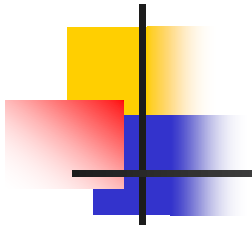
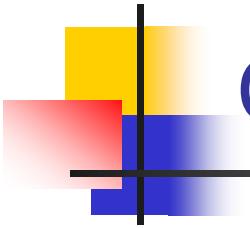


INTERNET AND TCP/IP

INTERNET

- The Internet is a network of networks. Millions of computers all over the world are connected through the Internet. Computer users on the Internet can contact one another anywhere in the world. If your computer is connected to the Internet, you can connect to millions of computers. You can gather information and distribute your data. It is very much similar to the telephone connection where you can talk with any person anywhere in the world.
- In Internet a huge resource of information is accessible to people across the world. Information in every field starting from education, science, health, medicine, history, and geography to business, news, etc. can be retrieved through Internet. You can also download programs and software packages from anywhere in the world. Due to the tremendous information resources the Internet can provide, it is now indispensable to every organisation

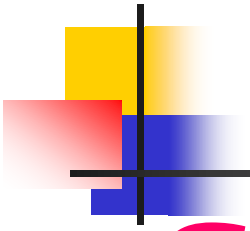


Origin of Internet

In 1969 Department of Defense (DOD) of USA started a network called ARPANET (Advanced Research Projects Administration Network) with one computer at California and three at Utah. Later on other universities and R & D institutions were allowed to connect to the Network. APARNET quickly grew to encompass the entire American continent and became a huge success. Every university in the country wanted to become a part of ARPANET. So the network was broken into two smaller parts MILNET for managing military sites and ARPANET (smaller) for managing non-military sites. Around 1980, NSFNET (National Science Foundation Network) was created. With the advancement of modern communication facilities, other computers were also allowed to be linked up with any computer of NSFNET. By 1990 many computers were looking up to NSFNET giving birth to Internet.

How Internet functions

Internet is not a governmental organisation. The ultimate authority of the Internet is the Internet Society. This is a voluntary membership organisation whose purpose is to promote global information exchange. Internet has more than one million computers attached to it.



Security Protocols in the Internet

31.1 IP Level Security

- *Security Association*
  - *Two Modes*
  - *Two Security Protocols*
    - *Authentication Header (AH)*
    - *Encapsulating Security Payload (ESP)*

Figure 31.1 Transport mode

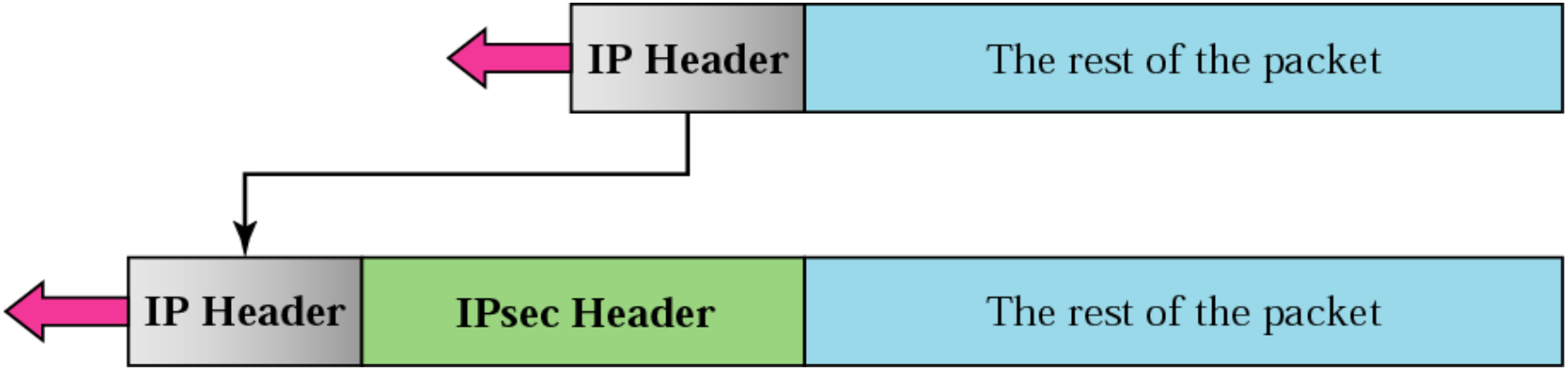


Figure 31.2 Tunnel mode

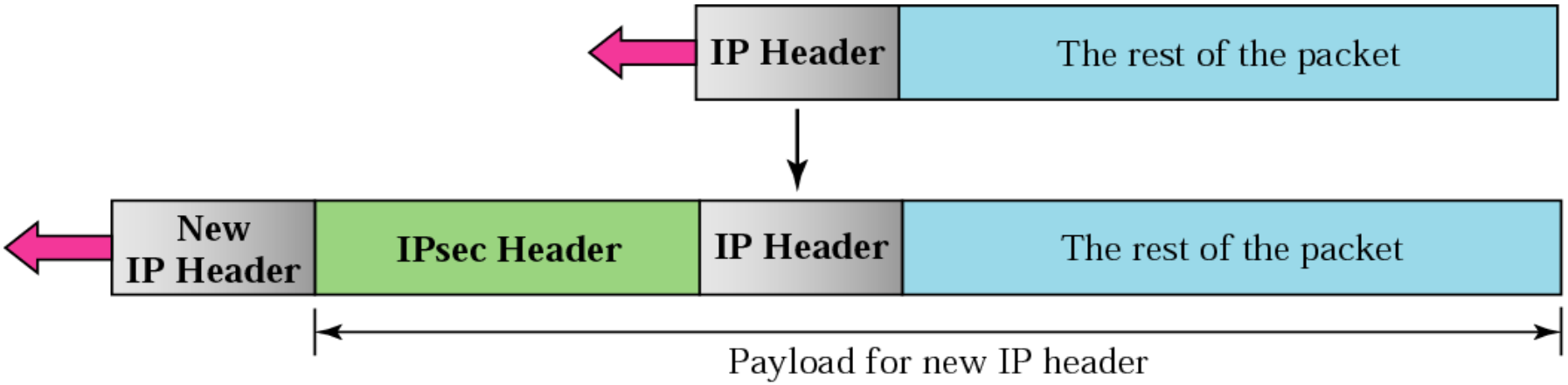
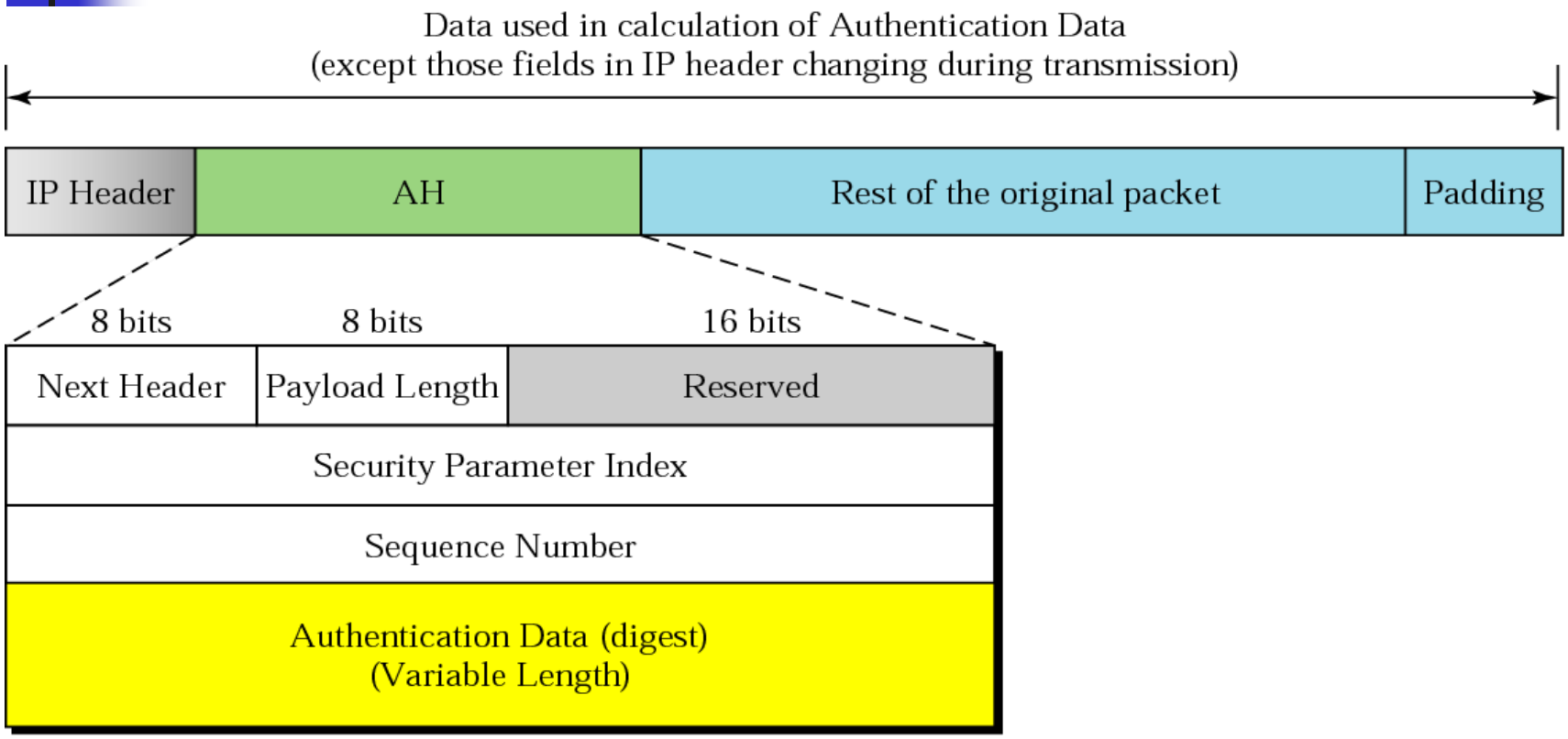


