

Chapter IV

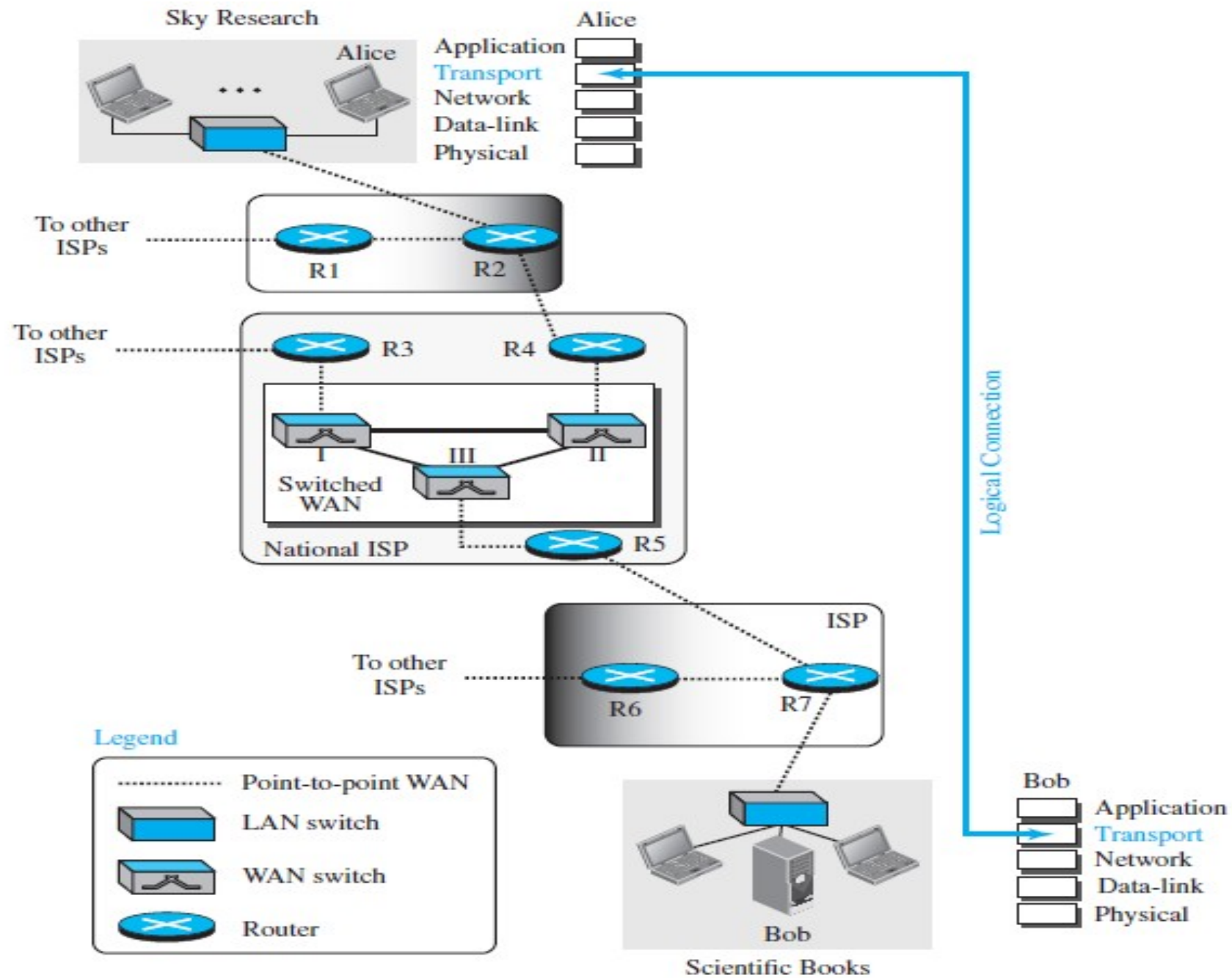
Transport and Application Layer

Data Communication and Computer Networks

(CSE 3205)

Contents

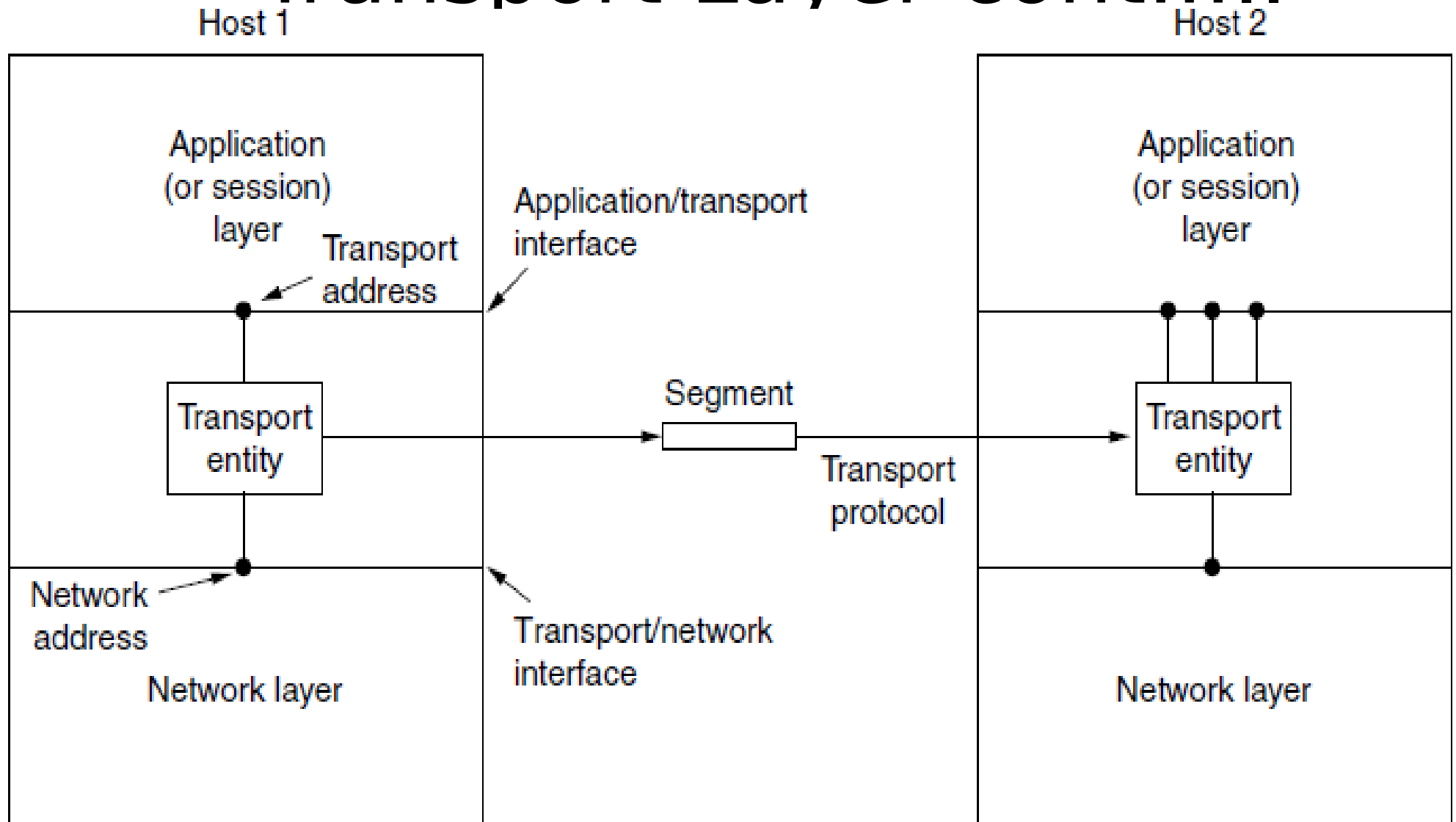
- Transport layer and its service
- Elements of Transport Protocols
- Reliable Data Transfer: TCP
- Connectionless Transport: UDP
- Congestion Control



