the IPv4 packet uses the Fragment Offset field and the MF flag in the IP header to reconstruct the packet when it arrives at the destination host.

- **TTL (Time-to-Live, 8-bit):** Indicates the remaining "life" of the packet
- The TTL value is decreased by at least one each time the packet is processed by a router (that is, each hop). When the value becomes zero, the router discards or drops the packet and it is removed from the network data flow
- **Protocol (8-bits):** Indicates the data payload type that the packet is carrying (TCP/UDP).

- **Destination Address(32 bits):** value that represents the packet destination Network layer host address
- **Source Address (32 bit):** value that represents the packet source Network layer host address

Address Depletion Problem in Internet

Because of limited number of IP and increasing demand of IP in internet over years lead to depletion of IP address

Solution of depletion are mainly

1. NAT
2. Subnetting
3. IPv6

Network Address Translation (NAT)

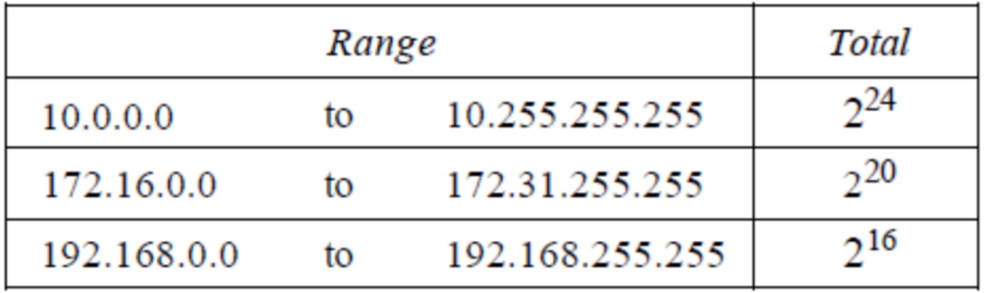
- IP address have public range and private range

- Public range is used for communication in internet and can used only

with permission of internet authorities

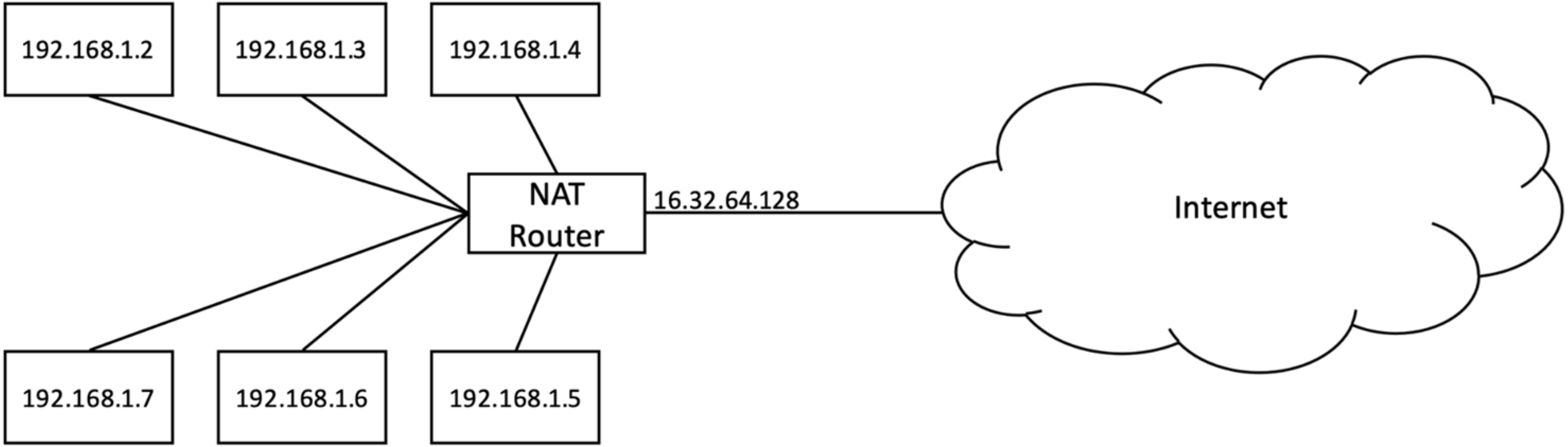
- Private IP can be used for local communication without permission of Internet authorities

Given below table shows private ranges of class A,B,C



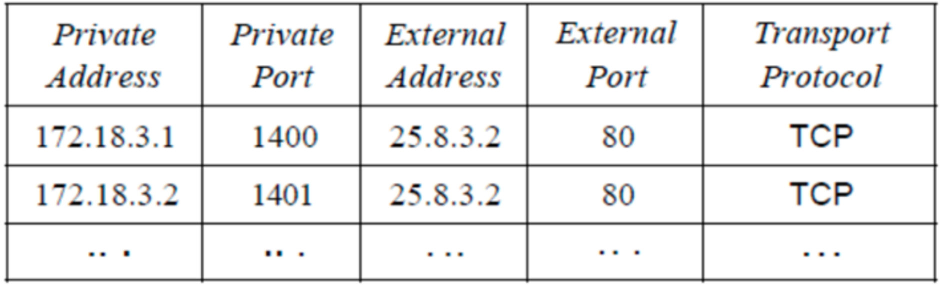
Range			*Total*
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

- Public IP should be unique globally
- Private IP should be unique inside a organization, not globally
- NAT router consist of public IP in exit interface and internal interface consist of Private IPs



- Address Translation : Replace outgoing packets Source IP address as NAT router public IP and replaces incoming packet Destination IP with private (Private to public and public to private)
- Translation is done with help of translation table which consist of IP address of private range and public range and port address

Below table showing Translation table in NAT



Private Address	*Private Port*	*External Address*	*External Port*	*Transport Protocol*
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
.. .	.. .	. . .	. . .	. . .

Limitations of IPv4

- Exponential growth of the Internet and the impending exhaustion of the IPv4 address space
- Need for simpler configuration
- Requirement for security at the IP level
- Need for better support for prioritized and real-time delivery of data

IPv6

- An IPv6 address consists of 16 bytes (octets); it is 128 bits long
- IPv6 specifies hexadecimal colon notation. In this notation,
- 128 bits is divided into eight sections, each 2 bytes in length. Two bytes in hexadecimal
- notation requires four hexadecimal digits. Therefore, the address consists of 32 hexadecimal
- digits, with every four digits separated by a colon
- 128 bits = 16 bytes = 32 hexadecimal digits
- IPv6 has a much larger address space; 2^128 addresses are available

Example IPv6

FDEC: 0074 : 0000 : 0000 : 0000 : BOFF : 0000 : FFFO

- Types of IPv6 Address

- Unicast address : Packet delivered to one node

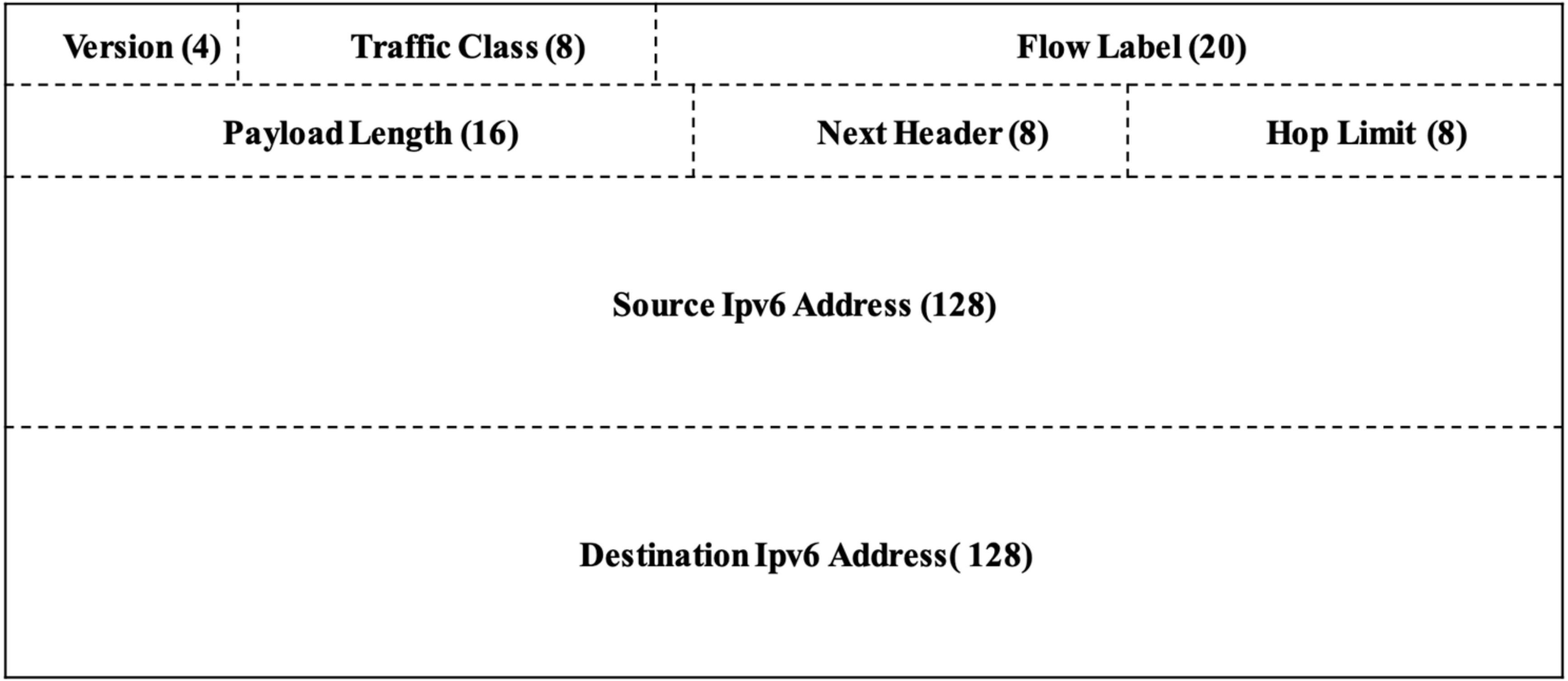
- Multicast address : Packet delivered to group of nodes

- Any cast address : Similar to multicast but delivered to nearest node • Reserved Address

IPv6 Features

1. New header format
2. Large address space
3. Stateless and stateful address configuration
4. IPsec header support required
5. Better support for prioritized delivery
6. New protocol for neighboring node interaction 7. Extensibility

IPV6 Header Format



Version (4)

Traffic Class (8)

Flow Label (20)

Payload Length (16)

Next Header (8)

Hop Limit (8)

Source Ipv6 Address (128)

Destination Ipv6 Address(128)

- **Version (4 bit):** Indicates version (6) of IP packet.

