Data Communications and Networking Fourth Edition

Forouzan

Chapter 20

Network Layer: Internet Protocol

20-1 INTERNETWORKING

In this section, we discuss internetworking, connecting networks together to make an internetwork or an internet.

Topics discussed in this section:

Need for Network Layer
Internet as a Datagram Network
Internet as a Connectionless Network

Figure 20.1 *Links between two hosts*

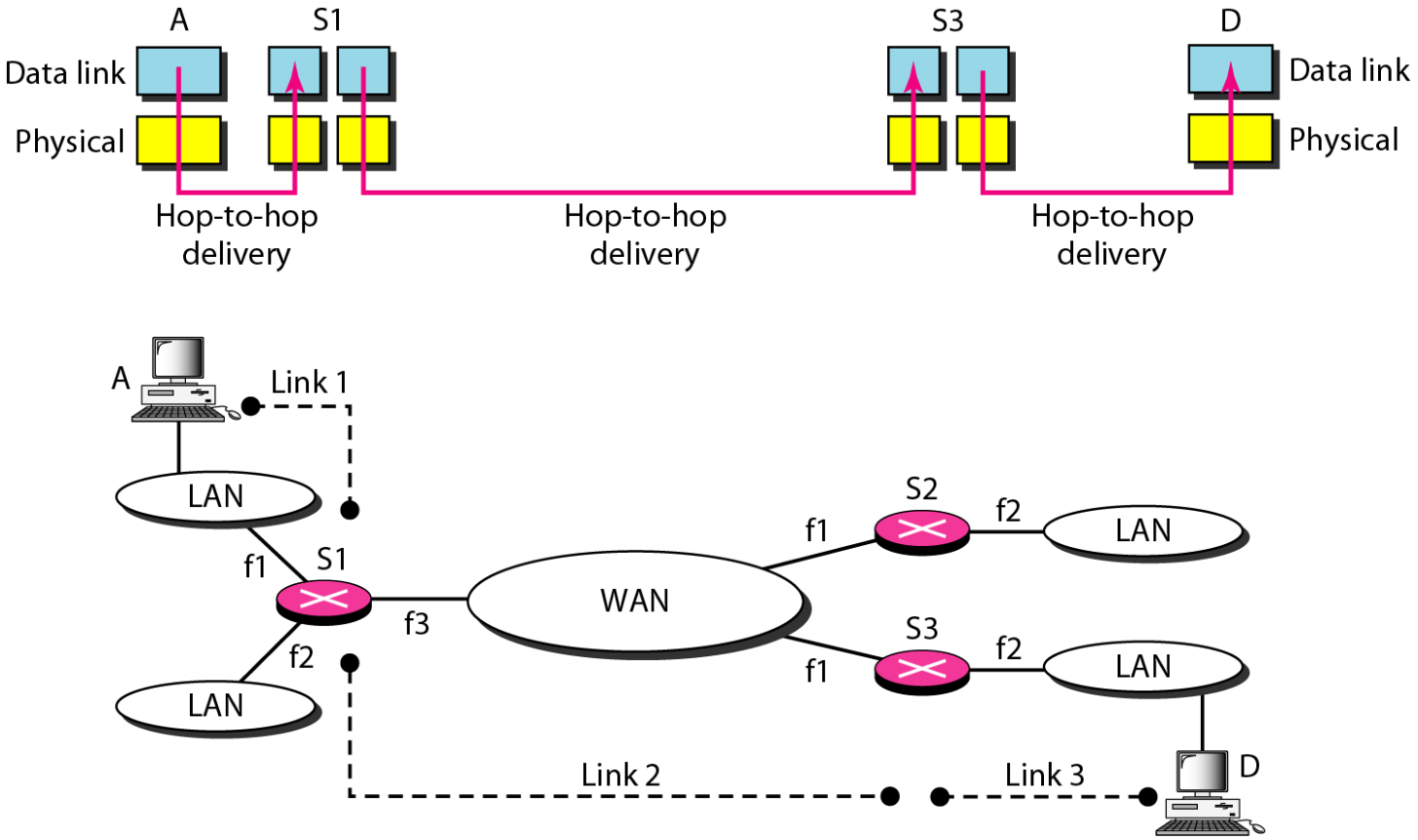


Figure 20.2 *Network layer in an internetwork*

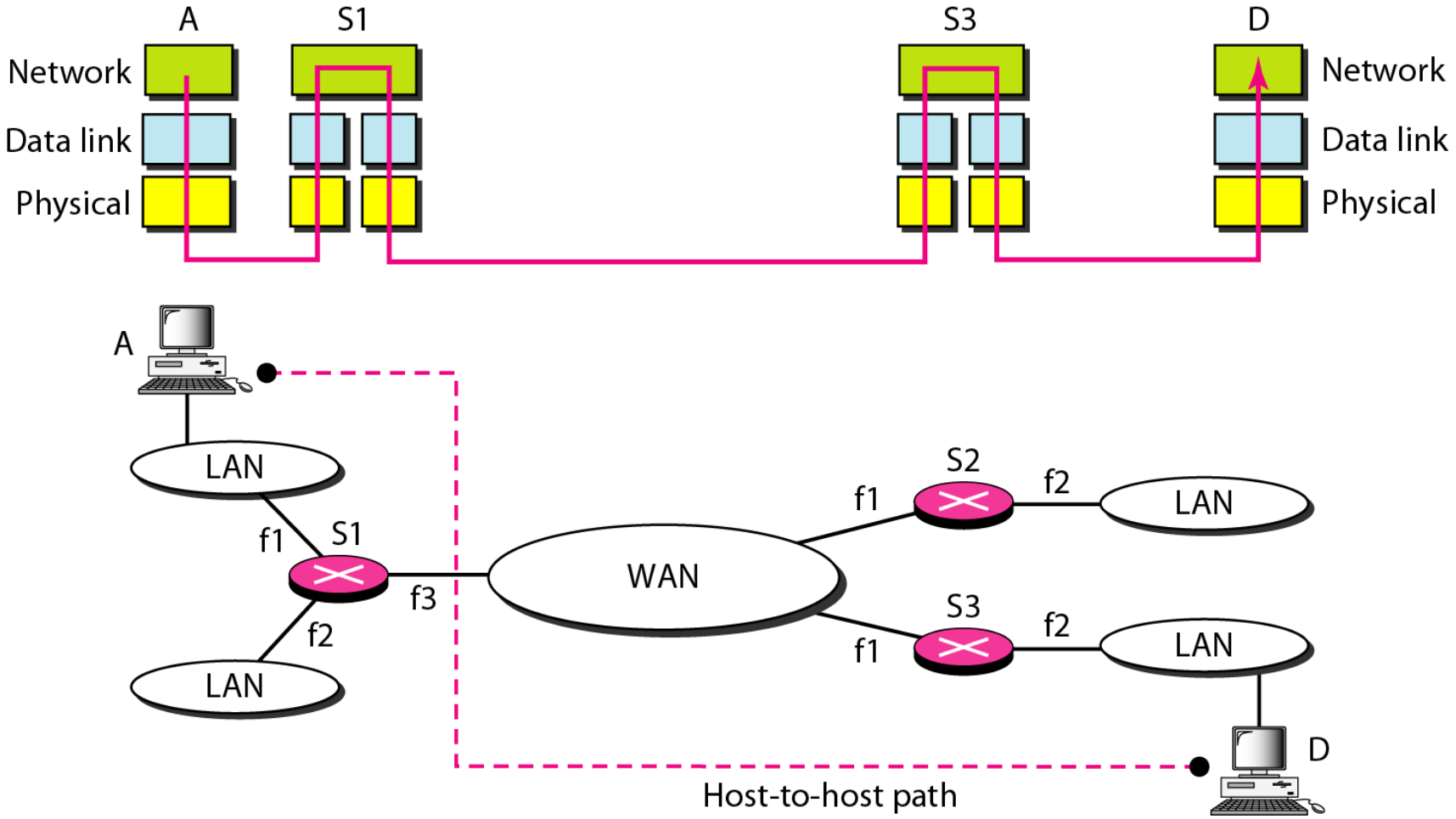
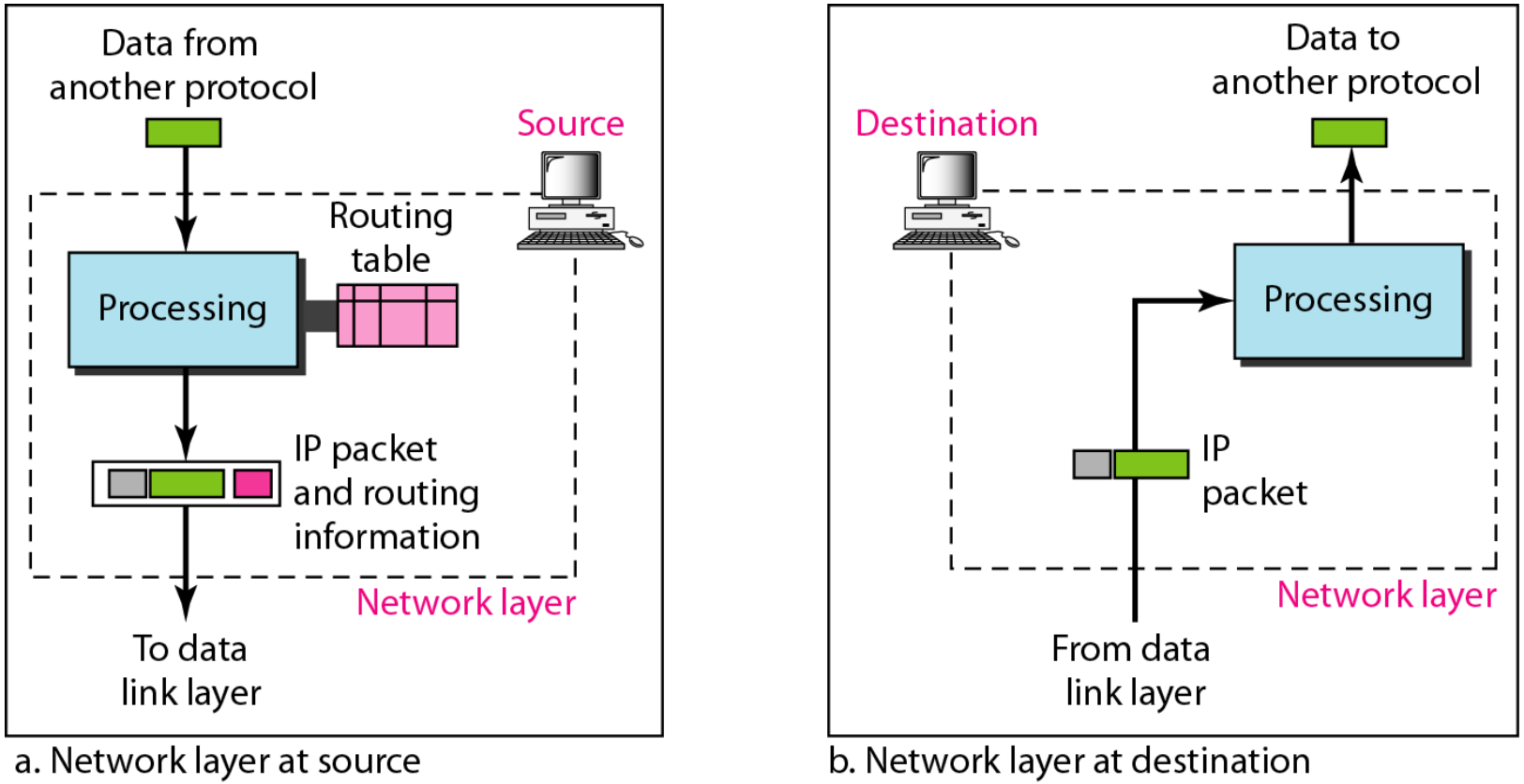