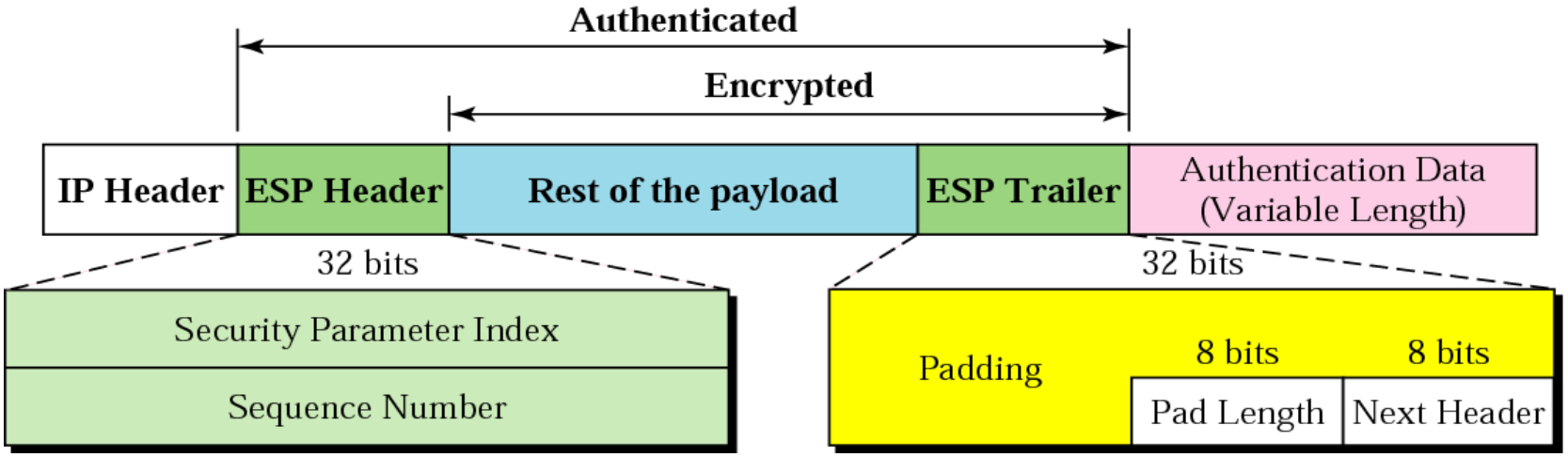
Figure 31.3 AH



Note:

The AH protocol provides source authentication and data integrity, but not privacy.

Figure 31.4 ESP



Note:

ESP provides source authentication, data integrity, and privacy.

31.2 Transport Layer Security

Position of TLS

Two Protocols

Figure 31.5 Position of TLS

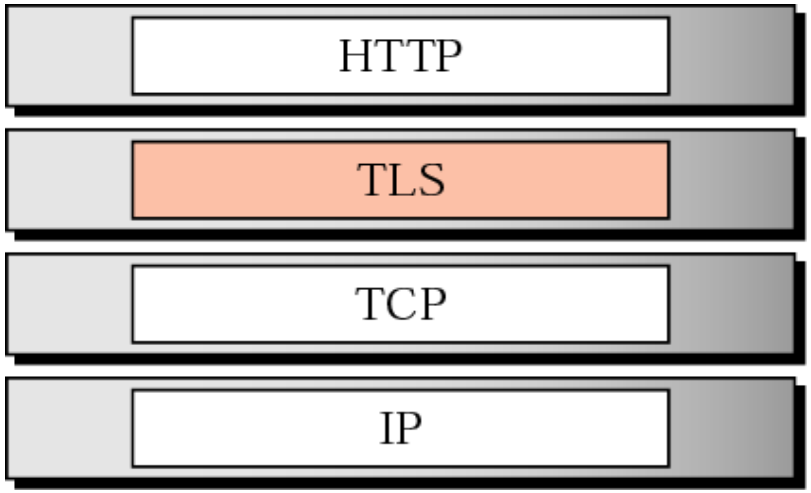
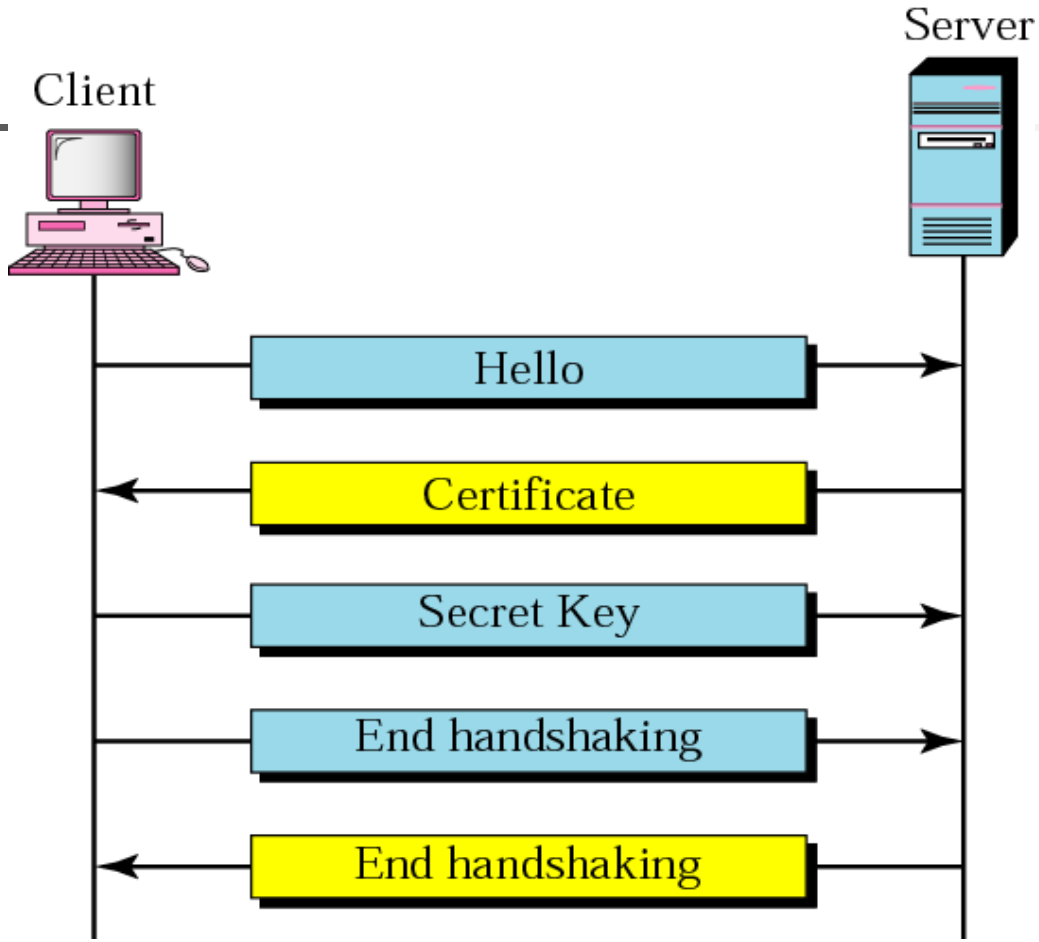