Transport Layer and its services

- The transport protocol provides an **end-to-end (process-to-process)** data transfer service that shields upper-layer protocols from the details of the intervening network or networks.
- A transport protocol can be either connection oriented or connectionless.
- If the underlying network or internetwork service is unreliable (i.e. IP), then a reliable connection-oriented transport protocol becomes quite complex.
- The basic cause of this complexity is the need to deal with the relatively large and variable **delays experienced** between end systems.
- The transport protocol provides services to transport service (TS) users, such as FTP, SMTP, and TELNET.

Transport Layer cont.....

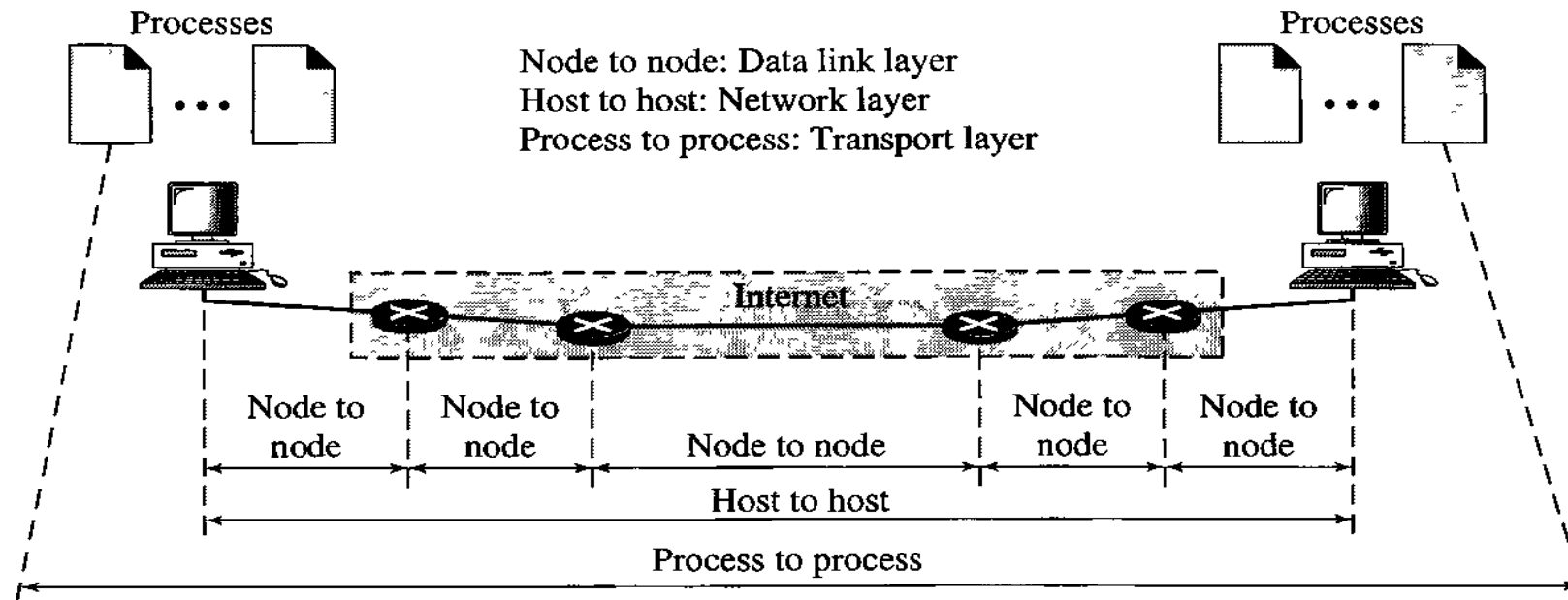


The network, transport, and application layers.

