

COMPUTER NETWORK

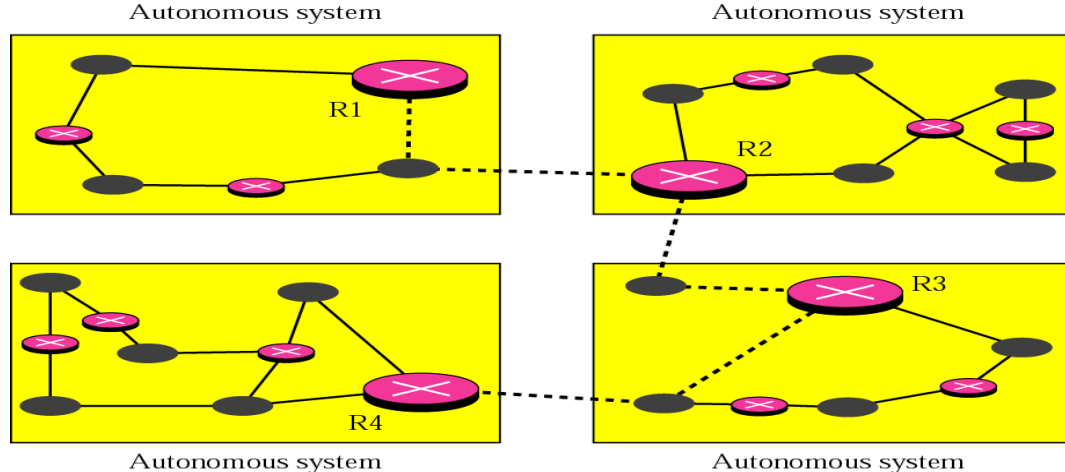
By:
Dr. Ankush Agarwal

NETWORK LAYER

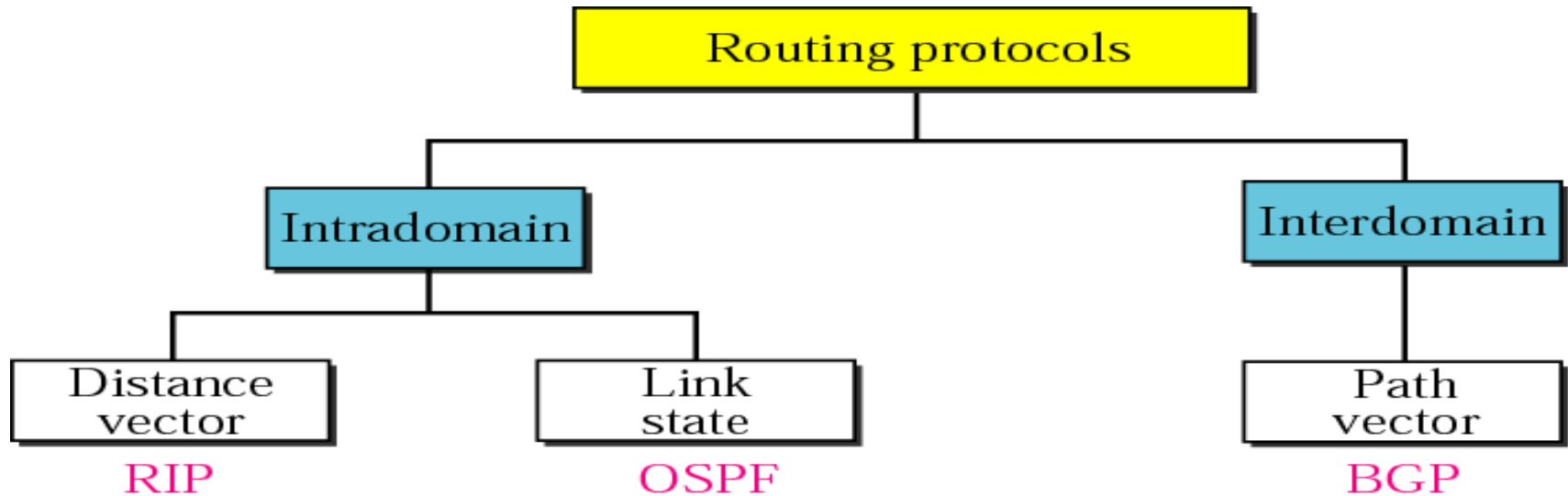


Autonomous systems

- An autonomous system is a set of networks and routers under the control of a single administrative authority
- Routing within an autonomous system is intra-domain routing
- Routing between autonomous systems is inter-domain routing

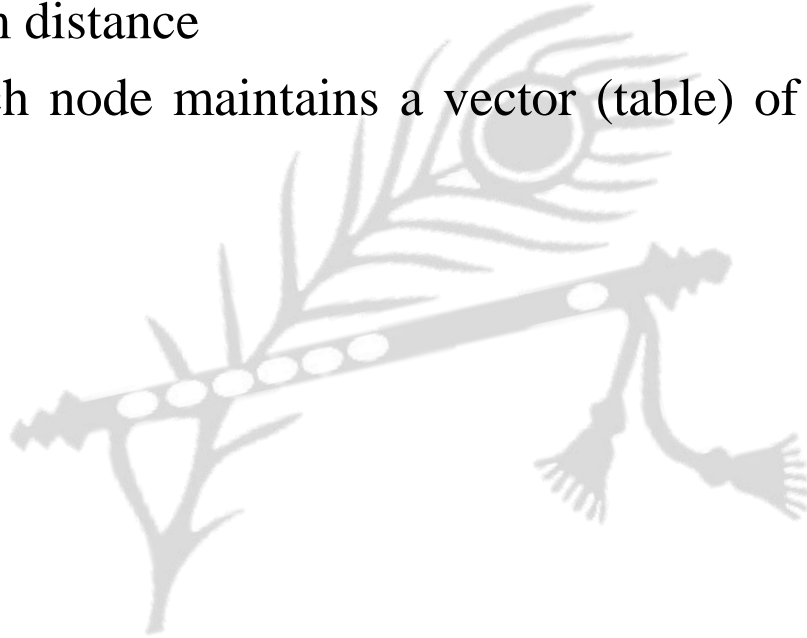


Popular routing protocols



Distance Vector Routing

- In distance vector routing, the least cost route between any two nodes is the route with minimum distance
- In this protocol each node maintains a vector (table) of minimum distances to every node



Distance Vector Routing tables

To Cost Next

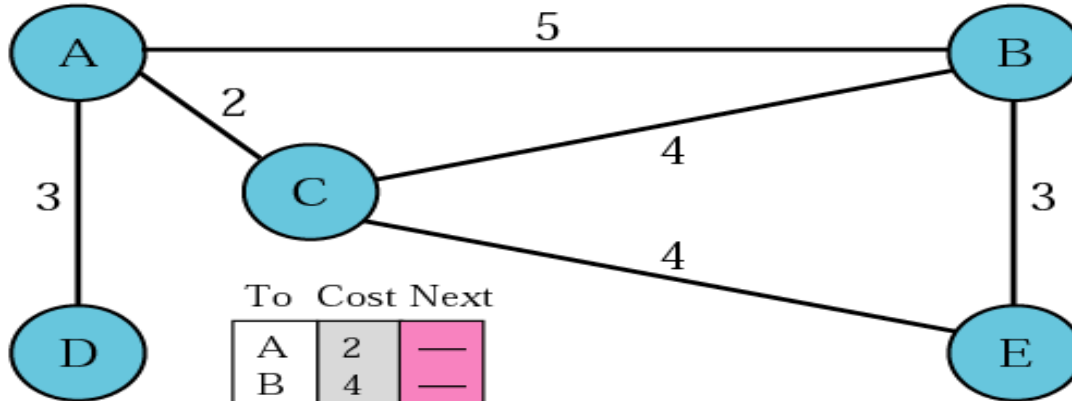
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

A'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	5	—
B	0	—
C	4	—
D	8	A
E	3	—

B's table

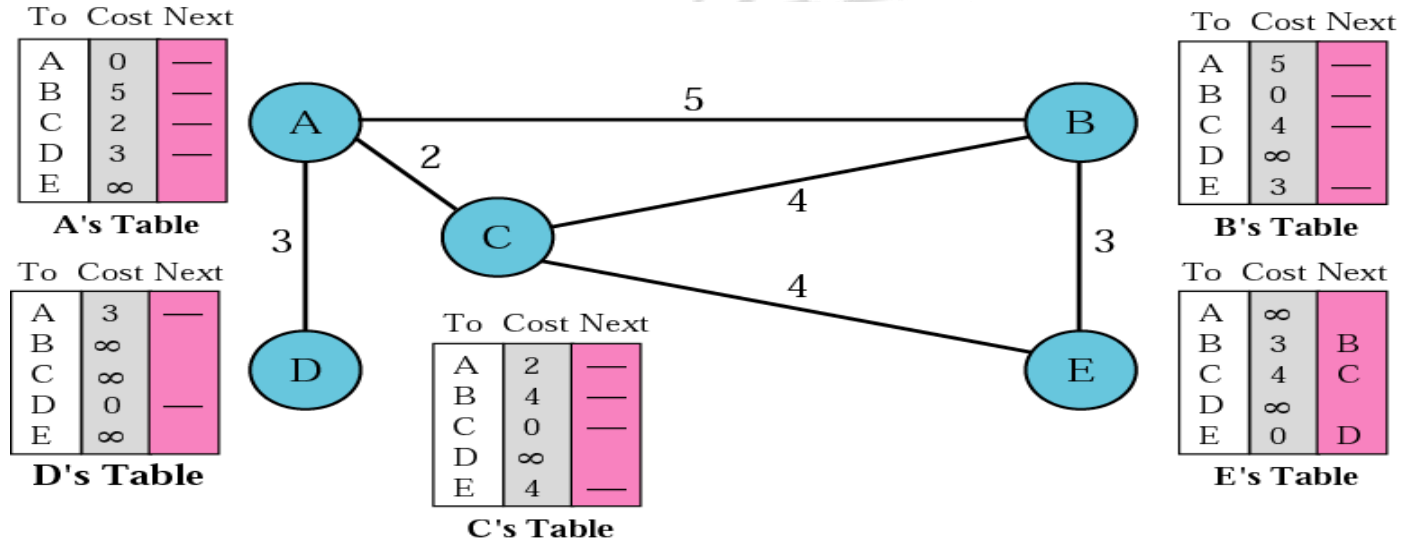
To Cost Next

A	6	C
B	3	—
C	4	—
D	9	C
E	0	—

E's table

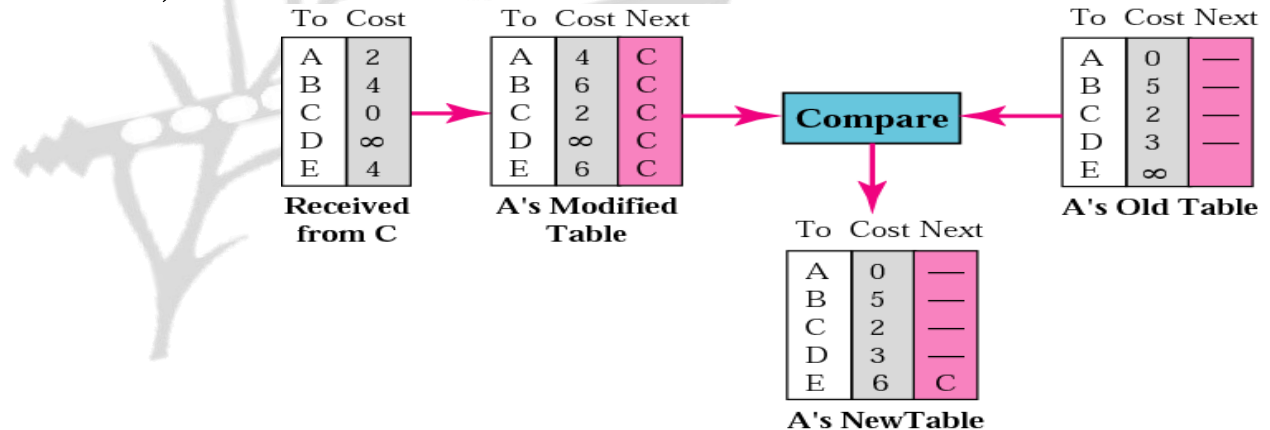
Initialization of tables in distance vector routing

- In distance vector routing, each node shares its table with its immediate neighbor periodically (eg every 30s) and when there is a change

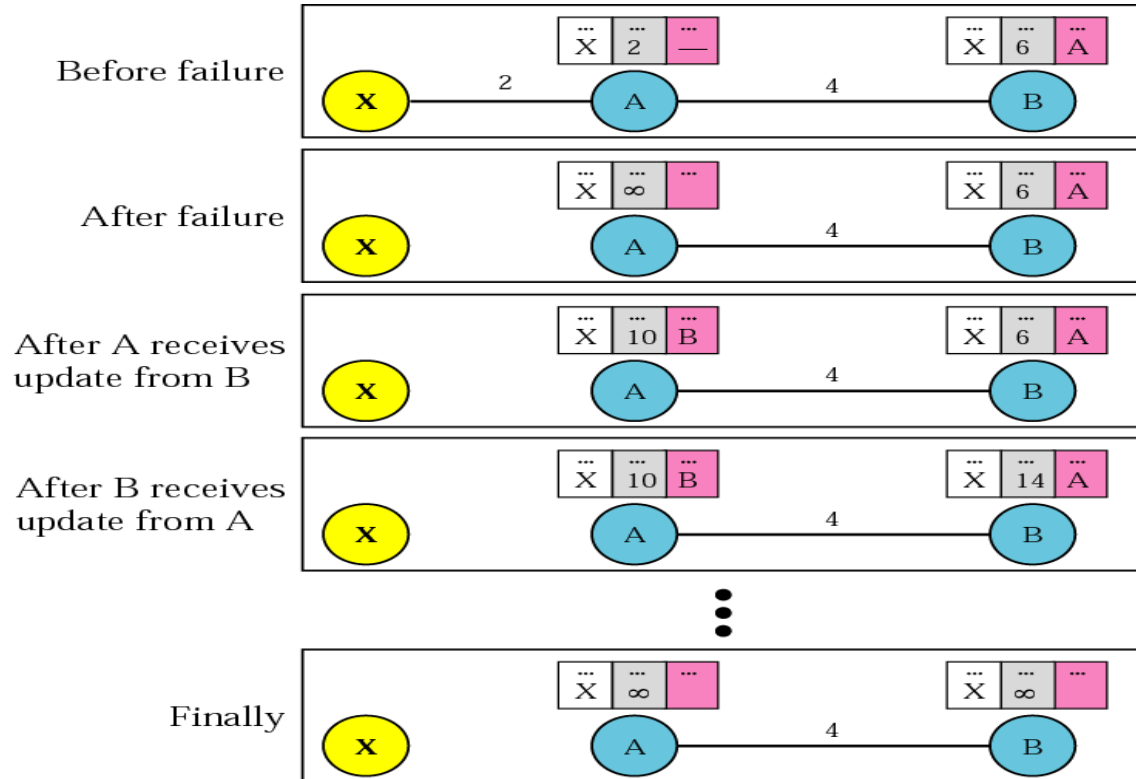


Updating in distance vector routing

- Step 1: Add cost (2) to table received from neighbor (C)
- Step 2: Compare Modified Table with Old Table (row by row)
- If Next node entry is different, select the row with the smaller cost, if tie, keep the old one
- If next node entry the same, select the new row value

