Principles of Electronic Communication Systems

Third Edition

Louis E. Frenzel, Jr.

Chapter 15

Internet Technologies

Topics Covered in Chapter 15

- 15-1: Internet Applications
- 15-2: Internet Transmission Systems
- 15-3: Storage Area Networks
- 15-4: Internet Security

15-1: Internet Applications

- The **Internet** is a worldwide interconnection of computers by means of a complex network of many networks.
- Anyone can connect to the Internet for the purpose of communicating and sharing information with almost any other computer on the Internet.
- The Internet is a communication system that accomplishes one of three broad uses:
  - Share resources
  - Share files or data
  - Communication.

15-1: Internet Applications

- The primary applications of the Internet are:
  - E-mail
  - File transfer
  - The World Wide Web
  - E-commerce
  - Searches
  - Voice over Internet Protocol
  - Video

15-1: Internet Applications

- **E-mail** is the exchange of notes, letters, memos, and other personal communication by way of e-mail software and service companies.
- **File transfer** refers to the ability to transfer files of data or software from one computer to another.
- The **World Wide Web** is a specialized part of the Internet where companies, organizations, the government, or individuals can post information for others to access and use.

15-1: Internet Applications

- **E-commerce** refers to doing business over the Internet, usually buying and selling goods and services by way of the Web.
- An Internet **search** allows a person to look for information on any given topic. Several companies offer the use of free search "engines," which are specialized software that can look for websites related to the desired search topic.

15-1: Internet Applications

- **Voice over Internet Protocol (VoIP)** is the technique of replacing standard telephone service with a digital voice version with calls taking place over the Internet.
- **Video over Internet Protocol.** Video or TV over the Internet (IPTV) is becoming more common. The video (and accompanying audio) is digitized, compressed, and sent via the Internet. It is expected to gradually replace some video transmitted over the air and by cable television systems.

15-1: Internet Applications

How the Internet Works

- The Internet is the ultimate data communication network. It uses virtually every type of data communication equipment and technique.
- The information is transmitted as serial binary pulses, usually grouped as bytes (8-bit chunks) of data within larger groups called packets.

15-1: Internet Applications

How the Internet Works: Internet Addresses

- Each individual or computer on the Internet must have some kind of identifier or address.
- The Internet uses a simplified name-addressing scheme that defines a particular hierarchy.
- The upper level of the hierarchy is called a **top-level domain (TLD).**

15-1: Internet Applications

How the Internet Works: Internet Addresses

- Common domains and their address segments include:

Domain	**Address segment**
Commercial companies	.com
Educational institutions	.edu
Nonprofit organizations	.org
Military	.mil
Government	.gov
Internet service providers	.net
Air transportation	.aero
Business	.biz

15-1: Internet Applications

How the Internet Works: Internet Addresses

Domain	**Address segment**
Cooperatives	.coop
Information sites	.info
International organizations	.int
Mobile	.mobi
Museums	.museum
Families and individuals	.name
Professions	.pro
Travel-related companies	.travel
Country	.us, .uk, .fr, .jp, .de (United States, United Kingdom, France, Japan, Germany)

15-1: Internet Applications

How the Internet Works: Internet Addresses

- Another part of the address is the **host name**.
- The host refers to the particular computer connected to the Internet.
- The host name is often the name of the company, organization, or department sponsoring the computer.

15-1: Internet Applications

How the Internet Works: E-mail Addresses

- The first part of the address is the user’s name or some abbreviation, concatenation, or nickname.
- The complete address might look like:

  <billbob@xyz.net>

- The user name is separated from the host by the @ symbol.
- Note the dot between the host name and the domain name. This address gets converted to a series of numbers used by computers on the Internet to identify and locate one another.

15-1: Internet Applications

How the Internet Works: WWW Addresses

- To locate sites on the Web, you use a special address called a **uniform resource locator (URL).**
- A typical URL is <http://www.abs.com/newinfo>.
- The first part of the URL specifies the communication protocol to be used, in this case hypertext transfer protocol (http).
- The www designates the World Wide Web.
- The abs.com part is the domain or the computer on which the website exists.
- The item after the slash (/) indicates a directory within the website software.

15-1: Internet Applications

How the Internet Works: Initial Connections

- A PC can be connected to the Internet in many ways.
- The most common way is through a modem that connects to the telephone system.
- A common way of connecting to the Internet is to use a LAN to which your PC may be connected.
- Most company and organization PCs are almost always connected to a LAN.
- The familiar telephone system is the first link to the Internet and typically connects you to a facility known as an Internet service provider (ISP).

15-1: Internet Applications

How the Internet Works: Broadband Connections

- A **broadband connection** is a fast Internet connection provided by a local telephone company.
- Typical dial-up connections speeds are between 19.2–40 kbps.
- The most widely used broadband connection is a cable TV modem. Data transfer rates can reach 6 Mbps.
- The second most widely used broadband connection is the **digital subscriber line (DSL).** It gives a data rate from 1.5 to 6 Mbps.

15-1: Internet Applications

How the Internet Works: Internet Service Provider

- An ISP is a company set up especially to tap into the network known as the Internet.
- It can be an independent company, a local telephone company, or a cable TV company.
- The ISP has one or more servers to which are connected many modems, DSLs, or cable connections from subscribers.
- It is usually the ISP that provides e-mail service and the software you use in communication over the Internet.

15-2: Internet Transmission Systems

Frame Relay

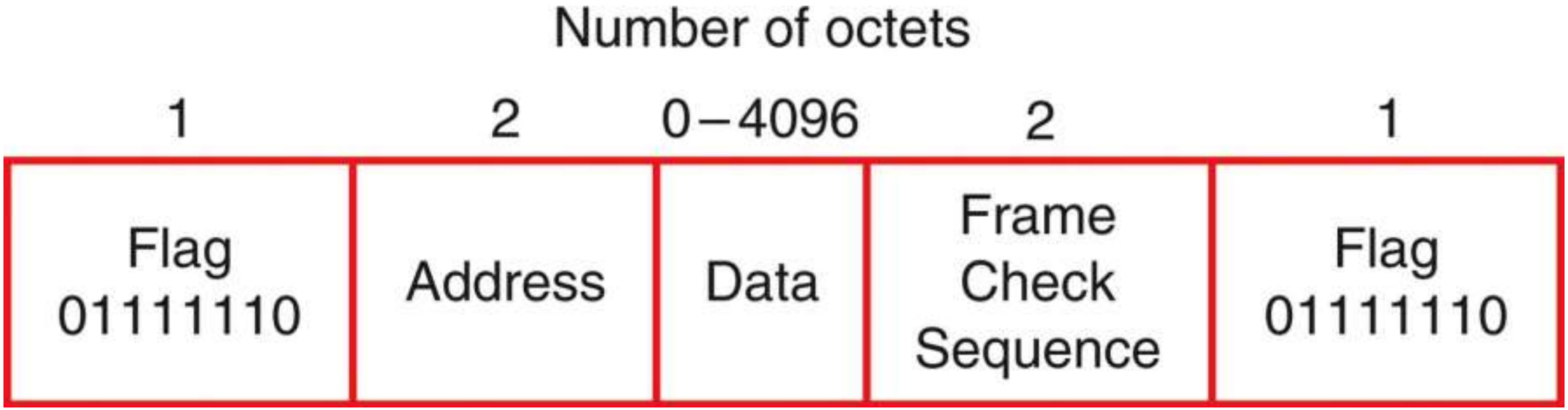
- Frame Relay (FR) is a packet-switching protocol standardized by the ITU-T.
- It packages data to be transmitted into FR frames that have the following structure:
    - 8-bit flags signal the beginning and ending of a packet.
    - A two-octet (byte) address field contains all the details regarding the exact destination of the packet through the network.

15-2: Internet Transmission Systems

Frame Relay

- The data field is variable and may contain up to 4096 octets.
- A two-octet **frame check sequence (FCS)** is an error detection code that is compared to the FCS calculated from the received data. If any transmission error occurs, the receiving unit asks for a retransmission.

15-2: Internet Transmission Systems



Number of octets

1	2	0–4096	2	1
Flag 01111110	Address	Data	Frame Check Sequence	Flag 01111110

Figure 15-1: A Frame Relay (FR) frame or packet.

15-2: Internet Transmission Systems

Frame Relay

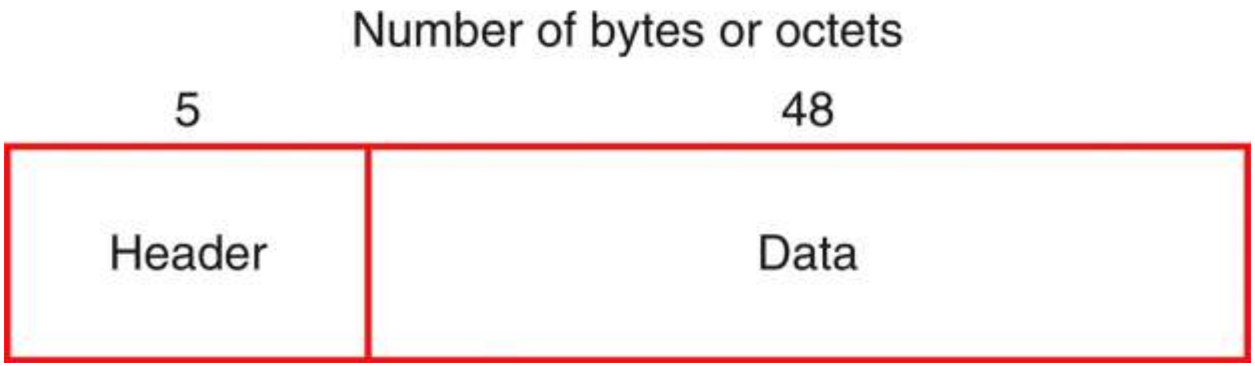
- FR is protocol-independent in that it can carry the data from any other transmission method such as Ethernet.
- The most common use of FR is in LAN-to-LAN connections where the LANs are widely separated, as in two different company locations.

15-2: Internet Transmission Systems

Asynchronous Transfer Mode

- **Asynchronous transfer mode (ATM)** is also a packet-switching system for transmitting data.
- It uses very short 53-byte packets with a 48-byte data payload.
- A 5-byte header designates the destination as well as the type of data to be handled.
- Any kind of data may be transmitted in this way including voice, video, and computer data.

15-2: Internet Transmission Systems



Number of bytes or octets

5

48

Header

Data

Figure 15-2: An ATM packet.

15-2: Internet Transmission Systems

SONET

- The **Synchronous Optical Network (SONET)** was developed to transmit digitized telephone calls in T1 format over fiber-optic cable at high speeds.
- SONET is used between telephone central offices, between central offices and long-distance carrier facilities, and for long-distance transmission.
- Most Internet backbones are SONET point-to-point connections or rings.
- SONET is by far the most widely used optical data transmission network in the United States.

15-2: Internet Transmission Systems

SONET

- SONET is a time-division multiplexing (TDM) transmission scheme that sends time-interleaved data in fixed-length frames of 810 bytes.
- The frame format consists of nine 90-byte rows. The bytes are transmitted consecutively from left to right and from top to bottom.
- In each row 4 bytes is for overhead, and 86 bytes per row is for data payload.
- The overhead bytes contain framing, control, parity, and pointer information for managing the payload.

15-2: Internet Transmission Systems

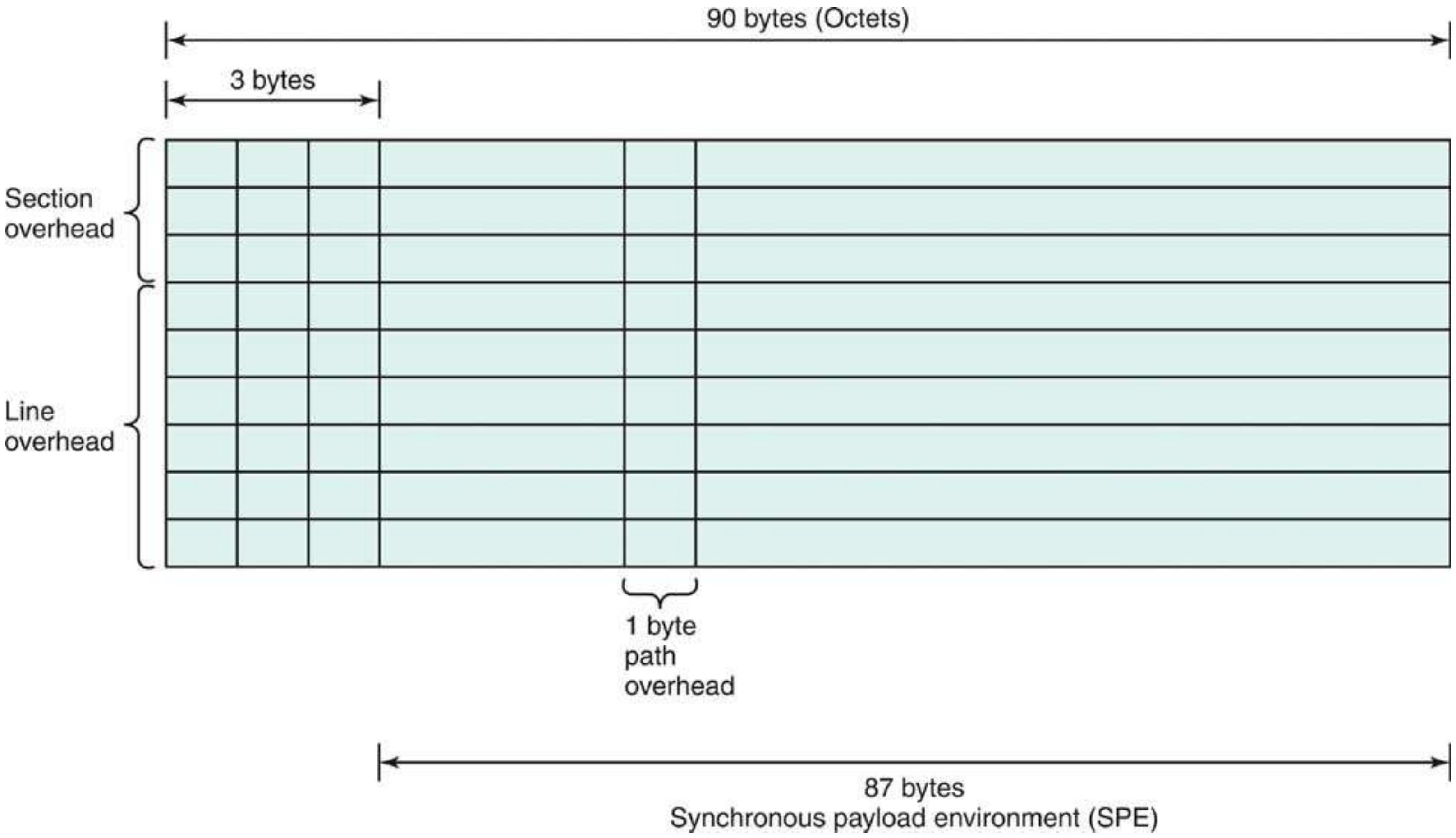


Figure 15-4: SONET frame format.

15-2: Internet Transmission Systems

Routers

- The **router** is the single most important piece of equipment in the Internet.
- Cisco Systems is the world’s largest router manufacturer.
- Routers interconnect the various segments of the WAN backbones, as well as other networks.
- The routers connect to one another and to the various servers to form a large mesh network connected usually by fiber-optic cable.

15-2: Internet Transmission Systems

Routers

- A router is an intelligent computerlike device.
- It examines the internet protocol (IP) destination addresses of all packets transmitted to it to determine the best next path for the data to take to its destination.
- The router stores information in a routing table about the other routers and networks to which it is connected and about any nearby networks.
- This information is compared to the destination address on all incoming packets, and routing algorithms determine the best (closest, fastest) connection and then retransmit the packet.

15-2: Internet Transmission Systems

Routers

- A modern router consists of a group of line cards that plug into connectors on a printed-circuit board back plane.
- The back plane contains the copper interconnecting lines to allow the line cards to transmit and receive data from one another.
- Transfer speeds are typically many gigabits per second.
- The line cards communicate with one another through a switch fabric.
- Superfast electronic switches connect the line cards.

15-2: Internet Transmission Systems

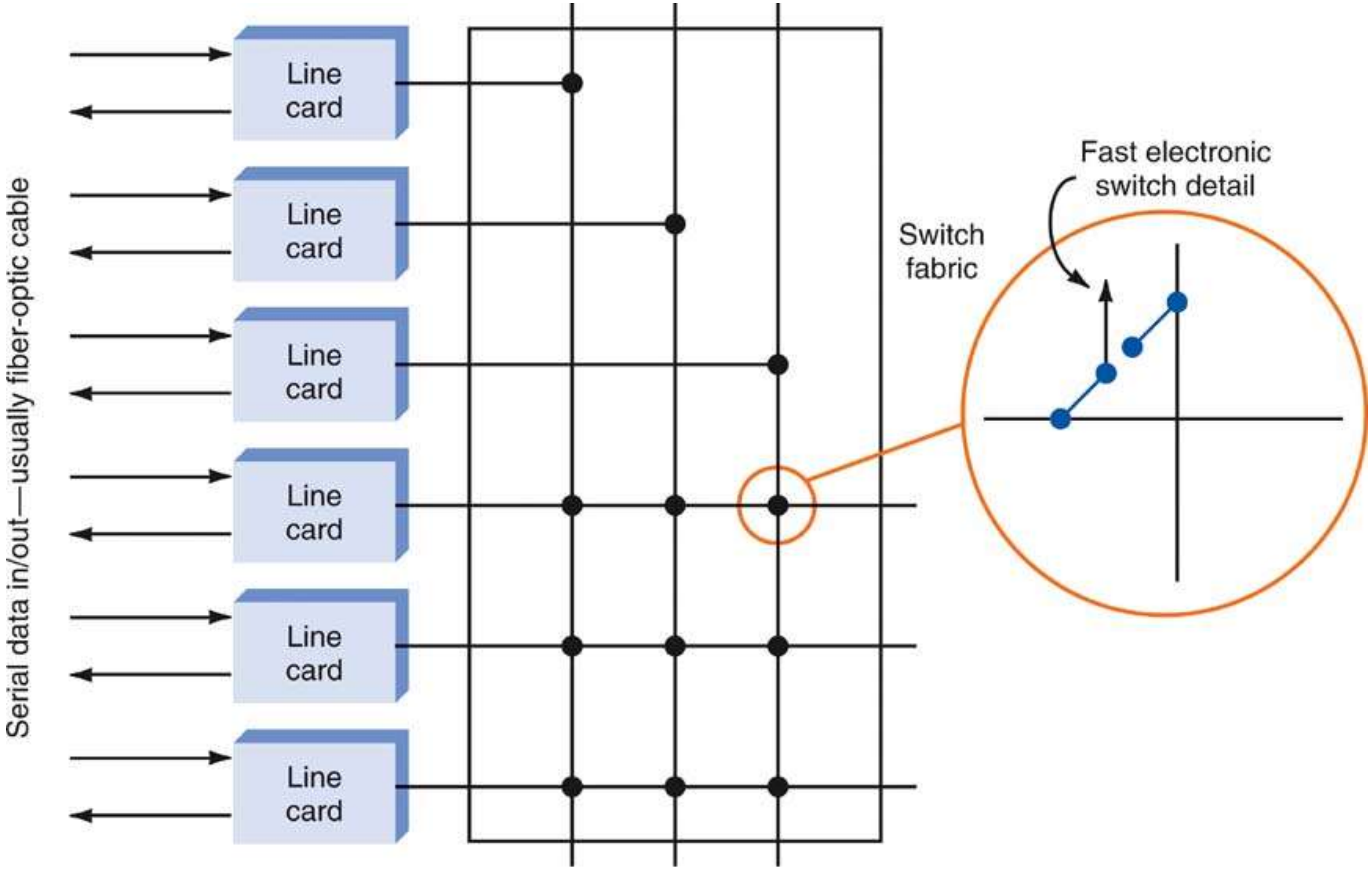

Serial data in/out—usually fiber-optic cable
Line card
Line card
Line card
Line card
Line card
Line card
Switch fabric
Fast electronic switch detail

Figure 15-5: General block diagram of a router.

15-2: Internet Transmission Systems

The Internet Backbone

- The **Internet backbone** is a group of companies that install, service, and maintain large nationwide and even worldwide networks of high-speed fiber-optic cable.
- The companies own the equipment and operate it to provide universal access to the Internet.
- **Network access points (NAPs)** connect the backbone providers to one another to provide multiple paths between computers.

15-2: Internet Transmission Systems

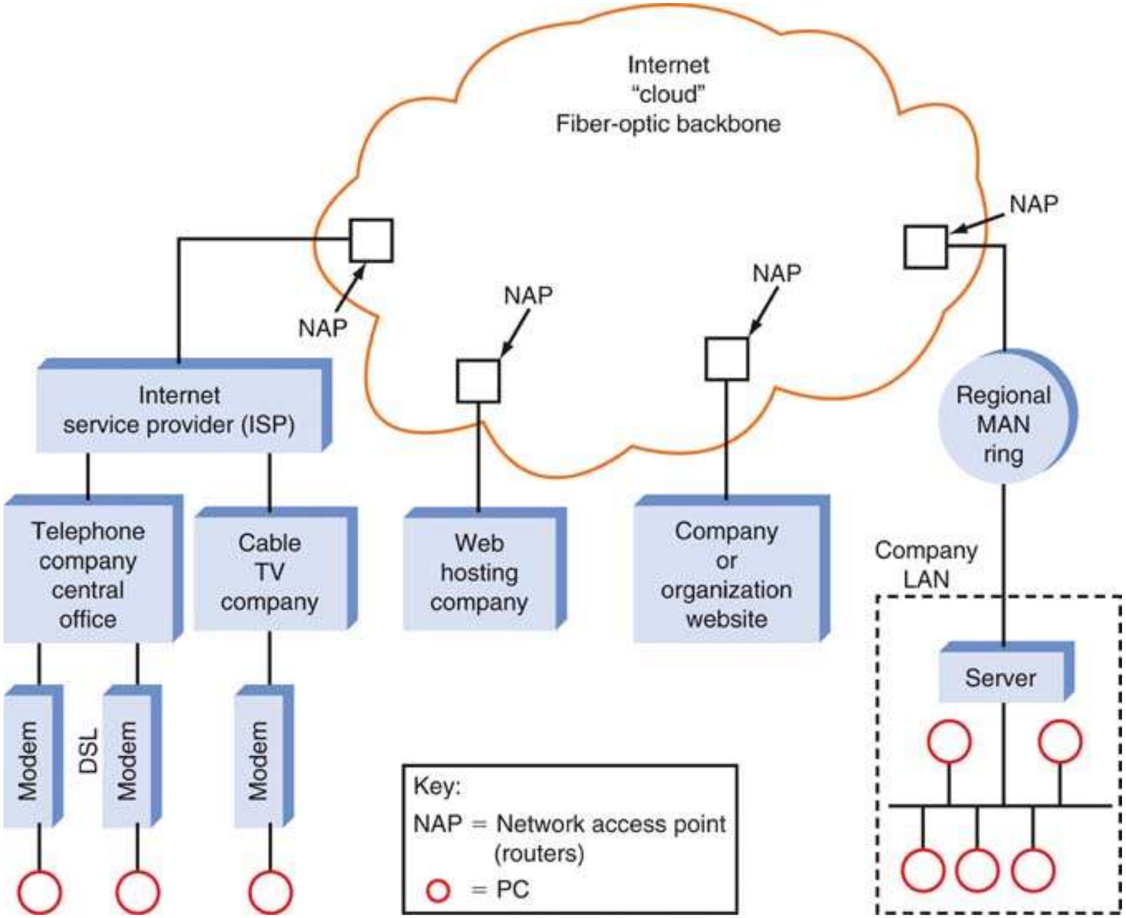


Figure 15-6: Simplified diagram of the Internet.

15-2: Internet Transmission Systems

The Packet-Switching Transmission System

- The Internet is a packet-switching system.
- Data to be sent is divided up into short chunks called **packets** or **datagrams** and transmitted one at a time.
- Packets are typically less than 1500 **octets** long.
  - **Octet** is another name for a byte, an 8-bit word.
- Not all packets take the same path through the system.
- The packets may arrive at the receiving end out of the order in which they were sent.

15-2: Internet Transmission Systems

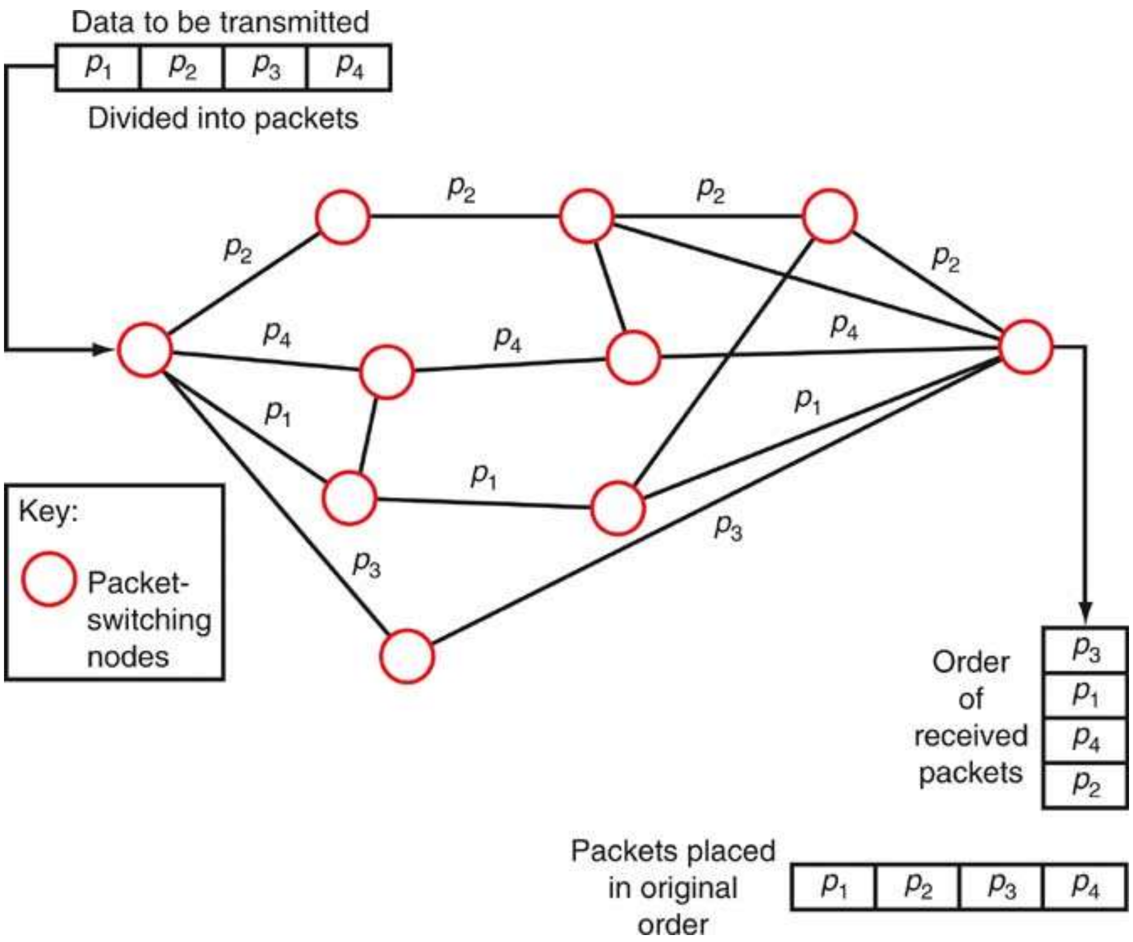


Figure 15-7: The packet-switching concept showing nodes in the backbone.

15-2: Internet Transmission Systems

The Packet-Switching Transmission System

- Packet switching requires a set of software protocols that make sure that the data is properly partitioned, transmitted, received, and reassembled.
- On the Internet, these protocols are called **TCP/IP.**
- **TCP** means **Transmission Control Protocol**, and **IP** means **Internet Protocol**.

15-2: Internet Transmission Systems

The Packet-Switching Transmission System

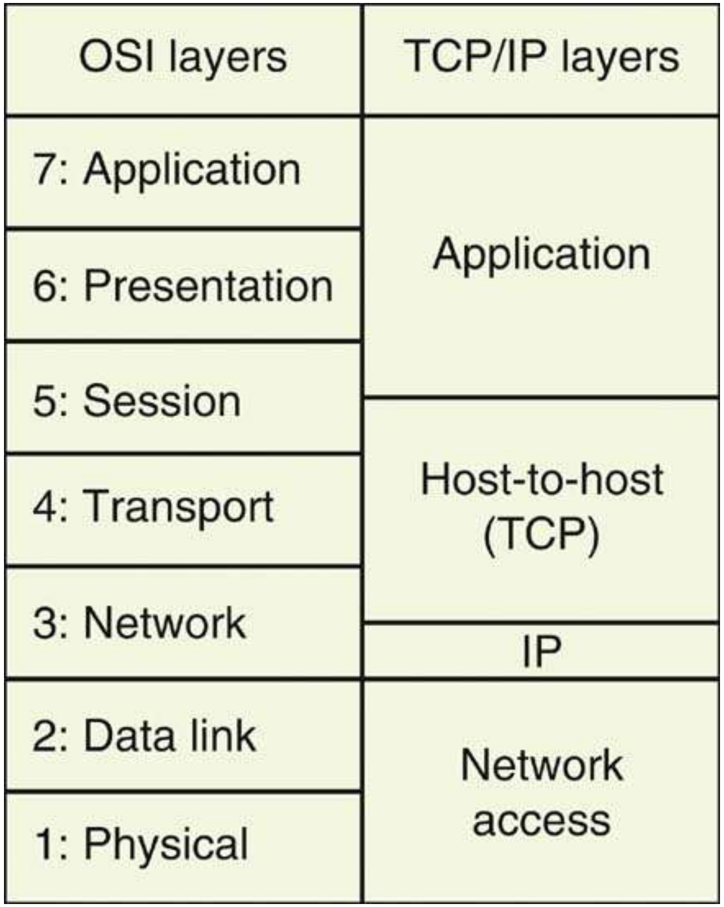
- TCP/IP is a layered protocol similar to the OSI seven-layer model.
- TCP/IP does not implement all seven layers, although the effect is the same.
- The upper, or applications, layer works with other protocols that implement the desired application.

15-2: Internet Transmission Systems

The Packet-Switching Transmission System

- The most widely used protocols are
  - **TELNET**, which permits a remote PC to connect via the telephone system to the Internet.
  - **File transfer protocol (FTP),** which facilitates the transmission of long files of data
  - **Simple mail transfer protocol (SMTP),** which implements e-mail
  - **Hypertext transfer protocol (http),** which provides access to the World Wide Web.

15-2: Internet Transmission Systems



OSI layers	TCP/IP layers
7: Application	Application
6: Presentation	
5: Session	
4: Transport	Host-to-host (TCP)
3: Network	IP
2: Data link	Network access
1: Physical	

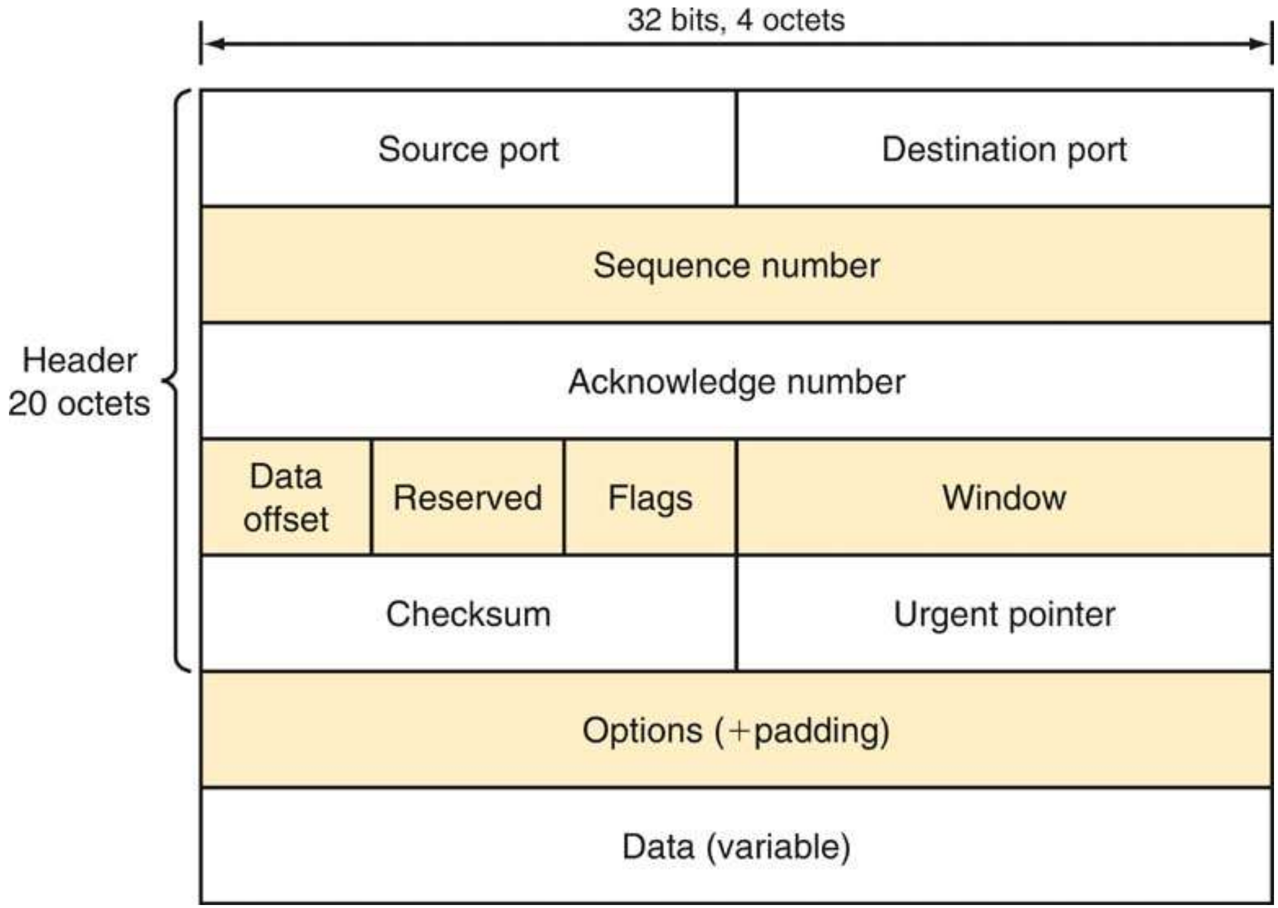
Figure 15-8: Comparing the OSI and TCP/IP layers.

15-2: Internet Transmission Systems

The Packet-Switching Transmission System

- The **host-to-host layer** is TCP.
  - TCP is used only to prepare the packets for transmission and reassemble the packets when received.
  - It does not implement the actual packet transmission over the Internet.
- The **IP layer** uses the IP protocol.
  - The IP layer ensures that the packet gets to its destination over the Internet.
- The **network access layer** contains the physical layer connection.

15-2: Internet Transmission Systems



32 bits, 4 octets

Header 20 octets

Source port

Destination port

Sequence number

Acknowledge number

Data offset

Reserved

Flags

Window

Checksum

Urgent pointer

Options (+padding)

Data (variable)

Figure 15-9: TCP headers.

15-2: Internet Transmission Systems

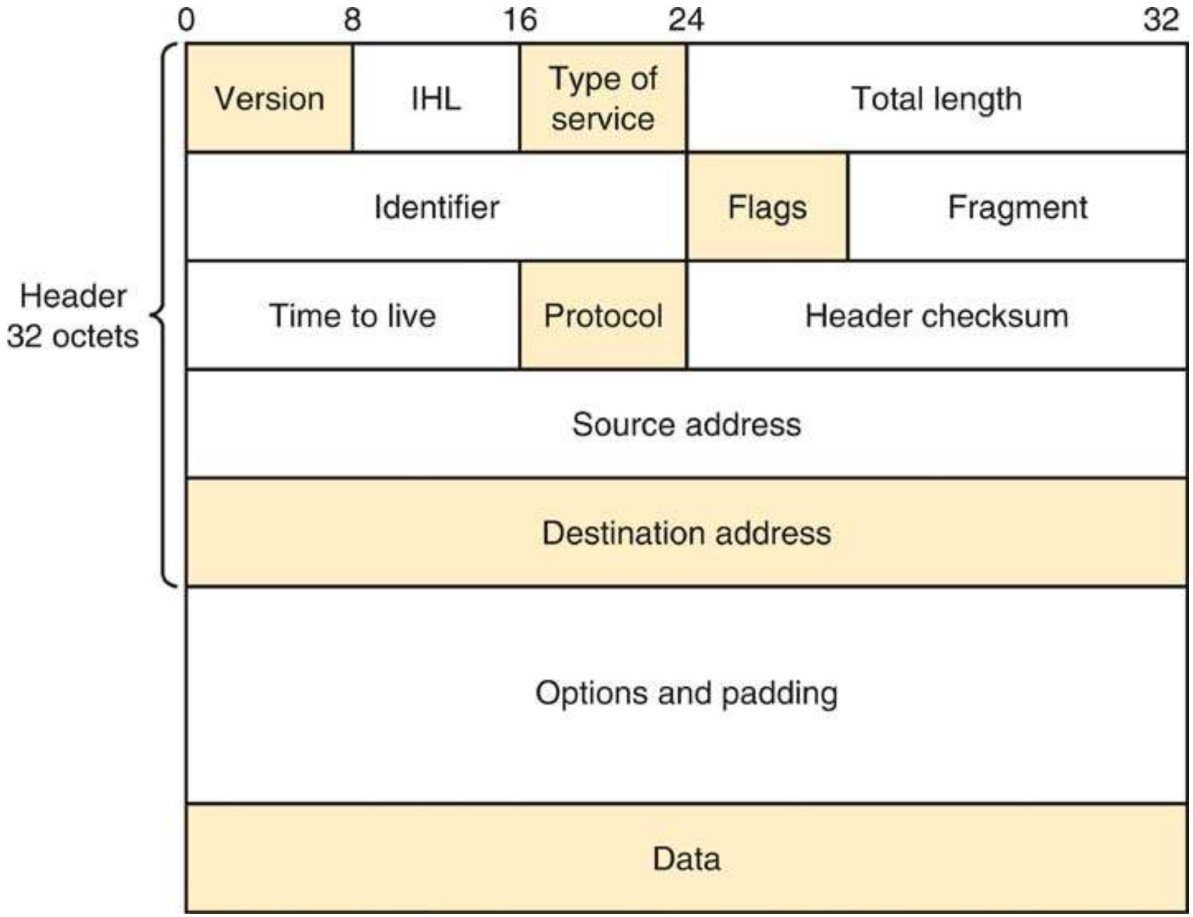


Figure 15-10: IP header (IPv4).

15-2: Internet Transmission Systems

UDP

- The **User Datagram Protocol (UDP)** is another protocol used at the transport level.
- UDP provides a connectionless service for applications.
- UDP uses IP to route its packets throughout the Internet.
- It is used when the arrival of a message is not absolutely critical.
- It is also used in real-time applications.

15-2: Internet Transmission Systems

Internet and Addressing

- Routers identify the destination network to which a packet is bound by using the network IP address.
- All devices on that network share the same network address, but have unique host addresses.
- When a computer receives a packet from the router, the computer first checks the destination **MAC (media access control) address** of the packet at the data link layer.

15-2: Internet Transmission Systems

Internet and Addressing

- If it matches, it’s then passed on to the network layer.
- At the network layer, it checks the packet to see if the destination IP address matches the computer’s IP address.
- From there, the packet is processed as required by the upper layers.

15-2: Internet Transmission Systems

Internet and Addressing

- The format of an IP address is called dotted decimal, and it consists of four numbers from 0 to 255 separated by periods or dots:

  35.75.123.250

- IP addresses are organized into five classes, of which we normally use three (A, B, and C). These three classes identify workstations, routers, switches, and other devices.

15-2: Internet Transmission Systems

Internet and Addressing

- The first octet of an IP address determines its class.
- Depending on the class to which the address belongs, we can determine which portion of the address is the network ID and which is the host ID.

Table 15–2	**Identifying Network and Host ID**		
Class	**Range of First Octet**	**Number of Network ID Bits**	**Number of Host ID Bits**
A	1–126	8	24
B	128–191	16	16
C	192–223	24	8

15-2: Internet Transmission Systems

Network Mask

- The router uses a special sequence of bits called the **network mask** to determine if the packet is being sent to its network.
- The network mask has all 1s in the network ID and all 0s in the host ID.
- This mask is then logically ANDed to the packet, and the router will see if the destination host is on its network.
- **Subnetting** is a technique that splits networks into smaller networks to help routers more efficiently route packets and manage the size of their router tables,

15-2: Internet Transmission Systems

MAC Address Versus IP Address

- The media access control (MAC) address is a unique address assigned to the physical device.
- The IP address is a logical address used to determine where in the network a host is located.
- The MAC identifies the manufacturer and has a unique number associated with it.
- The IP address is used to find out where the MAC is so that packets can be routed to the host.

15-3: Storage Area Networks

- **Storage-area networks (SANs)** are one of the faster-growing segments of data communications.
- SANs and similar storage systems provide a way to meet the Internet’s nearly insatiable need for data storage.
- Special storage systems have been created to hold these massive data resources, and special networks and communications systems have been developed to ensure rapid access to this data.

15-3: Storage Area Networks

- Large, flexible systems using fast serial data transfer are available for SANs applications.
- One of these systems is called **network attached storage (NAS).** These systems are made up of a **redundant array of independent disks (RAID)** or **just a bunch of disks (JBOD).**
- These large boxes of disk drives are typically connected to a PC or server by way of the installed Ethernet LAN.

15-3: Storage Area Networks

- They are assigned an IP address so that data can be accessed in a file format. Anyone connected to the LAN can access the data on the disks if authorization is provided.
- The connection between the servers and the SAN is made usually by a fiber-optic network known as **Fibre Channel (FC).**
- A newer connection system called **iSCSI** or **Internet SCSI** ("I skuzzy") uses the installed Ethernet LAN plus Ethernet switches.

15-3: Storage Area Networks

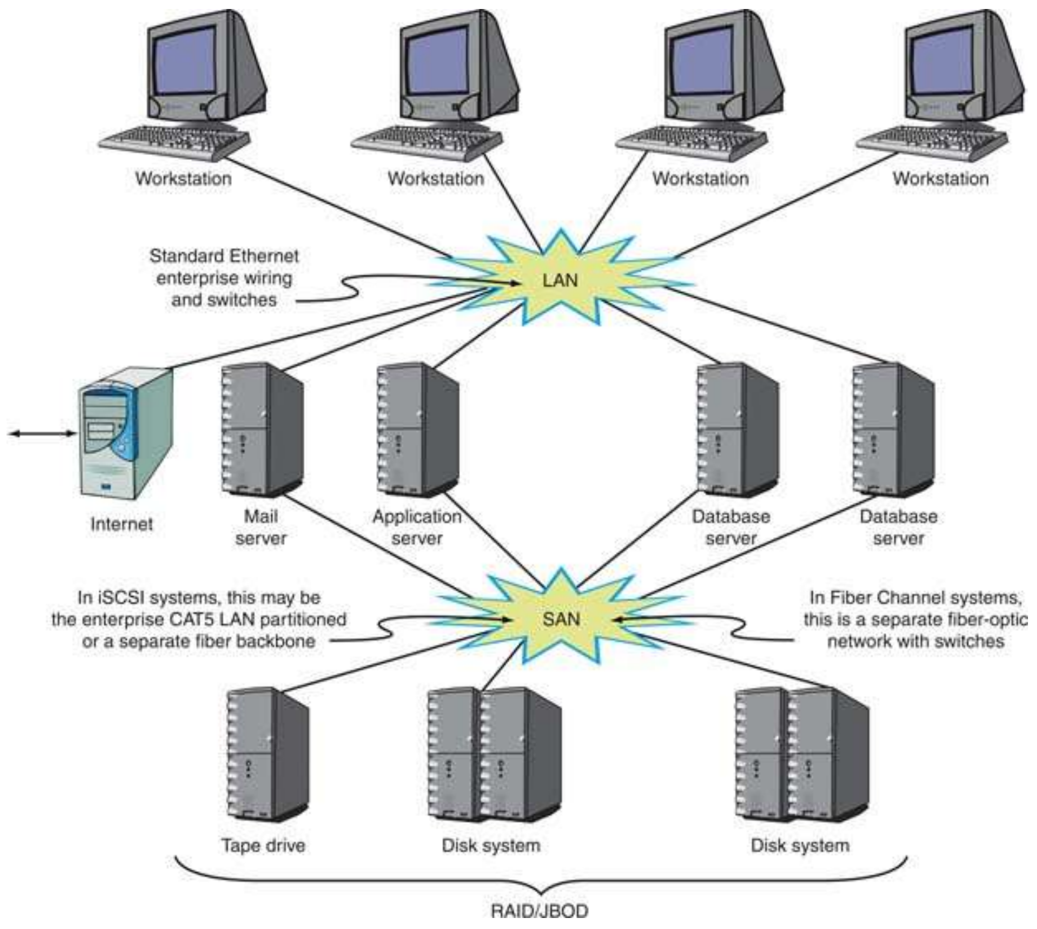

Workstation
Workstation
Workstation
Workstation
Standard Ethernet enterprise wiring and switches
LAN
Internet
Mail server
Application server
Database server
Database server
In iSCSI systems, this may be the enterprise CAT5 LAN partitioned or a separate fiber backbone
SAN
In Fiber Channel systems, this is a separate fiber-optic network with switches
Tape drive
Disk system
Disk system
RAID/JBOD

Figure 15-12: The basic architecture of a SAN.