- **Traffic Class (8 bit):** Facilitates the handling of real time data by router. It Prioritize the packets (packet is send /dropped based on priority)

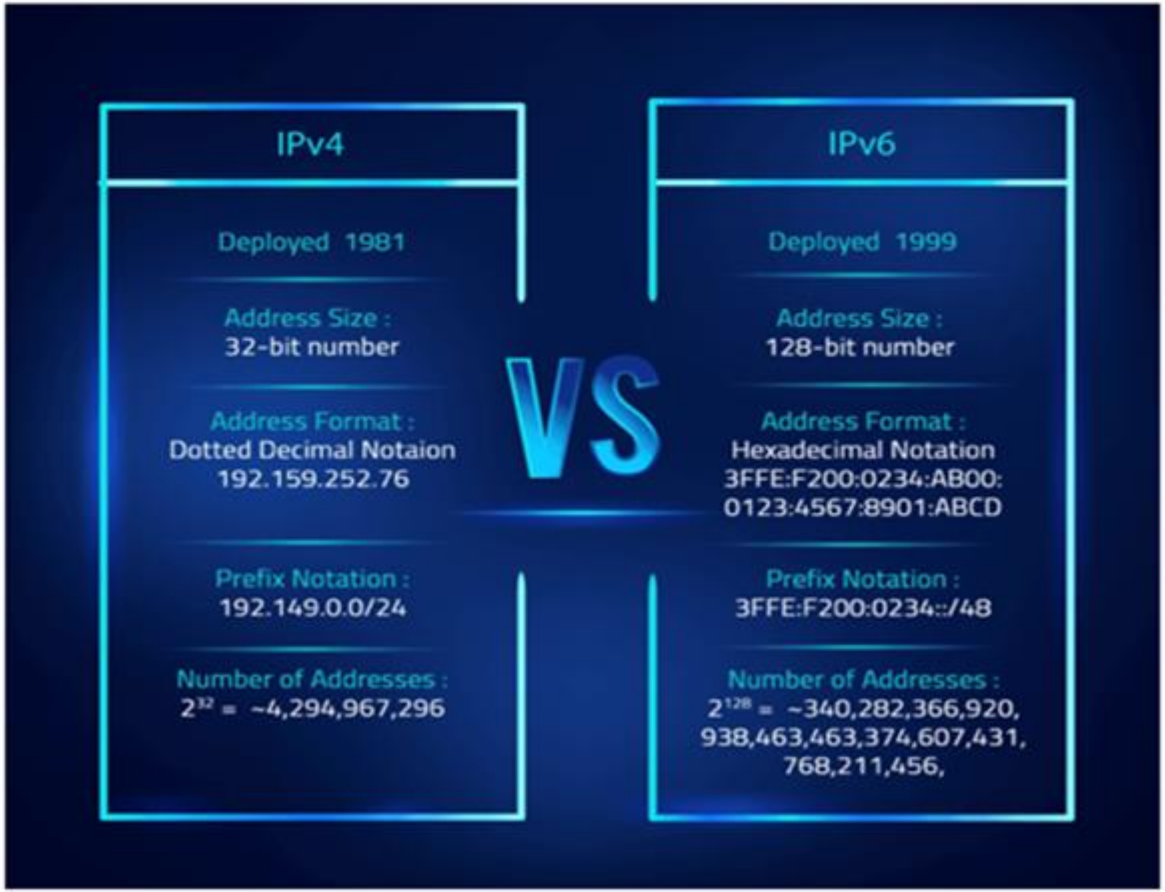
- **Flow Control (20 bit):** Used to label sequences of packets that require the same treatment for more efficient processing on routers.

- **Payload Length (16 bit):** Length of data carried after IPv6 header.

- **Next Header (8 bit):** Identifies the higher level protocol(identify the start of higher level header) **Hop Limit (8 bit):** This field indicates how long packet can remain in network.

- **Source Address (128 bit):** This Field indicates the IPv6 address from which packet is generated.

- **Destination Address (128 bit):** This field indicates the IPv6 address to which packet is going



IPv4

Deployed 1981

Address Size :
32-bit number

Address Format :
Dotted Decimal Notaion
192.159.252.76

Prefix Notation :
192.149.0.0/24

Number of Addresses :
2^{32} = ~4,294,967,296

VS

IPv6

Deployed 1999

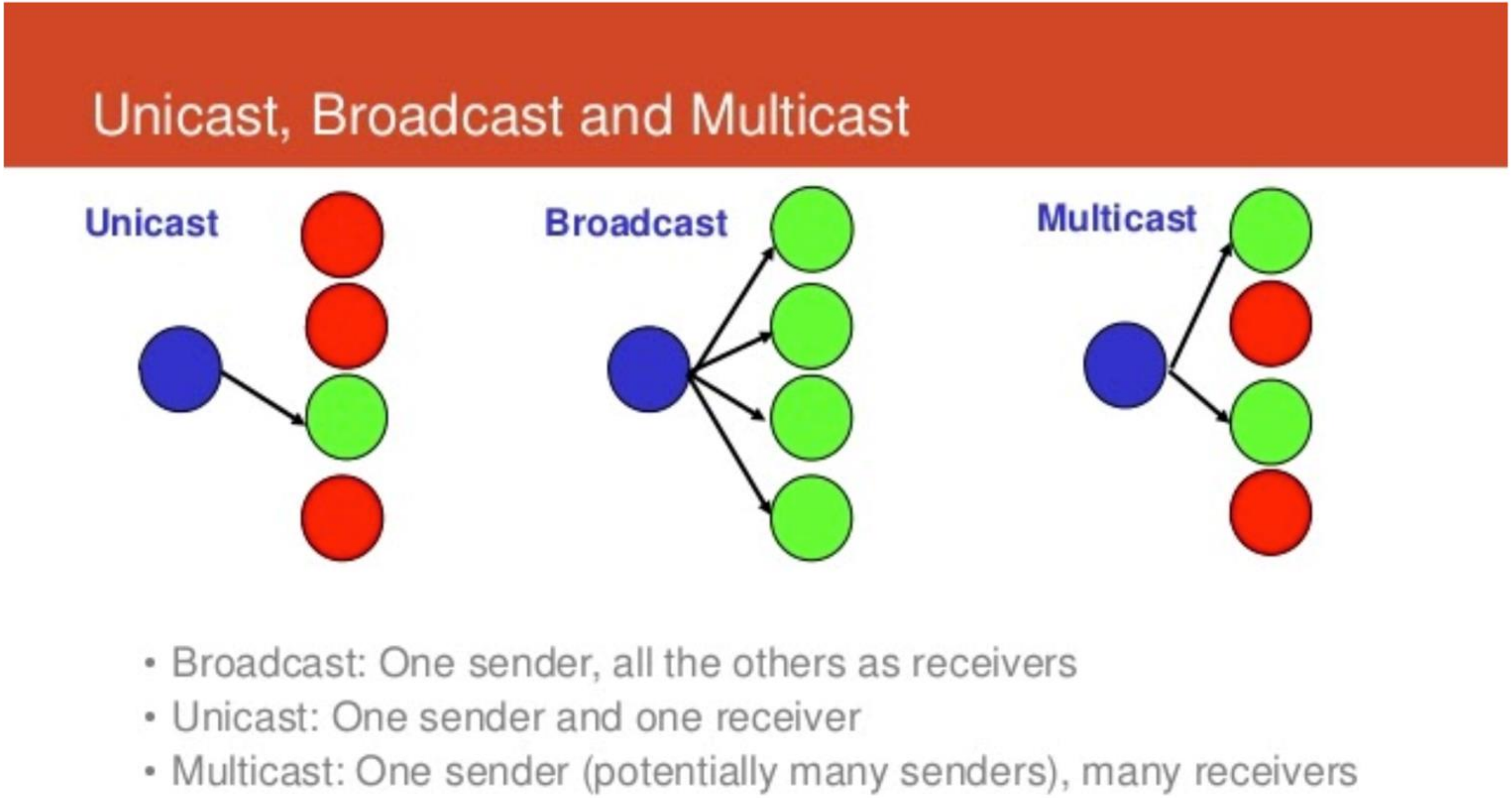
Address Size :
128-bit number

Address Format :
Hexadecimal Notation
3FFE:F200:0234:AB00:
0123:4567:8901:ABCD

Prefix Notation :
3FFE:F200:0234::/48

Number of Addresses :
2^{128} = ~340,282,366,920,
938,463,463,374,607,431,
768,211,456,