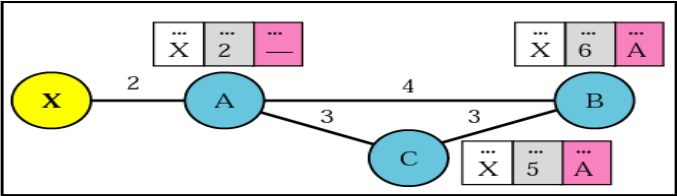


Two-node instability

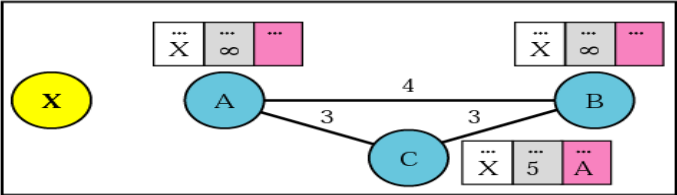


Three-node instability

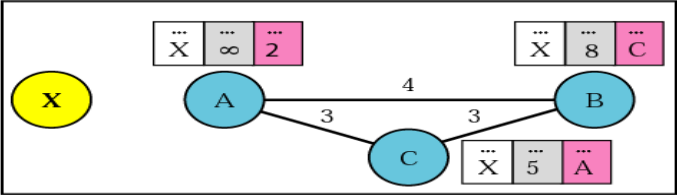
Before failure



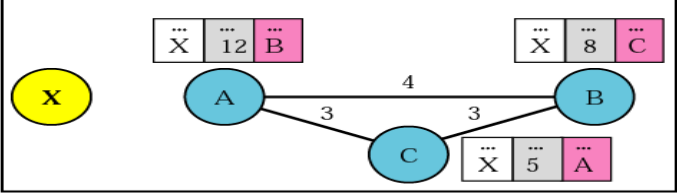
After A sends the route to B and C, but the packet to C is lost



After C sends the route to B

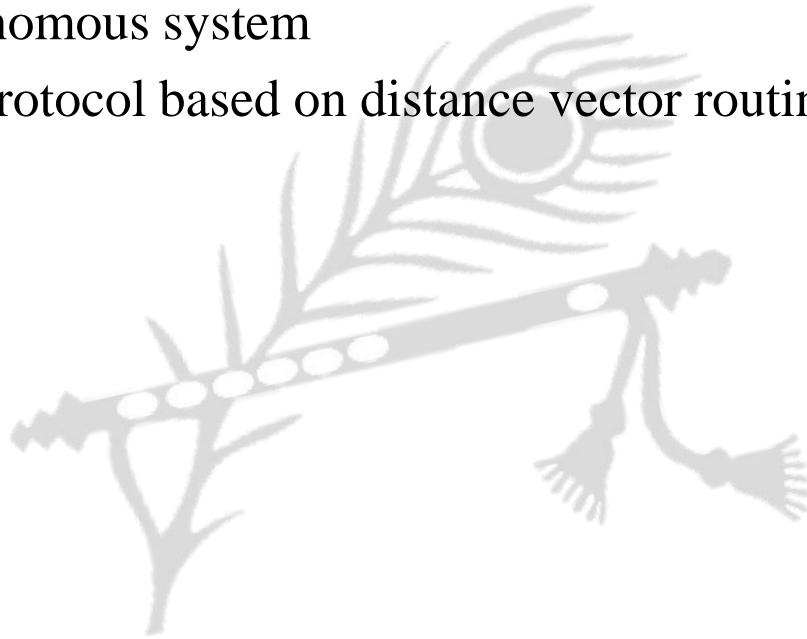


After B sends the route to A



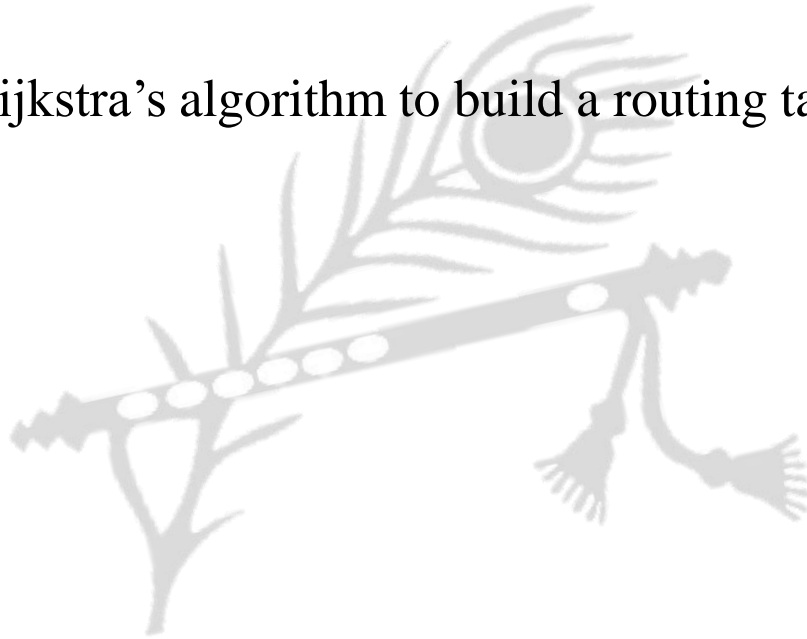
Routing Information Protocol

- The Routing Information Protocol (RIP) is an intra-domain routing protocol used inside an autonomous system
- It is a very simple protocol based on distance vector routing



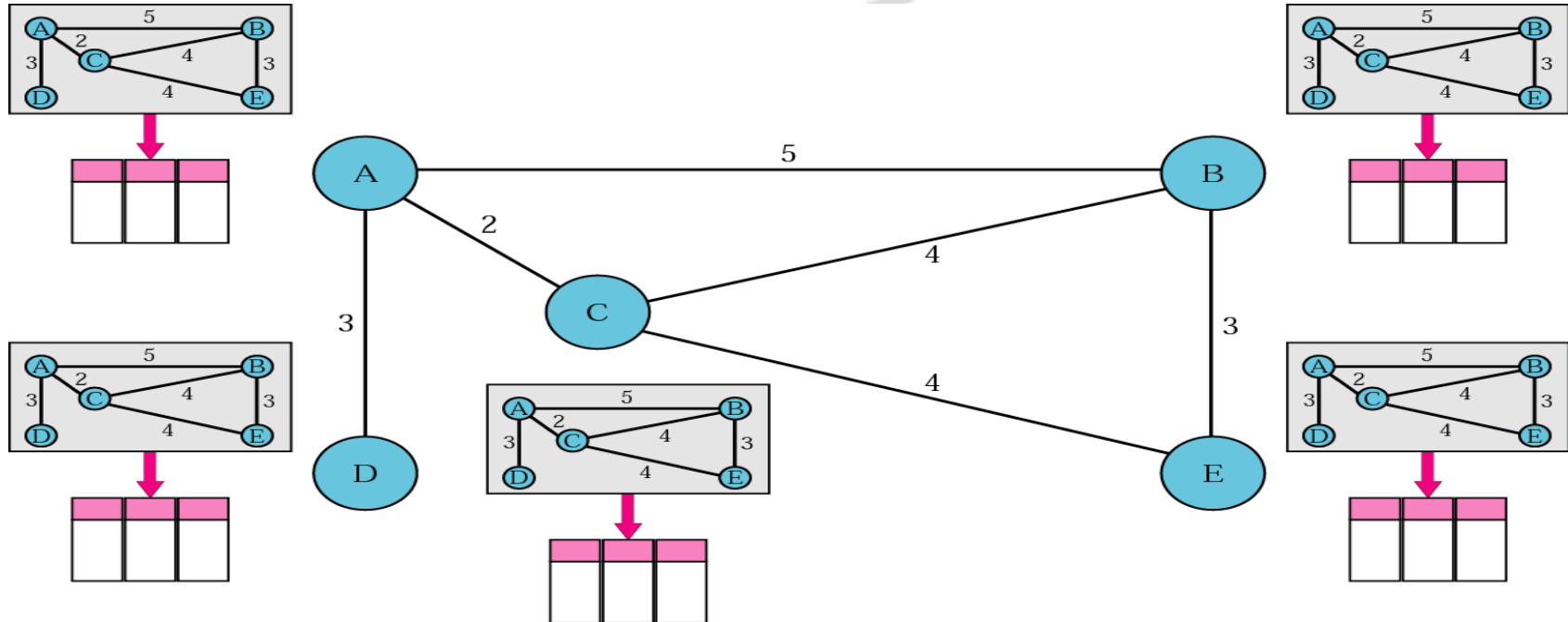
Link state routing

- In link state routing, each node in the domain has the entire topology of the domain
- The node can use Dijkstra's algorithm to build a routing table



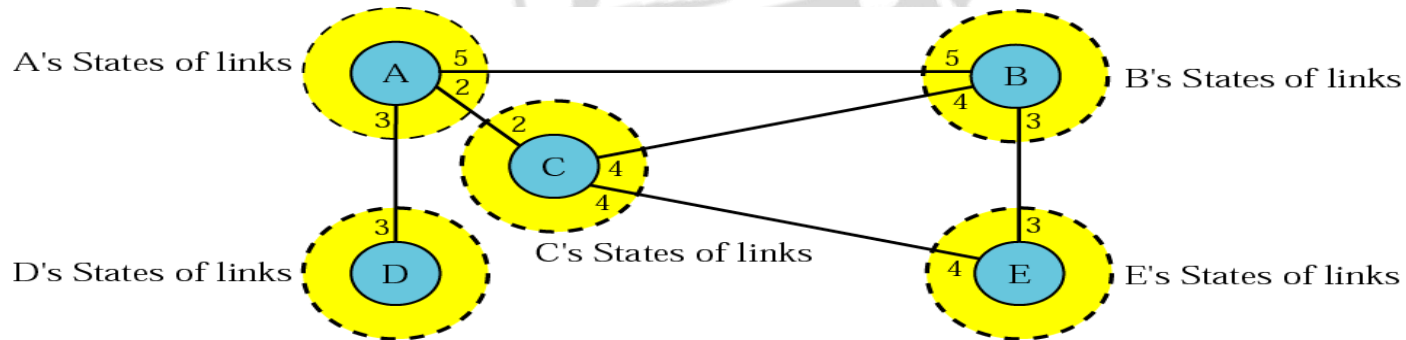
Concept of link state routing

Every router has knowledge about the network, but from its own perspective

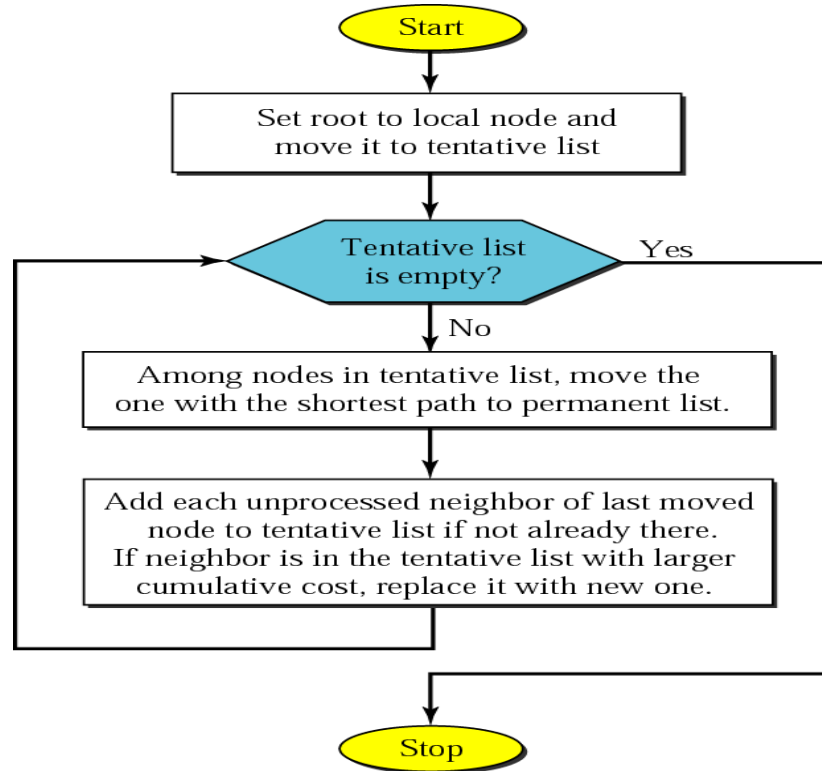


Link state knowledge

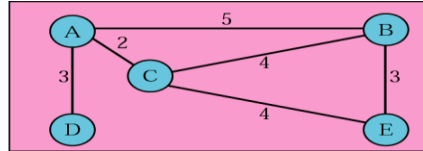
- Each router knows (maintains) its states of its links
- Each router floods this info (via a Link State Packet) to other routers periodically (to check the change in topology)
- Each router takes this data and using Dijkstra's algorithm, creates the shortest path tree and corresponding routing table