15-3: Storage Area Networks

Fibre Channel

- **Fibre Channel** is an optical fiber transmission standard.
- It defines a protocol and a fiber-optic physical layer (PHY) that can be used to connect computers and storage systems in a loop or ring, point-to-point or through switches.
- Today systems transmit at 1, 2, 4, or 10 Gbps.
- A very high data rate is essential in a SAN if any large block of data is going to be accessed by a user in a reasonable time.

15-3: Storage Area Networks

Fibre Channel

- One of the primary advantages of the FC SAN is that it is inherently secure.
- Since it is not connected to the LAN or the Internet, it is essentially immune to outside hacking, virus, spam, or other attacks normally associated with the Internet.

15-3: Storage Area Networks

Internet SCSI

- FC is used in more than 90 percent of all SANs because of its speed, flexibility, and reliability.
- Its main downside is high cost.
- A lower-cost SAN connection system called **Internet SCSI (iSCSI)** has been developed recently.
- It uses standard off-the-shelf Ethernet components and TCP/IP software so widely available.

15-3: Storage Area Networks

Internet SCSI

- The primary benefit of an iSCSI SAN is its lower cost and use of existing LAN wiring or the Internet.
- The main disadvantage is that such systems are at risk to hacking, viruses, and other such security problems.
- This can be taken care of by using security software and data encryption methods, but these increase the cost and greatly slow down all data transmission operations.

15-3: Storage Area Networks

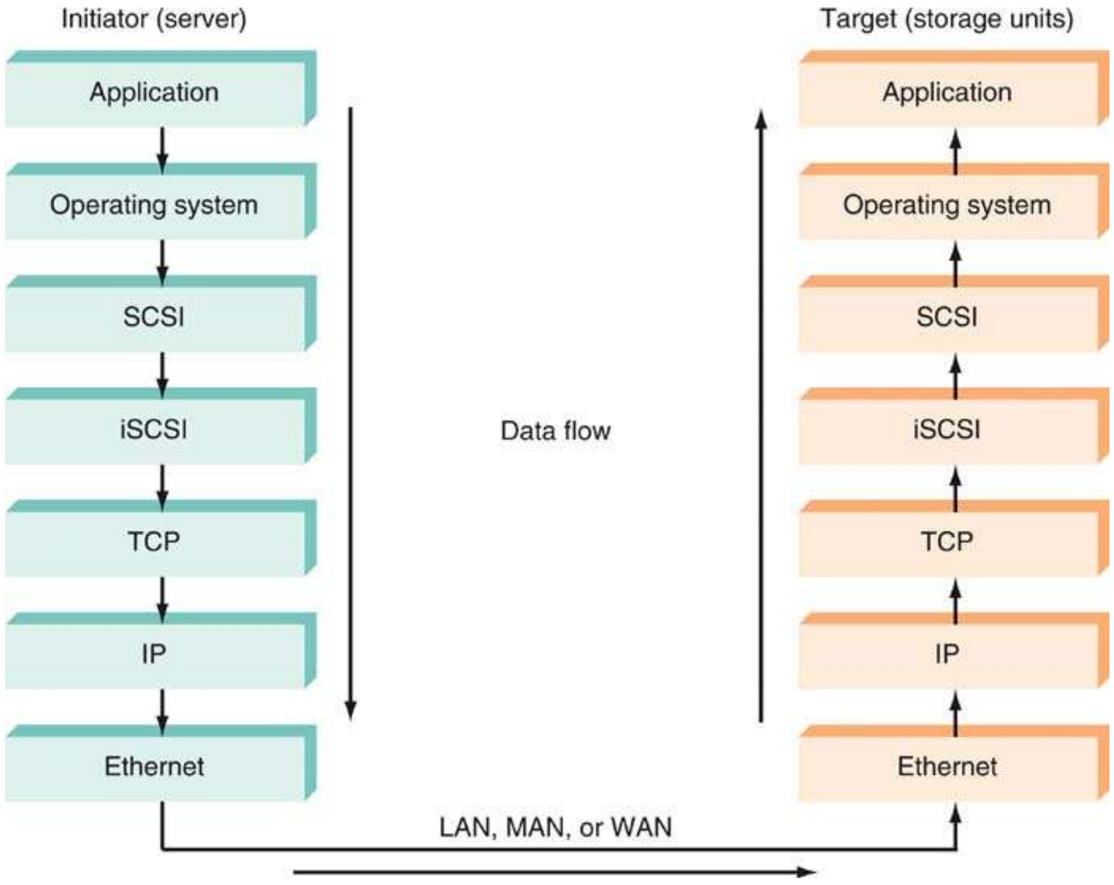


Figure 15-13: The sequence of operations for accessing data by using the iSCST protocol.

15-4: Internet Security

- One of the most important aspects of the Internet is **security** of the data being transmitted.
- **Security** refers to protecting the data from interception and protecting the sending and receiving parties from unwanted threats such as viruses and spam.
- It also means protecting the equipment and software used in the networks.

15-4: Internet Security

- The Internet or any network-connected computer is subject to threats by hackers, individuals who deliberately try to steal data or damage computer systems and software just for the challenge.
- Wireless systems are very vulnerable to hacker attacks because radio waves are easily picked up and used by anyone with an appropriate receiver.
- Over the past years, security for wireless systems has been developed and widely deployed.

15-4: Internet Security

- Most security measures are implemented in software.
- Some security techniques can be implemented in hardware such as data encryption chips.

15-3: Storage Area Networks

Types of Security Threats

- The most common form of threat is the ability of a hacker to link to an existing network and literally read the data being transmitted.
- Some types of connections permit disk files to be accessed, e-mail files to be read, data to be modified, and new unwanted data to be added.
- There are a huge number of specific ways in which data can be read, stolen, compromised, or corrupted.

15-4: Internet Security

Types of Security Threats: Viruses

- A virus is a small program designed to implement some nefarious action in a computer.
- A virus typically rides along with some other piece of information or program so that it can be surreptitiously inserted into the computer’s hard drive or RAM.
- The virus program is then executed by the processor to do its damage.

15-4: Internet Security

Types of Security Threats: Viruses

- Viruses typically interfere with the operating system, causing it to do unwanted things or not to perform certain functions.
- Viruses can affect the executable programs on the computer, the file directory, the data files themselves, and the boot programs.
- Some computer viruses are designed to spread themselves within the computer or to be retransmitted to others in e-mails. These viruses are called **worms.**

15-4: Internet Security

Types of Security Threats: Spam

- A more recent threat is unwanted ads and solicitations via e-mail called **spam.**
- Spam is not damaging, but it clogs up the e-mail system with huge quantities of unwanted data.
- It uses transmission time and bandwidth that could be used in a more productive way.
- Spam is not illegal, but you must remove the spam yourself, wasting your valuable time and memory space in your e-mail system.

15-4: Internet Security

Types of Security Threats: Spyware

- **Spyware** is software that monitors a computer and its user while he or she accesses the Internet or e-mail.
- It collects data about how that user uses the Internet such as Internet website access, shopping, etc.
- It uses this information to send unsolicited ads and spam.
- Some examples of dangerous practices are:
  - Capture of credit card numbers,
  - Delivery of unsolicited pop-up ads.

15-4: Internet Security

Types of Security Threats: Denial-of-Service (DoS) Attacks

- This is a process that transmits errors in the communications protocol and causes the computer to crash or hang up.
- This type of vandalism doesn’t steal information. It prevents the user from accessing the operating system, programs, data files, applications programs, or communications links.
- It is the easiest form of attack and serves no purpose other than to hurt others.

15-4: Internet Security

Security Measures: Encryption and Decryption

- Special software or hardware is used to protect data and prevent malicious hacking.
- **Encryption** is the process of obscuring information so that it cannot be read by someone else.
- It involves converting a message to some other form that makes it useless to the reader.
- **Decryption** is the reverse process that translates the encrypted message back to readable form.

15-4: Internet Security

Security Measures: Encryption and Decryption

- There are two basic types of encryption: **secret key encryption (SKE),** also called **private key encryption,** and **public key encryption (PKE).**
- There are dozens of different types of encryption methods.
- **Hash functions** are a kind of one-way encryption that allow you to determine if the original message has been changed in any way during transmission. Hash functions help to ensure data integrity.

15-4: Internet Security

Security Measures: Authentication

- **Authentication** is the process of verifying that you are who you say you are.
- Authentication ensures that the identities of the transmitting and receiving parties have not been stolen or simulated.
- Digital authentication allows computer users to access the Internet, other networks, computers, software, or resources such as bank accounts.
- It is used in most Internet transactions such as e-commerce.

15-4: Internet Security

Security Measures: Authentication

- The most common methods of authentication are the use of passwords or **personal identification numbers (PIN).**
- Passwords and PINs are often encrypted before transmission so they cannot be stolen.
- **Biometric methods** of identification are being used as security tightens with more and more transactions.
- Biometric ID methods are fingerprint scans, retinal eye scans, voiceprints, and video facial recognition.

15-4: Internet Security

Security Measures: Authentication

- The most commonly used process of authentication in network communications is the use of **digital certificates.**
- Also known as **certificate-based authentication,** this method uses hashing and public key encryption to verify identity in various transactions.
- Companies known as **certification authorities (CAs)** issue public keys to individuals or organizations and vouch for their identity.

15-4: Internet Security

Security Measures: Secure Socket Layer (SSL)

- The processes of encryption/decryption and authentication are combined into a protocol known as the **Secure Socket Layer (SSL).**
- The process makes the exchange of private information such as credit card numbers safe and secure.
- E-commerce would not exist without SSL.
- A more advanced version of SSL called **Transport Layer Security (TLS)** usually resides in layers 5, 6, or 7 of the OSI model.

15-4: Internet Security

Security Measures: Firewalls

- A **firewall** is a piece of software that monitors network transmissions and inspects the incoming information to see if it conforms to a set of guidelines established by the software or the organization or person owning the network.
- The firewall controls the flow of traffic from the Internet to a LAN or PC or between LANs or other networks.
- The most common type of firewall operates at the network layer in the OSI model.

15-4: Internet Security

Security Measures: Firewalls

- Firewalls are the first line of defense against intrusions by unwanted sources.
- Today, any computer connected to the Internet should have a firewall.
- These are available as a software program loaded into a PC that screens according to the guidelines set up by the software producer.

15-4: Internet Security

Security Measures: Antivirus, Antispam, and Antispyware Software

- Antivirus and antispyware programs scan all files on the hard drive either automatically or on command.
- The antivirus software looks for a pattern of code unique to each virus. When it is identified, the software removes the virus or quarantines and isolates the infected file.
- Antispyware works the same way by scanning all files, searching for patterns that designate a spyware program. It then removes the program.

15-4: Internet Security

Security Measures: Virtual Private Network (VPN).

- One method of LAN security uses software to block off segments of a network or create a subnetwork using software to assign access only to authorized users.
- This is referred to as a **virtual LAN** or **VLAN**.
- A popular alternative is to create a secure connection through the Internet by using a **virtual private network (VPN).**
- In a VPN, the data to be transmitted is encrypted, encapsulated in a special packet, and then sent over the Internet.

15-4: Internet Security

Security Measures: Wireless Security

- Security in wireless systems is important because it is easy to capture a radio signal containing important information.
- A directional antenna and sensitive receiver designed for the specific wireless service, such as a wireless LAN and a computer, are needed.
- Wireless data can be protected by encryption, and a number of special methods have been developed especially for wireless systems.

Chapter 2

Network Models

2.1 LAYERED TASKS

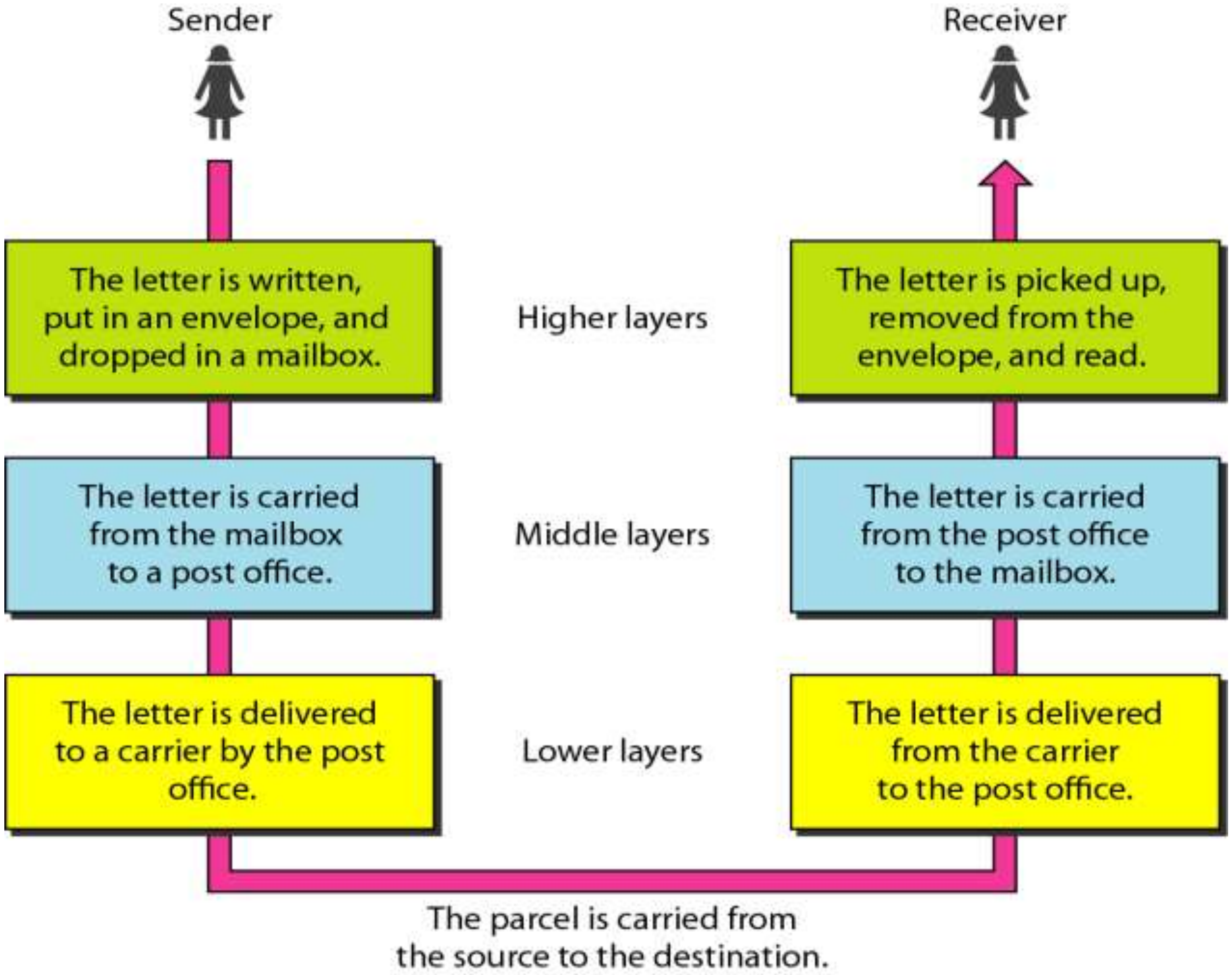
We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal mail. The process of sending a letter to a friend would be complex if there were no services available from the post office.

Topics discussed in this section:

Sender, Receiver, and Carrier
Hierarchy

Layered Tasks

- Sender, Receiver and Carrier


Sender
Receiver
The letter is written, put in an envelope, and dropped in a mailbox.
Higher layers
The letter is picked up, removed from the envelope, and read.
The letter is carried from the mailbox to a post office.
Middle layers
The letter is carried from the post office to the mailbox.
The letter is delivered to a carrier by the post office.
Lower layers
The letter is delivered from the carrier to the post office.
The parcel is carried from the source to the destination.

Layered Tasks

- Hierarchy
  - Higher Layer
  - Middle Layer
  - Lower Layer

- Services
  - The Each layer uses the services of the layer immediately below it.

2.2 THE OSI MODEL

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

ISO is the organization.
OSI is the model.

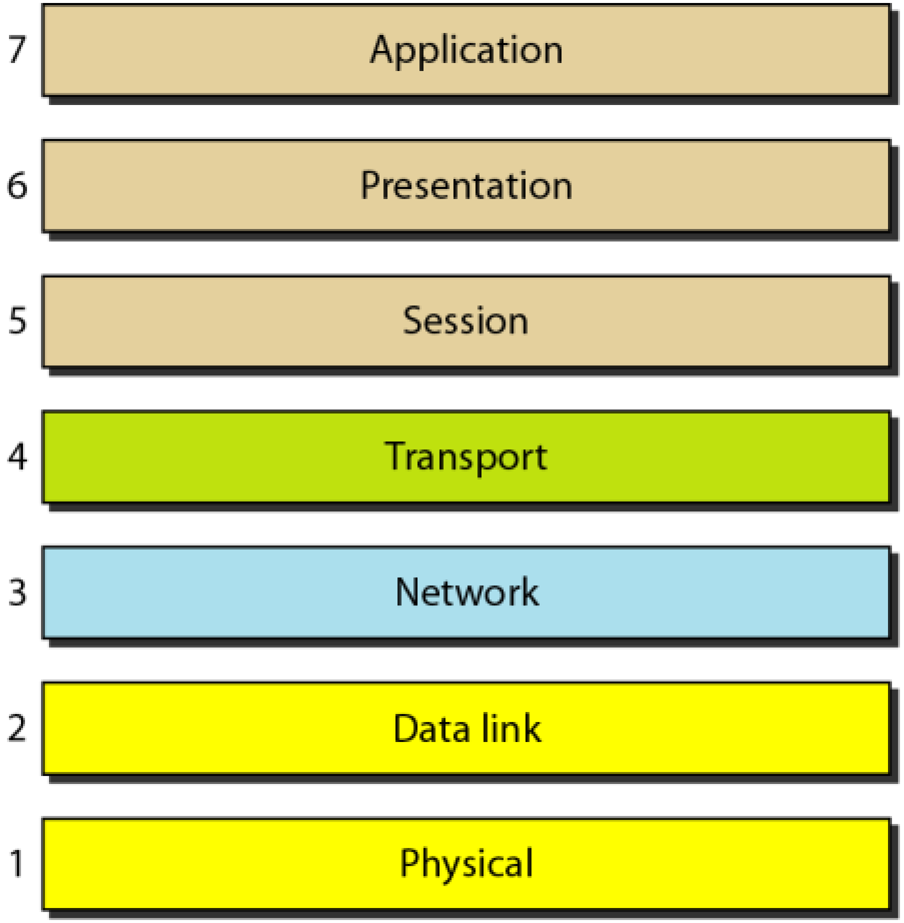
Topics discussed in this section:

Layered Architecture
Peer-to-Peer Processes
Encapsulation

Layered Architecture

- The OSI model is composed of seven layers ;
  - Physical (layer1), Data link (layer2), Network (layer3)
  - Transport (layer4), Session (layer5), Presentation (layer6)
  - Application (layer7)
- Layer
  - Designer identified which networking functions had related uses and collected those functions into discrete groups that became the layers.
  - The OSI model allows complete interoperability between otherwise incompatible systems.
  - The Each layer uses the services of the layer immediately below it.

Layered Architecture (cont'd)



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data link

1 Physical

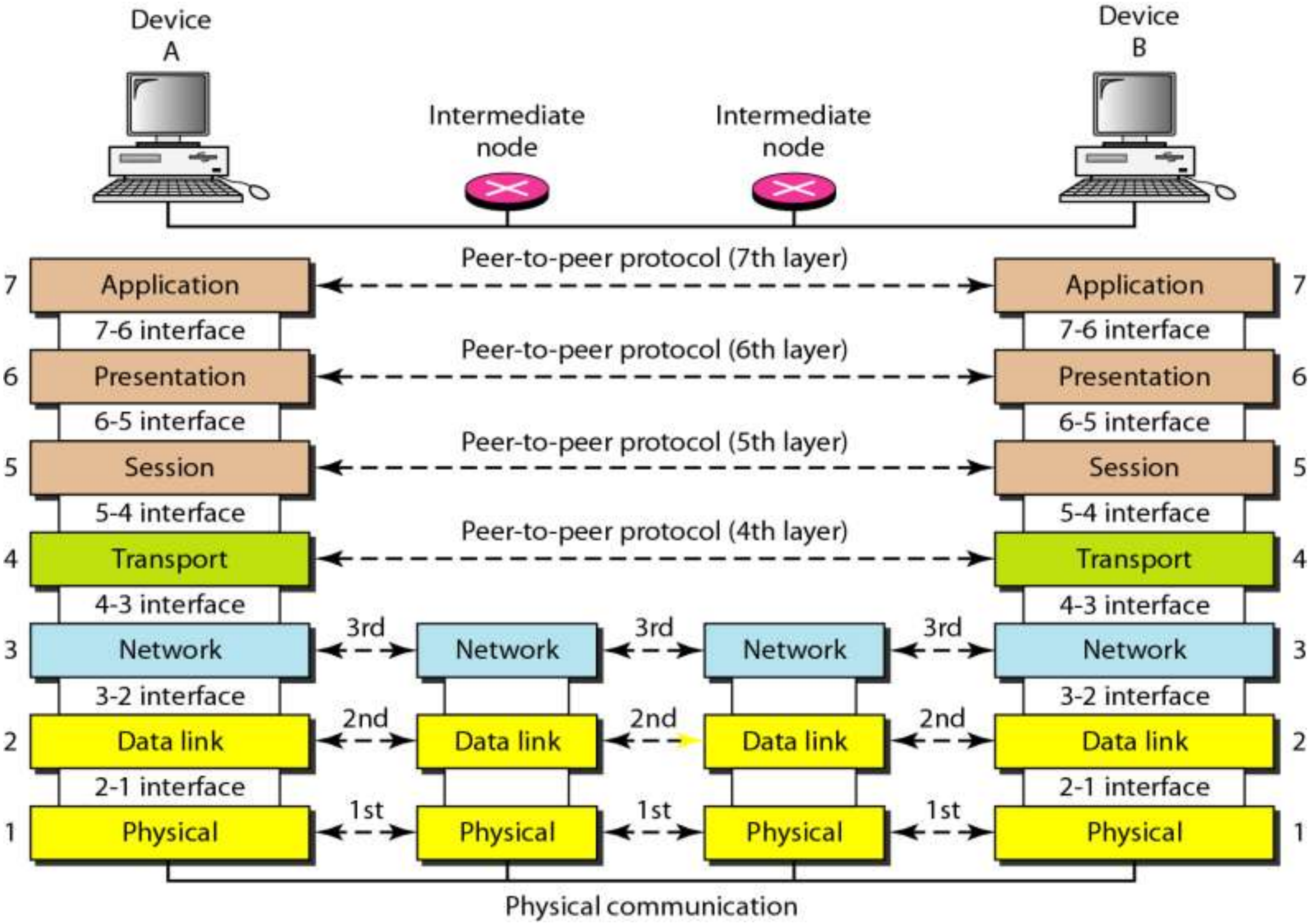
Figure 2.2 ***Seven layers of the OSI model***

Peer-to-peer Processes

- Layer x on one machine communicates with layer x on another machine - called Peer-to-Peer Processes.
- Interfaces between Layers
  - Each interface defines what information and services a layer must provide for the layer above it.
  - Well defined interfaces and layer functions provide modularity to a network
- Organizations of the layers
  - Network support layers : Layers 1, 2, 3
  - User support layer : Layer 5, 6, 7
    - It allows interoperability among unrelated software systems
  - Transport layer (Layer 4) : links the two subgroups

Peer-to-peer Processes (cont'd)

Figure 2.3 *The interaction between layers in the OSI model*

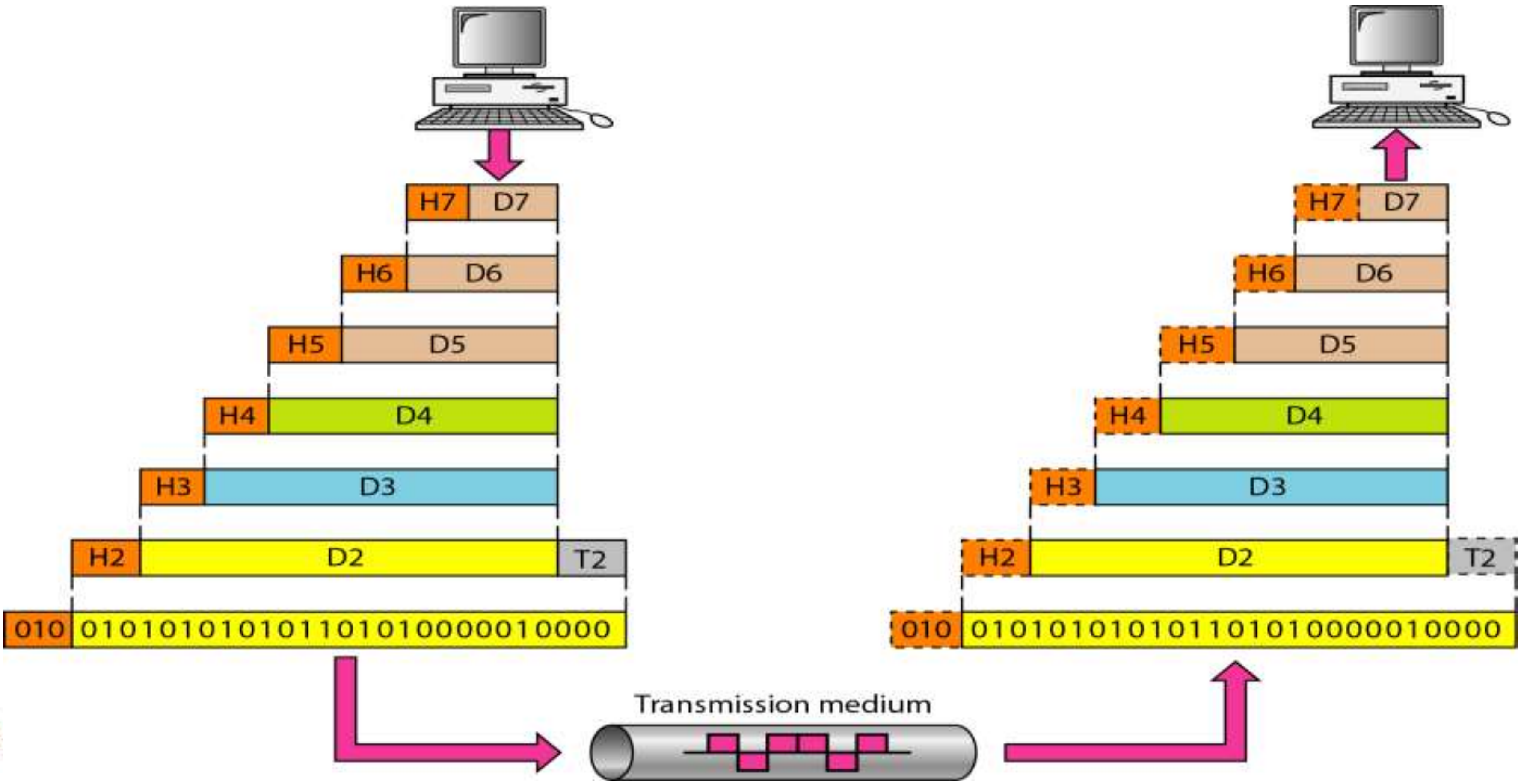


Kyung Hee University

Peer-to-peer Processes (cont’d)

Figure 2.4 *An exchange using the OSI model*

- ❑ **The data portion of a packet at level N-1 carries the whole packet from level N. – The concept is called encapsulation.**



2.3 LAYERS IN THE OSI MODEL

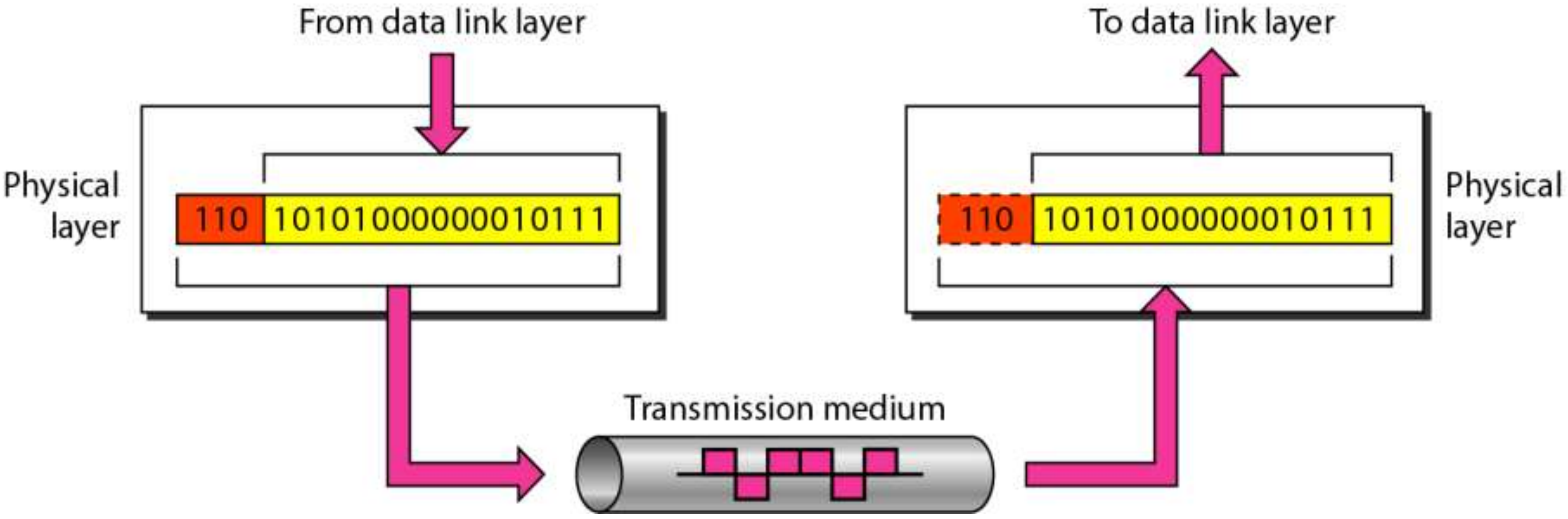
In this section we briefly describe the functions of each layer in the OSI model.

Topics discussed in this section:

Physical Layer
Data Link Layer
Network Layer
Transport Layer
Session Layer
Presentation Layer
Application Layer

Physical Layer

- Physical layer coordinates the functions required to transmit a bit stream over a physical medium.



- The physical layer is responsible for movements of individual bits from one hop (node) to the next.

Physical Layer

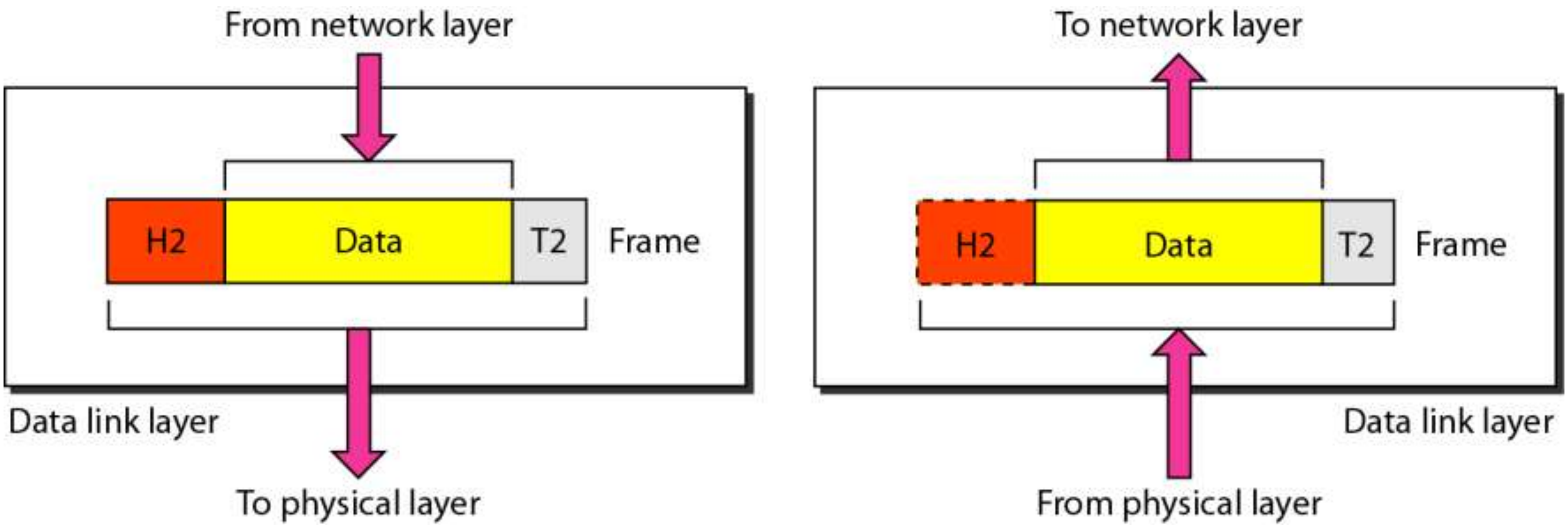
- Physical layer is concerned with the following:

(deal with the mechanical and electrical specification of the primary connections: cable, connector)

  - Physical characteristics of interfaces and medium
  - Representation of bits
  - Data rate : transmission rate
  - Synchronization of bits
  - Line configuration
  - Physical topology
  - Transmission mode

Data Link Layer

- The data link layer is responsible for moving frames from one hop (node) to the next.

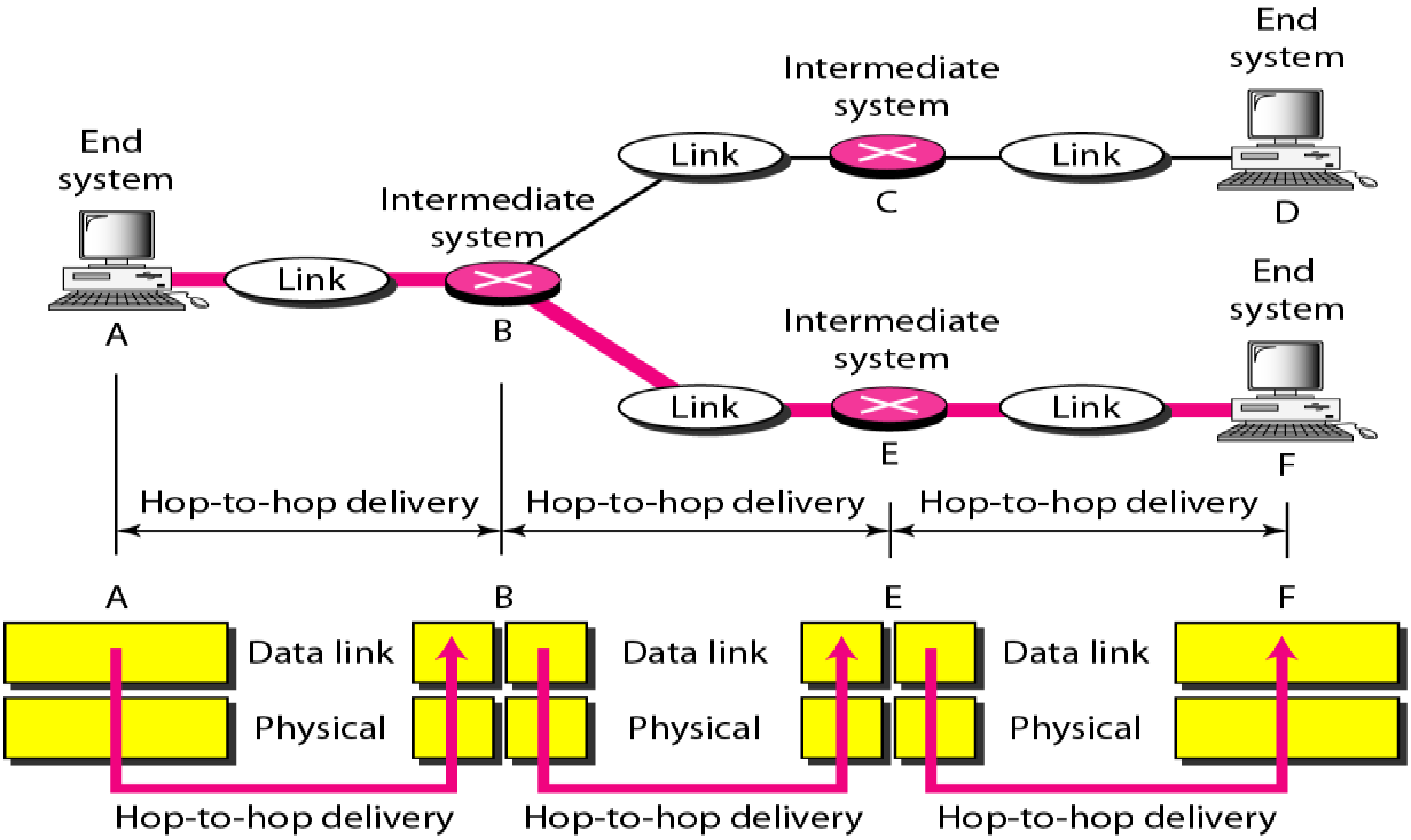


Data Link Layer

- Major duties
  - Framing
  - Physical addressing
  - Flow control
  - Error control
  - Access control

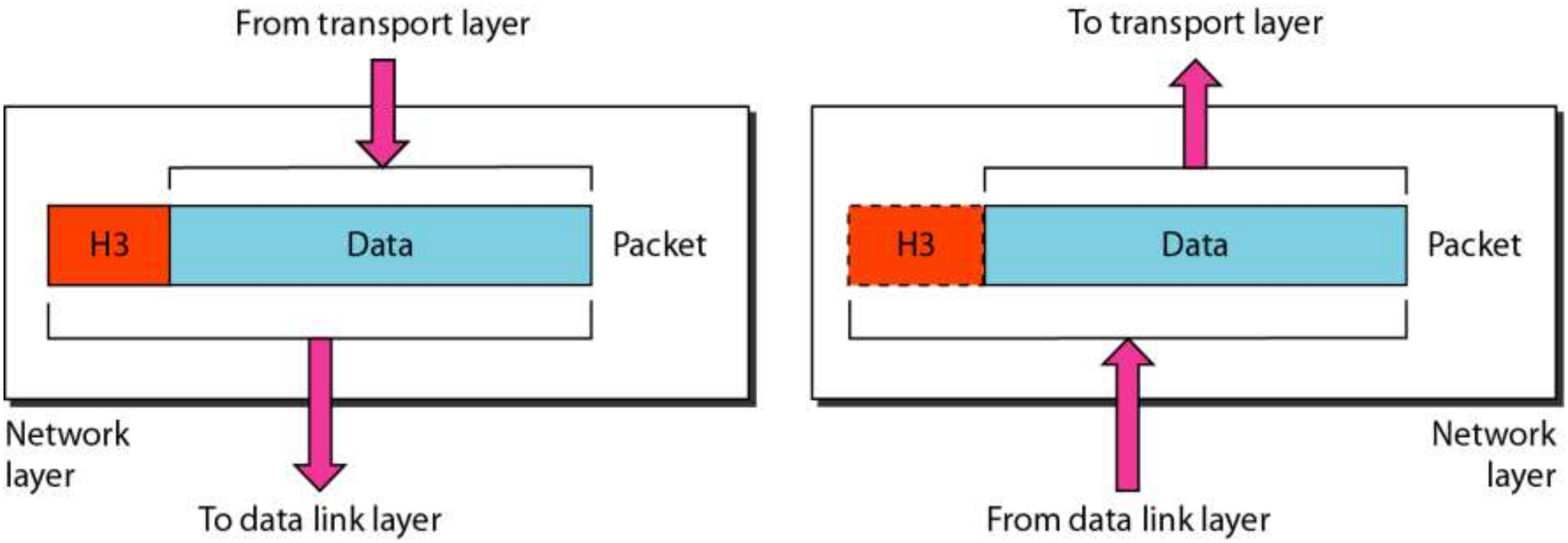
Data Link Layer

- Hop-to-hop (node-to-node) delivery



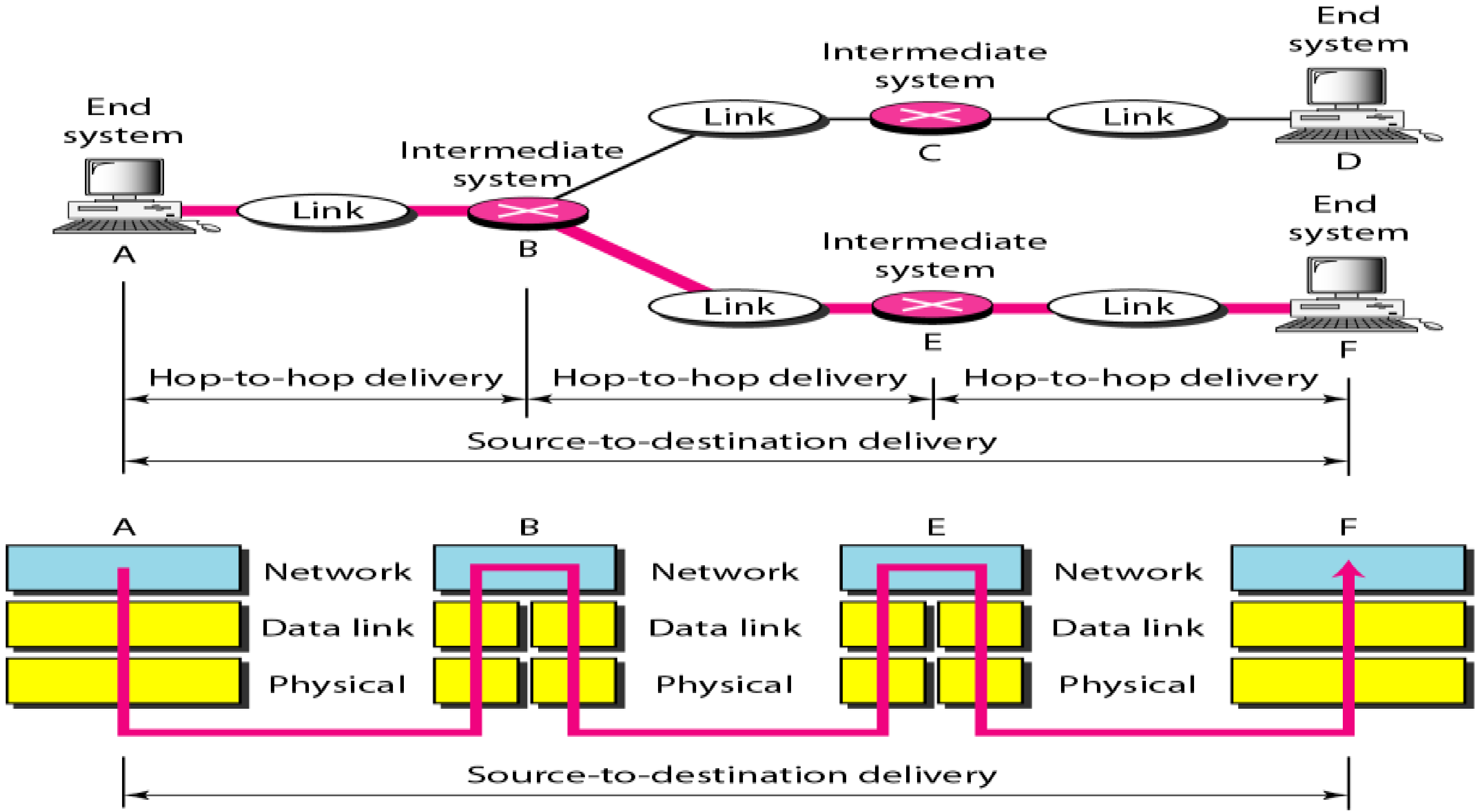
Network Layer

- The network layer is responsible for the delivery of individual packets from the source host to the destination host.