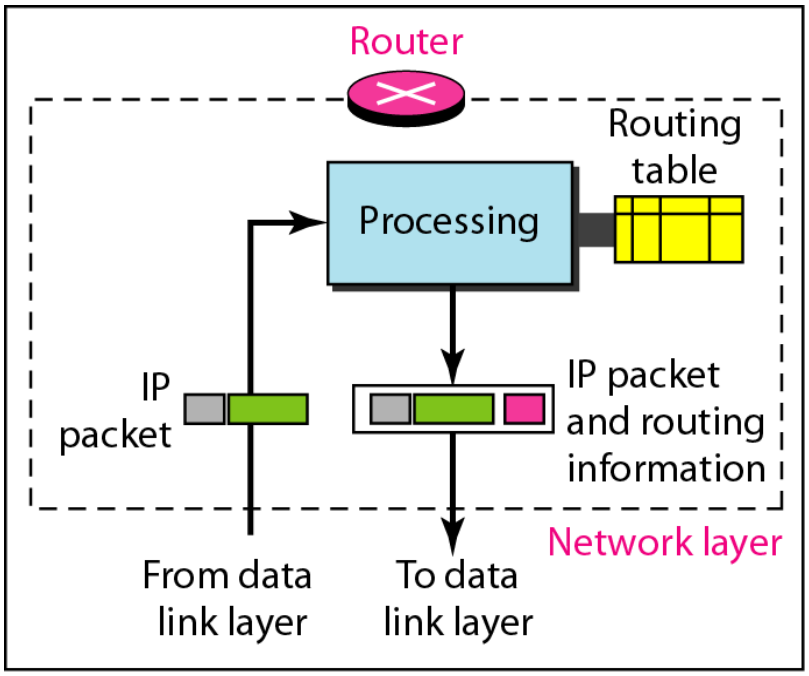
Figure 20.3 *Network layer at the source, router, and destination*



a. Network layer at source

b. Network layer at destination

Figure 20.3 *Network layer at the source, router, and destination (continued)*

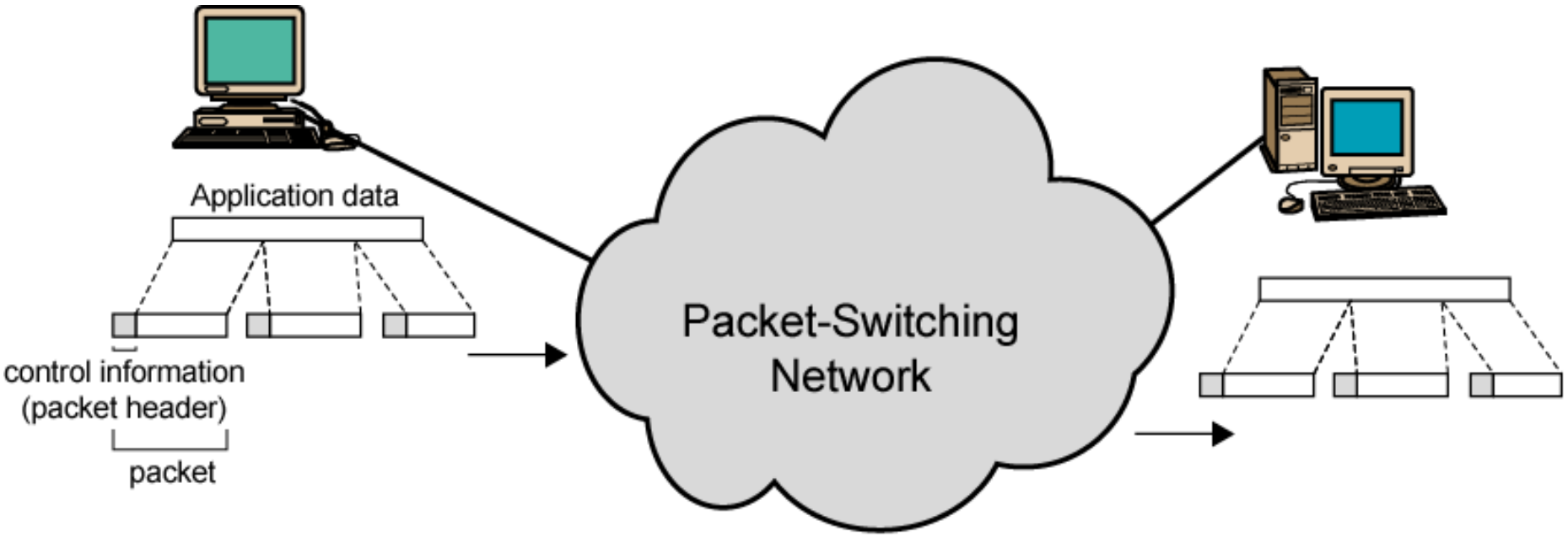


c. Network layer at a router

Packet Switching

- Data transmitted in small packets
  - Typically less than 1500 bytes (why?)
  - Longer messages split into series of packets
  - Each packet contains a portion of user data plus some control info
- Control info
  - Routing (addressing) info
- Packets are received, stored briefly (buffered) and past on to the next node
  - Store and forward

Use of Packets



William Stallings.. Data and Computer Communications, 7/E, Prentice Hall, 2004.