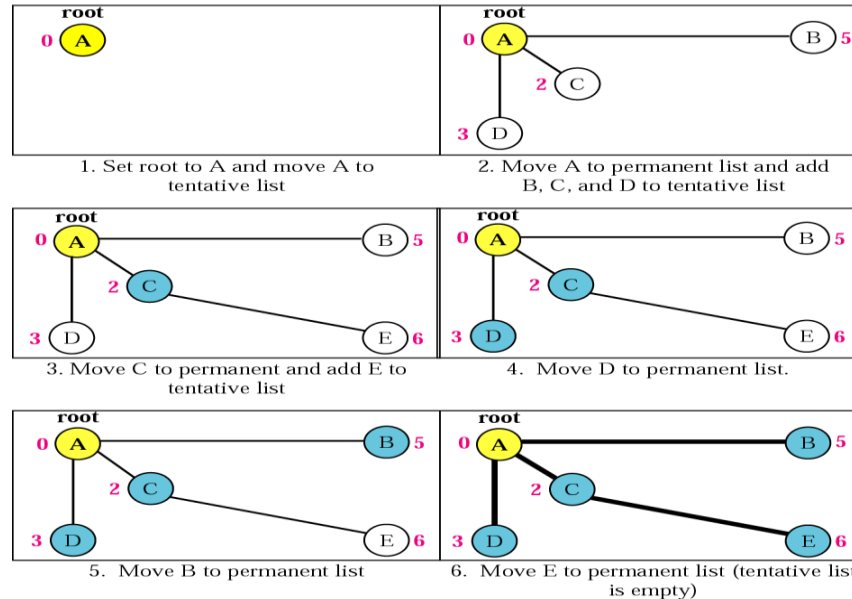
Dijkstra algorithm



Example of formation of shortest path tree

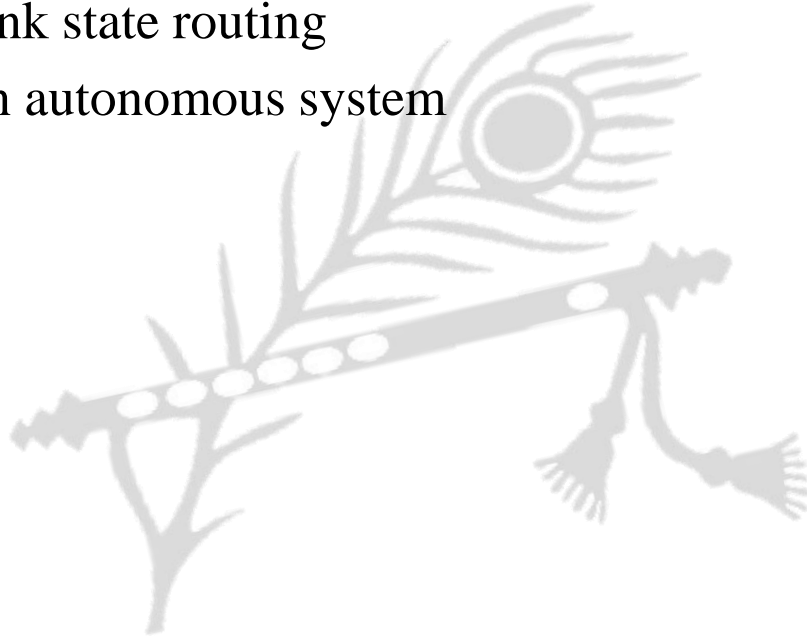


Topology



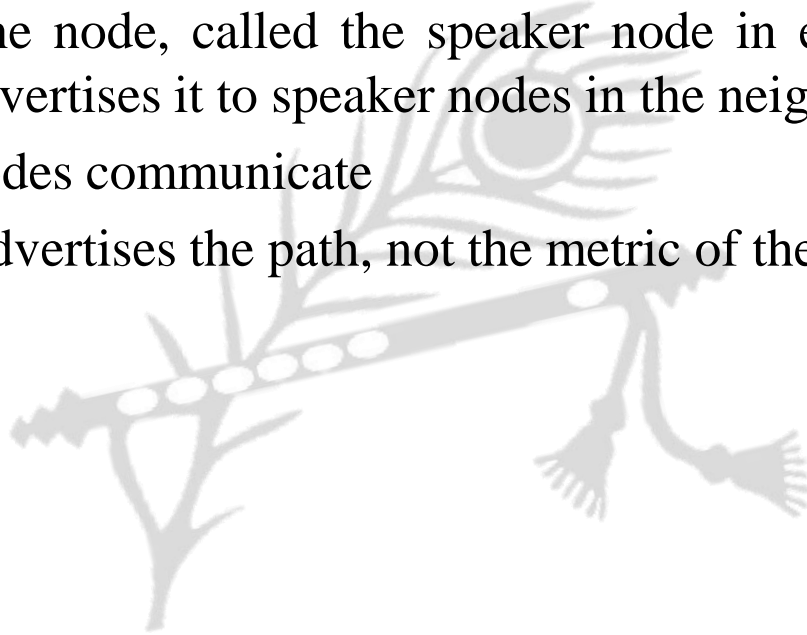
OSPF

- The Open Shortest Path First (OSPF) protocol is an intra-domain routing protocol based on link state routing
- Its domain is also an autonomous system



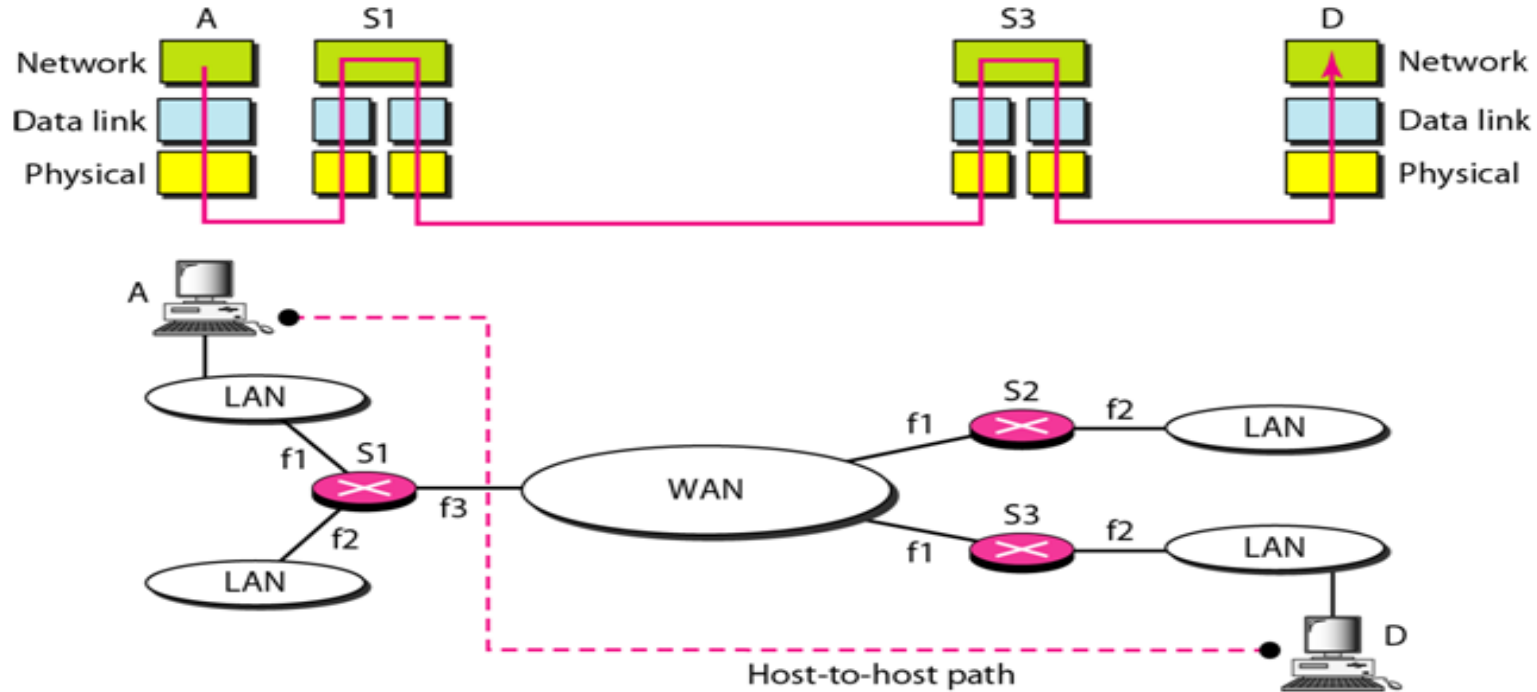
Path Vector Routing

- Path vector routing is similar to distance vector routing
- There is at least one node, called the speaker node in each AS that creates a routing table and advertises it to speaker nodes in the neighboring ASs
- Only the speaker nodes communicate
- The speaker node advertises the path, not the metric of the nodes



- Border Gateway Protocol (BGP) is an inter-domain routing protocol using path vector routing
- It first appeared in 1989 and has gone through four versions
- BGP interconnects three different types of AS
 - Stub AS, e.g. a corporate network
 - Multihomed AS, e.g. a large corporate network with connections to multiple ASs, but does not allow traffic to pass thru (transient)
 - Transit AS - one that allows transient traffic, such as an Internet backbone

Transmission using Network Layer

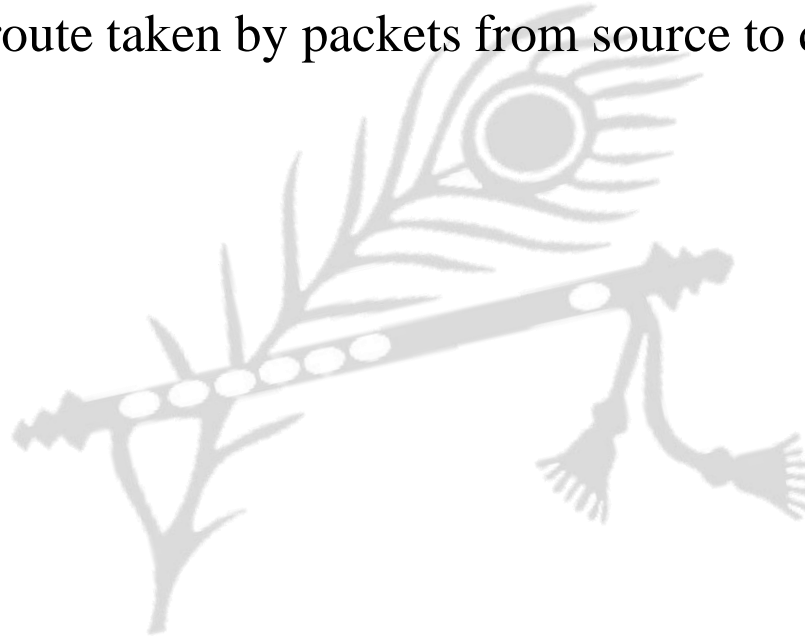


Network Layer

- Services
 - Routing and Forwarding
 - Host to Host Delivery (Using IP Addressing)
 - transport segment from sending to receiving host
 - on sending side encapsulates segments into datagrams
 - on receiving side, delivers segments to transport layer
 - network layer protocols in every host, router
 - router examines header fields in all IP datagrams passing through it

Two key network-layer functions

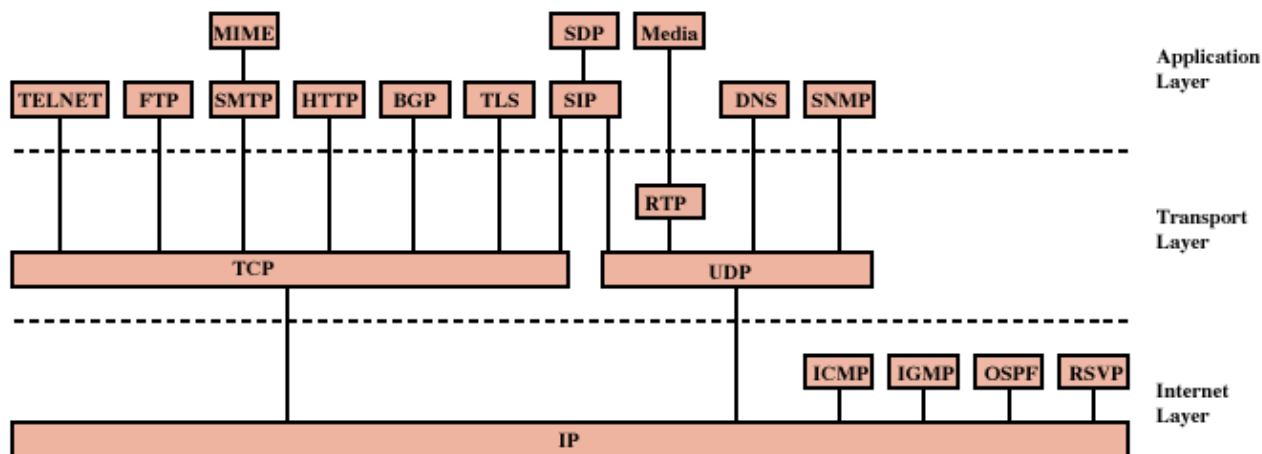
- forwarding: move packets from router's input to appropriate router output
- routing: determine route taken by packets from source to destination



Some basics of IP

- The term internet is short for “internetworking”
 - interconnection of networks with different network access mechanisms, addressing, different routing techniques, etc.
- An internet
 - Collection of communications networks interconnected by layer 3 switches and/or routers
- The Internet - note the uppercase I
 - The global collection of individual machines and networks
- IP (Internet Protocol)
 - most widely used internetworking protocol
 - foundation of all internet-based applications

Protocols of TCP/IP Protocol Suite

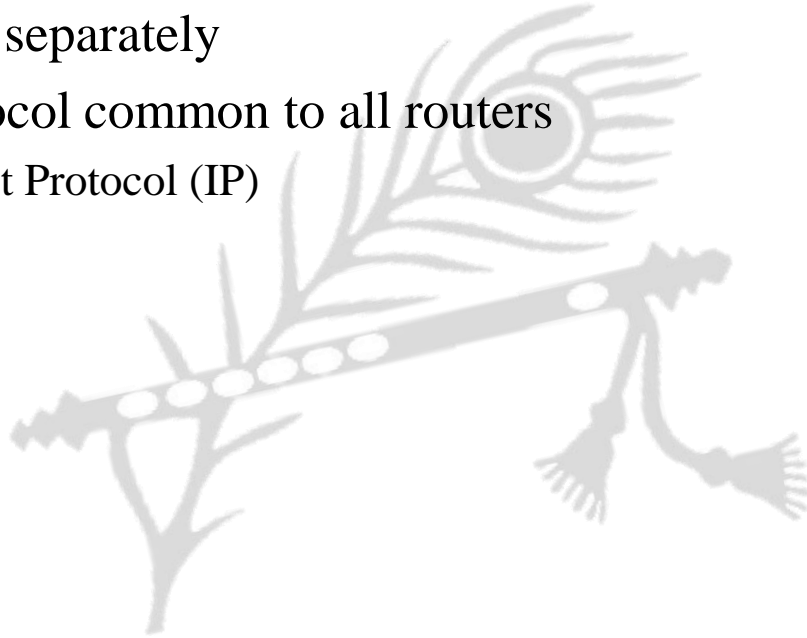


BGP = Border Gateway Protocol
 DNS = Domain Name System
 FTP = File Transfer Protocol
 HTTP = Hypertext Transfer Protocol
 ICMP = Internet Control Message Protocol
 IGMP = Internet Group Management Protocol
 IP = Internet Protocol
 MIME = Multi-Purpose Internet Mail Extension
 OSPF = Open Shortest Path First

