COMPUTER NETWORK (BCA301)

DEPARTMENT OF COMPUTER SCIENCE

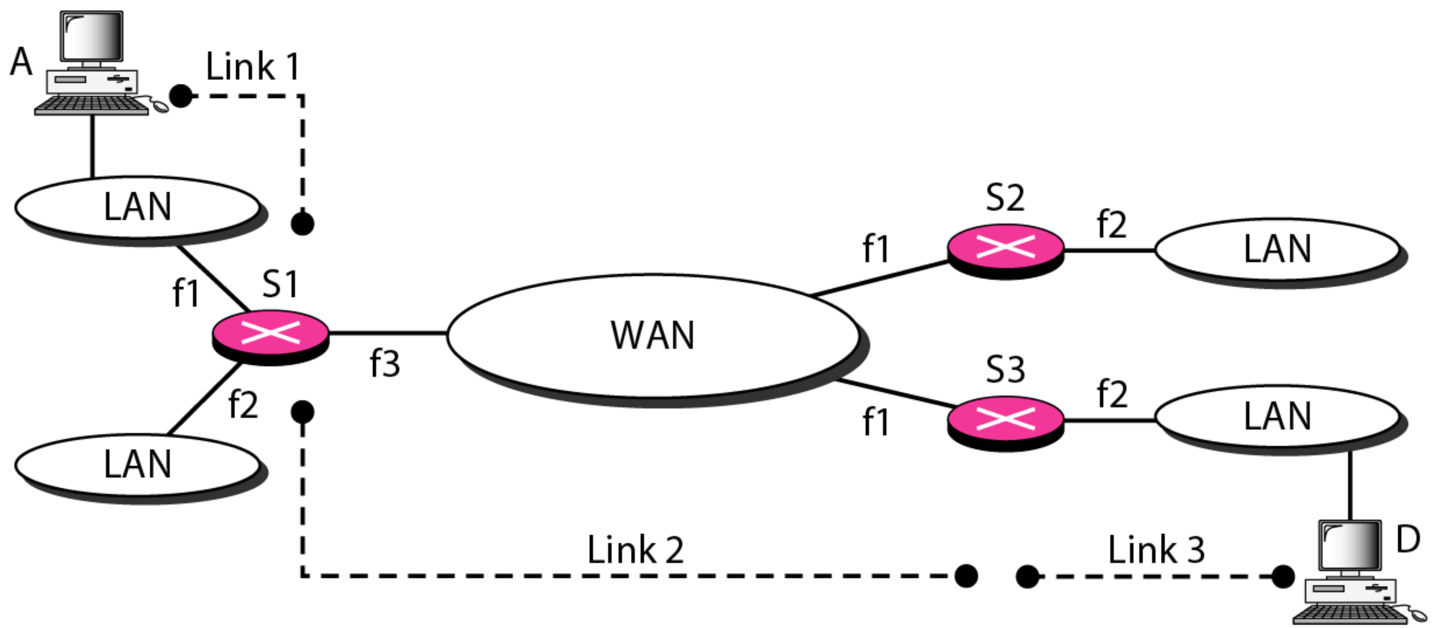
PROGRAMME: BCA

CENTRAL UNIVERSITY OF ORISSA
KORAPUT

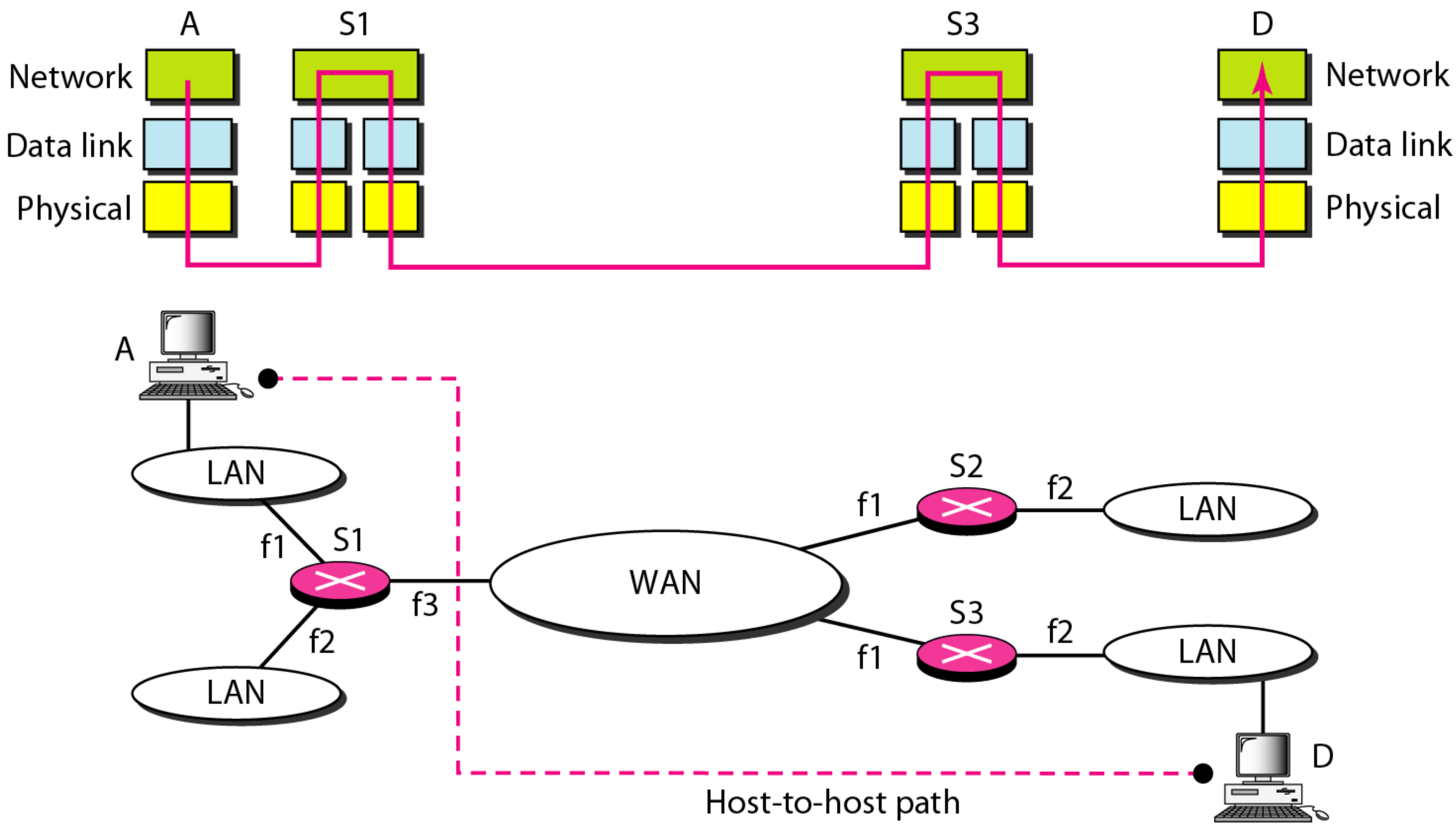
INTERNETWORKING

- The physical and data link layers of a network operate locally.
- These two layers are jointly responsible for data delivery on the network from one node to the next.
- To solve the problem of delivery through several links, the network layer (or the internetwork layer, as it is sometimes called) was designed.
- The network layer is responsible for host-to-host delivery and for routing the packets through the routers or switches.
-