Elements of Transport Protocols

Process to Process communication

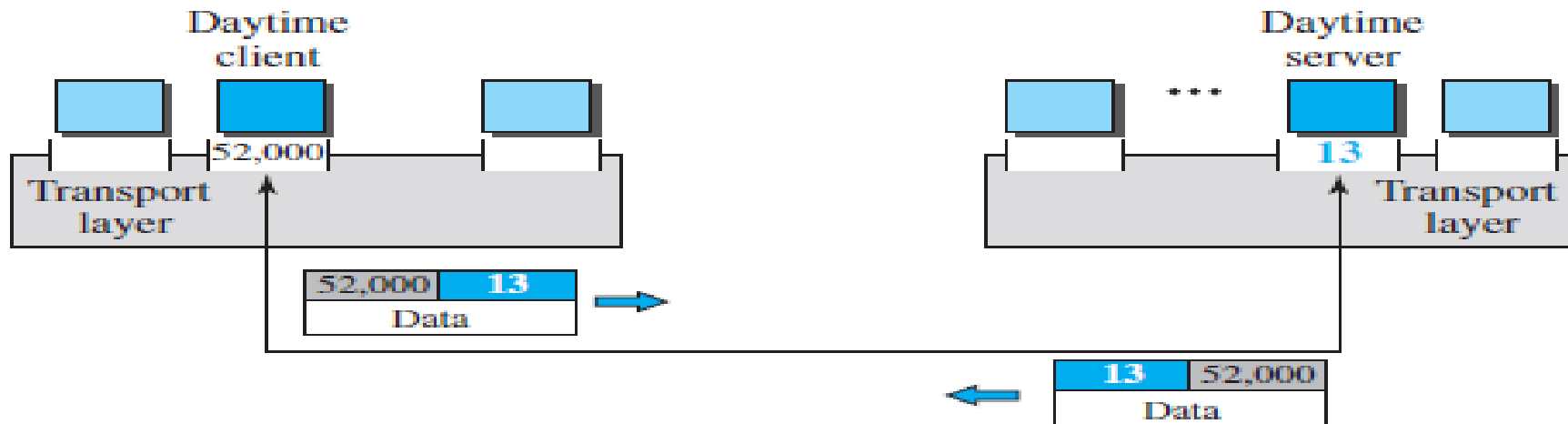
- The first duty of a transport-layer protocol is to provide process-to-process communication. A process is an application-layer entity that uses the services of the transport layer.
- A transport-layer protocol is responsible for delivery of the message to the appropriate process.



Elements of Transport Protocols cont....

Addressing: Port Numbers

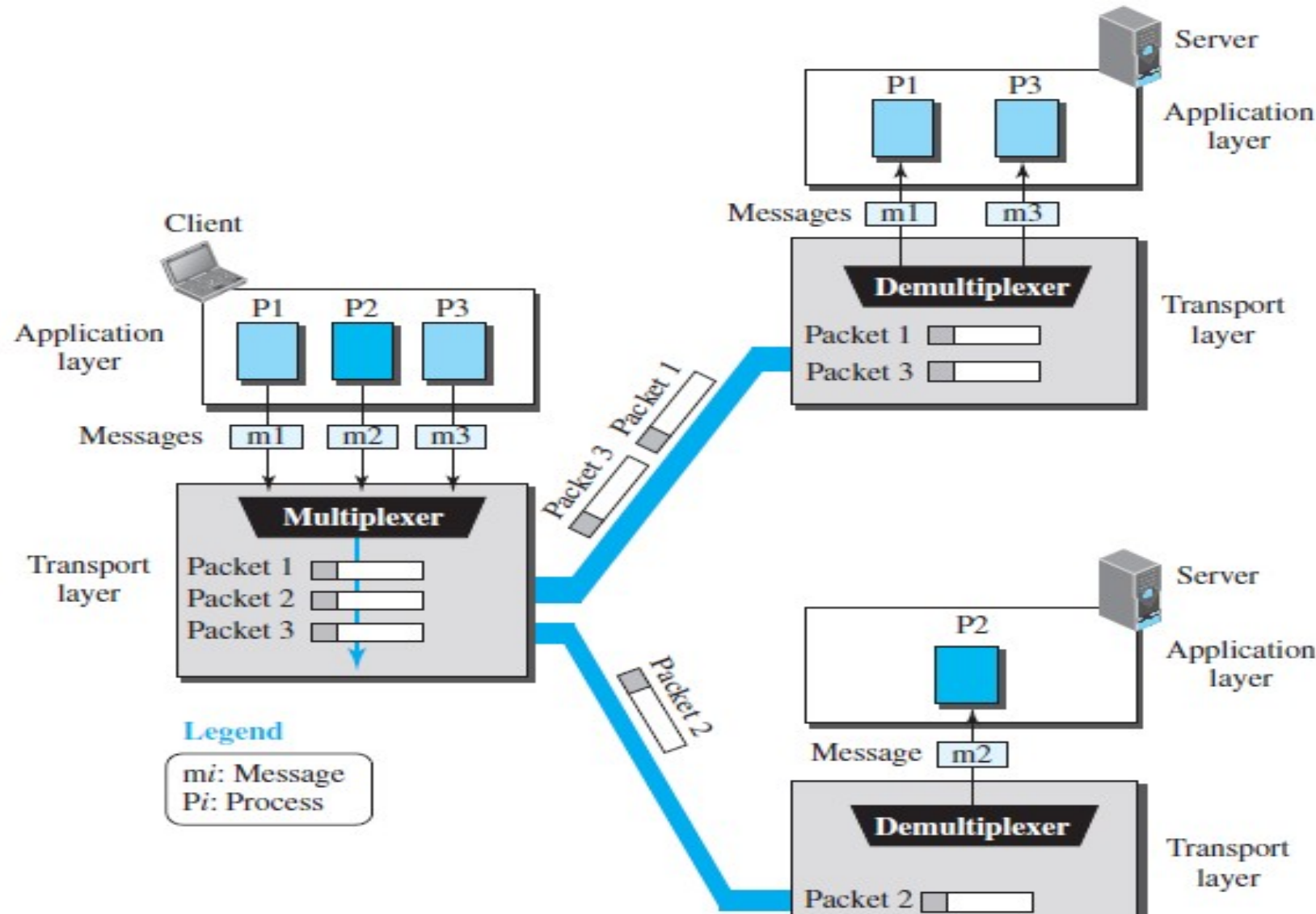
- For the purpose of process to process communication, we must define the **local host, local process, remote host, and remote process**.
- The local host and the remote host are defined using IP addresses. To define the processes, we need second identifiers, called ***port numbers***.
- The client program and the server process define their own port number (mostly temporary and permanent respectively).



Elements of Transport Protocols cont...