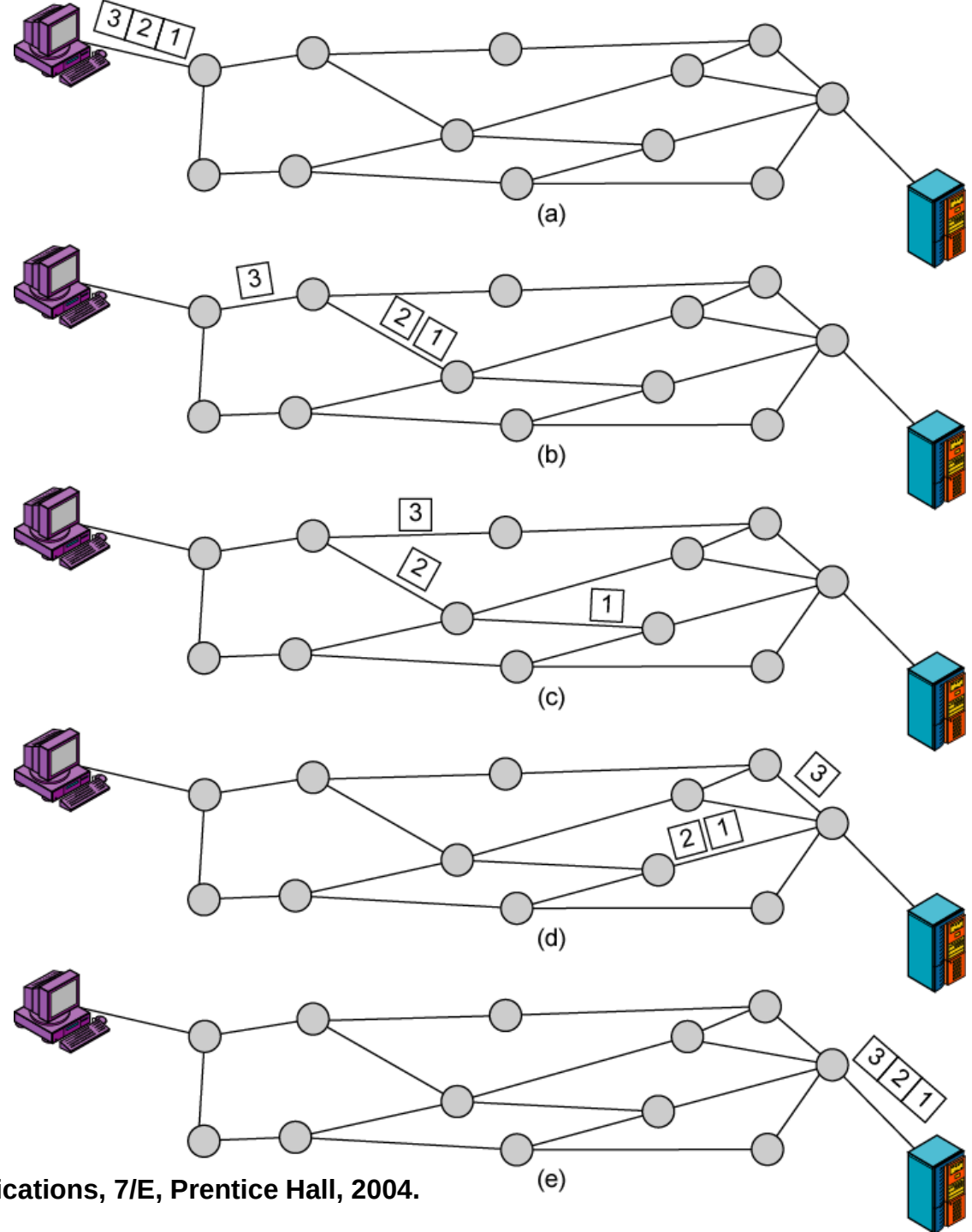
Switching Technique

- Station breaks long message into packets
- Packets sent one at a time to the network
- Packets handled in two ways
  - Datagram
  - Virtual circuit

Datagram

- Each packet treated independently
- Packets can take any practical route
- Packets may arrive out of order
- Packets may go missing
- Up to receiver to re-order packets and recover from missing packets

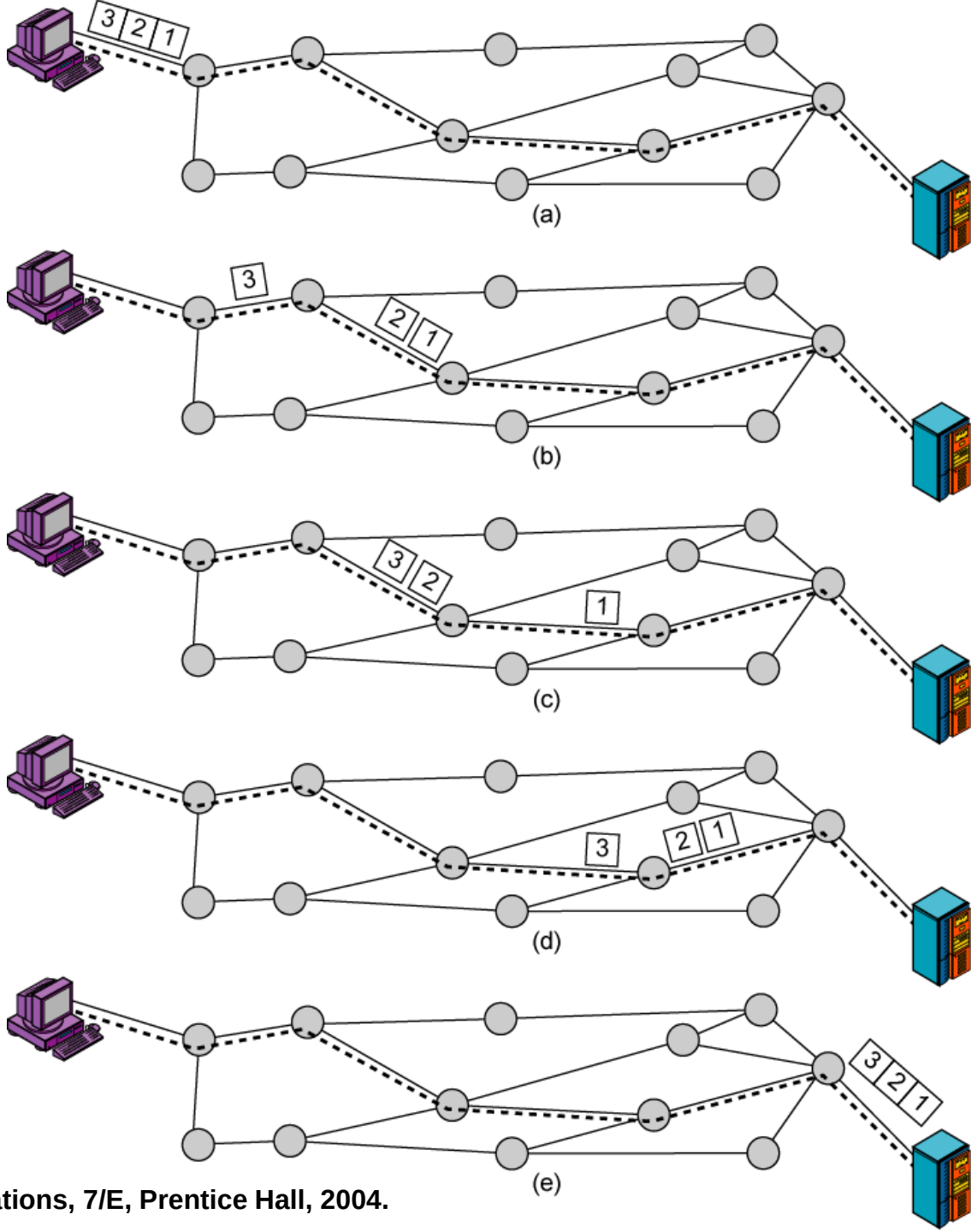
Datagram Diagram



Virtual Circuit

- Preplanned route established before any packets sent
- Call request and call accept packets establish connection (handshake)
- Each packet contains a virtual circuit identifier instead of destination address
- No routing decisions required for each packet
- Clear request to drop circuit
- Not a dedicated path

Virtual Circuit Diagram



Virtual Circuits v Datagram

- Virtual circuits
  - Network can provide sequencing and error control
  - Packets are forwarded more quickly
    - No routing decisions to make
  - Less reliable
    - Loss of a node looses all circuits through that node
- Datagram
  - No call setup phase
    - Better if few packets
  - More flexible
    - Routing can be used to avoid congested parts of the network

Note

Switching at the network layer in the Internet uses the datagram approach to packet switching.