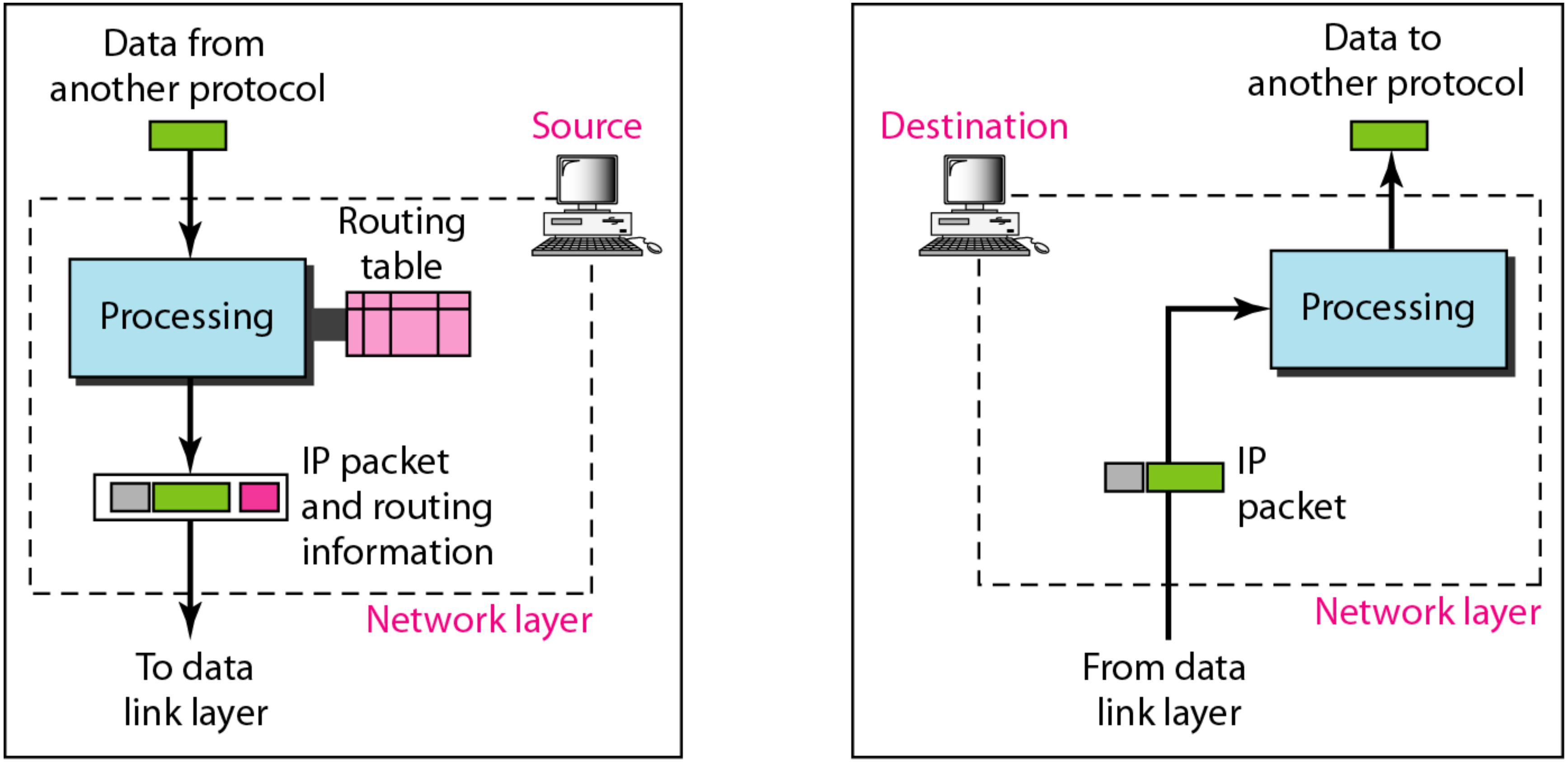
Links between Two Hosts



Network layer in an Internetwork



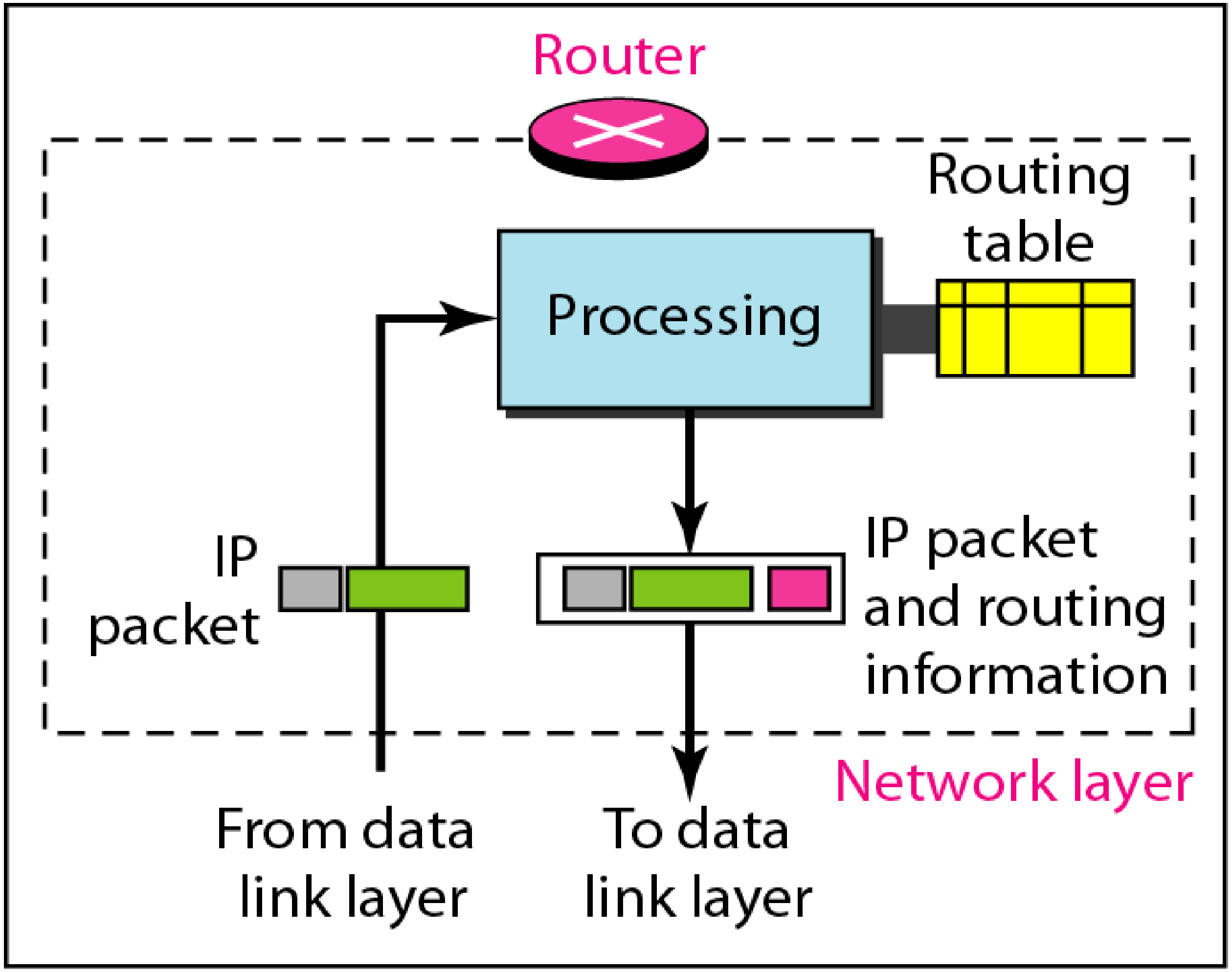
Network layer at the source, router, and destination



a. Network layer at source

b. Network layer at destination

Network layer at the source, router, and destination (continued)



c. Network layer at a router

Internet as a Datagram Network

- Switching can be divided into three broad categories: circuit switching, packet switching, and message switching.
- Packet switching uses either the virtual circuit approach or the datagram approach.
- The Internet has chosen the datagram approach to switching in the network layer.
-

Internet as a Connectionless Network

- Delivery of a packet can be accomplished by using either a connection-oriented or a connectionless network service.
- The Internet is made of so many heterogeneous networks that it is almost impossible to create a connection from the source to the destination without knowing the nature of the networks in advance.