Multiplexing/demultiplexing

- With proto perfo
- The t the demu
- That proto acces
- The funct



transport
protocol

multiplexing;
performs

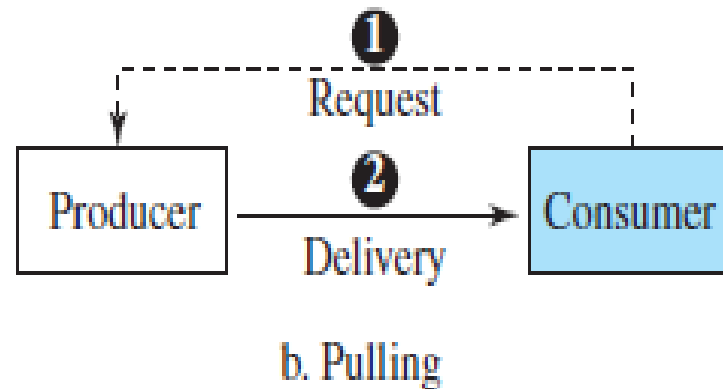
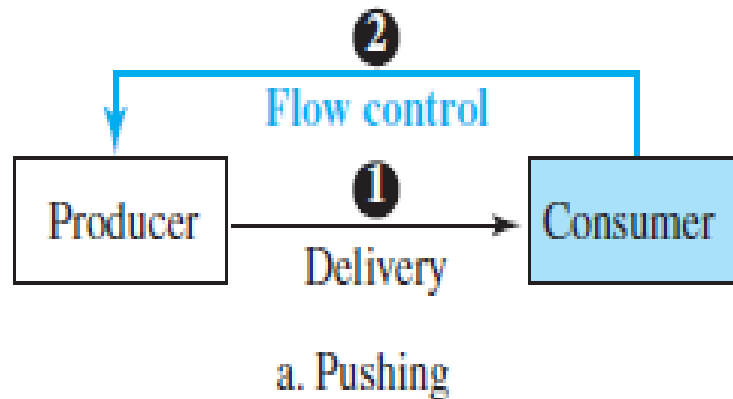
transport
or service

demultiplexing
that it uses.

Elements of Transport Protocols cont...

Flow Control

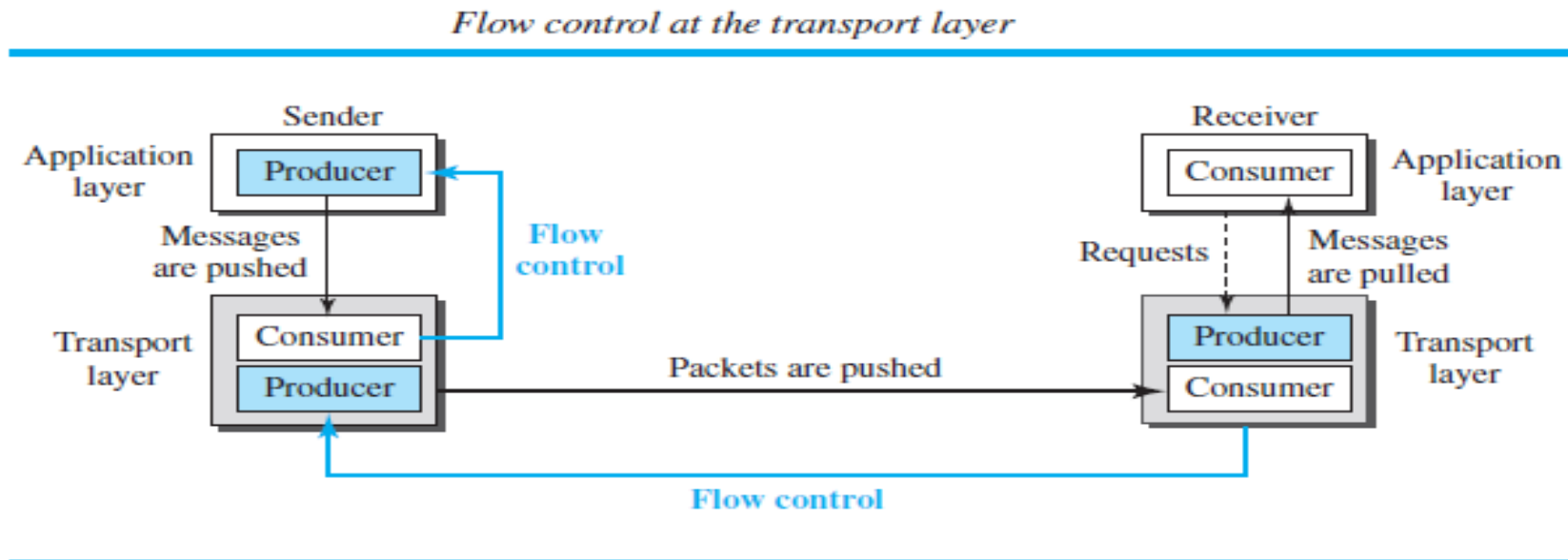
- Whenever an entity produces items and another entity consumes them, there should be a balance between production and consumption rates.
- If the sender delivers items whenever they are produced without a prior request from the consumer the delivery is referred to as pushing. If the producer delivers the items after the consumer has requested them, the delivery is referred to as pulling.



- Flow control is only required when we use a pushing method.

Elements of Transport Protocols cont...

- In communication at the transport layer, we are dealing with **four entities: sender process, sender transport layer, receiver transport layer, and receiver process.**
- We need at least two cases of flow control: from the sending transport layer to the sending application layer and from the receiving transport layer to the sending transport layer.



Elements of Transport Protocols cont...

Error Control

- In the Internet, since the underlying network layer (IP) is unreliable, we need to make the transport layer reliable if the application requires reliability.
- Reliability can be achieved to add error control services to the transport layer. **Error control at the transport layer is responsible for**
 1. Detecting and discarding corrupted packets.
 2. Keeping track of lost and discarded packets and resending them.
 3. Recognizing duplicate packets and discarding them.
 4. Buffering out-of-order packets until the missing packets arrive.