RSVP = Resource ReSerVation Protocol
 RTP = Real-Time Transport Protocol
 SDP = Session Description Protocol
 SIP = Session Initiation Protocol
 SMTP = Simple Mail Transfer Protocol
 SNMP = Simple Network Management Protocol
 TCP = Transmission Control Protocol
 TLS = Transport Layer Security
 UDP = User Datagram Protocol

Internet Protocol (IP)

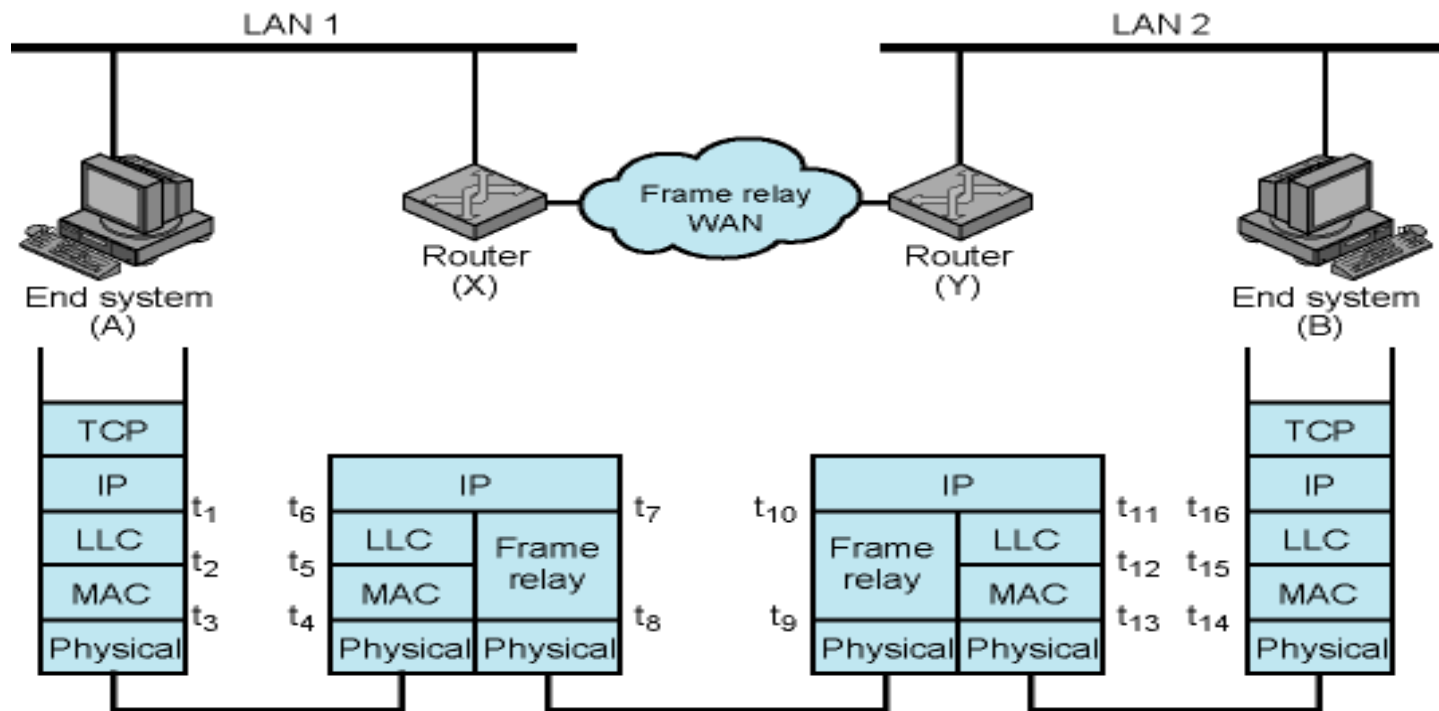
- IP provides connectionless (datagram) service
- Each packet treated separately
- Network layer protocol common to all routers
 - which is the Internet Protocol (IP)



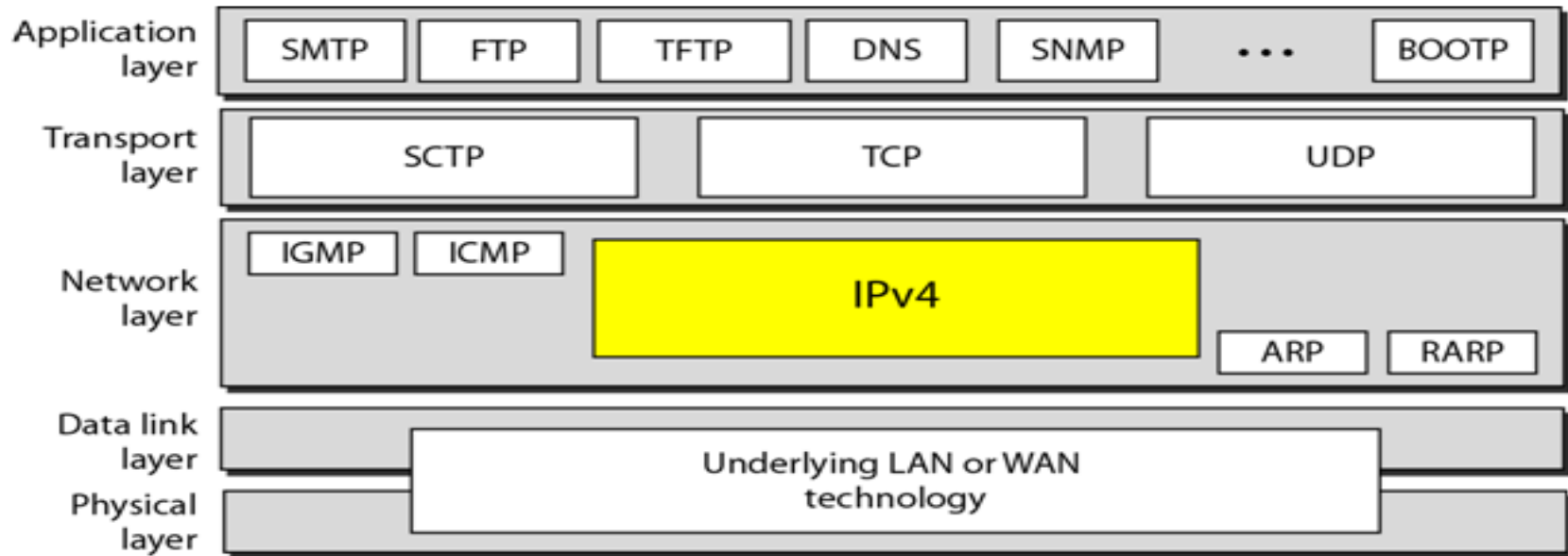
Connectionless Internetworking (General)

- Advantages
 - Flexible and robust
 - e.g. in case of congestion or node failure, packets find their way easier than connection-oriented services
 - No unnecessary overhead for connection setup
 - Can work with different network types
- Disadvantage
 - Unreliable
 - Not guaranteed delivery
 - Not guaranteed order of delivery
 - Reliability is responsibility of next layer up (e.g. TCP)

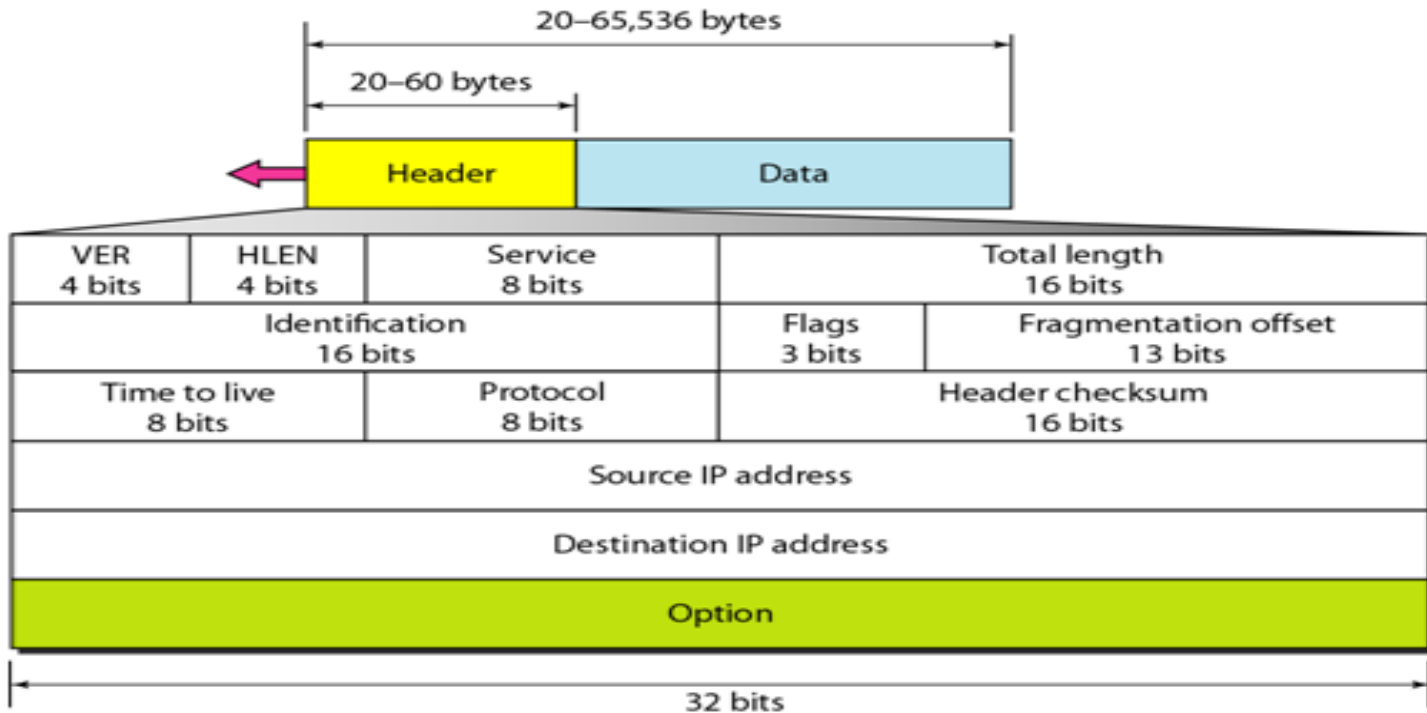
Example Internet Protocol Operation



Internet Protocol (IP) Version 4

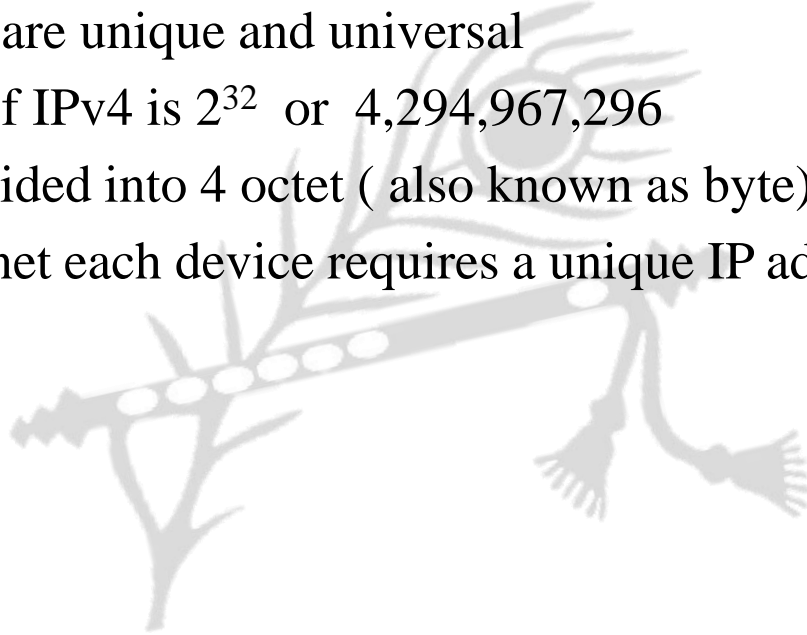


Header + Data using IPv4



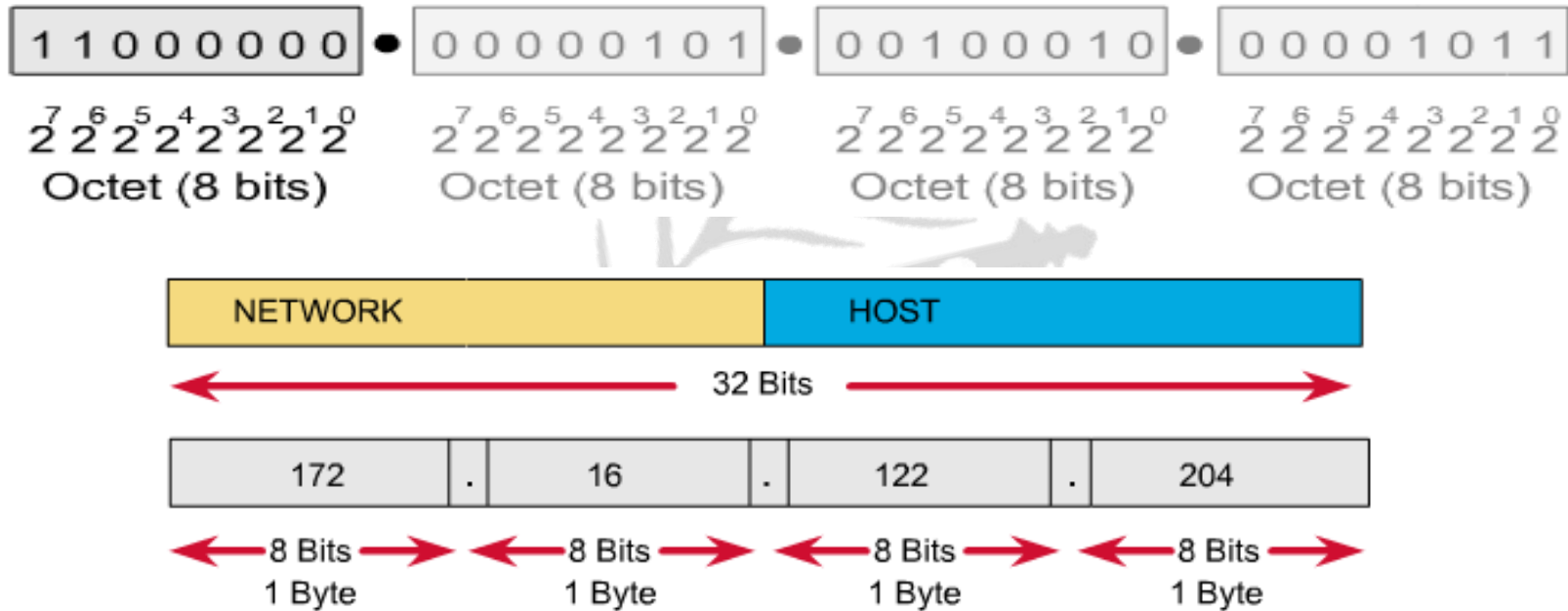
Header + Data using IPv4

- An IPv4 address is 32 bits long
- The IPv4 addresses are unique and universal
- The address space of IPv4 is 2^{32} or 4,294,967,296
- 32 bit address is divided into 4 octet (also known as byte)
- To connect on internet each device requires a unique IP address