Connection-oriented Vs Connectionless Network

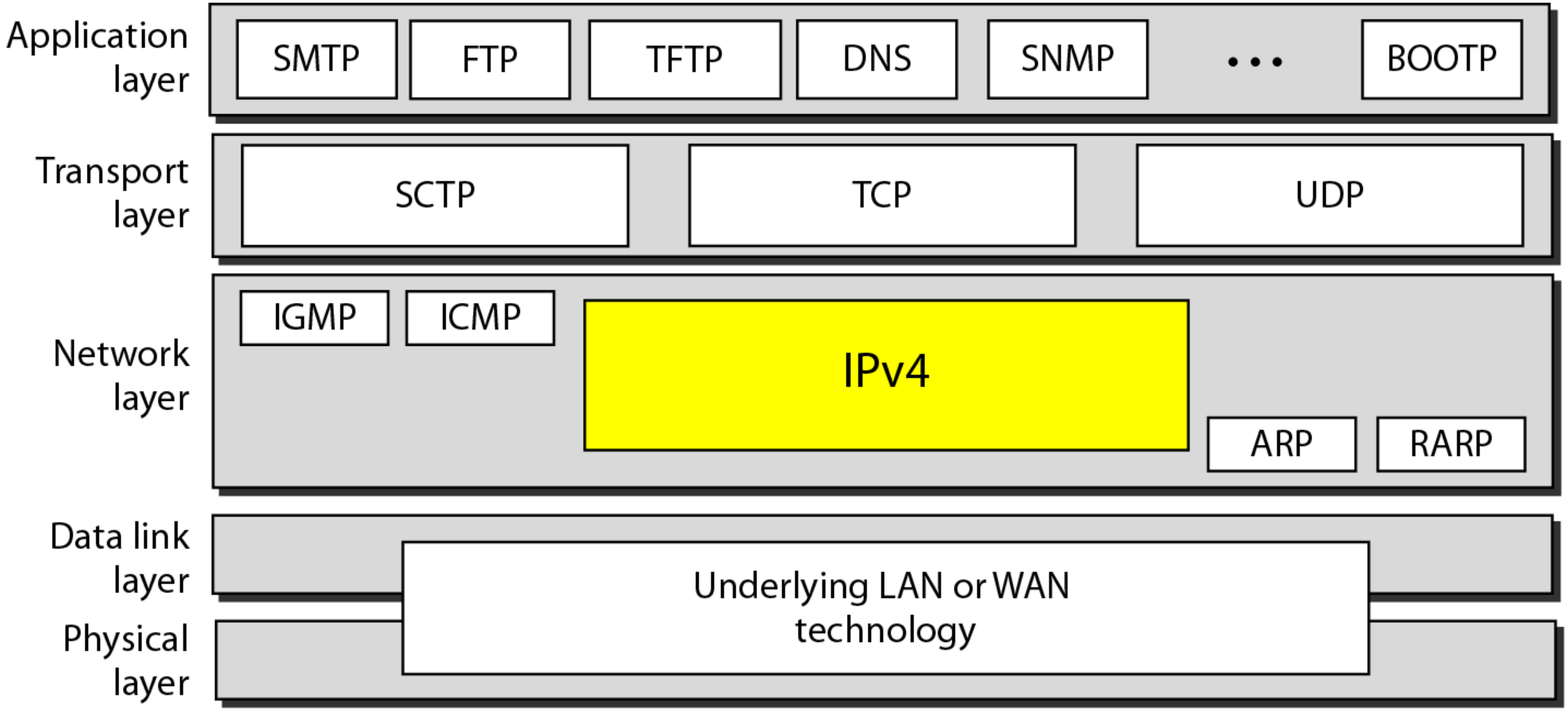
- In a connection-oriented service, the source first makes a connection with the destination before sending a packet.
- When the connection is established, a sequence of packets from the same source to the same destination can be sent one after another.
- In this case, there is a relationship between packets.
- They are sent on the same path in sequential order.
- A packet is logically connected to the packet traveling before it and to the packet traveling after it.
- When all packets of a message have been delivered, the connection is terminated.
- the decision about the route of a sequence of packets with the same source and destination addresses can be made only once, when the connection is established.
- Switches do not recalculate the route for each individual packet

- In conneetionless service, the network layer protocol treats each packet independently, with each packet having no relationship to any other packet.
- The packets in a message mayor may not travel the same path to their destination.
- This type of service is used in the datagram approach to packet switching. The Internet has chosen this type of service at the network layer.

IPv4

- The Internet Protocol version 4 (IPv4) is the delivery mechanism used by the TCP/IP protocols.
- IPv4 is an unreliable and connectionless datagram protocol-a best-effort delivery service.
- The term *best-effort* means that IPv4 provides no error control or flow control (except for error detection on the header).
- If reliability is important, IPv4 must be paired with a reliable protocol such as TCP.
- IPv4 relies on a higher-level protocol to take care of all these problems.
- IPv4 is also a connectionless protocol for a packet-switching network that uses the datagram approach.
- This means that each datagram is handled independently, and each datagram can follow a different route to the destination.
- This implies that datagrams sent by the same source to the same destination could arrive out of order. Also, some could be lost or corrupted during transmission.

