

# Network Layer

13

- It is responsible for the source to destination delivery of a packet across multiple networks.
- If two systems are attached to different networks with devices like routers, then N/W layer is used.
- Thus DLL oversees the delivery of the packet between the two systems on same network and the network layer ensures that the packet gets its point of origin to its final destination.

# Functions of Network Layer

14

- **Internetworking:** It provides Internetworking.
- **Logical Addressing:** When packet is sent outside the network, N/W layer adds Logical (network) address of the sender & receiver to each packet.
- Network addresses are assigned to local devices by n/w administrator and assigned dynamically by special server called DHCP (Dynamic Host Configuration Protocol)
- **Routing:** When independent n/w are connected to create internetwork several routes are available to send the data from S to D. These n/w are interconnected by routers & gateways that route the packet to final destination.

# Contents

- Internet Protocol
  - Version 4
  - Address depletion problem
  - NAT
  - Sub netting
  - Version 6
  - Header IPv4
  - Header IPv6
- Routing
  - Classless and Classful
  - Static and dynamic
  - Interior and exterior
  - Distance vector and Link state
  - Routing Algorithms
    - RIP
    - OSPF
    - BGP

# Need for Network layer

- The network layer is responsible for host-to-host delivery
- Routing the packets through the routers or switches
- The network layer at the source is responsible for creating a packet from the data coming from another protocol
- The network layer is responsible for checking its routing table to find the routing information

# 1 IP Address v4

- An IPv4 address is 32 bits long
- The IPv4 addresses are unique and universal
- IPv4 uses 32-bit addresses, which means that the address space is  $2^{32}$  or 4,294,967,296 (Maximum available theoretically)
- IPv4 have 2 types of notations:
  1. Dotted decimal  
Denoted in decimal format each byte is separated by dot eg: 117.149.29.2  
Mostly used by human configurations
  2. Binary notation  
In binary format eg: 01110101 10010101 00011101 00000010  
Mostly used by devices for processing

# 1.1 IPv4 Classes(Classfull Address)

- The address space is divided into five classes: A, B, C, D, and E
- Division is based on the first byte in doted decimal format

## Class A

Range of first octet or byte is between 0 to 127

First byte is network and last 3 bytes are Host (N.H.H.H)

First bit always will be zero (0xxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx)

Used for unicasting, valid host IP

## Class B

Range of first octet or byte is between 128 to 191

First 2 bytes is network and last 2 byte are Host (N.N.H.H)

First bit always will be zero (10xxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx)

Used for unicasting, valid host IP

# 1.1 IPv4 Classes

## Class C

Range of first octet or byte is between 192 to 223

First 3 bytes is network and last byte are Host (N.N.N.H)

First bit always will be zero (110xxxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx)

Used for unicasting, valid host IP

## Class D

Range of first octet or byte is between 224 to 239

First 2 bytes is network and last 2 byte are Host (N.N.H.H)

First bit always will be zero (1110xxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx)

Used for Multicasting, Special Address

## Class E

Range of first octet or byte is between 240 to 255

First 2 bytes is network and last 2 byte are Host (N.N.H.H)

First bit always will be zero (1111xxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx)

Used for research purpose

# 1.1.1 Netid & Host ID

- **Class A** :- first byte netid and last 3 bytes hostid (N.H.H.H)
- **Class B** :- first 2 bytes netid and last 2 bytes hostid (N.N.H.H)
- **Class C** :- first 3 bytes netid and last byte hostid (N.N.N.H)
- Subnet mask helps to identify netid and hostid
- CIDR value is total number of network bits in subnetmask



# 1.1.2 Subnet Mask and CIDR in Classful IPv4

- The mask can help us to find the netid and the hostid
  - *For example, the mask for a class A address has eight 1s, which means the first 8 bits of any address in class A define the netid; the next 24 bits define the hostid.*
- CIDR value is number 1's (ones) in the subnet mask(network bits), usually for class A,B,C CIDR values will be 8,16,24 respectively

Given below table shows various subnet mask, CIDR values of class A,B,C

<i>Class</i>	<i>Binary</i>	<i>Dotted-Decimal</i>	<i>CIDR</i>
A	11111111 00000000 00000000 00000000	255.0.0.0	8
B	11111111 11111111 00000000 00000000	255.255.0.0	16
C	11111111 11111111 11111111 00000000	255.255.255.0	24

# 1.2 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. Sub netting
  3. IPv6

# 1.3 Network Address Translation(NAT)

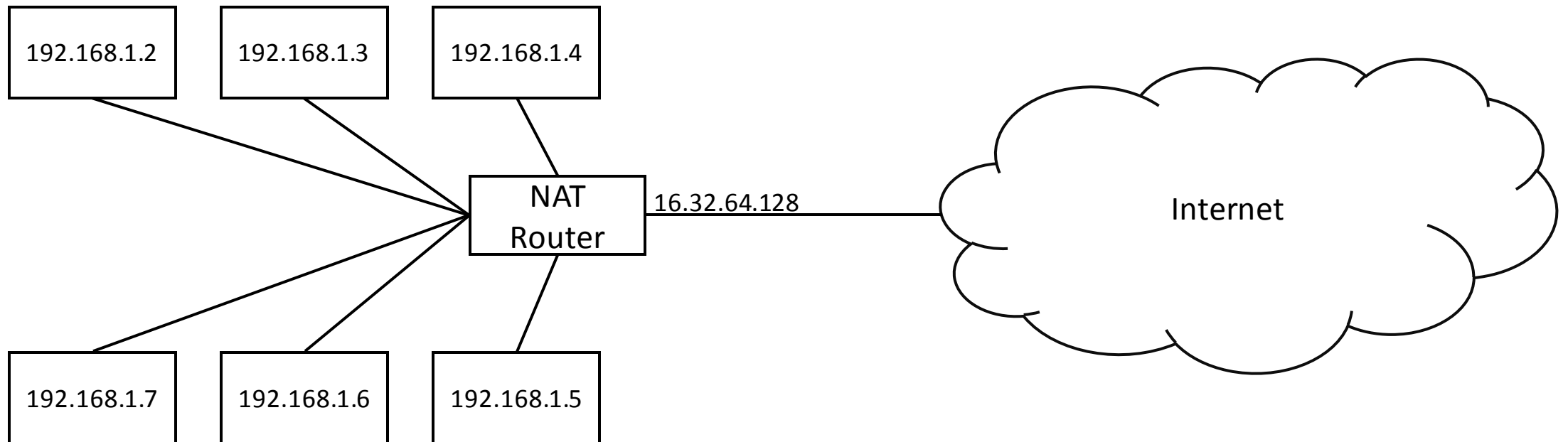
- IP address have public range and private range
- Public range is used for communication in internet and can used only with permission of internet authorities
- Private IP can be used for local communication without permission of Internet authorities

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

<i>Range</i>			<i>Total</i>
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	$2^{16}$

# 1.3 Network Address Translation(NAT)

- 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



# 1.3 Network Address Translation(NAT)

- 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

<i>Private Address</i>	<i>Private Port</i>	<i>External Address</i>	<i>External Port</i>	<i>Transport Protocol</i>
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
...	...	...	...	...

# 1.4 Classless Addressing

- There is no classes hierarchy in the IP address but address is still granted in blocks.

## **Restriction**

- To simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks:
  1. The addresses in a block must be contiguous, one after another.
  2. The number of addresses in a block must be a power of 2 (1, 2, 4, 8, ..)
  3. The first address must be evenly divisible by the number of addresses.

# 1.4.1 Subnetting

- Subnetting means creating subnetwork
- Subnetting means increasing networks bits(i.e. 1s) in subnet mask
- If network bit is increased host bits will be decreased, so number of host will be decreased
- A Class A network have 8 bits for network ( $2^{24}$  IP address available) if you wanted smaller block IP from class A increase the network bits / decreasing host bits

## 1.4.2. Supernetting

- Supernetting means creating bigger network from smaller one
- Supernetting means decreasing networks bits(i.e. 1s) in subnet mask
- If network bit is decreased host bits will be increased, so number of host will be decreased
- A Class C network have 24 bits for network ( $2^8$  IP address available) if you wanted bigger block IP from class C decrease the network bits / increasing host bits
- Supernetting just opposite of subnetting



## 1.4.3. VLSM (Variable Length Subnet Mask)

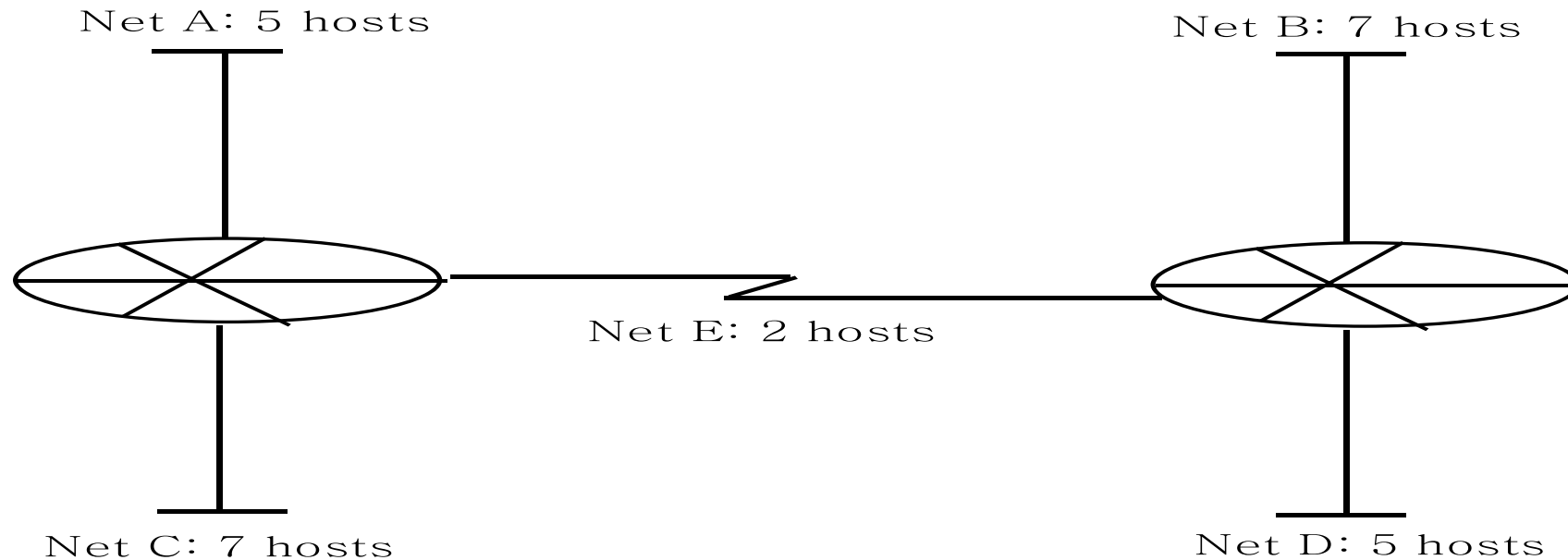
- Subnetting and supernetting is achieved by varying default subnet mask
- Usually in classful IP address have 8,16,24 default CIDR values for Class A, B, C respectively, but in classless IP no default CIDR value / subnet mask is available CIDR value may be varying

## 1.4.4. Subnetting/supernetting Steps

- Identify needed block size (always in power of 2 i.e.  $2^2, 2^3, 2^4, \dots 2^{31}$ )
  - If multiple block size is needed assign largest block first
- Find the host bits from block size (if block size  $2^n$  no of host bit is n)
- From host bits find the CIDR (CIDR=32-n)
- Find subnet mask convert CIDR into doted decimal format (ex:255.255.240.0)
- Find wild card mask (255.255.255.255 - 255.255.240.0= 0.0.15.255)
- Add the first IP in the range to get last IP address

# 1.5 Subnetting Problem Example

- Class C network of 200.15.5.0 is given, subnet the network in order to create the network in the given figure with the host requirement shown.