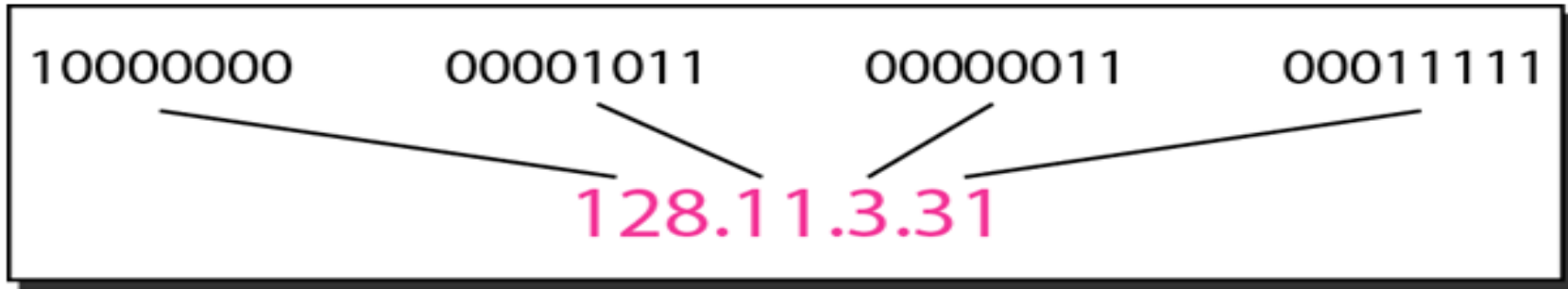


IPv4 Addressing

- IP Address as a 32-bit binary number (Four Octet)



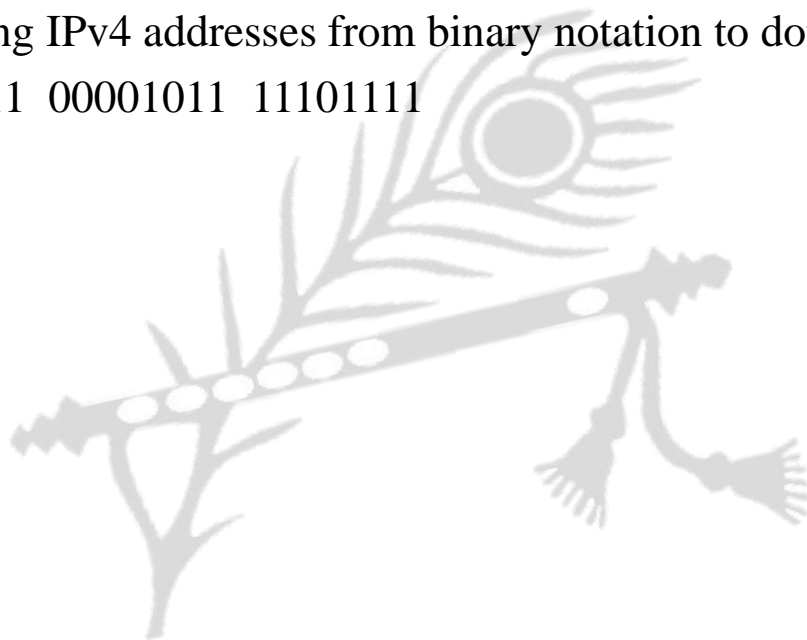
Binary to DDN conversion



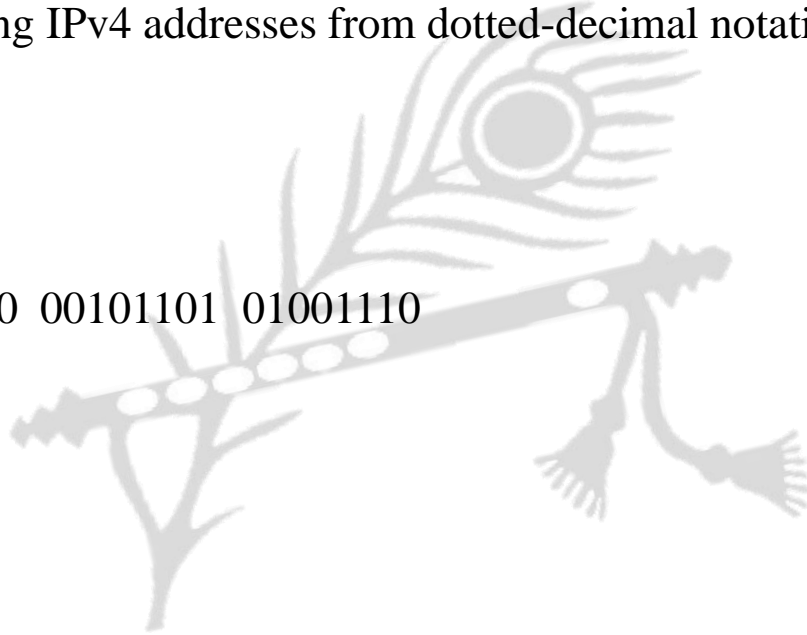
- Eg:
 - Change the following IPv4 addresses from binary notation to dotted-decimal notation
 - 10000001 00001011 00001011 11101111

Solution

- 129.11.11.239



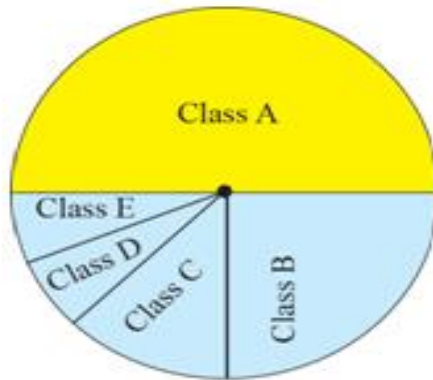
- Eg:
 - Change the following IPv4 addresses from dotted-decimal notation to binary notation
 - 111.56.45.78
- Solution
 - 01101111 00111000 00101101 01001110



- Eg:
 - Find the error, if any, in the following IPv4 addresses
 - a. 111.56.045.78
 - b. 221.34.7.8.20
 - c. 75.45.301.14
 - d. 11100010.23.14.67
- Solution
 - a. There should be no leading zeroes (045)
 - b. We may not have more than 4 bytes in an IPv4 address
 - c. Each byte should be less than or equal to 255
 - d. A mixture of binary notation and dotted-decimal notation

IPv4 Addressing Classification

- IPv4 addresses can be classified on 2 ways
 - Classful Addressing
 - Classless Addressing



Class A: $2^{31} = 2,147,483,648$ addresses, 50%

Class B: $2^{30} = 1,073,741,824$ addresses, 25%

Class C: $2^{29} = 536,870,912$ addresses, 12.5%

Class D: $2^{28} = 268,435,456$ addresses, 6.25%

Class E: $2^{28} = 268,435,456$ addresses, 6.25%

Classful addressing

- In classful addressing, the address space is divided into five classes: A, B, C, D, and E

	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

a. Binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–239			
Class E	240–255			

b. Dotted-decimal notation

Classful addressing

Class	Net ID bits	Host ID bits	Binary	DDN	No of networks	No of host/Nw	Default mask	CIDR
A (2^{31})	8	24	0	0-127	$2^7=128$	2^{24}	255.0.0.0	/8
B (2^{30})	16	16	10	128-191	2^{14}	2^{16}	255.255.0.0	/16
C (2^{29})	24	8	110	192-223	2^{21}	2^8	255.255.255.0	/24
D (2^{28})	NA	NA	1110	224-239	NA	NA	NA	NA
E (2^{28})	NA	NA	1111	240-255	NA	NA	NA	NA


CIDR = classless Interdomain Routing Notation

DDN = Dotted Decimal Notation

- Eg:
 - Find the class of each address
 - a. 00000001 00001011 00001011 11101111
 - b. 11000001 10000011 00011011 11111111
 - c. 14.23.120.8
 - d. 252.5.15.111
- Solution
 - a. The first bit is 0. This is a class A address
 - b. The first 2 bits are 1; the third bit is 0. This is a class C address
 - c. The first byte is 14; the class is A
 - d. The first byte is 252; the class is E

Classes and Blocks

- The classful addressing wastes a large part of the address space



<i>Class</i>	<i>Number of Blocks</i>	<i>Block Size</i>	<i>Application</i>
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

Structure of IPv4 Address

- Consists of Net ID and Host ID

<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

- Mask
 - 32-bit number of contiguous 1's followed by contiguous 0's
 - To help to find the net ID and the host ID

Use of IPv4 Address

- Subnetting
 - Divide a large address block into smaller sub-groups
 - Use of flexible net mask
- Supernetting
 - Exhausted class A and B address space
 - Huge demand for class B address space
 - To combine several contiguous address spaces into a larger single address space

Classless Addressing

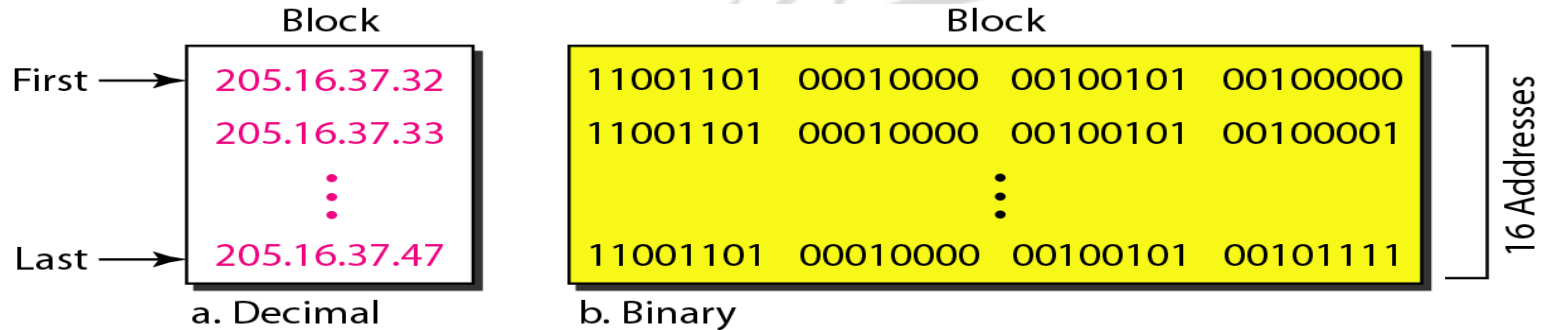
- To overcome the depletion of address space
- Restriction
 - The addresses in a block must be contiguous
 - The number of addresses in a block must be a power of 2
 - The first address must be evenly divisible by the number of address
- Mask
 - Consists of n consecutive 1's followed by zeros
 - n can be any number b/w 0 and 32

Classless Addressing

- In IPv4 addressing, a block of addresses can be defined as x.y.z.t /n, in which x.y.z.t defines one of the addresses and the /n defines the mask
- The first address in the block can be found by setting the rightmost $32 - n$ bits to 0s
- The last address in the block can be found by setting the rightmost $32 - n$ bits to 1s
- The number of addresses in the block can be found by using the formula 2^{32-n}

Eg

- Figure shows a block of addresses, in both binary and dotted-decimal notation, granted to a small business that needs 16 addresses



- We can see that the restrictions are applied to this block. The addresses are contiguous. The number of addresses is a power of 2 ($16 = 2^4$), and the first address is divisible by 16.

Eg:

- A block of addresses is granted to a small organization. We know that one of the addresses is 205.16.37.39/28. What is the first address in the block?