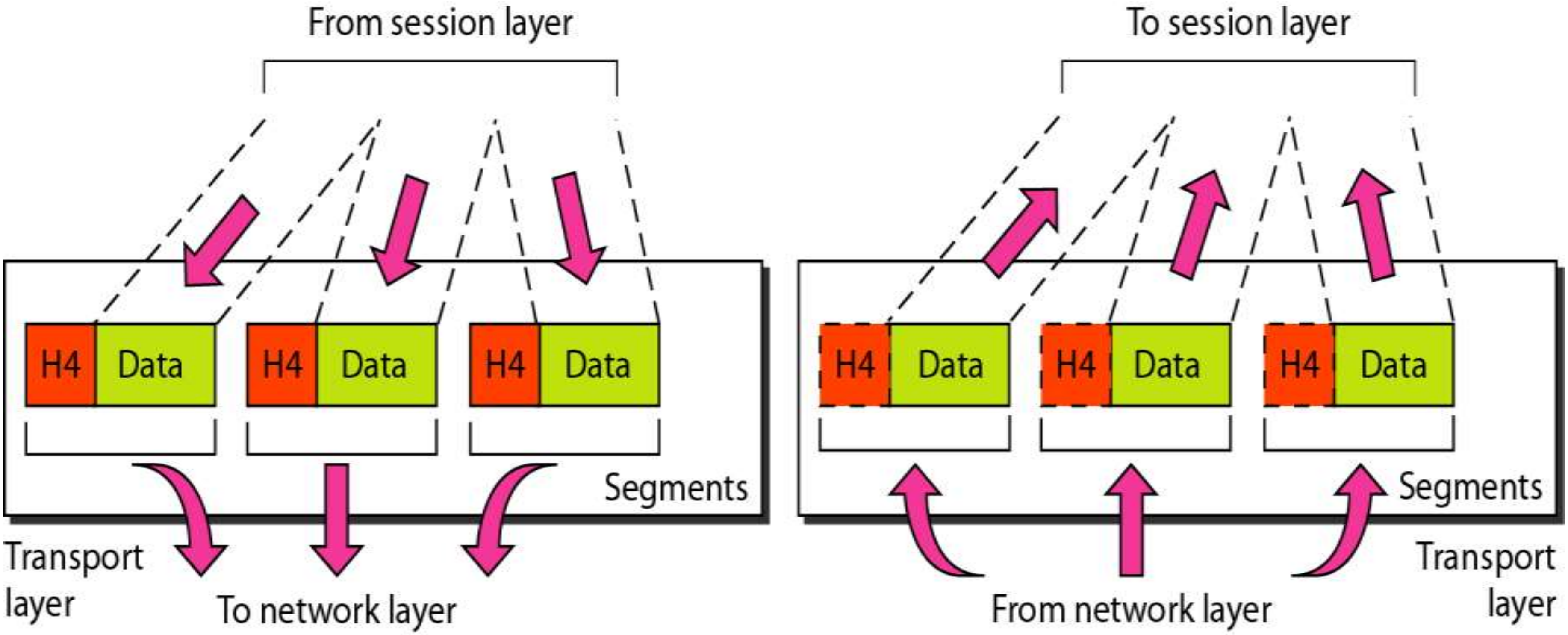
Network Layer

- Logical addressing
- Routing

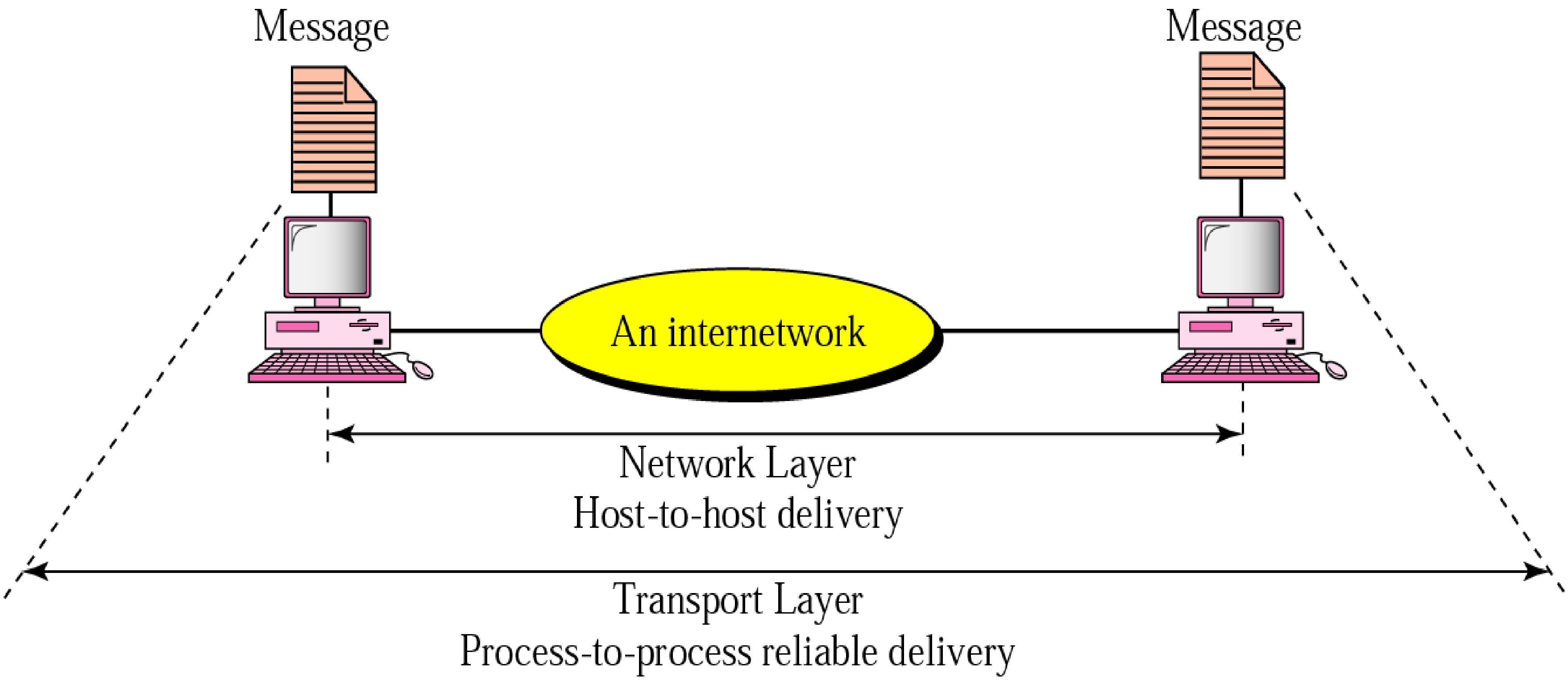


Transport Layer

❑ The transport layer is responsible for the delivery of a message from one process to another.



Transport Layer

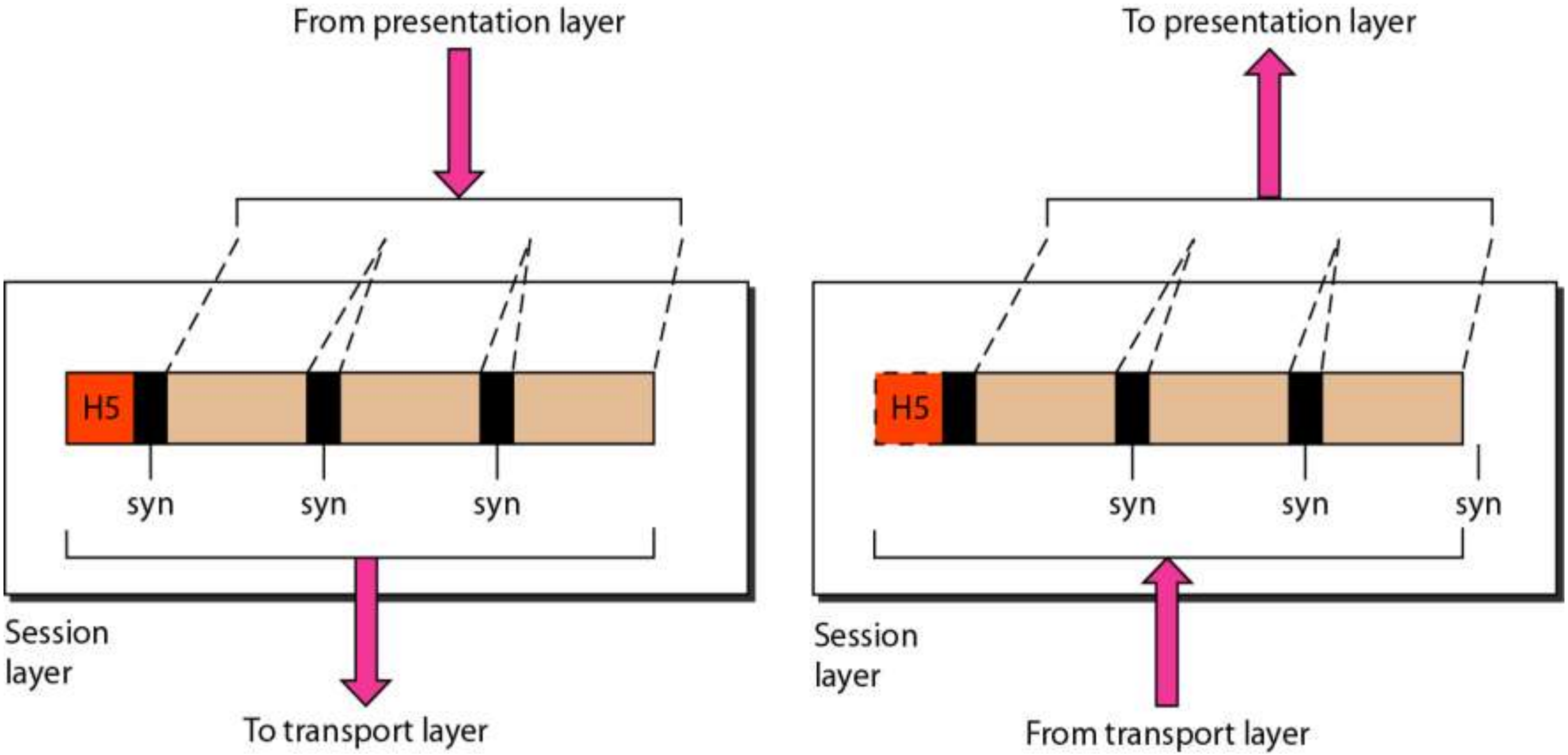


Transport Layer

- ❑ Service port addressing
- ❑ Segmentation and reassembly
- ❑ Connection control
- ❑ Flow control
- ❑ Error control

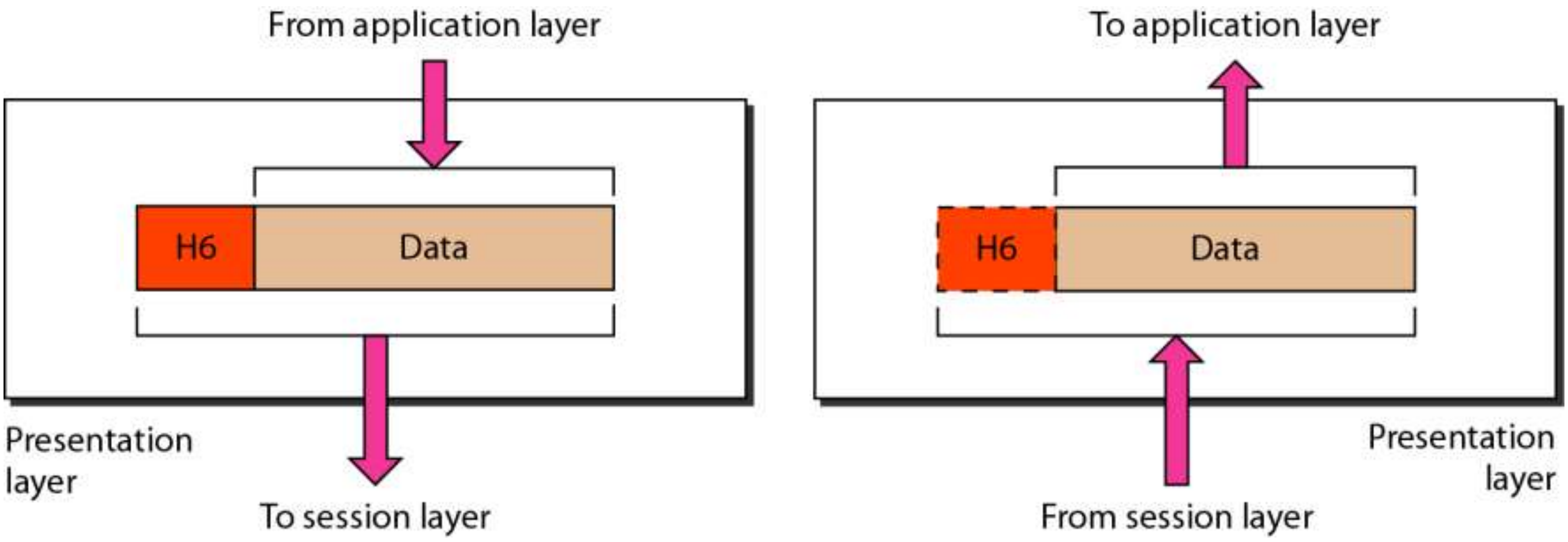
Session Layer

- The session layer is responsible for dialog control and synchronization.



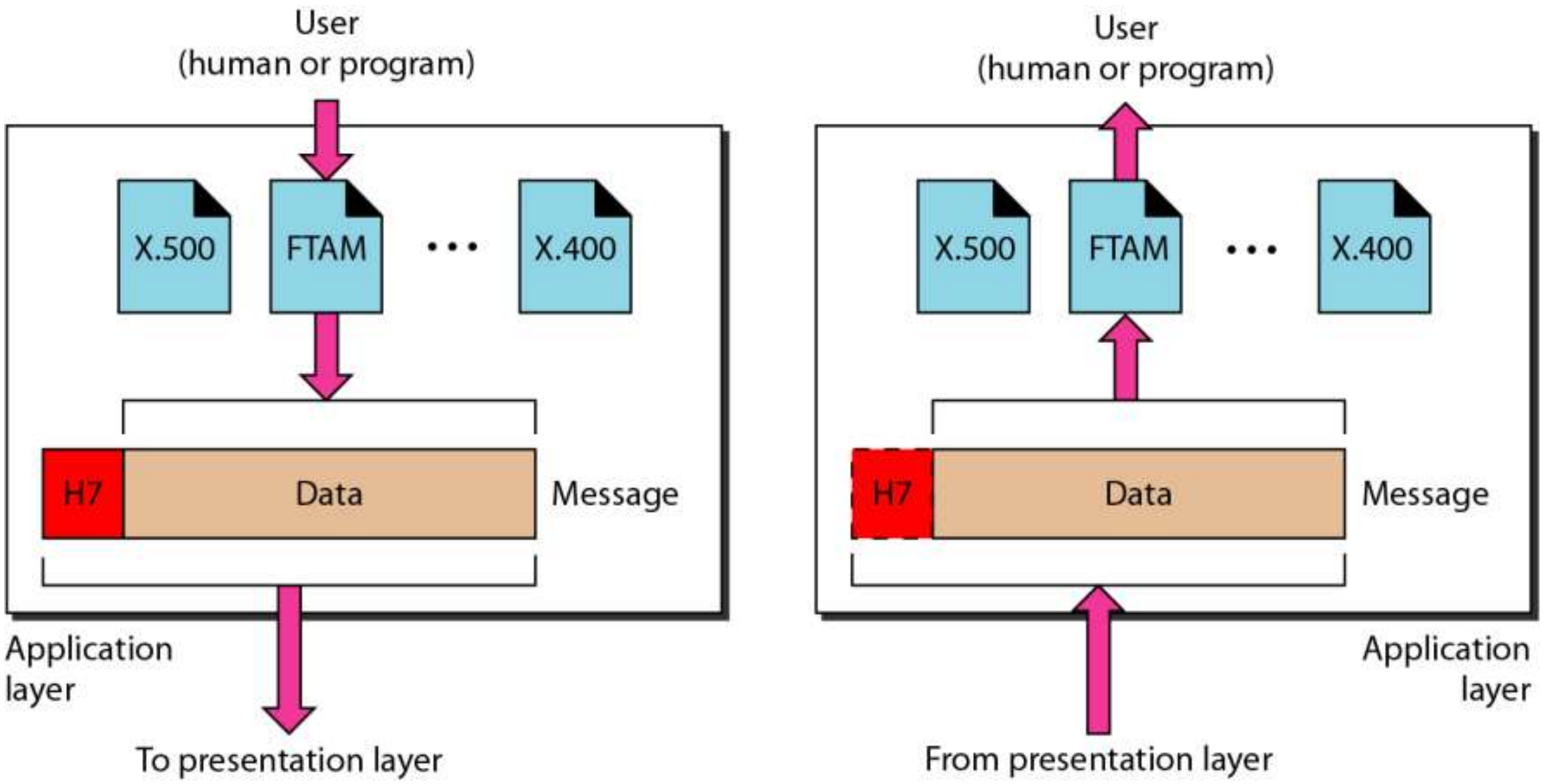
Presentation Layer

- The presentation layer is responsible for translation, compression, and encryption



Application Layer

- The application layer is responsible for providing services to the user.

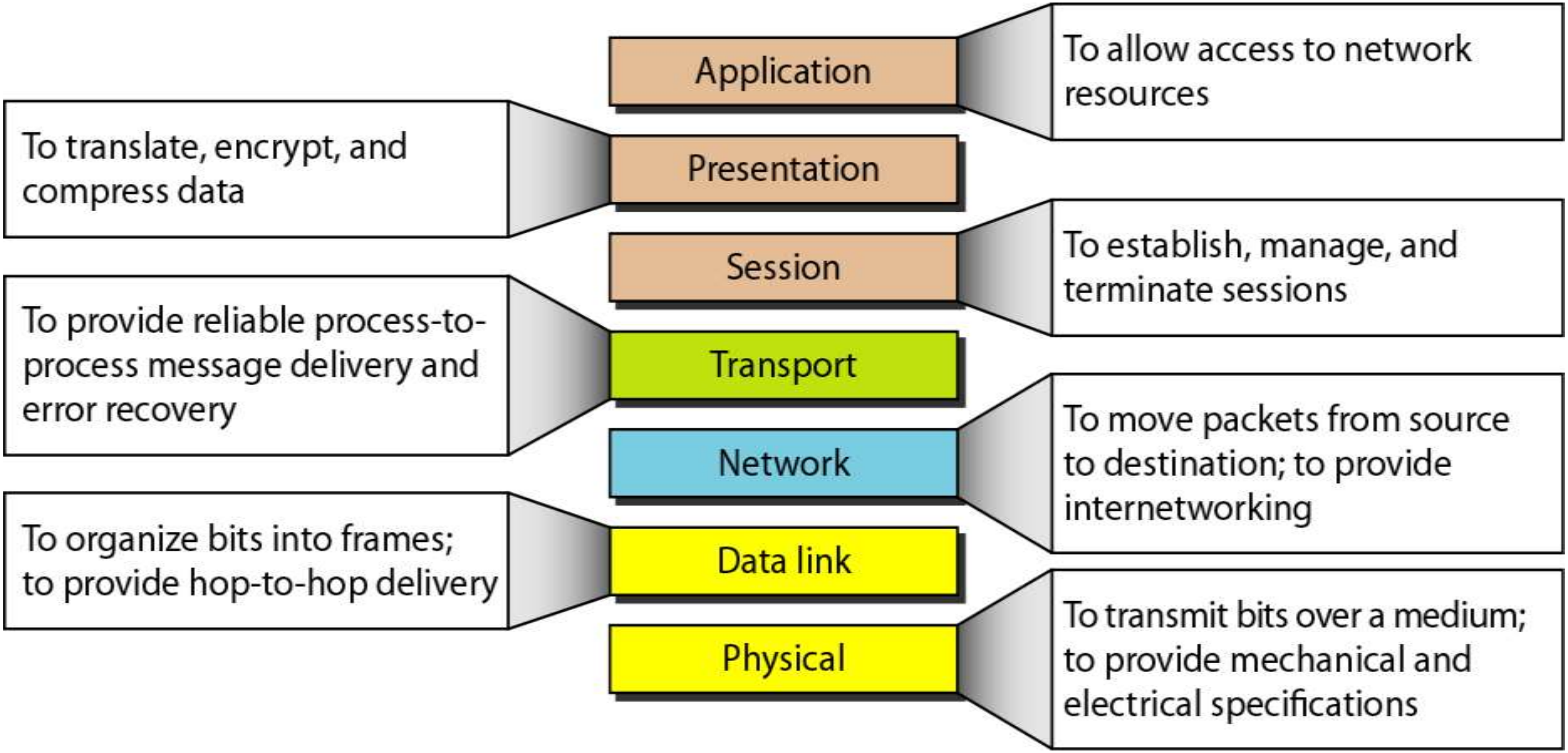


Application Layer

- The major duties of the application
  - Network virtual terminal
  - File transfer, access, and management
  - Mail services
  - Directory services

Summary of Layers

Figure 2.15 *Summary of layers*


Application
To allow access to network resources
To translate, encrypt, and compress data
Presentation
Session
To establish, manage, and terminate sessions
To provide reliable process-to-process message delivery and error recovery
Transport
Network
To move packets from source to destination; to provide internetworking
To organize bits into frames; to provide hop-to-hop delivery
Data link
Physical
To transmit bits over a medium; to provide mechanical and electrical specifications

2.4 TCP/IP PROTOCOL SUITE

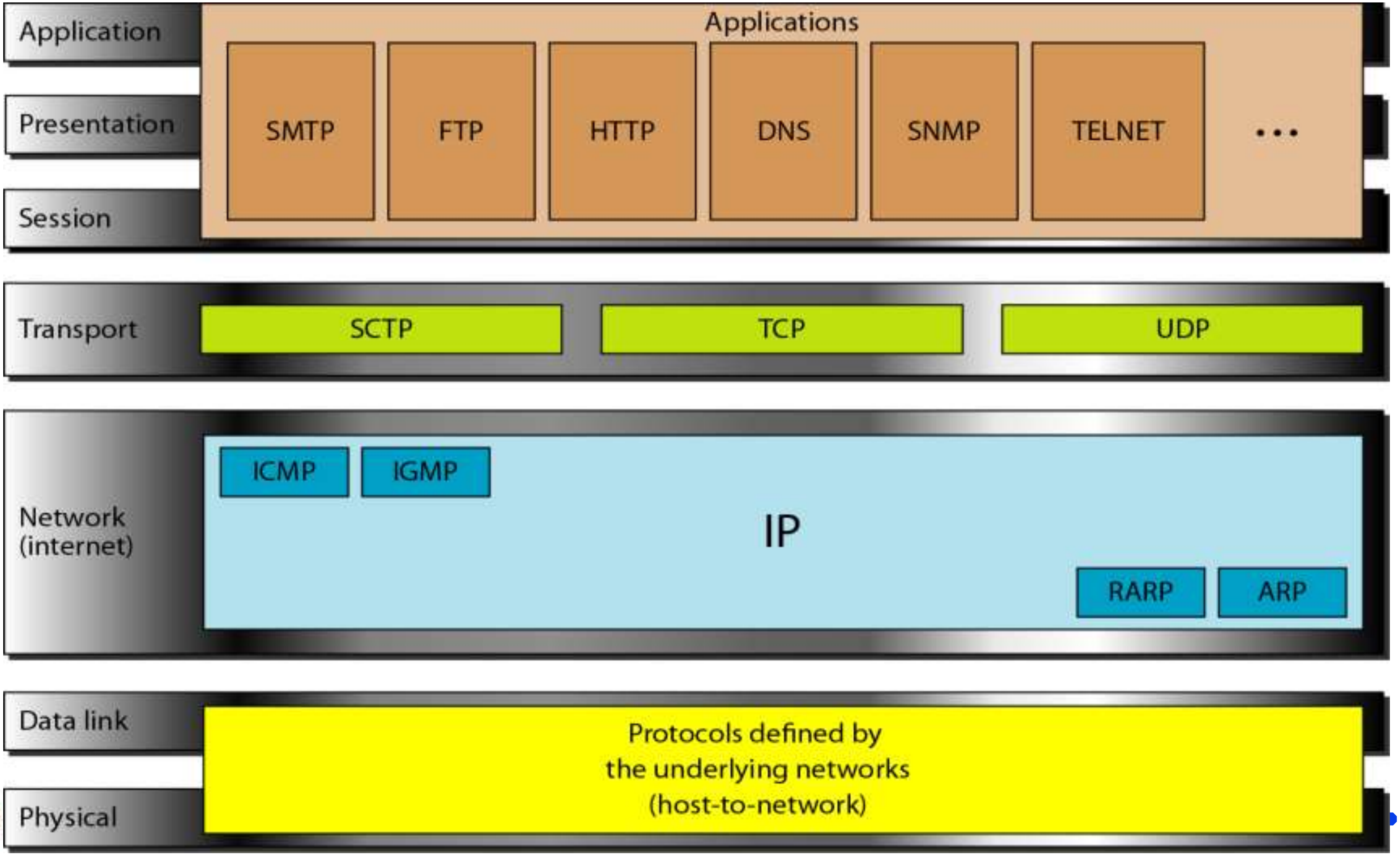
The layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.

Topics discussed in this section:

Physical and Data Link Layers
Network Layer
Transport Layer
Application Layer

TCP/IP Protocol Suite

Figure 2.16 ***TCP/IP and OSI model***



Physical and Data Link Layers

- At the physical and data link layers, TCP/IP does not define any specific protocol.
- It supports all the standard and proprietary protocols.
- A network in a TCP/IP internetwork can be a local-area network or a wide-area network.

Network Layer

- TCP/IP supports the Internetworking Protocol.
- IP uses four supporting protocols : ARP, RARP, ICMP, and IGMP.
  - IP (Internetworking Protocol)
  - ARP (Address Resolution Protocol)
  - RARP (Reverse Address Resolution Protocol)
  - ICMP (Internet Control Message Protocol)
  - IGMP (Internet Group Message Protocol)

Transport Layer

- The transport layer was represented in TCP/IP by two protocols : TCP and UDP.
  - IP is a host-to-host protocol
  - TCP and UDP are transport level protocols responsible for delivery of a message from a process to another process.
- UDP (User Datagram Protocol)
- TCP (Transmission Control Protocol)
- SCTP (Stream Control Transmission Protocol)

Application Layer

- The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model.
- Many protocols are defined at this layer.

2-5 ADDRESSING

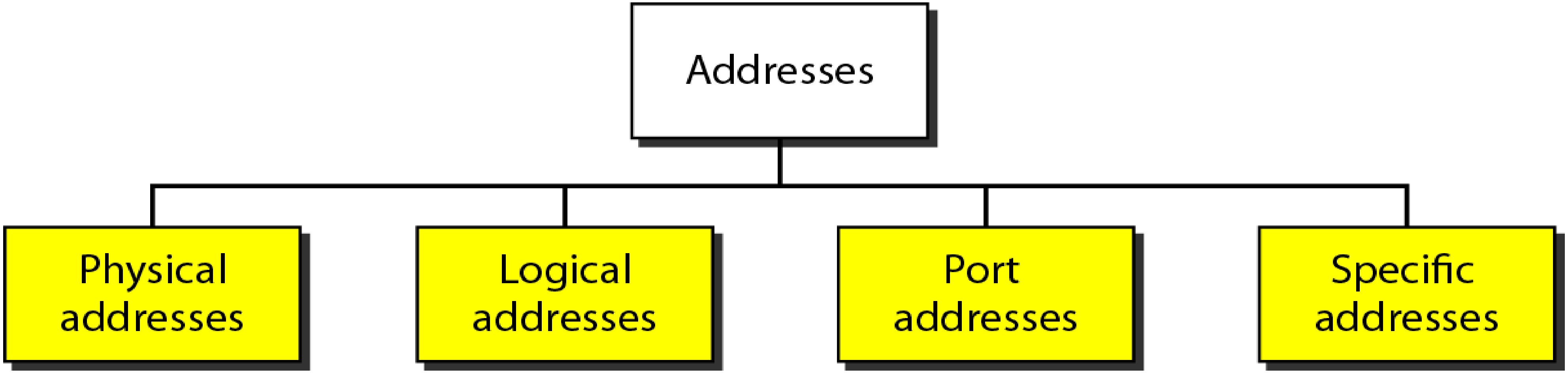
Four levels of addresses are used in an internet employing the TCP/IP protocols: physical, logical, port, and specific.

Topics discussed in this section:

Physical Addresses
Logical Addresses
Port Addresses
Specific Addresses

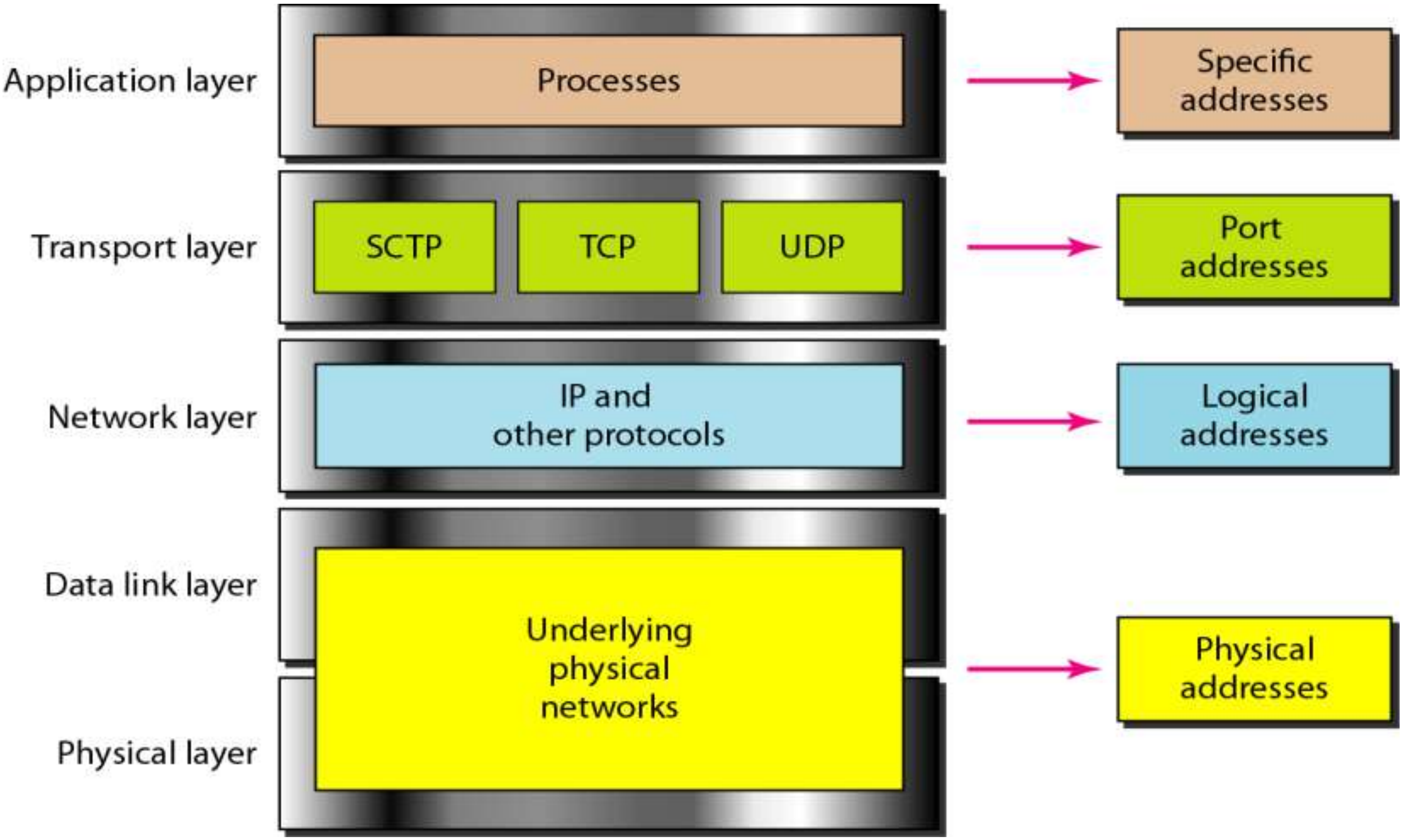
Addresses

Figure 2.17 ***Addresses in TCP/IP***



Physical Addresses

Figure 2.18 ***Relationship of layers and addresses in TCP/IP***



Physical Addresses

- The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN.
- It is included in the frame used by the data link layer.
  - The physical addresses have authority over the network (LAN or WAN).
  - The size and format of these addresses vary depending on the network.

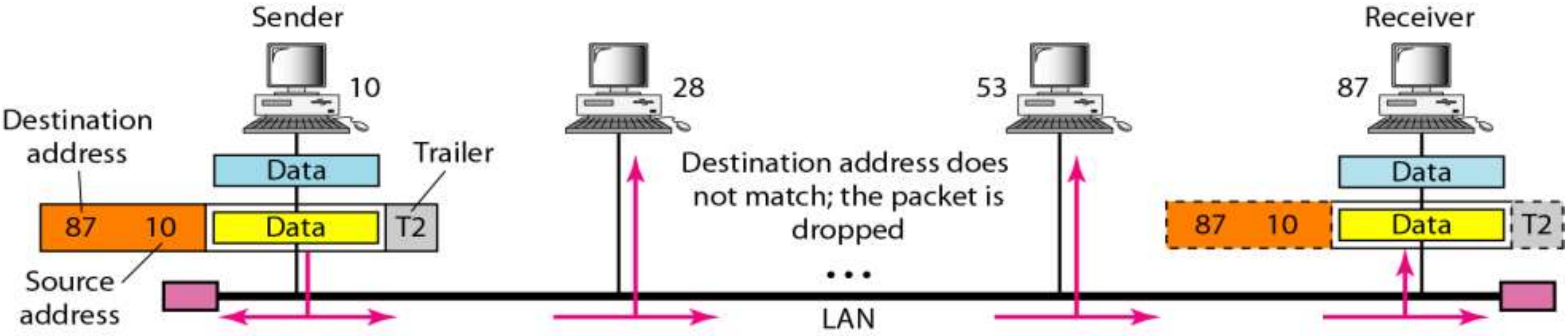
Physical Addresses (cont'd)

Example 2.1

In Figure 2.19 a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (bus topology LAN). As the figure shows, the computer with physical address 10 is the sender, and the computer with physical address 87 is the receiver.

Physical Addresses (cont'd)

Figure 2.19 ***Physical addresses***



Physical Addresses (cont'd)

Example 2.2

As we will see in Chapter 13, most local-area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below:

07:01:02:01:2C:4B

A 6-byte (12 hexadecimal digits) physical address.

Logical Addresses

- Logical addresses are necessary for universal communications that are independent of underlying physical networks.
  - Physical addresses are not adequate in an internetwork environment where different networks can have different address formats.
  - A universal addressing system is needed in which host can be identified uniquely, regardless of the underlying physical network.

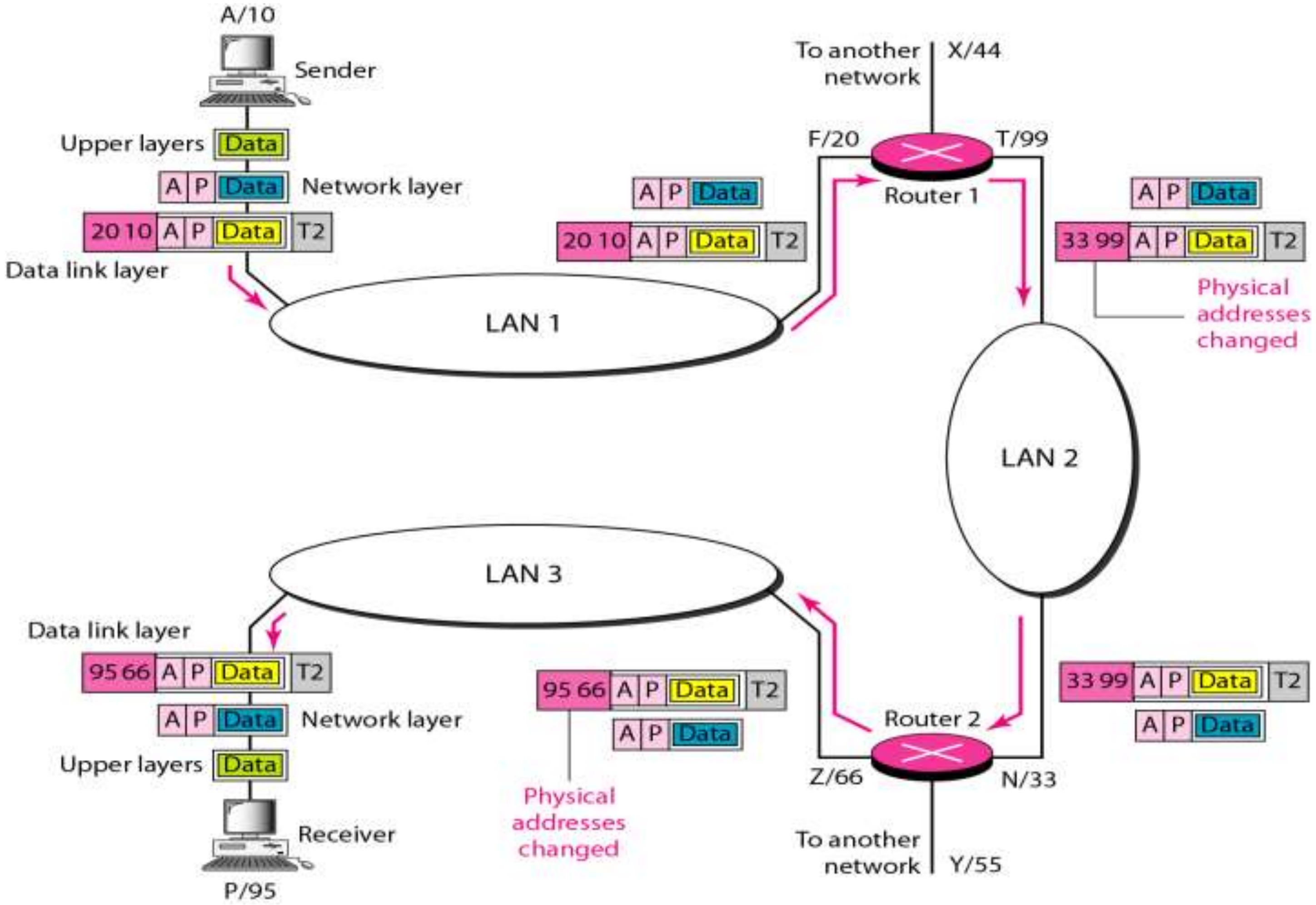
Logical Addresses (cont'd)

Example 2.3

Figure 2.20 shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses. Each router, however, is connected to three networks (only two are shown in the figure). So each router has three pairs of addresses, one for each connection.

Logical Addresses (cont'd)

Figure 2.20 ***IP addresses***



The physical addresses will change from hop to hop, but the logical addresses usually remain the same.

Port Addresses

- The IP and the physical address are necessary for a quantity of data to travel from a source to the destination host.
- The end object of Internet communication is a process communicating with another process.
- For these processes to receive data simultaneously, we need a method to label assigned to a process is called a port address.
- A port address in TCP/IP is 16 bits in length.

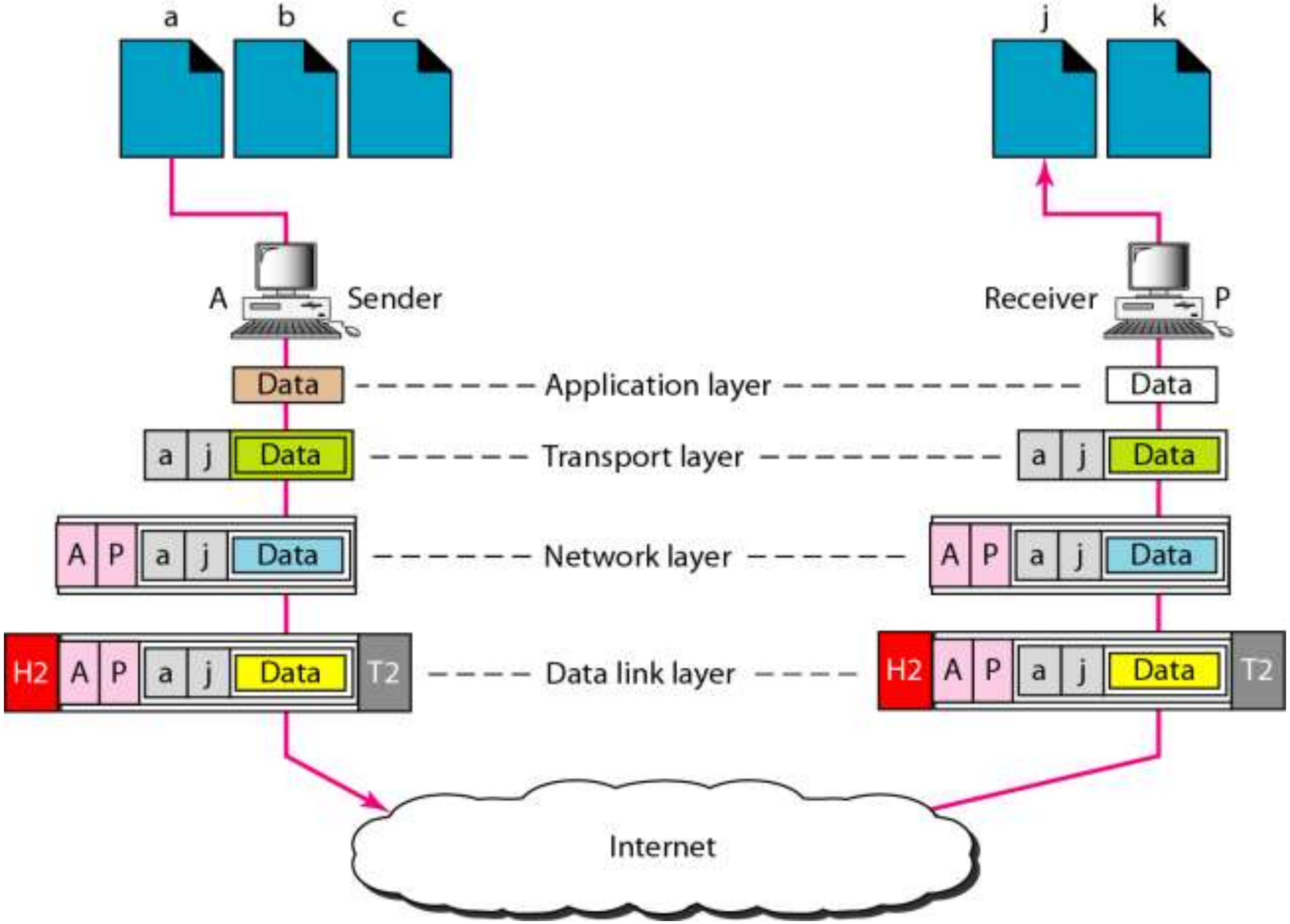
Port Addresses (cont'd)

Example 2.4

Figure 2.21 shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses a, b, and c. The receiving computer is running two processes at this time with port addresses j and k. Process a in the sending computer needs to communicate with process j in the receiving computer. Note that although physical addresses change from hop to hop, logical and port addresses remain the same from the source to destination.

Port Addresses (cont'd)

Figure 2.21 ***Port addresses***



The physical addresses will change from hop to hop, but the logical and port addresses usually remain the same.

Port Addresses (cont'd)

Example 2.5

As we will see in Chapter 23, a port address is a 16-bit address represented by one decimal number as shown.

753

A 16-bit port address represented as one single number.