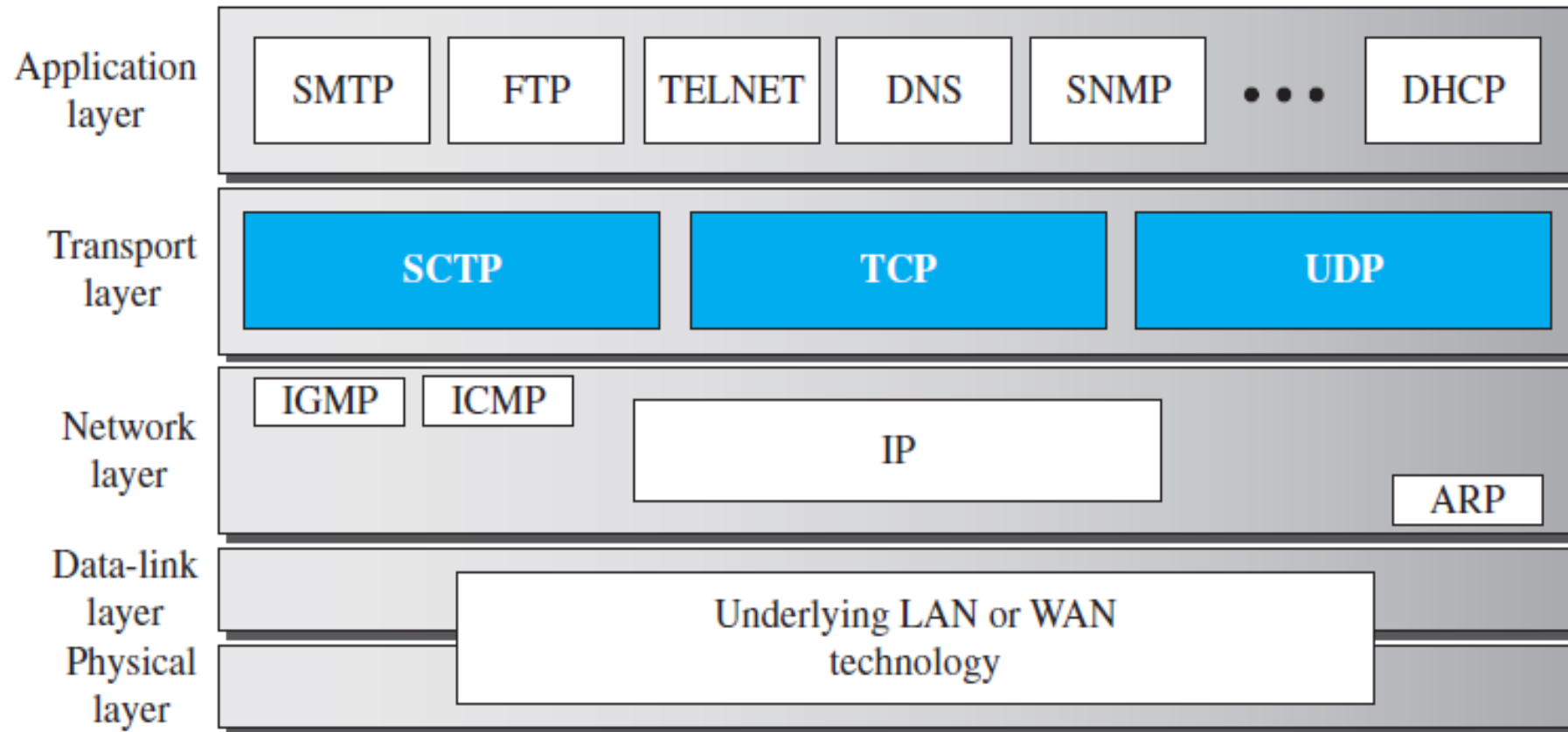
Elements of Transport Protocols cont...

Congestion Control

- Congestion in a network may occur if the **load on the network, the number of packets sent to the network, is greater than the capacity of the network the number of packets a network can handle**. Congestion happens in any system that involves waiting (on road traffic).
- **Congestion control refers to the mechanisms and techniques that control the congestion and keep the load below the capacity.**
- Congestion in a network occurs because routers and switches have queues. If a router cannot process the packets at the same rate at which they arrive, the queues become overloaded and congestion occurs.
- Congestion at the transport layer is actually the result of congestion at the **network layer**, which manifests itself at the transport layer.