Solution

- The binary representation of the given address is

11001101 00010000 00100101 00100111

- If we set 32–28 rightmost bits to 0, we get

11001101 00010000 00100101 00100000

or

205.16.37.32

Eg:

- Find the last address for the block in previous example

Solution

- The binary representation of the given address is

11001101 00010000 00100101 00100111

- If we set 32 – 28 rightmost bits to 1, we get

11001101 00010000 00100101 00101111

or

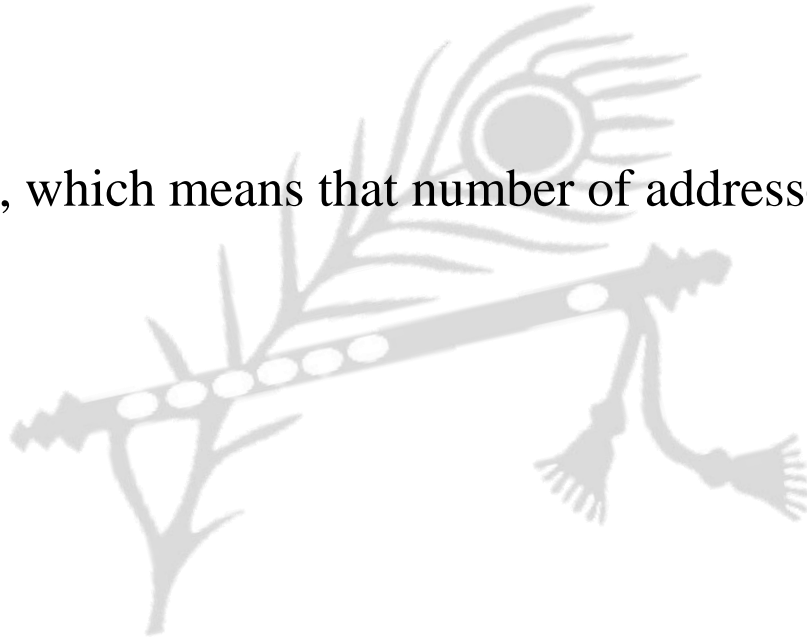
205.16.37.47

Eg:

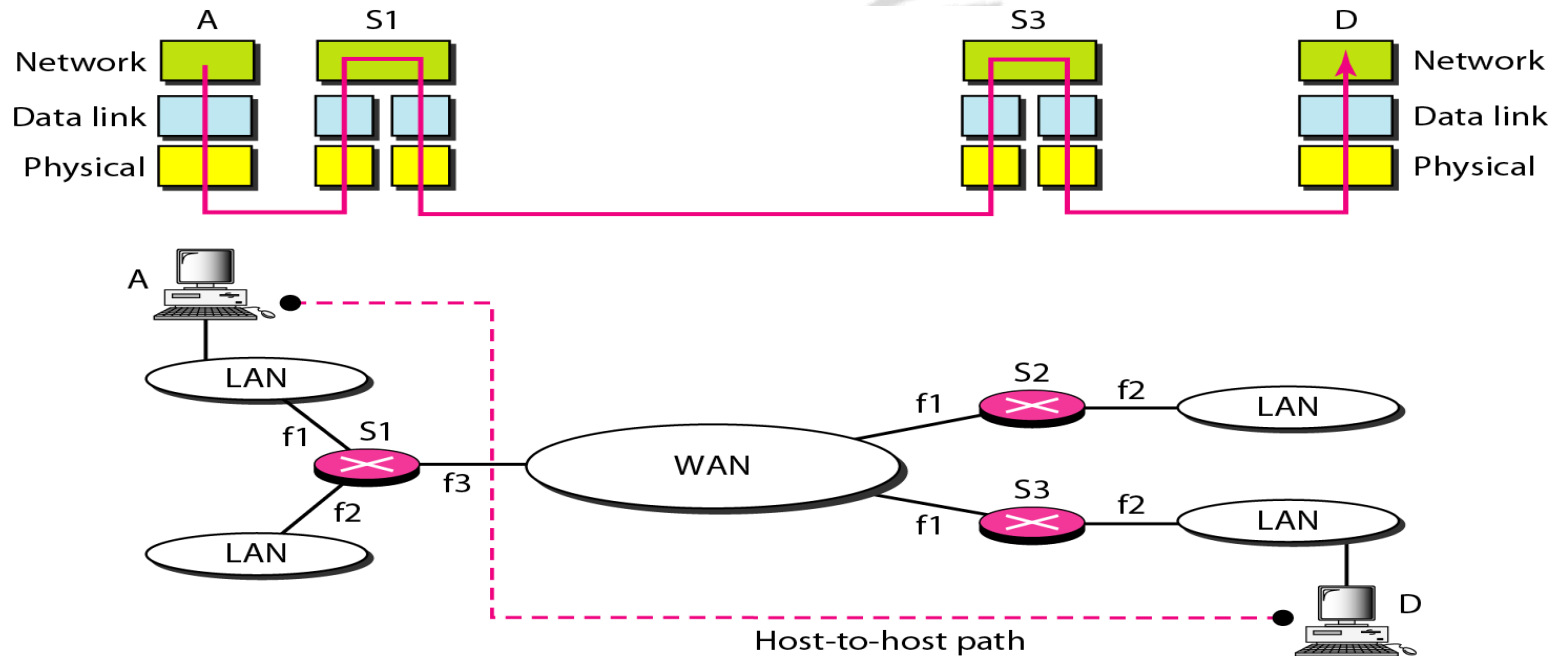
- Find the number of addresses in the previous example

Solution

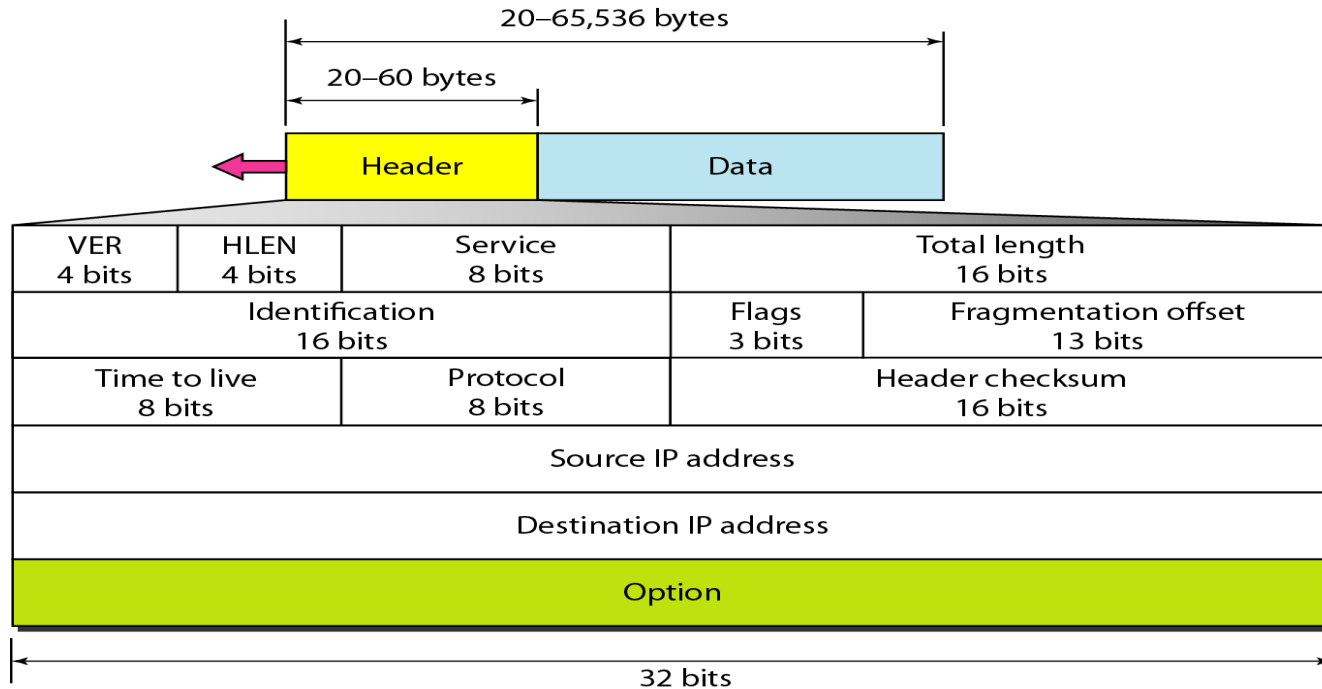
- The value of n is 28, which means that number of addresses is 2^{32-28} or 16



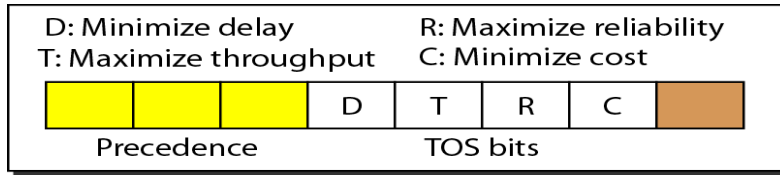
- Connecting networks together to make an internetwork or an internet



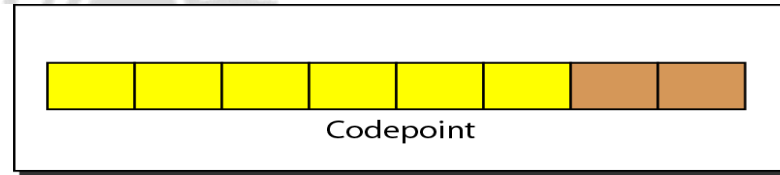
IPv4 datagram format



Service type or differentiated services



Service type



Differentiated services

Types of service

<i>TOS Bits</i>	<i>Description</i>
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

Default types of service

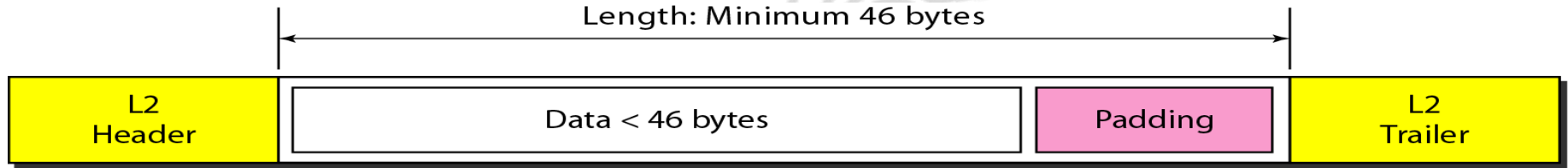
<i>Protocol</i>	<i>TOS Bits</i>	<i>Description</i>
ICMP	0000	Normal
BOOTP	0000	Normal
NNTP	0001	Minimize cost
IGP	0010	Maximize reliability
SNMP	0010	Maximize reliability
TELNET	1000	Minimize delay
FTP (data)	0100	Maximize throughput
FTP (control)	1000	Minimize delay
TFTP	1000	Minimize delay
SMTP (command)	1000	Minimize delay
SMTP (data)	0100	Maximize throughput
DNS (UDP query)	1000	Minimize delay
DNS (TCP query)	0000	Normal
DNS (zone)	0100	Maximize throughput

Protocol values

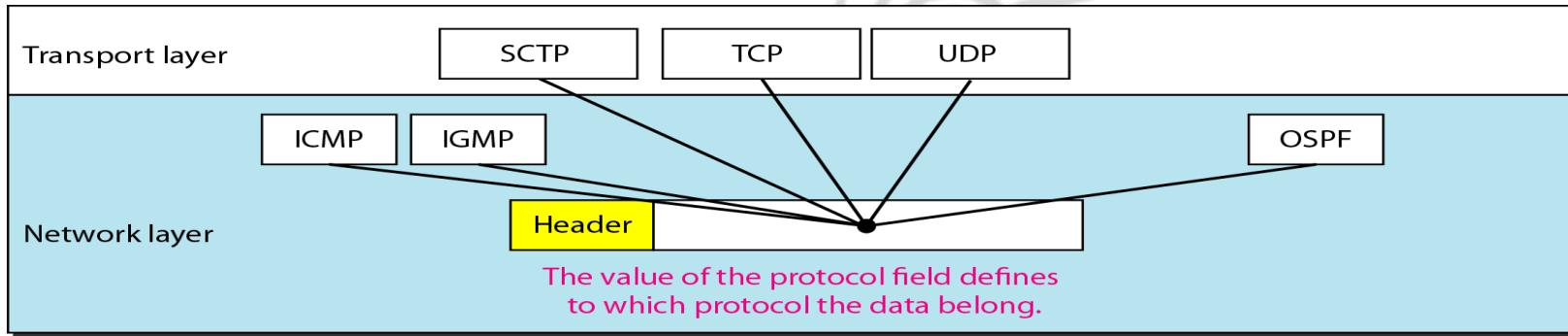
<i>Value</i>	<i>Protocol</i>
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

Encapsulation of a small datagram in an Ethernet frame

- The total length field defines the total length of the datagram including the header



Protocol field and encapsulated data



Example

- An IPv4 packet has arrived with the first 8 bits as shown:

01000010

- The receiver discards the packet. Why?

Solution

- There is an error in this packet. The 4 leftmost bits (0100) show the version, which is correct. The next 4 bits (0010) show an invalid header length ($2 \times 4 = 8$)
- The minimum number of bytes in the header must be 20. The packet has been corrupted in transmission

Example

- In an IPv4 packet, the value of HLEN is 1000 in binary. How many bytes of options are being carried by this packet?

Solution

- The HLEN value is 8, which means the total number of bytes in the header is 8×4 , or 32 bytes
- The first 20 bytes are the base header, the next 12 bytes are the options.

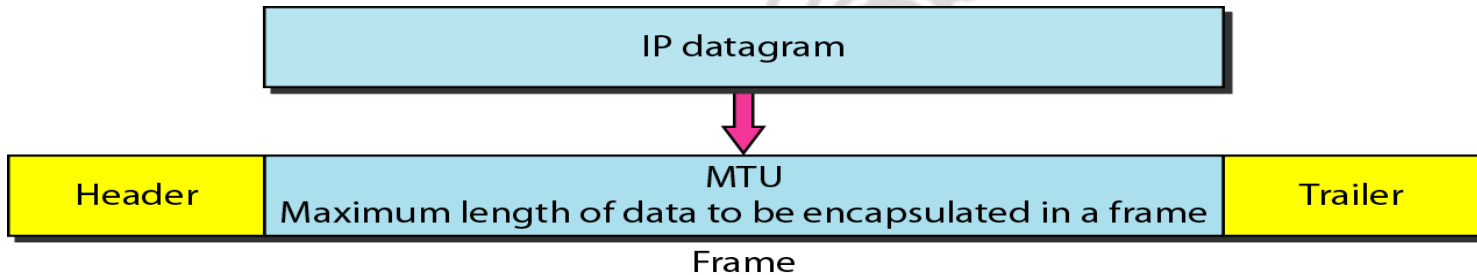
Example

- An IPv4 packet has arrived with the first few hexadecimal digits as shown.
0x45000028000100000102 ...
- How many hops can this packet travel before being dropped? The data belong to what upper-layer protocol?