Position of IPv4 in TCP/IP protocol suite



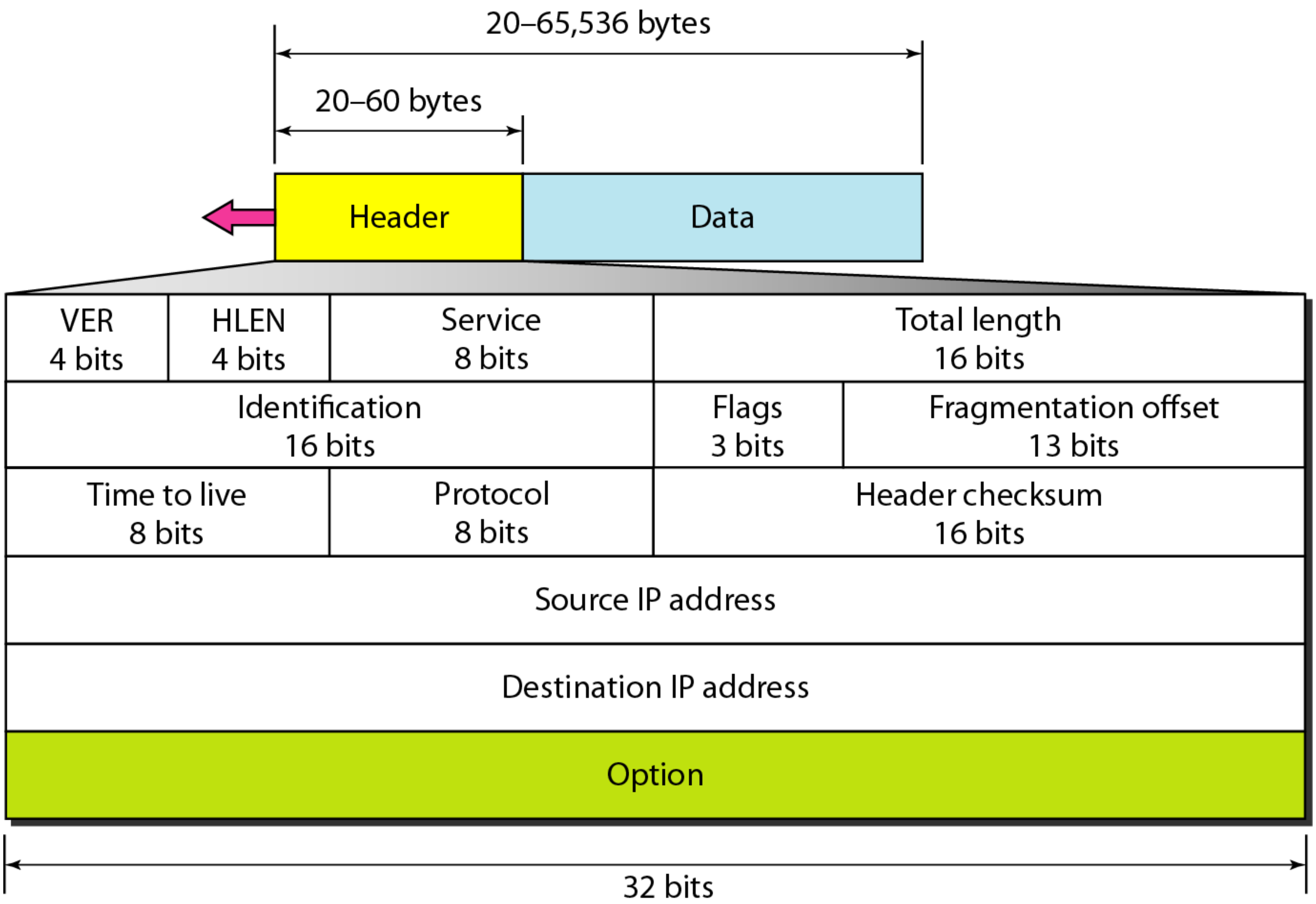
Datagram

- A datagram is a variable-length packet consisting of two parts: header and data.
- The header is 20 to 60 bytes in length and contains information essential to routing and delivery.
- **Version (VER):**This 4-bit field defines the version of the IPv4 protocol.
- **Header length (HLEN):**This 4-bit field defines the total length of the datagram header in 4-byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes).
- **Services:** IETF has changed the interpretation and name of this 8-bit field. This field, previously called service type, is now called differentiated services.
- **Total length:** This is a In-bit field that defines the total length (header plus data) of the IPv4 datagram in bytes. To find the length of the data coming from the upper layer, subtract the header length from the total length. The header length can be found by multiplying the value in the HLEN field by 4.

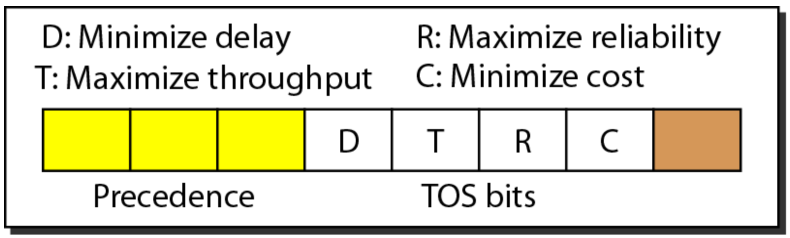
IPv4 Datagram Format

- **Identification:**This field is used in fragmentation.
- **Flags:** This field is used in fragmentation.
- **Fragmentation offset:** This field is used in fragmentation.
- **Time to live:** A datagram has a limited lifetime in its travel through an internet. This field was originally designed to hold a timestamp, which was decremented by each visited router. The datagram was discarded when the value became zero.
- **Protocol:** This 8-bit field defines the higher-level protocol that uses the services of the IPv4 layer. An IPv4 datagram can encapsulate data from several higher-level protocols such as TCP, UDP, ICMP, and IGMP. This field specifies the final destination protocol to which the IPv4 datagram is delivered.
- **Checksum:**
- **Source address:** This 32-bit field defines the IPv4 address of the source. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.
- **Destination address:** This 32-bit field defines the IPv4 address of the destination. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.