Specific Addresses

- Some applications have user-friendly addresses that are designed for that specific address.
  - E-mail address
  - URL (Universal Resource Locator)

Q & A

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*

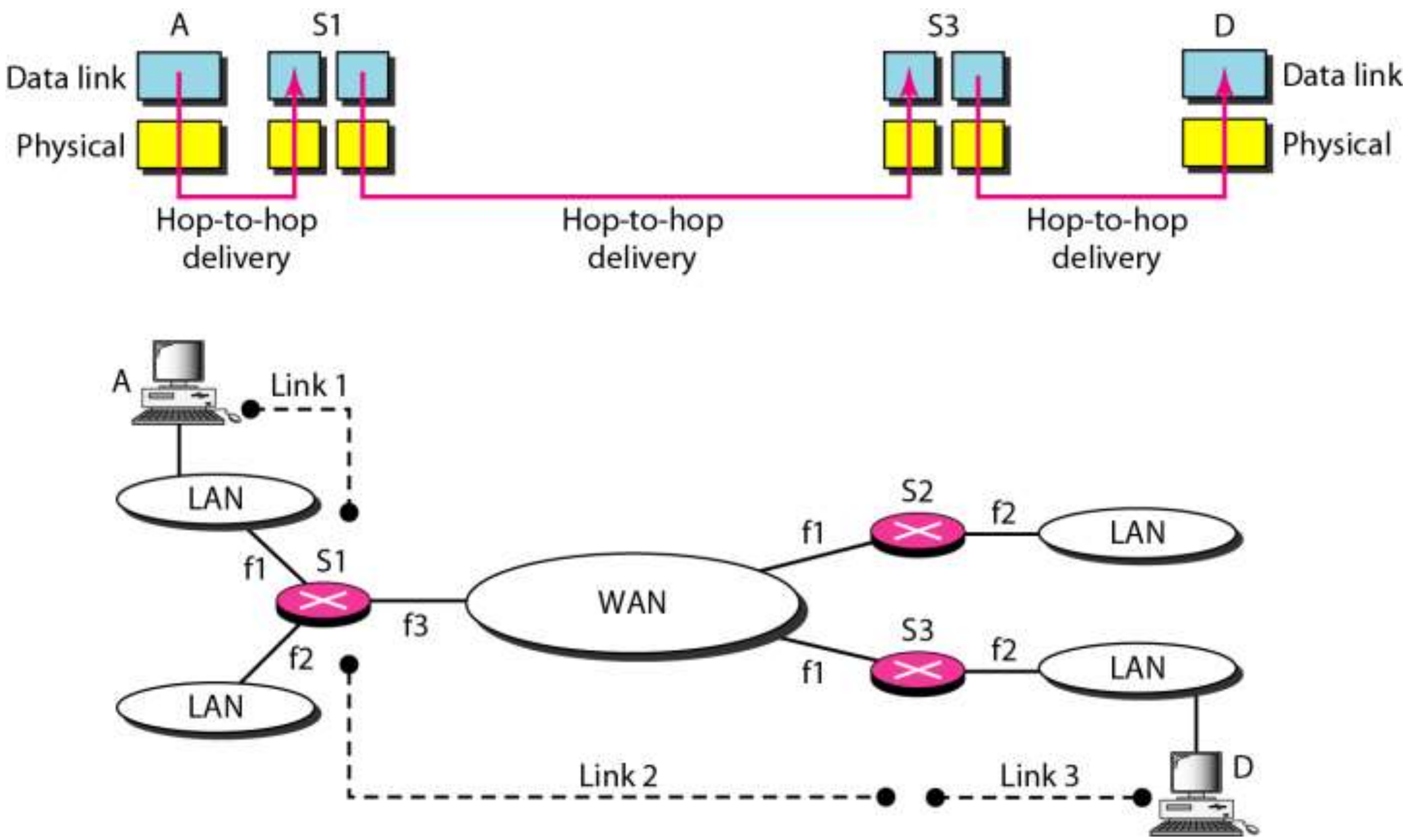


Figure 20.2 *Network layer in an internetwork*

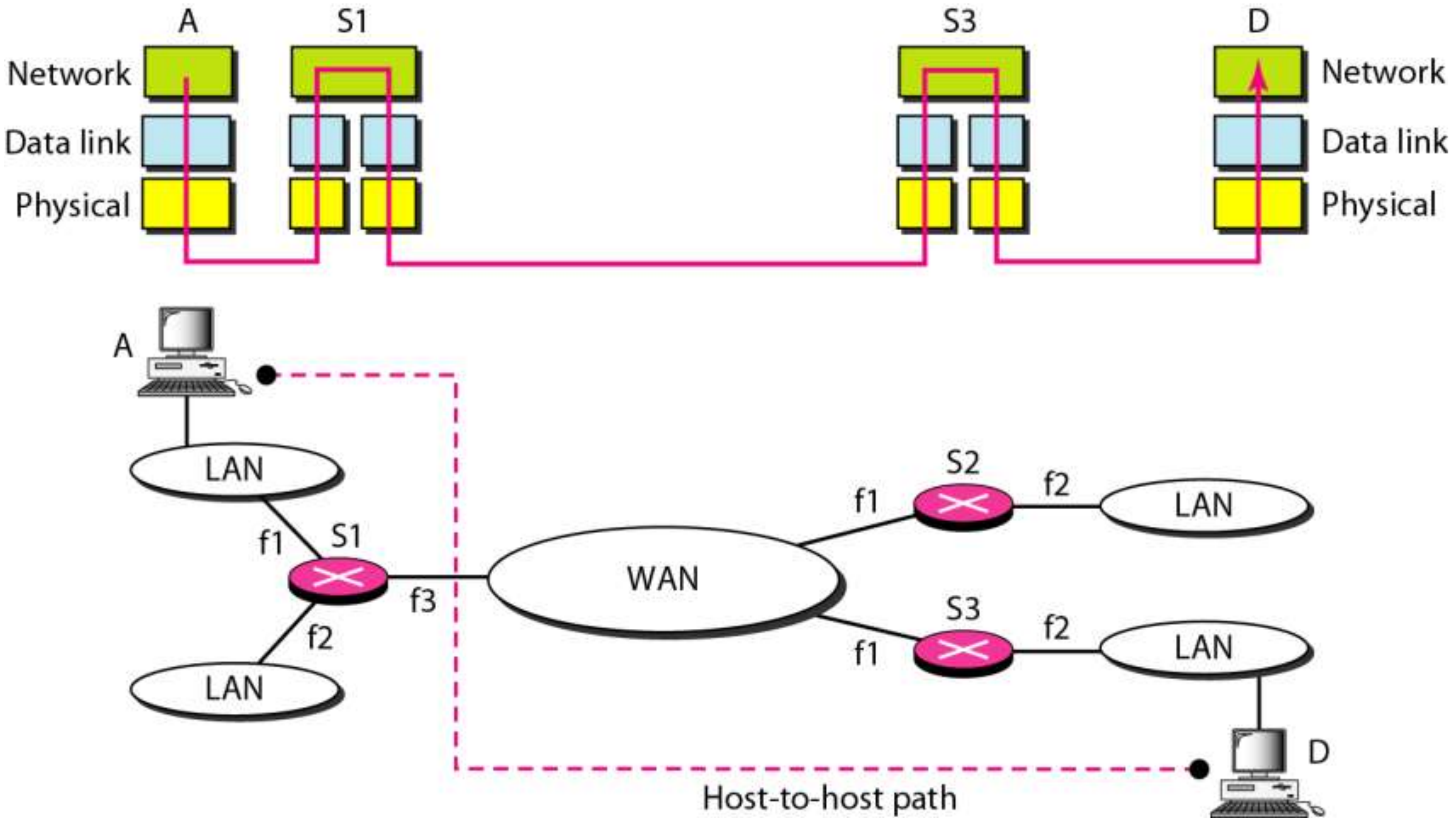
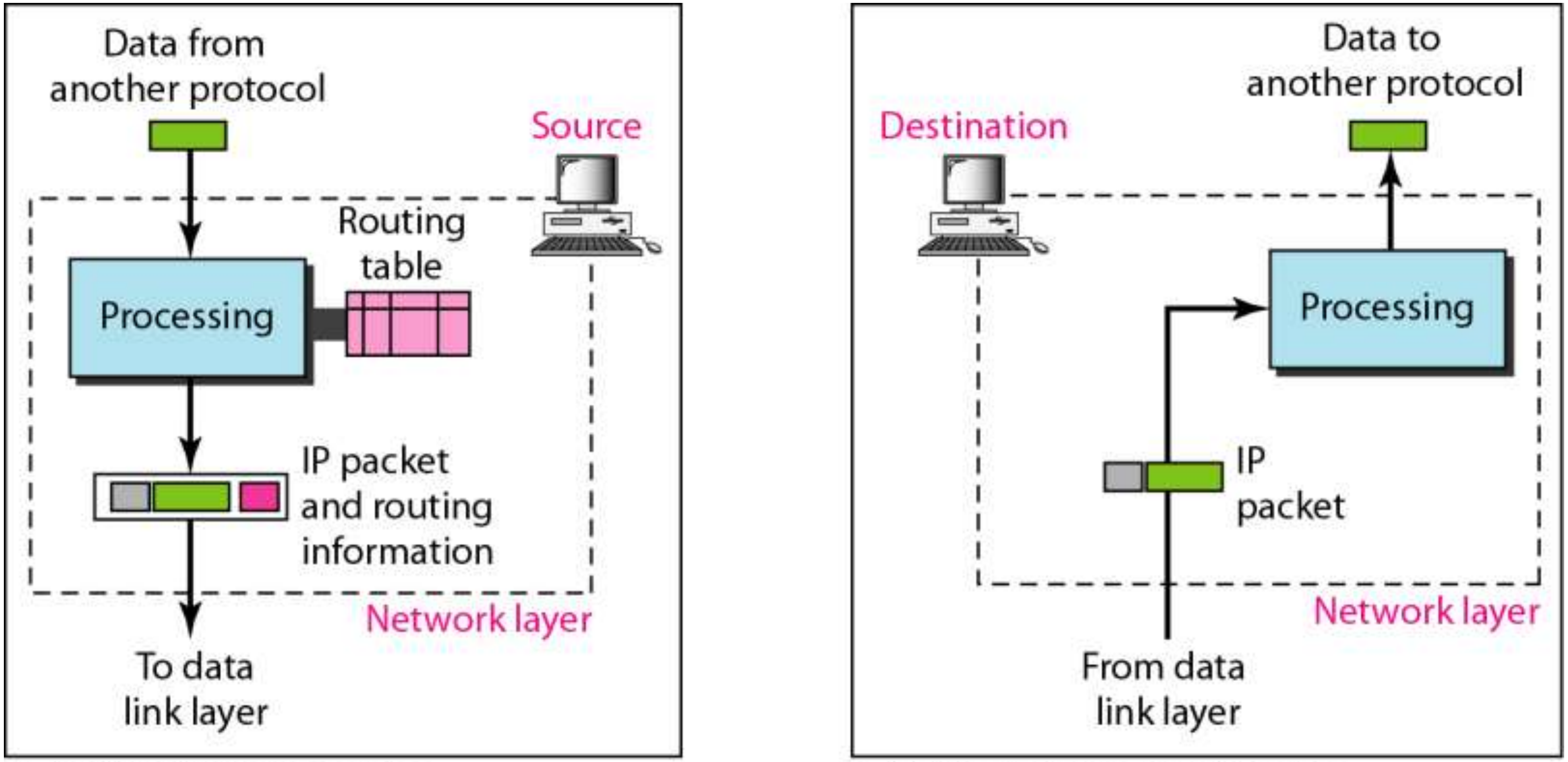


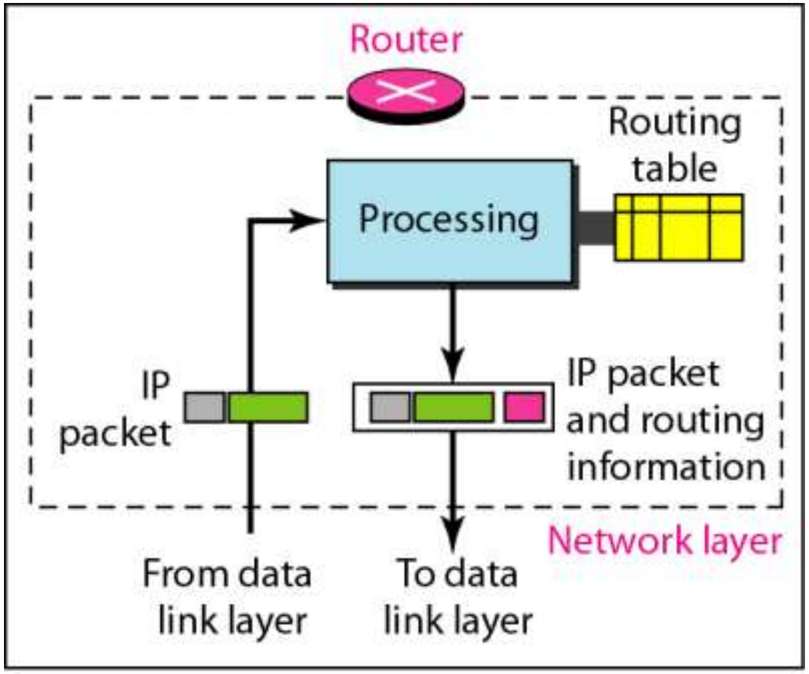
Figure 20.3 *Network layer at the source, router, and destination*



a. Network layer at source

b. Network layer at destination

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



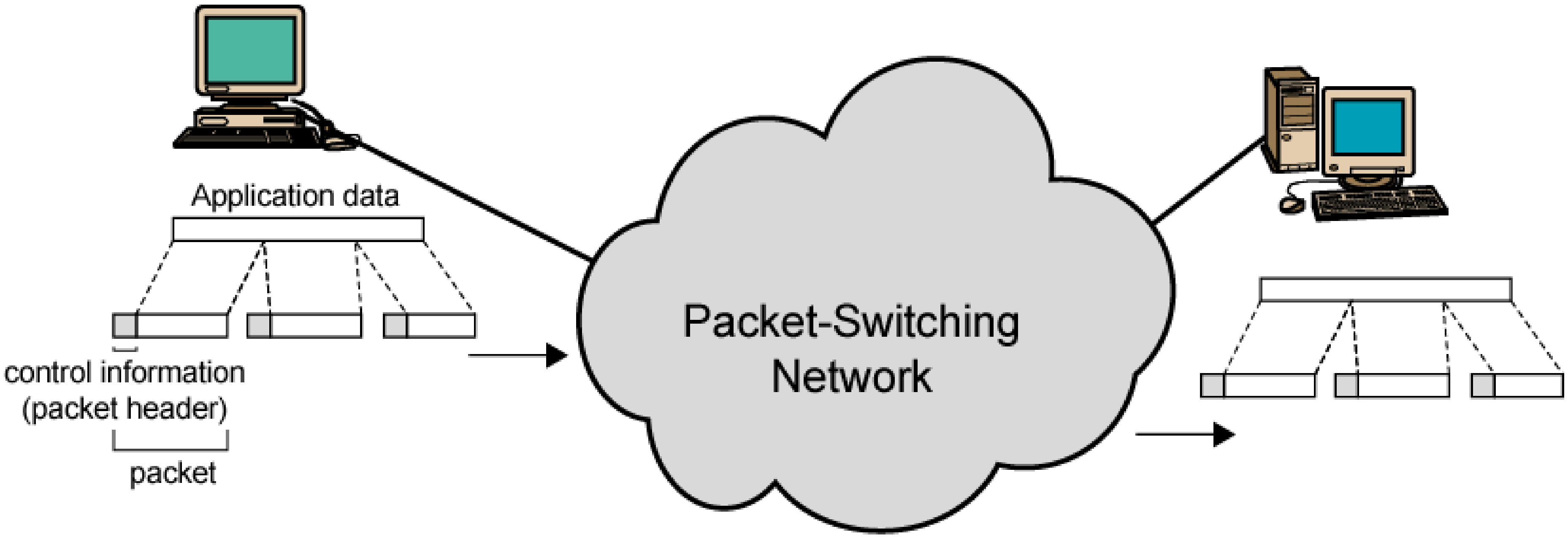
c. Network layer at a router

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

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

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

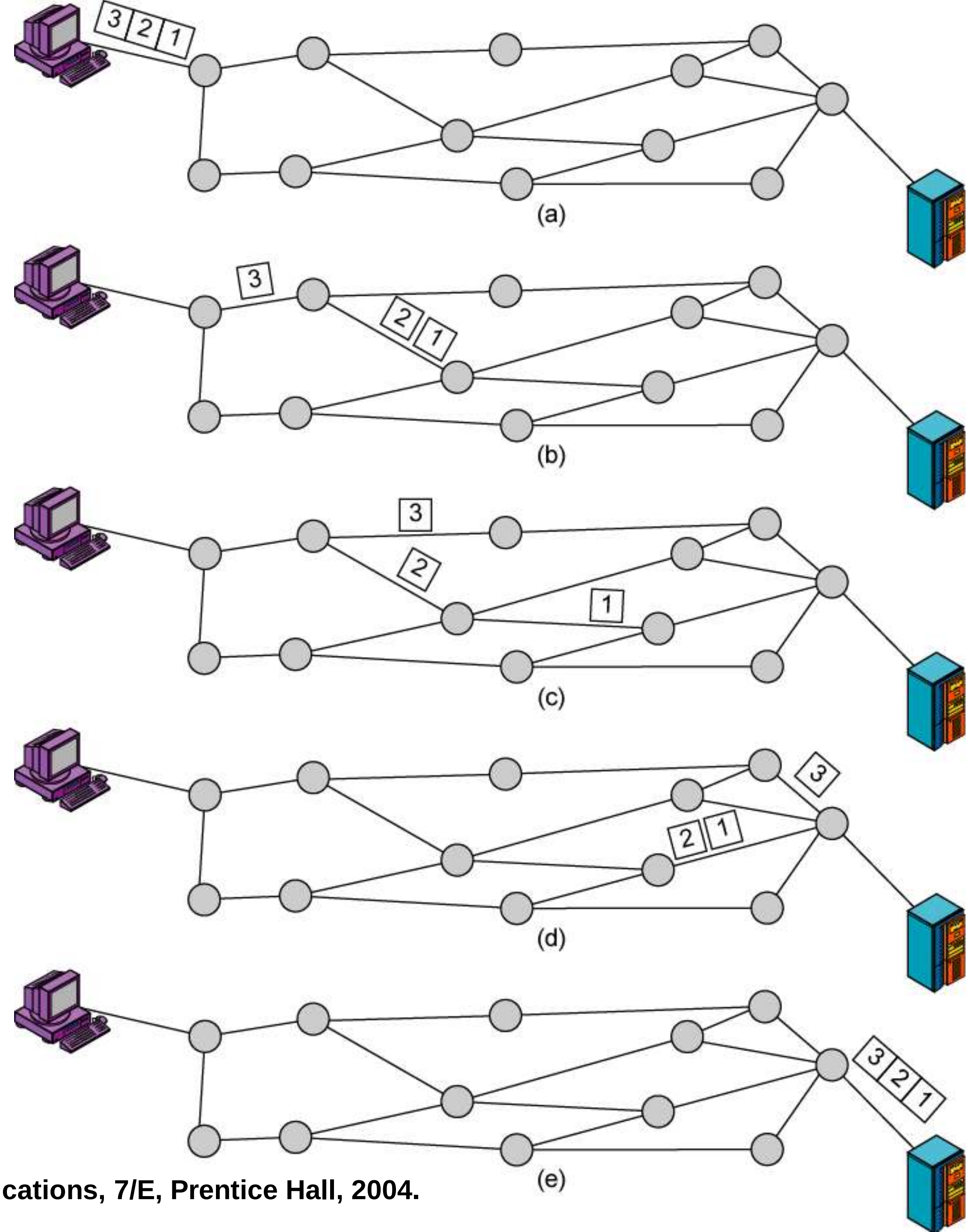
William Stallings.. Data and Computer Communications, 7/E, Prentice Hall, 2004.

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

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

Datagram Diagram



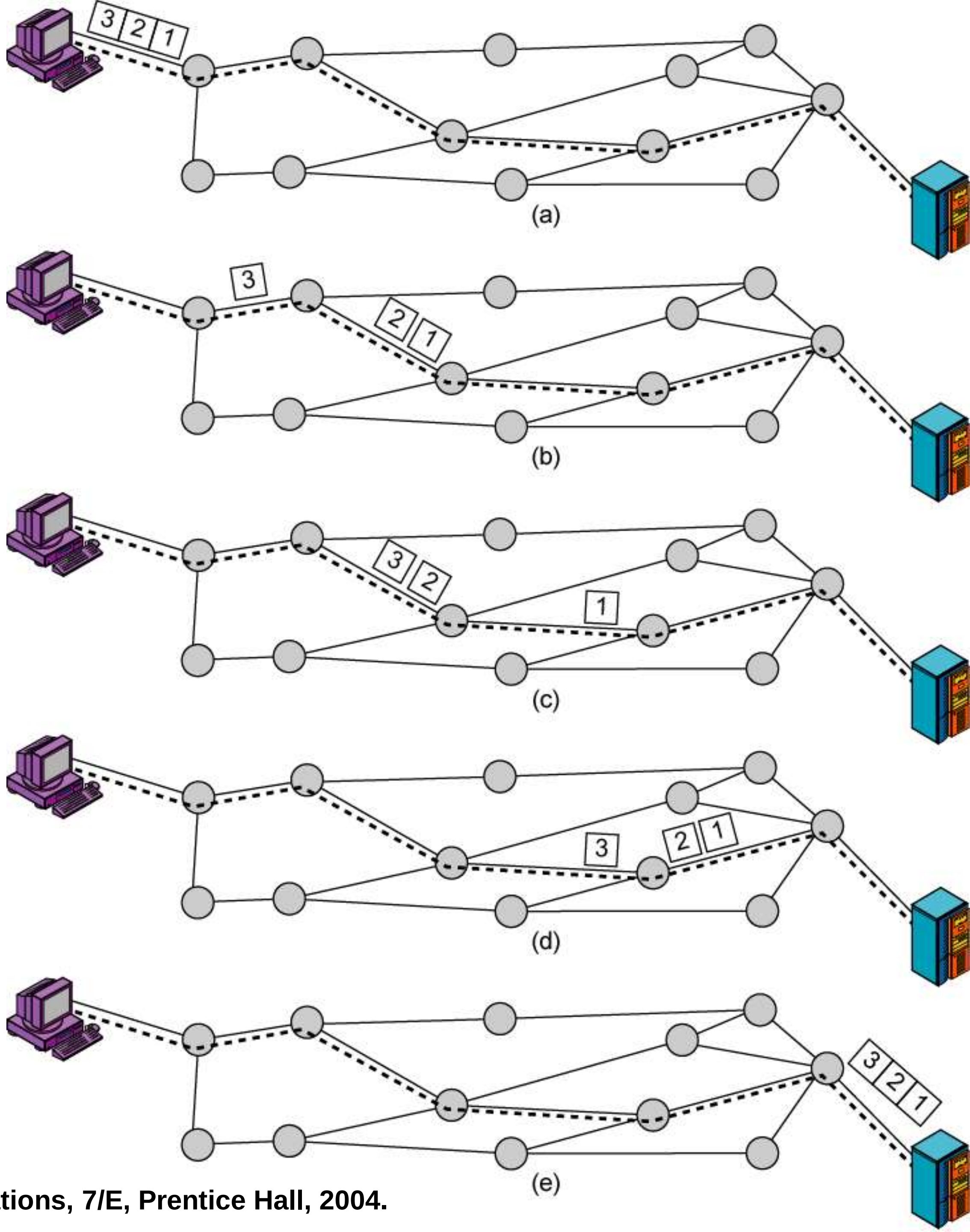
William Stallings.. Data and Computer Communications, 7/E, Prentice Hall, 2004.

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

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

Virtual Circuit Diagram



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

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

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

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.

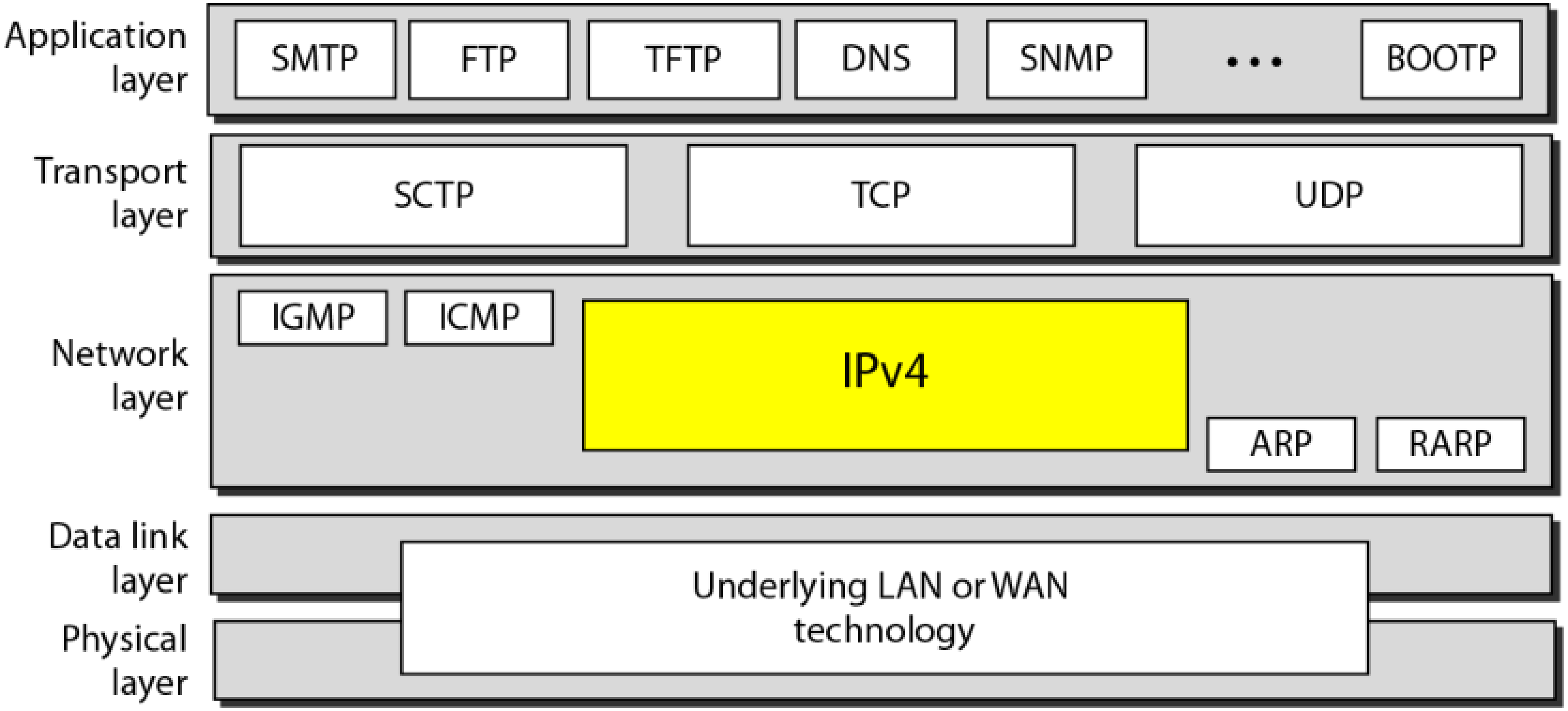
20-2 IPv4

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*



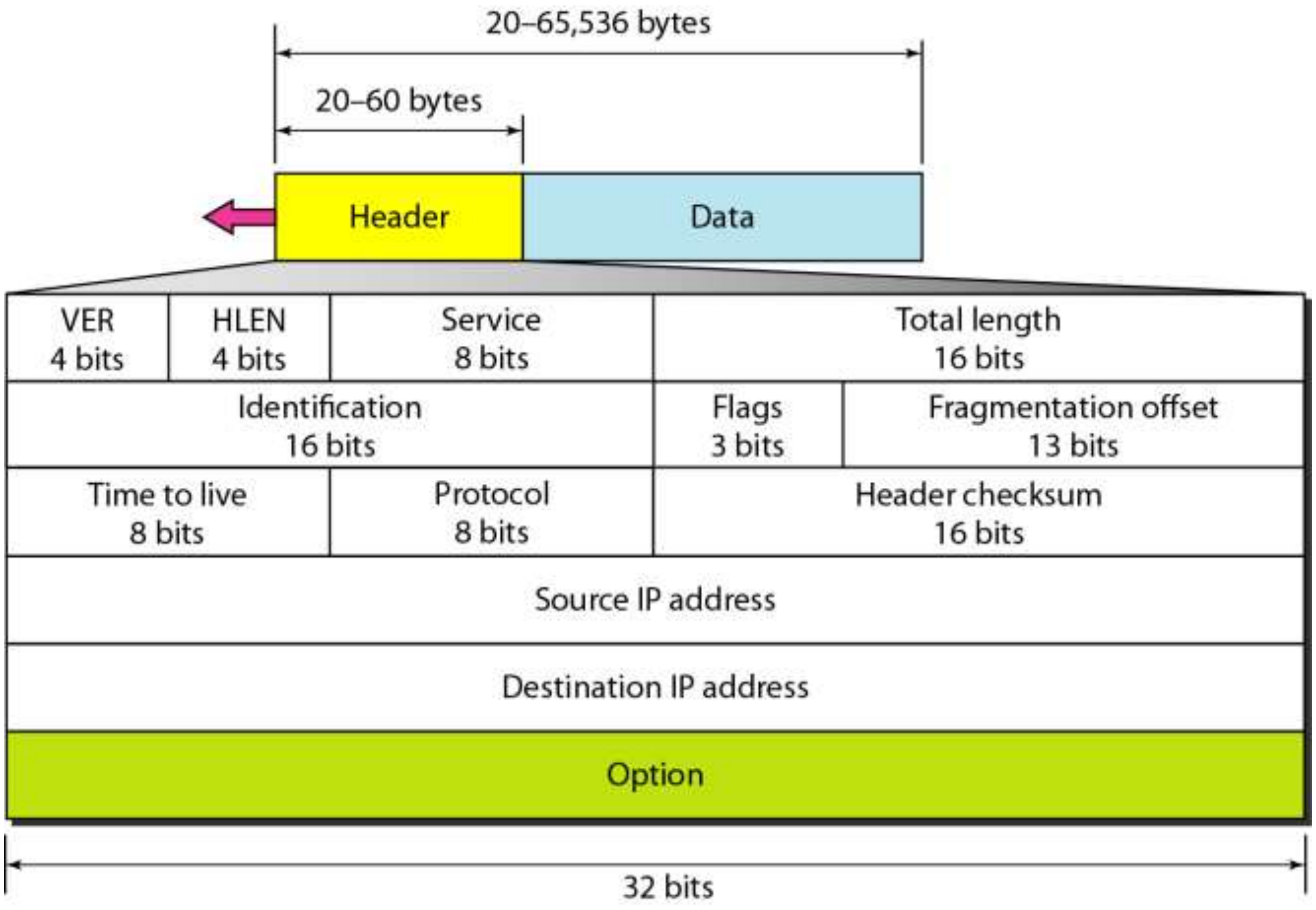
Note

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*



VER 4 bits | HLEN 4 bits | Service 8 bits | Total length 16 bits

Identification 16 bits | Flags 3 bits | Fragmentation offset 13 bits

Time to live 8 bits | Protocol 8 bits | Header checksum 16 bits

Source IP address

Destination IP address

Option

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.

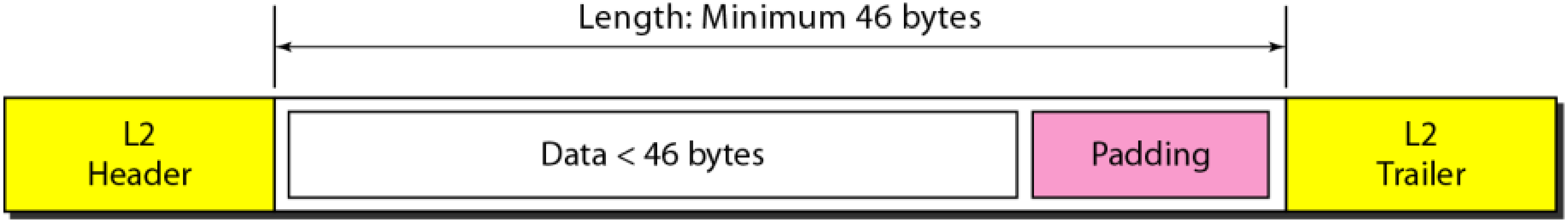
IPv4 Datagram Format

- 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

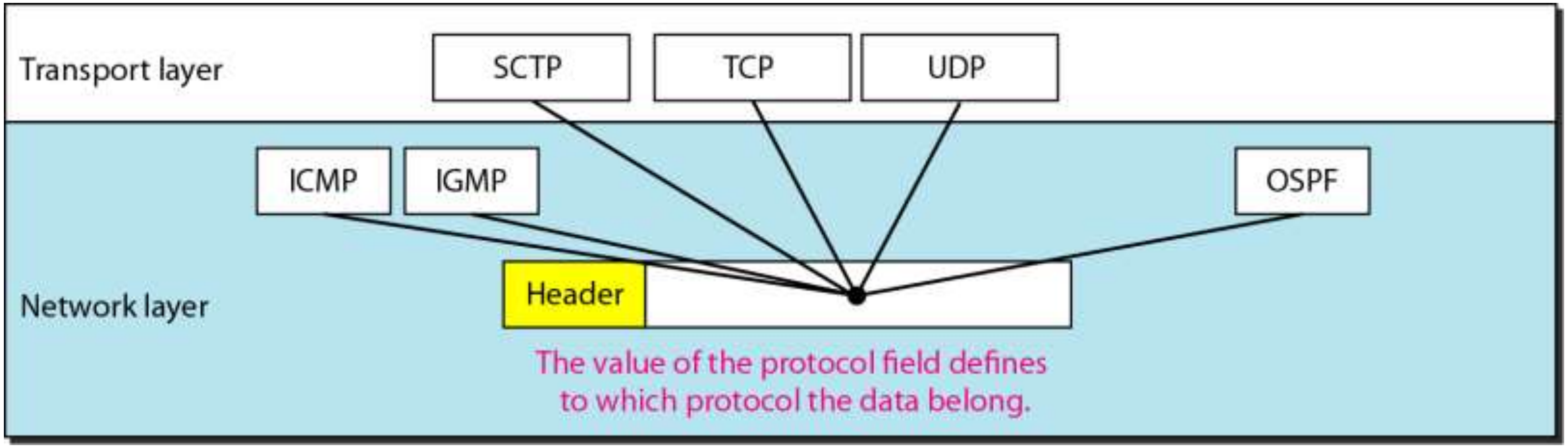
The total length field defines the total length of the datagram including the header.

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



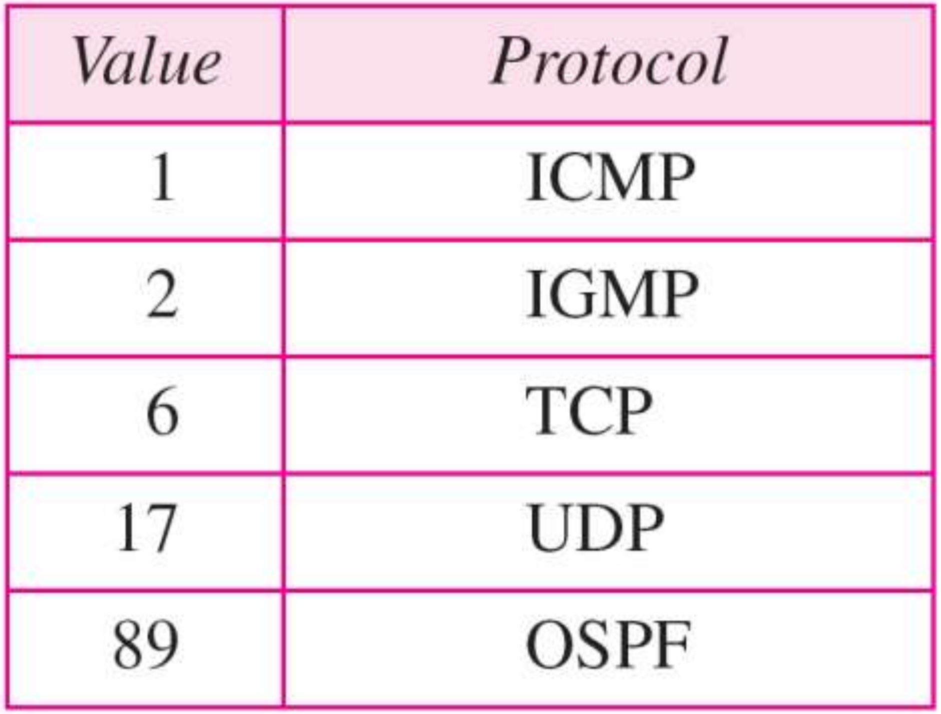
One of the reason why “total length” field is required.

Figure 20.8 *Protocol field and encapsulated data*



The value of the protocol field defines to which protocol the data belong.

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 × 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)*

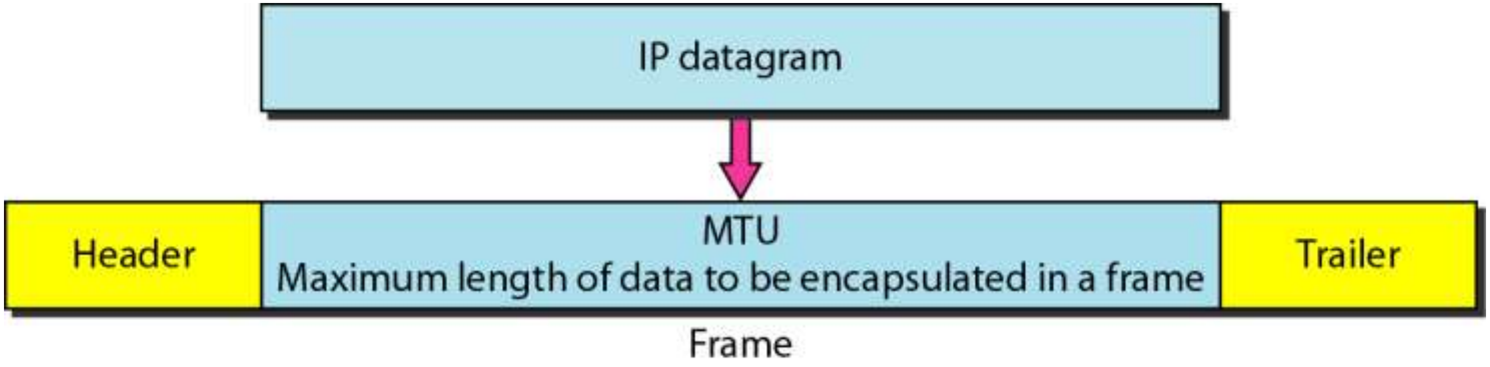
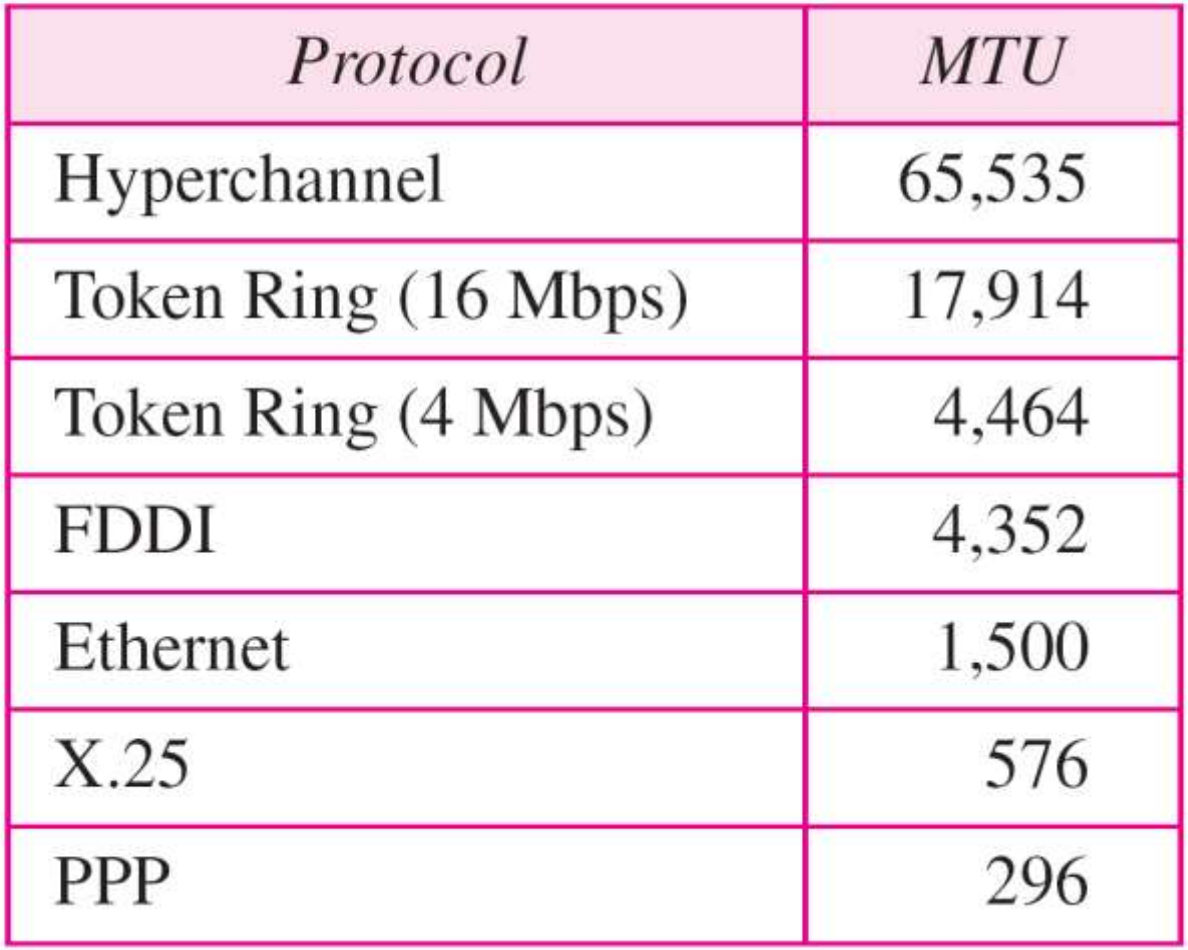


Table 20.5 ***MTUs for some networks***

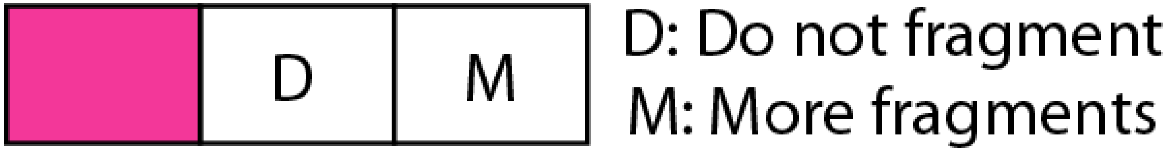


Protocol	*MTU*
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

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.