Solution

- To find the time-to-live field, we skip 8 bytes. The time-to-live field is the ninth byte, which is 01
- This means the packet can travel only one hop. The protocol field is the next byte (02), which means that the upper-layer protocol is IGMP

Maximum transfer unit (MTU)



MTUs for some networks

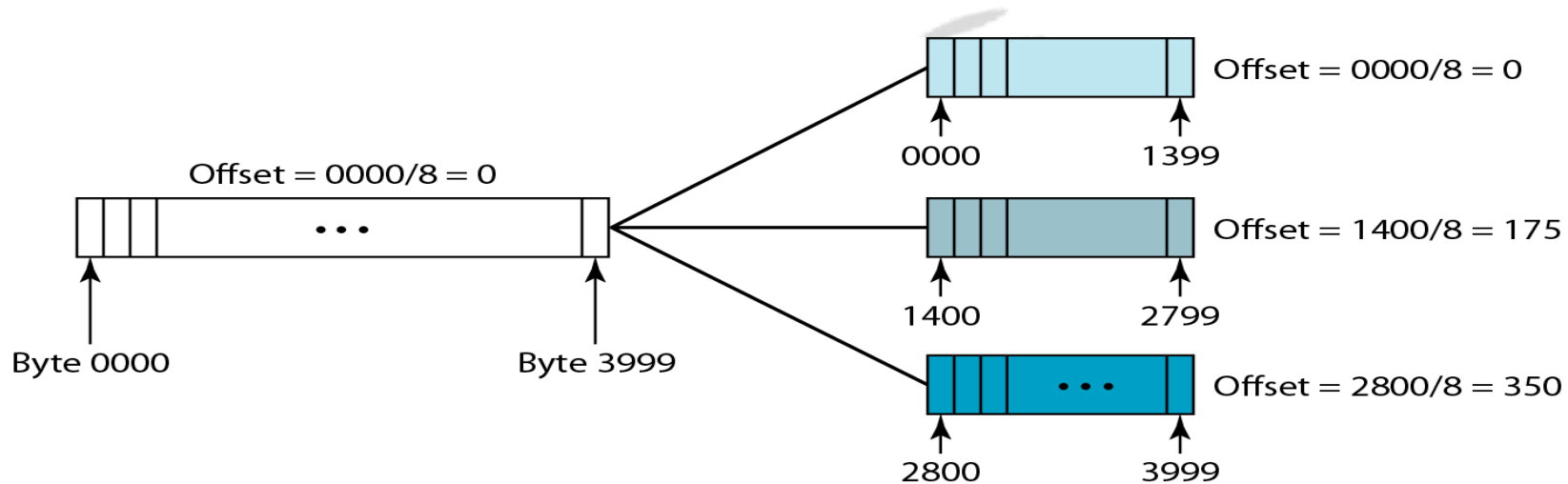
<i>Protocol</i>	<i>MTU</i>
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

Flags used in fragmentation

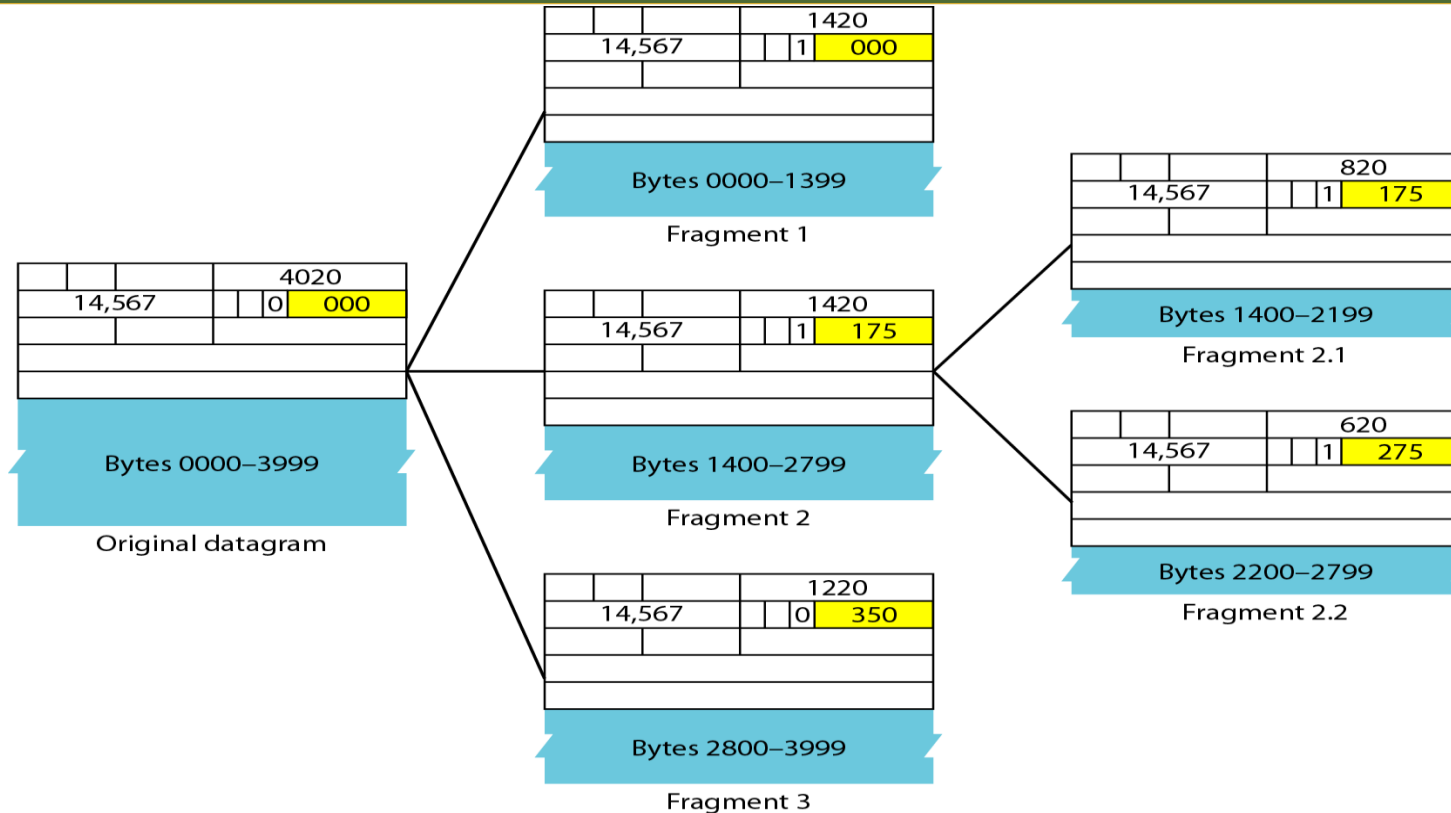


D: Do not fragment
M: More fragments

Fragmentation example



Detailed fragmentation example



Example

- A packet has arrived with an M bit value of 0. Is this the first fragment, the last fragment, or a middle fragment? Do we know if the packet was fragmented?

Solution

- If the M bit is 0, it means that there are no more fragments; the fragment is the last one
- However, we cannot say if the original packet was fragmented or not. A non-fragmented packet is considered the last fragment

Example

- A packet has arrived with an M bit value of 1. Is this the first fragment, the last fragment, or a middle fragment? Do we know if the packet was fragmented?

Solution

- If the M bit is 1, it means that there is at least one more fragment. This fragment can be the first one or a middle one, but not the last one
- We don't know if it is the first one or a middle one; we need more information (the value of the fragmentation offset)

Example

- A packet has arrived with an M bit value of 1 and a fragmentation offset value of 0. Is this the first fragment, the last fragment, or a middle fragment?

Solution

- Because the M bit is 1, it is either the first fragment or a middle one
- Because the offset value is 0, it is the first fragment

Example

- A packet has arrived in which the offset value is 100. What is the number of the first byte? Do we know the number of the last byte?

Solution

- To find the number of the first byte, we multiply the offset value by 8. This means that the first byte number is 800
- We cannot determine the number of the last byte unless we know the length

Example

- A packet has arrived in which the offset value is 100, the value of HLEN is 5, and the value of the total length field is 100. What are the numbers of the first byte and the last byte?

Solution

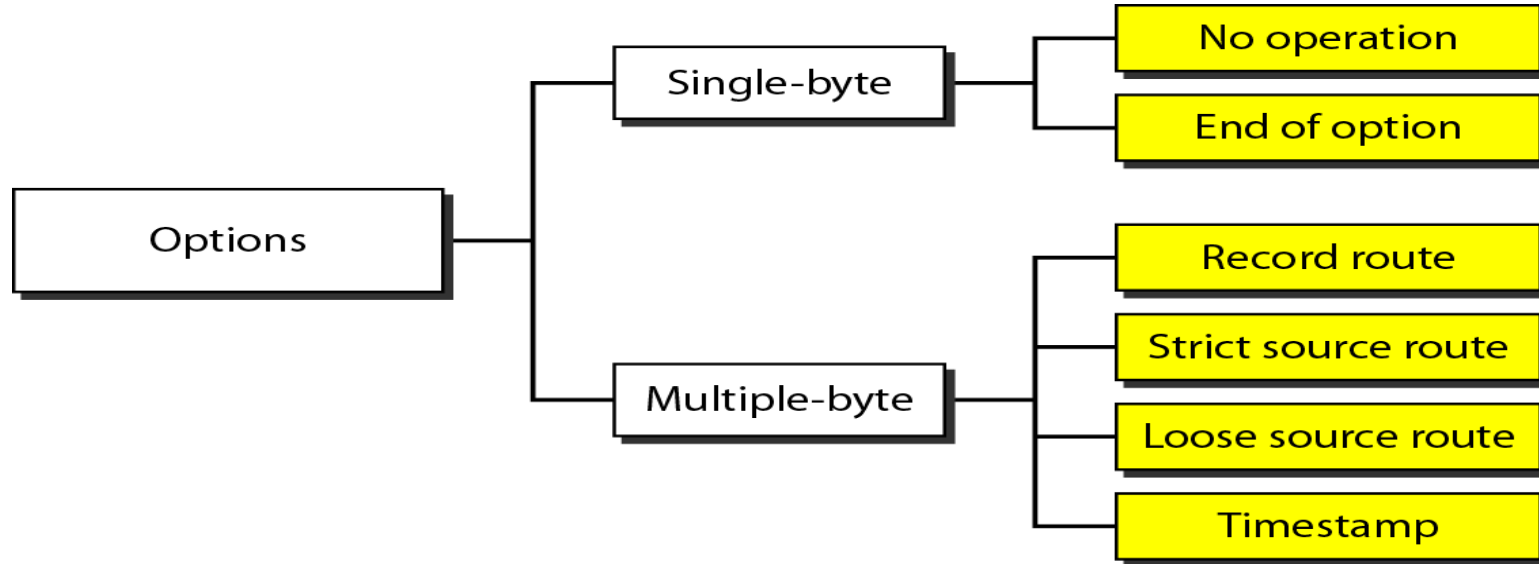
- The first byte number is $100 \times 8 = 800$
- The total length is 100 bytes, and the header length is 20 bytes (5×4), which means that there are 80 bytes in this datagram. If the first byte number is 800, the last byte number must be 879

Example

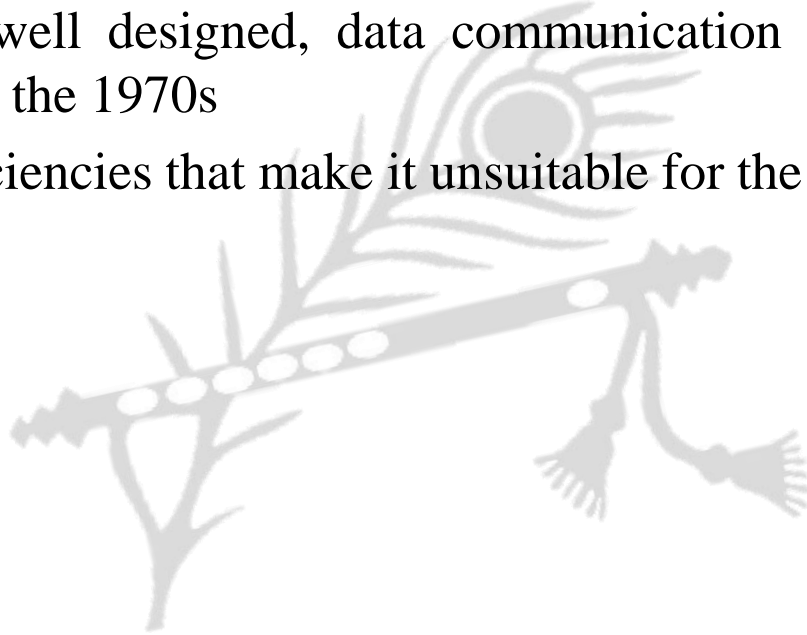
- An example of a checksum calculation for an IPv4 header without options. The header is divided into 16-bit sections. All the sections are added and the sum is complemented. The result is inserted in the checksum field

4	5	0	28		
1			0	0	
4	17	0			
10.12.14.5					
12.6.7.9					
4, 5, and 0	→	4	5	0	0
28	→	0	0	1	C
1	→	0	0	0	1
0 and 0	→	0	0	0	0
4 and 17	→	0	4	1	1
0	→	0	0	0	0
10.12	→	0	A	0	C
14.5	→	0	E	0	5
12.6	→	0	C	0	6
7.9	→	0	7	0	9
Sum	→	7	4	4	E
Checksum	→	8	B	B	1