# 1.5 Subnetting Problem Example

- Network Requirements

Network	No of Hosts	Total no of IP	Block size
A	5	7	8
B	7	9	16
C	7	9	16
D	5	7	8
E	2	4	4

- Number of hosts represents only valid HOST IP
- Total no of IP represents Host IP+ Network ID + broadcast ID
- Rule : Block size  $\geq$  Total no IP
- Assign blocks in ascending order(B,C,A,D,E)

## **Network B**

Host IP needed = 7

No of IP required =9 (Including Network ID and Broadcast ID)

Block size required  $16 = 2^4$  (8 blocks is not enough because only 6 valid host)

No of host bit = 4

CIDR =  $32-4=28$

Subnet mask =255.255.255.240

Wild card mask= 0.0.0.15

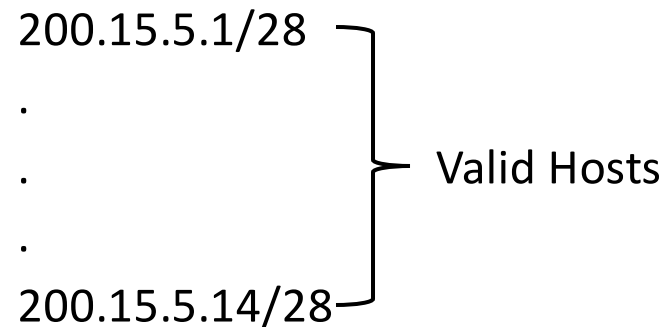
200.15.5.0 + → First IP (given in Question)  
0.0.0.15 → Wildcard mask

-----  
200.15.5.15 → Last IP in range

Valid host IP is in the range

200.15.5.0/28 → Network id

200.15.5.1/28  
.  
.  
.  
200.15.5.14/28



Valid Hosts

200.15.5.15/28 → Broadcast id

## Network C

Host IP needed = 7

No of IP required = 9 (Including Network ID and Broadcast ID)

Block size required  $16 = 2^4$  (8 blocks is not enough because only 6 valid host)

No of host bit = 4

CIDR =  $32 - 4 = 28$

Subnet mask = 255.255.255.240

Wild card mask = 0.0.0.15

200.15.5.16 + → First IP (200.15.5.15 is already assigned)

0.0.0.15 → Wildcard mask

-----

200.15.5.31 → Last IP in range

Valid host IP is in the range

200.15.5.16/28 → Network id

200.15.5.17/28

.

.

.

200.15.5.30/28



Valid Hosts

200.15.5.31/28 → Broadcast id



## **Network A**

Host IP needed = 5

No of IP required = 7 (Including Network ID and Broadcast ID)

Block size required  $8 = 2^3$

No of host bit = 3

CIDR =  $32 - 3 = 29$

Subnet mask = 255.255.255.248

Wild card mask = 0.0.0.7

200.15.5.32 + → First IP (200.15.5.31 is already assigned)

0.0.0.7 → Wildcard mask

-----

200.15.5.39 → Last IP in range

Valid host IP is in the range

200.15.5.32/29 → Network id

200.15.5.33/29

.

.

.

200.15.5.38/29



Valid Hosts

200.15.5.39/29 → Broadcast id

## **Network D**

Host IP needed = 5

No of IP required = 7 (Including Network ID and Broadcast ID)

Block size required  $8 = 2^3$

No of host bit = 3

CIDR =  $32 - 3 = 29$

Subnet mask = 255.255.255.248

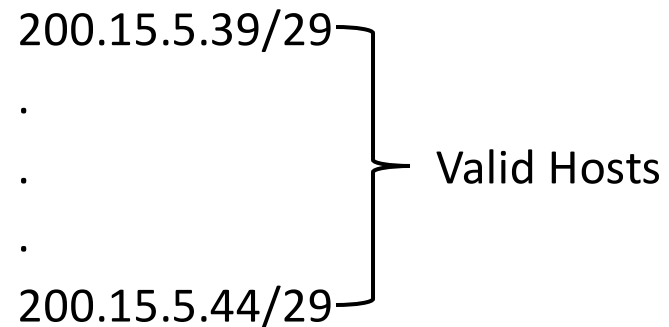
Wild card mask = 0.0.0.7

200.15.5.40 + → First IP (200.15.5.40 is already assigned)  
0.0.0.7 → Wildcard mask

-----  
200.15.5.46 → Last IP in range

Valid host IP is in the range

200.15.5.38/29 → Network id



200.15.5.45/29 → Broadcast id

## **Network E**

Host IP needed = 2

No of IP required = 4 (Including Network ID and Broadcast ID)

Block size required  $4 = 2^2$

No of host bit = 2

CIDR =  $32 - 3 = 30$

Subnet mask = 255.255.255.252

Wild card mask = 0.0.0.3

200.15.5.46 + → First IP (200.15.5.31 is already assigned)

0.0.0.3 → Wildcard mask

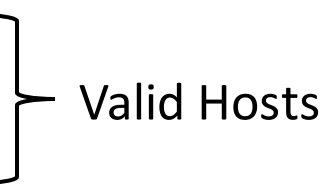
-----

200.15.5.49 → Last IP in range

Valid host IP is in the range

200.15.5.46/30 → Network id

200.15.5.47/30  
200.15.5.48/30



Valid Hosts

200.15.5.49/30 → Broadcast id

## 1.6. 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

## 1.7. 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



# 1.7. IPv6

## 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

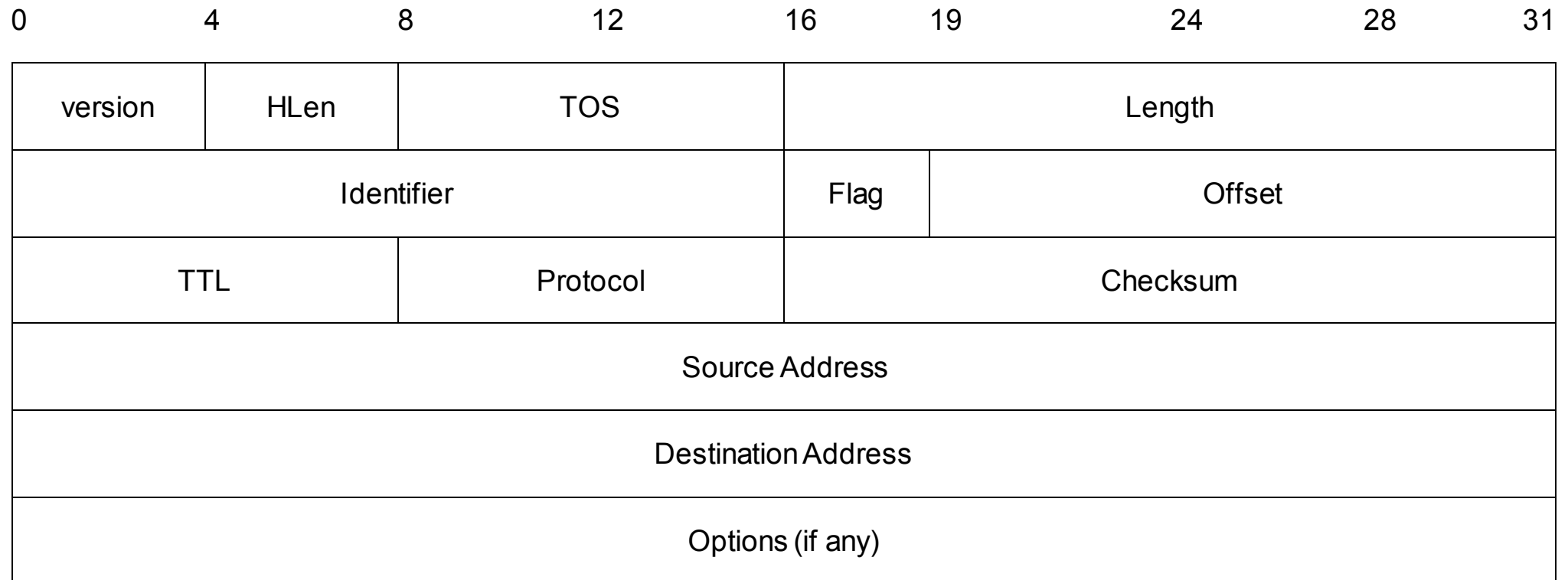
# 1.7.1. IPv6 Features

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

# Comparison of IPv4 and IPv6

<b>Feature</b>	<b>IPv4</b>	<b>IPv6</b>
Address length	32 bits	128 bits
IPsec header support	Optional	Required
Prioritized delivery support	Some	Better
Fragmentation	Hosts and routers	Hosts only
Packet size	576 bytes	1280 bytes
Checksum in header	Yes	No
Options in header	Yes	No
Link-layer address resolution	ARP (broadcast)	Multicast Neighbor Discovery messages
Multicast membership	IGMP	Multicast Listener Discovery (MLD)
Router Discovery	Optional	Required
Uses broadcasts	Yes	No
Configuration	Manual, DHCP	Automatic, DHCPv6

# 1.8. IPv4 Header Format



# 1.8. IPv4 Header Format

- **Version (4 bits):** Indicates the version number, In this case 4
- **HLEN (Header Length ,4 bits):** Length of header 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

# 1.8. IPv4 Header Format

- 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.

\* *MTU - Maximum Transfer Unit*

# 1.8. IPv4 Header Format

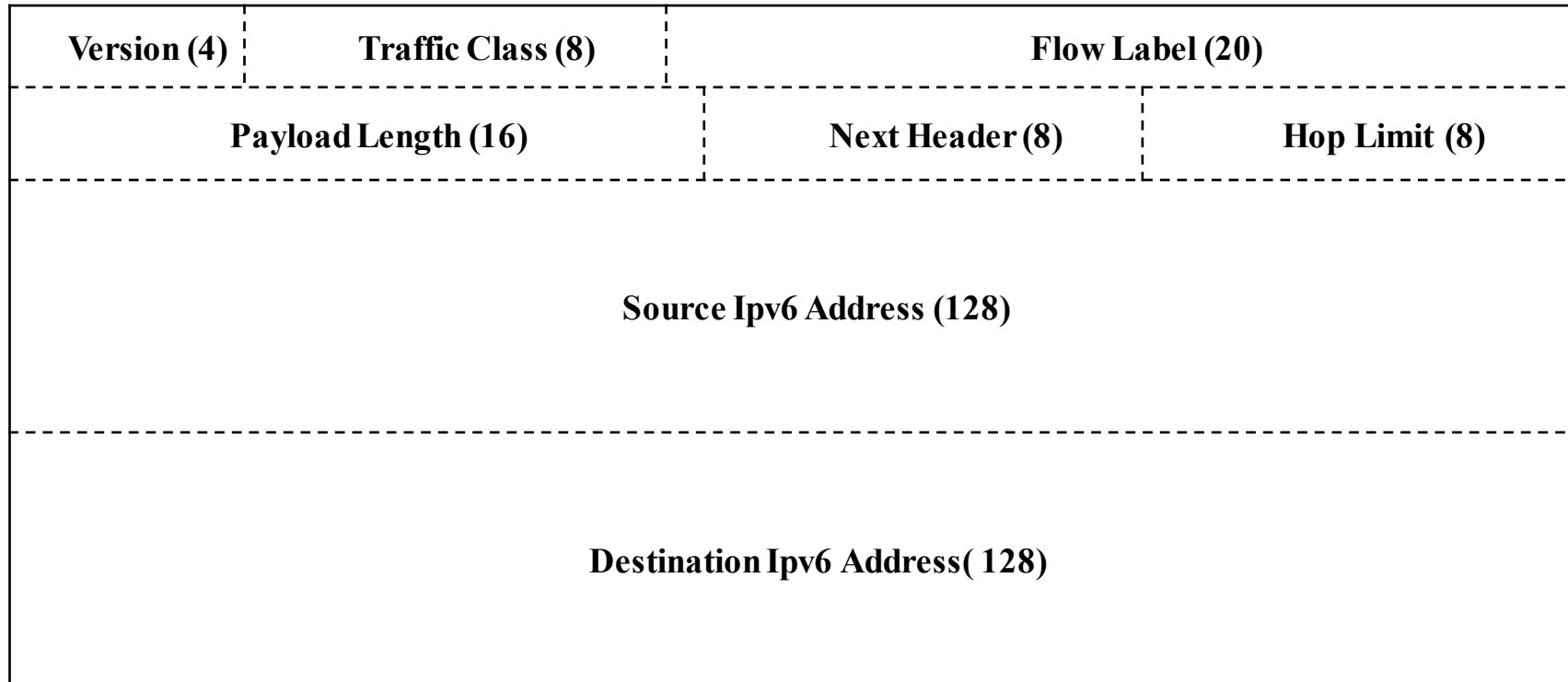
- **TTL (Time-to-Live, 8-bit):** Indicates the remaining "life" of the packet
- The TTL value is decreased by at least one each time the packet is processed by a router (that is, each hop). When the value becomes zero, the router discards or drops the packet and it is removed from the network data flow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

## 1.8. IPv4 Header Format

- **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



# 1.9. IPv6 Header Format



# 1.9. IPv6 Header Format

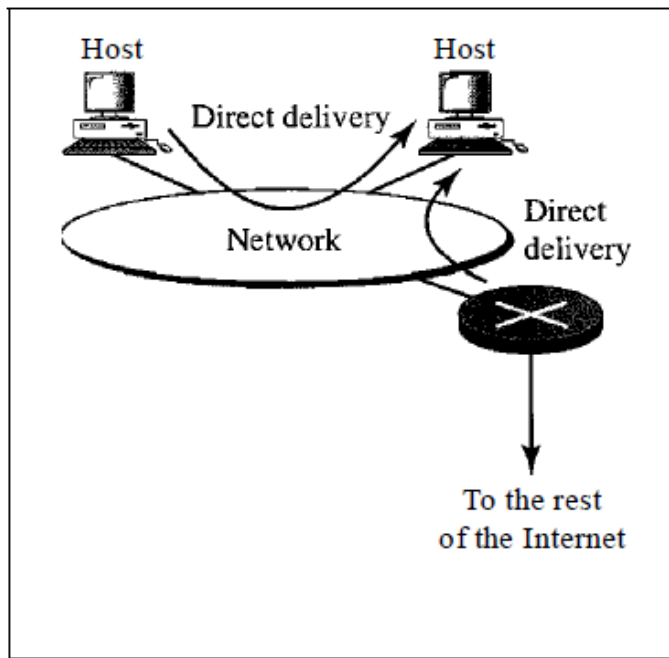
- **Version (4 bit):** Indicates version (6) of IP packet.
- **Traffic Class (8 bit):** Facilitates the handling of real time data by router. It Prioritize the packets (packet is send /dropped based on priority)
- **Flow Control (20 bit):** Used to label sequences of packets that require the same treatment for more efficient processing on routers.
- **Payload Length (16 bit):** Length of data carried after IPv6 header.