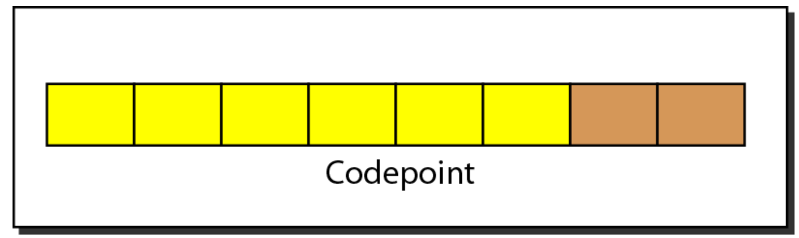
IPv4 Datagram Format



Service type or differentiated services



Service type



Differentiated services

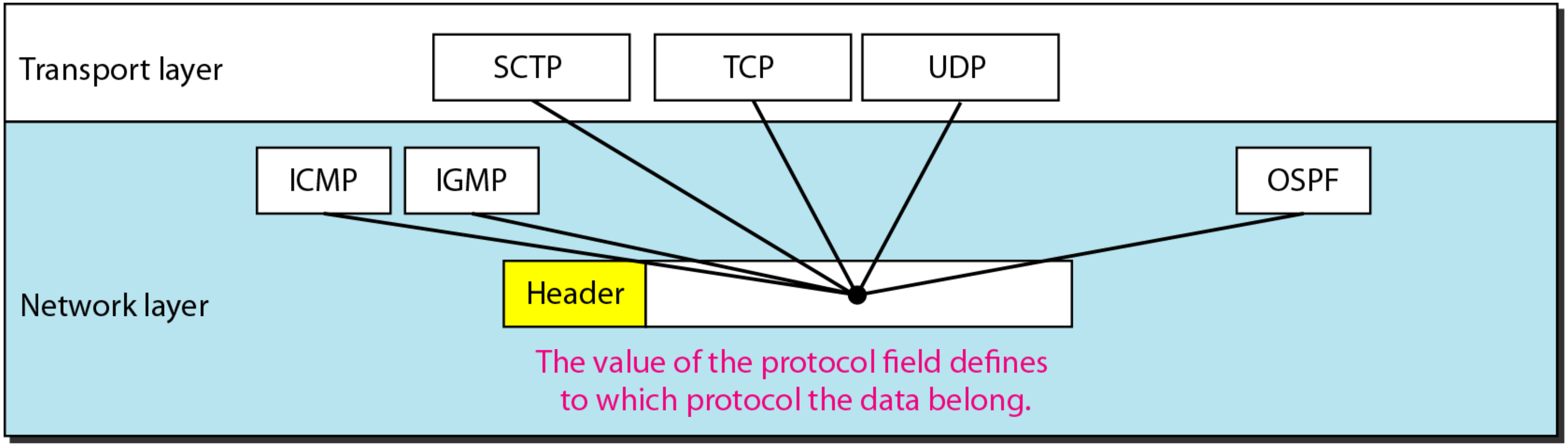
Types of service

TOS Bits	*Description*
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

Default types of service

Protocol	*TOS Bits*	*Description*
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 field and encapsulated data