Note

Communication at the network layer in the Internet is connectionless.

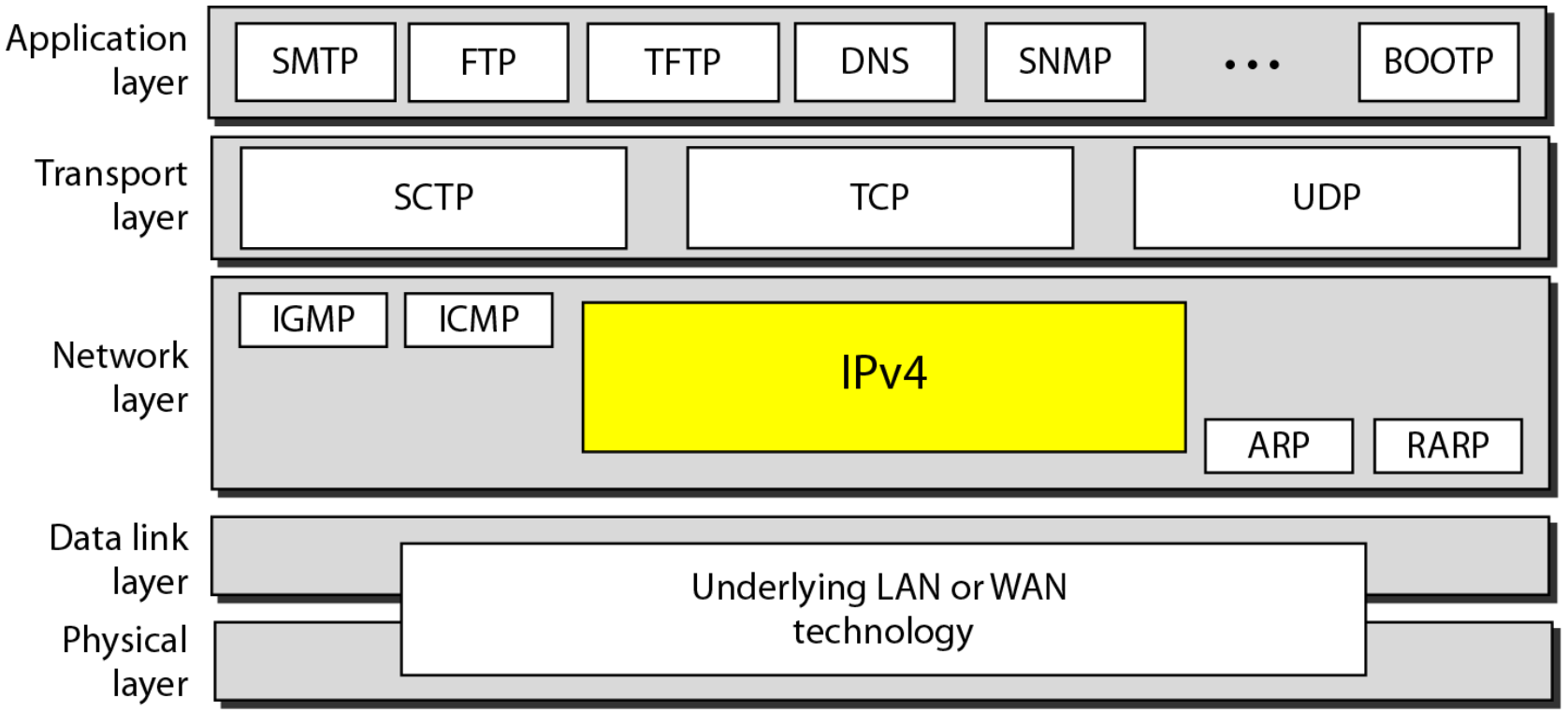
20-2 IPv4

The Internet Protocol version 4 (IPv4) is the delivery mechanism used by the TCP/IP protocols.

Topics discussed in this section:

Datagram
Fragmentation
Checksum
Options

Figure 20.4 *Position of IPv4 in TCP/IP protocol suite*



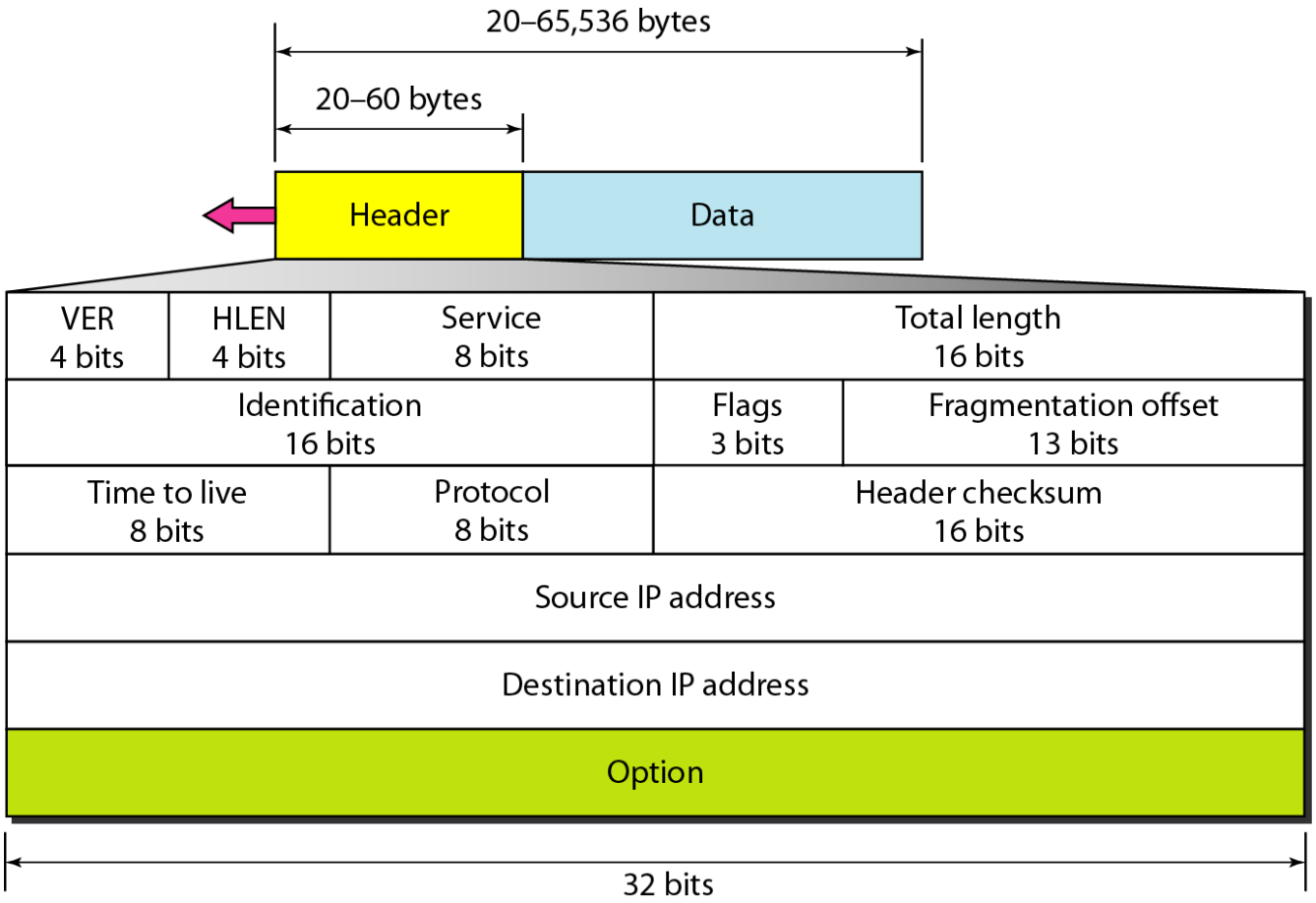
Note

IPv4 is an unreliable and connectionless datagram protocol – a best effort delivery

Best effort means that IPv4 provides no error control (except for error detection on the header) or flow control

IPv4 does its best to get a transmission through to its destination, but with no guarantees

Figure 20.5 *IPv4 datagram format*



IPv4 Datagram Format

- Version (VER): version of the IP protocol. Currently, the version is 4.
- Header length (HLEN): the total length of the datagram header in 4-byte words.
- Services: service type or differentiated services (not used now).
- Total length: total length (header plus data) of the datagram in bytes.
  - Total length of data = total length – header length

IPv4 Datagram Format

- Identification: used in fragmentation (discussed later).
- Flags: used in fragmentation (discussed later).
- Fragmentation offset: used in fragmentation (discussed later).
- Time to live: it is used to control the maximum number hops visited by the datagram.
- Protocol: defines the higher-level protocol that uses the services of the IPV4 layer.