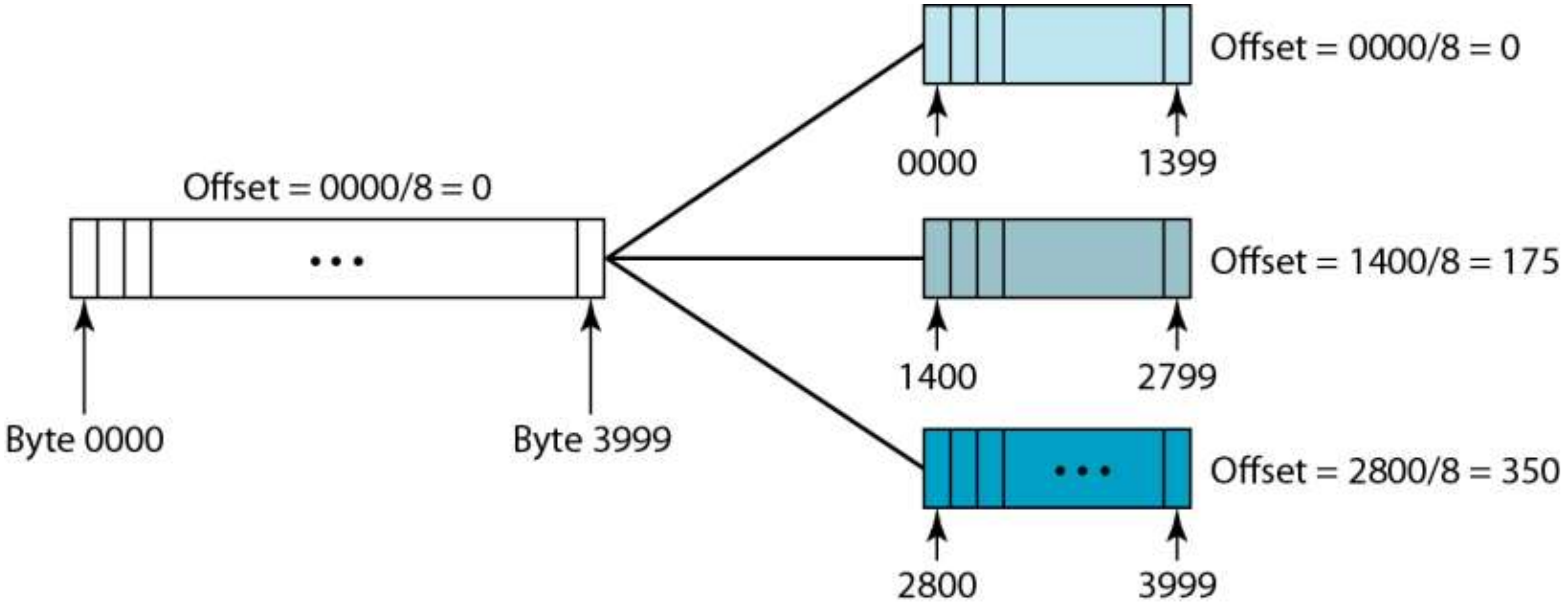
Figure 20.10 *Flags (3 bits) used in fragmentation*



- 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

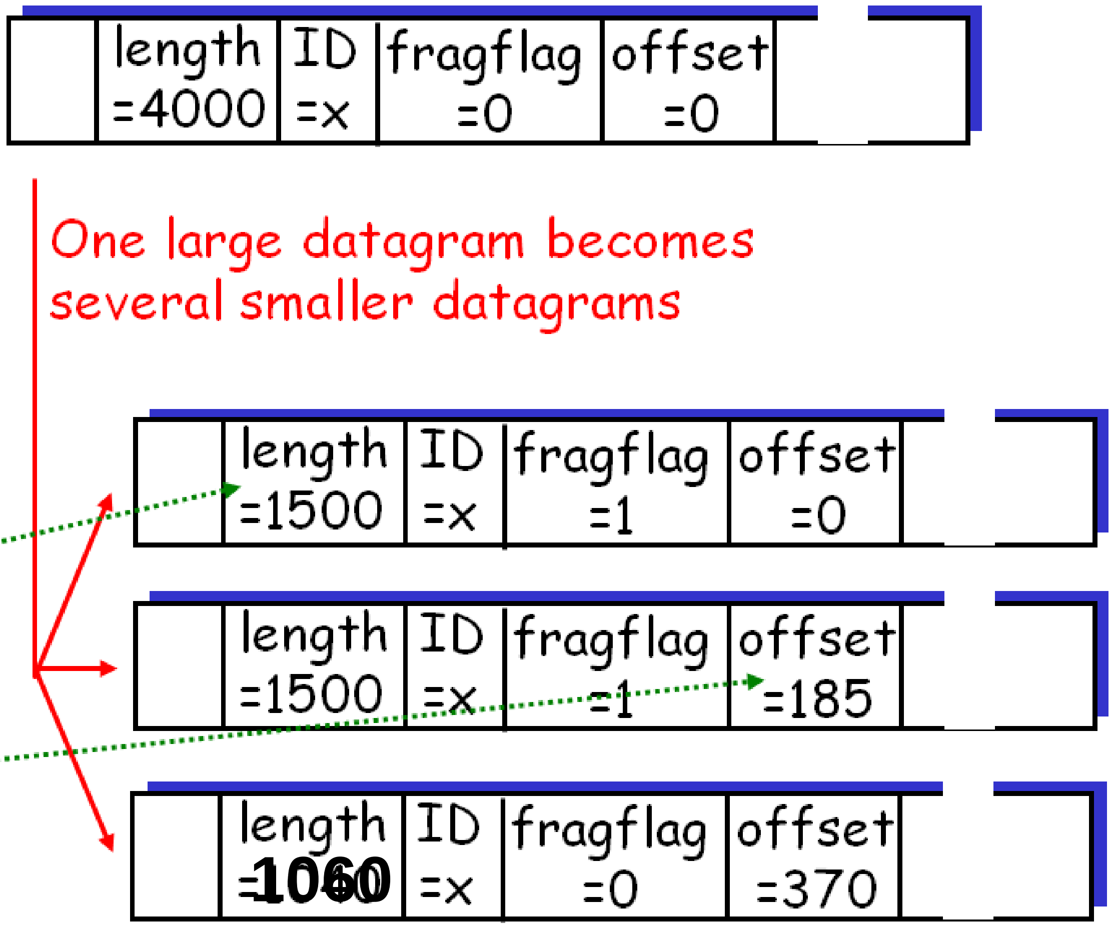
Figure 20.11 *Fragmentation example*



IP Fragmentation and Reassembly

Example

- 4000 byte datagram
- MTU = 1500 bytes



One large datagram becomes several smaller datagrams

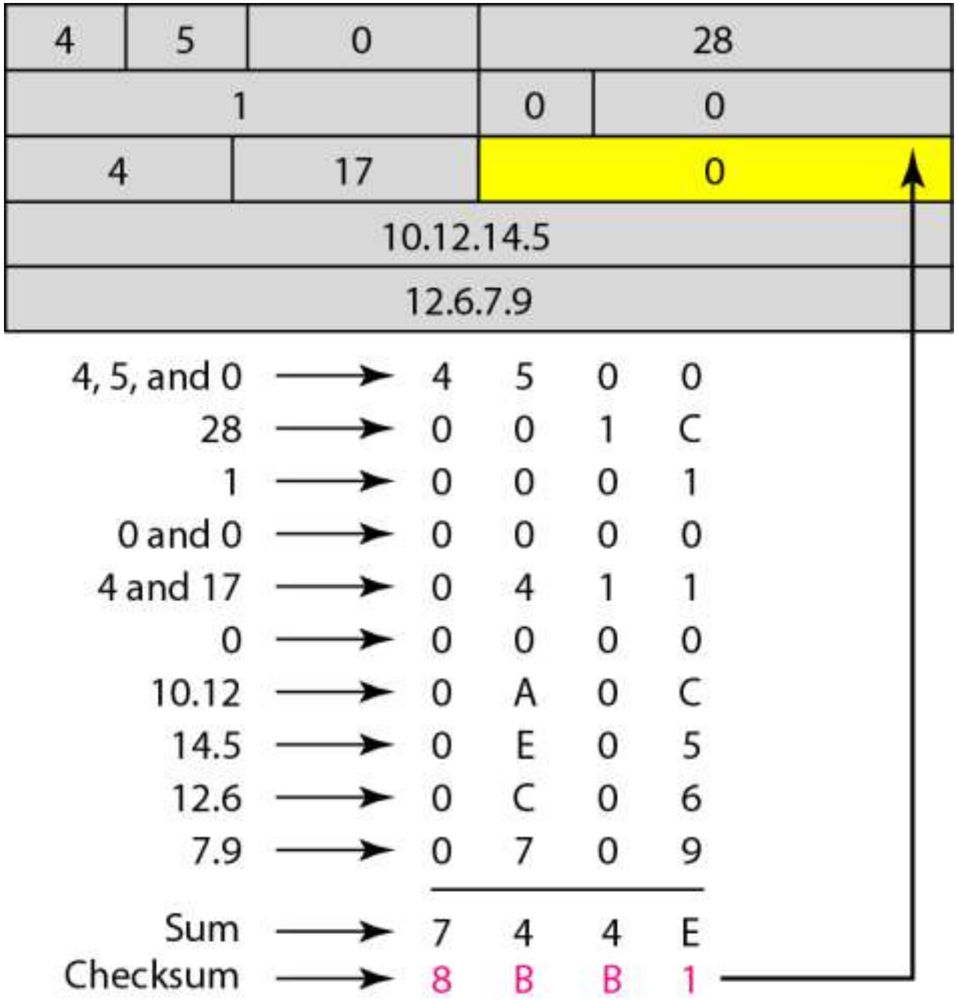
1480 bytes in data field

offset = 1480/8

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*



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

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*

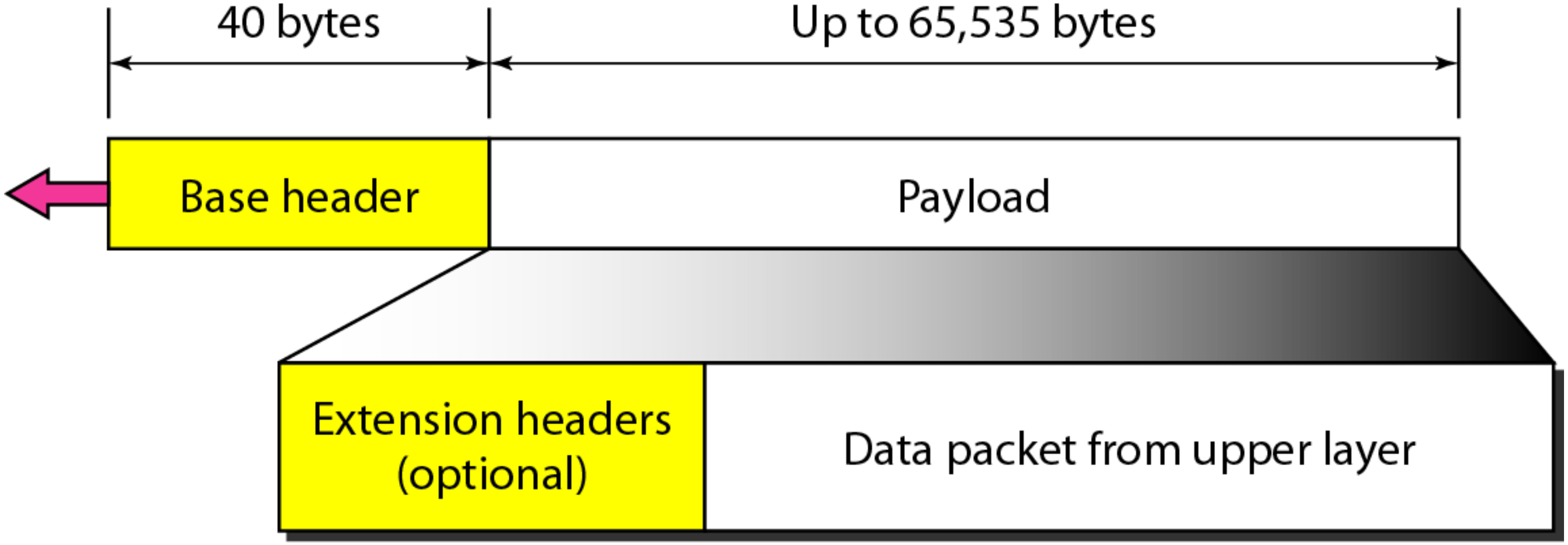


Figure 20.16 *Format of an IPv6 datagram*

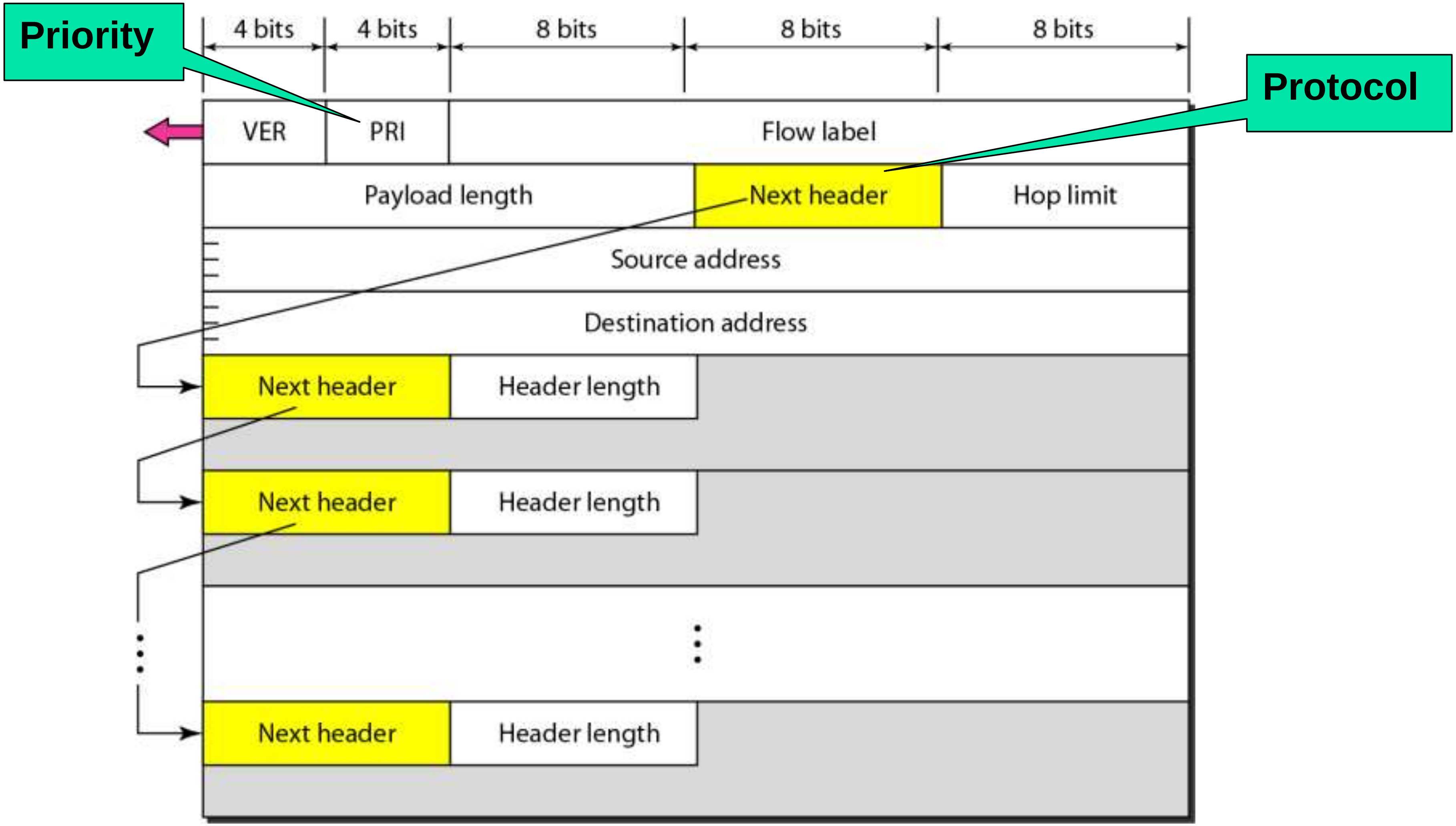
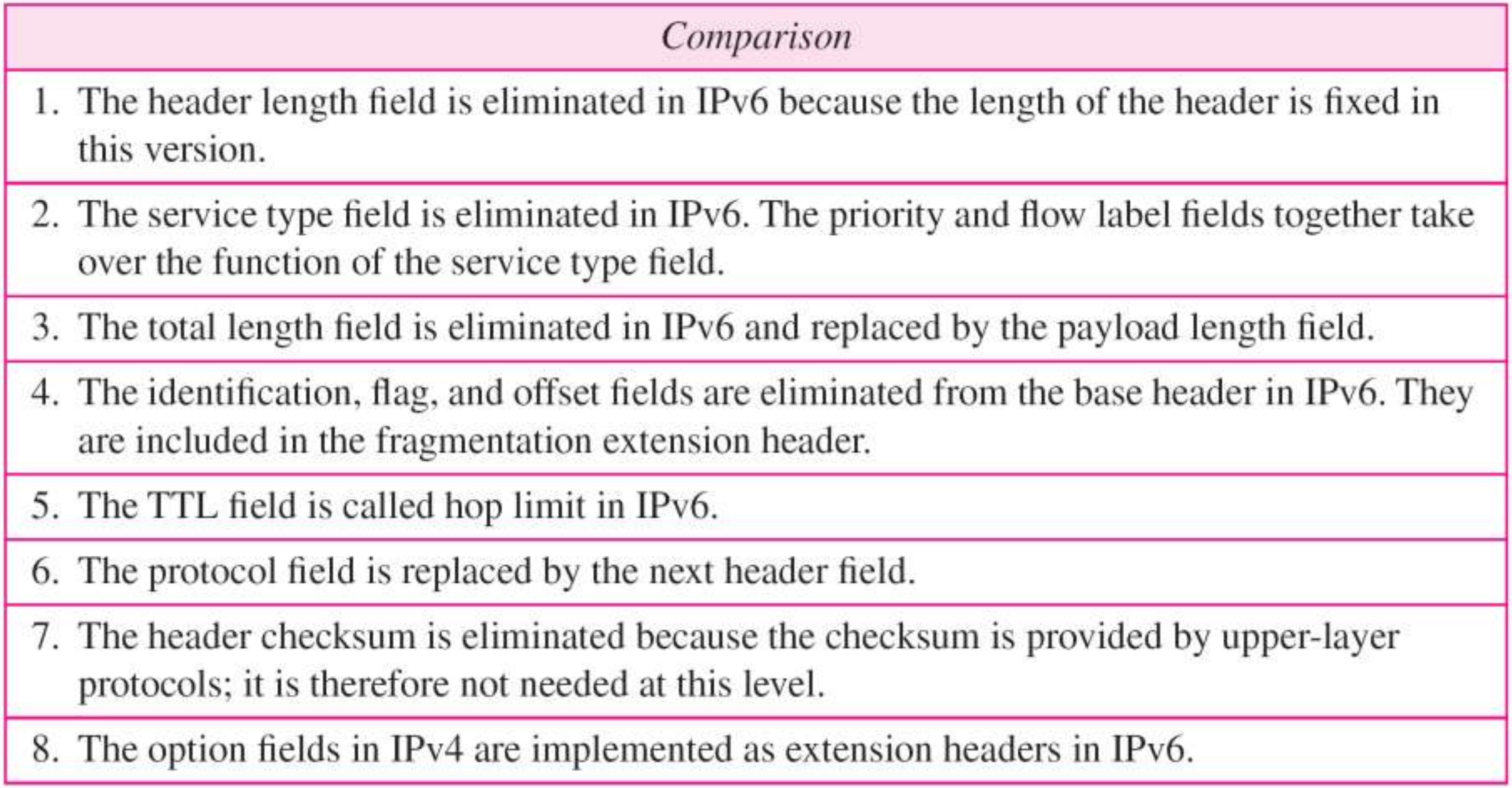


Table 20.9 *Comparison between IPv4 and IPv6 packet headers*



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*

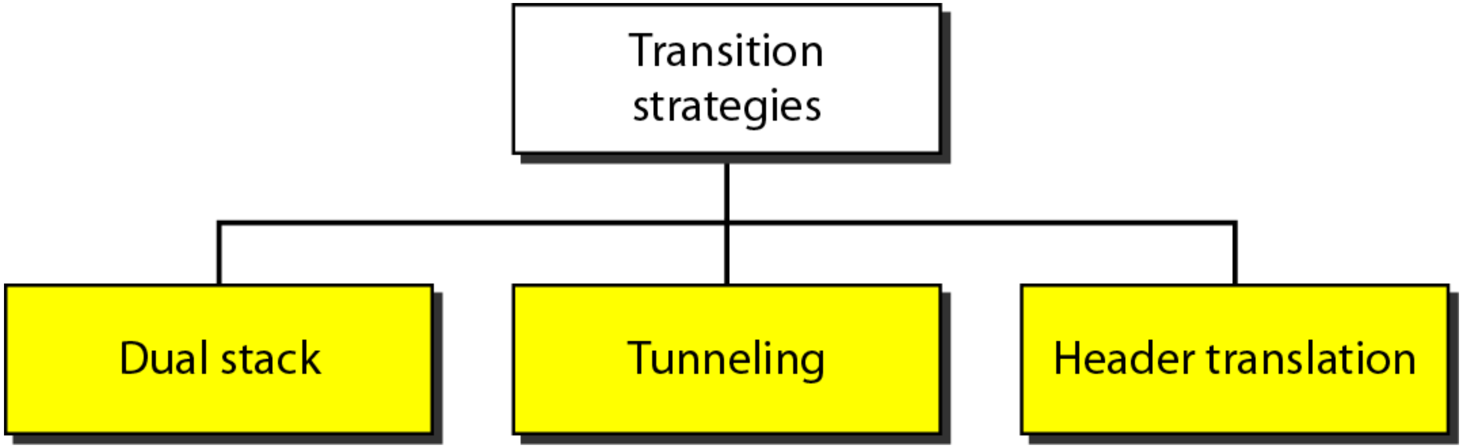
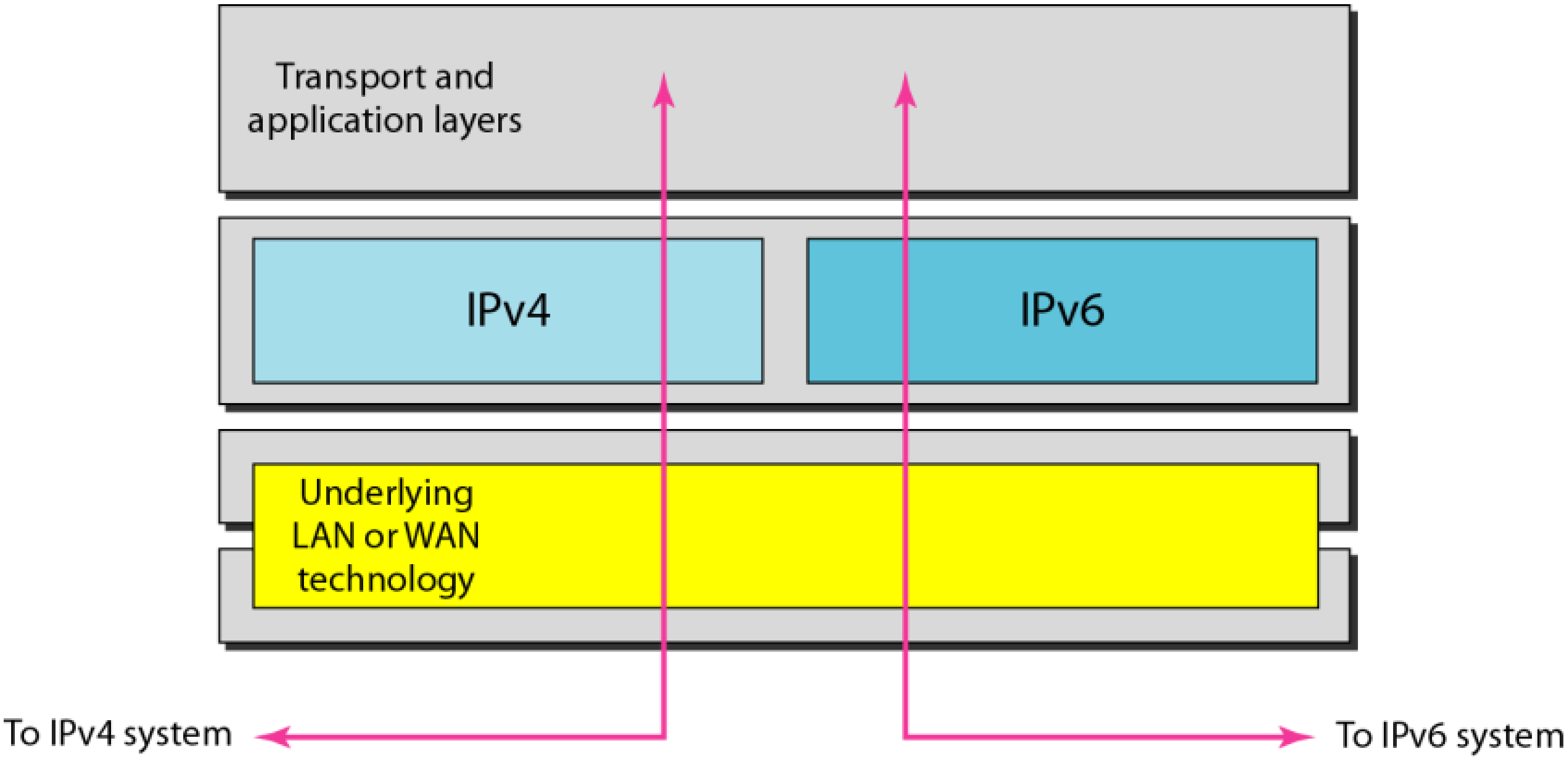
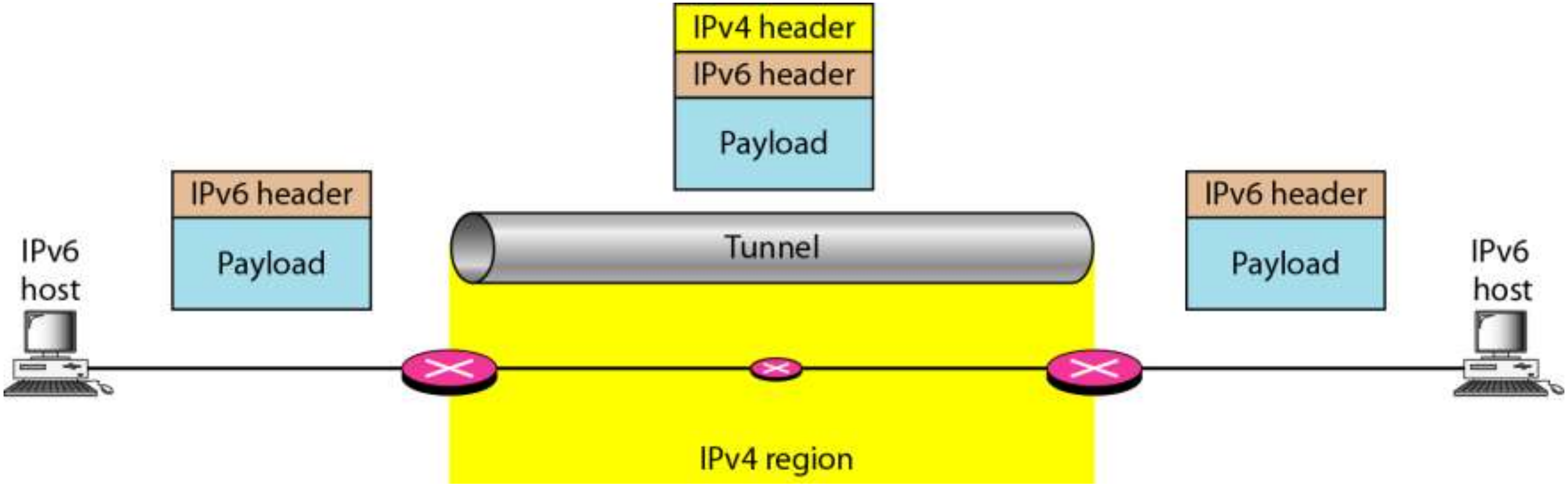


Figure 20.19 *Dual stack*


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

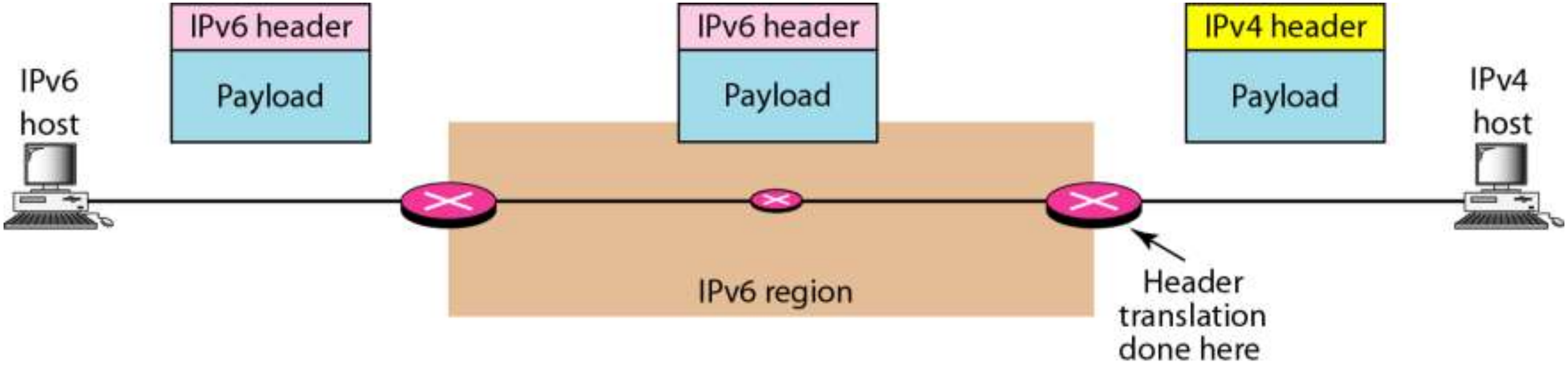
Host uses DNS query result to determine which IP to use

Figure 20.20 *Tunneling strategy*



Popular used right now in many countries

Figure 20.21 *Header translation strategy*



Chapter 23

Process-to-Process Delivery: UDP, TCP, and SCTP

23-1 PROCESS-TO-PROCESS DELIVERY

The transport layer is responsible for process-to-process delivery—the delivery of a packet, part of a message, from one process to another. Two processes communicate in a client/server relationship, as we will see later.

Topics discussed in this section:

Client/Server Paradigm
Multiplexing and Demultiplexing
Connectionless Versus Connection-Oriented Service
Reliable Versus Unreliable
Three Protocols

Note

The transport layer is responsible for process-to-process delivery.

Figure 23.1 *Types of data deliveries*

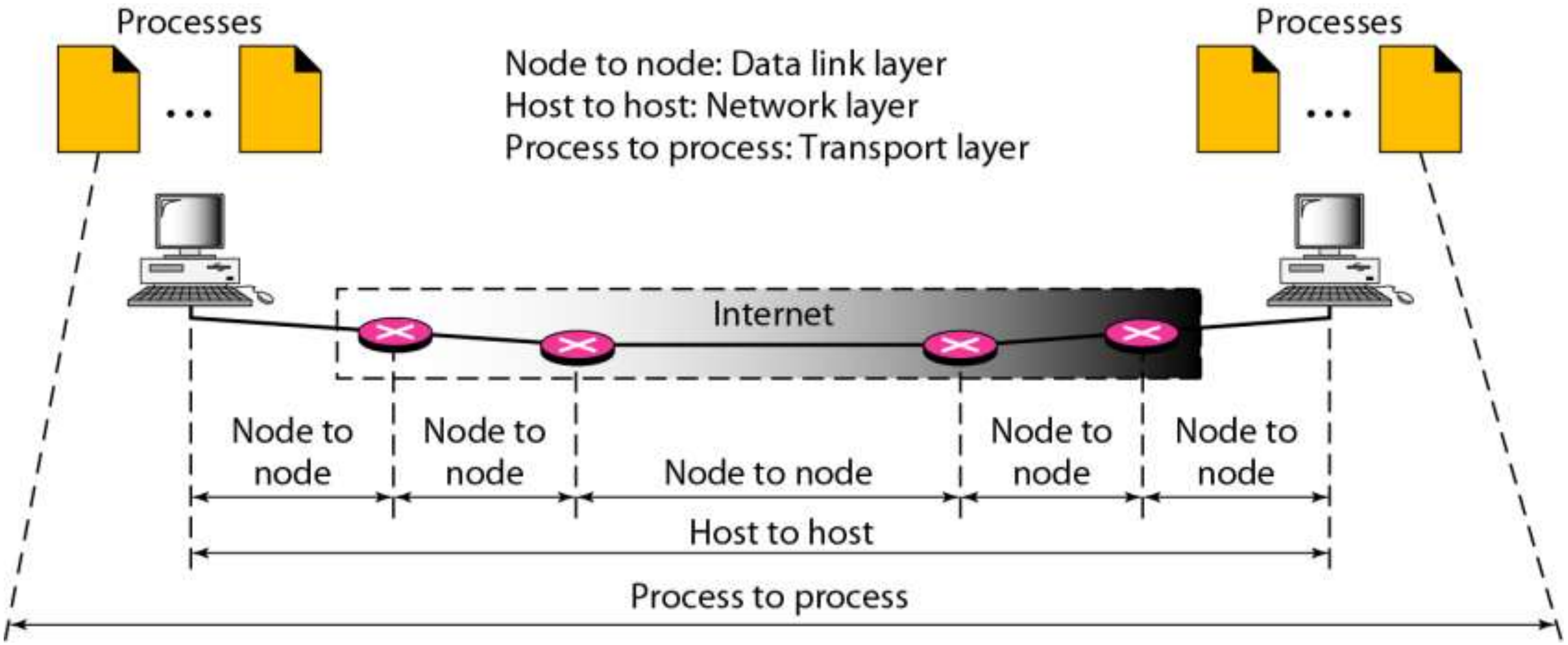


Figure 23.2 *Port numbers*

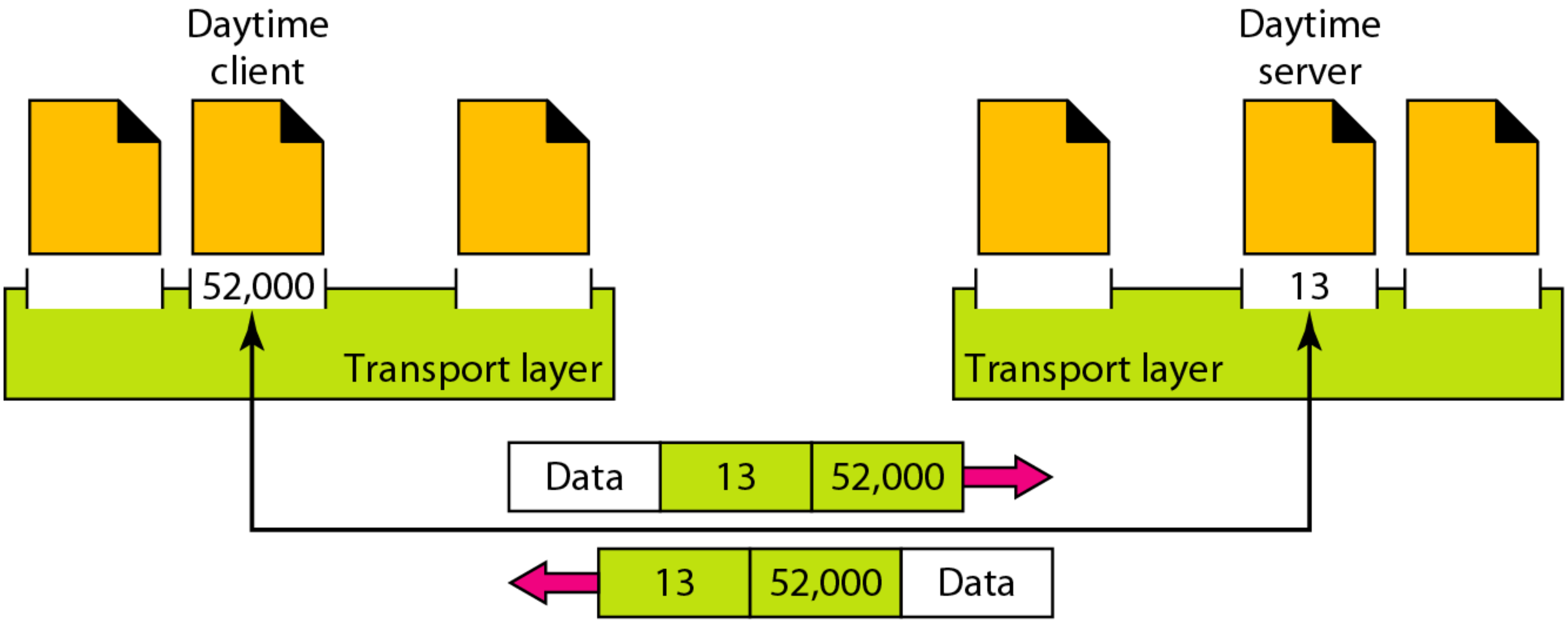


Figure 23.3 *IP addresses versus port numbers*

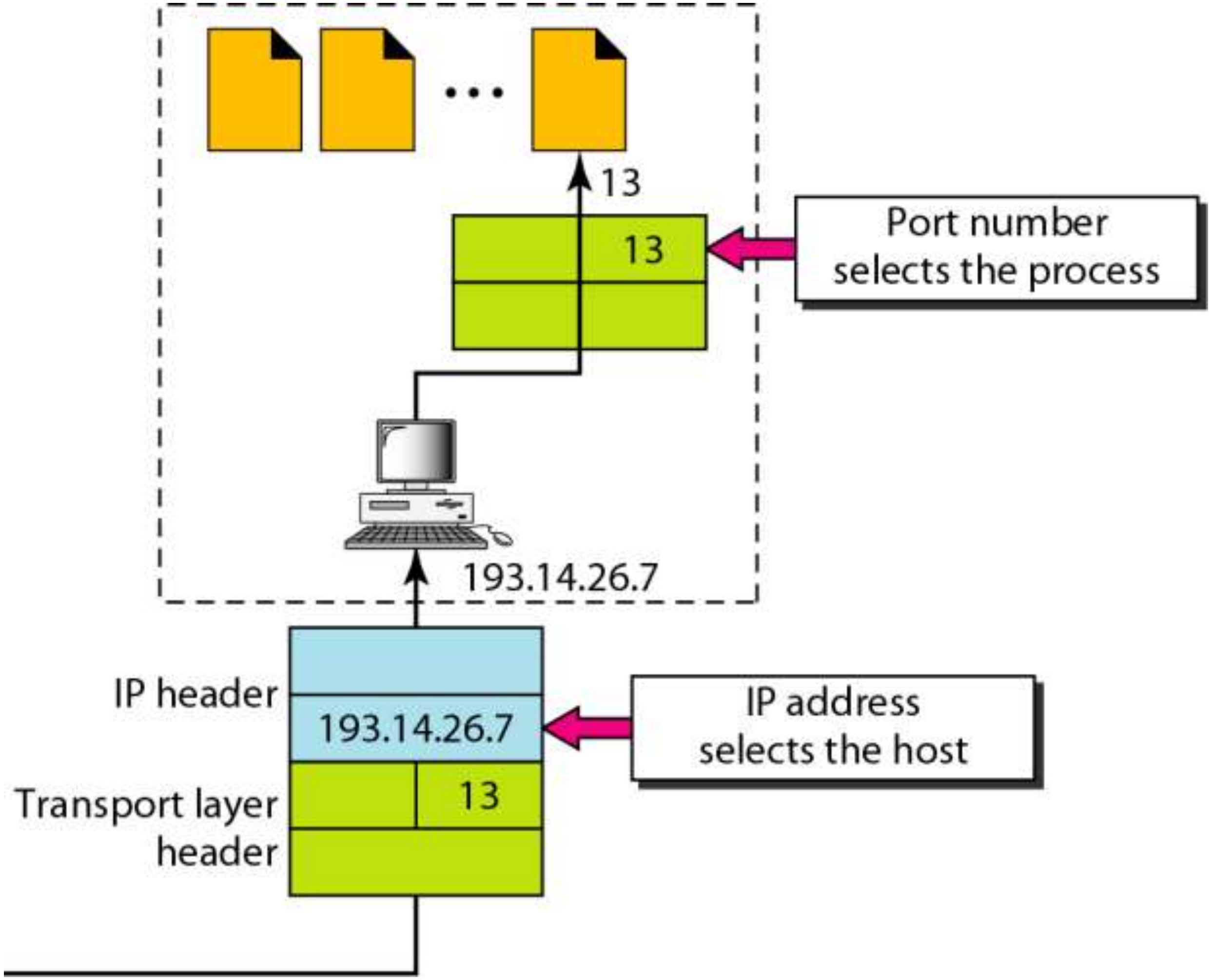


Figure 23.4 *IANA ranges*

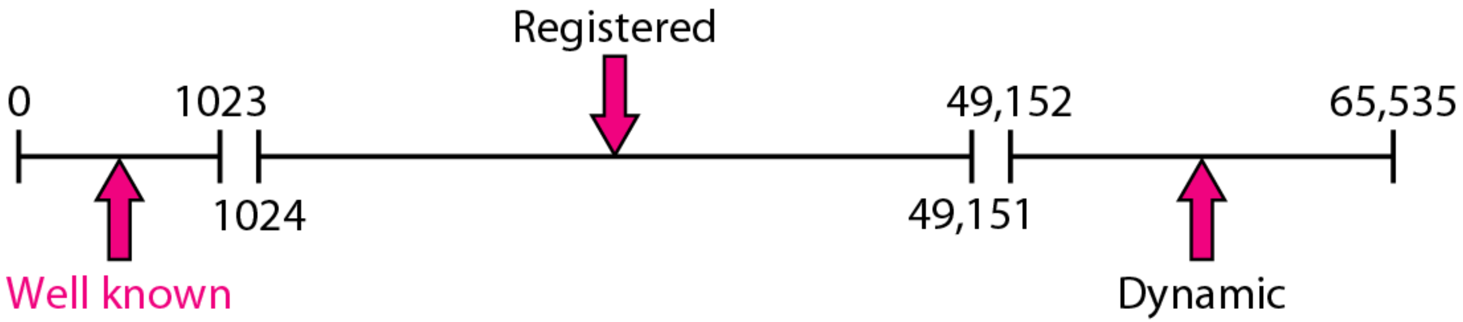


Figure 23.5 *Socket address*

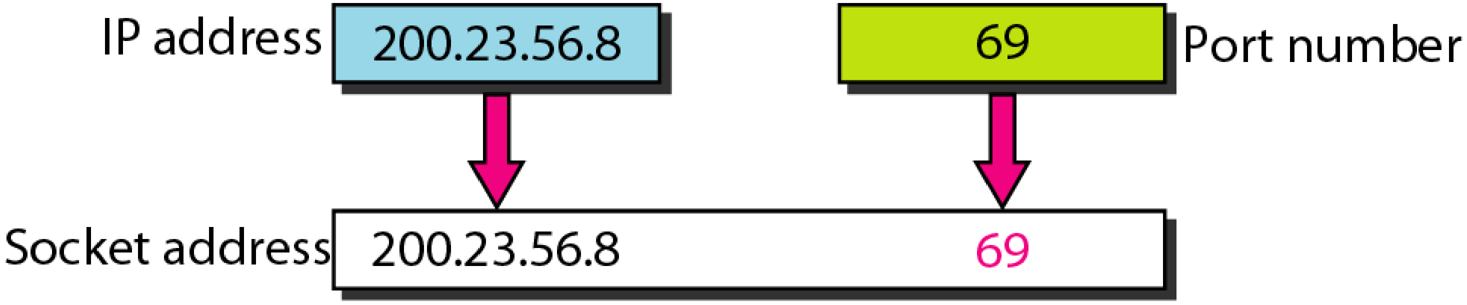


Figure 23.6 *Multiplexing and demultiplexing*

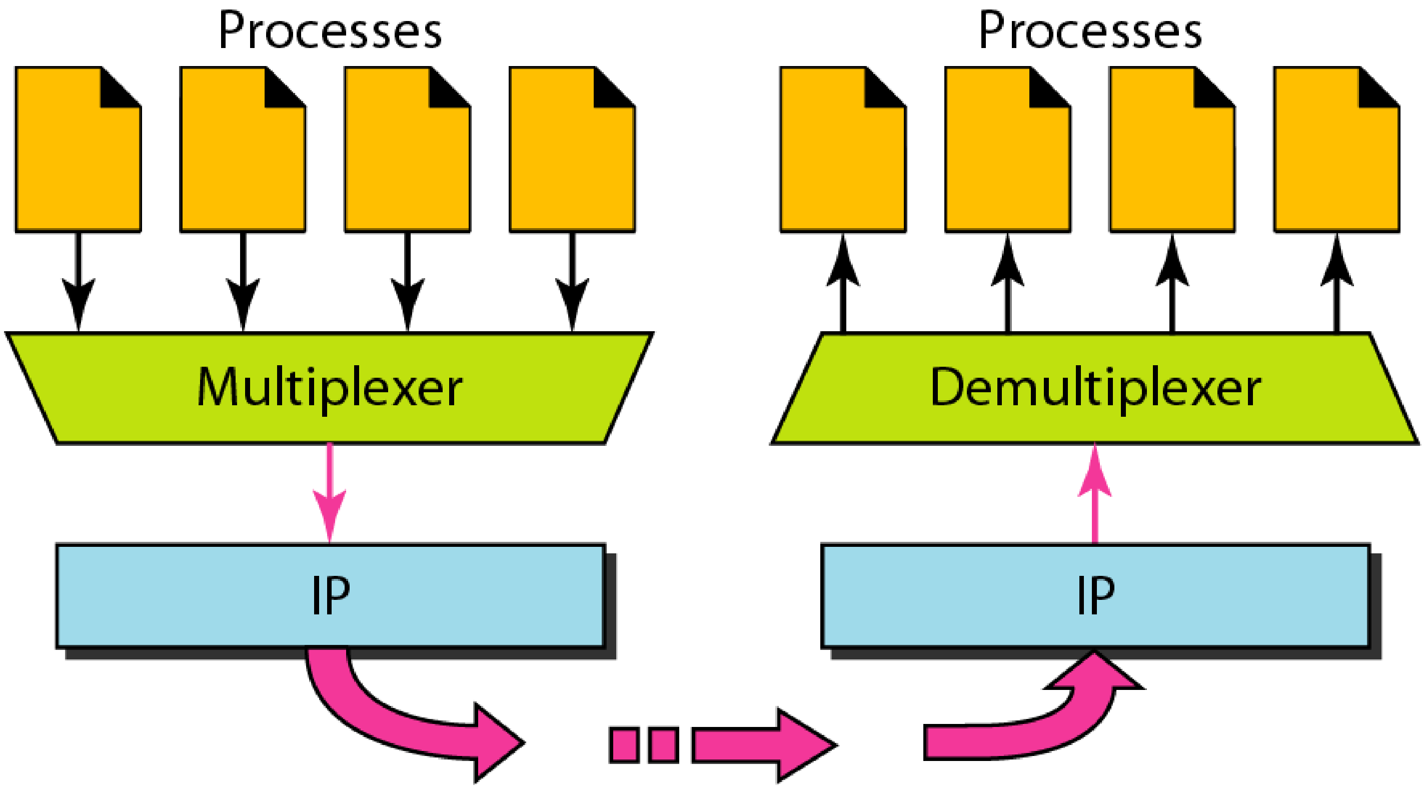


Figure 23.7 *Error control*

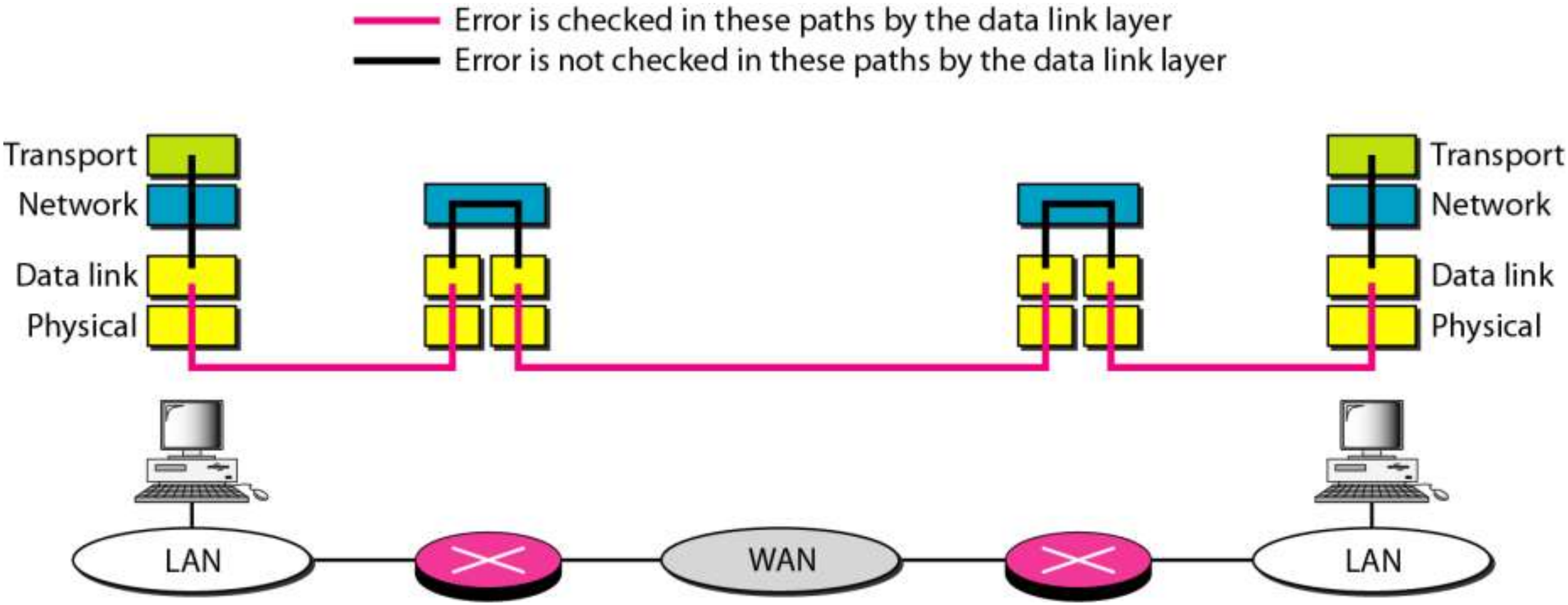
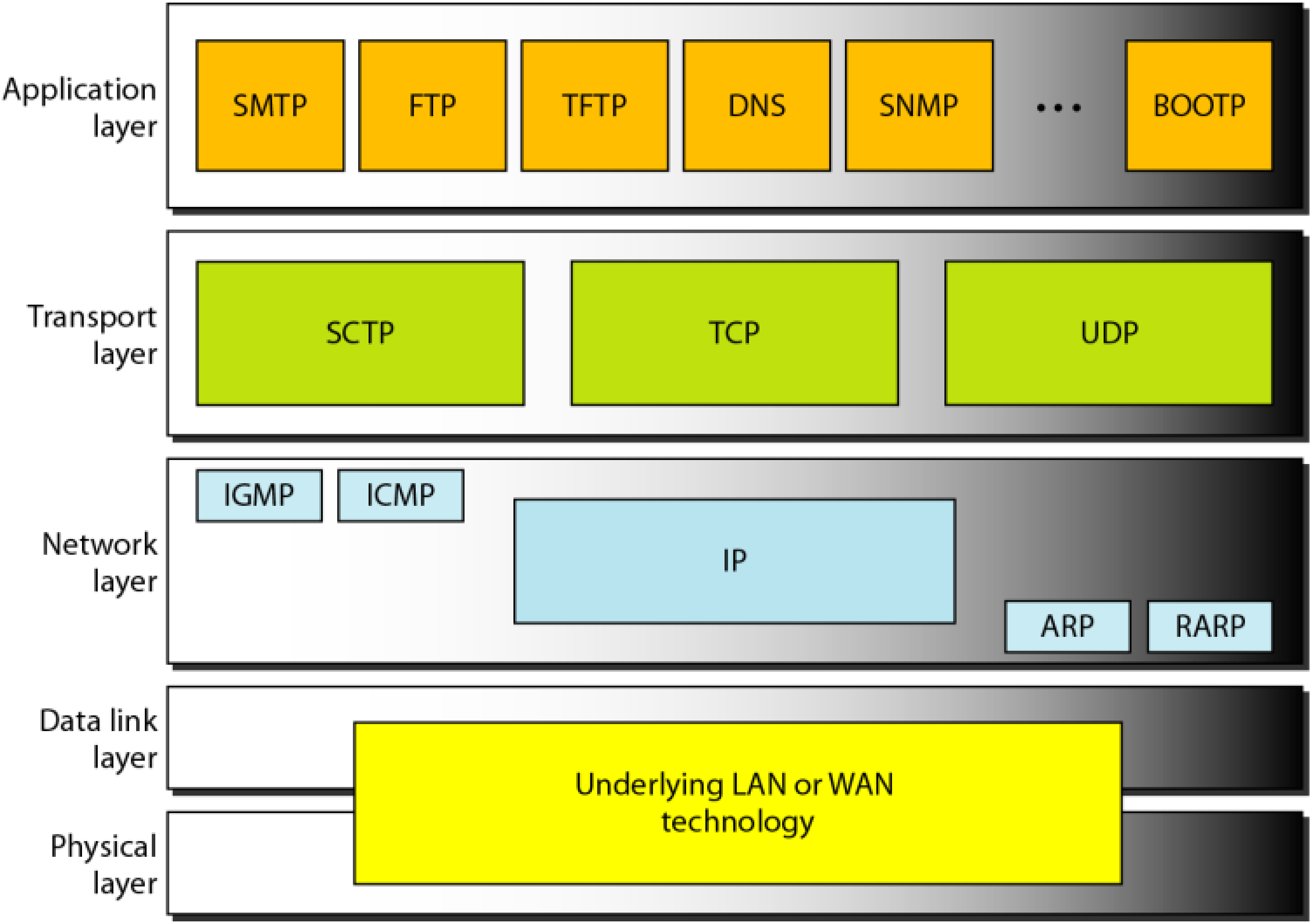

Error is checked in these paths by the data link layer
Error is not checked in these paths by the data link layer
Transport
Network
Data link
Physical
Transport
Network
Data link
Physical
LAN
WAN
LAN

Figure 23.8 *Position of UDP, TCP, and SCTP in TCP/IP suite*



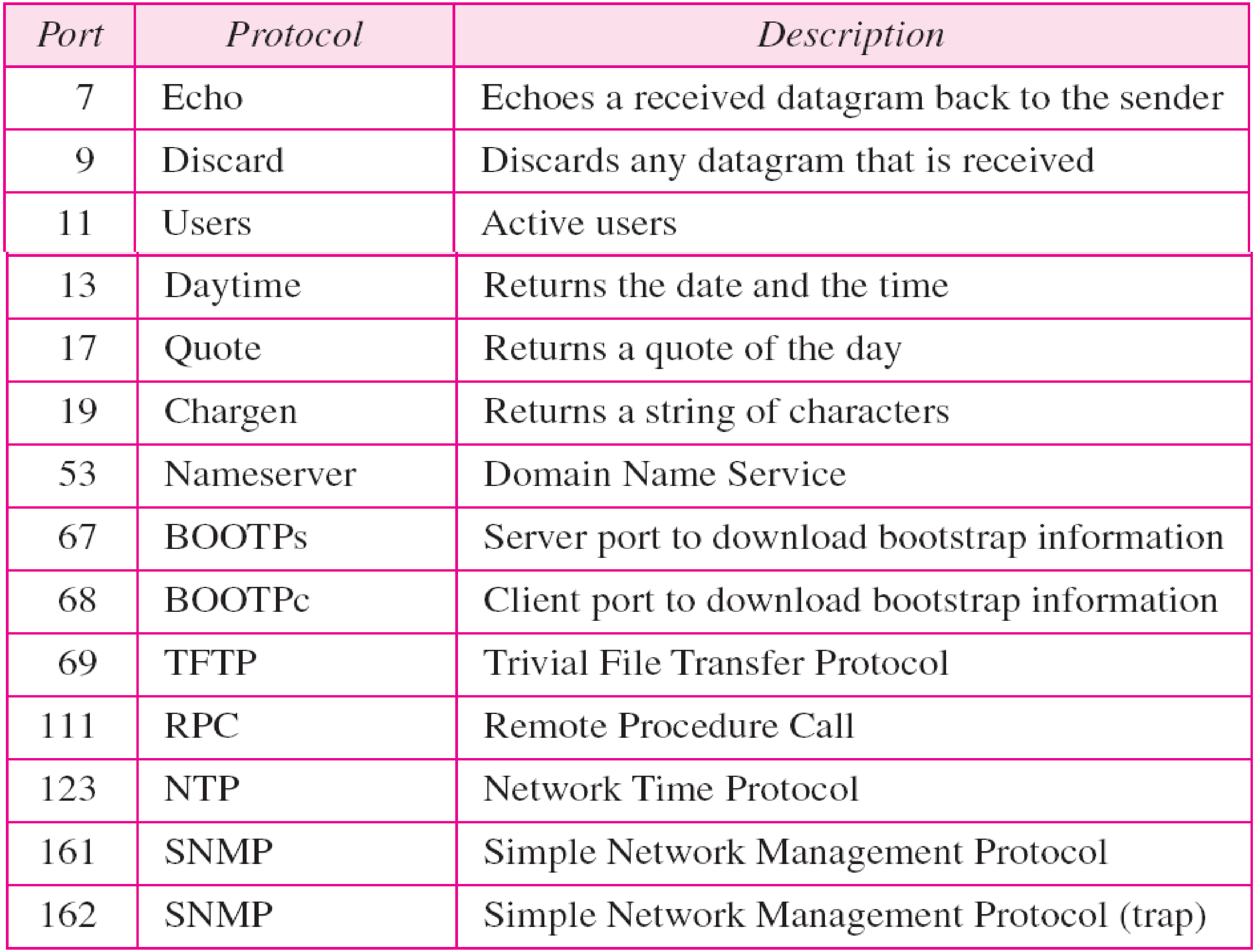
23-2 USER DATAGRAM PROTOCOL (UDP)

The User Datagram Protocol (UDP) is called a connectionless, unreliable transport protocol. It does not add anything to the services of IP except to provide process-to-process communication instead of host-to-host communication.