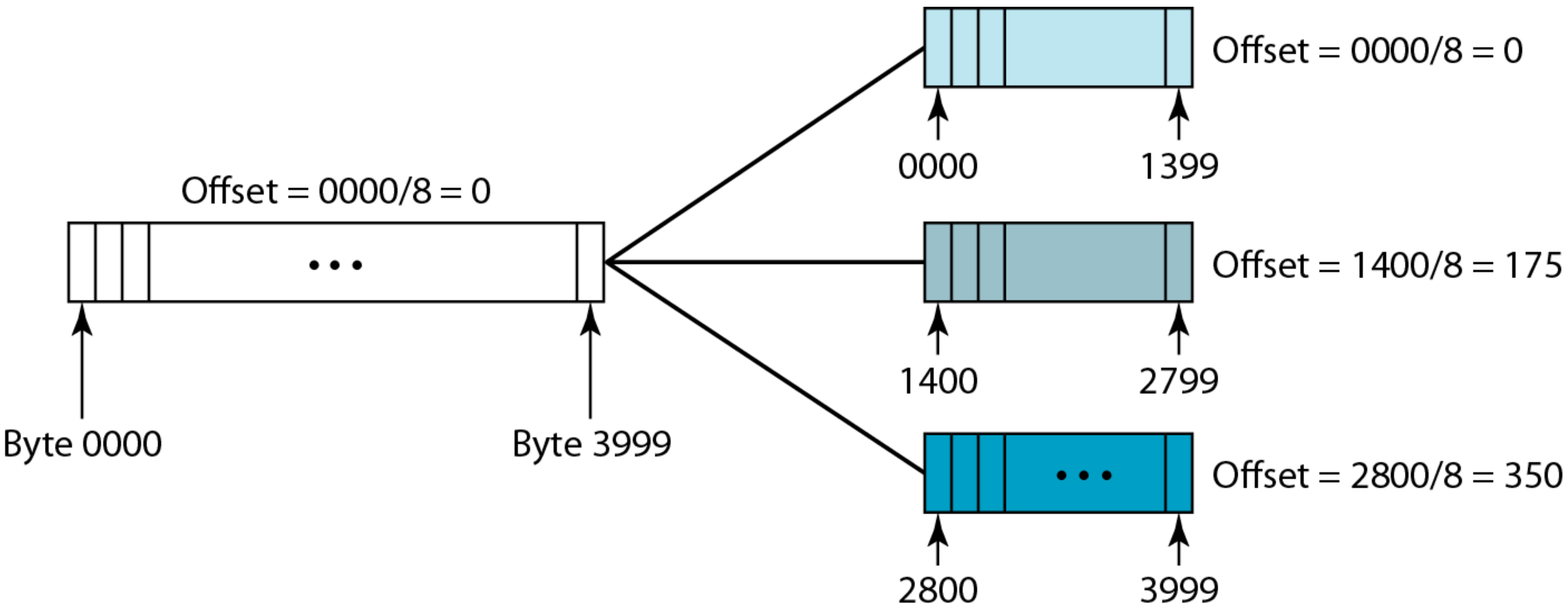
Values for codepoints

Value	*Protocol*
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

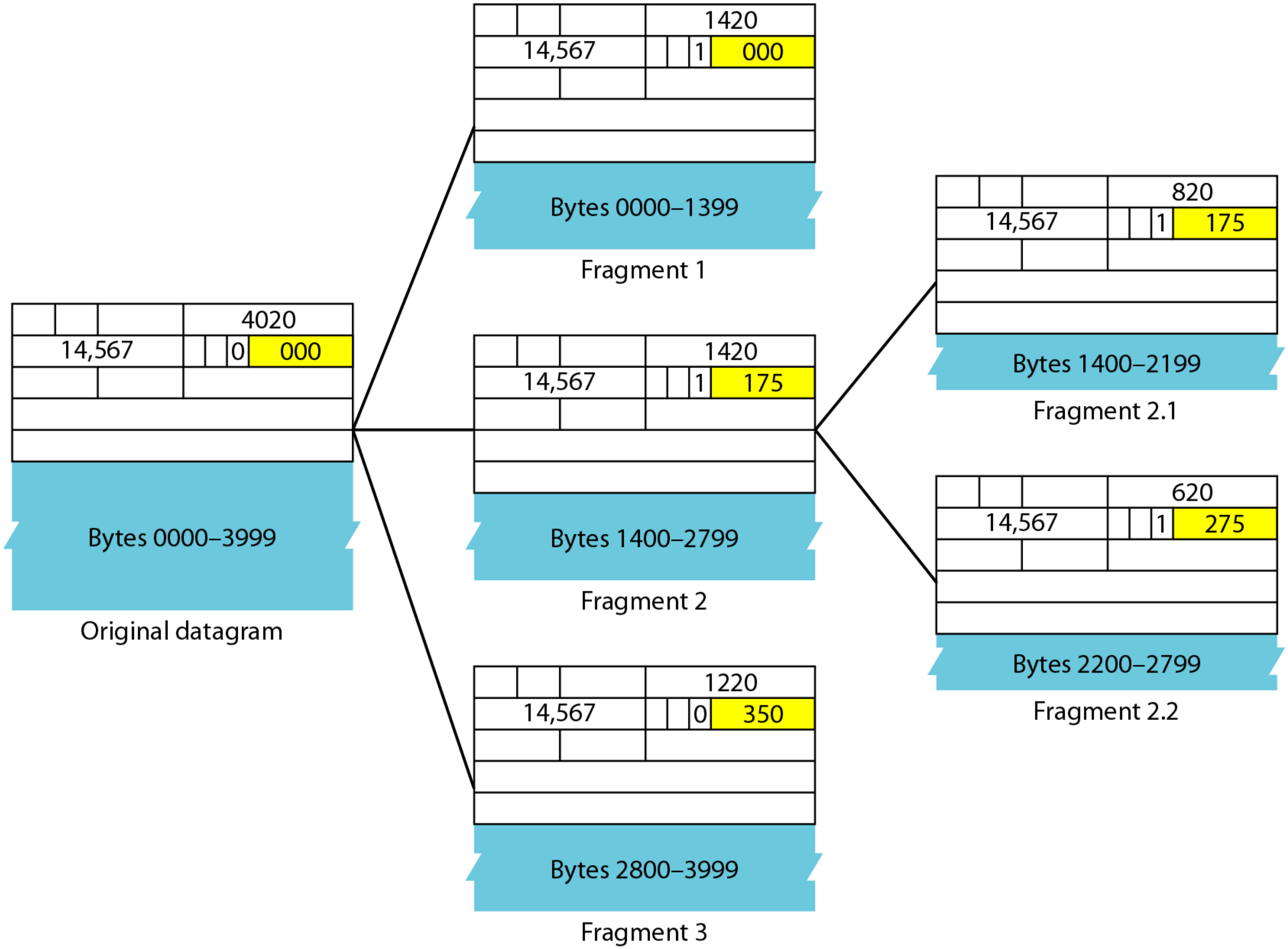
Fragmentation

- A datagram can travel through different networks.
- Each router decapsulates the IPv4 datagram from the frame it receives, processes it, and then encapsulates it in another frame.
- The format and size of the received frame depend on the protocol used by the physical network through which the frame has just traveled.
- The format and size of the sent frame depend on the protocol used by the physical network through which the frame is going to travel.
-

Fragmentation example



Detailed fragmentation example



Maximum Transfer Unit (MTU)

- Each data link layer protocol has its own frame format in most protocols.
- When a datagram is encapsulated in a frame, the total size of the datagram must be less than this maximum size, which is defined by the restrictions imposed by the hardware and software used in the network.
- The source usually does not fragment the IPv4 packet.
- The transport layer will instead segment the data into a size that can be accommodated by IPv4 and the data link layer in use.
- When a datagram is fragmented, each fragment has its own header with most of the fields repeated, but with some changed.