# 1.9. IPv6 Header Format

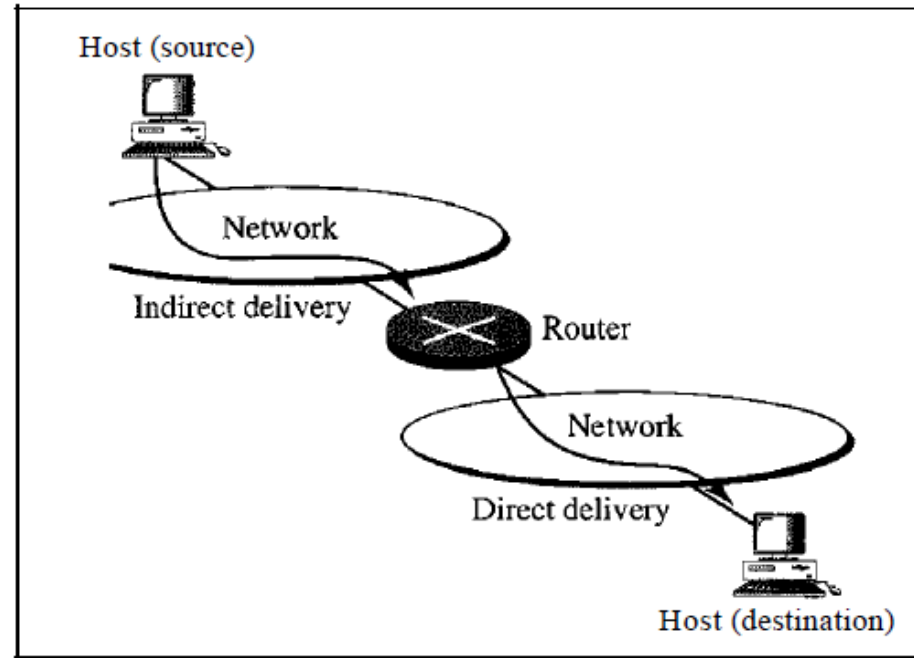
- **Next Header (8 bit):** Identifies the higher level protocol(identify the start of higher level header) **Hop Limit (8 bit):** This field indicates how long packet can remain in network.
- **Source Address (128 bit):** This Field indicates the IPv6 address from which packet is generated.
- **Destination Address (128 bit):** This field indicates the IPv6 address to which packet is going

## 2. Routing

- There is two types of packet delivery
  1. Direct delivery : inside a network(LAN)
  2. Indirect : between different network



a. Direct delivery

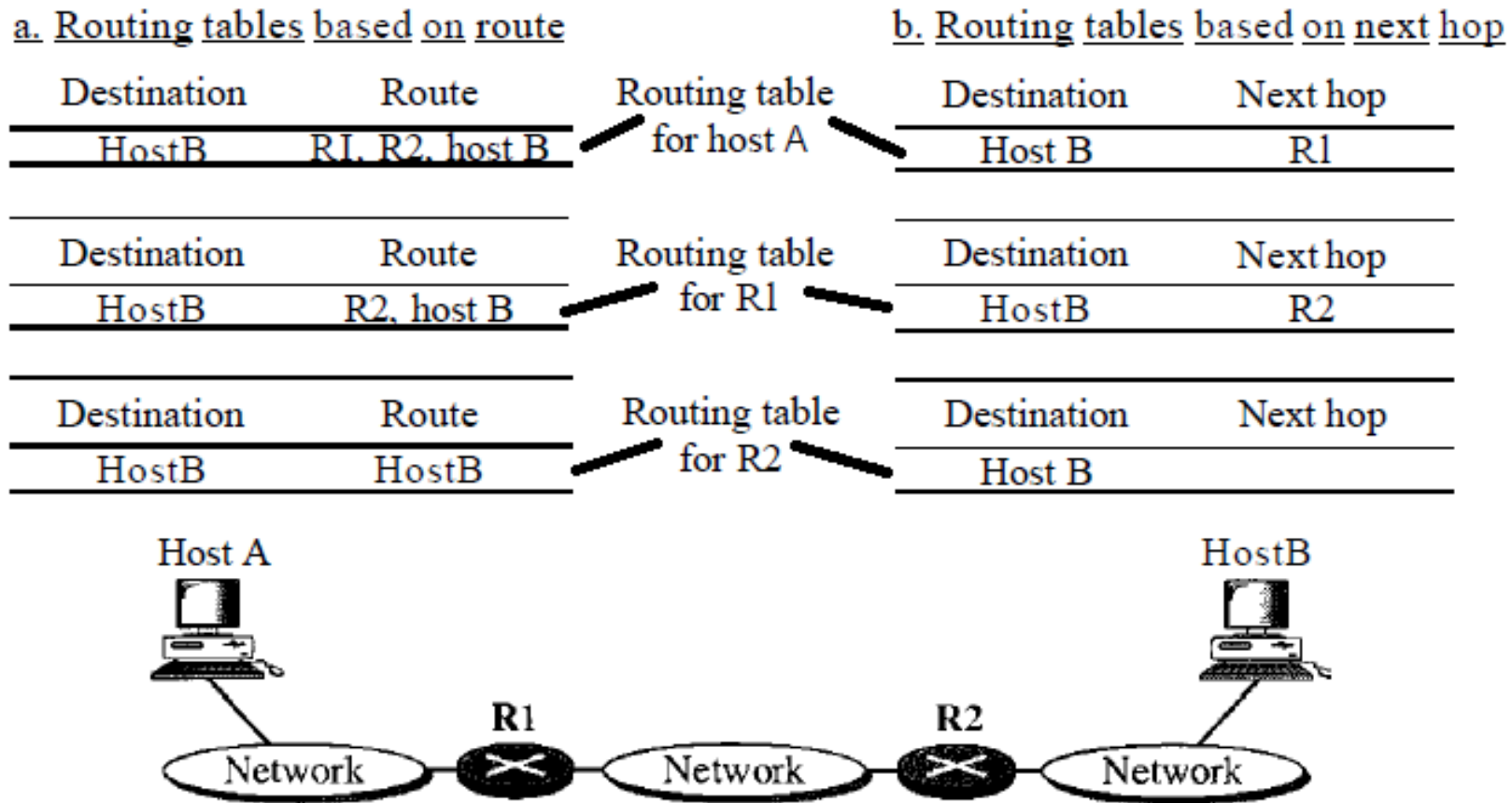


b. Indirect and direct delivery

## 2.1 Forwarding Techniques(Packet Forwarding)

- Forwarding means to place the packet in its route to its destination
- Forwarding requires a host or a router to have a routing table
- Forwarding techniques(based on routing table entry)
  1. Next hop method Vs Route method
  2. Network specific Vs Host specific
  3. Default route

## 2.1.1 Route based vs Next hop method



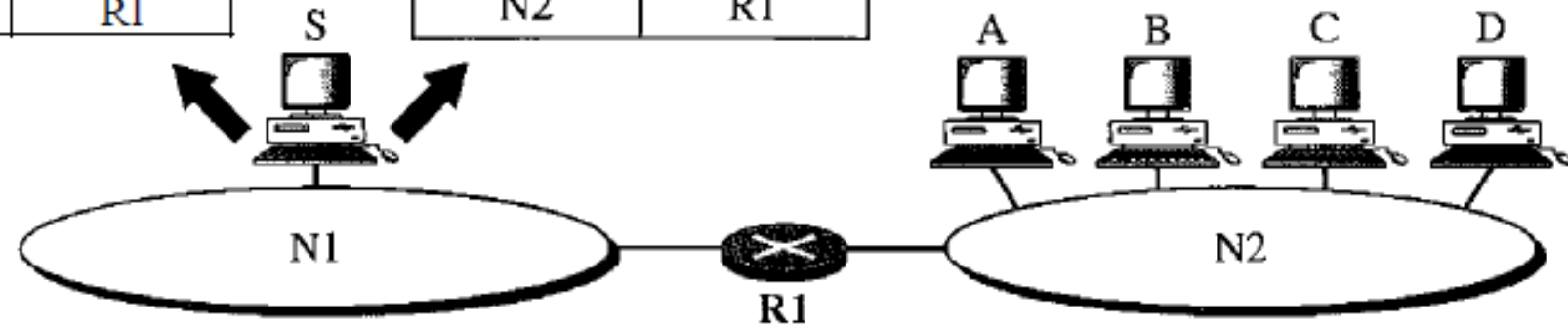
## 2.1.2. Host specific vs Network specific

Routing table for host S based on host-specific method

Destination	Next hop
A	R1
B	R1
C	R1
D	R1

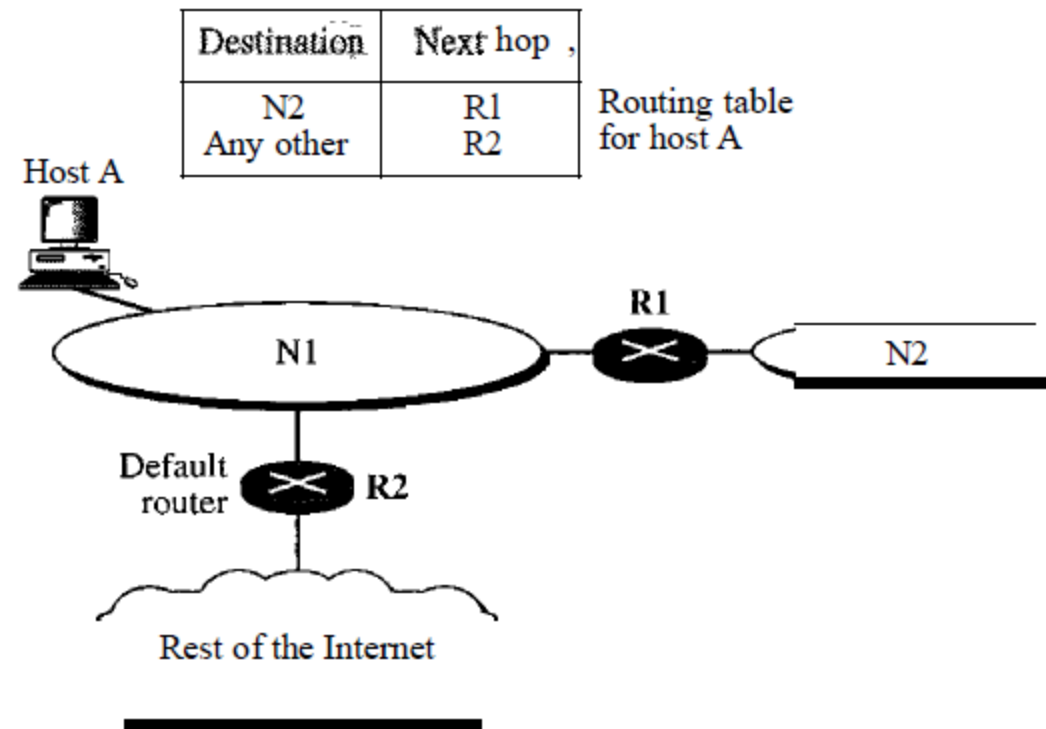
Routing table for host S based on network-specific method

Destination	Next hop
N2	R1



## 2.1.3. Default route

- Default route is entered in routing table with help of 0.0.0.0 (IP) which means any network.





## 2.2. Static Routing Table

- **Static routing table** contains information entered manually
- The administrator enters the route for each destination into the table
- The table must be manually altered by the administrator.
- A static routing table can be used in a small internet that does not change very often, or in an experimental internet for troubleshooting
- It is poor strategy to use a static routing table in a big network such as the Internet.