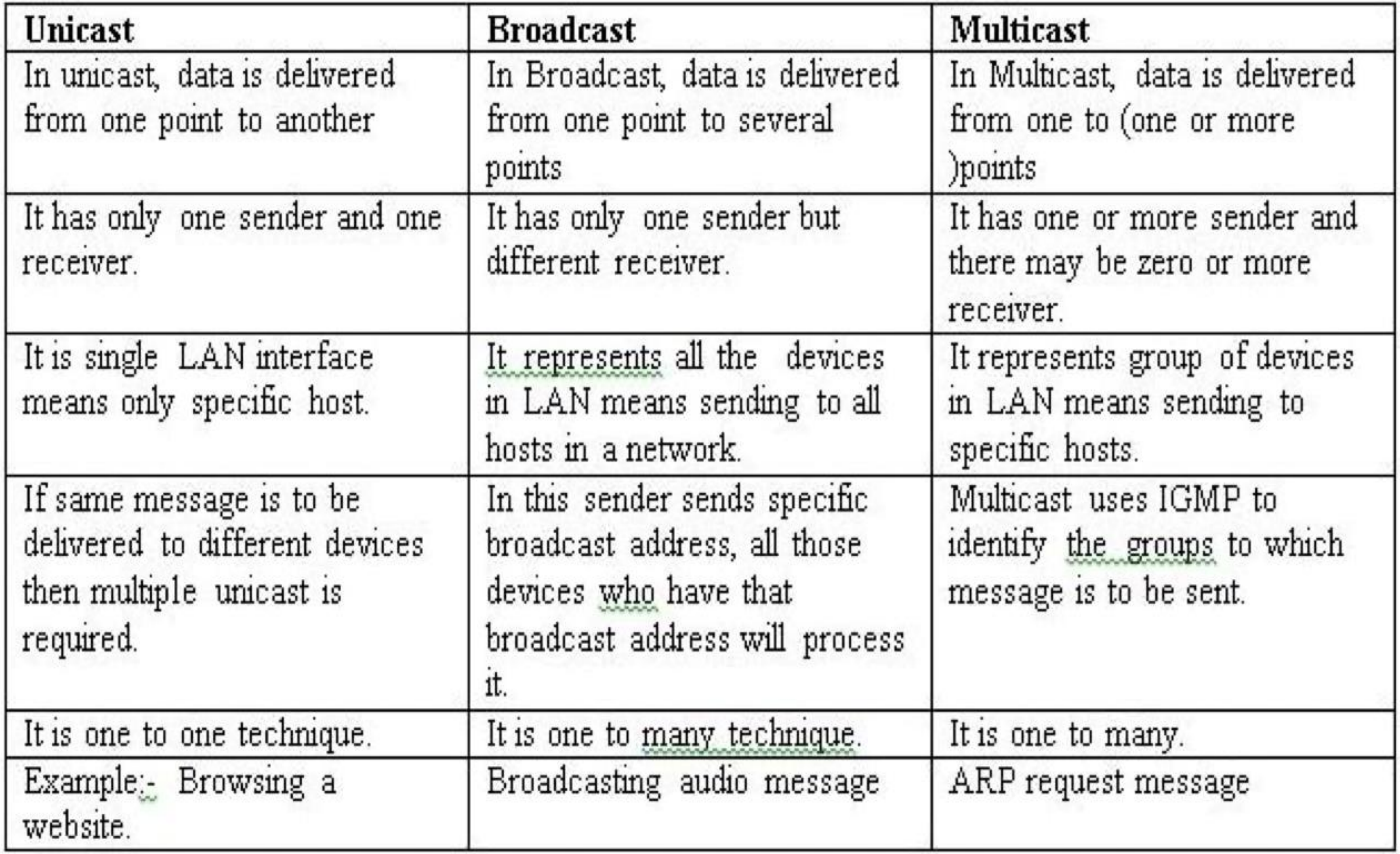
IPv6 - Addressing Modes



Unicast, Broadcast and Multicast

- Broadcast: One sender, all the others as receivers
- Unicast: One sender and one receiver
- Multicast: One sender (potentially many senders), many receivers

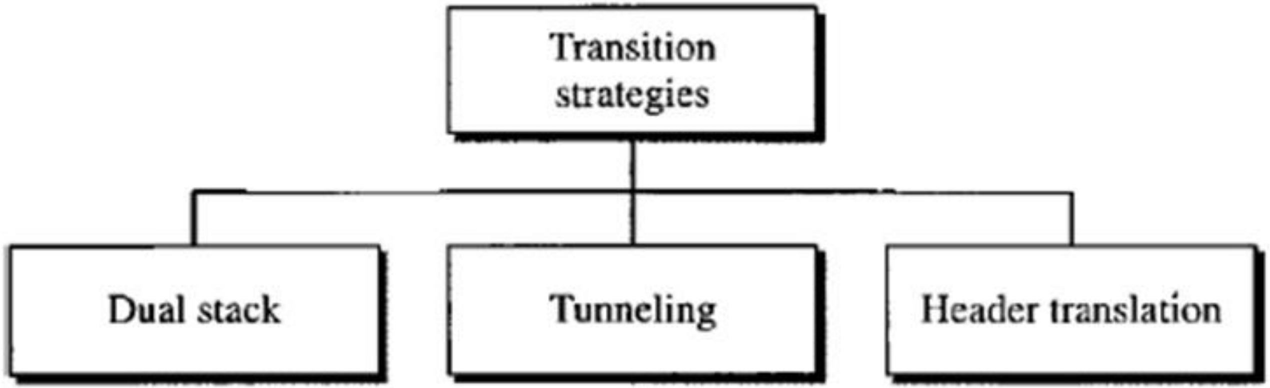
Multicast (Anycast)



Unicast	Broadcast	Multicast
In unicast, data is delivered from one point to another	In Broadcast, data is delivered from one point to several points	In Multicast, data is delivered from one to (one or more)points
It has only one sender and one receiver.	It has only one sender but different receiver.	It has one or more sender and there may be zero or more receiver.
It is single LAN interface means only specific host.	It represents all the devices in LAN means sending to all hosts in a network.	It represents group of devices in LAN means sending to specific hosts.
If same message is to be delivered to different devices then multiple unicast is required.	In this sender sends specific broadcast address, all those devices who have that broadcast address will process it.	Multicast uses IGMP to identify the groups to which message is to be sent.
It is one to one technique.	It is one to many technique.	It is one to many.
Example:- Browsing a website.	Broadcasting audio message	ARP request message

TRANSITION FROM IPv4 TO IPv6

Figure 20.18 *Three transition strategies*

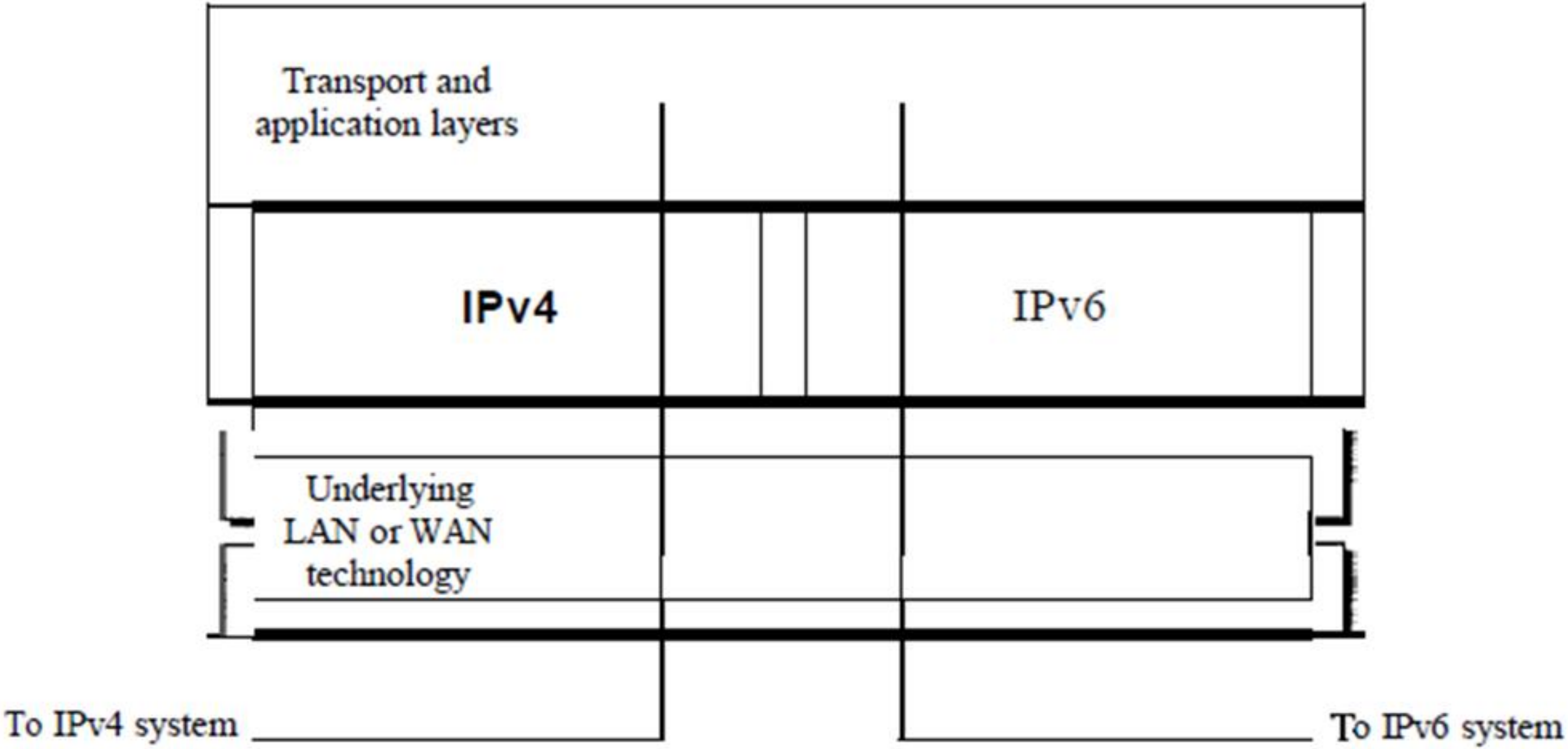


Dual Stack

- It is recommended that all hosts, before migrating completely to version 6, have a dual stack of protocols.

- In other words, a station must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6.

Figure 20.19 *Dual stack*


Transport and application layers
IPv4
IPv6
Underlying LAN or WAN technology
To IPv4 system
To IPv6 system

Tunneling

- Tunneling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4.

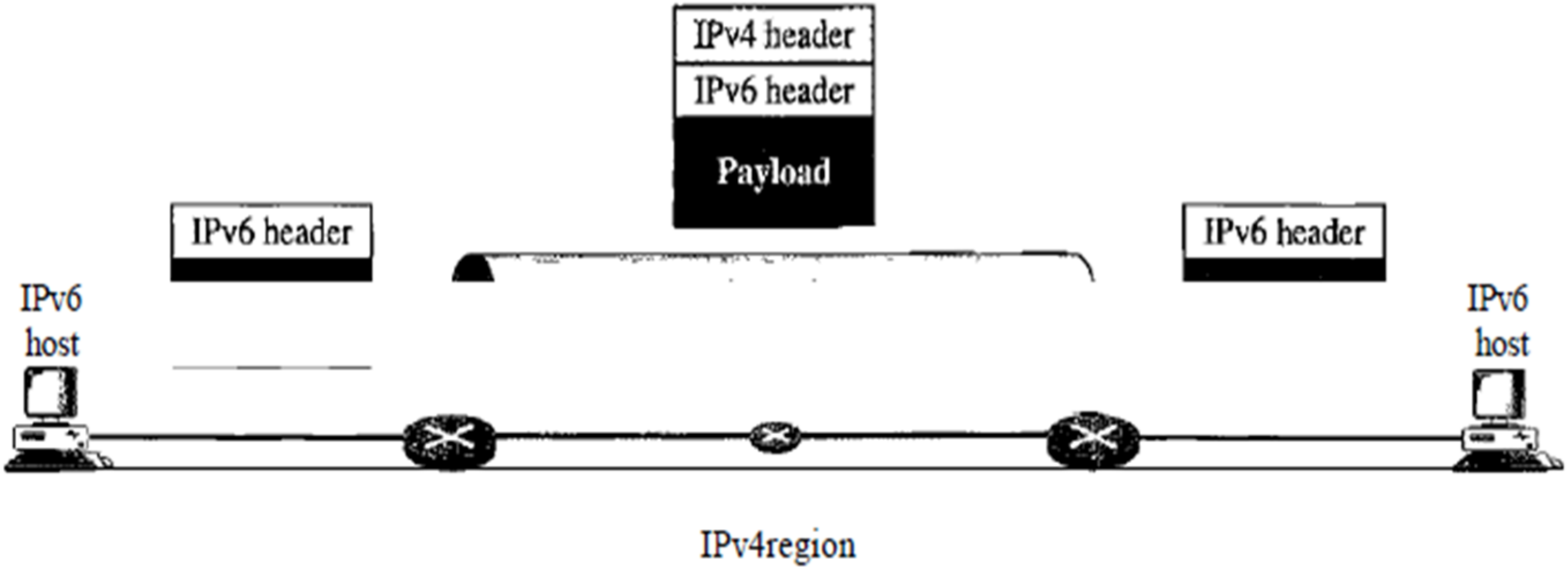
- To pass through this region, the packet must have an IPv4 address.