- A datagram can be fragmented several times before it reaches the final destination.

- In IPv4, a datagram can be fragmented by the source host or any router in the path although there is a tendency to limit fragmentation only at the source.
- The reassembly of the datagram, however, is done only by the destination host because each fragment becomes an independent datagram.
- Whereas the fragmented datagram can travel through different routes, and we can never control or guarantee which route a fragmented datagram may take, all the fragments belonging to the same datagram should finally arrive at the destination host.
- The host or router that fragments a datagram must change the values of three fields: flags, fragmentation offset, and total length. The rest of the fields must be copied.

IPv6

- IPv4 has some deficiencies that make it unsuitable for the fast-growing Internet.
- ➢ Despite all short-term solutions, such as subnetting, classless addressing, and NAT, address depletion is still a long-term problem in the Internet.
- ➢ The Internet must accommodate real-time audio and video transmission.
- ➢ No encryption or authentication is provided by IPv4.

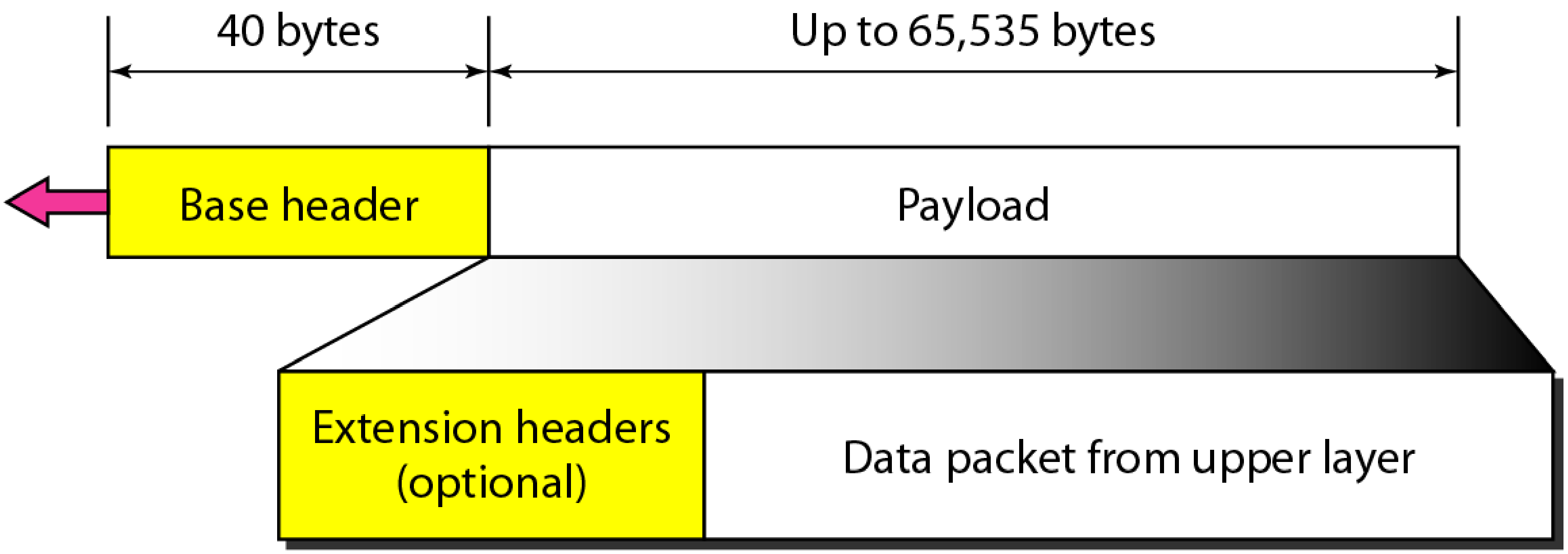
To overcome these deficiencies, IPv6 (Internetworking Protocol, version 6), also known as IPng (Internetworking Protocol, next generation), was proposed and is now a standard.