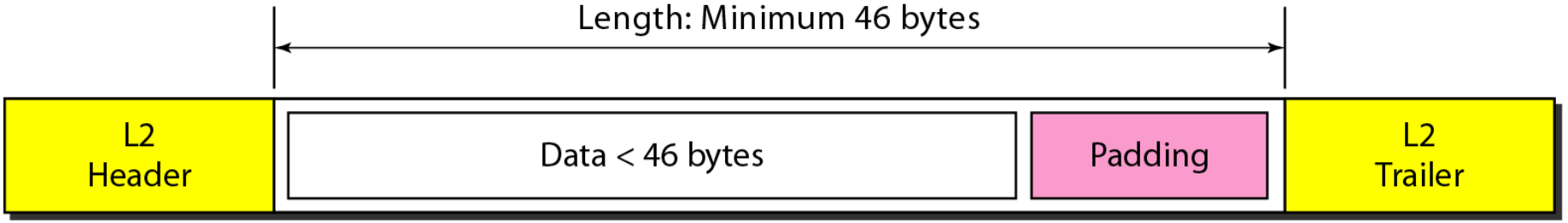
IPv4 Datagram Format

- Checksum: 1's compliment checksum (introduced in Chapter 10).
- Source address: is the IPv4 address of the source.
- Destination address: is the IPv4 address of the source.

Note

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

Figure 20.7 *Encapsulation of a small datagram in an Ethernet frame*



One of the reason why "total length" field is required.

Figure 20.8 *Protocol field and encapsulated data*

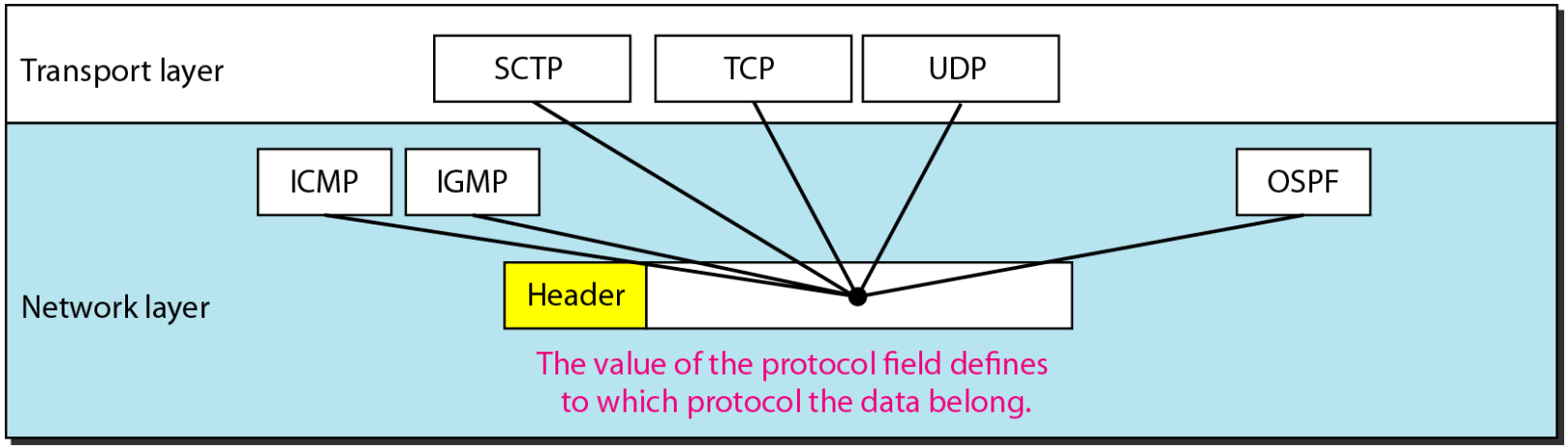


Table 20.4 ***Protocol values***

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

Example 20.1

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 20.2

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 20.3

In an IPv4 packet, the value of HLEN is 5, and the value of the total length field is 0x0028. How many bytes of data are being carried by this packet?

Solution

The HLEN value is 5, which means the total number of bytes in the header is 5 × 4, or 20 bytes (no options). The total length is 40 bytes, which means the packet is carrying 20 bytes of data (40 − 20).