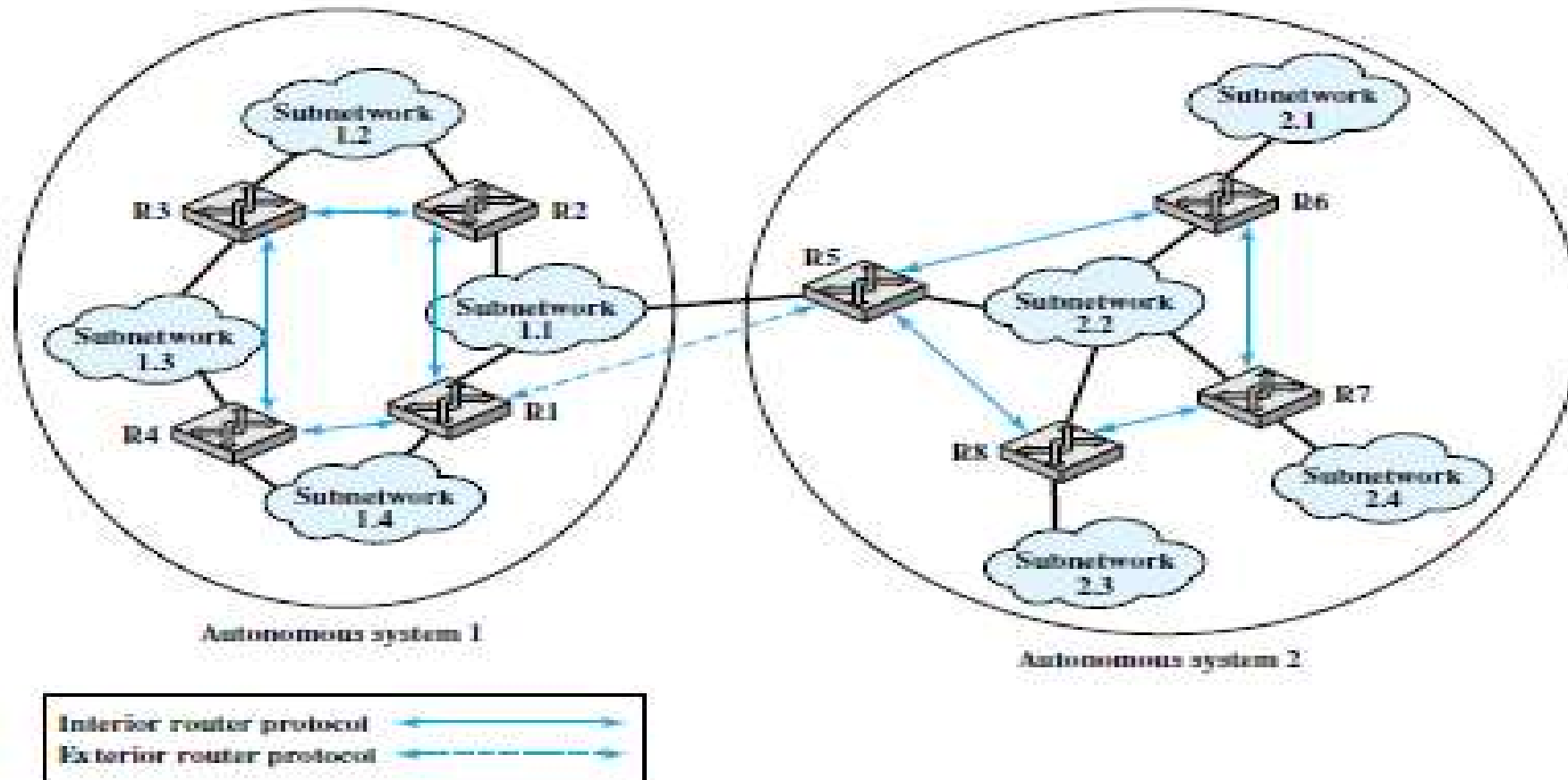
## 2.3. Dynamic Routing

- A dynamic routing table is updated periodically by using one of the dynamic routing protocols such as RIP, OSPF, or BGP.
- Whenever there is a change in the Internet, such as a shutdown of a router or breaking of a link, the dynamic routing protocols update all
- the tables in the routers (and eventually in the host) automatically.
- The routers in a big internet such as the Internet need to be updated dynamically for efficient delivery of the IP packets

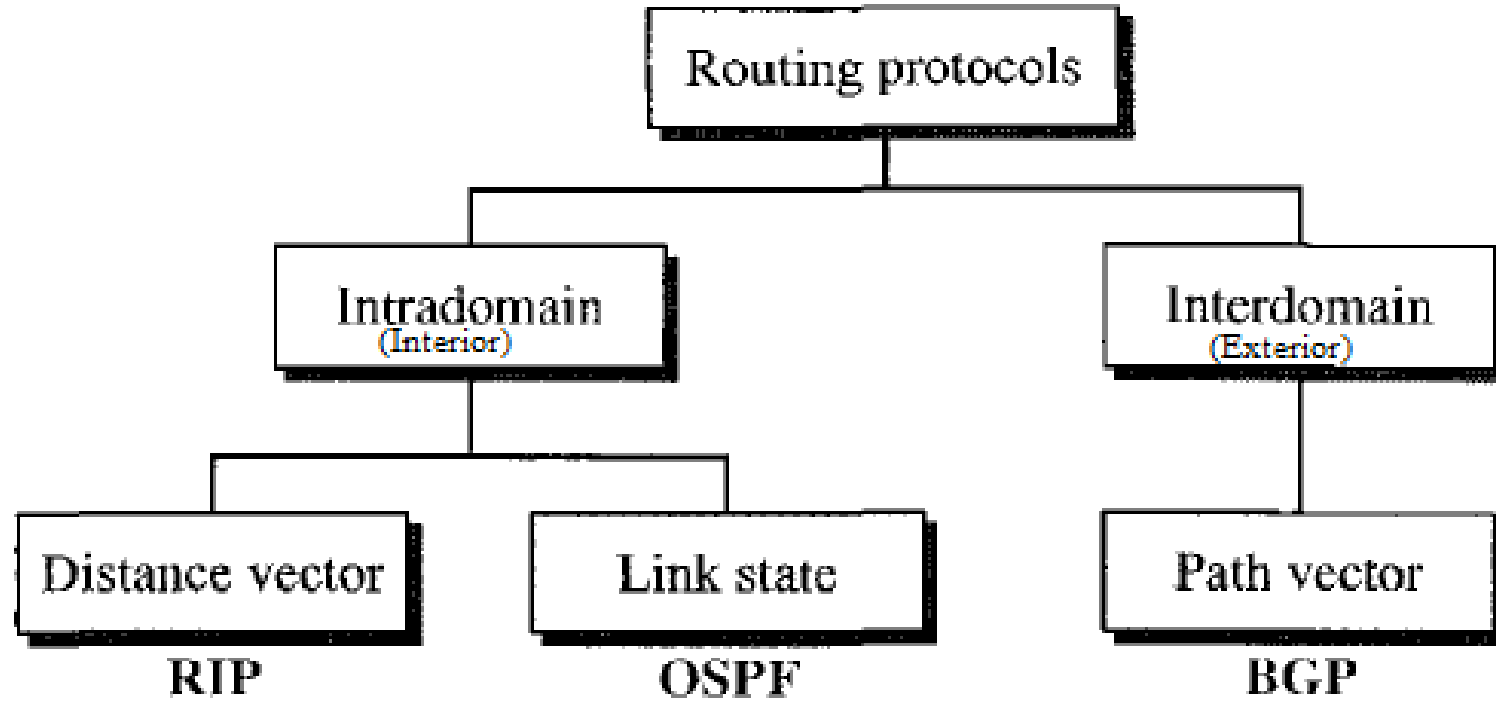
## 2.4. Autonomous System (AS)

- Large internet is divided into group of small networks
- AS is a group of networks and routers under the **authority of a single administration**
- Dynamic routing is divided into **interior and exterior** routing protocol
- Routing inside an autonomous system is referred to as **intra-domain routing (Interior Routing)**
- Routing between autonomous systems is referred to as **inter-domain routing (Exterior Routing)**
- Autonomous system can have one or more **intra-domain** routing protocols to handle routing inside the autonomous system

## 2.4.1 Interior and Exterior Routing in AS



## 2.4.1 Interior and Exterior Routing Protocols



## 2.5. Metrics

### *Metric in real world means measure*

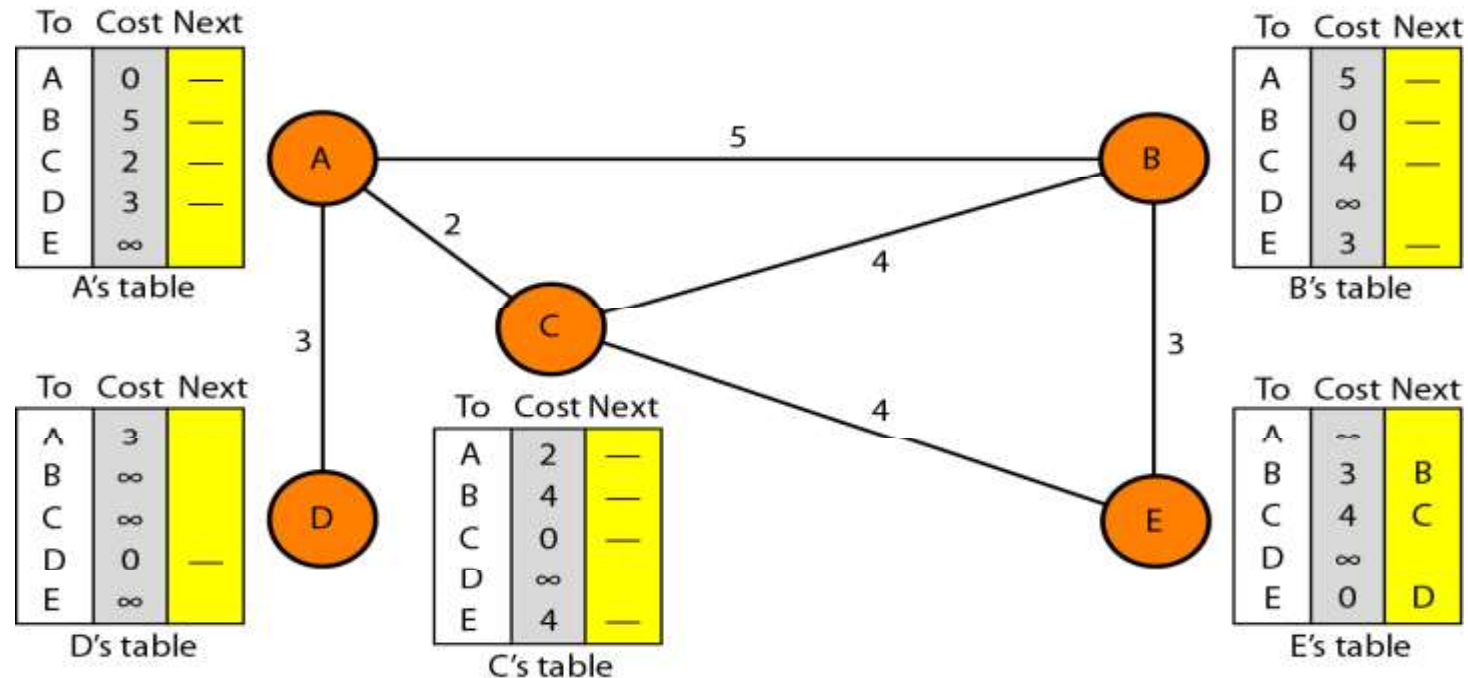
- **Router metrics** are metrics used by a router to make routing decisions
- Metric is the cost assigned for passing through a network
- The total metric of a particular route is equal to the metrics of networks that comprise the route
- A router chooses the route with smallest metric