- So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exits the region.

- It seems as if the IPv6 packet goes through a tunnel at one end and emerges at the other end.

- To make it clear that the IPv4 packet is carrying an IPv6 packet as data, the protocol value is set to 41.

Figure 20.20 *Tunneling strategy*



Header translation

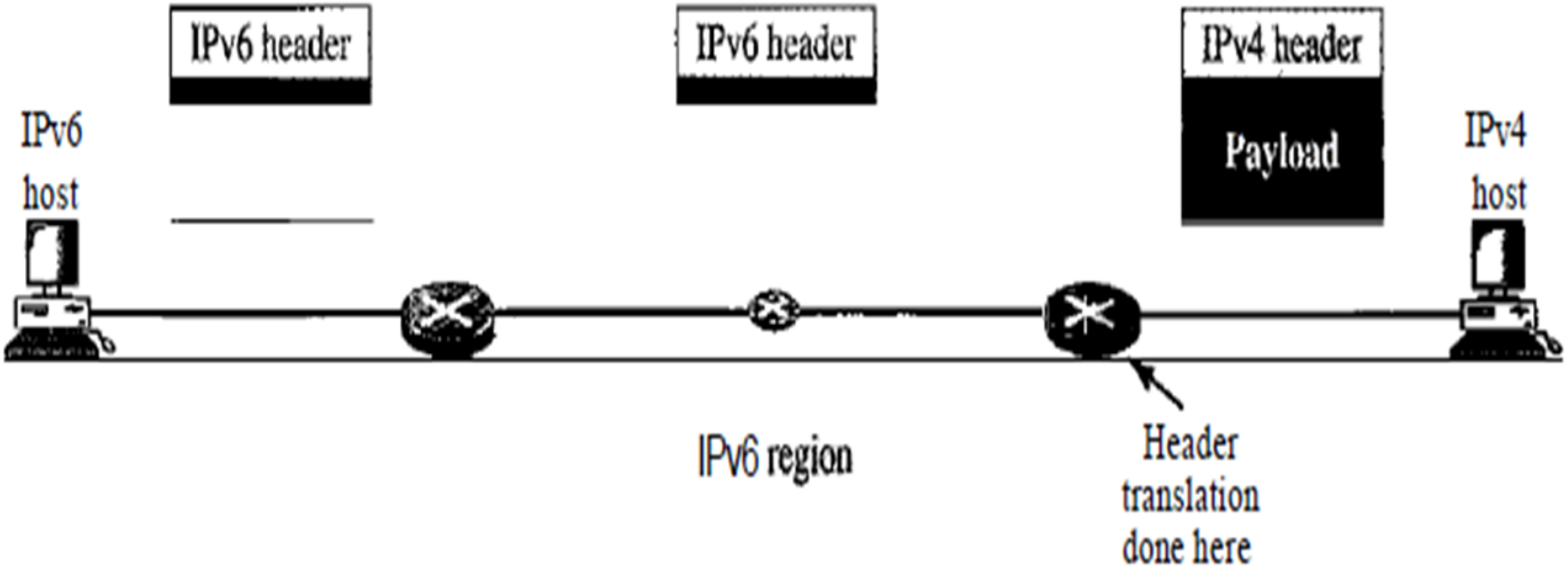
- Header translation is necessary when the majority of the Internet has moved to IPv6 but some systems still use IPv4.

- The sender wants to use IPv6, but the receiver does not understand IPv6.

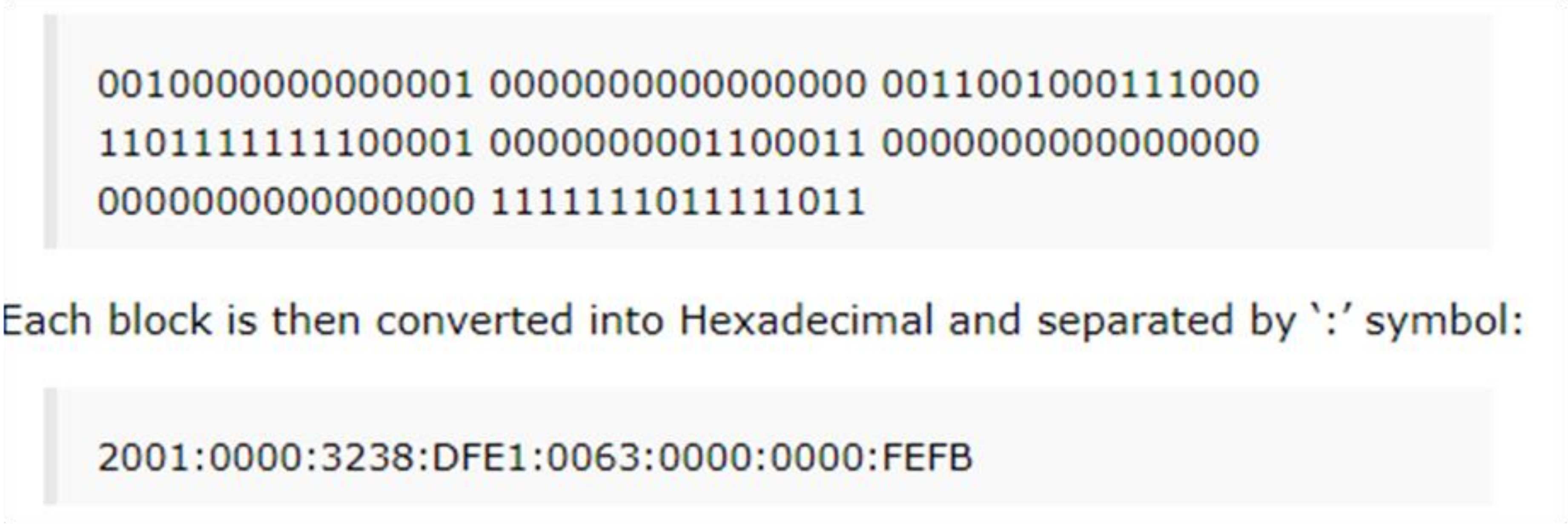
- Tunneling does not work in this situation because the packet must be in the IPv4 format to be understood by the receiver.

- In this case, the header format must be totally changed through header translation. The header of the IPv6 packet is converted to an IPv4 header

Figure 20.21 *Header translation strategy*



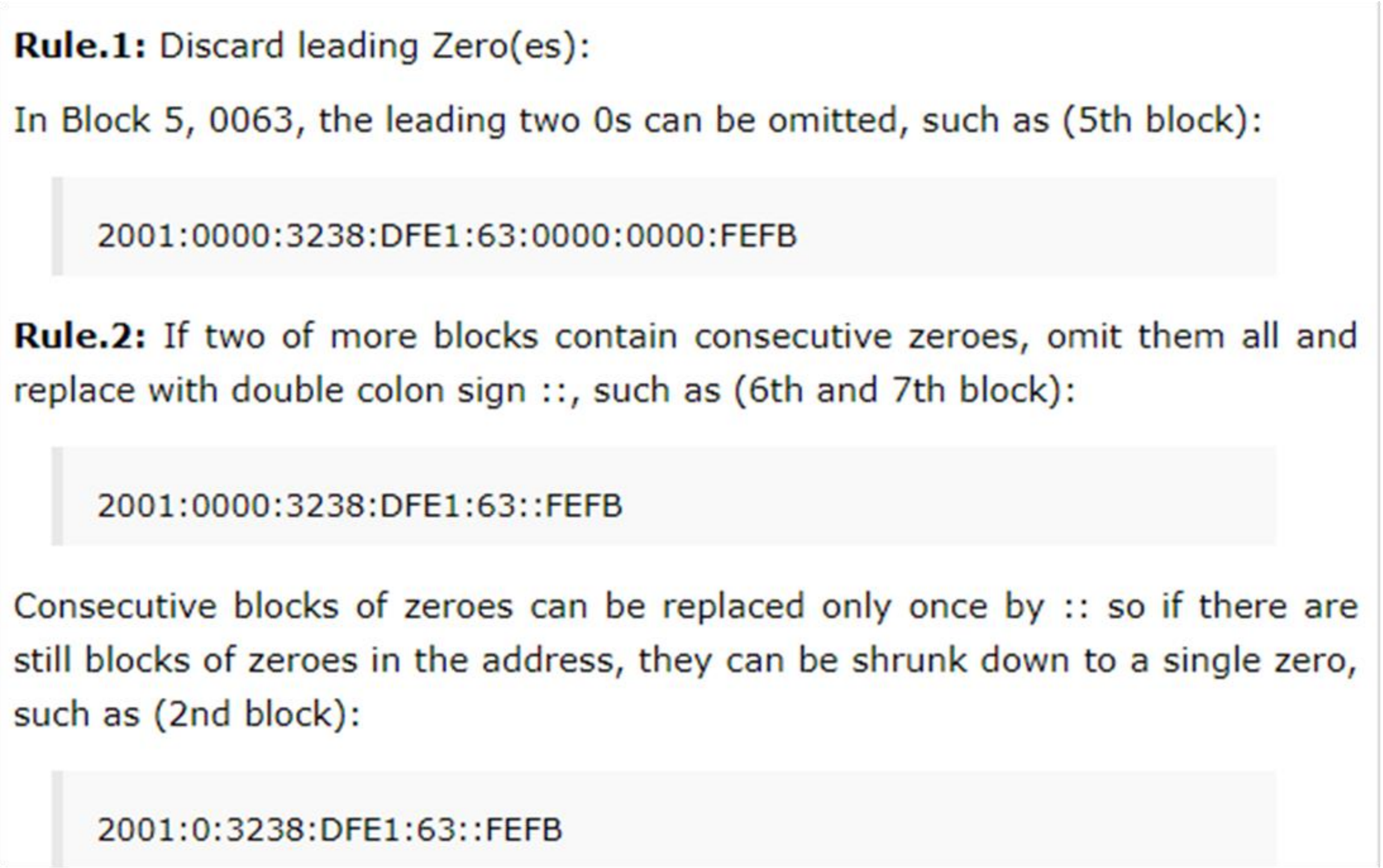
Address of IPV6



```
0010000000000001 0000000000000000 0011001000111000
1101111111100001 0000000001100011 0000000000000000
0000000000000000 1111111011111011
```

Each block is then converted into Hexadecimal and separated by ‘:’ symbol:

```
2001:0000:3238:DFE1:0063:0000:0000:FEFB
```



Rule.1: Discard leading Zero(es):

In Block 5, 0063, the leading two 0s can be omitted, such as (5th block):

```
2001:0000:3238:DFE1:63:0000:0000:FEFB
```

Rule.2: If two of more blocks contain consecutive zeroes, omit them all and replace with double colon sign ::, such as (6th and 7th block):

```
2001:0000:3238:DFE1:63::FEFB
```

Consecutive blocks of zeroes can be replaced only once by :: so if there are still blocks of zeroes in the address, they can be shrunk down to a single zero, such as (2nd block):

```
2001:0:3238:DFE1:63::FEFB
```

ROUTING

- When a device has multiple paths to reach a destination, it always **selects one path by preferring it over others.**
- This selection process is termed as **Routing.**
- Routing is done by special network devices called routers
- A router is always configured with some **default route.**
- A default route tells the router where to forward a packet if there is **no route found for specific destination.**
- In case there are multiple path existing to reach the same destination, router can make decision based on the following information:

- Hop Count: refers to the number of **intermediate devices** through which data must pass between source and destination.