Figure 31.6 Handshake protocol



31.3 Application Layer Security

Pretty Good Privacy

Figure 31.7 PGP at the sender site

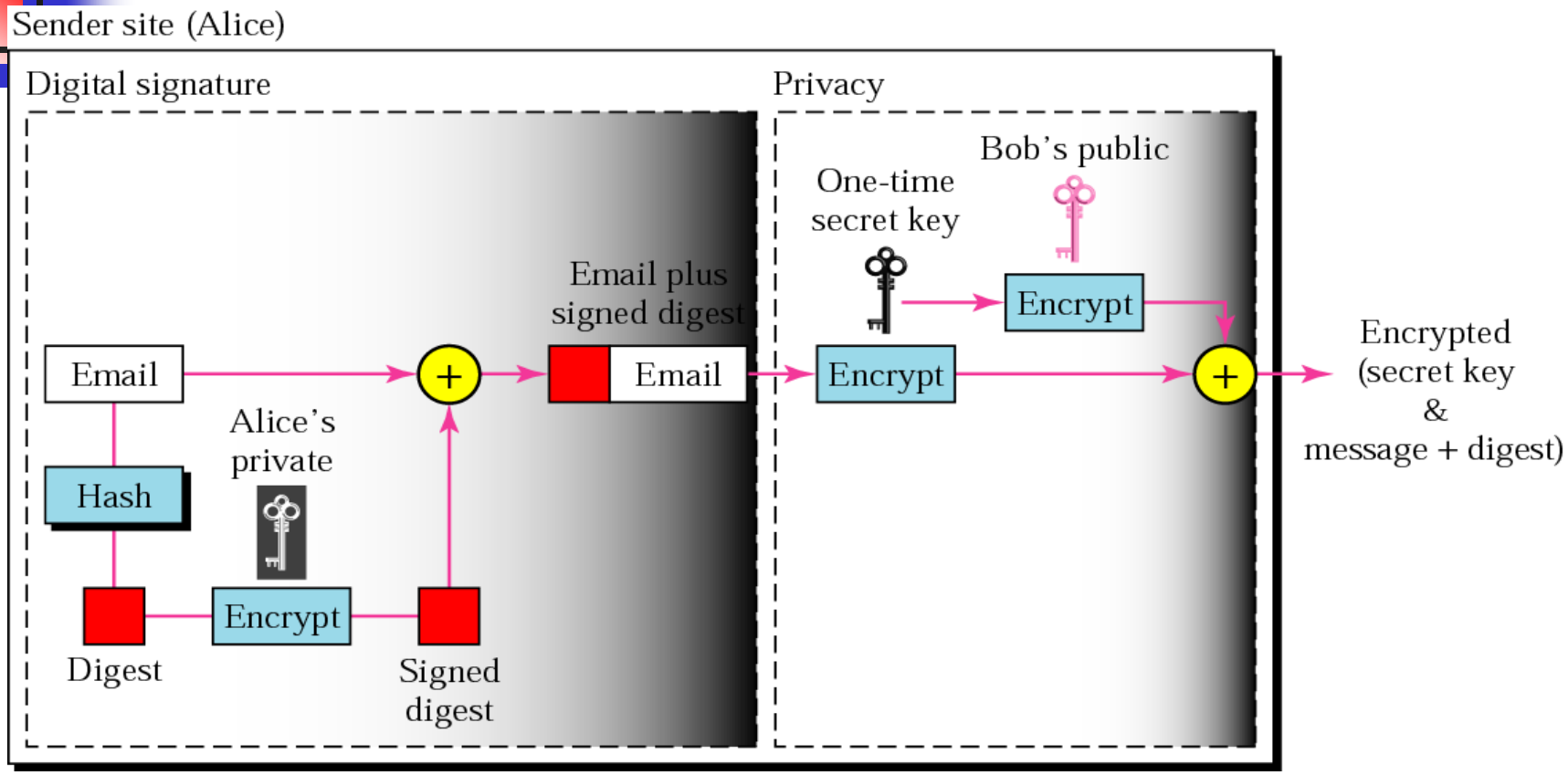
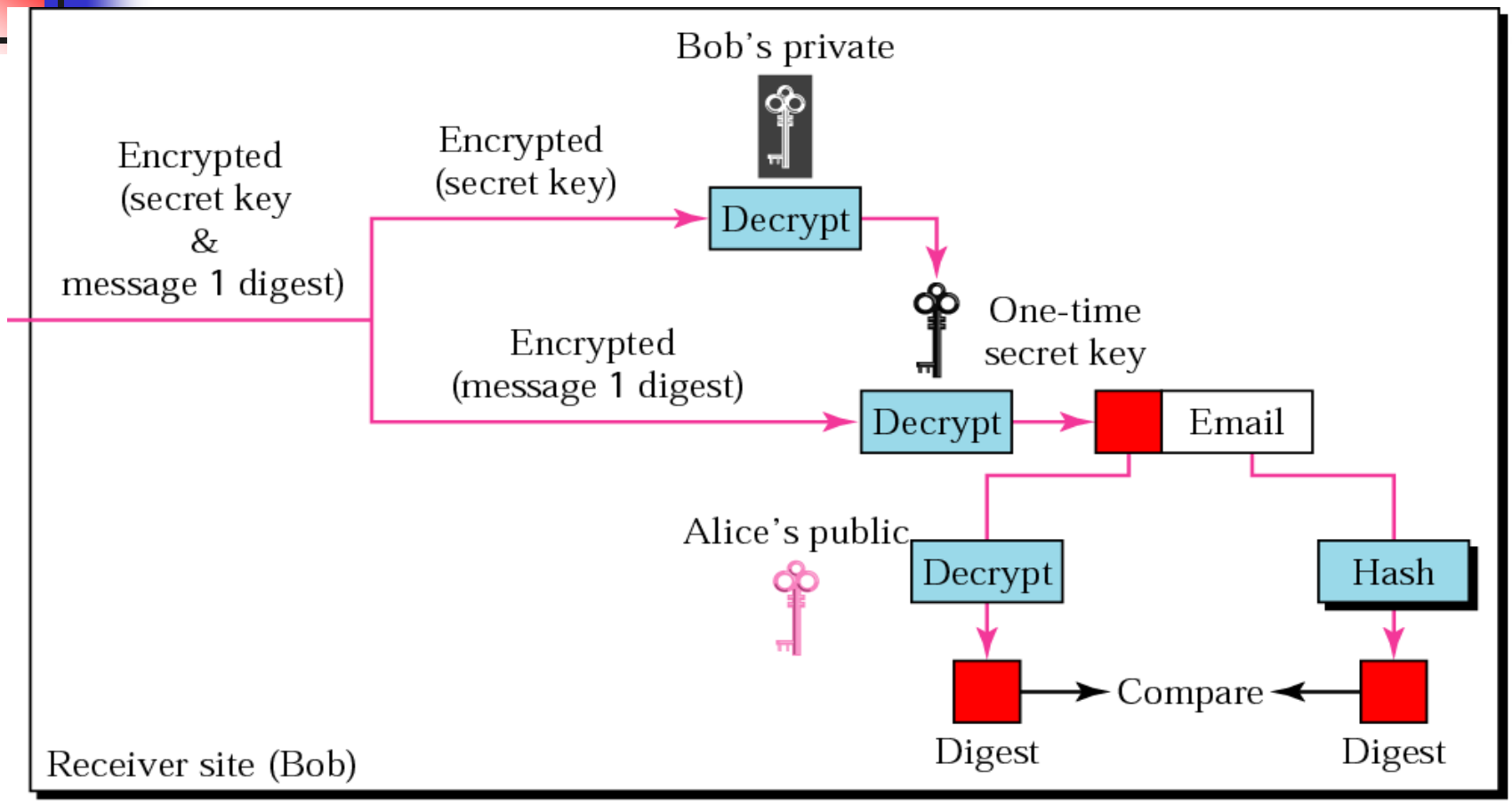


Figure 31.8 PGP at the receiver site



31.4 Firewalls

- *Packet-Filter Firewalls*
- *Proxy Firewalls*

Figure 31.9 Firewall

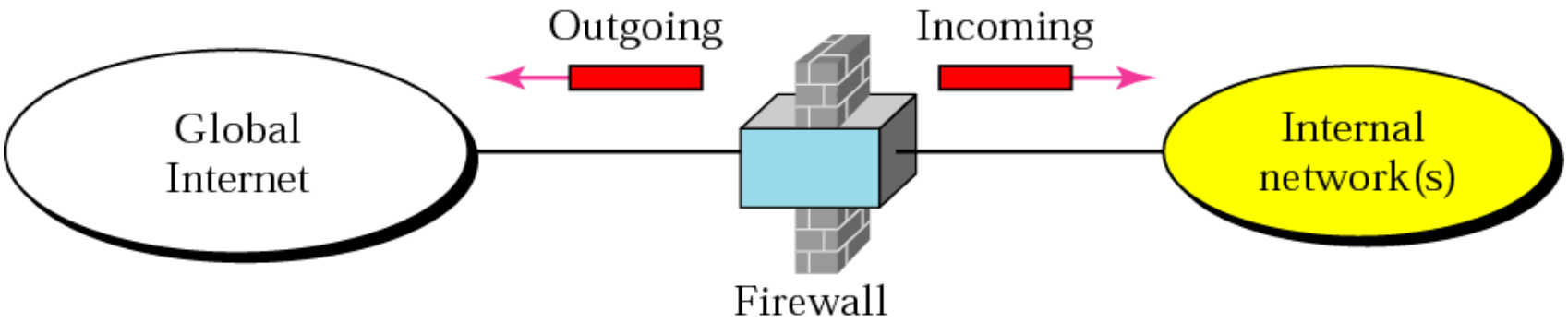
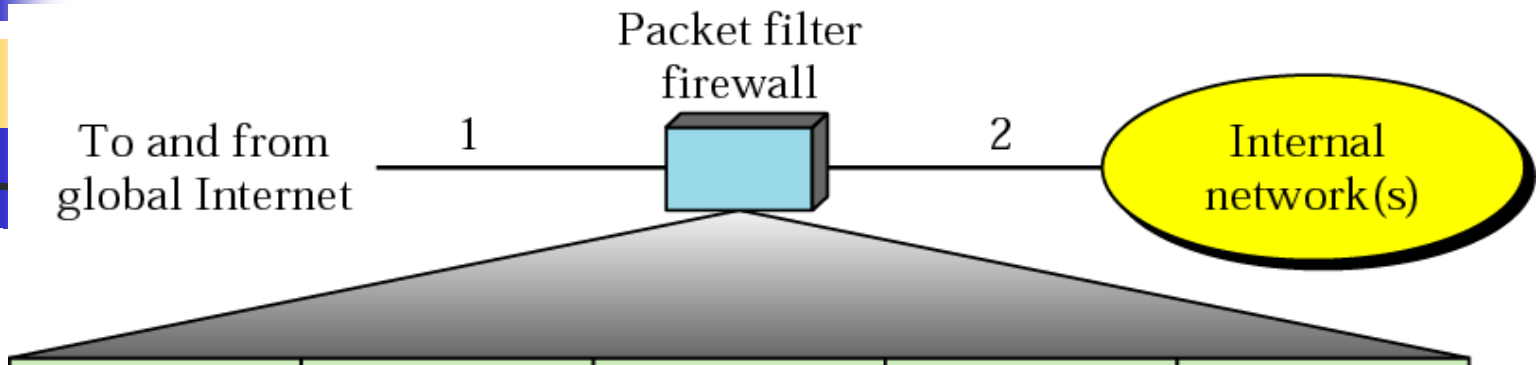