## 2.6. Distance Vector Routing (RIP)

- 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

## 2.6.1. Initialization

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



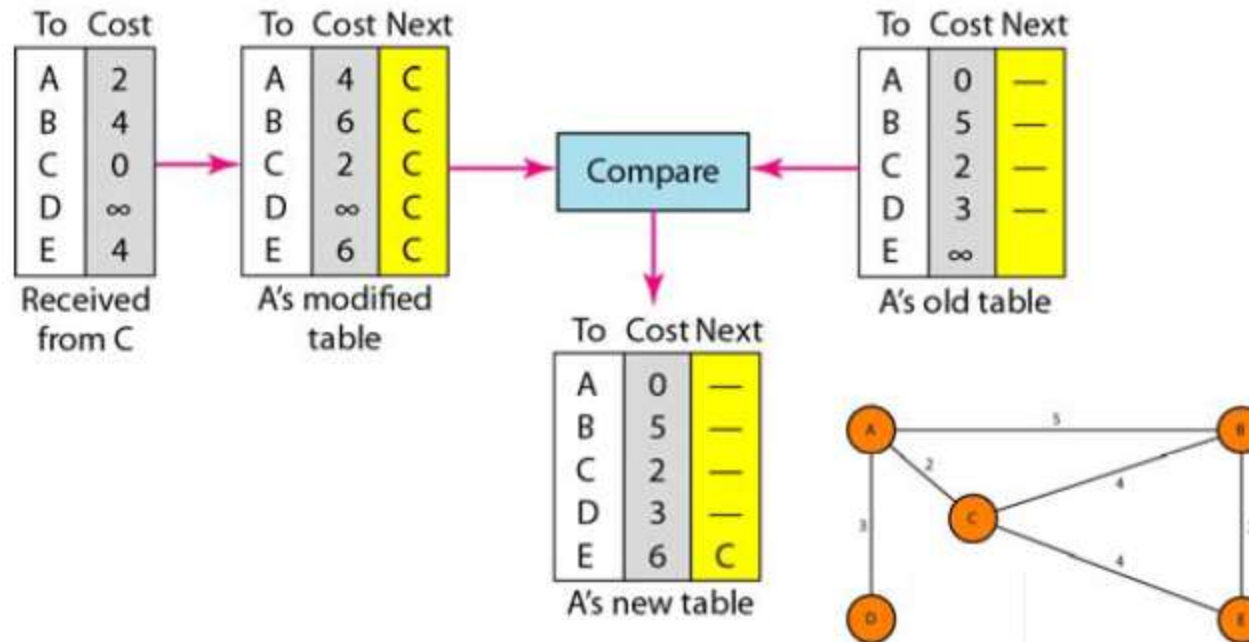


## 2.6.2. Sharing

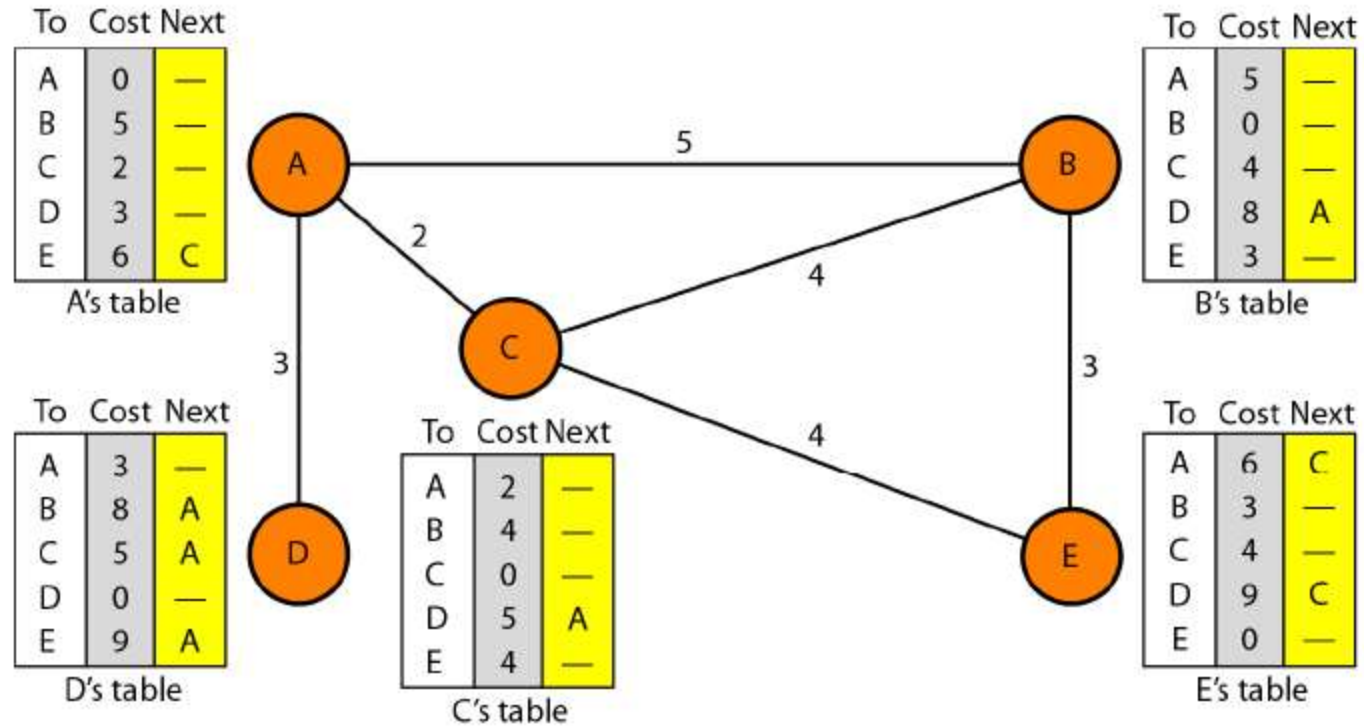
- 2 types of sharing(updates)
  1. Periodic
  2. Triggered
- Directly connected neighbours exchange(share) updates periodically (on the order of several seconds 30 sec)
- Whenever table changes (called *triggered* update)

## 2.6.3. 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



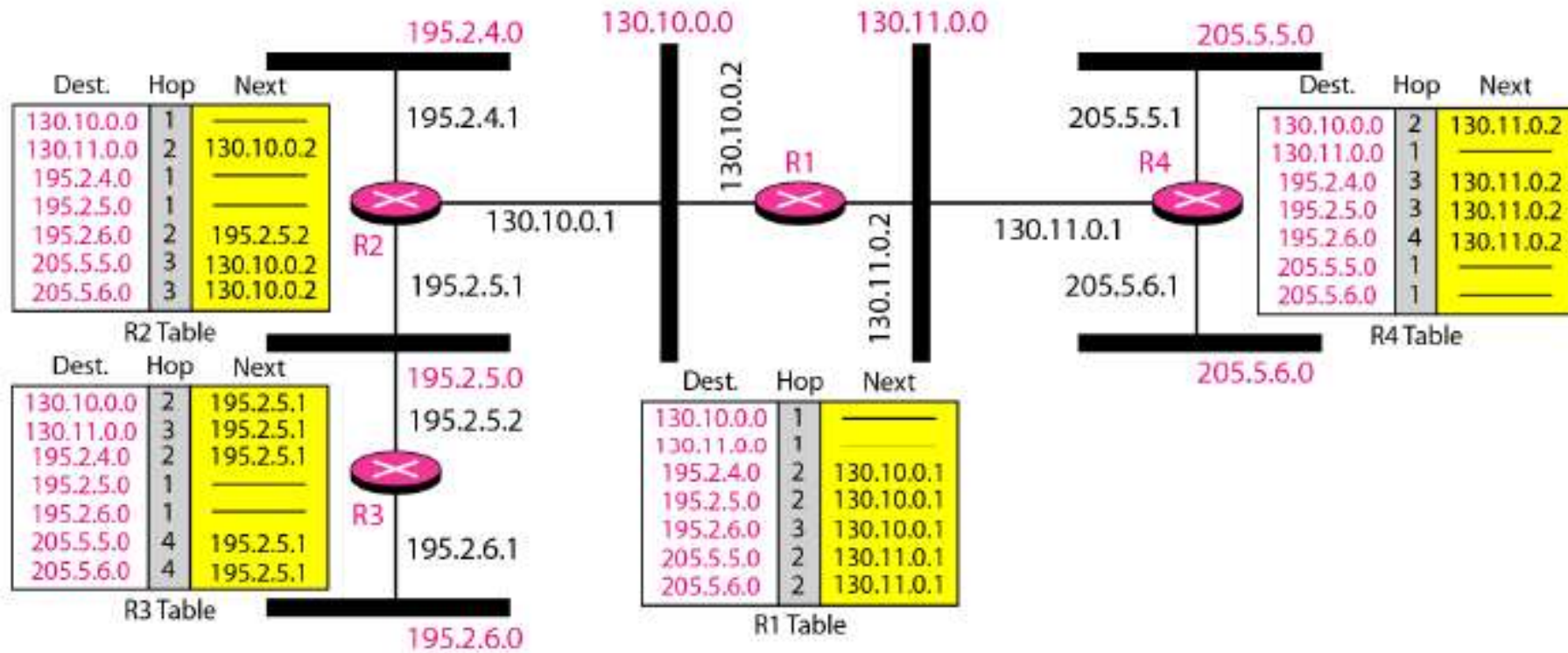
## 2.6.4. Final Routing Table



## 2.6.5. Routing Information Protocol(RIP)

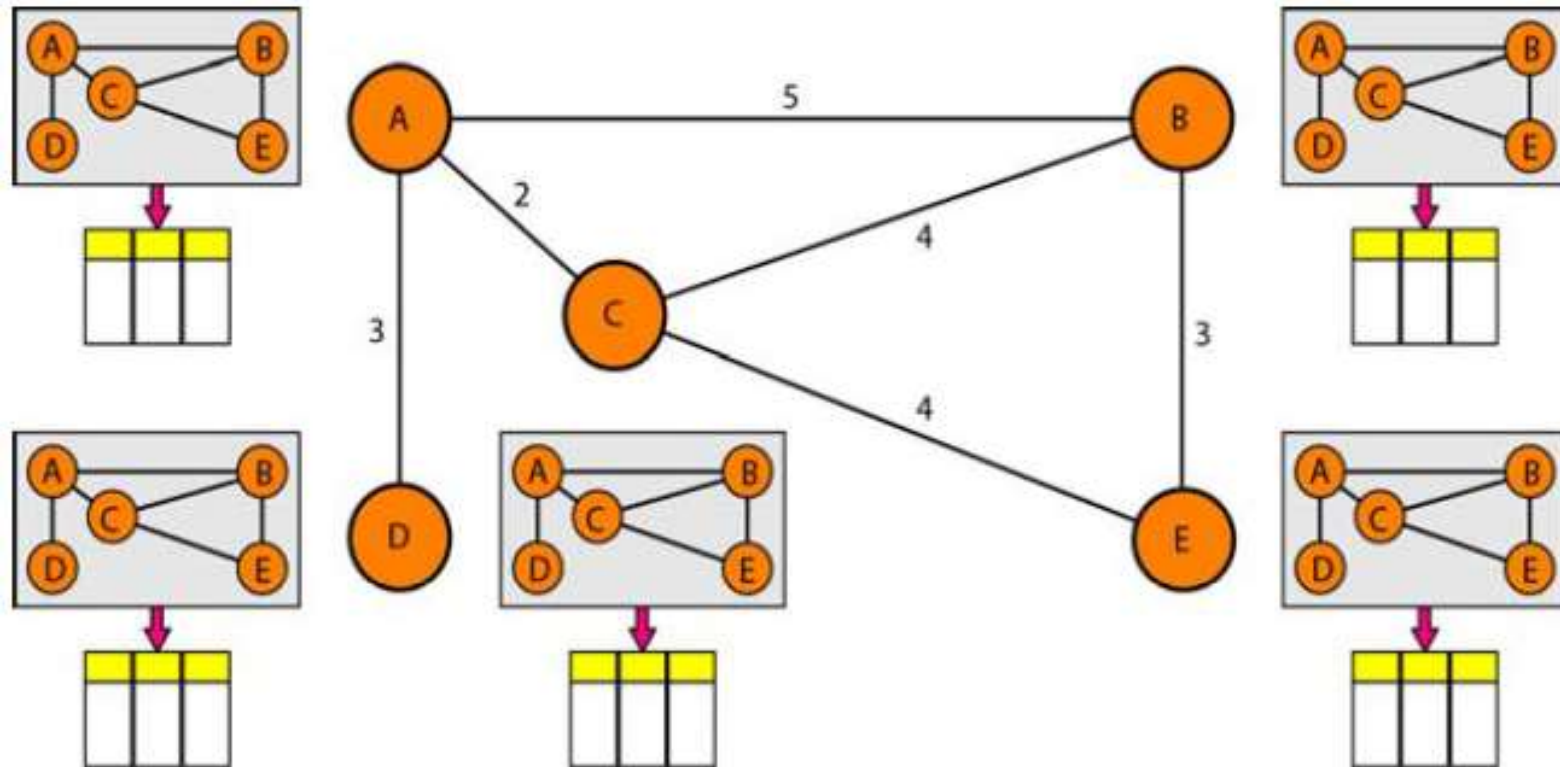
- RIP is based on Distance Vector(DV) routing protocol
- Interior routing protocol(Inside Autonomous System only)
- The destination in a routing table is a network, which means the first column defines a network address
- Distance is defined as the number of links (networks) to reach the destination(Hop counting)
- Metric in RIP is called a hop count(Number of router)
- Infinity is defined as 16, which means that any route in an autonomous system using RIP cannot have more than 15 hops(Max 15 router)

## 2.6.6. RIP Routing Table



## 2.7. Link State Routing (OSPF)

- Each node in the domain has the entire topology of the domain.
- The node can use Dijkstra's algorithm to build a routing table.



## 2.7.1. Routing Table Updates in Link State

- Steps in Updating process
  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

## 2.7.2. Link State packet

LSP consist of Following details

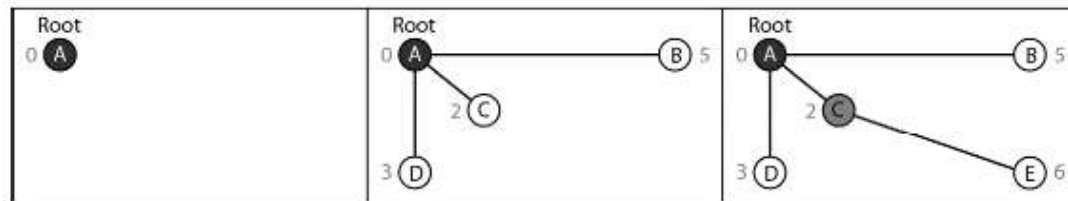
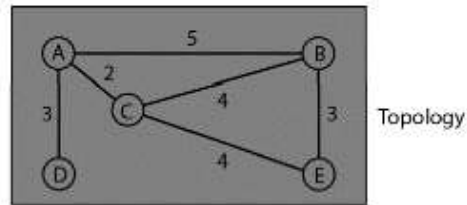
- ID of the node that created the LSP
- Cost of link to each directly connected neighbour
- Sequence number
- Time-to-live (TTL) for this packet
- Link State Packet Creation (LSP)
  1. *When there is a change in the topology of the domain*
  2. *Periodic (60 sec to 2 hours according to implementation)*



## 2.7.3. Routing table Updates

- Formation Shortest path tree In A

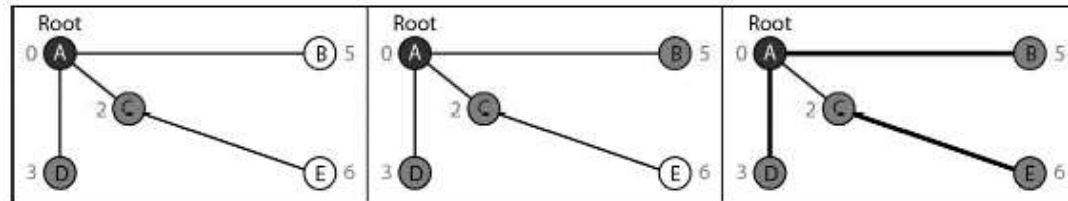
- Final Routing table of A



1. 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.