- Bandwidth: the amount of data that can be transmitted in a fixed amount of time.

- Metric : is a unit that help the router choose the best route among multiple feasible routes to a destination.

- Delay: **delay** of a **network** specifies how long it takes for a bit of data to travel across the **network** from one node or endpoint to another

Routing Technique

- Routing is the process of selecting best paths in a network.
- In packet switching networks, routing directs packet forwarding through intermediate nodes.

Static Vs Dynamic Routing

- In static routing the routes are described by fixed paths through a data network.
- The routes are entered by system administrator.
- The whole network can be configured by using static routes.

- **Advantages of Static Routing**
- Minimal CPU/Memory overhead
- No bandwidth overhead (updates are not shared between routers)

Disadvantages of Static Routing

- Infrastructure changes must be manually adjusted
- No “dynamic” fault tolerance if a link goes down
- Impractical on large network

Dynamic Routing

- Dynamic routing protocols are the applications which discover network destinations dynamically.
- Routers will communicate the adjacent routers which informs the network to which each router is connected.
- These routers adjusts automatically in a network when traffic changes.

Advantages of Dynamic Routing

- Simpler to configure on larger networks
- Will dynamically choose a different (or better) route if a link goes down
- Ability to load balance between multiple links

Static Vs Dynamic Routing

- Static routing **manually sets up the optimal paths** between the source and the destination computers.
- On the other hand, the dynamic routing uses **dynamic protocols to update the routing table** and to **find the optimal path** between the source and the destination computers.
- The static routing is **suitable for very small networks** and they cannot be used in large networks.
  As against this, dynamic routing is **used for larger networks**.
- The manual routing has **no specific routing algorithm**.
  The dynamic routers are **based on various routing algorithms like OSPF (Open Shortest Path First), IGRP (Interior Gateway Routing Protocol) and RIP (Routing Information Protocol).**

- The static routing is the **simplest way of routing** the data packets from a source to a destination in a network.
  The dynamic routing uses **complex algorithms for routing** the data packets.
- The static routing has the **advantage that it requires minimal memory.**
  Dynamic router, however, **require large memory,** depending on the routing algorithms used.
- The **network administrator finds out the optimal** path and makes the changes in the routing table in the case of static routing.
  In the dynamic routing algorithm, **the algorithm and the protocol is responsible for routing the packets and making the changes** accordingly in the routing table.

Routing Table

- A routing table is **a set of r**ules, often viewed in table format that is used to determine **where data packets traveling** over an Internet Protocol (IP) network **will be directed.**
- All IP-enabled devices, including routers and switches, use routing tables.
- A routing table contains the information necessary to forward a packet along the best path toward its destination.
- Each packet contains information about its **origin and destination.**
- When a packet is received, a network device examines the packet and matches it to the routing table entry providing the best match for its destination.
- The table then provides the device with **instructions for sending the packet to the next hop on its route** across the network.

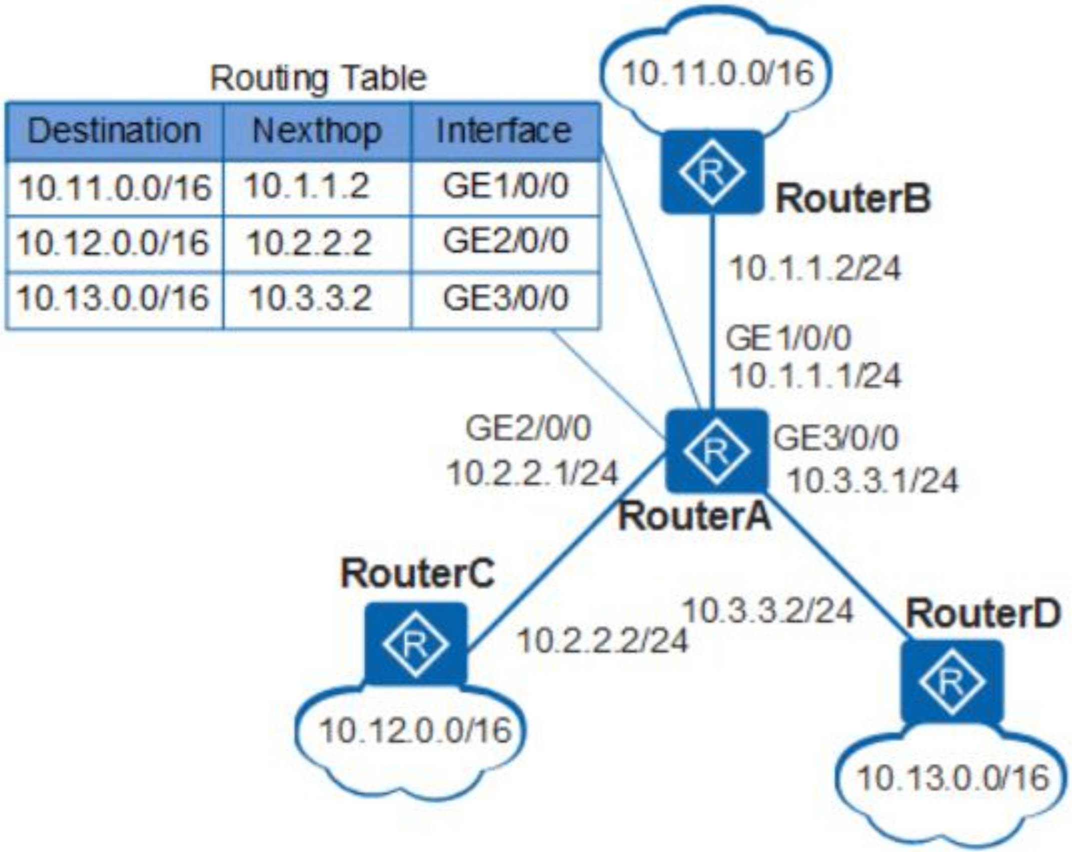
- A basic routing table includes the following information:
- Destination: The IP address of the packet's final destination
- Next hop: The IP address to which the packet is forwarded
- Interface: The outgoing network interface the device should use when forwarding the packet to the next hop or final destination
- Metric: Assigns a cost to each available route so that the most cost-effective path can be chosen
- Routes: Includes directly-attached subnets, indirect subnets that are not attached to the device
- Reference count: no of active use for each route

- Routing tables can be **maintained manually or dynamically.**

- Tables for **static network** devices **do not change unless a network administrator manually changes them.**

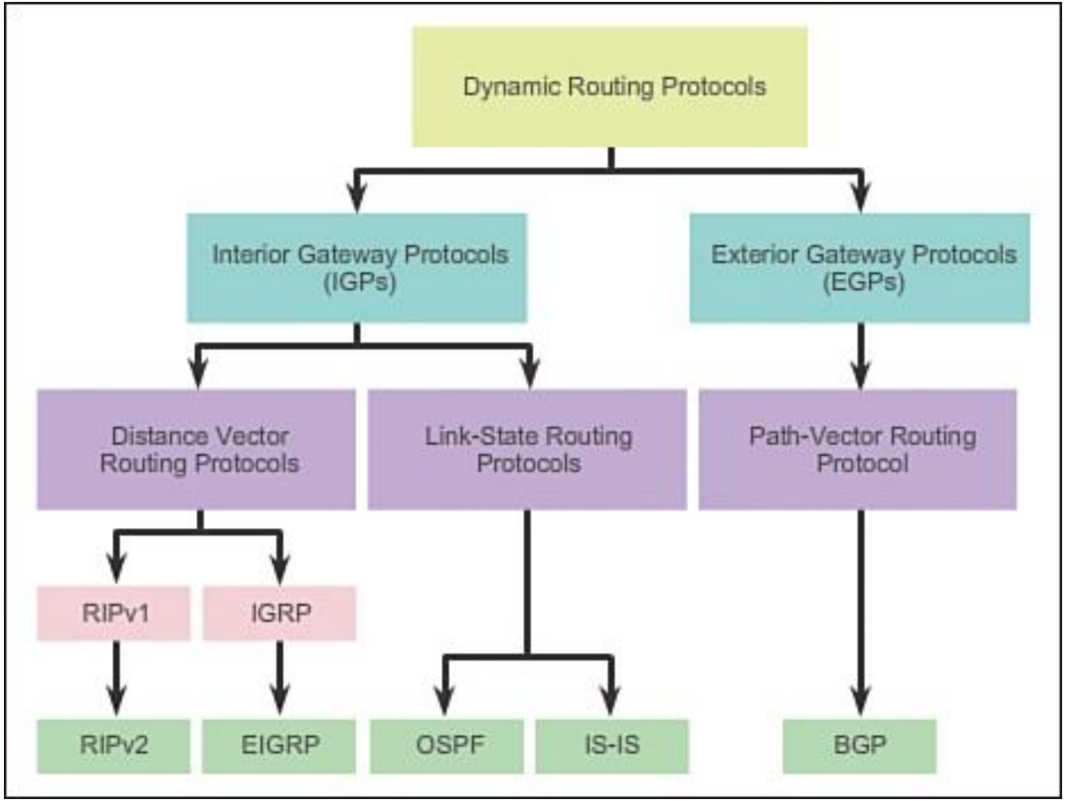
- In dynamic routing, devices build and **maintain their routing tables automatically by using routing protocols** to exchange information about the surrounding network topology.