Figure 20.9 *Maximum transfer unit (MTU)*

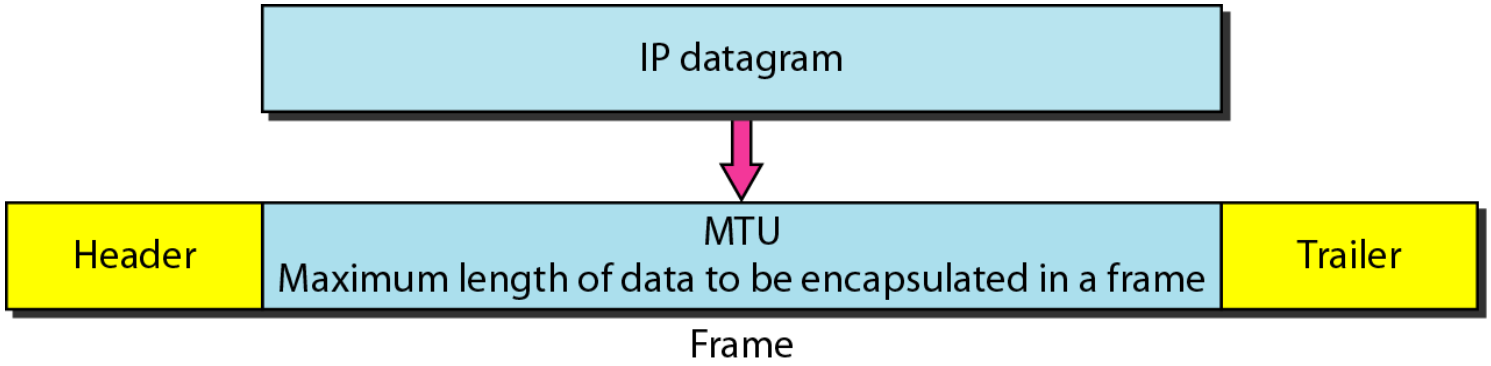


Table 20.5 *MTUs for some networks*

Protocol	*MTU*
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

Fields Related to Fragmentation

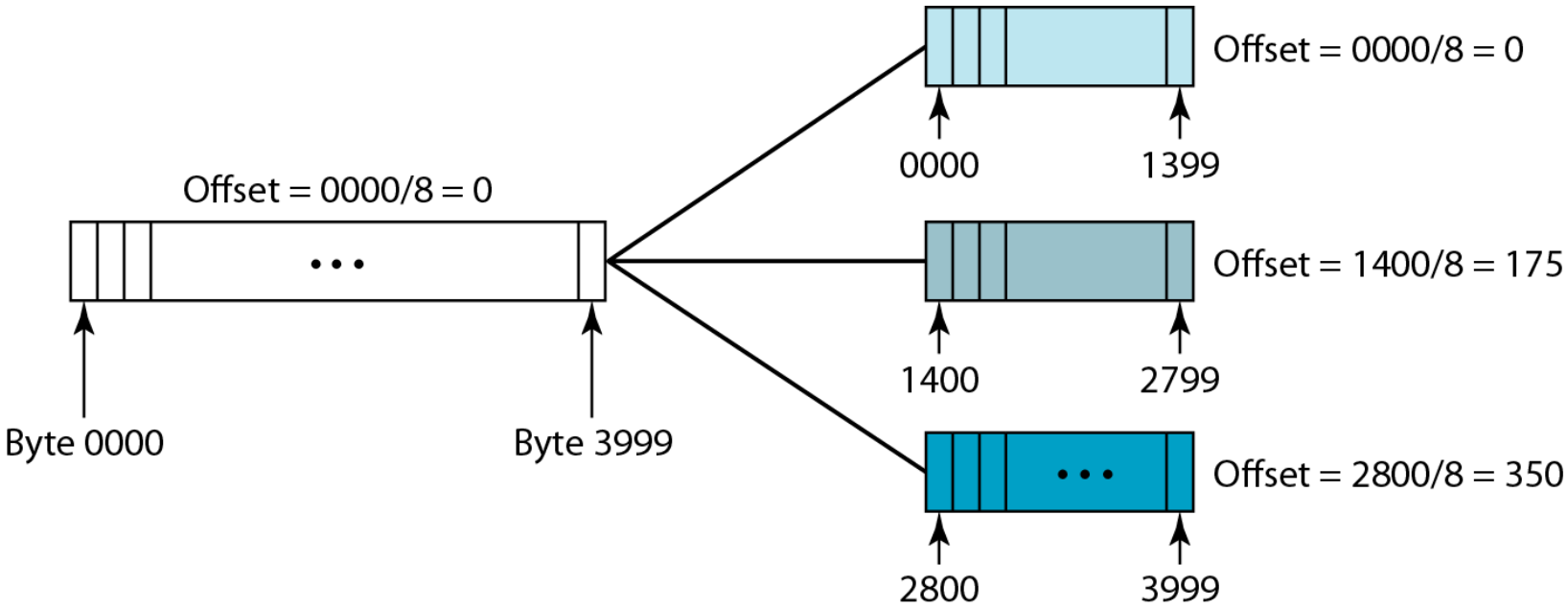
- **Identification:** identifies a datagram originating from the source host. A combination of the identification and source address must uniquely define a datagram as it leaves the source node.
- **Flags:** see next slide.
- **Fragmentation offset:** is the offset of the data in the original datagram measured in units of 8 bytes.

Figure 20.10 ***Flags (3 bits) used in fragmentation***

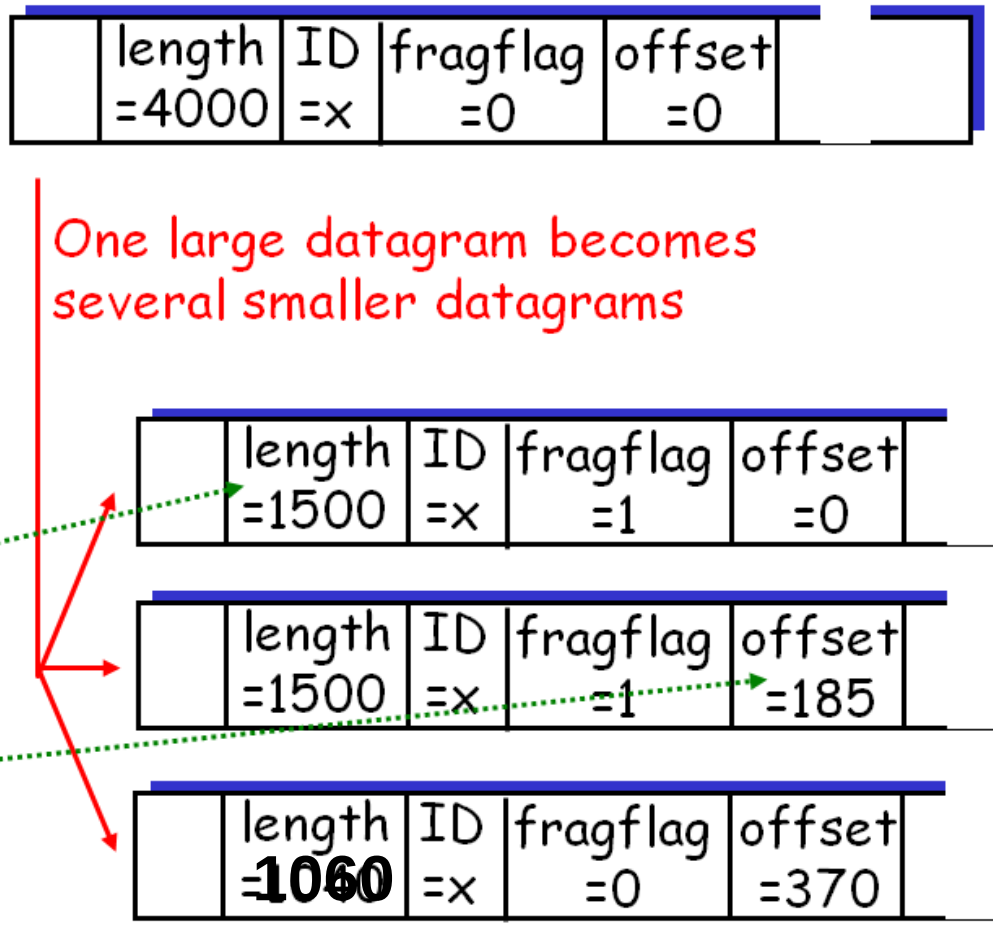
- first bit: reserved (not used)
- second bit: = 1 requires the packet not to be fragmented
  drops the packet if it is > MTU

- third bit: =1 more fragmented packets later
  =0 the last fragmented packet

Figure 20.11 *Fragmentation example*



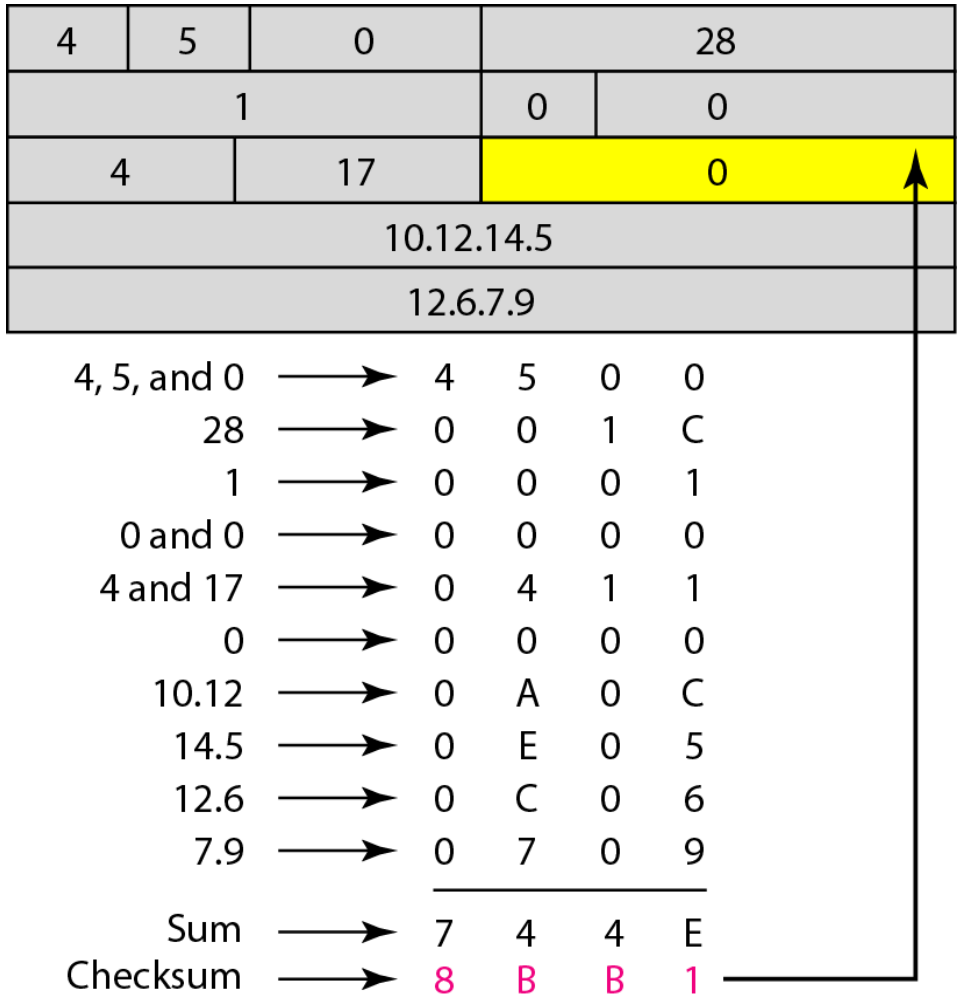
IP Fragmentation and Reassembly



IPv4 Checksum

- *IPv4 checksum use the 1's compliment method (chapter 10)*
- *Checksum only computes for IP header, not data*
  - *Upper layer has checksum for data portion*
  - *Header always changes in each router*
- *Header is chunked to 16-bit sections for computing*

Figure 20.13 *Example of checksum calculation in IPv4*



20-3 IPv6

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.