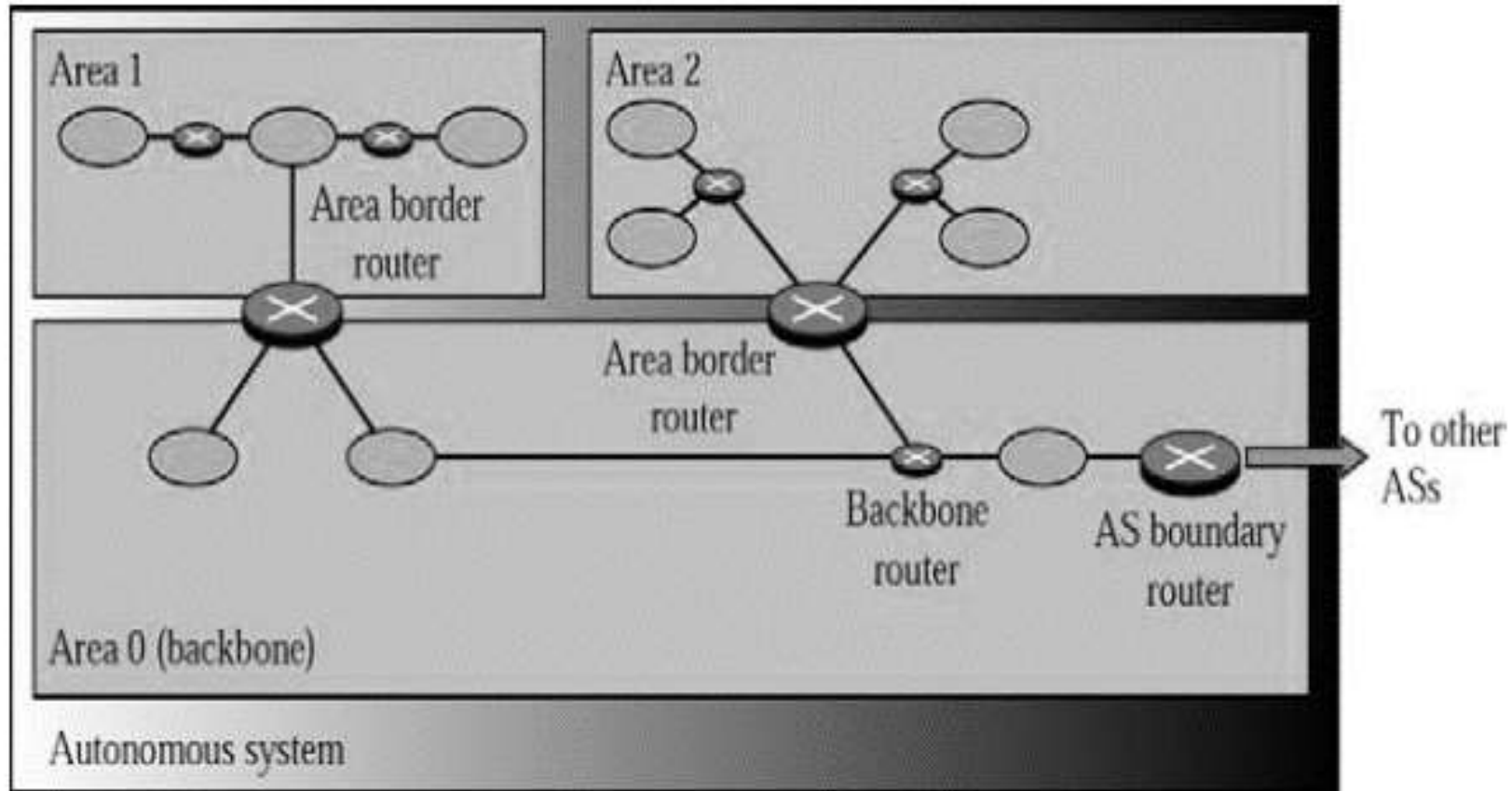
6. Move E to permanent list (tentative list is empty).

<i>Node</i>	<i>Cost</i>	<i>Next Router</i>
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

## 2.7.4. Open Shortest Path First(OSPF)

- OSPF divides an autonomous system into areas
- Each area is a collection of networks, hosts and routers
- Every router in the same area has the same link state database
- Special routers called autonomous system boundary routers are responsible for disseminate information about other autonomous systems into the current system.
- Metric used:
  - Administrator can assign the cost to each route based on type of service (minimum delay, maximum throughput...etc)

## 2.7.5. Autonomous System

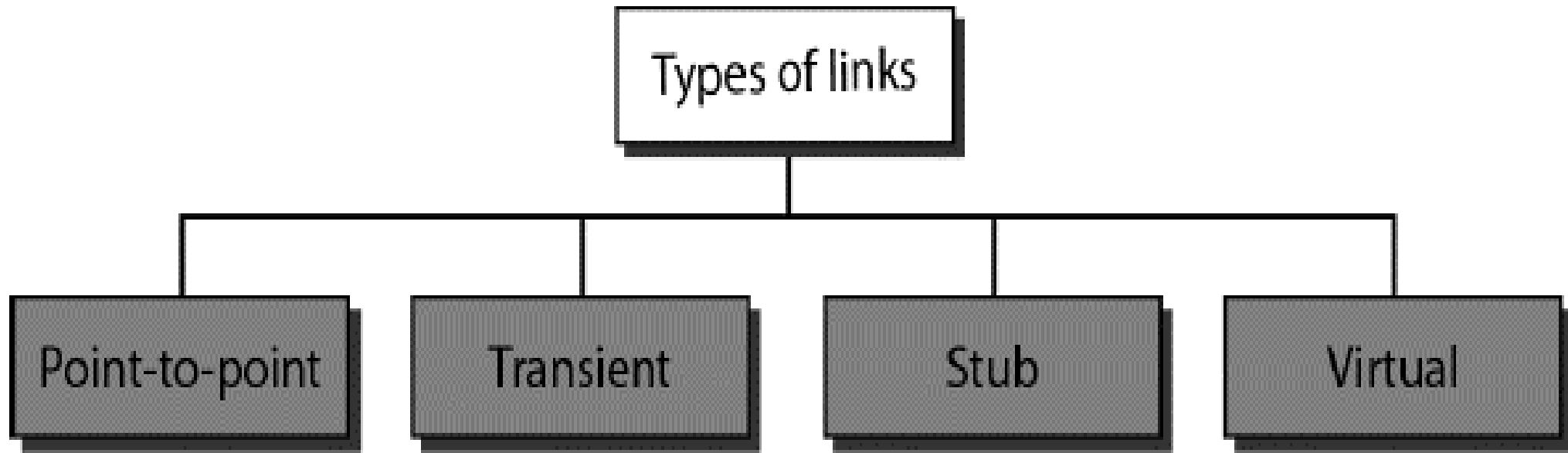


## 2.7.6. Areas in OSPF

- Area is a collection of networks, hosts, and routers all contained within an autonomous system.
- Routers inside an area flood the area with routing information.
- Area border routers: Summarize the information about the area and send it to other routers
- Backbone area [Primary area]: All the areas inside an autonomous system must be connected to the backbone
- Routers in the backbone area are called backbone routers. This area identification number is 0(in real world)

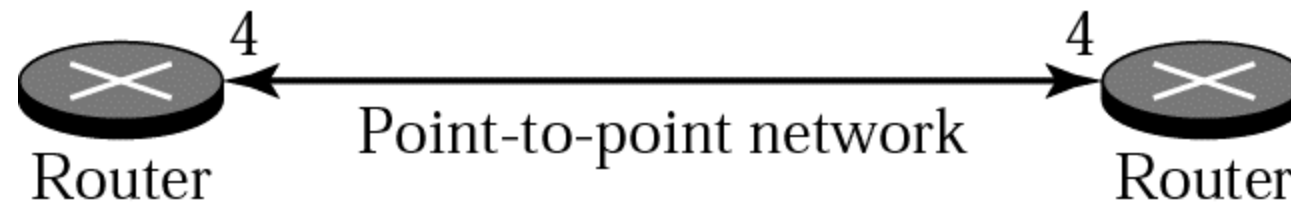
## 2.7.7. Types of Links in OSPF

- OSPF is based on Links
- There are 4 types of links



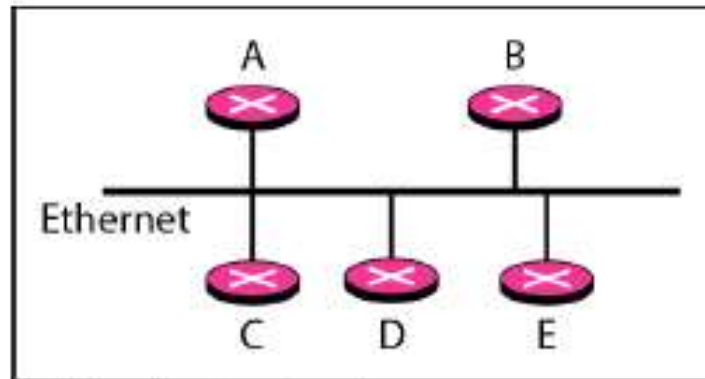
## 2.7.7.1. Point To Point

- Connects two routers without any other router or host in between.
- Directly connected routers using serial line.
- Only one neighbour for one router

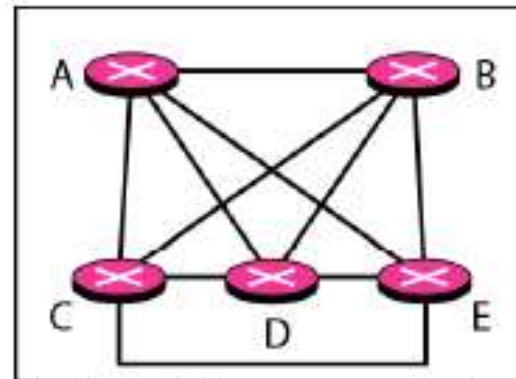


## 2.7.7.2. Transient Link

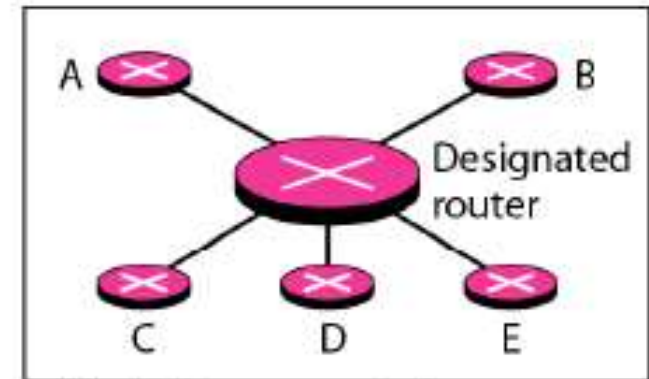
- A network with several routers attached to it
- Each router has many neighbours



a. Transient network



b. Unrealistic representation

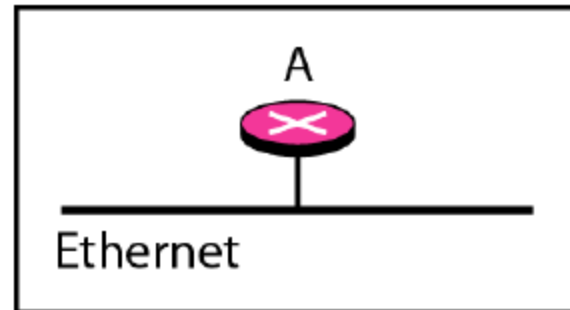


c. Realistic representation

*NB : Ethernet in Figure A means all router is connected into a switch*

## 2.7.7.3. Stub Link

- A **stub link** is a network that is connected to only one router
- The data packets enter the network through this single router and leave the network through this same router



a. Stub network

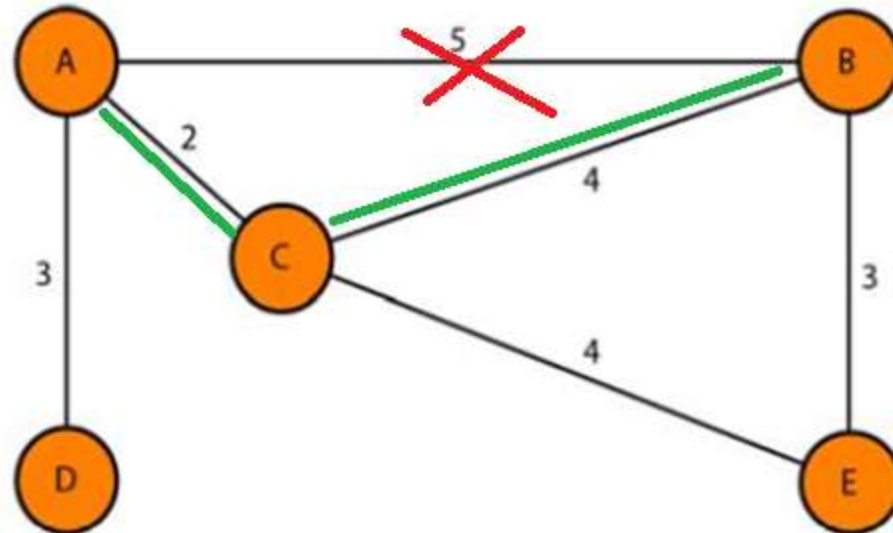


b. Representation



## 2.7.7.4. Virtual Link

- When the link between two routers is broken, the administration may create a **virtual link** between them, using a longer path that probably goes through several routers
- Consider A to B (cost = 5) Link is broken , Link can be created from A to B through C (A-C-B , Cost =6)