Advantages

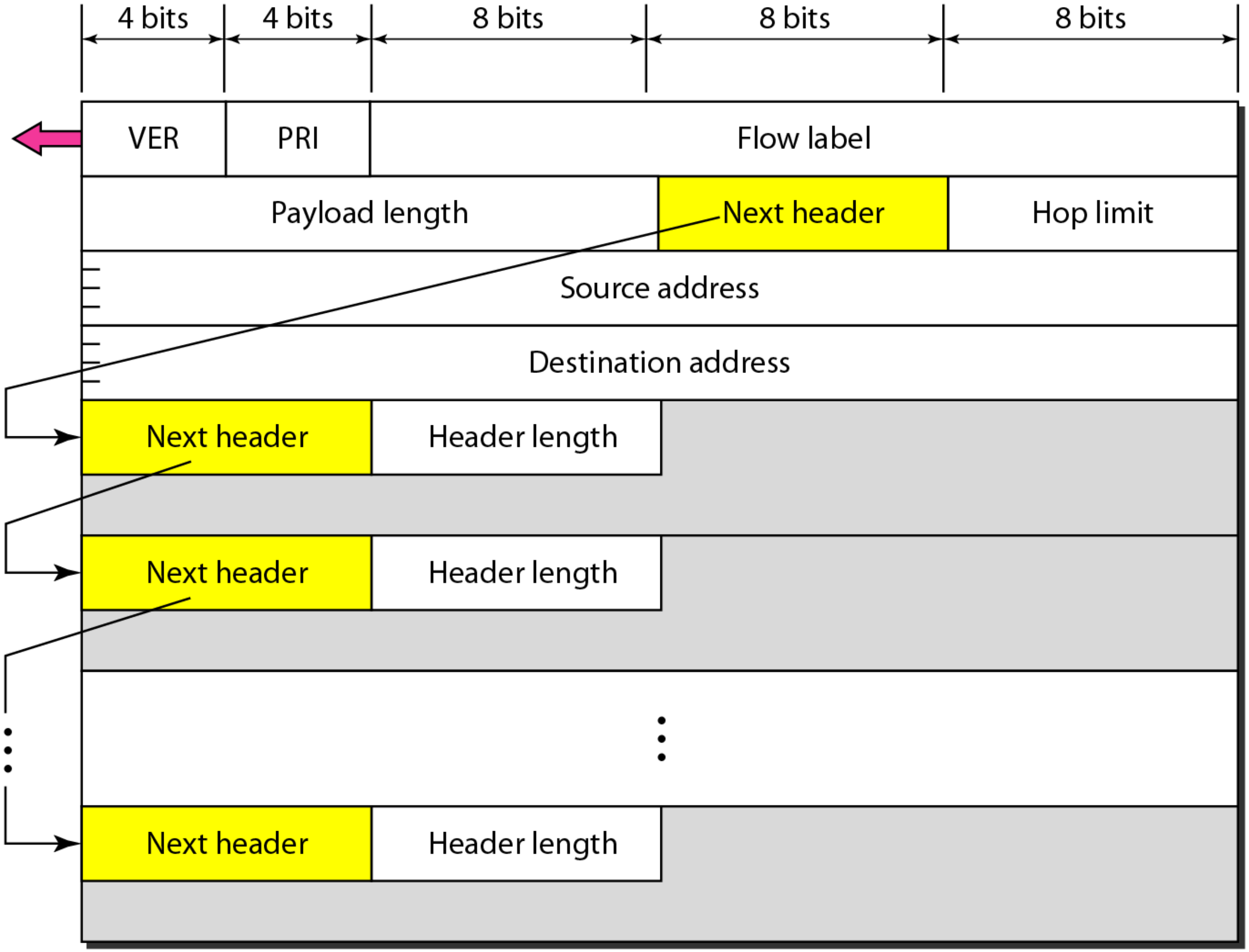
- Larger address space
- Better header format
- New options: It has new options to allow for additional functionalities
- Allowance for extension:IPv6 is designed to allow the extension of the protocol if required by new technologies or applications
- Support for resource allocation: It can be used to support traffic such as real-time audio and video
- Support for more security. The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet

IPv6 datagram header and payload

- Each packet is composed of a mandatory base header followed by the payload.
- The payload consists of two parts: optional extension headers and data from an upper layer.



Format of an IPv6 datagram



REFRENCES

- “ DATA COMMUNICATIONS AND NETWORKING ”, Behrouz A. Forouzan And Sophia Chung Fegan , Fourth Edition , McGraw-Hill