- Dynamic routing tables **allow devices to "listen" to the network and respond to occurrences like device failures and network congestion.**



Routing Table

Destination	Nexthop	Interface
10.11.0.0/16	10.1.1.2	GE1/0/0
10.12.0.0/16	10.2.2.2	GE2/0/0
10.13.0.0/16	10.3.3.2	GE3/0/0


Dynamic Routing Protocols
Interior Gateway Protocols (IGPs)
Exterior Gateway Protocols (EGPs)
Distance Vector Routing Protocols
Link-State Routing Protocols
Path-Vector Routing Protocol
RIPv1
IGRP
RIPv2
EIGRP
OSPF
IS-IS
BGP

Metrics

Metric in real world means measure

- **Router metrics** are metrics used by a router to make routing decisions
- Metric is the cost assigned for passing through a network
- The total metric of a particular route is equal to the metrics of networks that comprise the route
- A router chooses the route with smallest metric

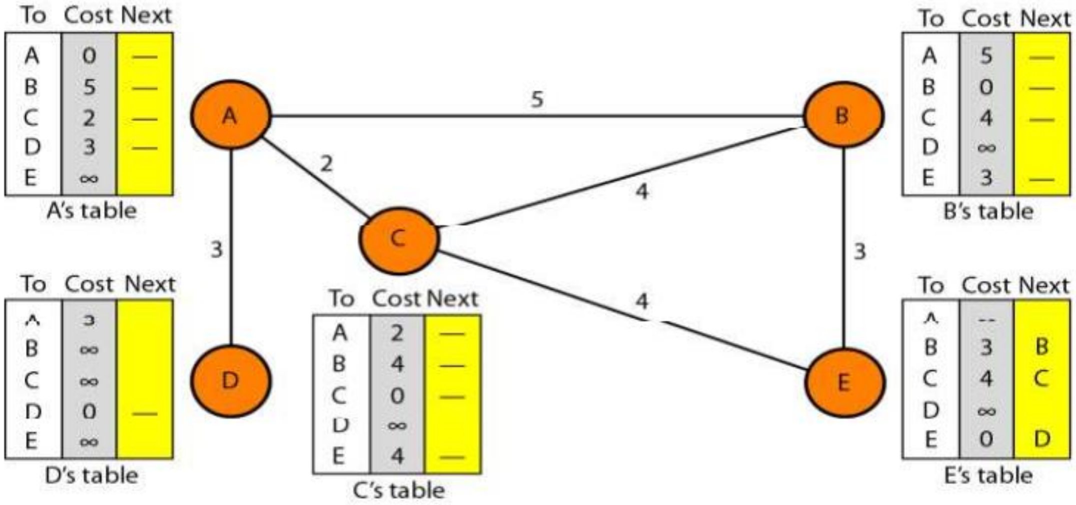
Distance Vector Routing

- Least-cost route between any two nodes is the route with minimum distance
- Each node maintains a set of triples**(Destination, Cost, NextHop)**
- The table at each node(router) also guides the packets to the desired node by showing the next stop in the route
- There is 2 steps in the route learning process

1. Initialization
2. Sharing

Initialization

- Initially routing table in each node consists the distance between itself and its immediate neighbors, those directly connected to it
- Not directly connected is marked infinities()



To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	∞	

A's table

To	Cost	Next
A	5	—
B	0	—
C	4	—
D	∞	
E	3	—

B's table

To	Cost	Next
A	3	
B	∞	
C	∞	
D	0	—
E	∞	

D's table

To	Cost	Next
A	2	—
B	4	—
C	0	—
D	∞	
E	4	—

C's table

To	Cost	Next
A	--	
B	3	B
C	4	C
D	∞	
E	0	D

E's table

Sharing

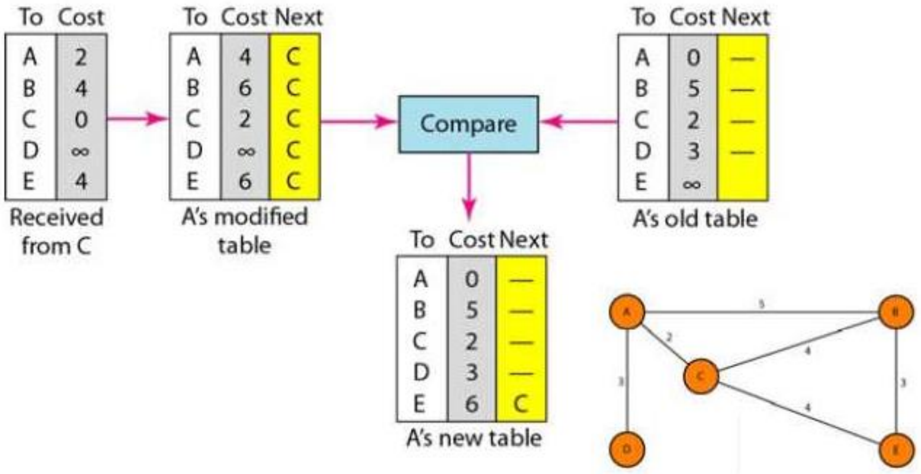
- 2 types of sharing(updates)

1. Periodic
2. Triggered

- Directly connected neighbors exchange(share) updates periodically (on the order of several seconds 30 sec)
- Whenever table changes (called *triggered* update)

Update Process

- Each update is a list of pairs: (**Destination, Cost)**
- Routing table will compare old routing table values with the shared table
- Updating of routing table is based on minimum cost



To	Cost
A	2
B	4
C	0
D	∞
E	4

Received from C

To	Cost	Next
A	4	C
B	6	C
C	2	C
D	∞	C
E	6	C

A's modified table

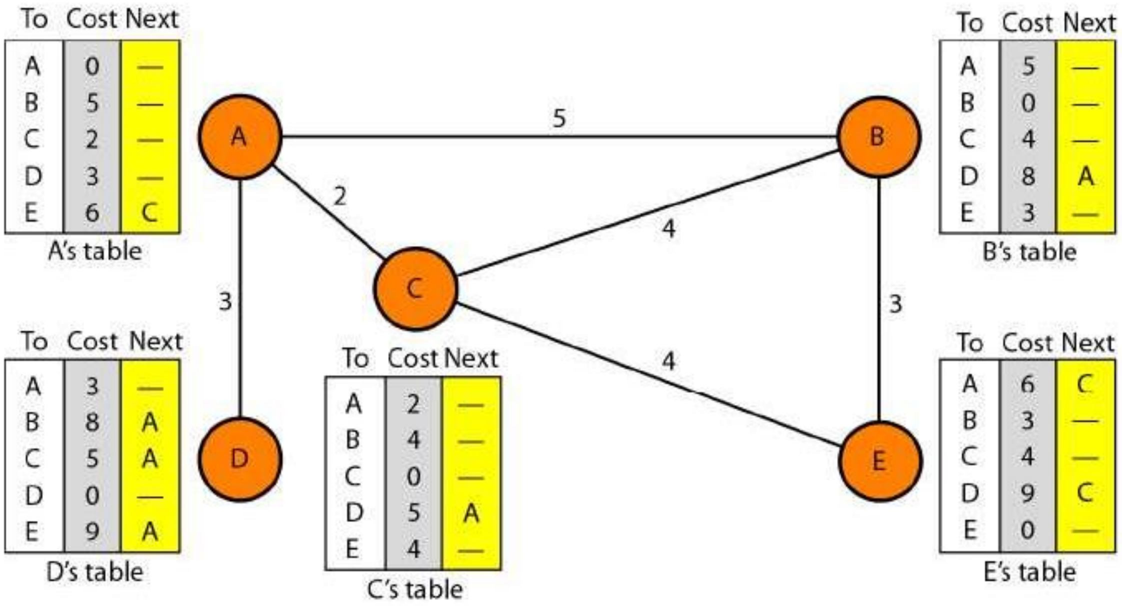
To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	∞	

A's old table

To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

A's new table

Final Routing Table



To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

A's table

To	Cost	Next
A	5	—
B	0	—
C	4	—
D	8	A
E	3	—

B's table

To	Cost	Next
A	3	—
B	8	A
C	5	A
D	0	—
E	9	A

D's table

To	Cost	Next
A	2	—
B	4	—
C	0	—
D	5	A
E	4	—

C's table

To	Cost	Next
A	6	C
B	3	—
C	4	—
D	9	C
E	0	—

E's table

LINK STATE ROUTING

- Link state routing has a different philosophy from that of distance vector routing.
- In link state routing, **each node in the domain has the entire topology** of the domain the list of nodes and links, how they are connected including the type, cost (metric), and condition of the links (up or down)-
- the node can use Dijkstra's algorithm to build a routing table.

Figure 22.20 *Concept oflink state routing*

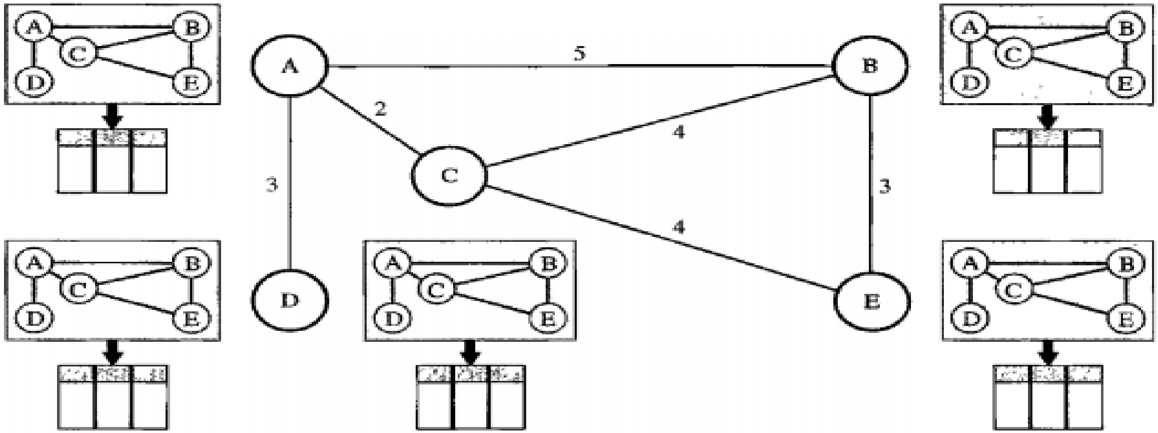
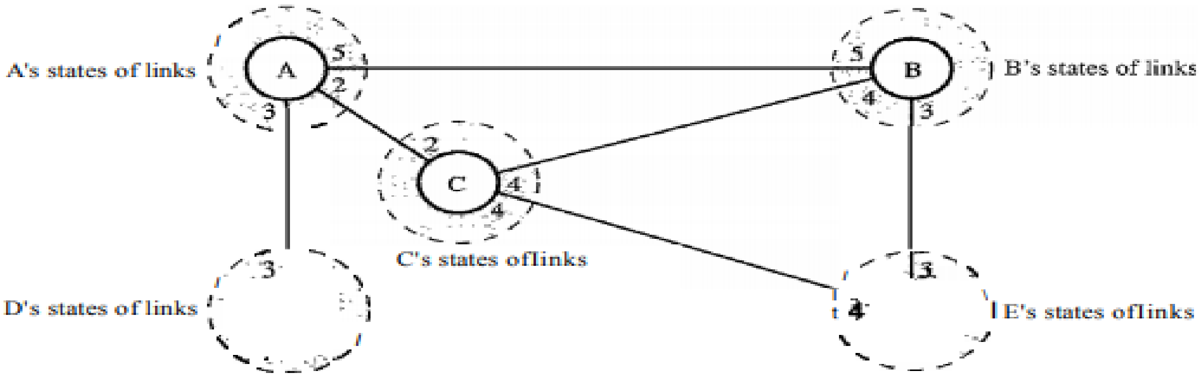