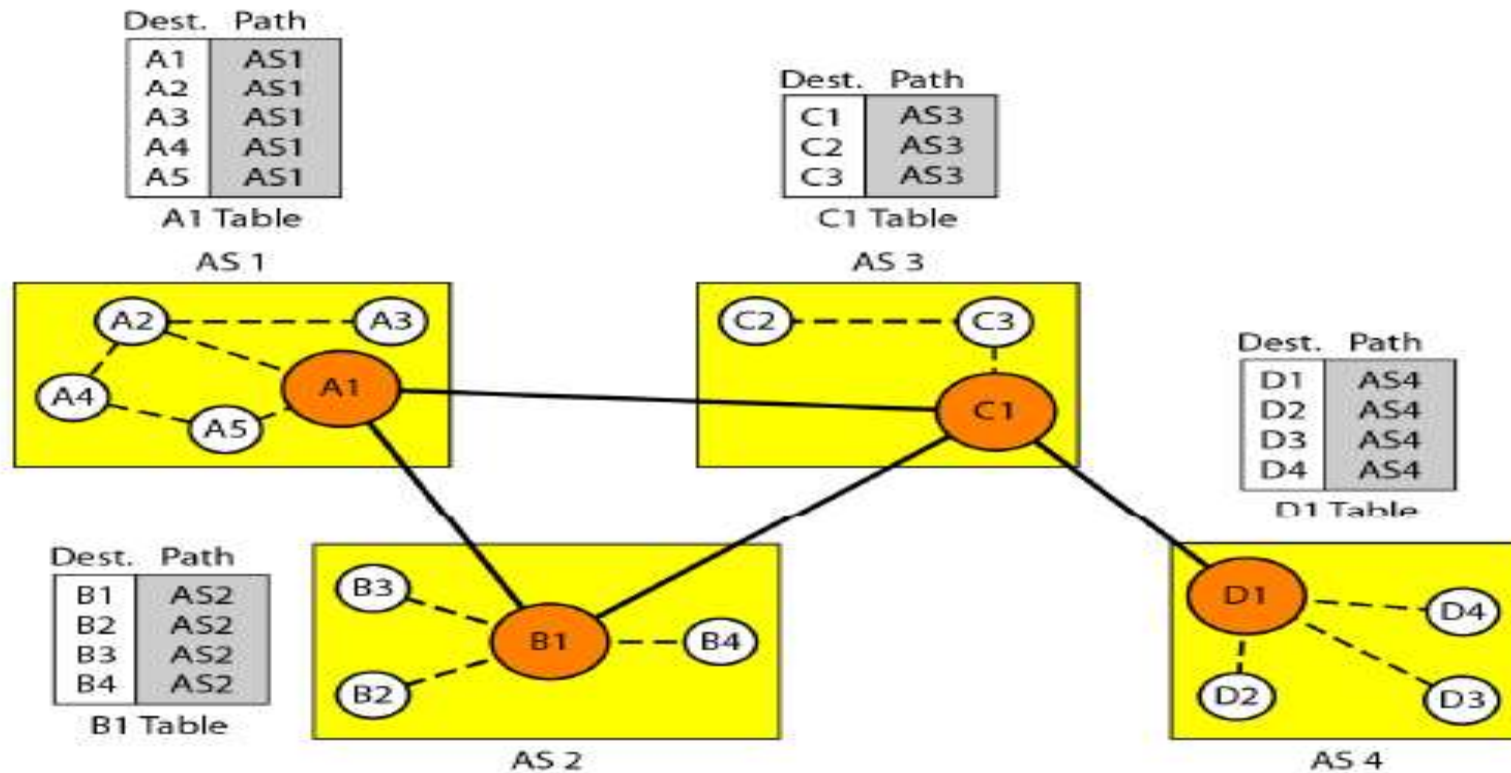


## 2.8. Path Vector (BGP)

- Path vector routing is inter domain routing protocol (exterior routing/ between AS)
- Each AS have at least one special node called speaker node
- Speaker node only can communicate with other AS
- In the Figure in next section A1, B1, C1, D1 are the speaker nodes.
- A speaker node advertises the path, not the metric of the nodes, in its autonomous system or other autonomous systems.

## 2.8.1. Initialization of Routing Tables

- Each speaker node have information of other node inside the AS only



## 2.8.2. Sharing & Updating of Routing Table

### **Sharing:**

- Speaker nodes will share the information of AS to other AS

### **Updating:**

- If multiple routes are received for a node path with minimum number of AS in between is selected.

## 2.8.3. Stable Routing Table

Dest.	Path
A1 ...	AS1
A5	AS1
B1 ...	AS1-AS2
B4	AS1-AS2
C1 ...	AS1-AS3
C3	AS1-AS3
D1 ...	AS1-AS2-AS4
D4	AS1-AS2-AS4

A1 Table

Dest.	Path
A1 ...	AS2-AS1
A5	AS2-AS1
B1 ...	AS2
B4	AS2
C1 ...	AS2-AS3
C3	AS2-AS3
D1 ...	AS2-AS3-AS4
D4	AS2-AS3-AS4

B1 Table

Dest.	Path
A1 ...	AS3-AS1
A5	AS3-AS1
B1 ...	AS3-AS2
B4	AS3-AS2
C1 ...	AS3
C3	AS3
D1 ...	AS3-AS4
D4	AS3-AS4

C1 Table

Dest.	Path
A1 ...	AS4-AS3-AS1
A5	AS4-AS3-AS1
B1 ...	AS4-AS3-AS2
B4	AS4-AS3-AS2
C1 ...	AS4-AS3
C3	AS4-AS3
D1 ...	AS4
D4	AS4

D1 Table

## 2.8.4. Border Gateway Protocol

- Inter domain (between AS) routing based on path vector
- Types of AS
  1. Stub AS
  2. Multihomed AS
  3. Transient AS
- Path attributes : List of attributes used by BGP to find best route
  1. Well Known Attribute
  2. Optional Attribute
- BGP Sessions: is a connection that is established between two BGP routers only for the sake of exchanging routing information
  1. E- BGP
  2. IBGP

## 2.8.4.1. Types of AS

- **Stub AS:** has only one connection to another AS. A host in one AS can send and receive data from another AS.
- **Multihomed AS:** Have many connections to a AS. It can send and receive data from many other AS. But will not allow data to pass through it.
- **Transient AS:** is a multihomed AS that also allows transient traffic (allow traffic to pass through)

## 2.8.4.2. Path Attributes

- **Well Known Attributes:** Attributes that BGP router must recognize, Its categories are:
  - **Well known mandatory :** is one that must appear in the description of a route.
  - **Well known discretionary :** is one that must be recognized by each router, but is not required to be included in every update message
- **Optional Attributes:** is one that needs not be recognized by every BGP router, Its categories are:
  - **Optional transitive attribute:** is one that must be passed to the next router by the router that has not implemented this attribute
  - **Optional nontransitive attribute:** is one that must be discarded if the receiving router has not implemented it

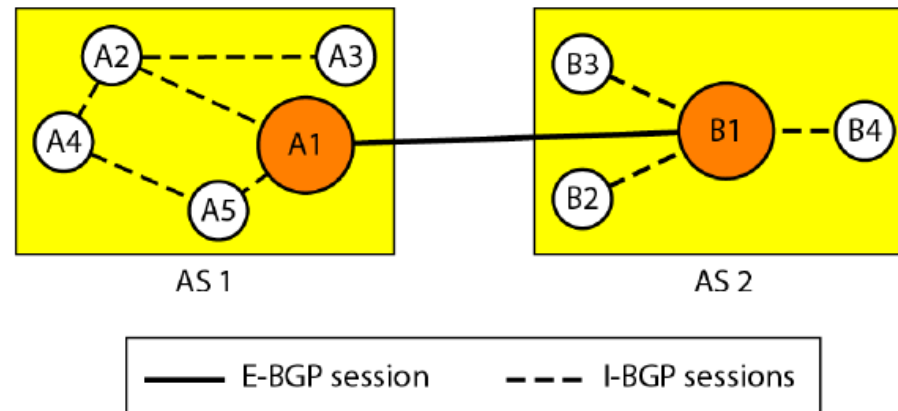


## 2.8.4.3. Path Attributes

- **Well Known Attributes:** Attributes that BGP router must recognize, Its categories are:
  - **Well known mandatory :** is one that must appear in the description of a route.
  - **Well known discretionary :** is one that must be recognized by each router, but is not required to be included in every update message
- **Optional Attributes:** is one that needs not be recognized by every BGP router, Its categories are:
  - **Optional transitive attribute:** is one that must be passed to the next router by the router that has not implemented this attribute
  - **Optional nontransitive attribute:** is one that must be discarded if the receiving router has not implemented it

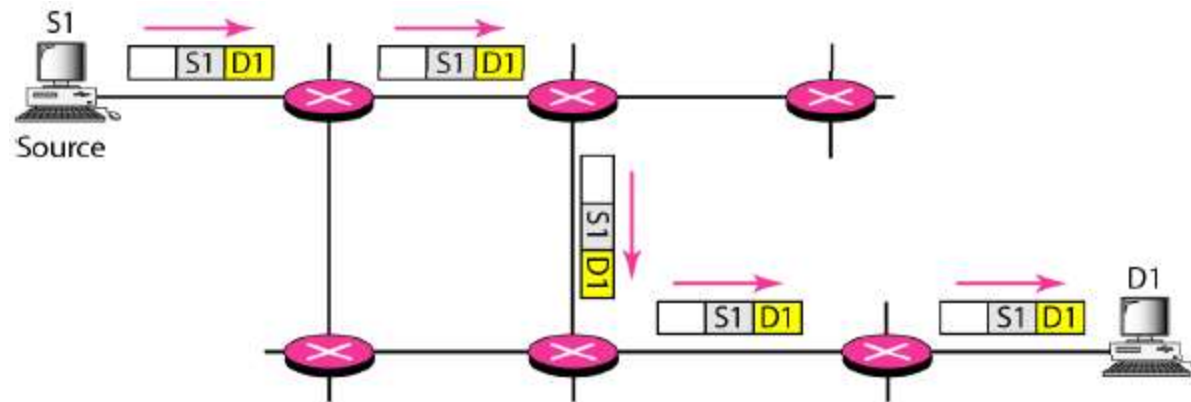
## 2.8.4.4. BGP Sessions

- A session is a connection that is established between two BGP routers only for the sake of exchanging routing information.
- BGP can have two types of sessions:
  1. **E-BGP(External) session:** is used to exchange information between two speaker nodes belonging to two different autonomous systems
  2. **I-BGP (Internal) session:** is used to exchange routing information between two routers inside an autonomous system