Topics discussed in this section:

Well-Known Ports for UDP
User Datagram
Checksum
UDP Operation
Use of UDP

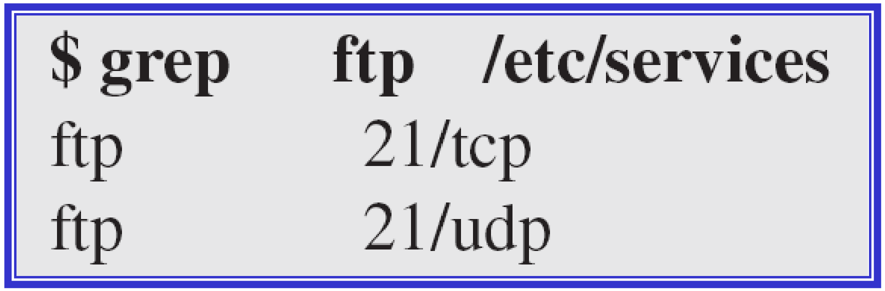
Table 23.1 *Well-known ports used with UDP*



Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
53	Nameserver	Domain Name Service
67	BOOTPs	Server port to download bootstrap information
68	BOOTPc	Client port to download bootstrap information
69	TFTP	Trivial File Transfer Protocol
111	RPC	Remote Procedure Call
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management Protocol
162	SNMP	Simple Network Management Protocol (trap)

Example 23.1

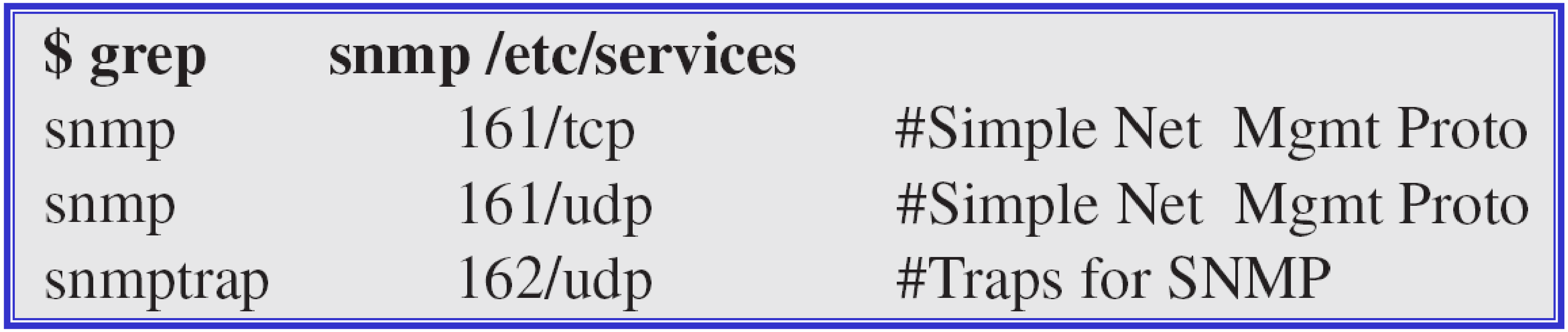
In UNIX, the well-known ports are stored in a file called /etc/services. Each line in this file gives the name of the server and the well-known port number. We can use the grep utility to extract the line corresponding to the desired application. The following shows the port for FTP. Note that FTP can use port 21 with either UDP or TCP.



```
$ grep     ftp    /etc/services
ftp          21/tcp
ftp          21/udp
```

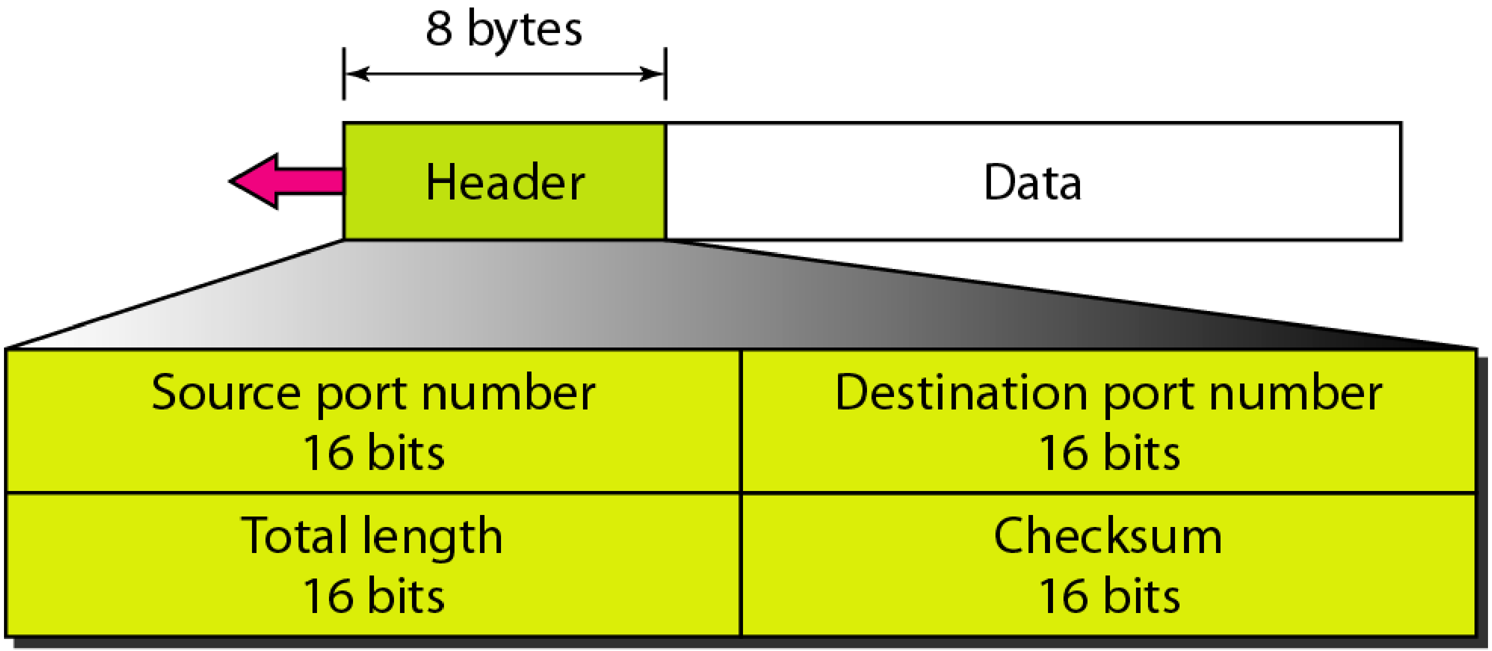
Example 23.1 (continued)

SNMP uses two port numbers (161 and 162), each for a different purpose, as we will see in Chapter 28.



```
$ grep      snmp /etc/services
snmp                161/tcp                #Simple Net  Mgmt Proto
snmp                161/udp                #Simple Net  Mgmt Proto
snmptrap            162/udp                #Traps for SNMP
```

Figure 23.9 *User datagram format*



8 bytes

Header

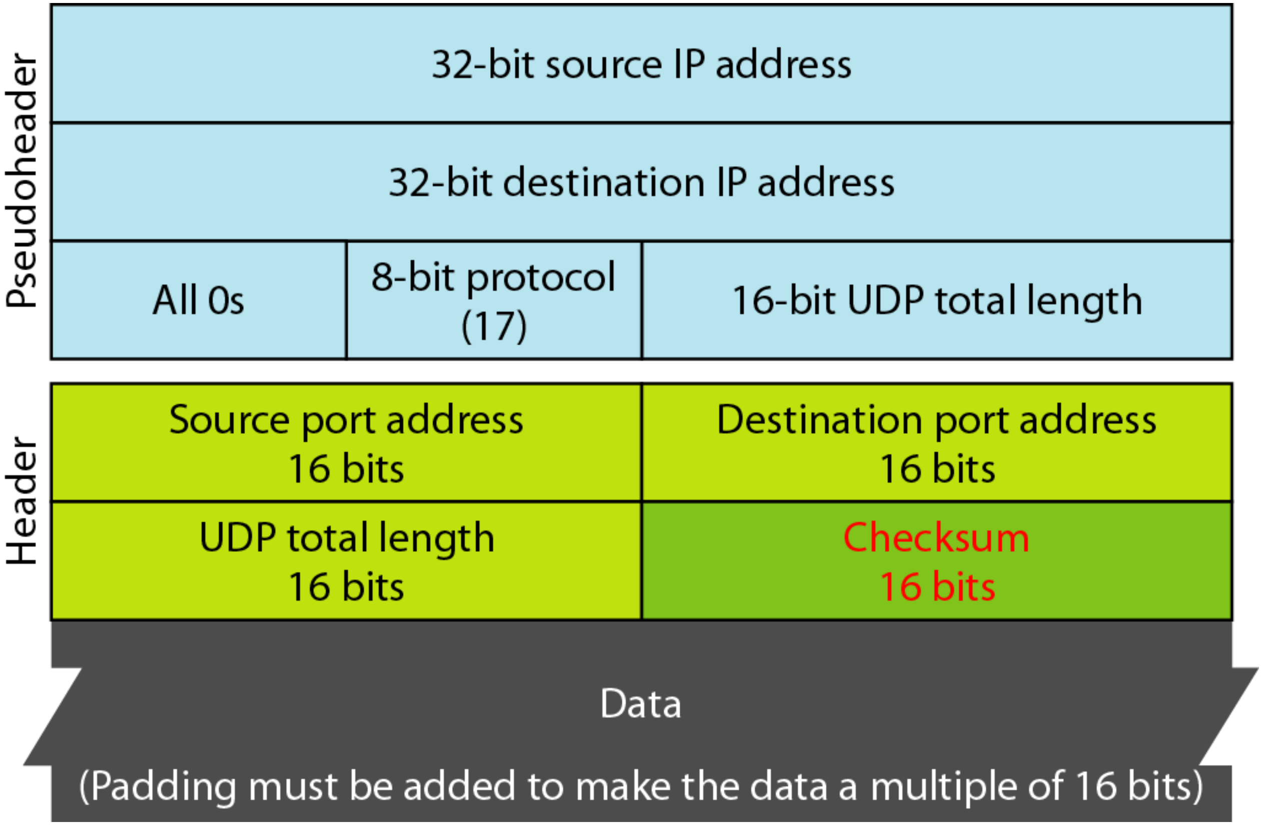
Data

Source port number 16 bits	Destination port number 16 bits
Total length 16 bits	Checksum 16 bits

Note

UDP length
= IP length – IP header's length

Figure 23.10 *Pseudoheader for checksum calculation*

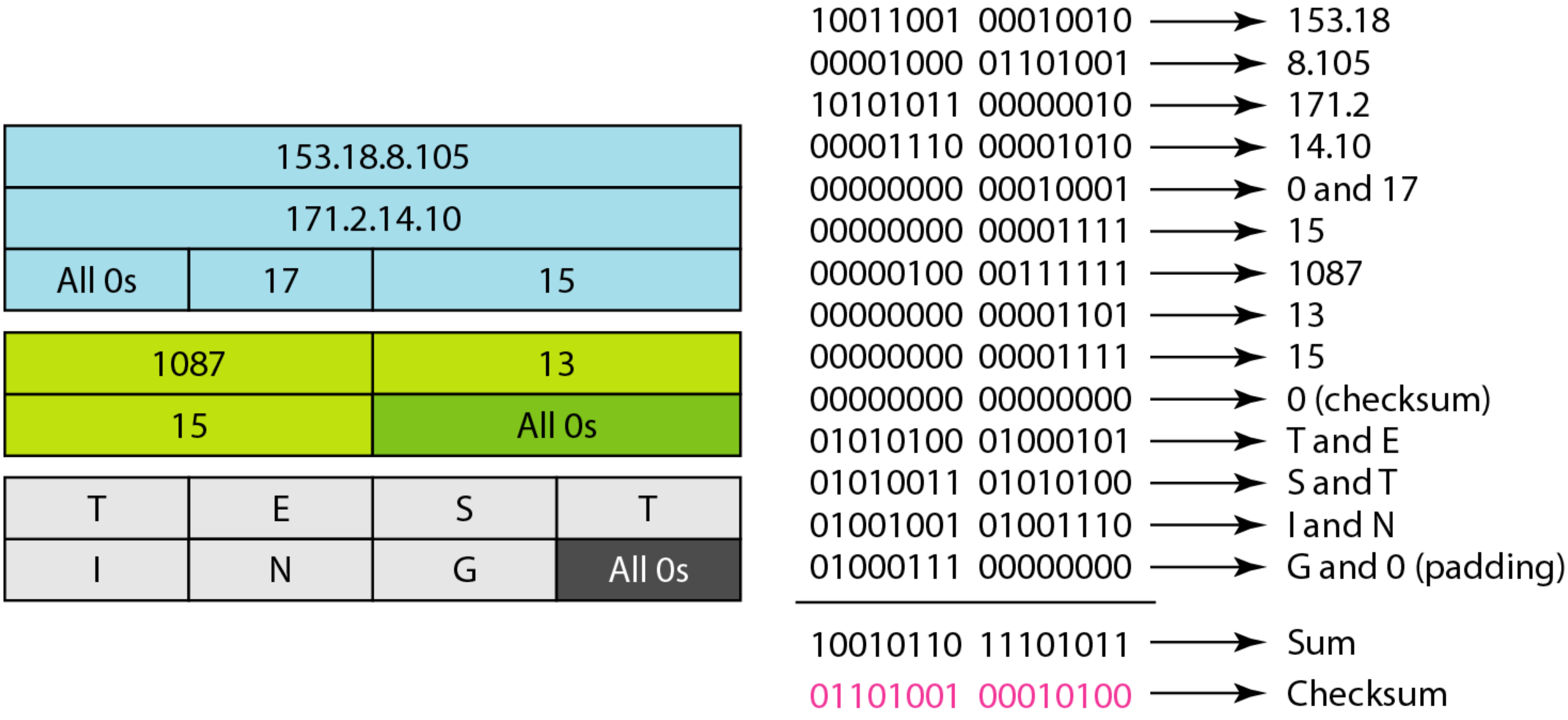


Pseudoheader
32-bit source IP address
32-bit destination IP address
All 0s
8-bit protocol (17)
16-bit UDP total length
Header
Source port address 16 bits
Destination port address 16 bits
UDP total length 16 bits
Checksum 16 bits
Data
(Padding must be added to make the data a multiple of 16 bits)

Example 23.2

Figure 23.11 shows the checksum calculation for a very small user datagram with only 7 bytes of data. Because the number of bytes of data is odd, padding is added for checksum calculation. The pseudoheader as well as the padding will be dropped when the user datagram is delivered to IP.

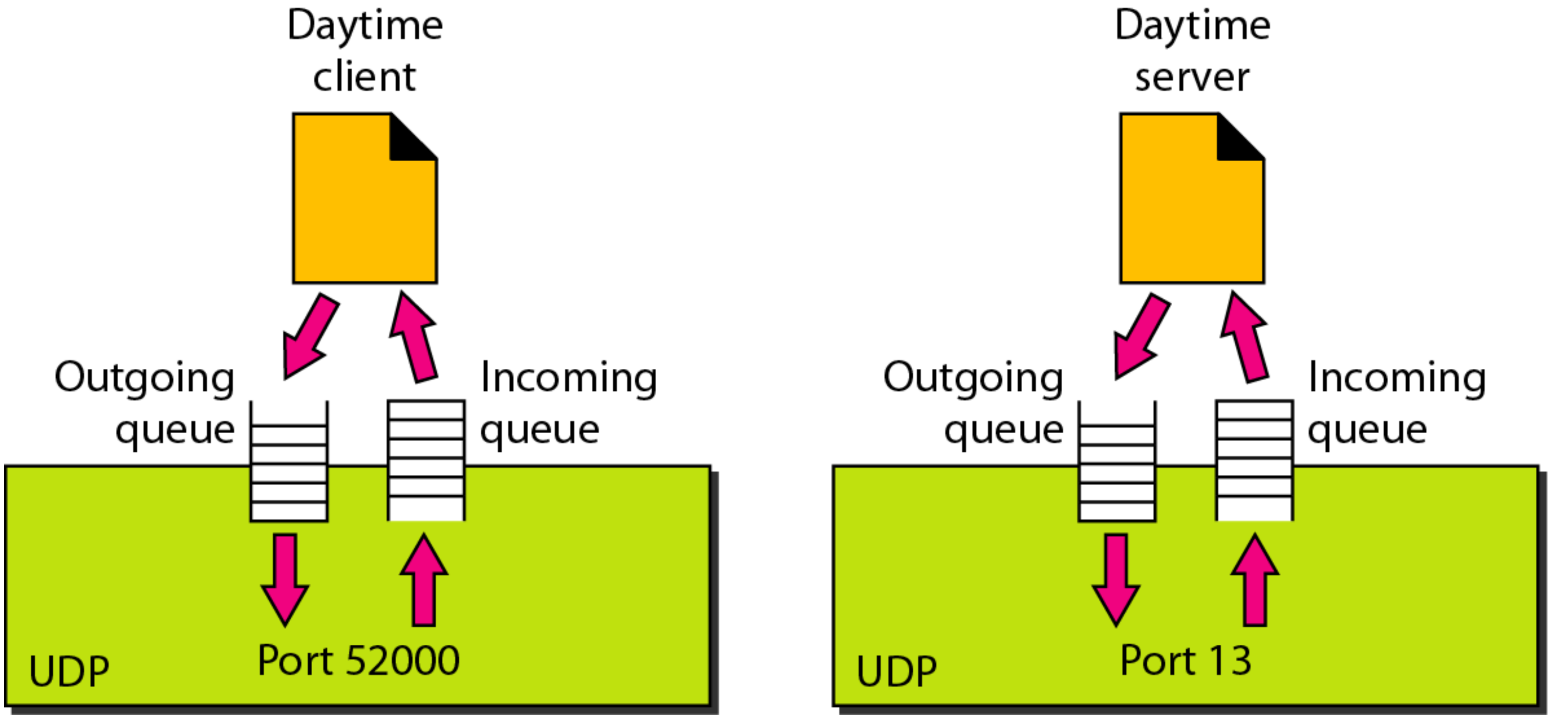
Figure 23.11 *Checksum calculation of a simple UDP user datagram*



153.18.8.105			
171.2.14.10			
All 0s	17	15	
1087		13	
15		All 0s	
T	E	S	T
I	N	G	All 0s

10011001 00010010	153.18
00001000 01101001	8.105
10101011 00000010	171.2
00001110 00001010	14.10
00000000 00010001	0 and 17
00000000 00001111	15
00000100 00111111	1087
00000000 00001101	13
00000000 00001111	15
00000000 00000000	0 (checksum)
01010100 01000101	T and E
01010011 01010100	S and T
01001001 01001110	I and N
01000111 00000000	G and 0 (padding)
10010110 11101011	Sum
01101001 00010100	Checksum

Figure 23.12 ***Queues in UDP***



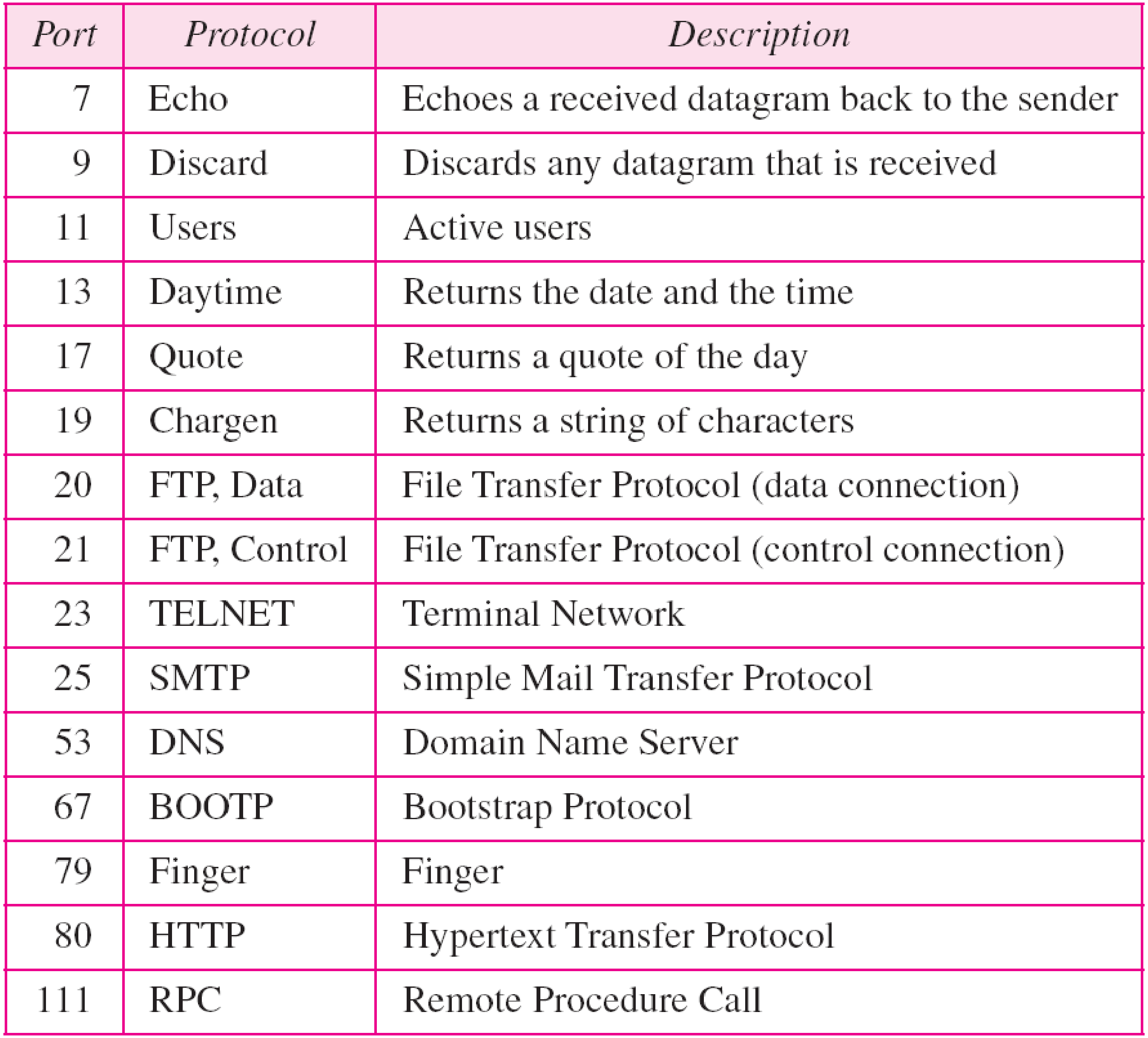
23-3 TCP

TCP is a connection-oriented protocol; it creates a virtual connection between two TCPs to send data. In addition, TCP uses flow and error control mechanisms at the transport level.

Topics discussed in this section:

TCP Services
TCP Features
Segment
A TCP Connection
Flow Control
Error Control

Table 23.2 *Well-known ports used by TCP*



Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
20	FTP, Data	File Transfer Protocol (data connection)
21	FTP, Control	File Transfer Protocol (control connection)
23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

Figure 23.13 *Stream delivery*

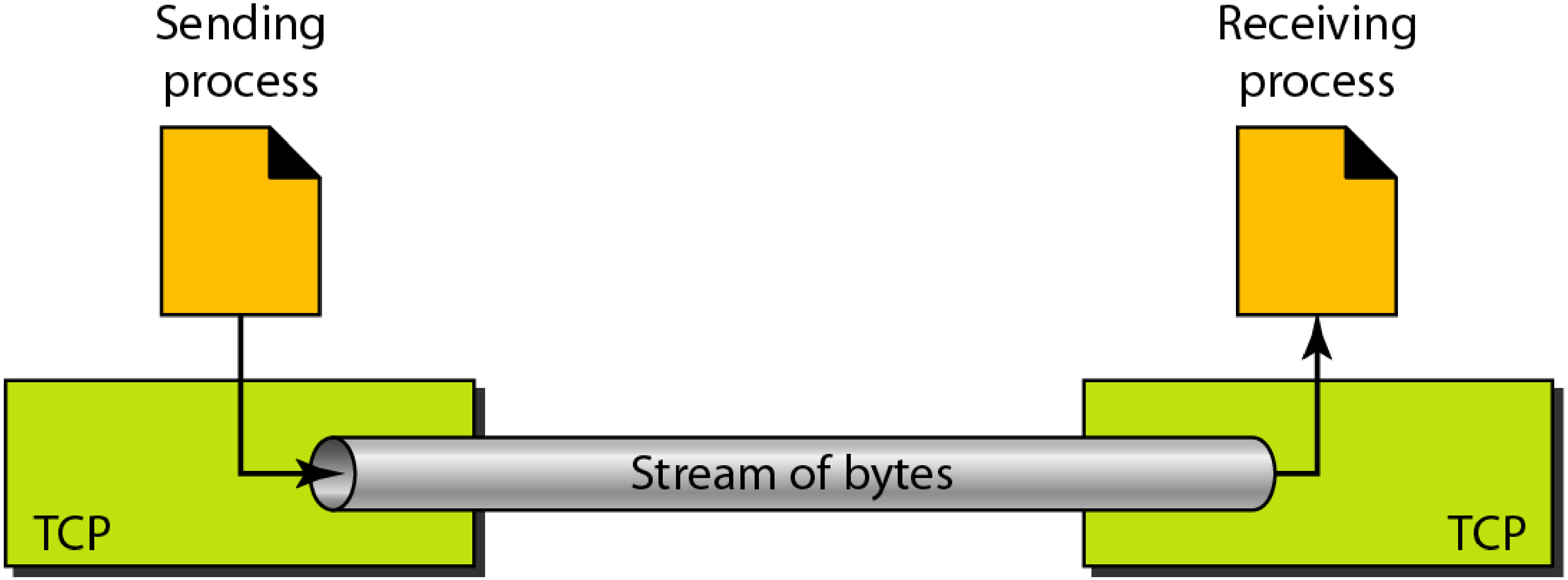


Figure 23.14 *Sending and receiving buffers*

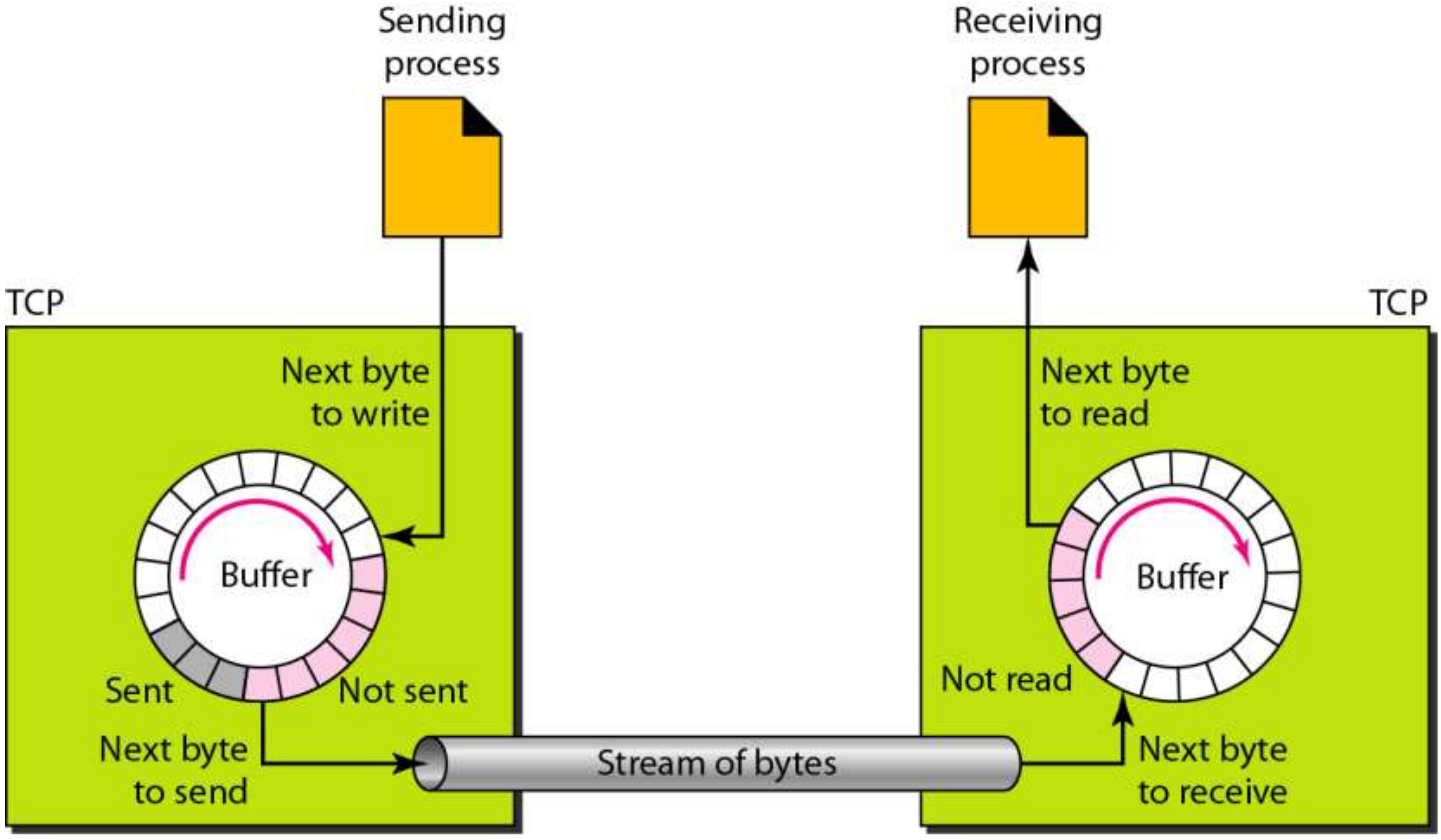
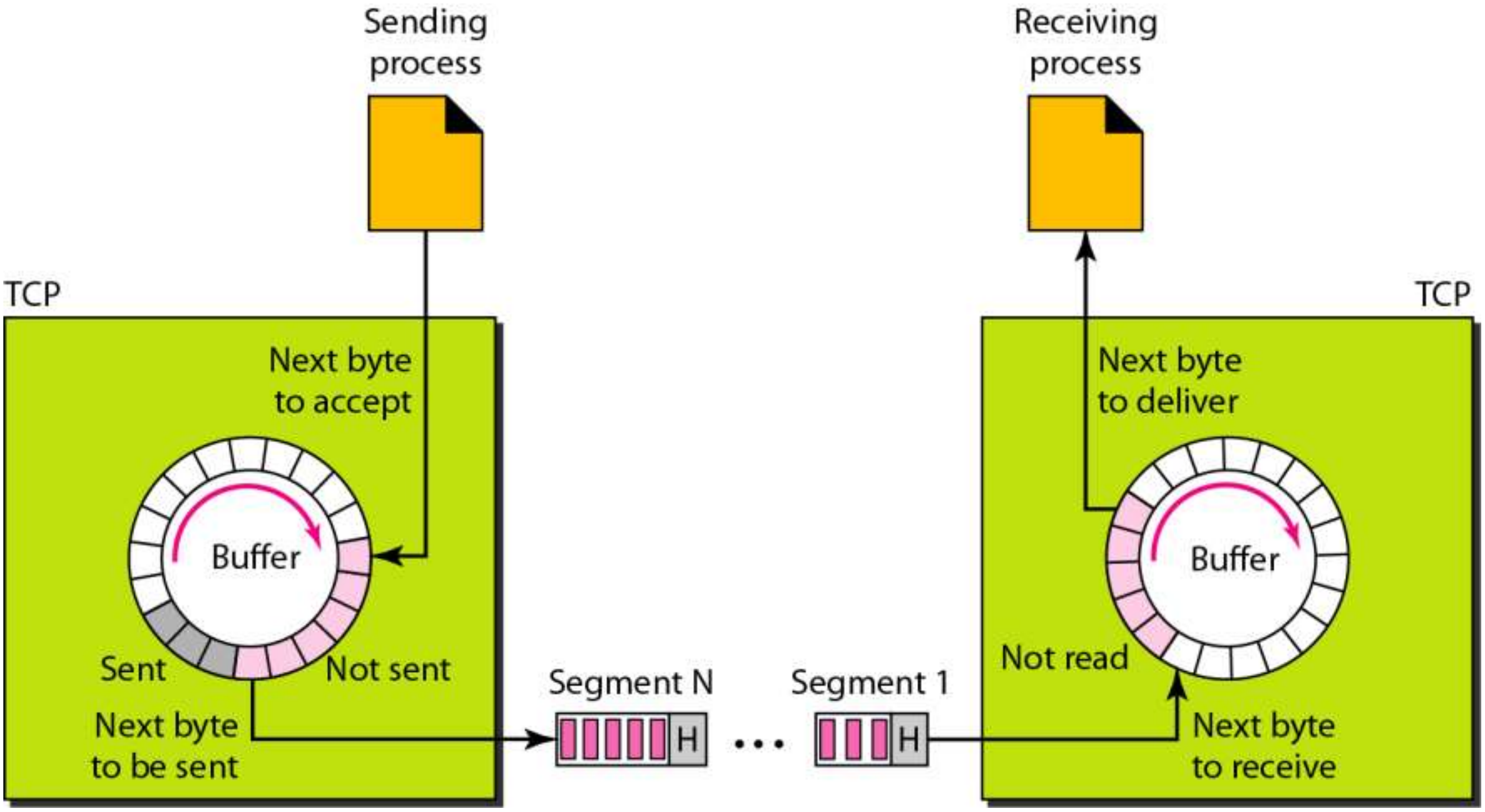


Figure 23.15 *TCP segments*

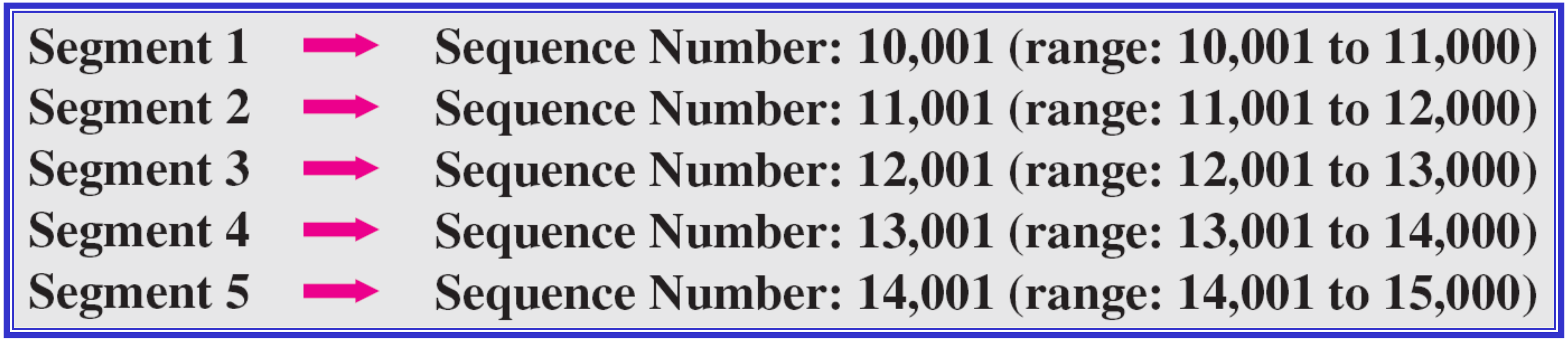


Note

The bytes of data being transferred in each connection are numbered by TCP. The numbering starts with a randomly generated number.

Example 23.3

The following shows the sequence number for each segment:



Segment 1	→	Sequence Number: 10,001 (range: 10,001 to 11,000)
Segment 2	→	Sequence Number: 11,001 (range: 11,001 to 12,000)
Segment 3	→	Sequence Number: 12,001 (range: 12,001 to 13,000)
Segment 4	→	Sequence Number: 13,001 (range: 13,001 to 14,000)
Segment 5	→	Sequence Number: 14,001 (range: 14,001 to 15,000)

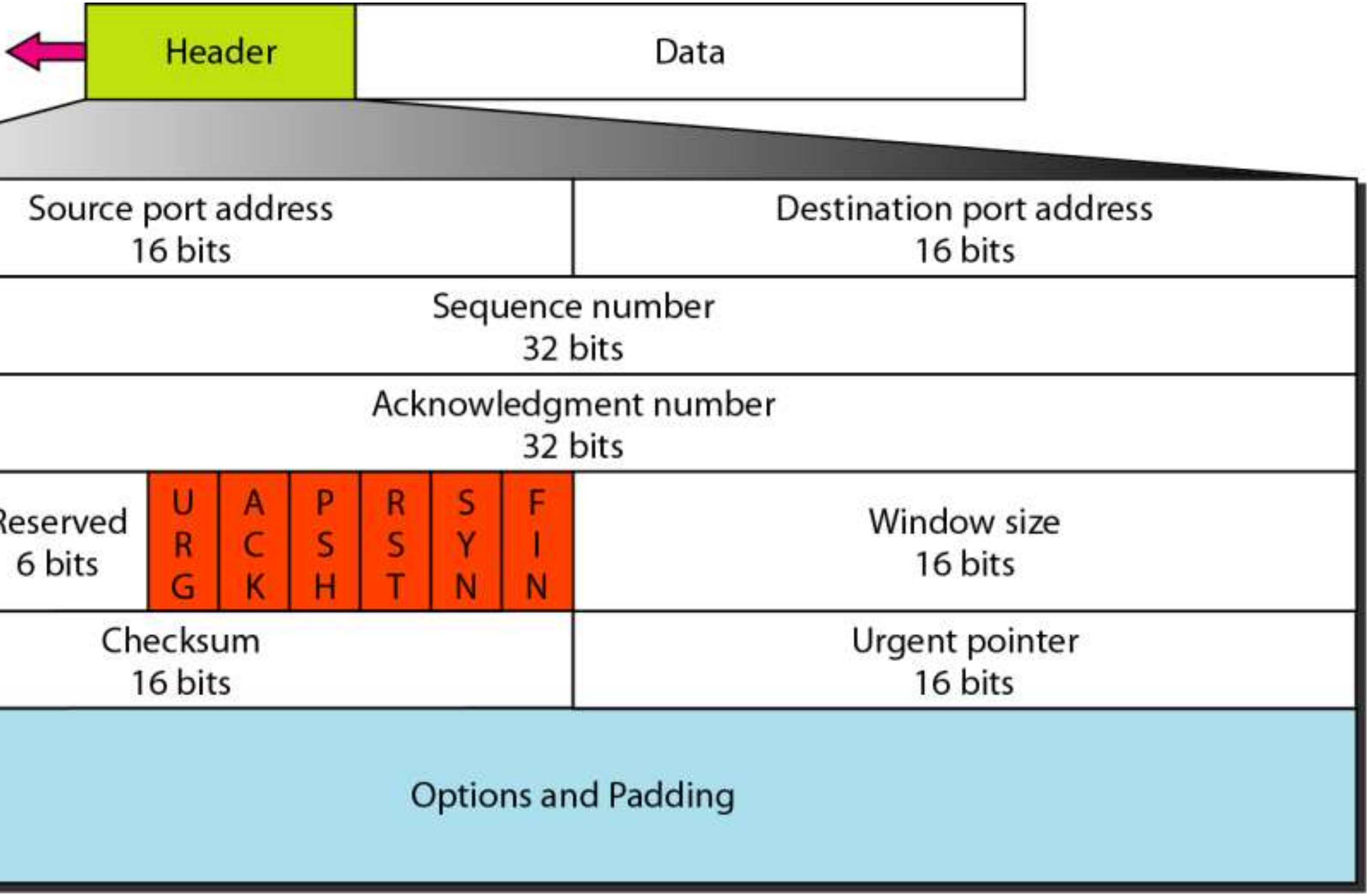
Note

The value in the sequence number field of a segment defines the number of the first data byte contained in that segment.