Figure 31.10 Packet-filter firewall

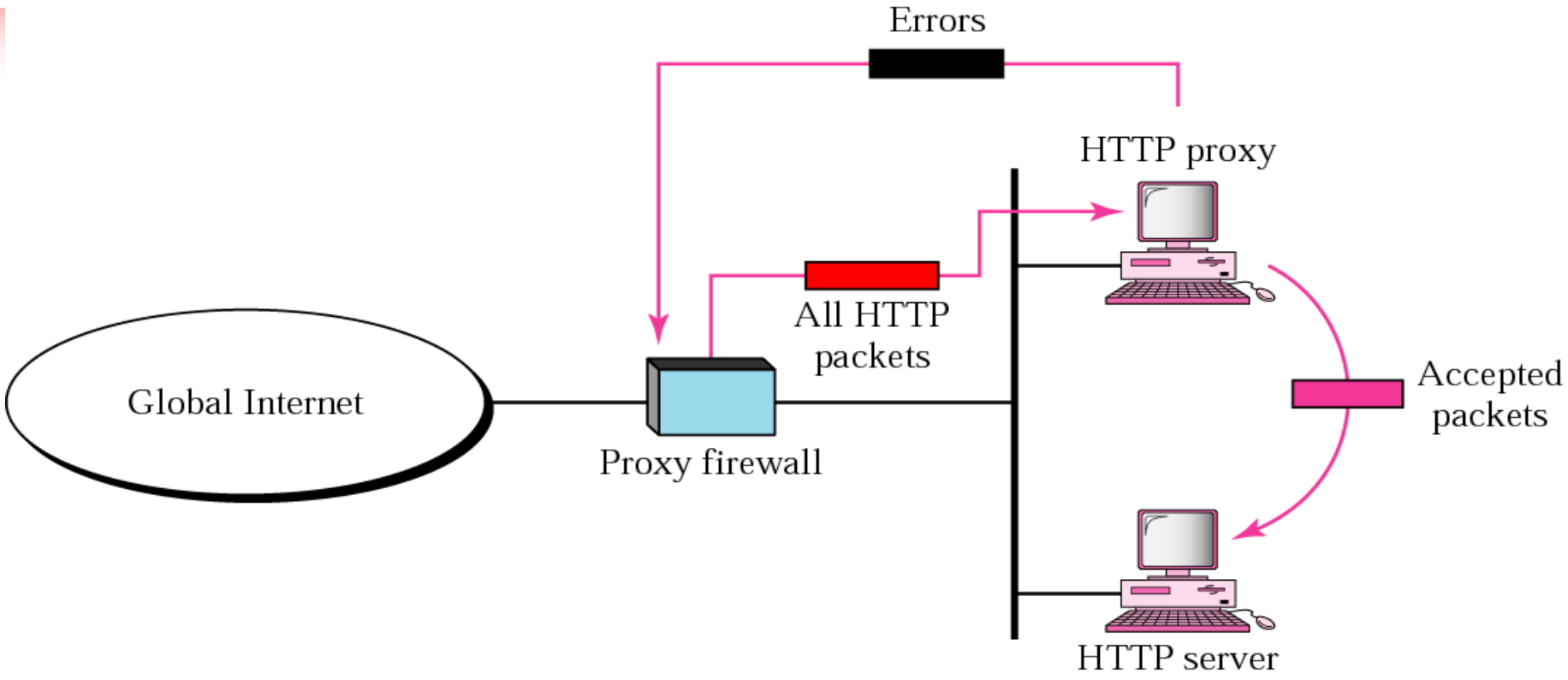


Interface	Source IP	Source Port	Destination IP	Destination Port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	80	*	*

Note:

A packet-filter firewall filters at the network or transport layer.

Figure 31.11 Proxy firewall



Note:

A proxy firewall filters at the application layer.

31. 5 Virtual Private Networks

Private Networks

Achieving Privacy

VPN Technology

Table 31.1 Addresses for private networks

Prefix	Range			Total
10/8	10.0.0.0	to	10.255.255.255	2^{24}
172.16/12	172.16.0.0	to	172.31.255.255	2^{20}
192.168/16	192.168.0.0	to	192.168.255.255	2^{16}