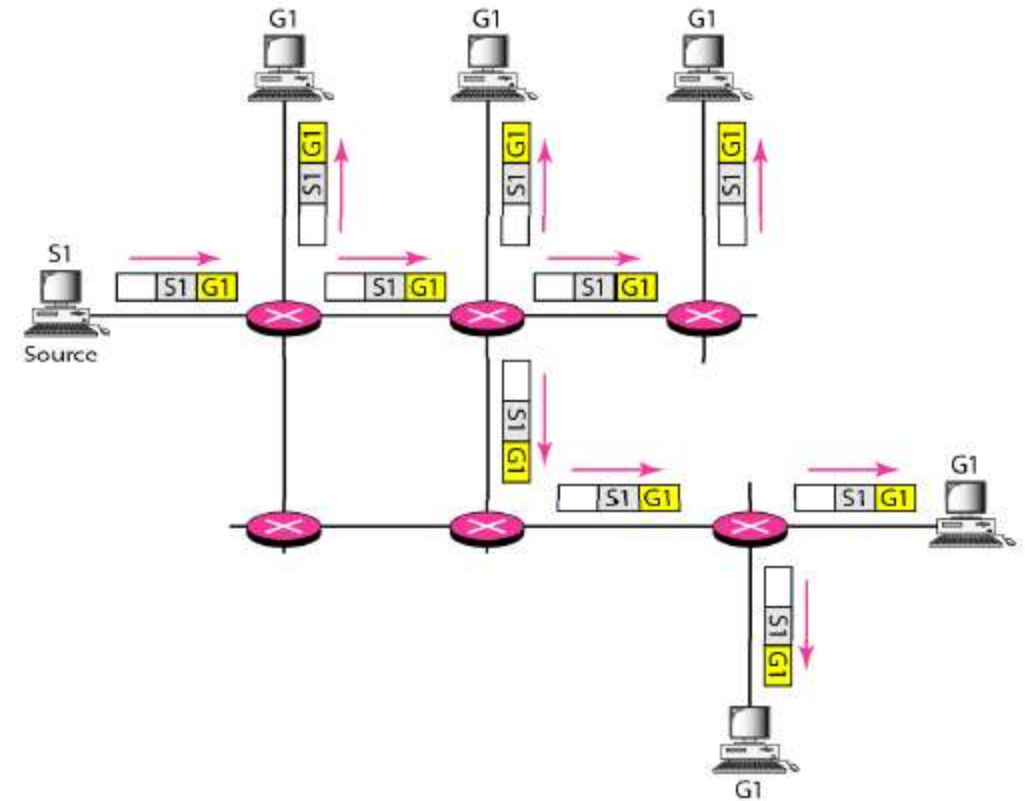
## 2.9. Unicasting vs Multicasting

- In unicast, the router forwards the received packet through only one of its interfaces
- Unicast (One to One)



## 2.9. Unicasting vs Multicasting

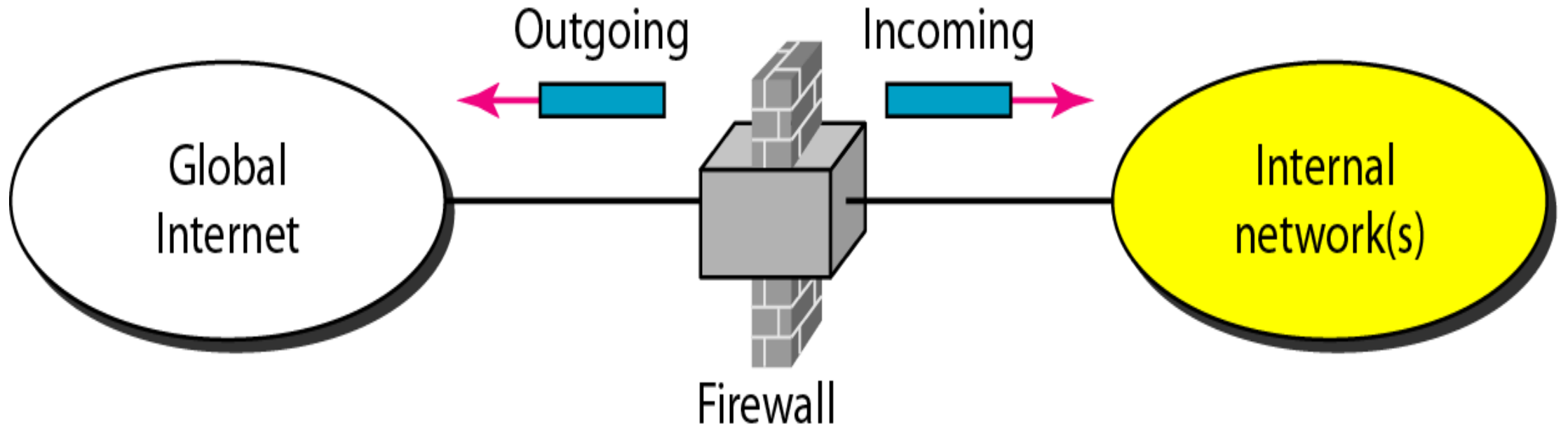
- In multicasting, the router may forward the received packet through several of its interfaces
- Multicasting (One to a Group)



## 6. Firewall

- A **firewall** is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet
- Firewall is designed to **forward** some packets and **filter** (not forward) others
- A firewall is a network security system designed to prevent unauthorized access to or from a private network
- Firewalls can be implemented in both hardware and software, or a combination of both
- Network firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected
- All messages entering or leaving the LAN pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria

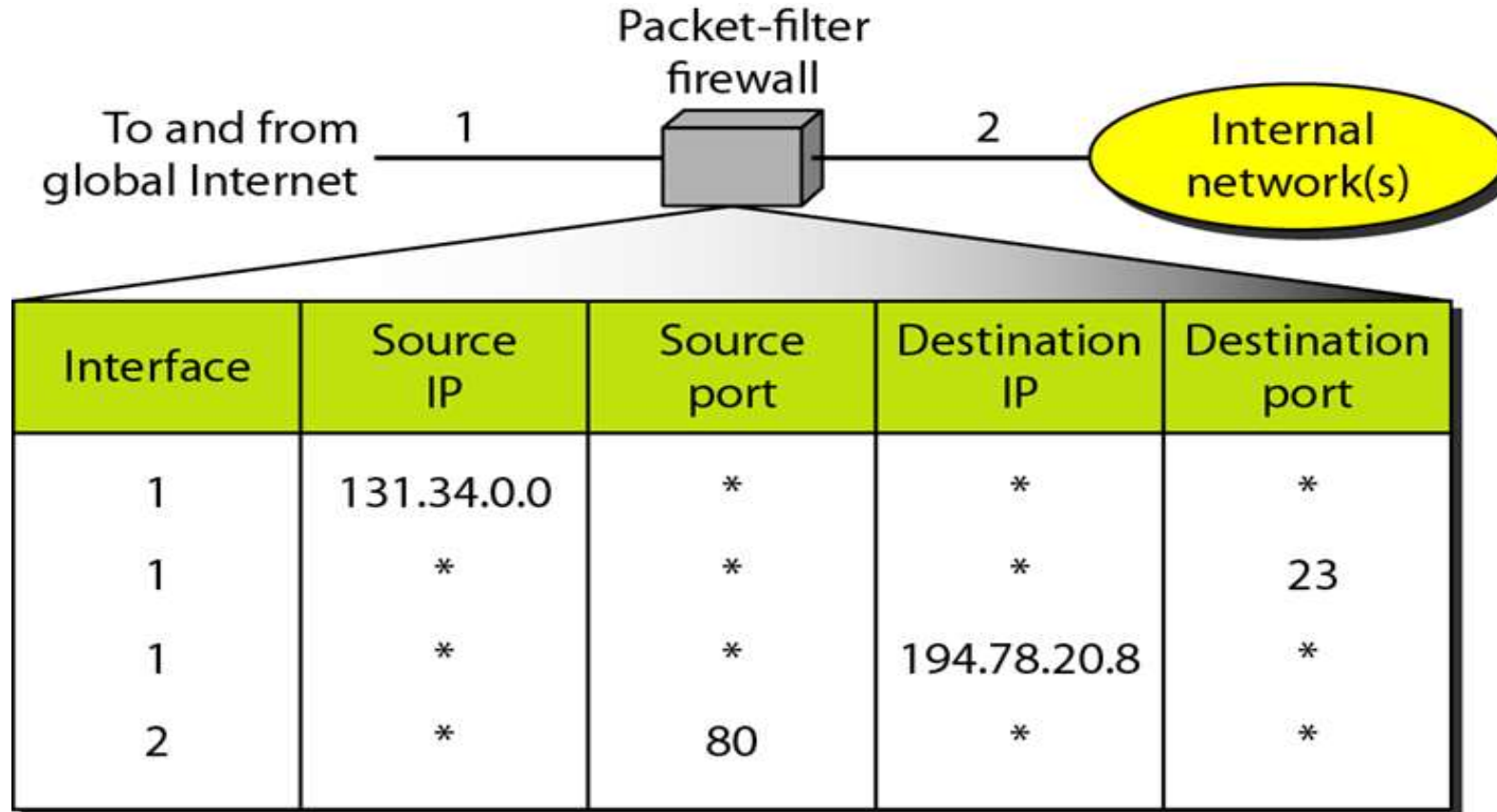
# 6. Firewall



# 6.1. Packet Filter Firewall

- A firewall can be used as a packet filter
- It can forward or block packets based on the information in the network layer and transport layer headers: source and destination IP addresses, source and destination port addresses, and type of protocol (TCP or UDP)
- A packet-filter firewall is a router that uses a filtering table to decide which packets must be discarded (not forwarded)

# 6.1. Packet Filter Firewall



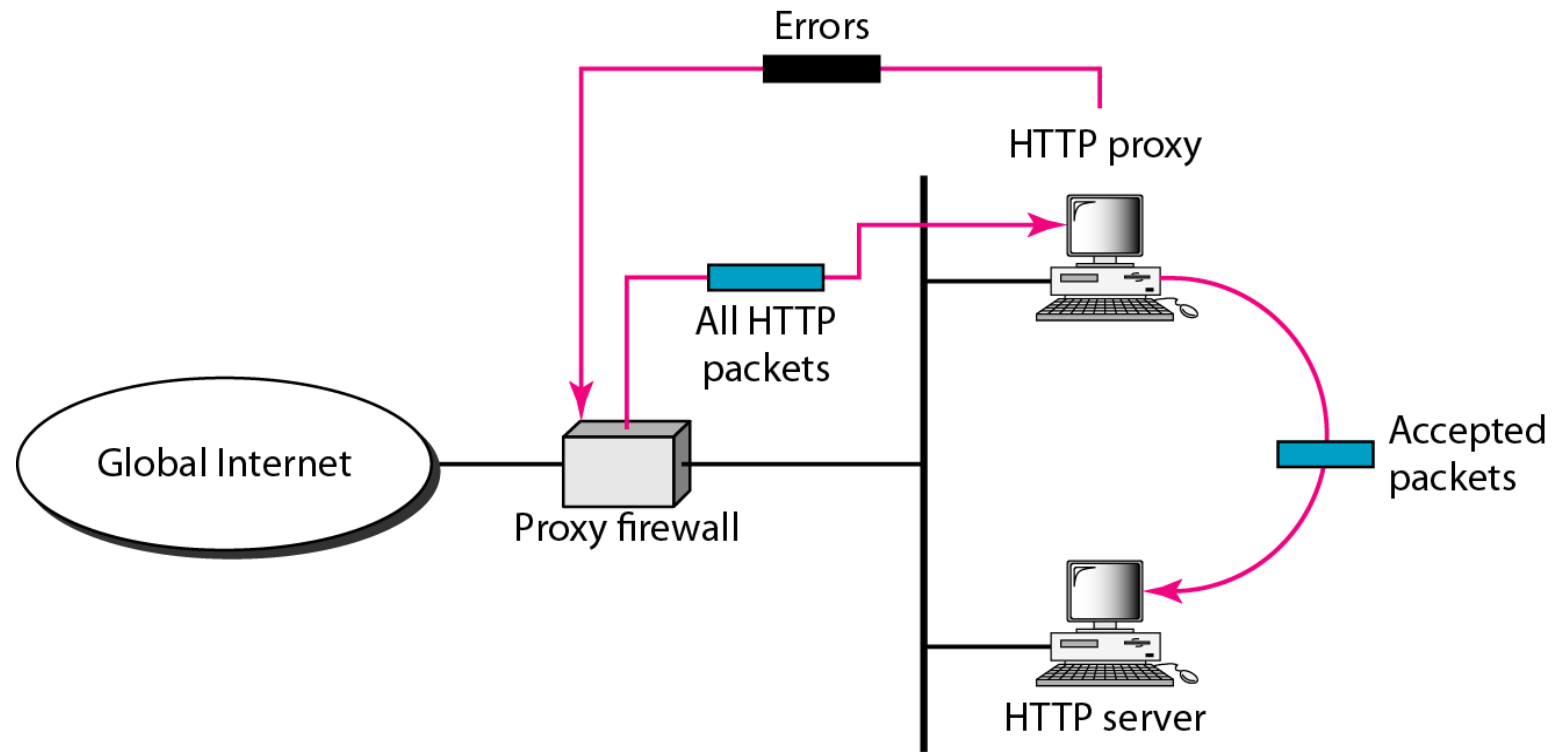
\* means any network



## 6.2. Proxy Firewall

- If we need to filter a message based on the information available in the message itself (at the application layer)
- If application level data (like text, URL, websites, links) is to be filtered then proxy firewall is best solution

# 6.2. Proxy Firewall



# 6.1. Types of Firewall (Hardware)

- Hardware firewalls is dedicated device which can be configured according to the need of large organization

## **Features**

- They are specialized devices
- Hardware firewalls tend to be expensive
- Complicated
- Difficult to upgrade,
- Difficult to configure

## 6.2. Types of Firewall-Software

- Hardware firewall can be configured in PC. It runs as a program in the PC and configuration can be done

### **Features**

- They are not specialized devices (Only special Programs in PC)
- Less expensive
- Easy to upgrade
- Easy to configure
- Less Complicated