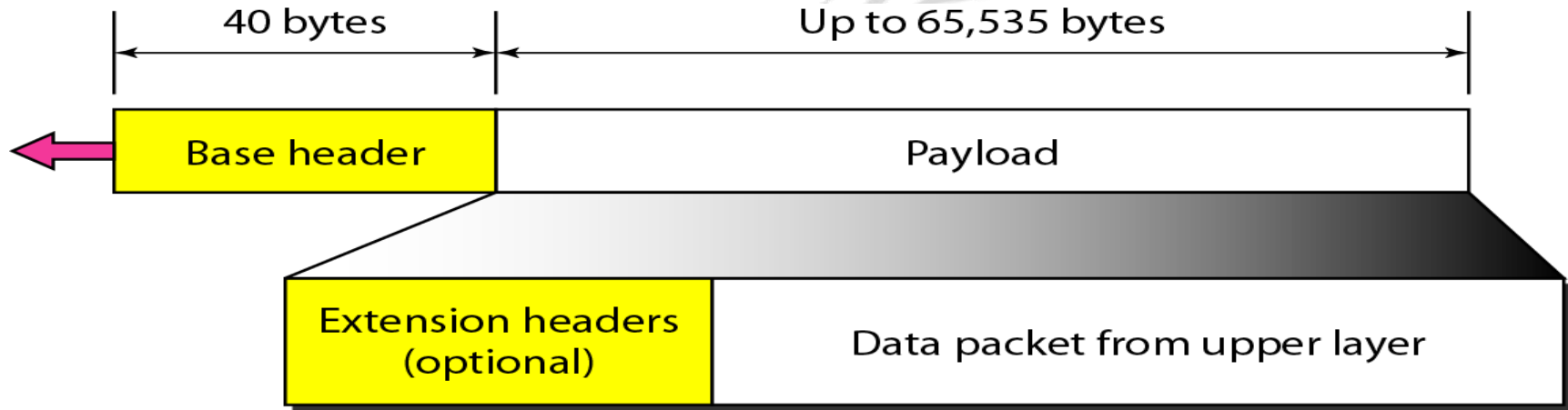
Taxonomy of options in IPv4



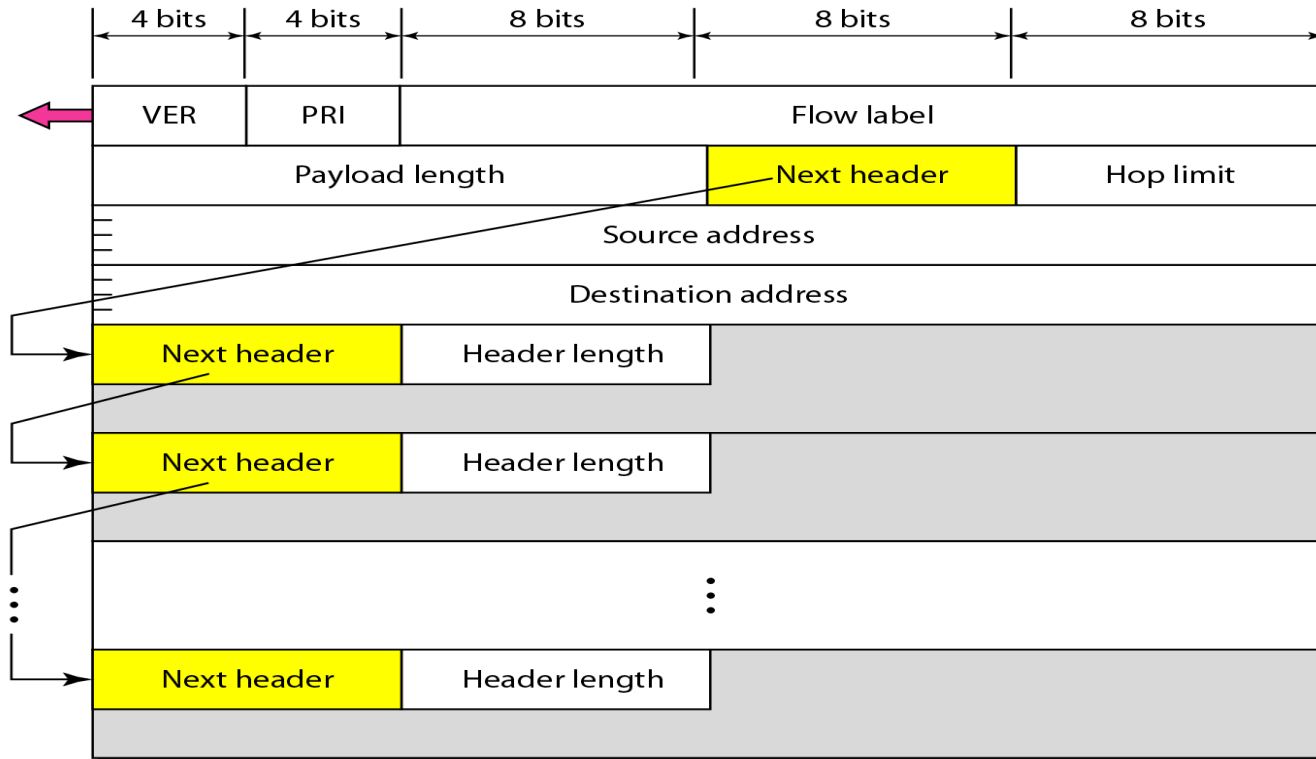
- The network layer protocol in the TCP/IP protocol suite is currently IPv4
- Although IPv4 is well designed, data communication has evolved since the inception of IPv4 in the 1970s
- IPv4 has some deficiencies that make it unsuitable for the fast-growing Internet



IPv6 datagram header and payload



Format of an IPv6 datagram



Next header codes for IPv6

<i>Code</i>	<i>Next Header</i>
0	Hop-by-hop option
2	ICMP
6	TCP
17	UDP
43	Source routing
44	Fragmentation
50	Encrypted security payload
51	Authentication
59	Null (no next header)
60	Destination option

Priorities for congestion-controlled traffic

<i>Priority</i>	<i>Meaning</i>
0	No specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

Priorities for noncongestion-controlled traffic

<i>Priority</i>	<i>Meaning</i>
8	Data with greatest redundancy
...	...
15	Data with least redundancy

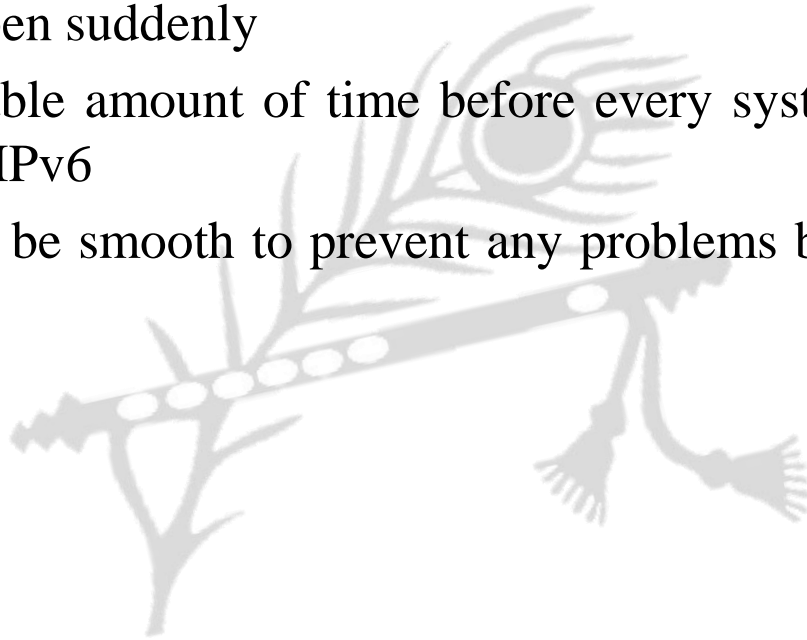
Comparison between IPv4 and IPv6 packet headers

Comparison

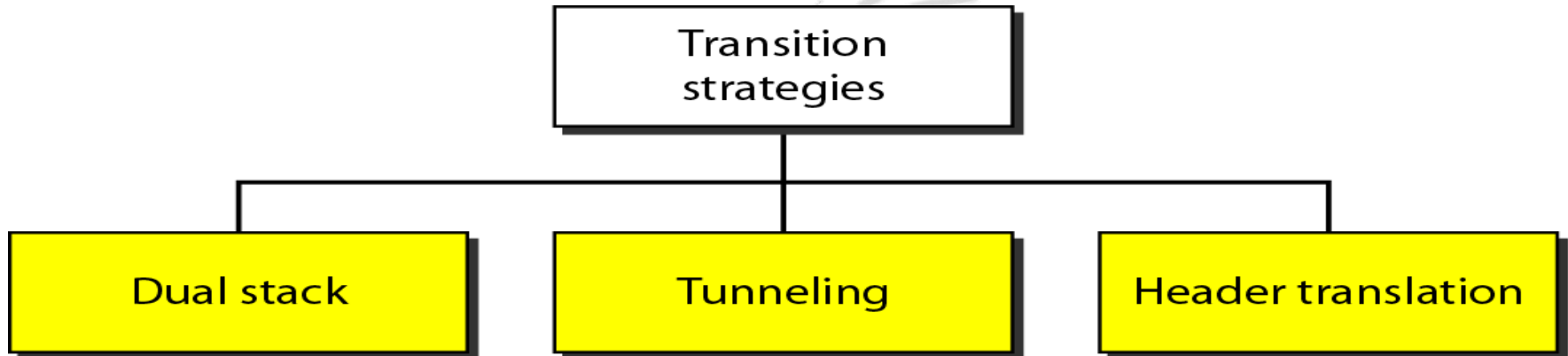
1. The header length field is eliminated in IPv6 because the length of the header is fixed in this version.
2. The service type field is eliminated in IPv6. The priority and flow label fields together take over the function of the service type field.
3. The total length field is eliminated in IPv6 and replaced by the payload length field.
4. The identification, flag, and offset fields are eliminated from the base header in IPv6. They are included in the fragmentation extension header.
5. The TTL field is called hop limit in IPv6.
6. The protocol field is replaced by the next header field.
7. The header checksum is eliminated because the checksum is provided by upper-layer protocols; it is therefore not needed at this level.
8. The option fields in IPv4 are implemented as extension headers in IPv6.

Transition from IPv4 to IPv6

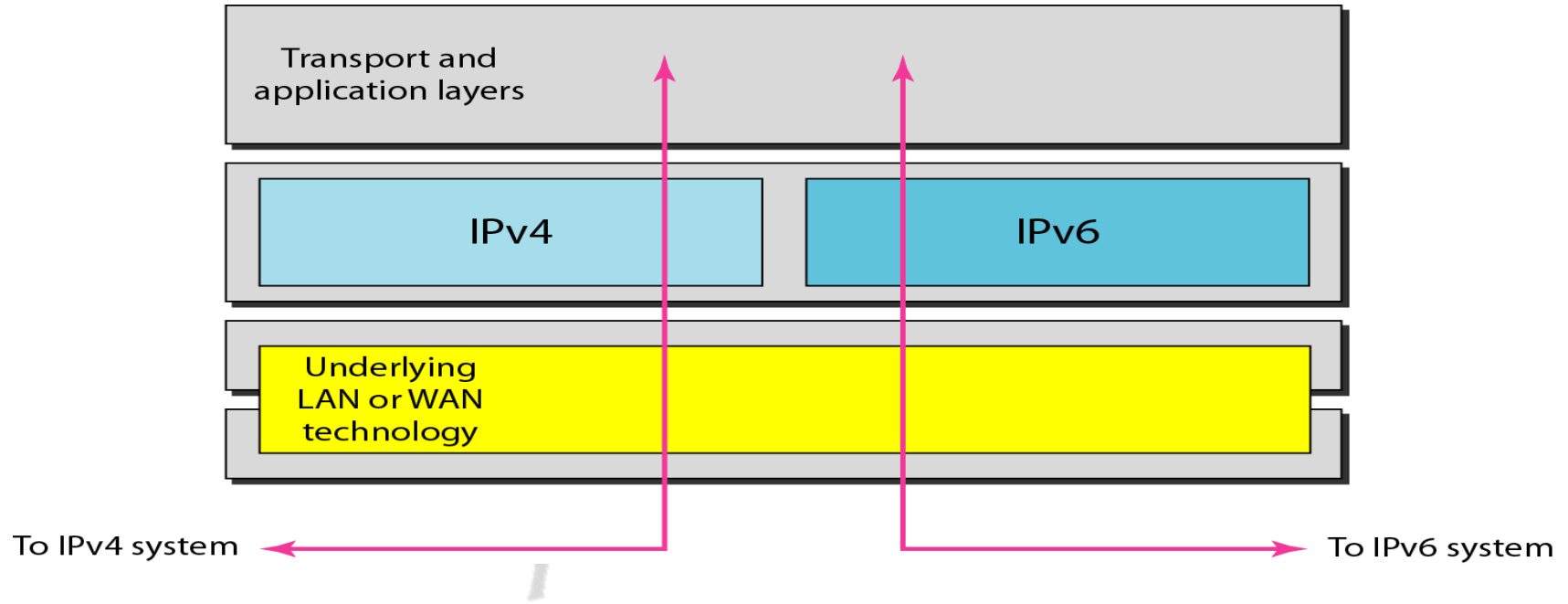
- Because of the huge number of systems on the Internet, the transition from IPv4 to IPv6 cannot happen suddenly
- It takes a considerable amount of time before every system in the Internet can move from IPv4 to IPv6
- The transition must be smooth to prevent any problems between IPv4 and IPv6 systems



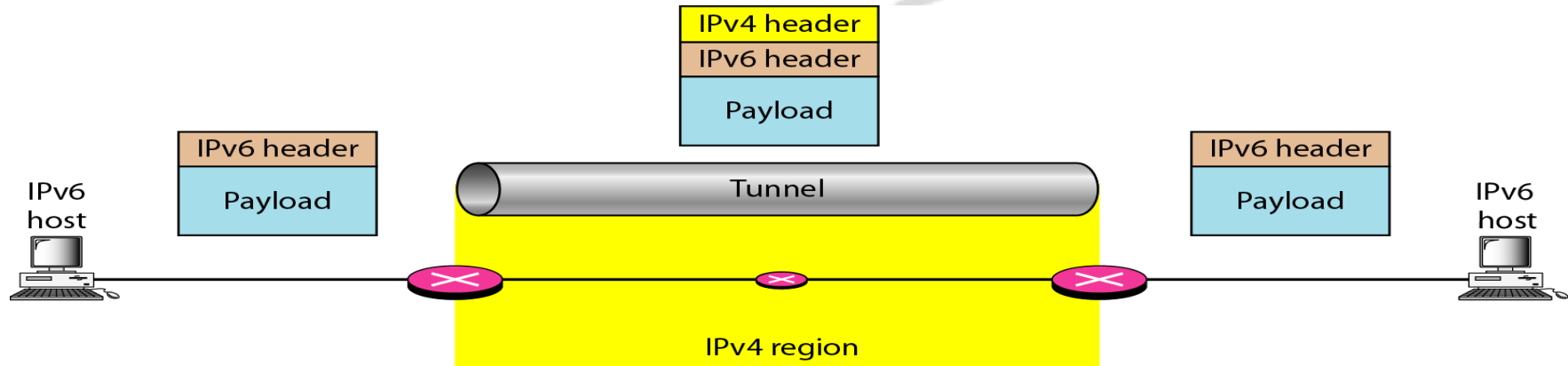
Three transition strategies



Dual stack



Tunneling strategy



Header translation strategy