Figure 31.12 Private network

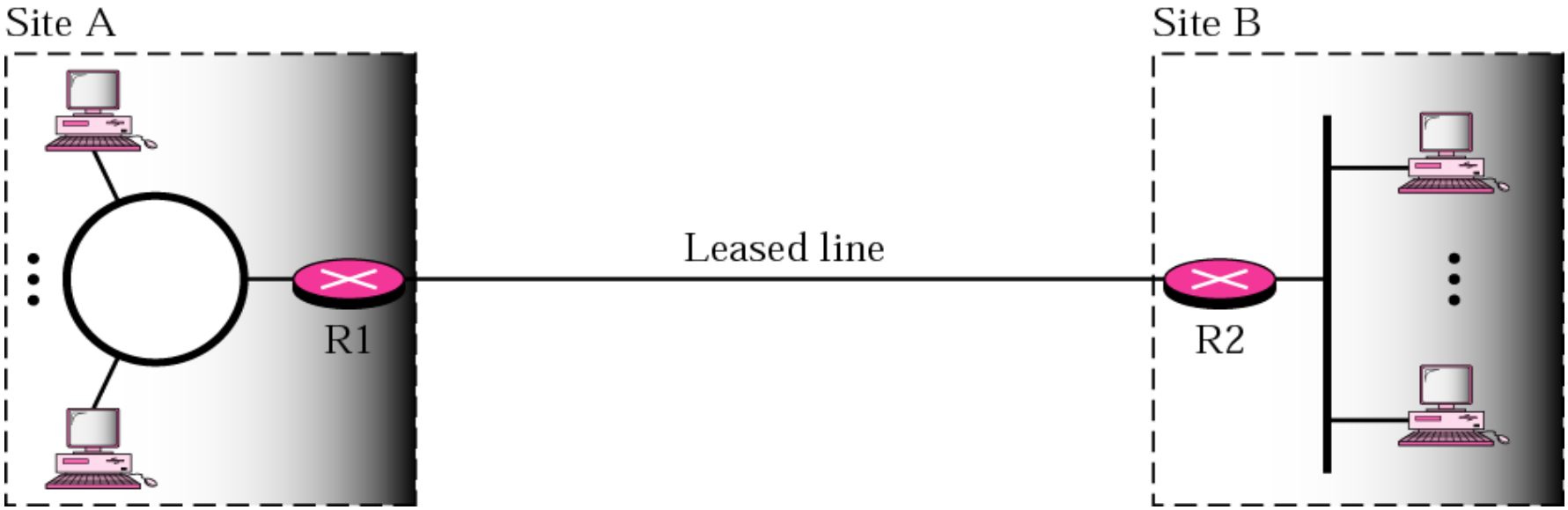


Figure 31.13 Hybrid network

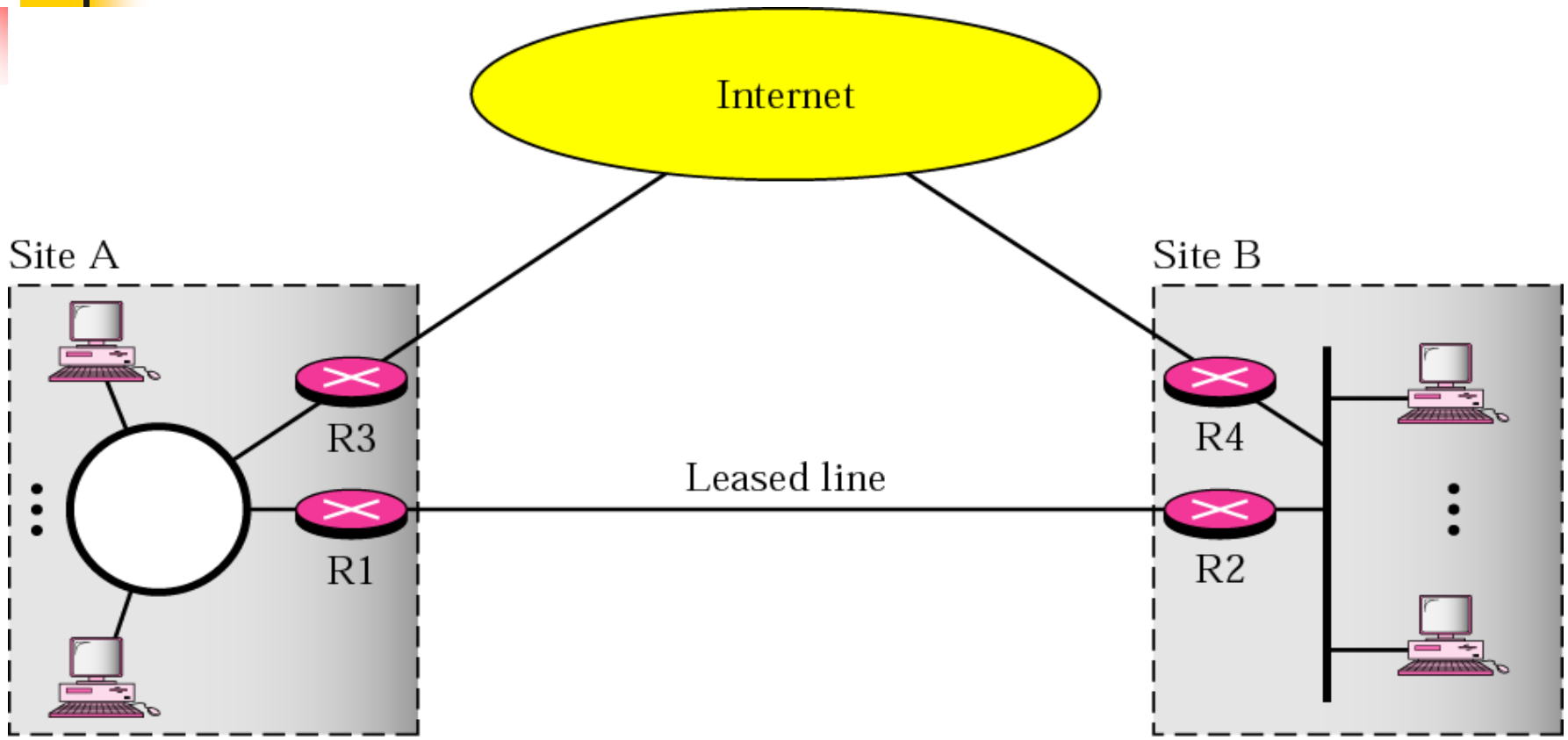


Figure 31.14 Virtual private network

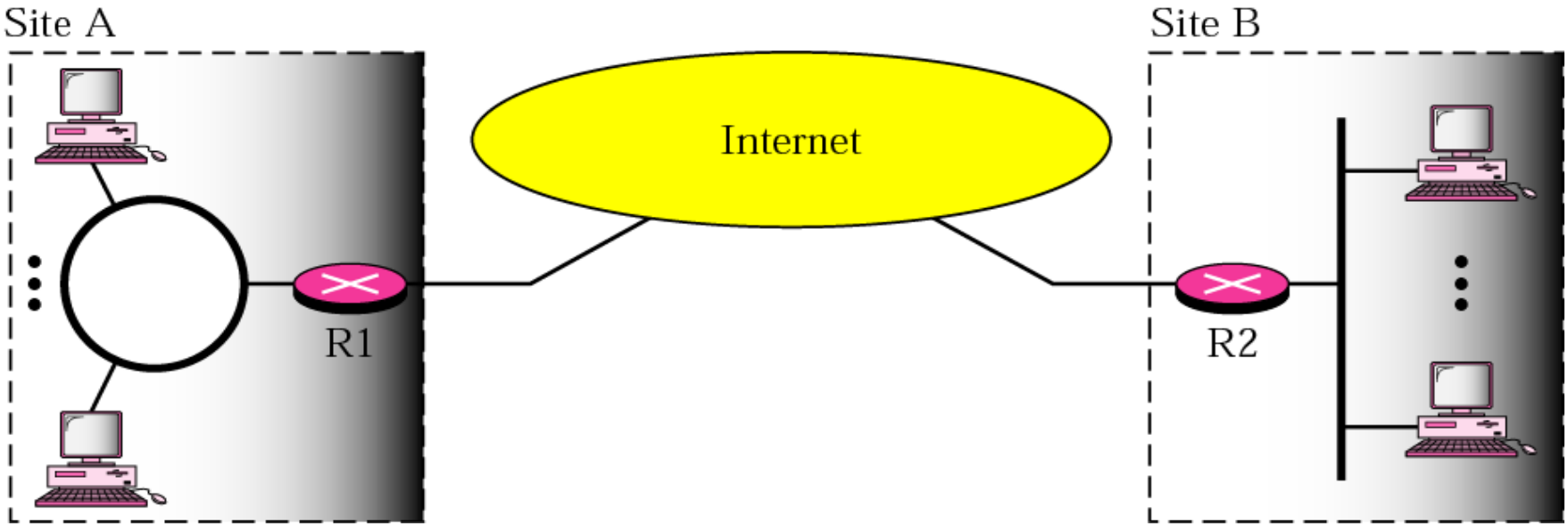
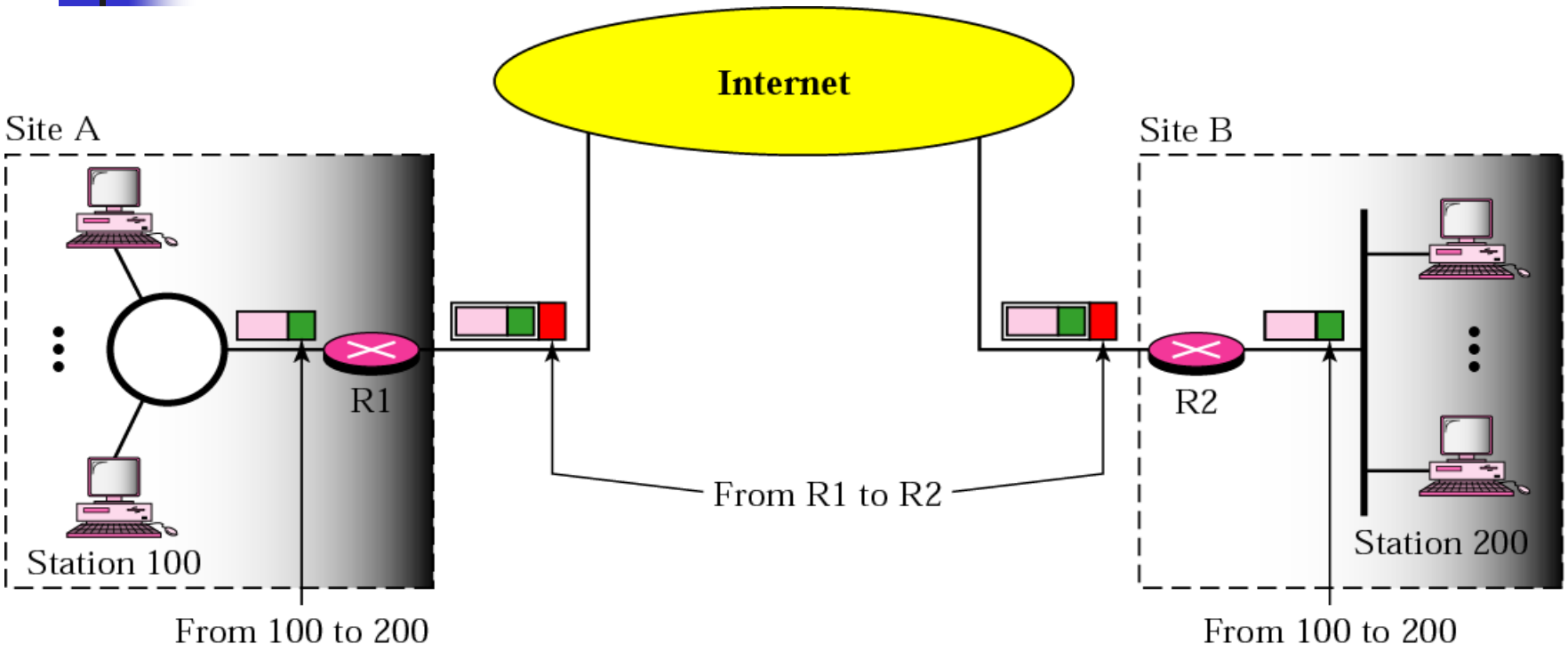
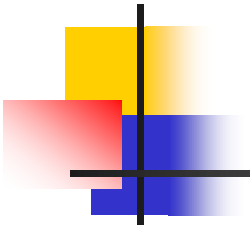


Figure 31.15 Addressing in a VPN





E-mail

E-mail stands for *electronic mail.* This is one of the most widely used features of Internet. Mails are regularly used today where with the help of postage stamp we can transfer mails anywhere in the world. With electronic mail the service is similar. But here data are transmitted through Internet and therefore within minutes the message reaches the destination may it be anywhere in the world. Therefore the mailing system is excessively fast and is being used widely for mail transfer.

Why Standards

- Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunication technology and processes.
- Standards provide guidelines to manufacturers, vendors government agencies and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications

Types

- De facto (by fact)- Standards that have not been approved by an organized body but have been adopted as standards through widespread use
- De jure(by law)-That have been legislated by an officially recognized body

Standards Organizations

- ISO-(International organization for Standardization)
- ITU-T (International Telecommunication Union-Telecommunication)
- ANSI(American National Standards Institute
- IEEE(Institute of Electrical and Electronics Engineers)
- EIA(Electronic Industries Association)

Protocols

•Protocol are used for communication between computers in different computer networks.

- Protocol achieves:
  - -What is communicated between computers?
  - -How it is communicated?
  - -When it is communicated?
  - -What conformance (bit sequence) between computers?