Note

The value of the acknowledgment field in a segment defines the number of the next byte a party expects to receive.
The acknowledgment number is cumulative.

Figure 23.16 *TCP segment format*



Header

Data

Source port address
16 bits

Destination port address
16 bits

Sequence number
32 bits

Acknowledgment number
32 bits

HLEN
4 bits

Reserved
6 bits

URG

ACK

PSH

RST

SYN

FIN

Window size
16 bits

Checksum
16 bits

Urgent pointer
16 bits

Options and Padding

Figure 23.17 *Control field*

URG: Urgent pointer is valid
ACK: Acknowledgment is valid
PSH: Request for push

RST: Reset the connection
SYN: Synchronize sequence numbers
FIN: Terminate the connection

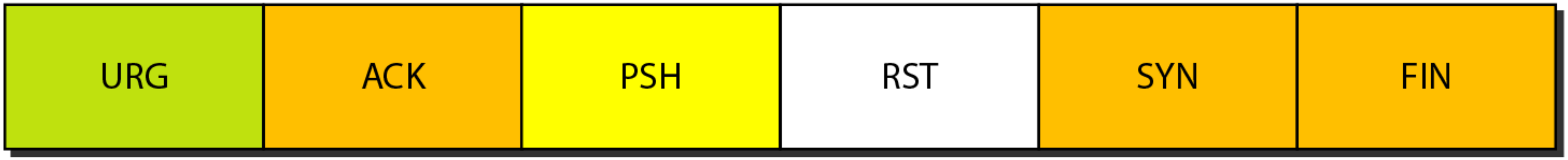
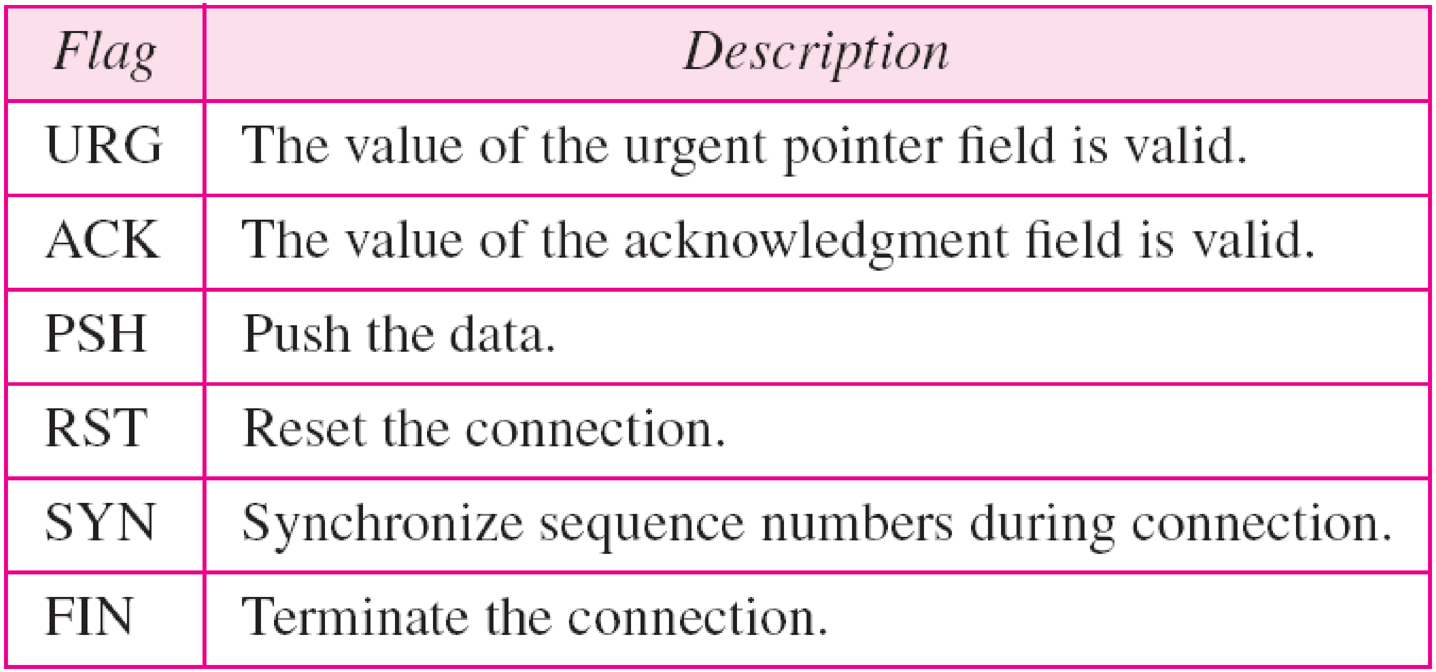
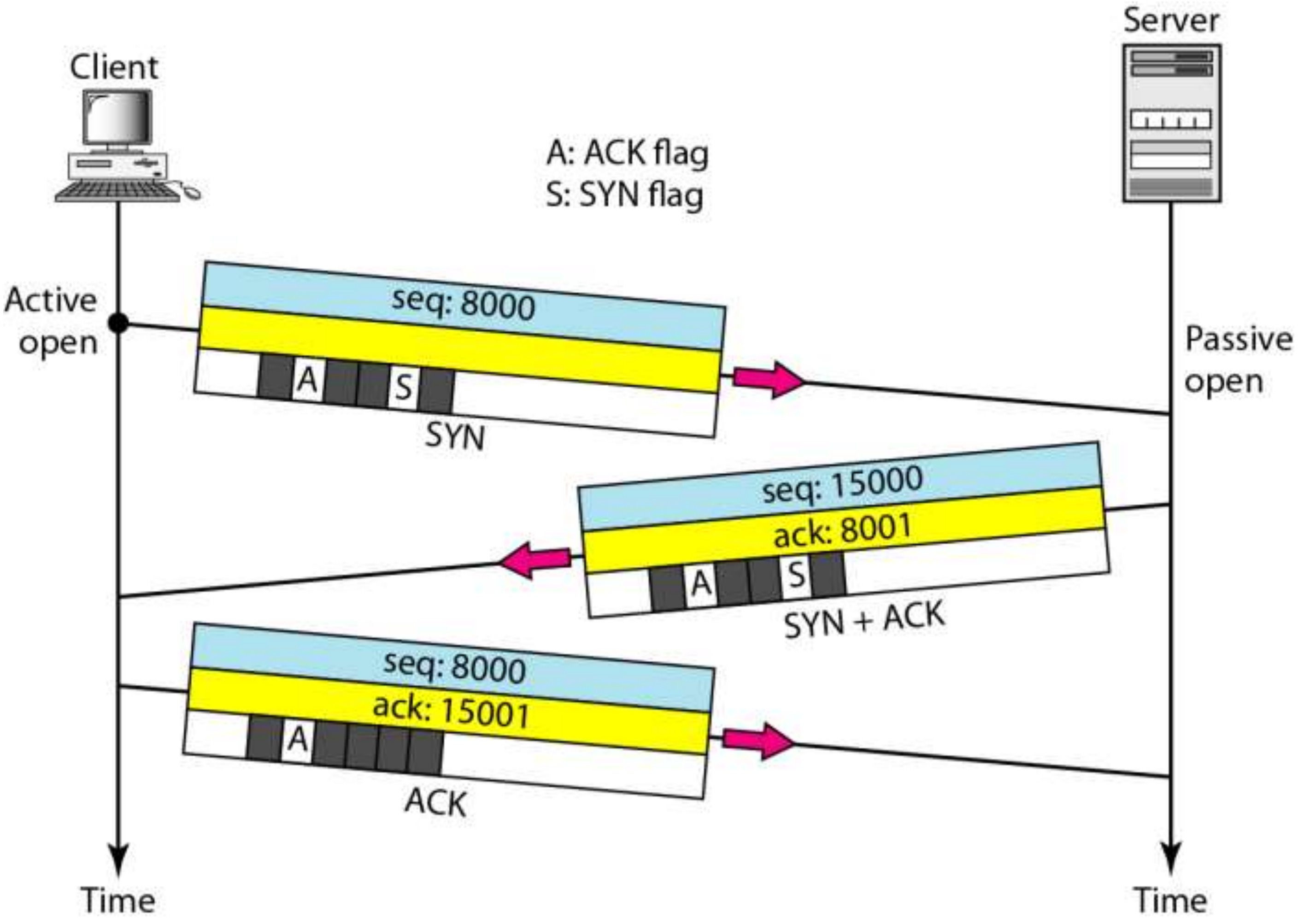


Table 23.3 ***Description of flags in the control field***



Flag	*Description*
URG	The value of the urgent pointer field is valid.
ACK	The value of the acknowledgment field is valid.
PSH	Push the data.
RST	Reset the connection.
SYN	Synchronize sequence numbers during connection.
FIN	Terminate the connection.

Figure 23.18 *Connection establishment using three-way handshaking*



Note

A SYN segment cannot carry data, but it consumes one sequence number.

Note

A SYN + ACK segment cannot carry data, but does consume one sequence number.

Note

An ACK segment, if carrying no data, consumes no sequence number.

Figure 23.19 *Data transfer*

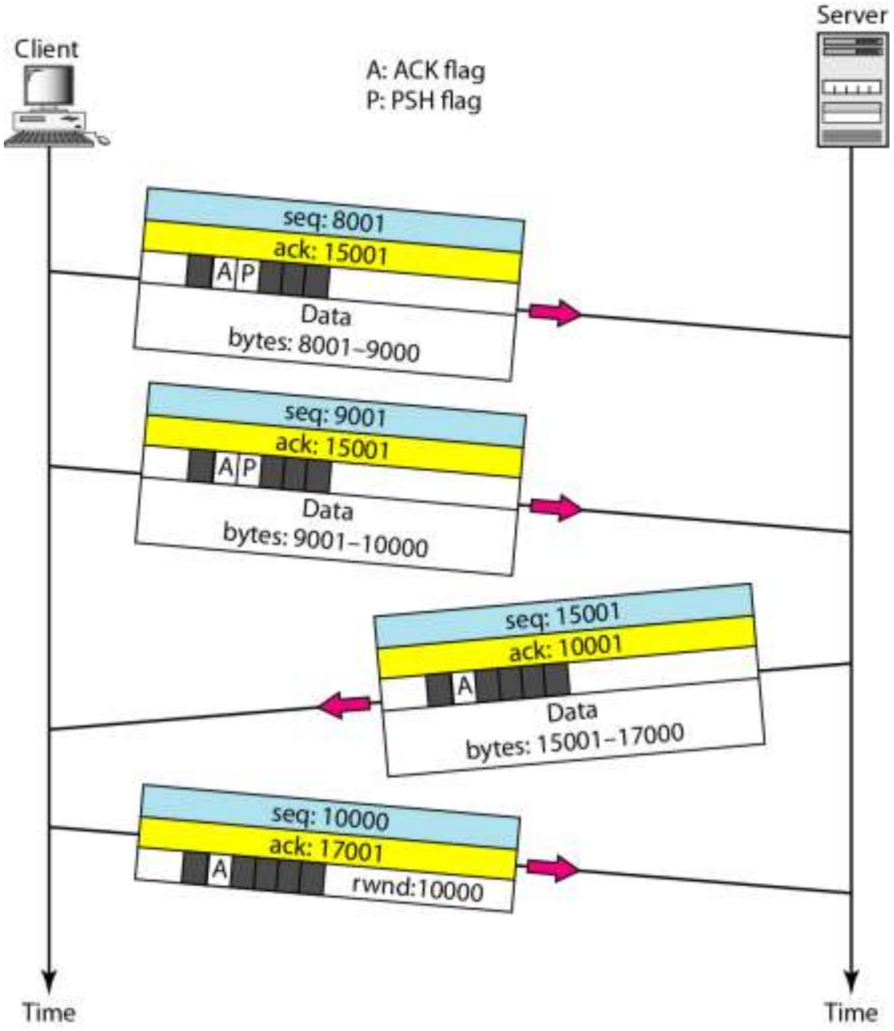
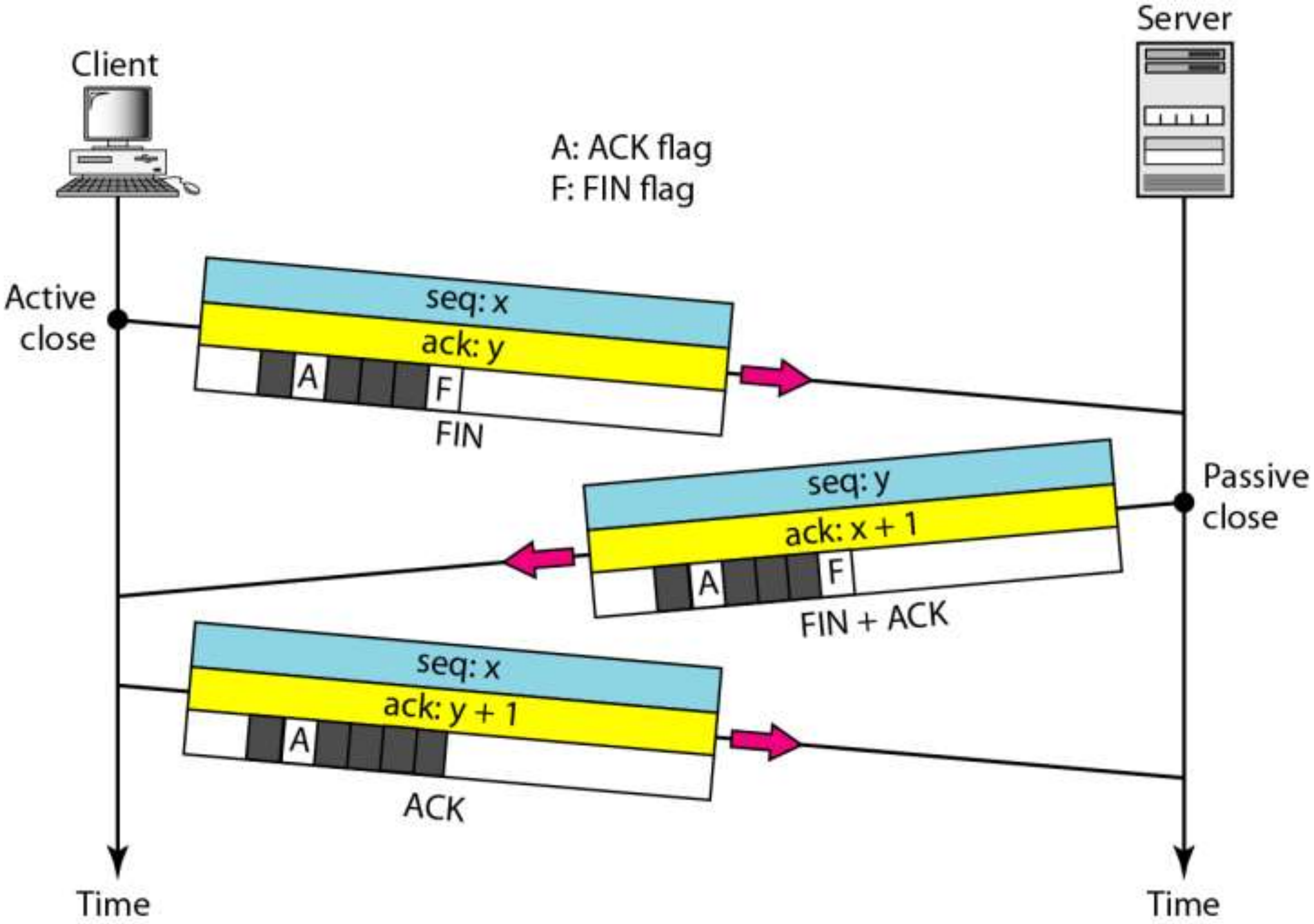


Figure 23.20 *Connection termination using three-way handshaking*



Note

The FIN segment consumes one sequence number if it does not carry data.

Note

The FIN + ACK segment consumes one sequence number if it does not carry data.

Figure 23.21 *Half-close*

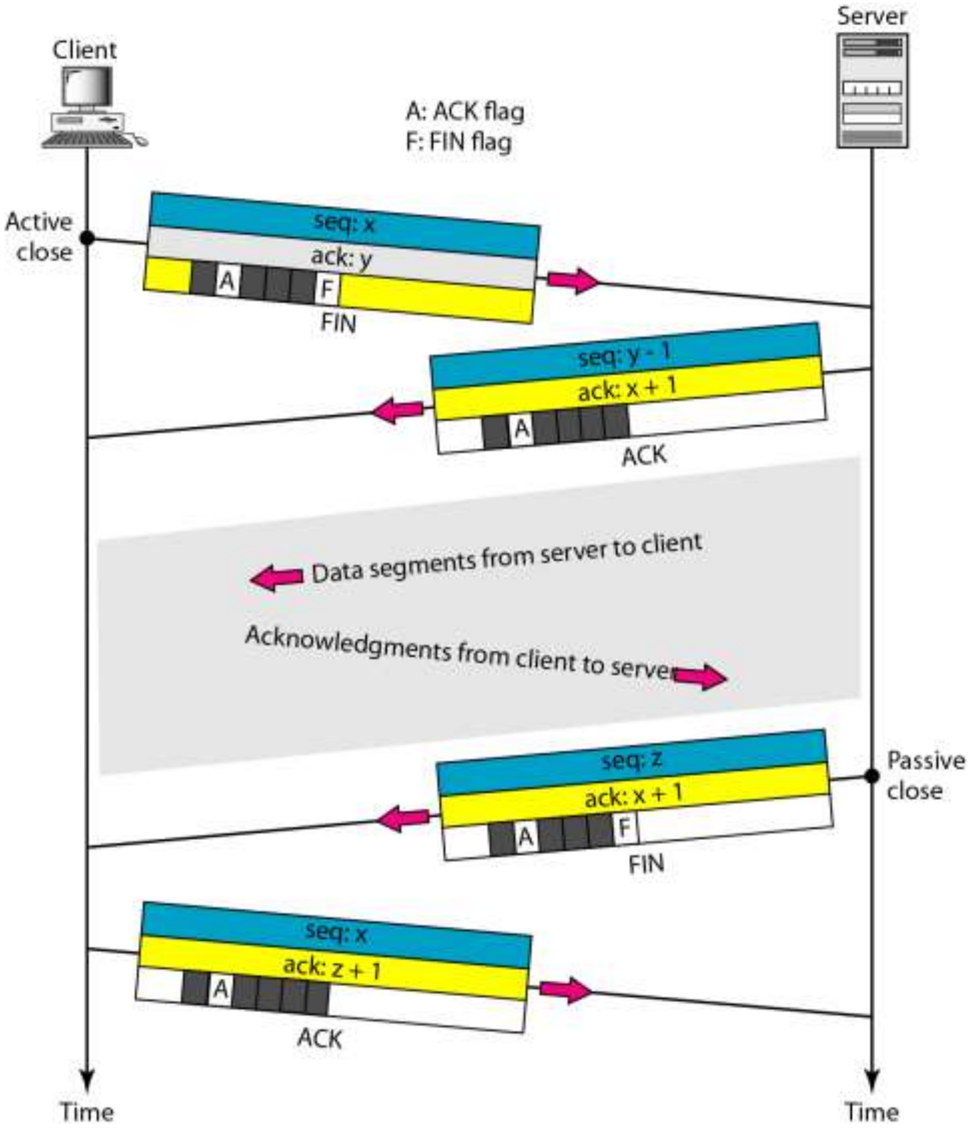
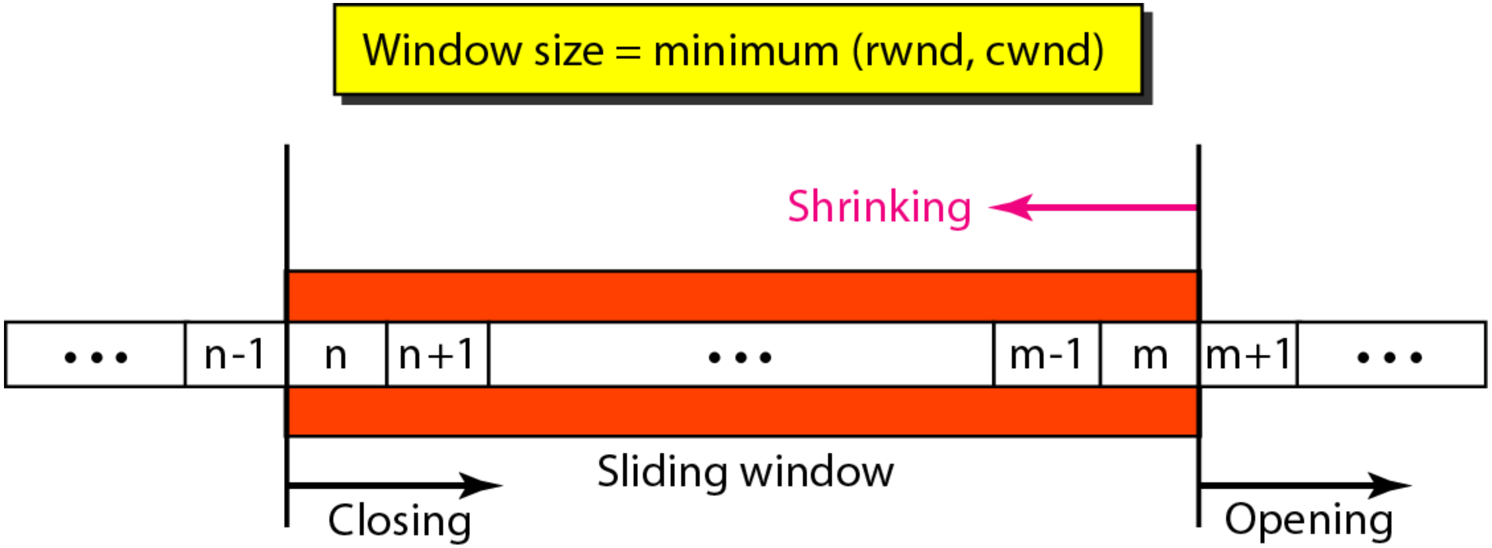


Figure 23.22 *Sliding window*



Note

A sliding window is used to make transmission more efficient as well as to control the flow of data so that the destination does not become overwhelmed with data.

TCP sliding windows are byte-oriented.

Example 23.4

What is the value of the receiver window (rwnd) for host A if the receiver, host B, has a buffer size of 5000 bytes and 1000 bytes of received and unprocessed data?

Solution

The value of rwnd = 5000 − 1000 = 4000. Host B can receive only 4000 bytes of data before overflowing its buffer. Host B advertises this value in its next segment to A.

Example 23.5

What is the size of the window for host A if the value of rwnd is 3000 bytes and the value of cwnd is 3500 bytes?

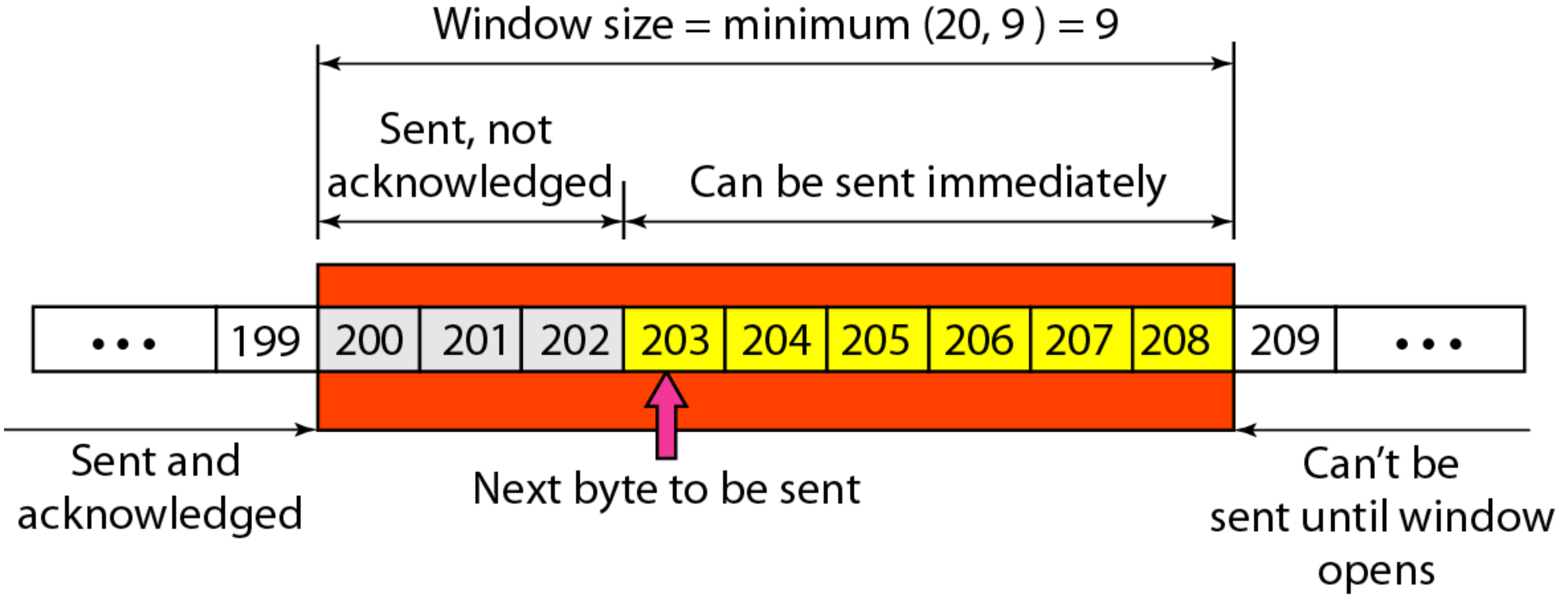
Solution

The size of the window is the smaller of rwnd and cwnd, which is 3000 bytes.

Example 23.6

Figure 23.23 shows an unrealistic example of a sliding window. The sender has sent bytes up to 202. We assume that cwnd is 20 (in reality this value is thousands of bytes). The receiver has sent an acknowledgment number of 200 with an rwnd of 9 bytes (in reality this value is thousands of bytes). The size of the sender window is the minimum of rwnd and cwnd, or 9 bytes. Bytes 200 to 202 are sent, but not acknowledged. Bytes 203 to 208 can be sent without worrying about acknowledgment. Bytes 209 and above cannot be sent.

Figure 23.23 *Example 23.6*



Note

Some points about TCP sliding windows:

- ❑ The size of the window is the lesser of rwnd and cwnd.
- ❑ The source does not have to send a full window’s worth of data.
- ❑ The window can be opened or closed by the receiver, but should not be shrunk.
- ❑ The destination can send an acknowledgment at any time as long as it does not result in a shrinking window.
- ❑ The receiver can temporarily shut down the window; the sender, however, can always send a segment of 1 byte after the window is shut down.

Note

ACK segments do not consume sequence numbers and are not acknowledged.

Note

In modern implementations, a retransmission occurs if the retransmission timer expires or three duplicate ACK segments have arrived.

Note

No retransmission timer is set for an ACK segment.

Note

Data may arrive out of order and be temporarily stored by the receiving TCP, but TCP guarantees that no out-of-order segment is delivered to the process.

Figure 23.24 ***Normal operation***

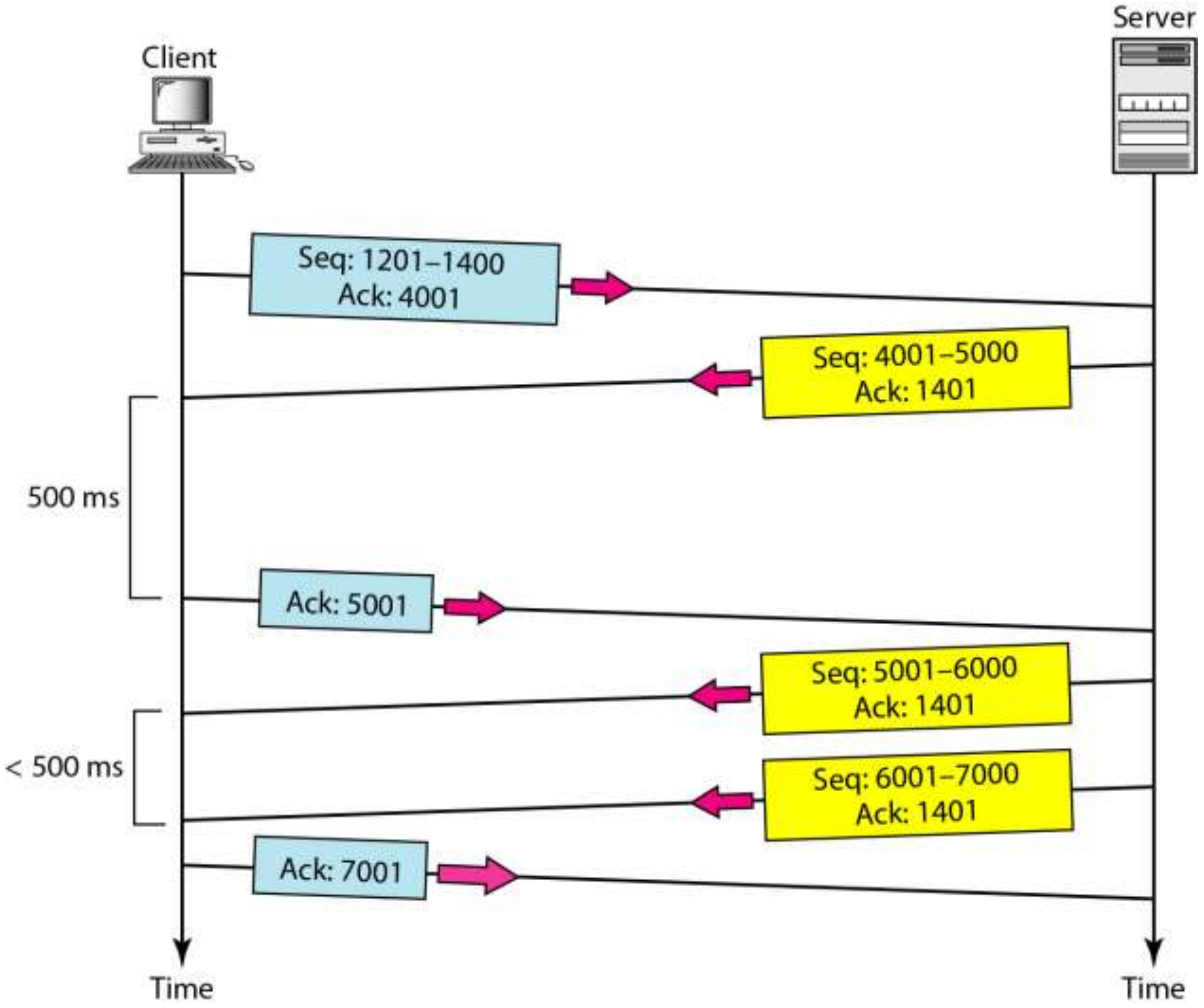
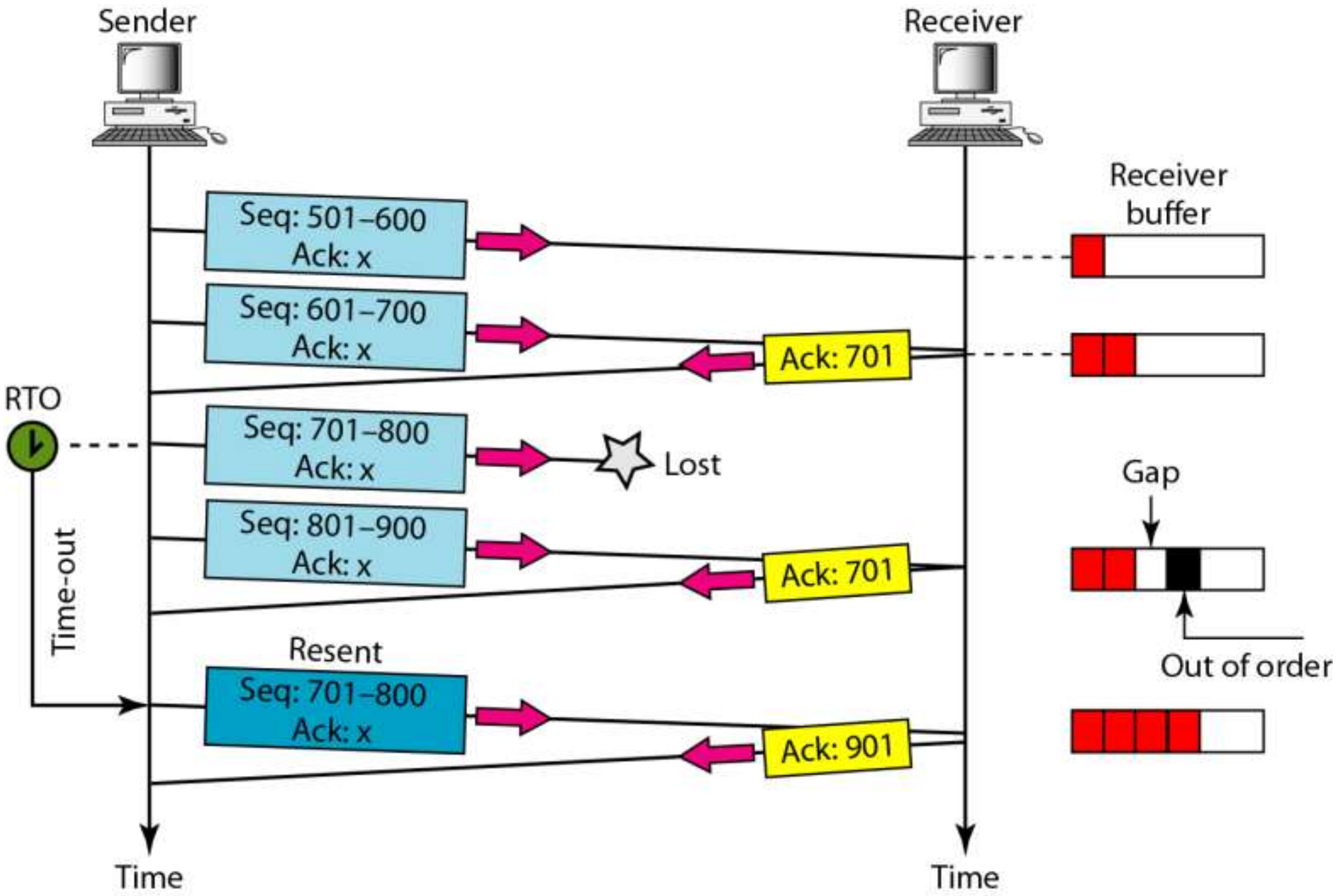


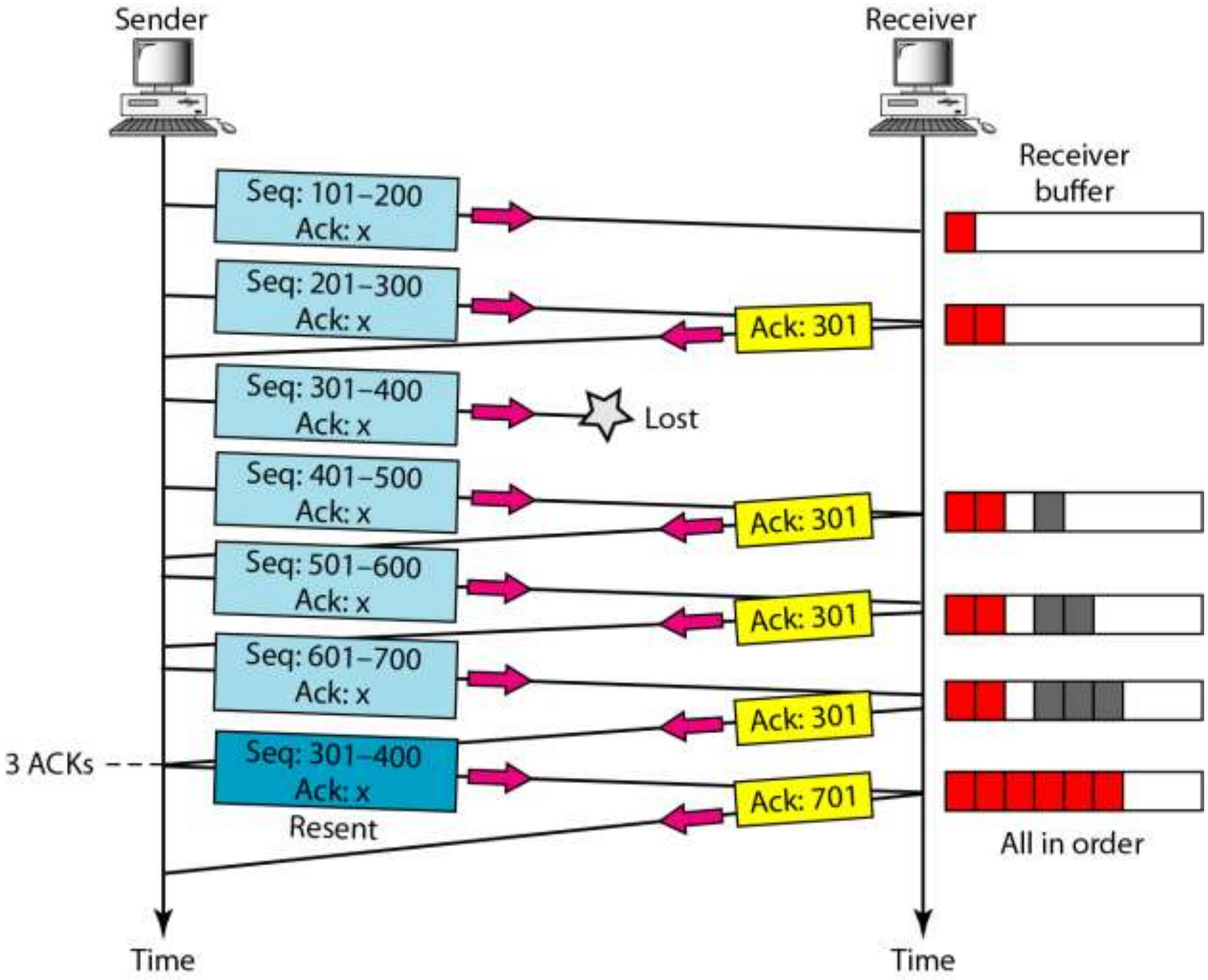
Figure 23.25 *Lost segment*



Note

The receiver TCP delivers only ordered data to the process.

Figure 23.26 *Fast retransmission*



23-4 SCTP

Stream Control Transmission Protocol (SCTP) is a new reliable, message-oriented transport layer protocol. SCTP, however, is mostly designed for Internet applications that have recently been introduced. These new applications need a more sophisticated service than TCP can provide.

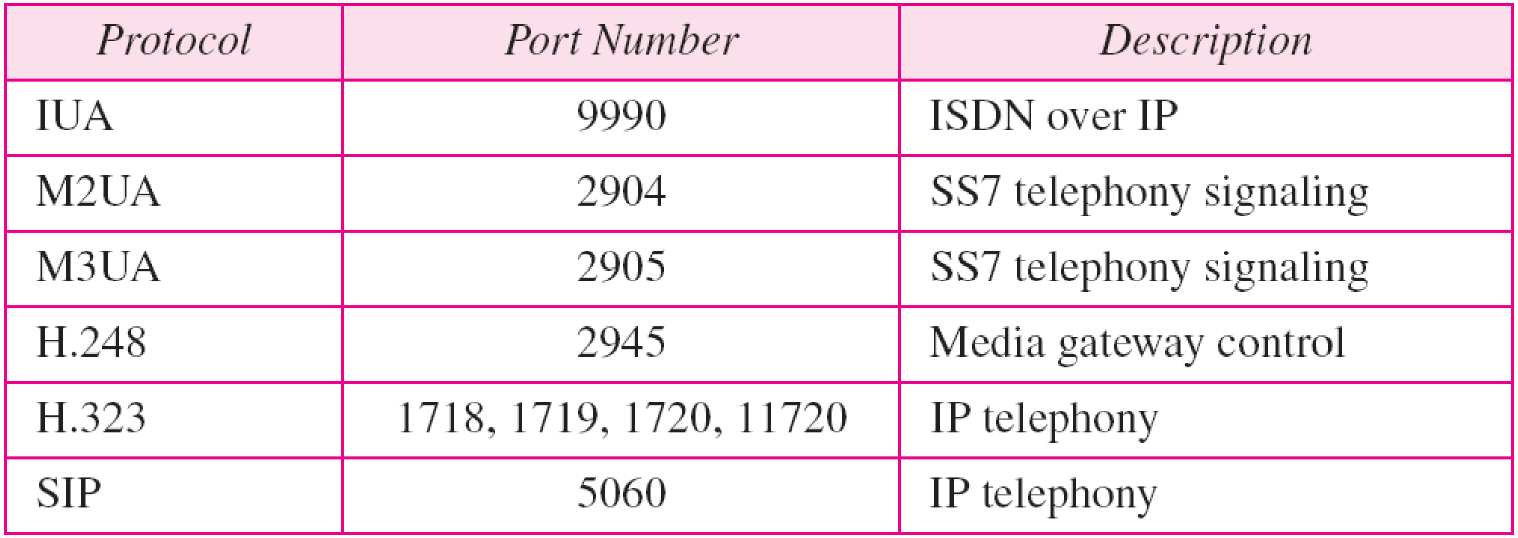
Topics discussed in this section:

SCTP Services and Features
Packet Format
An SCTP Association
Flow Control and Error Control

Note

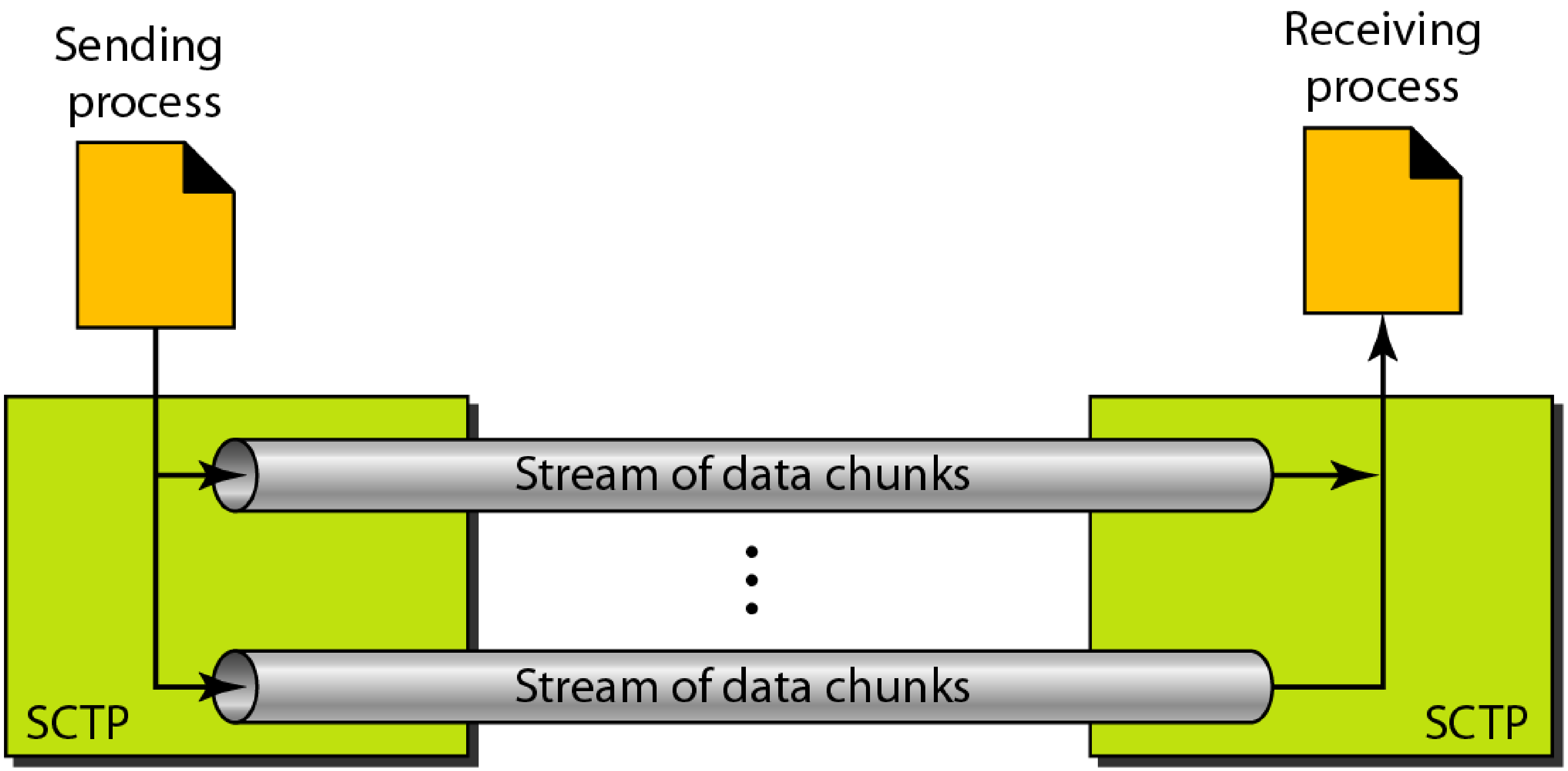
SCTP is a message-oriented, reliable protocol that combines the best features of UDP and TCP.