Transport Layer Protocols

Position of transport-layer protocols in the TCP/IP protocol suite



Reliable Data Transfer: TCP

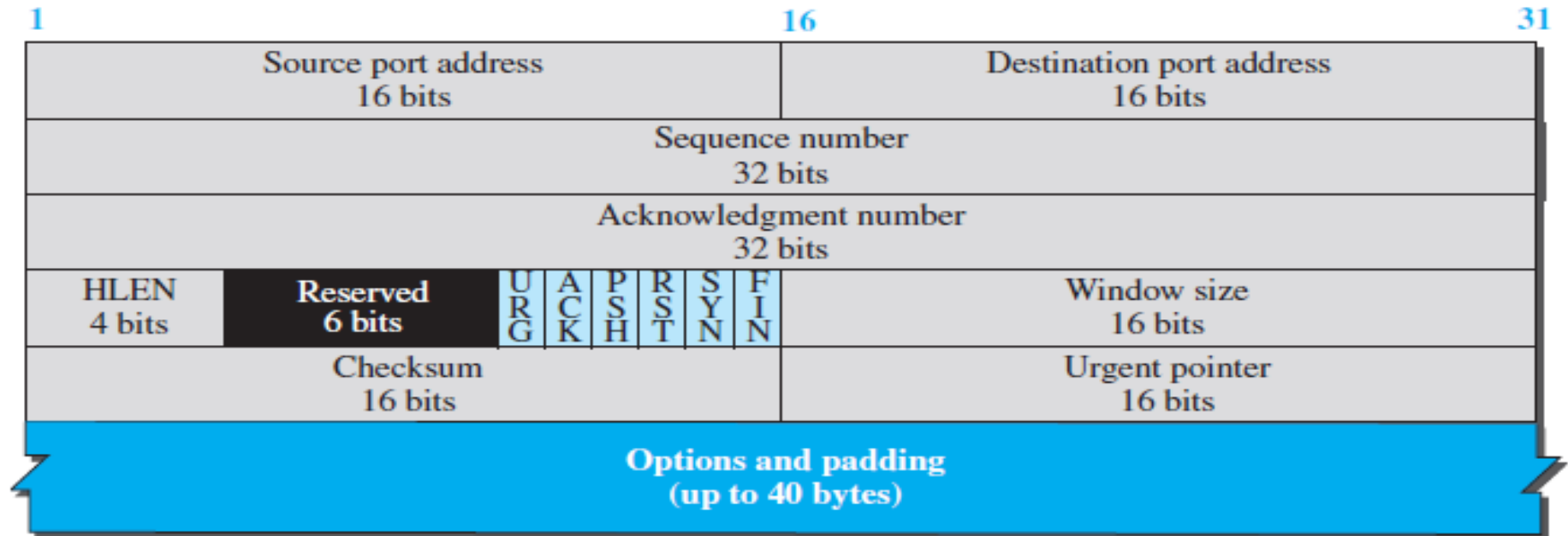
- TCP is designed to provide reliable communication between pairs of processes (TCP users) across a variety of reliable and unreliable networks and internets.
- TCP explicitly defines connection establishment, data transfer, and connection teardown phases to provide a connection-oriented service.
- To achieve this goal, TCP uses checksum, retransmission of lost or corrupted packets, cumulative and selective acknowledgments, and timers.
- TCP provides two useful facilities for labeling data: push and urgent:
 - **Data stream push:** Ordinarily, TCP decides when sufficient data have accumulated to form a segment for transmission. The TCP user can require TCP to transmit all outstanding data up to and including that labeled with a push flag. On the receiving end, TCP will deliver these data to the user in the same manner.
 - **Urgent data signaling:** This provides a means of informing the destination TCP user that significant or “urgent” data is in the upcoming data stream. It is up to the destination user to determine appropriate action.

TCP cont....

TCP header



a. Segment



b. Header

TCP cont.....

TCP Mechanisms

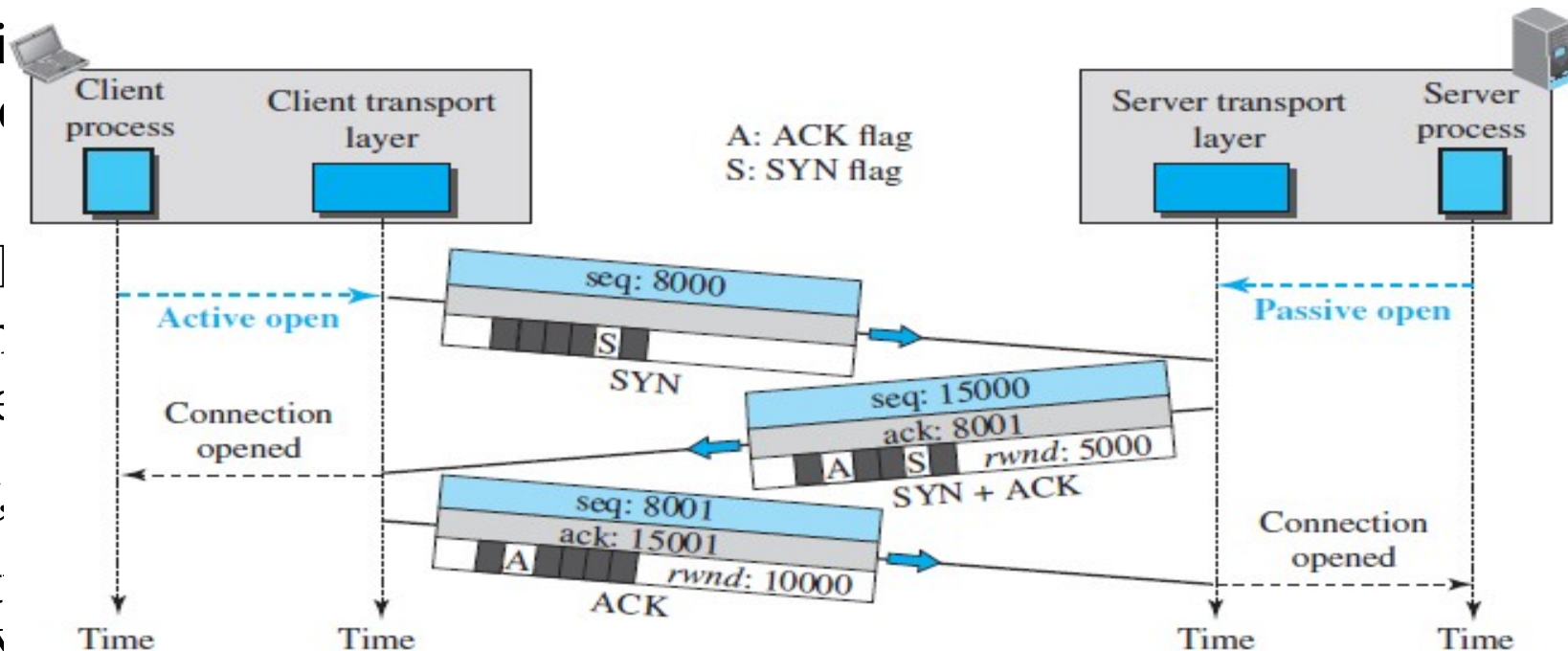
- We can group TCP mechanisms into the categories of connection establishment, data transfer, and connection termination.
- **Connection Establishment** in TCP always uses a three-way handshake. When the SYN flag is set, the segment is essentially a request for connection and functions.

- To initiate sequence setting

- The acknowledgment segment occupies

- Finally,

- If the time with SYN



the initial
X+1 by

receive a
, which

respond

TCP cont.....

Data Transfer

- Although data are transferred in segments over a transport connection, data transfer is viewed logically as consisting of a stream of octets. Hence every octet is numbered, modulo 2^{32} .
- Data are buffered by the transport entity on both transmission and reception.

Connection Termination

- The normal means of terminating a connection is a graceful close. Each TCP user must issue a CLOSE primitive. The transport entity sets the FIN bit on the last segment that it sends out, which also contains the last of the data to be sent on this connection.
- An abrupt termination occurs if the user issues an ABORT primitive.