Key elements of a protocol are

- SYNTAx: Data format and signal levels
- SEMANTICS: Control information for coordination and error handling
- TIMING: Synchronization, speed matching, and sequencing

Examples of protocols:

- WAN Protocol: TCP/IP
- LAN Protocol: Media Access Control; Contention; Token Passing

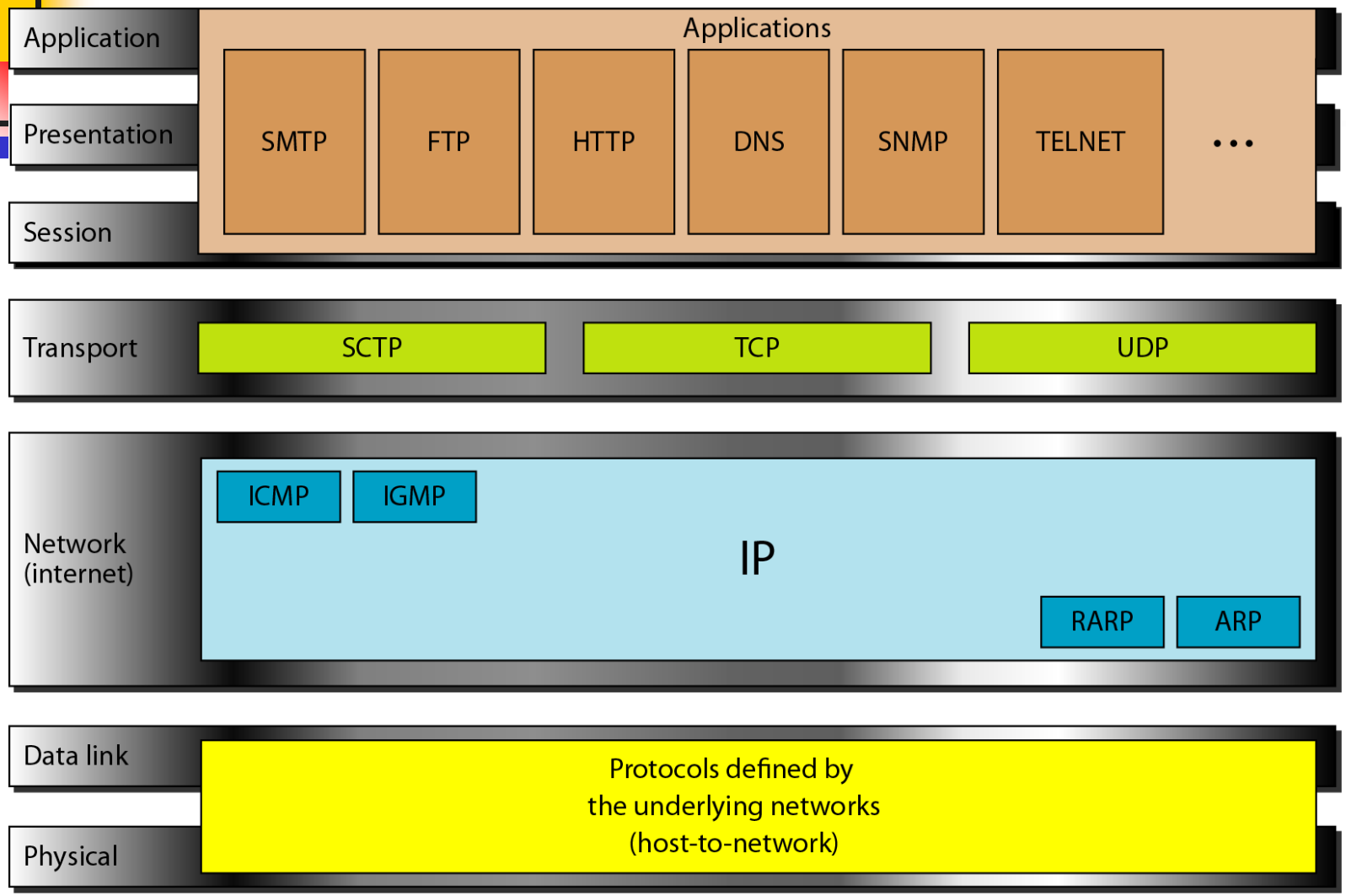
protocols perform the following functions

- Data sequencing: A long message to be transmitted is broken into smaller packets of fixed size for error free data transmission.
- Data Routing: It is the process of finding the most efficient route between source and destination before sending the data.
- Flow control: All machines are not equally efficient in terms of speed. Hence the flow control regulates the process of sending data between fast sender and slow receiver.
- Error Control: Error detecting and recovering is the one of the main function of communication software. It ensures that data are transmitted without any error.

2.4 TCP/IP Protocol Suites

- 5 Layer Model
  - Layer 5 Application layer
  - Layer 4 Transport layer
  - Layer 3 Network layer
  - Layer 2 Data Link layer
  - Layer 1 Physical layer

TCP/IP and OSI model



TCP/IP Protocol Suites (cont.)

- Physical and Data Link Layers
  - Does not define any specific protocol.
  - Support all the standard and proprietary protocols.
- Network Layer
  - IP (Internetworking Protocol)
  - ARP (Address Resolution Protocol)
  - RARP (Reverse Address Resolution Protocol)
  - ICMP (Internet Control Message Protocol)
  - IGMP (Internet Group Message Protocol)

IP (Internetworking Protocol)

- It is the transmission mechanism used by the TCP/IP protocol
- It is an unreliable connectionless protocol (best effort delivery)

  best effort means no error checking or tracking
- It supports datagram
- No facility for reordering datagram at destination

ARP (Address Resolution Protocol)

- It is used to associate a logical address with physical address
- On a typical N/W such as LAN each device on a link is identified by physical address or station address imprinted on NIC
- It is used to find the physical address of the node when its Internet address is known

RARP (Reverse Address Resolution Protocol)

- It is used to discover Internet address when it knows physical address
- It is used when a computer is connected to a network for the first time

(ICMP) Internet Control Message Protocol

- It is a mechanism used by hosts & gateways to send notiofication of datagram problems back to the sender
- It sends query & error reporting message

(IGMP) Internet Group Message Protocol

- It is used to facilitate the simultaneous transmission of message to a group of reception

TCP/IP Protocol Suites (cont.)

- Transport Layer
  - UDP (User Datagram Protocol)
  - TCP (Transmission Control Protocol)
  - SCTP (Stream Control Transmission Protocol)

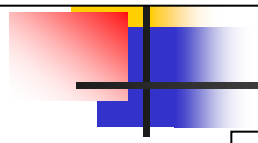
UDP (User Datagram Protocol)

- It is a process to process protocol that adds only port addresses, checksum error control and information to the data from the upper layer.

TCP (Transmission Control Protocol)

- It provides full transport layer services to the applications
- It is a reliable stream (connection oriented) transport protocol
- At Transmitter end TCP divides a stream of data into smaller units called segment.
- Add sequence number
- At the receiving end collects each datagram
- Reordering the datagram

SCTP (Stream Control Transmission Protocol)

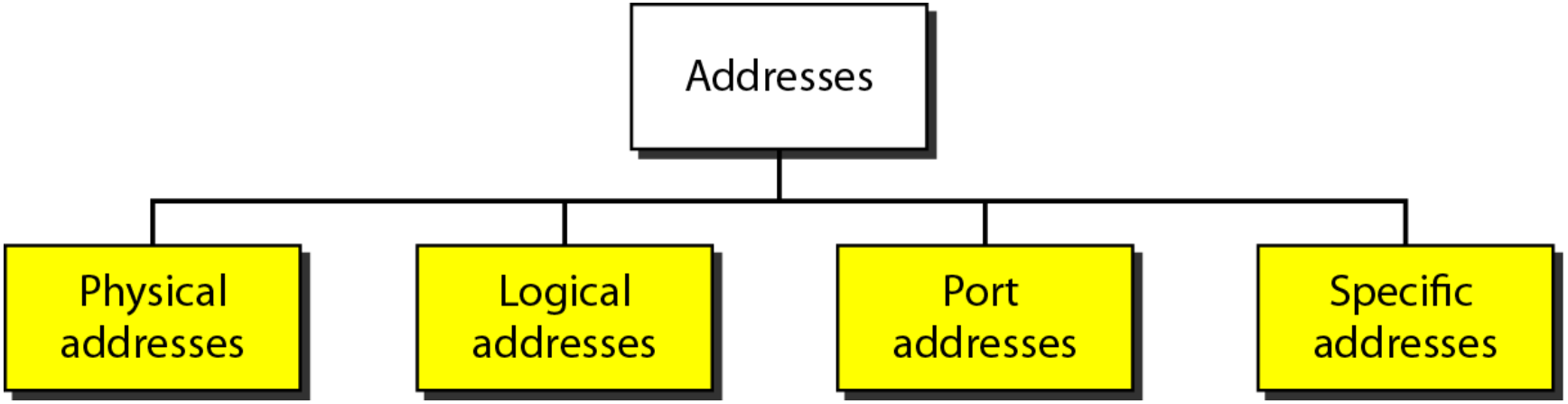


- It support for newer applications such as voice over the Internet
- It combines the best features of UDP and TCP