Table 23.4 *Some SCTP applications*



Protocol	*Port Number*	*Description*
IUA	9990	ISDN over IP
M2UA	2904	SS7 telephony signaling
M3UA	2905	SS7 telephony signaling
H.248	2945	Media gateway control
H.323	1718, 1719, 1720, 11720	IP telephony
SIP	5060	IP telephony

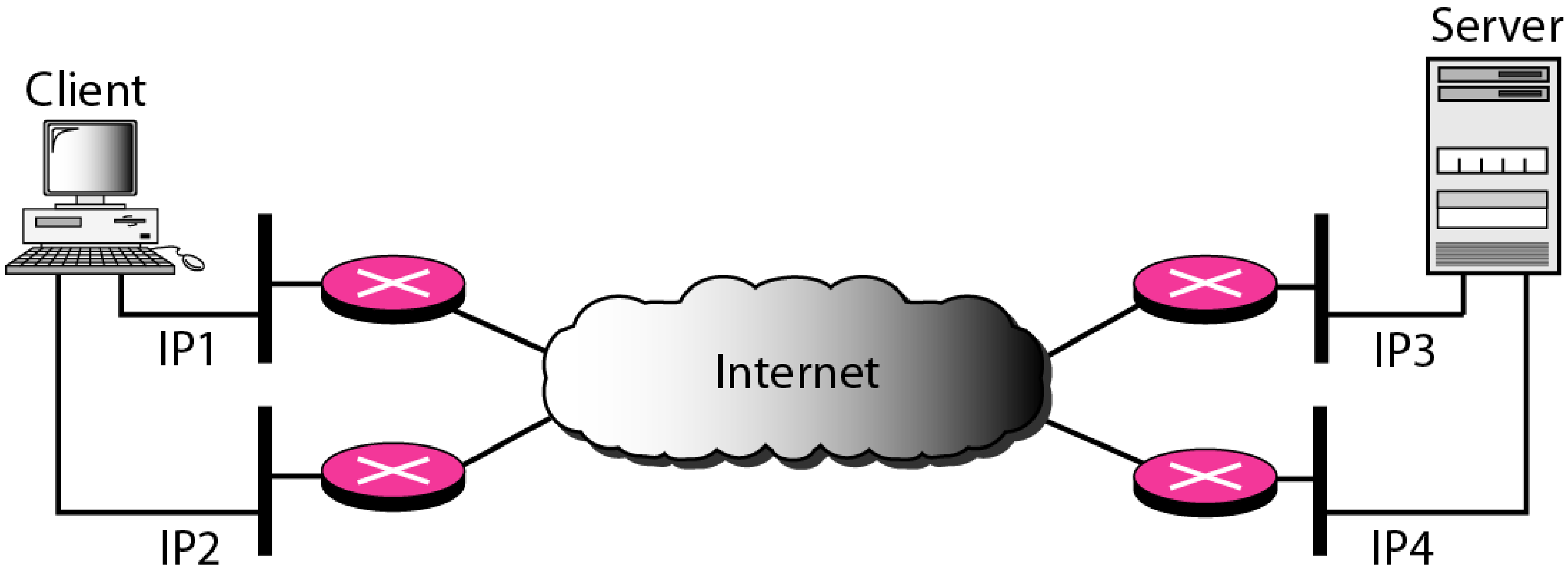
Figure 23.27 *Multiple-stream concept*



Note

An association in SCTP can involve multiple streams.

Figure 23.28 *Multihoming concept*



Note

SCTP association allows multiple IP addresses for each end.

Note

In SCTP, a data chunk is numbered using a TSN.

Note

To distinguish between different streams, SCTP uses an SI.

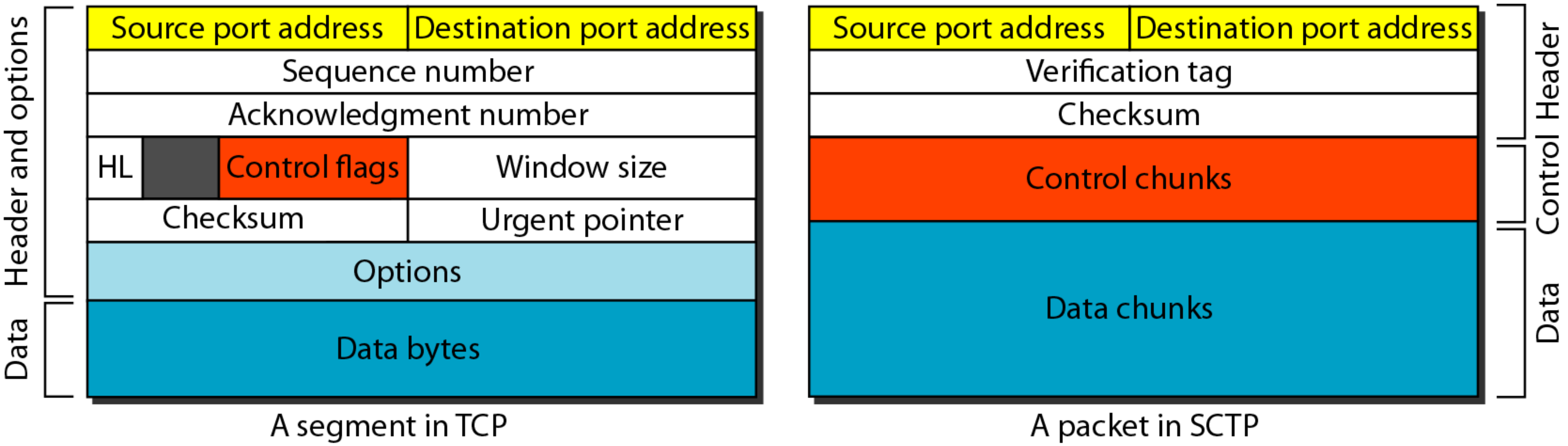
Note

To distinguish between different data chunks belonging to the same stream, SCTP uses SSNs.

Note

TCP has segments; SCTP has packets.

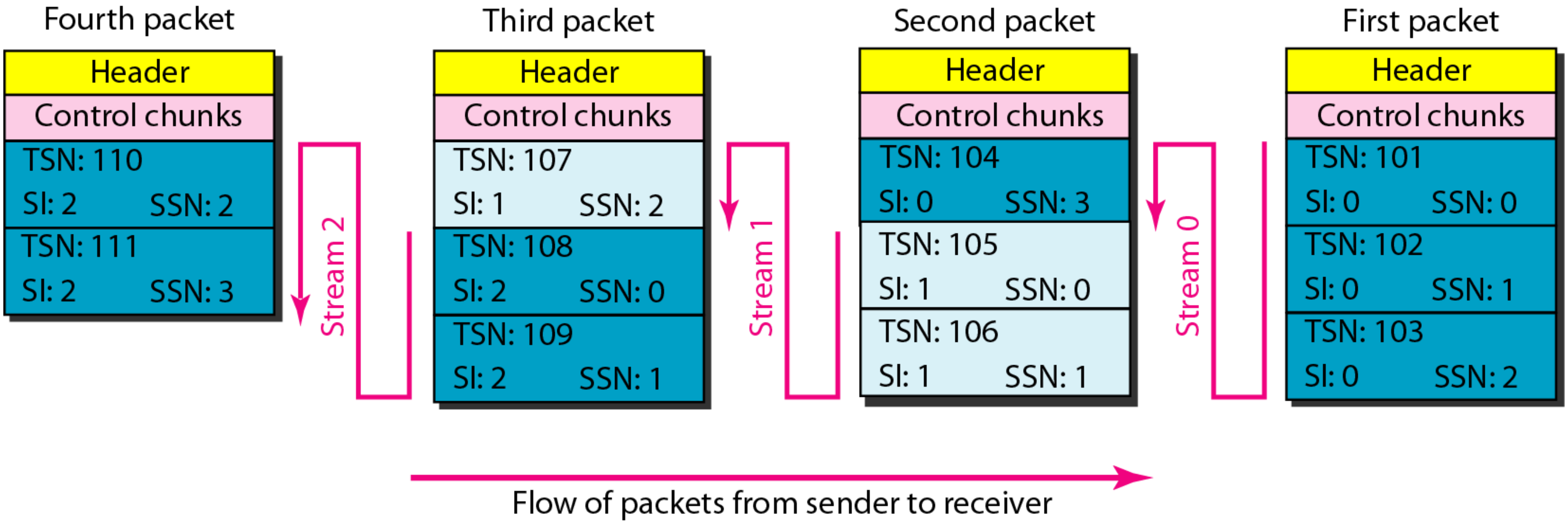
Figure 23.29 *Comparison between a TCP segment and an SCTP packet*



Note

In SCTP, control information and data information are carried in separate chunks.

Figure 23.30 *Packet, data chunks, and streams*



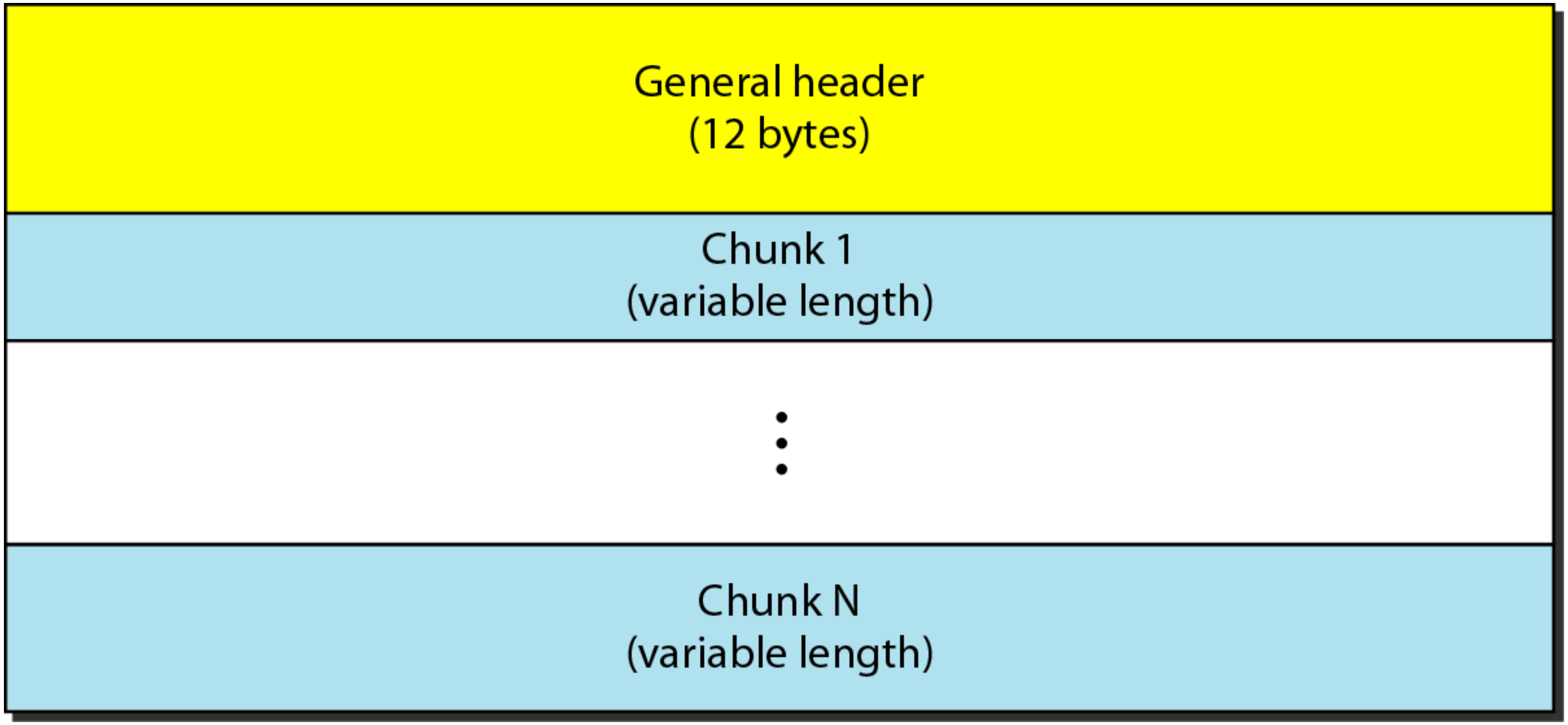
Note

**Data chunks are identified by three items: TSN, SI, and SSN.
TSN is a cumulative number identifying the association; SI defines the stream; SSN defines the chunk in a stream.**

Note

In SCTP, acknowledgment numbers are used to acknowledge only data chunks; control chunks are acknowledged by other control chunks if necessary.

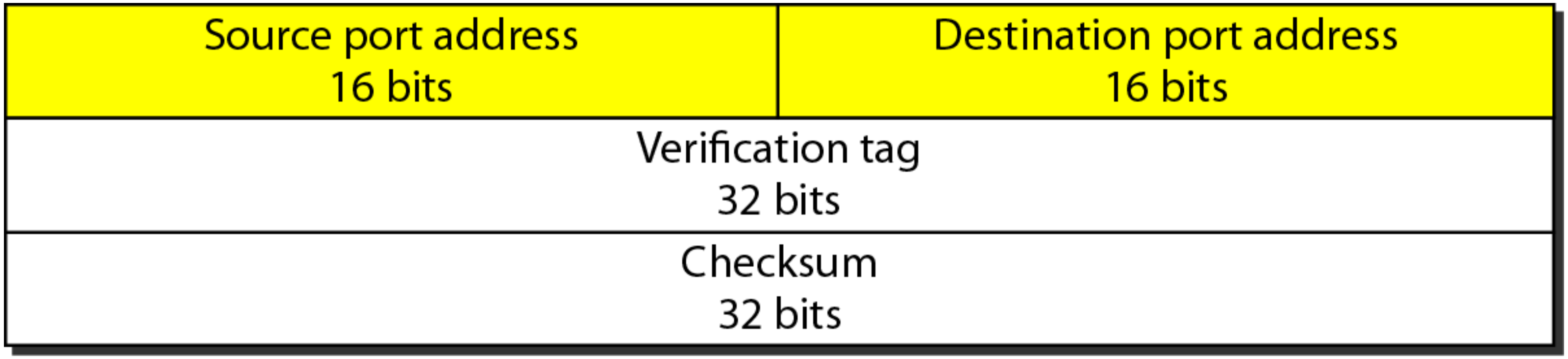
Figure 23.31 *SCTP packet format*



Note

In an SCTP packet, control chunks come before data chunks.

Figure 23.32 *General header*



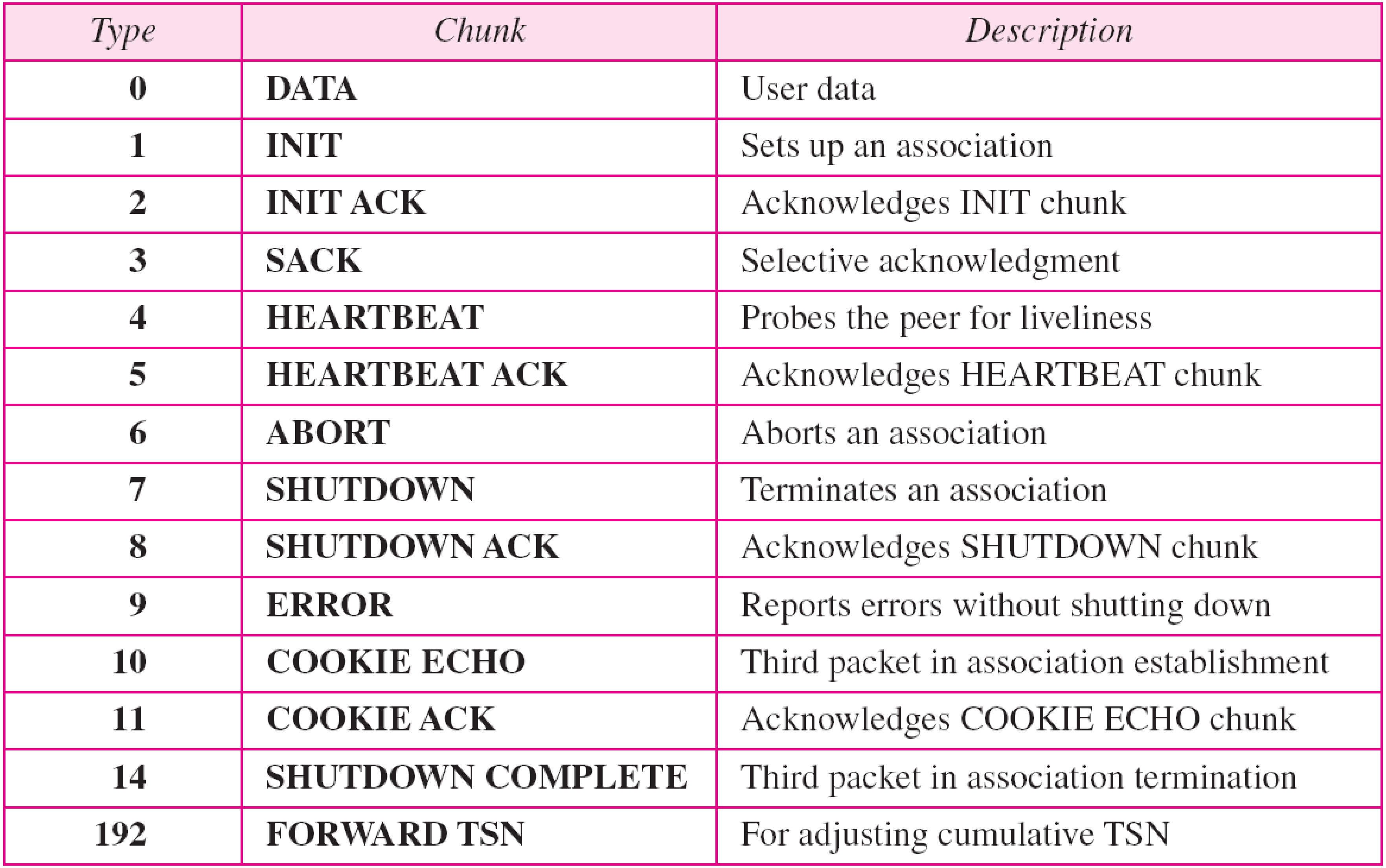
Source port address
16 bits

Destination port address
16 bits

Verification tag
32 bits

Checksum
32 bits

Table 23.5 ***Chunks***



Type	*Chunk*	*Description*
0	**DATA**	User data
1	**INIT**	Sets up an association
2	**INIT ACK**	Acknowledges INIT chunk
3	**SACK**	Selective acknowledgment
4	**HEARTBEAT**	Probes the peer for liveliness
5	**HEARTBEAT ACK**	Acknowledges HEARTBEAT chunk
6	**ABORT**	Aborts an association
7	**SHUTDOWN**	Terminates an association
8	**SHUTDOWN ACK**	Acknowledges SHUTDOWN chunk
9	**ERROR**	Reports errors without shutting down
10	**COOKIE ECHO**	Third packet in association establishment
11	**COOKIE ACK**	Acknowledges COOKIE ECHO chunk
14	**SHUTDOWN COMPLETE**	Third packet in association termination
192	**FORWARD TSN**	For adjusting cumulative TSN

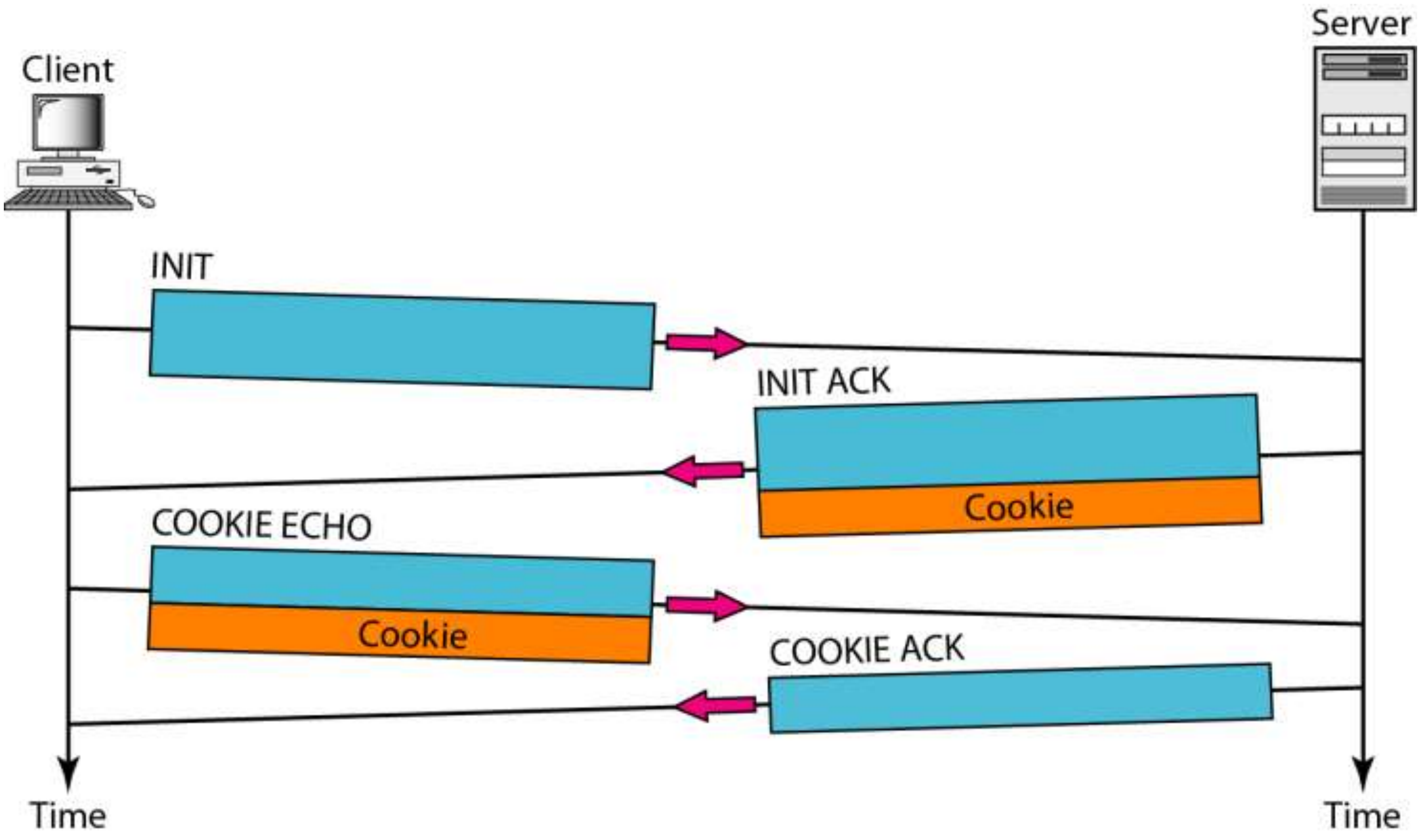
Note

A connection in SCTP is called an association.

Note

No other chunk is allowed in a packet carrying an INIT or INIT ACK chunk. A COOKIE ECHO or a COOKIE ACK chunk can carry data chunks.

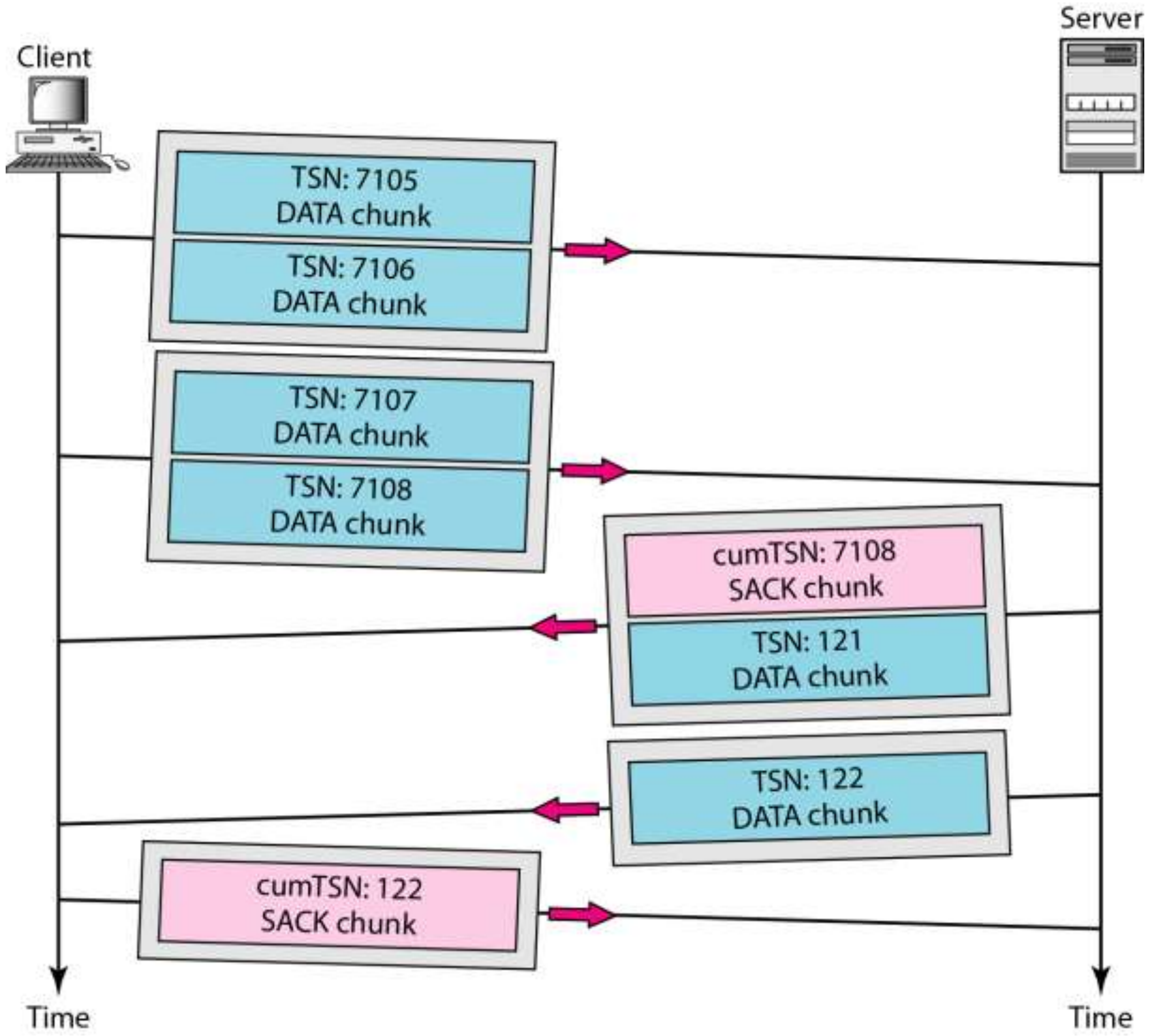
Figure 23.33 *Four-way handshaking*



Note

**In SCTP, only DATA chunks consume TSNs;
DATA chunks are the only chunks that are acknowledged.**

Figure 23.34 *Simple data transfer*



Note

The acknowledgment in SCTP defines the cumulative TSN, the TSN of the last data chunk received in order.

Figure 23.35 *Association termination*

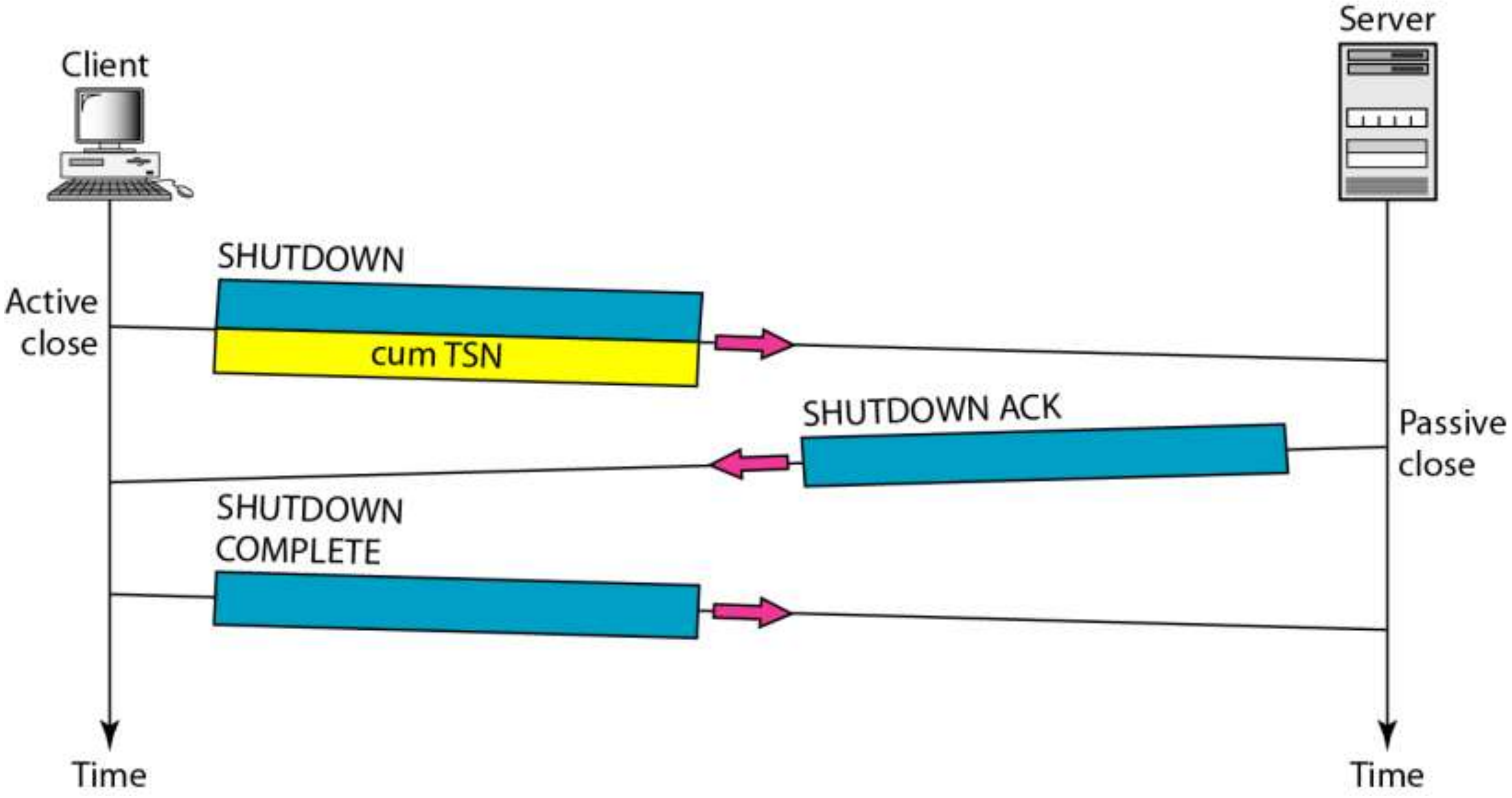


Figure 23.36 *Flow control, receiver site*

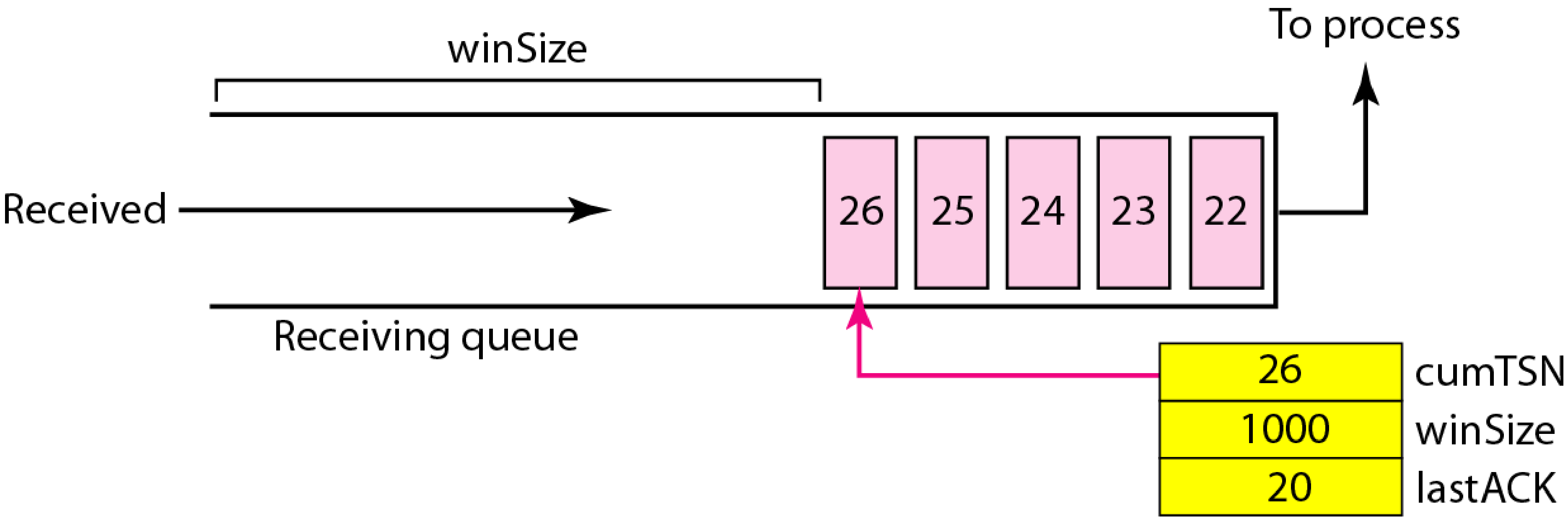


Figure 23.37 *Flow control, sender site*

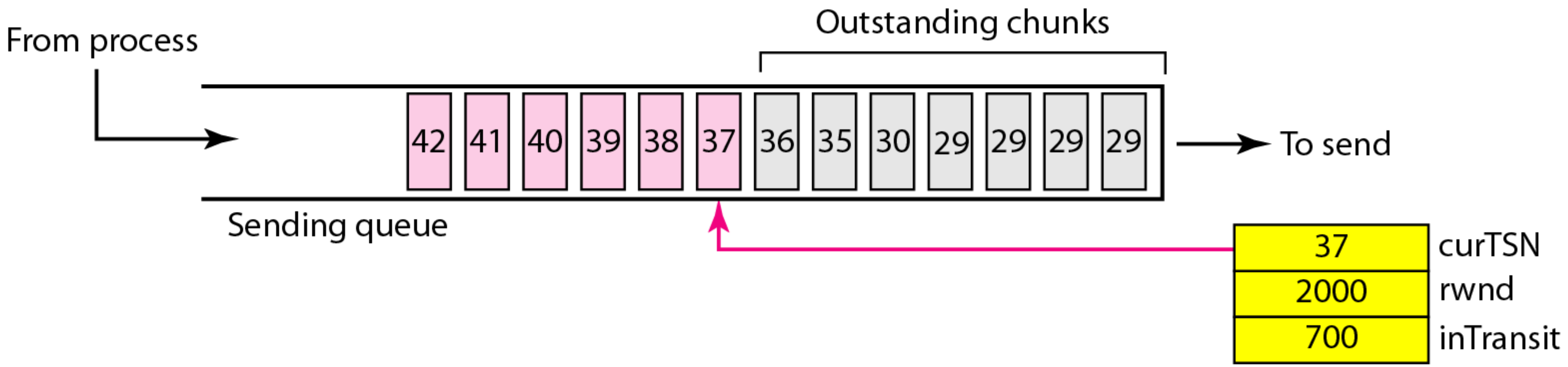


Figure 23.38 *Flow control scenario*

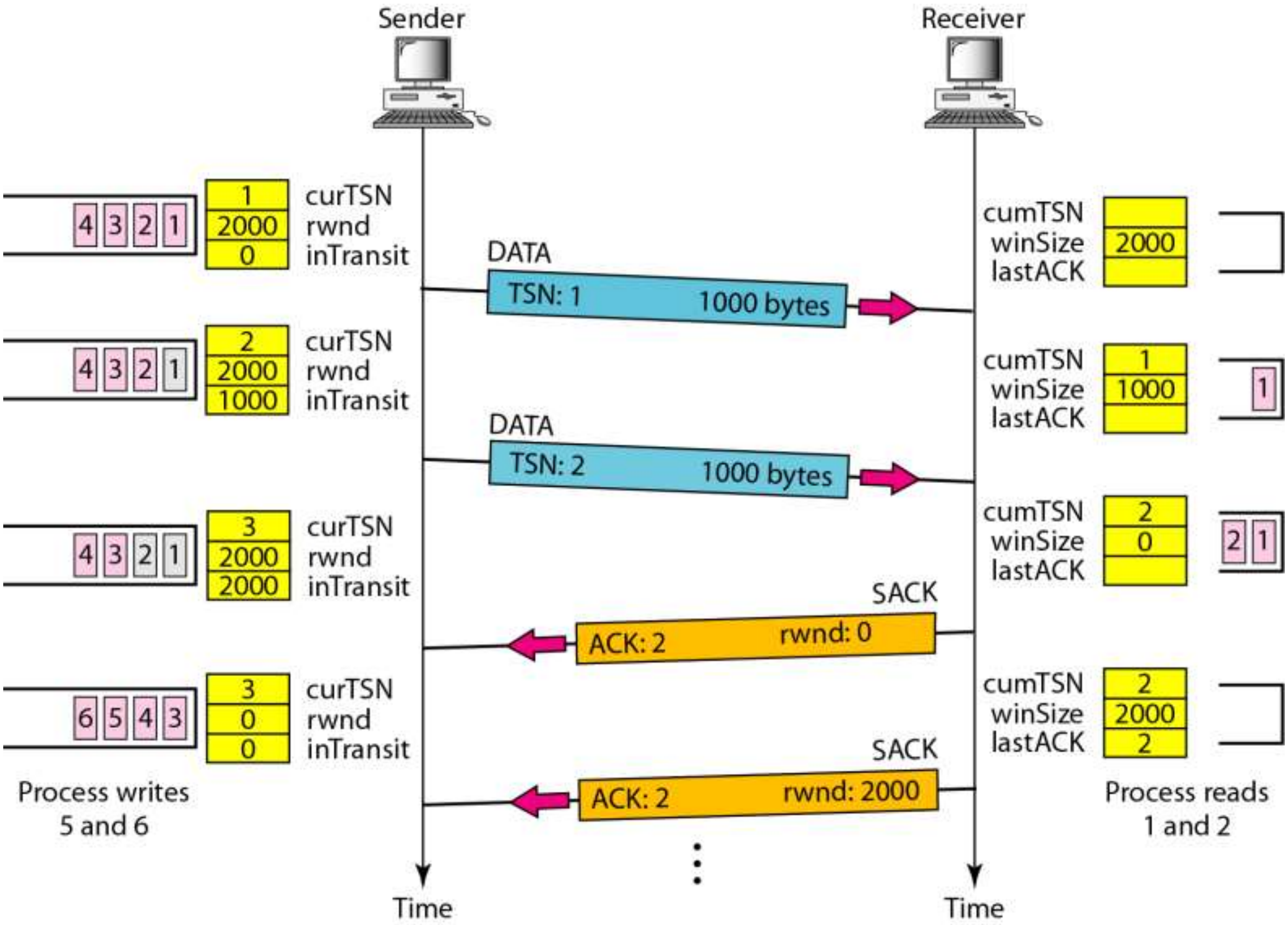


Figure 23.39 *Error control, receiver site*

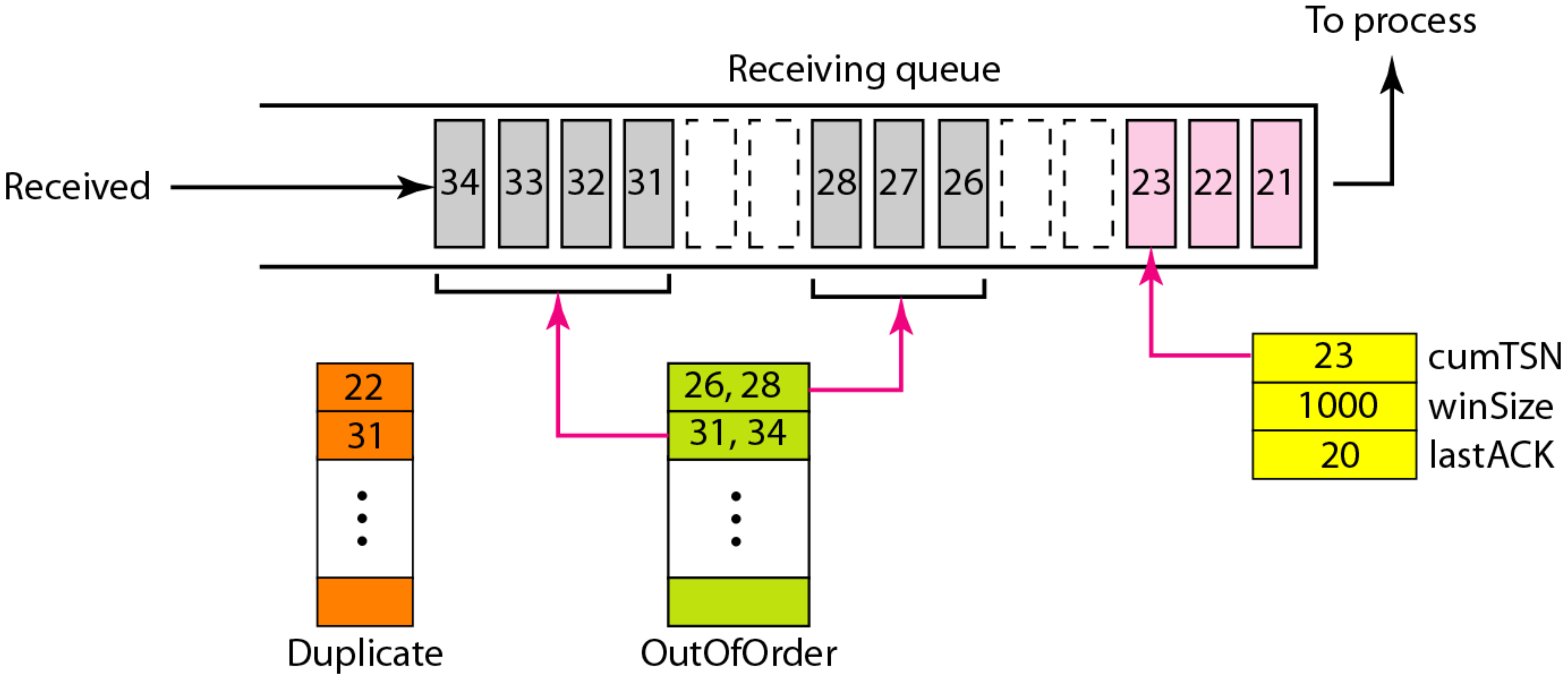
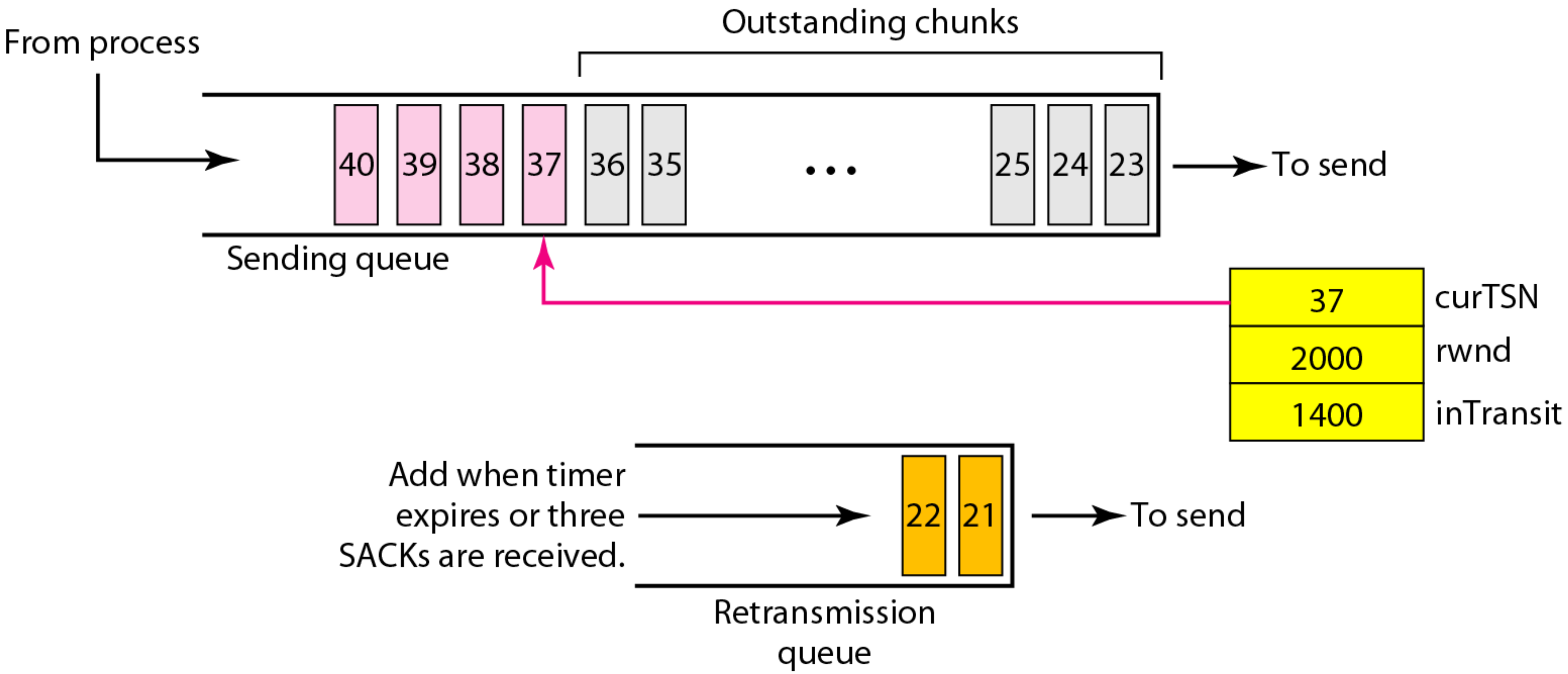


Figure 23.40 *Error control, sender site*


Outstanding chunks
From process
40
39
38
37
36
35
• • •
25
24
23
To send
Sending queue
37
curTSN
2000
rwnd
1400
inTransit
Add when timer expires or three SACKs are received.
22
21
To send
Retransmission queue