TCP.....

Example

- Suppose a TCP connection is transferring a file of 8000 bytes. The first byte is numbered 10,001. What are the sequence numbers for each segment if data are sent in four segments, each carrying 2000 bytes?

Solution

The following shows the sequence number for each segment:

Segment 1 Sequence Number: 10,001 (range: 10,001 to 12,000)

Segment 2 Sequence Number: 12,001 (range: 12,001 to 14,000)

Segment 3 Sequence Number: 14,001 (range: 14,001 to 16,000)

Segment 4 Sequence Number: 16,001 (range: 16,001 to 18,000)

TCP cont.....

TCP Implementation Policy Options

- The TCP standard provides a precise specification of the protocol to be used between TCP entities. The design areas for which options are specified are the following:
 - Send policy: in the **absence of both pushed data and a closed** transmission window, a sending TCP entity is free to transmit data at its own convenience.
 - Deliver policy: in the absence of a Push, a receiving TCP entity is free to deliver data at its own convenience
 - Accept policy: in order or in window
 - Retransmit policy: first, batch or individual
 - Acknowledge policy: **immediate or cumulative**

Congestion Control

- If the transport entities on many machines send too many packets into the network too quickly, the network will become congested, with performance degraded as packets are delayed and lost.
- Controlling congestion to avoid this problem is the **combined responsibility of the network and transport layers**.
- Congestion occurs at routers, so it is detected at the network layer. However, congestion is ultimately caused by traffic sent into the network by the transport layer.
- **The only effective way to control congestion is for the transport protocols to send packets into the network more slowly.**

Congestion Control cont.....

- Congestion has two main effects.
 - First, as congestion begins to occur, the transit time across a network or internetwork increases.
 - Second, as congestion becomes severe, network or internet nodes drop packets.
- The TCP flow control mechanism can be used to recognize the onset of congestion (by recognizing increased delay times and dropped segments) and to react by reducing the flow of data.
- If many of the TCP entities operating across a network exercise this sort of restraint, internet congestion is relieved.
- A number of techniques have been implemented that are intended to improve TCP congestion control characteristics.

Congestion Control cont.....

Desirable Bandwidth Allocation

Efficiency and Power:

- An efficient allocation of bandwidth across transport entities will use all of the network capacity that is available.

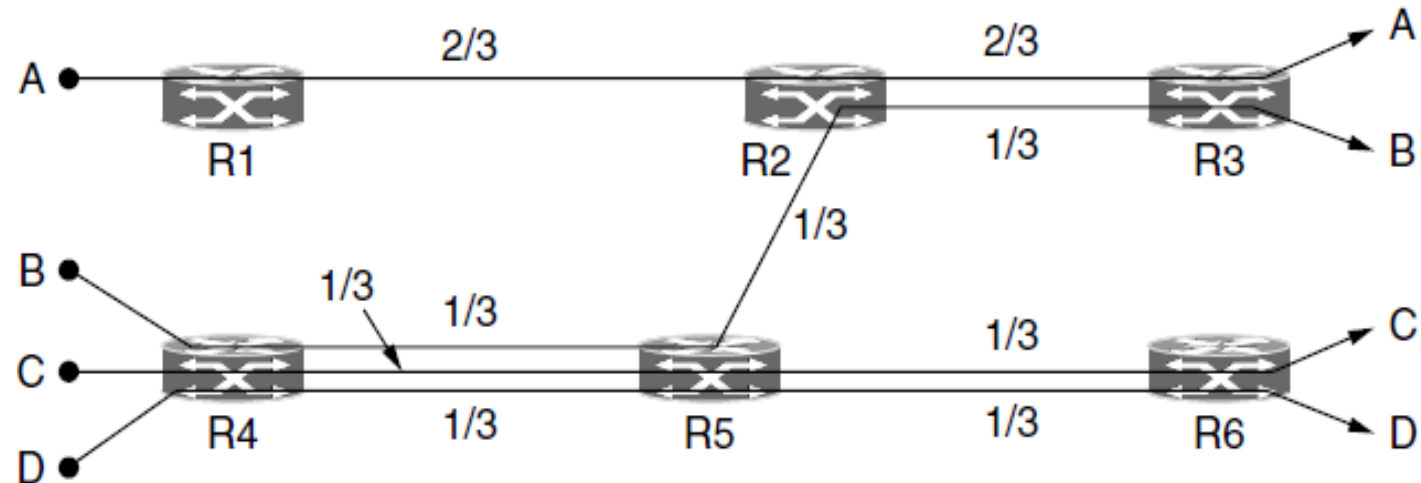
$$\textit{power} = \textit{load}/\textit{delay}$$

- Power will initially rise with offered load, as delay remains small and roughly constant, but will reach a maximum and fall as delay grows rapidly.
- The load with the highest power represents an efficient load for the transport entity to place on the network.

Congestion Control cont.....

Max-Min Fairness

- An allocation is max-min fair if the bandwidth given to one flow cannot be increased without decreasing the bandwidth given to another flow with an allocation that is no larger. That is, increasing the bandwidth of a flow will only make the situation worse for flows that are less well off.
- **Example:**