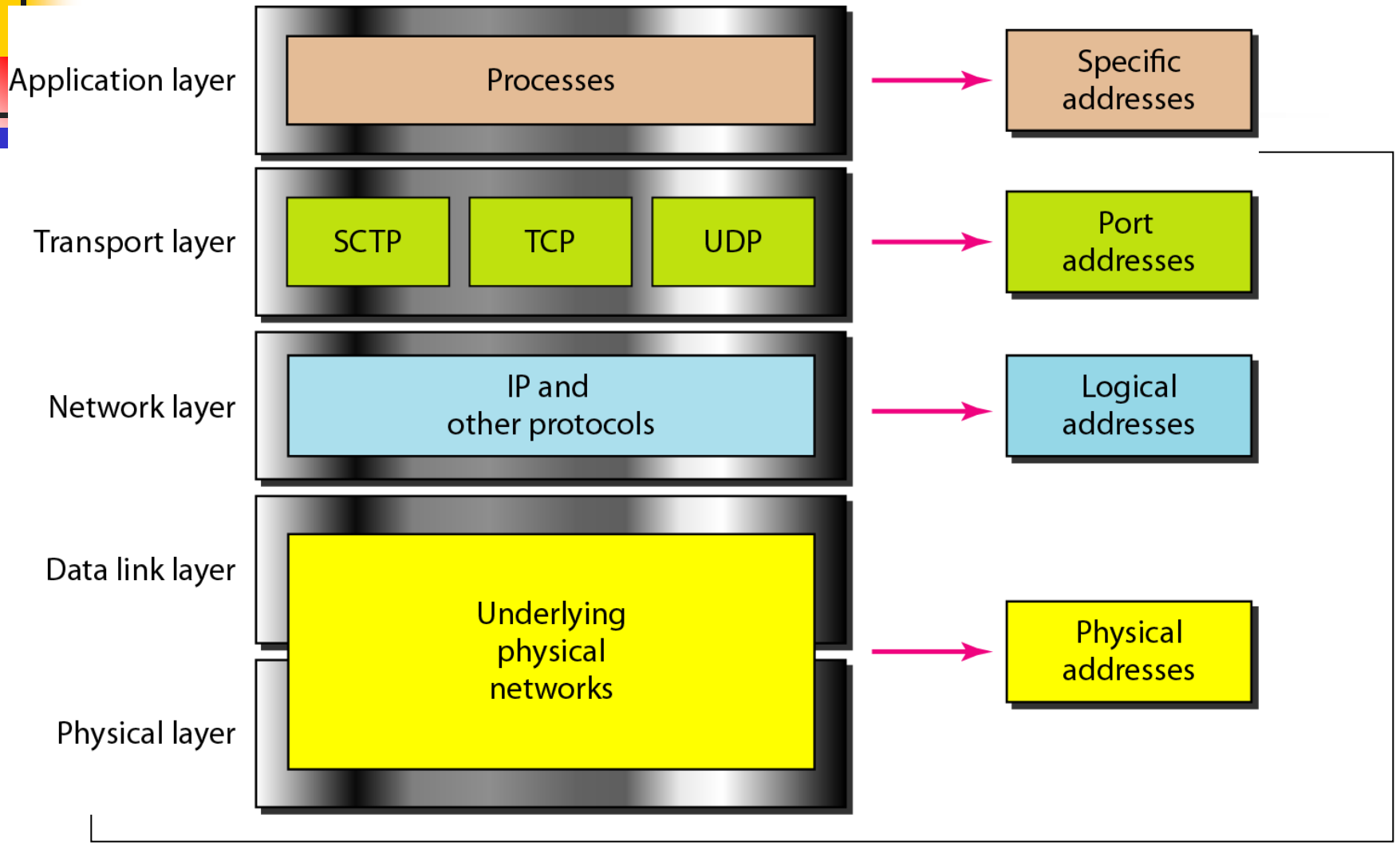
Application Layer

- Equivalent to the combined session, presentation, application layers in OSI

2.5 Addressing



Relations of layers and addresses in TCP/IP



Addressing

- Physical Addresses
  - Link address
  - Defined by its LAN or WAN
  - Included in the frame used by data link layer
  - The lowest level addresses
  - Size and format of the address depend on the network
    - Ethernet uses a 6-byte address

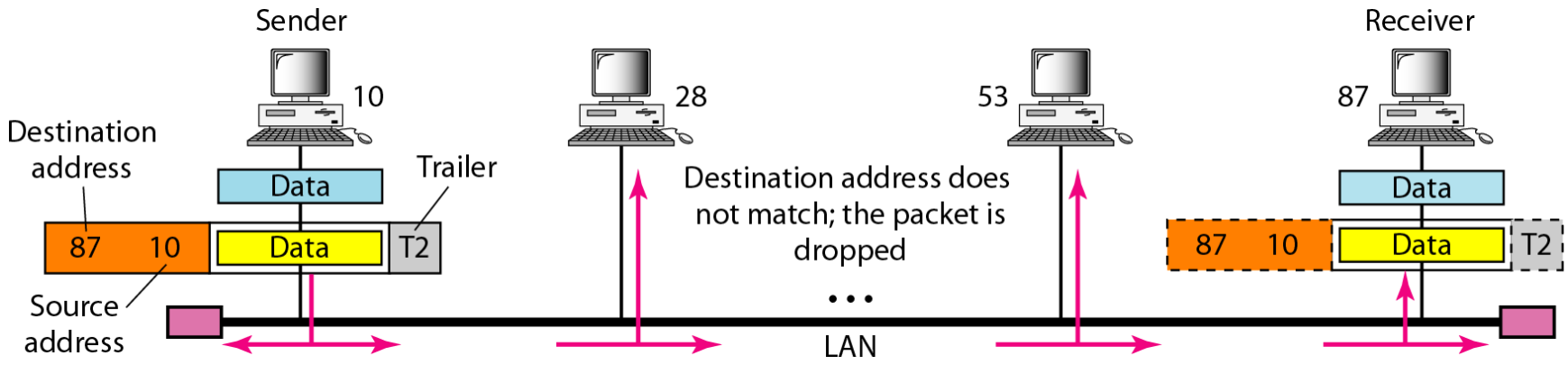
Example 2.2

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.

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

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

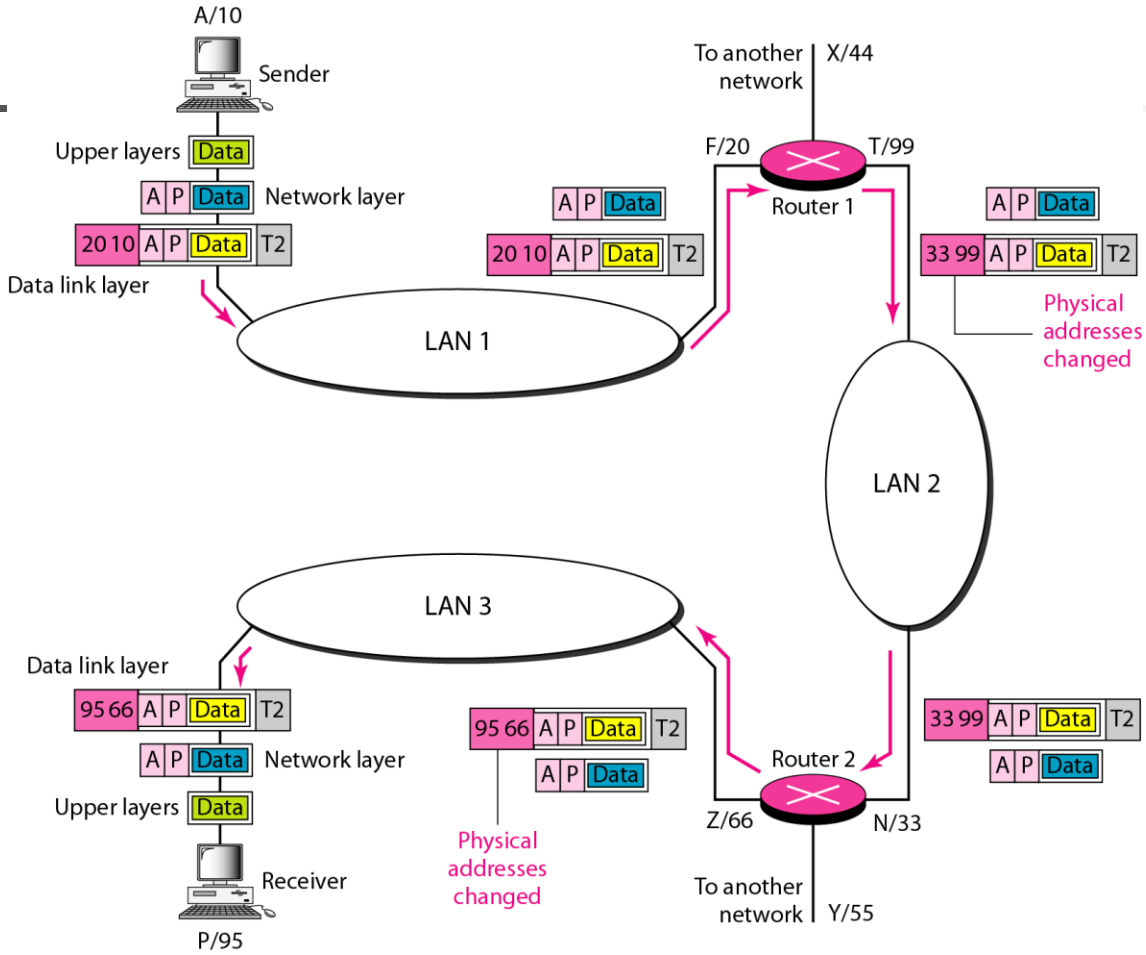
Physical Address



Addressing (cont.)