Figure 22.21 *Link state knowledge*



Building Routing Tables

- In link state routing, four sets of actions are required to ensure that each node has the routing table showing the least-cost node to every other node.
- 1. Creation of the states of the links by each node, called the link state packet (LSP).
- 2. Dissemination of LSPs to every other router, called flooding, in an efficient and reliable way.
- 3. Formation of a shortest path tree for each node.
- 4. Calculation of a routing table based on the shortest path tree.

Creation of Link State Packet (LSP)

- A link state packet can **carry a large amount of information.**
- For the moment, however, we assume that it carries a minimum amount of data: **the node identity, the list of links, a sequence number, and age.**

- The first two, node identity and the list of links, are **needed to make the topology.**
- The third, sequence number, **facilitates flooding and distinguishes** new LSPs from old ones.
- The fourth, age, **prevents old LSPs from remaining** in the domain for a long time.

LSPs are generated on two occasions:

- 1. When there is a change in the topology of the domain.
- 2. On a periodic basis. The timer set for periodic dissemination is normally in the range of 60 min or 2 h based on the implementation.

Flooding of LSPs

- After a node has prepared an LSP, it must be **disseminated to all other nodes**, not only to its neighbors. The **process is called flooding** and based on the following:

1. The creating **node sends a copy of the LSP** out of each interface.
2. A **node that rec**eives an LSP **compares it with the copy it may already have.**

If the newly arrived **LSP is older than the one** it has (found by checking the sequence number), **it discards the LSP**.

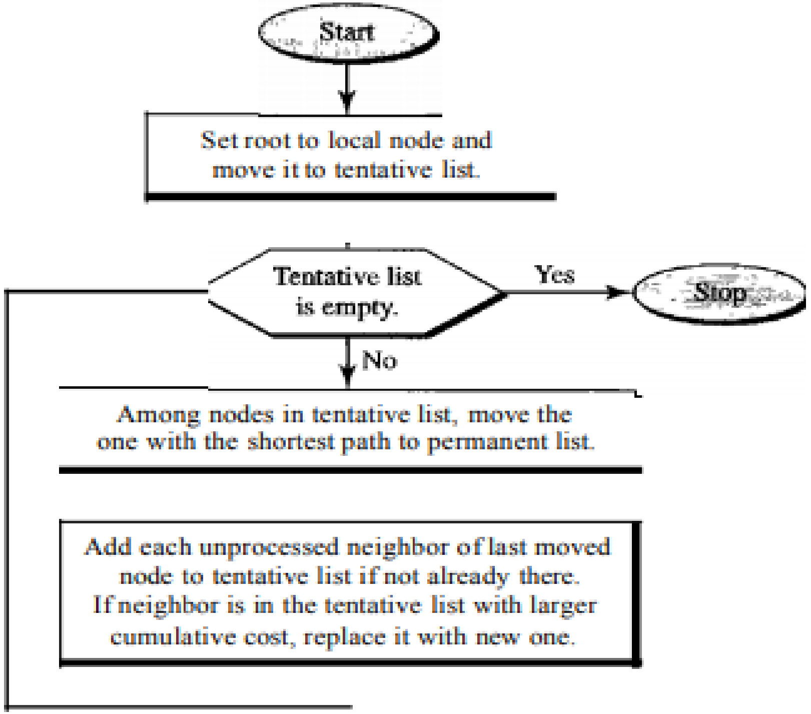
If it is newer, the node does the following:

a. It **discards the old LSP and keeps the new one**.

b. It **sends a copy of it out of each interface** except the one from which the packet arrived.

Formation of Shortest Path Tree: Dijkstra Algorithm

Figure 22.22 *Dijkstra algorithm*



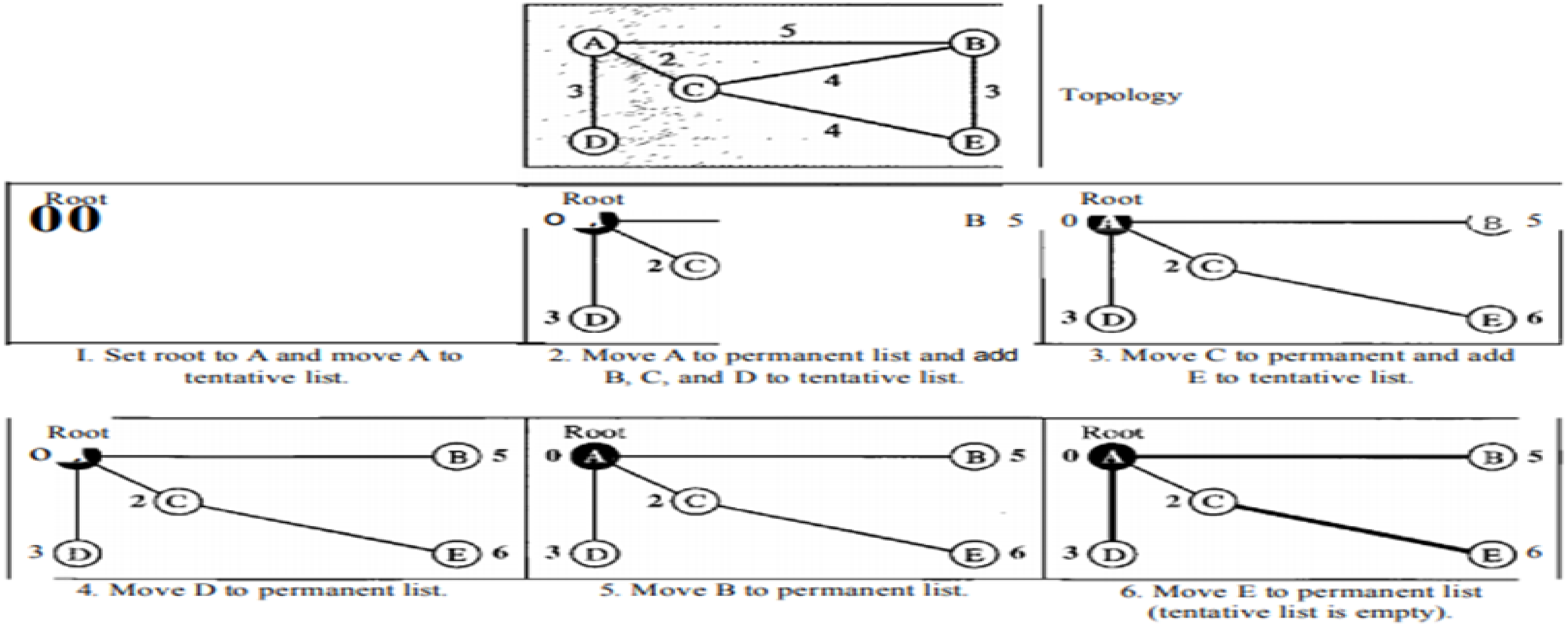
Set root to local node and move it to tentative list.

Tentative list is empty.

Among nodes in tentative list, move the one with the shortest path to permanent list.

Add each unprocessed neighbor of last moved node to tentative list if not already there. If neighbor is in the tentative list with larger cumulative cost, replace it with new one.

Figure 22.23 *Example offormation ofshortest path tree*



I. Set root to A and move A to tentative list.

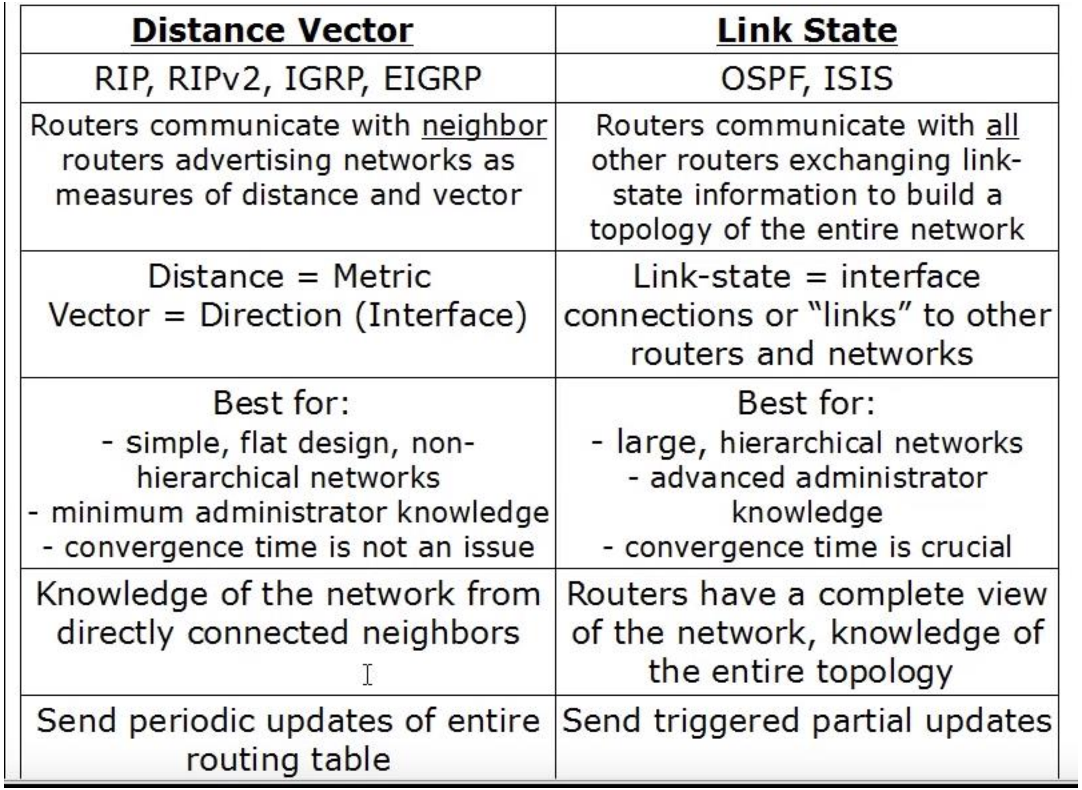
2. Move A to permanent list and add B, C, and D to tentative list.