Topics discussed in this section:

Advantages
Packet Format
Extension Headers

IPv6: Advantages

- Larger address space.
- Better header format.
- New options.
- Allowance for extensions.
- Support for resource allocation.
- Support for more security.

Figure 20.15 *IPv6 datagram header and payload*

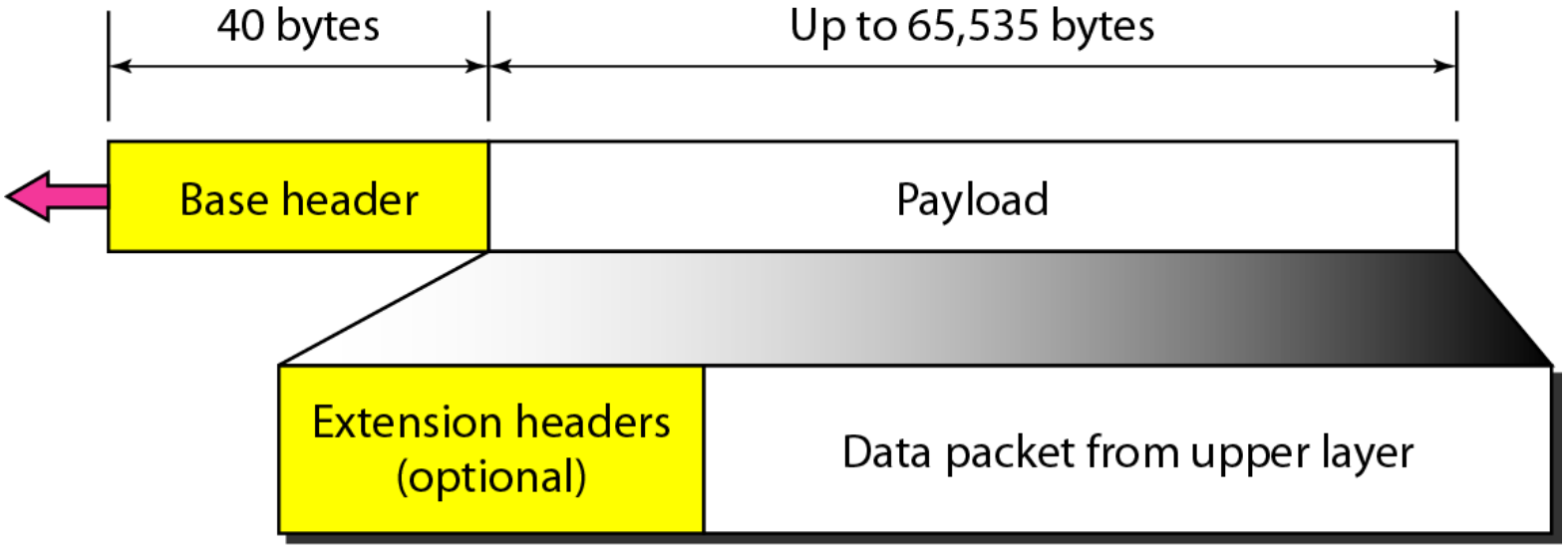


Figure 20.16 *Format of an IPv6 datagram*

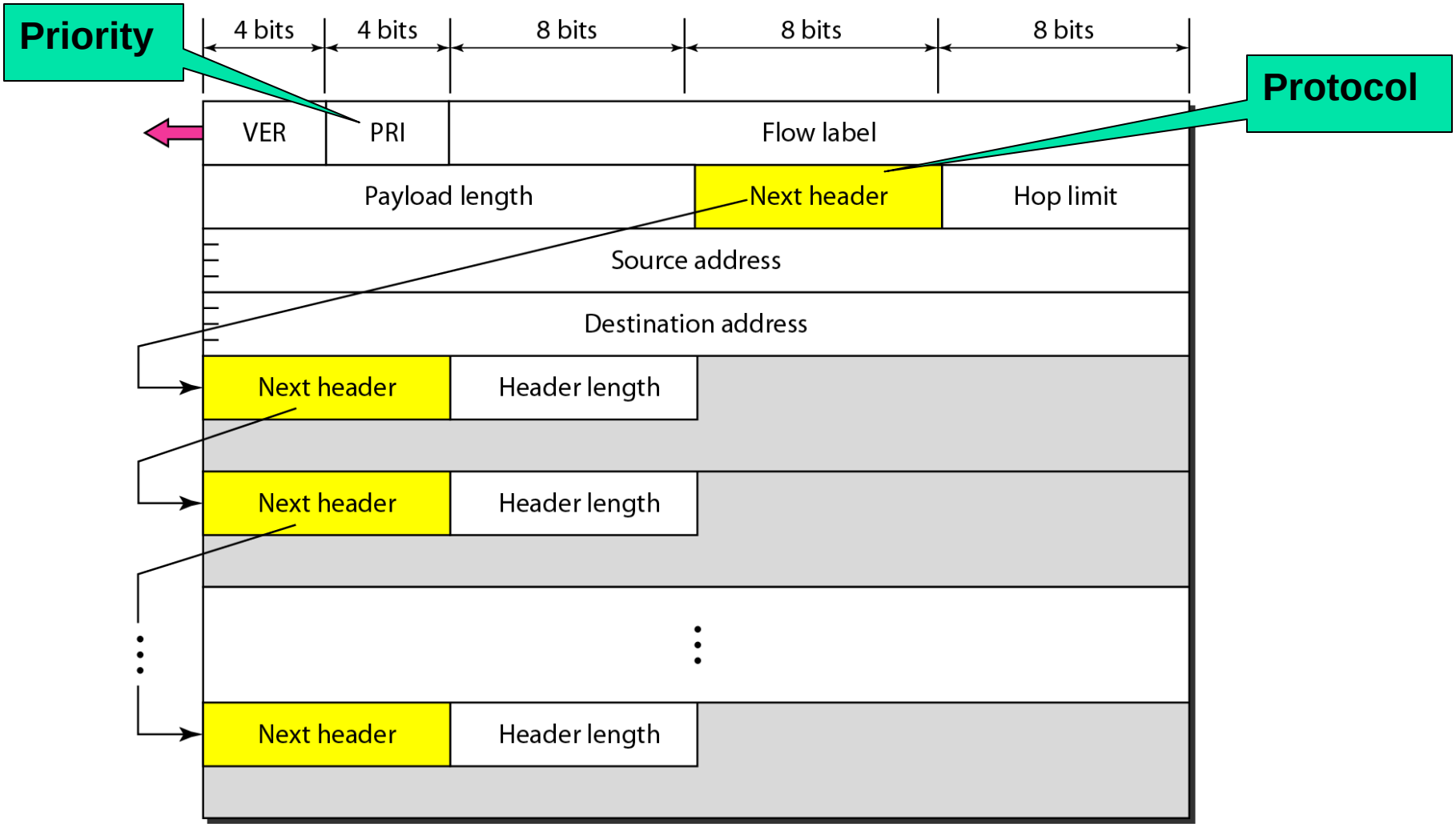


Table 20.9 *Comparison between IPv4 and IPv6 packet headers*

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.

20-4 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.