- Logical Addresses
  - Necessary for communications that are independent of underlying physical networks.
  - Each host can be identified uniquely
  - Currently a 32-bit address in the Internet
  - The physical addresses will change from hop to hop, but the logical addresses usually remain the same

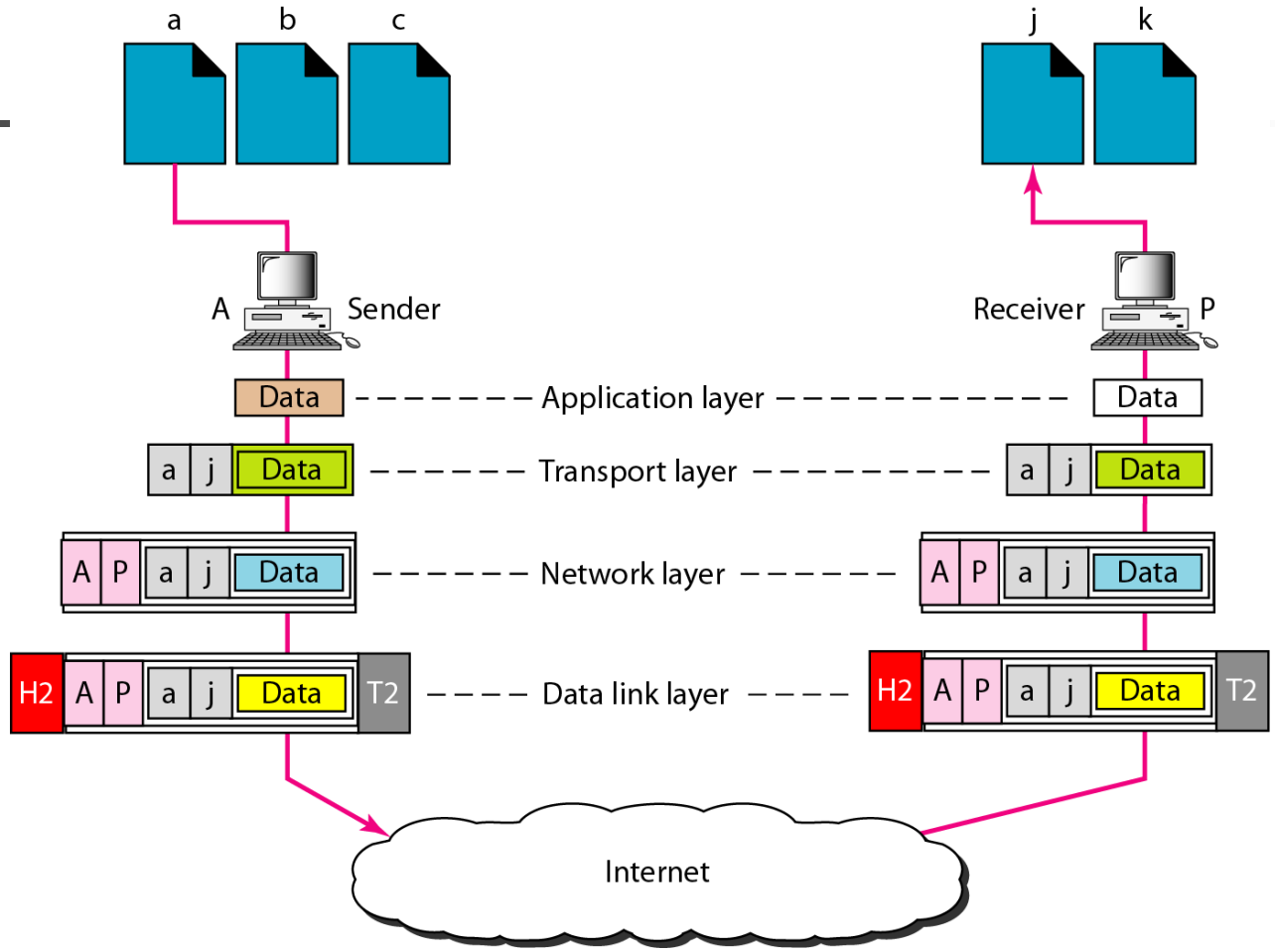
IP Addresses



Addressing

- Port Addresses
  - Internet communication
    - Process communicates with another process
    - Processes – TELNET, FTP, HTTP etc.
  - A method to label different processes.
  - 16 bits in TCP/IP
  - Represented by one decimal number, e.g. 23, 80, 753

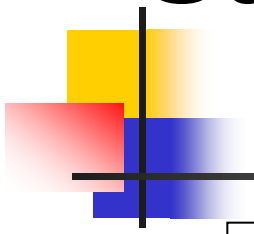
Port Addresses



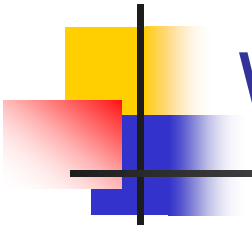
Addressing

- Specific Addresses
  - Email address – luoh@ipfw.edu
  - Web url – http://www.ects.ipfw.edu/~luoh

Summary



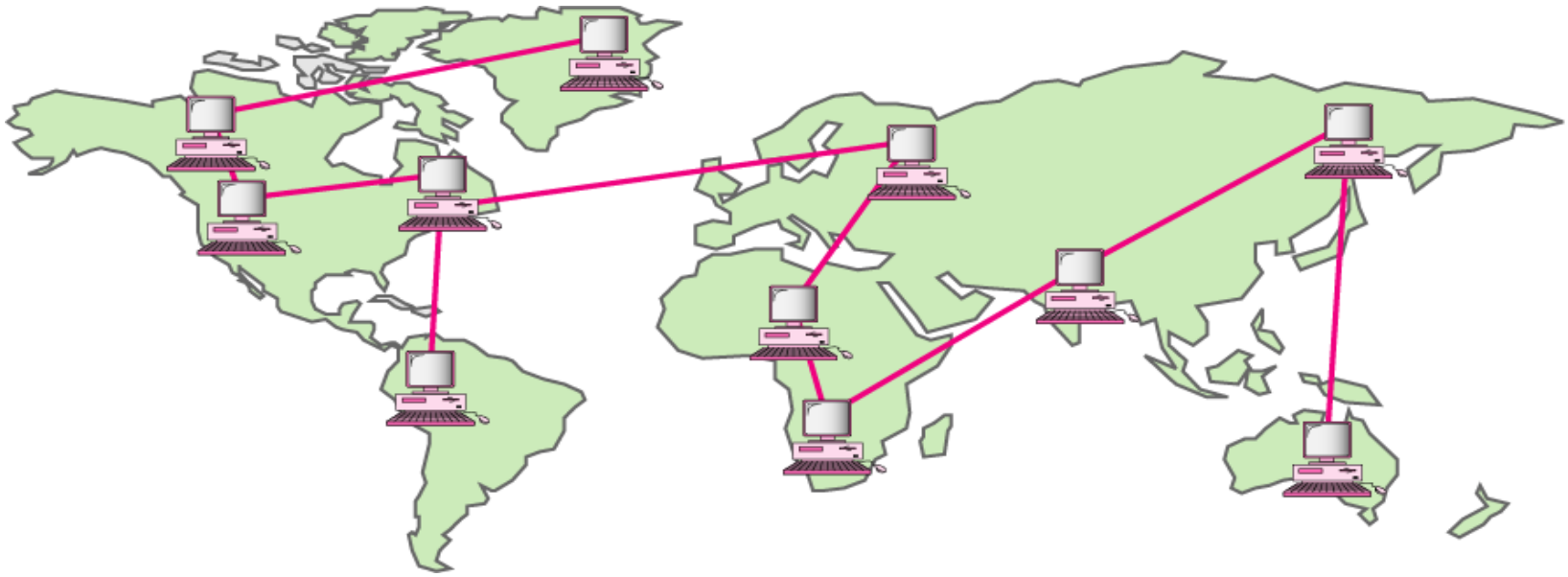
- Layered tasks
- The OSI model
- TCP/IP protocol suites
- Addressing



Wide Area Network

The term Wide Area Network (WAN) is used to describe a computer network spanning a regional, national or global area. For example, for a large company the head quarters might be at Delhi and regional branches at Bombay, Madras, Bangalore and Calcutta. Here regional centers are connected to head quarters through WAN. The distance between computers connected to WAN is larger. Therefore the transmission medium used are normally telephone lines, microwaves and satellite links.

WAN Cont...

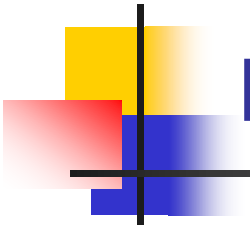


Characteristics of WAN

- Communication Facility: For a big company spanning over different parts of the country the employees can save long distance phone calls and it overcomes the time lag in overseas communications. Computer conferencing is another use of WAN where users communicate with each other through their computer system.

- Remote Data Entry: Remote data entry is possible in WAN. It means sitting at any location you can enter data, update data and query other information of any computer attached to the WAN but located in other cities. For example, suppose you are sitting at Madras and want to see some data of a computer located at Delhi, you can do it through WAN.

- Centralized Information: In modern computerized environment you will find that big organisations go for centralized data storage. This means if the organisation is spread over many cities, they keep their important business data in a single place. As the data are generated at different sites, WAN permits collection of this data from different sites and save at a single site



Examples of WAN

- Ethernet: Ethernet developed by Xerox Corporation is a famous example of WAN. This network uses coaxial cables for data transmission. Special integrated circuit chips called *controllers* are used to connect equipment to the cable.

- Arpanet: The Arpanet is another example of WAN. It was developed at Advanced Research Projects Agency of U. S. Department. This Network connects more than 40 universities and institutions throughout USA and Europe.

Difference between LAN and WAN

- LAN is restricted to limited geographical area of few kilometers. But WAN covers great distance and operate nationwide or even worldwide.
- In LAN, the computer terminals and peripheral devices are connected with wires and coaxial cables. In WAN there is no physical connection. Communication is done through telephone lines and satellite links.
- Cost of data transmission in LAN is less because the transmission medium is owned by a single organisation. In case of WAN the cost of data transmission is very high because the transmission medium used are hired, either telephone lines or satellite links.
- The speed of data transmission is much higher in LAN than in WAN. The transmission speed in LAN varies from 0.1 to 100 megabits per second. In case of WAN the speed ranges from 1800 to 9600 bits per second (bps
- Few data transmission errors occur in LAN compared to WAN. It is because in LAN the distance covered is negligible