3. Move C to permanent and add E to tentative list.

4. Move D to permanent list.

5. Move B to permanent list.

6. Move E to permanent list (tentative list is empty).



Distance Vector	**Link State**
RIP, RIPv2, IGRP, EIGRP	OSPF, ISIS
Routers communicate with neighbor routers advertising networks as measures of distance and vector	Routers communicate with all other routers exchanging link-state information to build a topology of the entire network

Distance = Metric
Vector = Direction (Interface)
	Link-state = interface connections or "links" to other routers and networks

Best for: - simple, flat design, non-hierarchical networks - minimum administrator knowledge - convergence time is not an issue	Best for: - large, hierarchical networks - advanced administrator knowledge - convergence time is crucial
Knowledge of the network from directly connected neighbors	Routers have a complete view of the network, knowledge of the entire topology
Send periodic updates of entire routing table	Send triggered partial updates

Routing Protocol

Routing information protocols (RIP)

- RIP (Routing Information Protocol) is a protocol type used in local area network and wide area network.

- RIP (Routing Information Protocol) type is categorized interior gateway protocol within the use of distance vector algorithm.

- Routing information protocols defined in 1988.

- It also has version 2 and nowadays both versions are in use.

- Technically it is outdated by more sophisticated techniques such as (OSPF) .

- Each RIP router maintains a routing table, which is a list of all the destinations (networks) it knows how to reach, along with the distance to that destination.

- RIP uses a distance vector algorithm to decide which path to put a packet on to get to its destination.

- It stores in its routing table the distance for each network it knows how to reach, along with the address of the "next hop" router -- another router that is on one of the same networks -- through which a packet has to travel to get to that destination.

- If it receives an update on a route, and the new path is shorter, it will update its table entry with the length and next-hop address of the shorter path;

Open shortest path first (OSPF)

- Open Shortest Path First (OSPF) is an active routing protocol used in internet protocol.

- Particularly it is a link state routing protocol and includes into the group of interior gateway protocol.

- Routers connect networks using the Internet Protocol (IP), and OSPF (Open Shortest Path First) is a router protocol used to find the best path for packets as they pass through a set of connected networks.

- OSPF is designated by the Internet Engineering Task Force (IETF)

- The OSPF routing protocol has largely replaced the older Routing Information Protocol (RIP) in corporate networks.

- Using OSPF, a router that learns of a change to a routing table (when it is reconfigured by network staff, for example) or detects a change in the network immediately multicasts the information to all other OSPF hosts in the network so they will all have the same routing table information.

- Unlike RIP, which requires routers to send the entire routing table to neighbors every 30 seconds, OSPF sends only the part that has changed and only when a change has taken place.

Border Gateway Protocol (BGP)

- Border Gateway Protocol (BGP) are the core routing protocol of the internet and responsible to maintain a table of Internet protocol networks which authorize network reaching capability between AS.

- The Border Gateway Protocol (BGP) expressed as path vector protocol.

- BGP router maintains a standard routing table used to direct packets in transit.

- This table is used in conjunction with a separate routing table, known as the routing information base (RIB), which is a data table stored on a server on the BGP router.

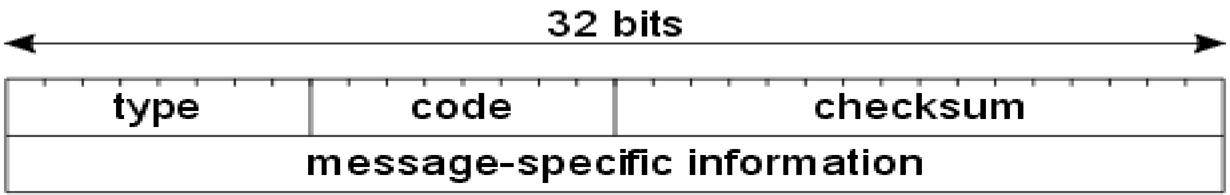
- The RIB contains route information both from directly connected external peers, as well as internal peers, and continually updates the routing table as changes occur.

- BGP is based on TCP/IP and uses client-server topology to communicate routing information, with the client-server initiating a BGP session by sending a request to the server.

Internet Control Message Protocol(ICMP)

- Since IP does not have a inbuilt mechanism for sending error and control messages.
- It depends on Internet Control Message Protocol(ICMP) to provide an error control.
- It is used for reporting errors and management queries.
- It is a supporting protocol and used by networks devices like routers for sending the error messages and operations information.

ICMP packet format



Type:

This defines the type of field message.

Code:

For error messages, this defines the sub type of field error.

Checksum:

The checksum is calculated by the header and the data that is used to detect the errors.

Data:

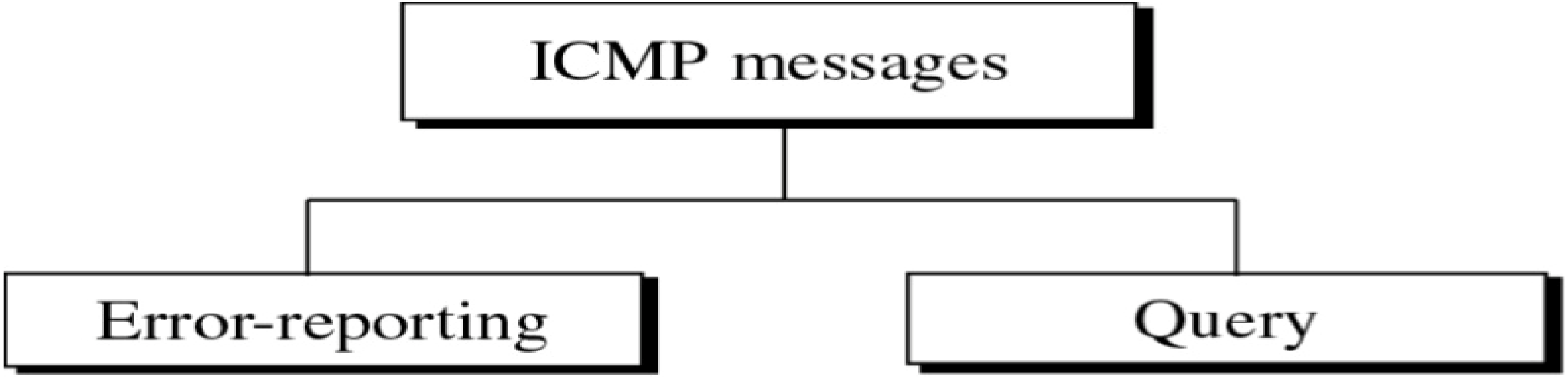
packet in this section contains the complete information of the packet.

Type:
This defines the type of field message.

Code:
For error messages, this defines the sub type of field error.

Checksum:
The checksum is calculated by the header and the data that is used to detect the errors.

Data:
packet in this section contains the complete information of the packet.



ICMP messages

Error-reporting

Query

Type	*Message*
3	Destination unreachable
4	Source quench
11	Time exceeded
12	Parameter problem
5	Redirection

Type	*Message*
8/0	Echo (request/reply)
13/14	Timestamp (req./rep.)
18/18	Address mask (req./rep.)
10/9	Router solicitation/advertisement

Destination un-reachable :
Destination unreachable is generated by the host or its inbound gateway to inform the client that the destination is unreachable for some reason.

Source quench message :
Source quench message is request to decrease traffic rate for messages sending to the host(destination).
when receiving host detects that rate of sending packets (traffic rate) to it is too fast it sends the source quench message to the source to slow the pace down so that no packet can be lost.

Parameter problem :
Whenever packets come to the router then calculated header checksum should be equal to received header checksum then only packet is accepted by the router.

If there is mismatch packet will be dropped by the router.

ICMP will take the source IP from the discarded packet and informs to source by sending parameter problem message.

Time exceeded message :

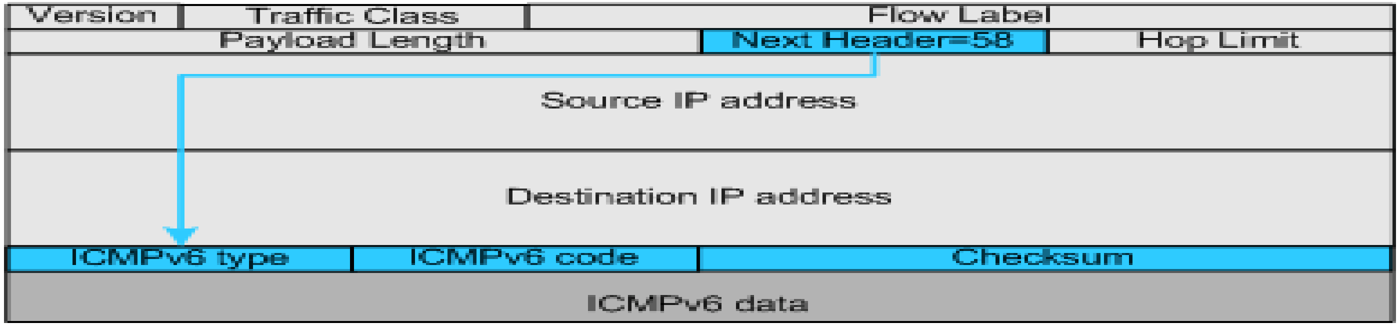
When some fragments are lost in a network then the holding fragment by the router will be dropped then ICMP will take source IP from discarded packet and informs to the source, of discarded datagram due to time to live field reaches to zero, by sending time exceeded message.

Redirection message :

Redirect requests data packets be sent on an alternate route. The message informs to a host to update its routing information (to send packets on an alternate route).

ICMPV6

- Internet Control Message Protocol (both ICMPv4 and ICMPv6) is a protocol which acts as a communication messenger protocol between the communicating devices in IP network.
- ICMP messages provide feedback, error reporting and network diagnostic functions in IP networks which are necessary for the smooth operation of IPv6.



Version

Traffic Class

Flow Label

Payload Length

Next Header=58

Hop Limit

Source IP address

Destination IP address

ICMPv6 type

ICMPv6 code

Checksum

ICMPv6 data

ASSIGNMENT

- Overview of Network Traffic Analysis
- Security Concept: Firewall and Router Access Control

THE END