Topics discussed in this section:

Dual Stack
Tunneling
Header Translation

Figure 20.18 *Three transition strategies*

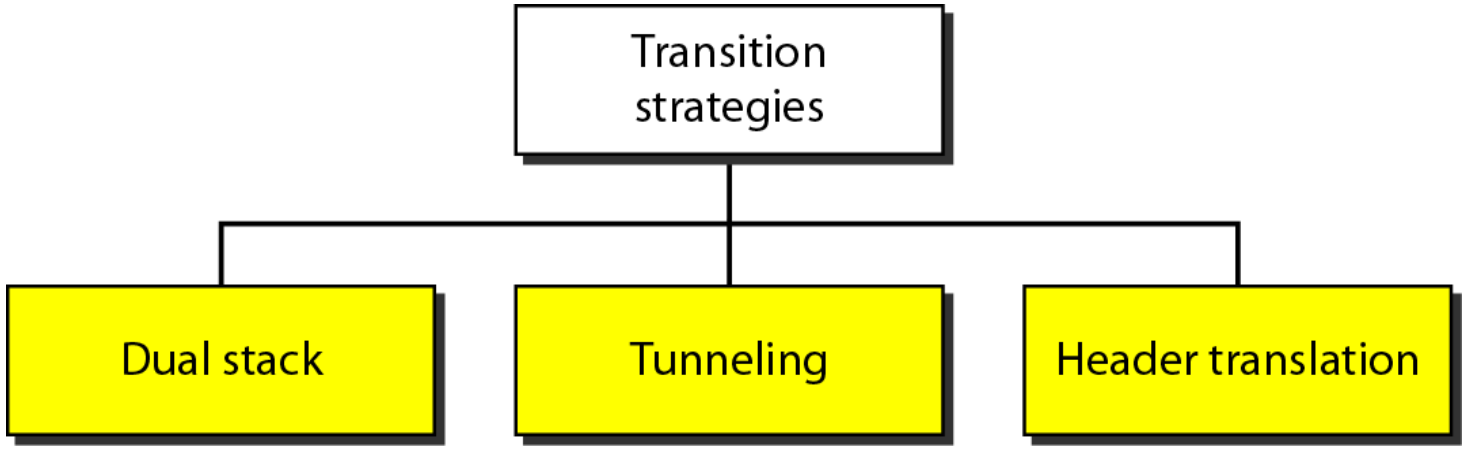
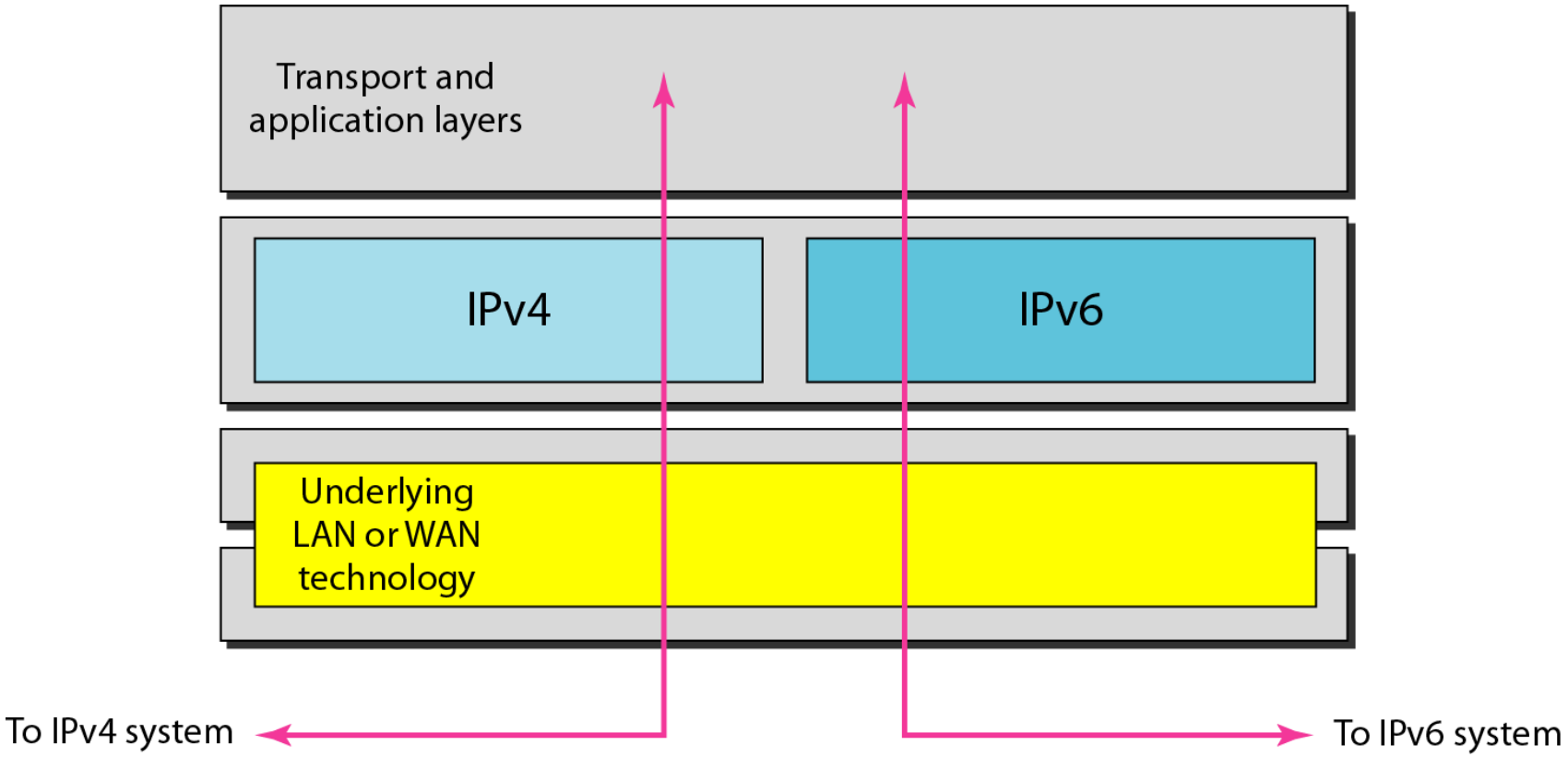
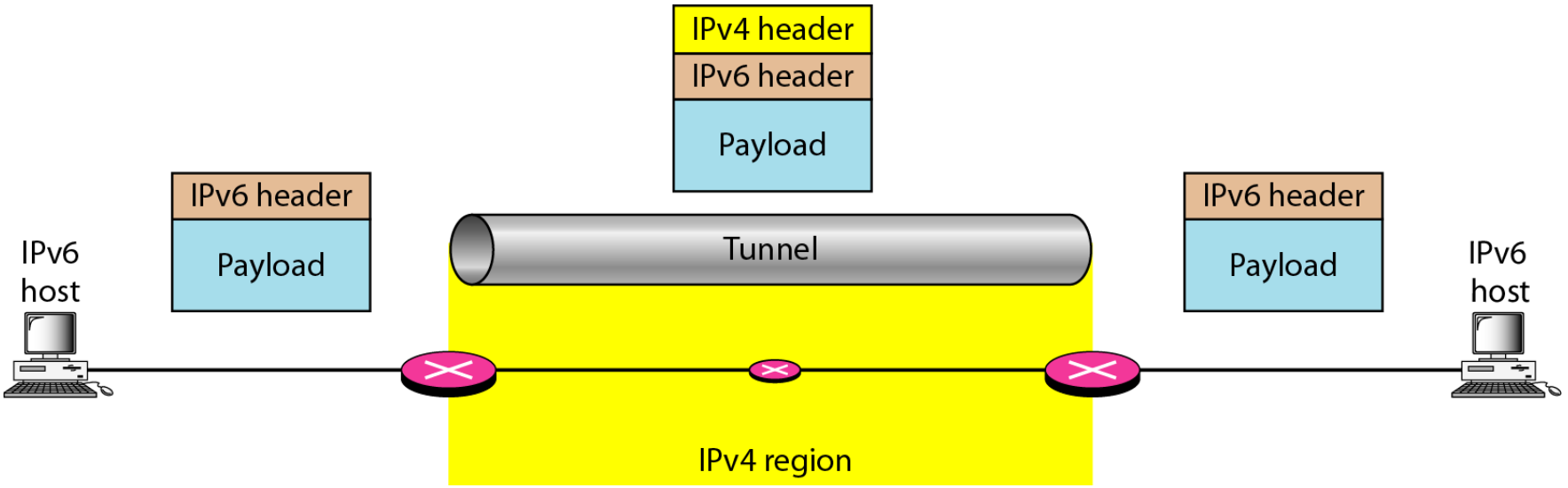


Figure 20.19 *Dual stack*



Host uses DNS query result to determine which IP to use

Figure 20.20 *Tunneling strategy*



Popular used right now in many countries

Figure 20.21 *Header translation strategy*