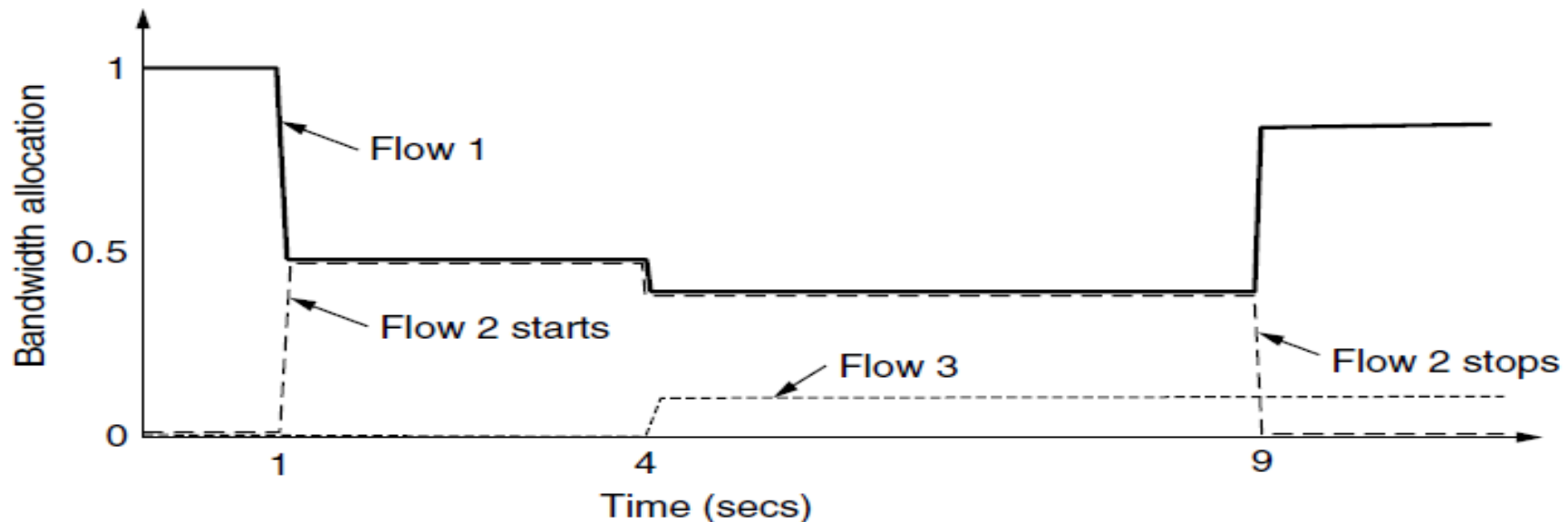


Max-min bandwidth allocation for four flows

Congestion Control cont.....

Convergence

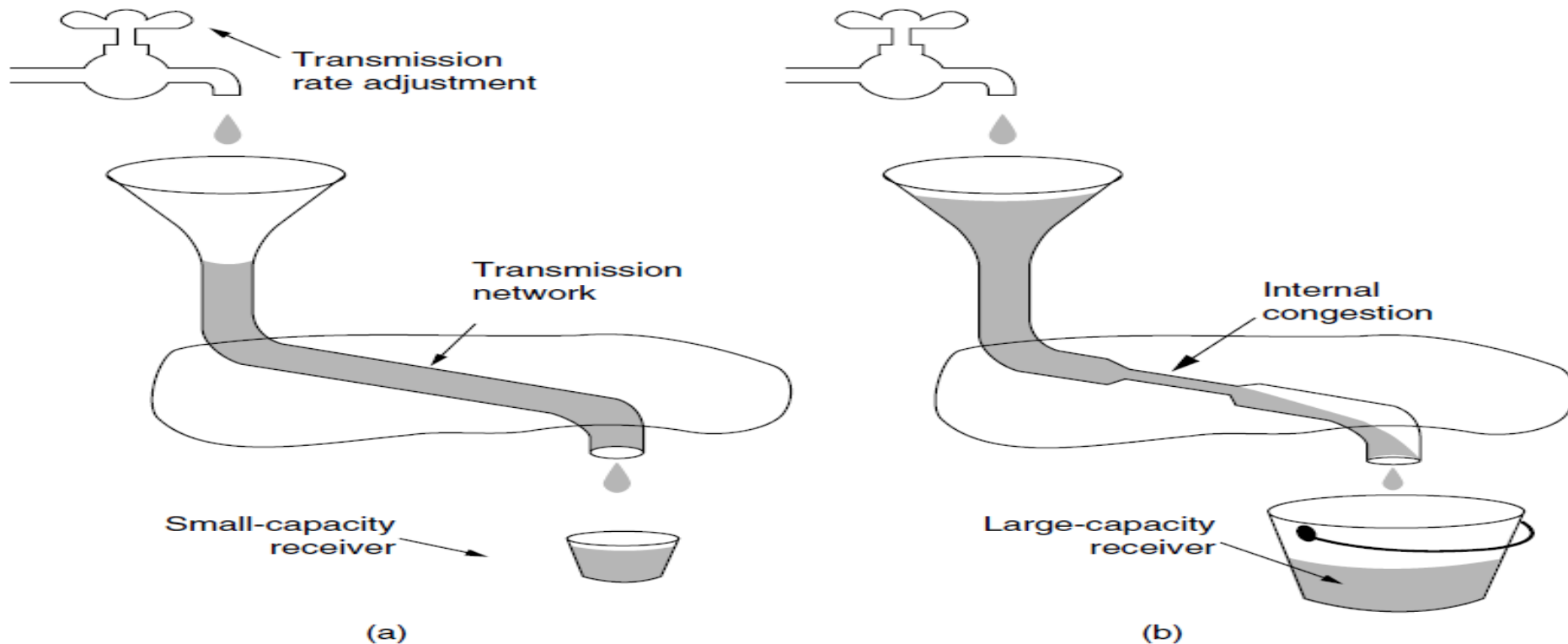
- A final criterion is that the congestion control **algorithm converge quickly** to a **fair and efficient allocation of bandwidth**.
- If the convergence is too slow, the algorithm will never be close to the changing operating point.
- If the algorithm is not stable, it may fail to converge to the right point in some cases, or even oscillate around the right point.



Congestion Control cont.....

Regulating the Sending Rate

- The sending rate may be limited by two factors. The first is flow control, in the case that there is **insufficient buffering at the receiver**.
- The second is congestion, in the case that there is **insufficient capacity in the network**.



Congestion Control cont.....

- The way that a transport protocol should regulate the sending rate depends on the form of the **feedback returned by the network**.
- Different network layers may return different kinds of feedback. The feedback may be explicit or implicit, and it may be precise or imprecise.
- An example of an explicit, precise design is when routers tell the sources the rate at which they may send.
- An explicit, imprecise design is the use of ECN (Explicit Congestion Notification) with TCP. In this design, routers set bits on packets that experience congestion to warn the senders to slow down, but they do not tell them how much to slow down.
- FAST TCP measures the roundtrip delay and uses that metric as a signal to avoid congestion.
- Finally TCP with drop-tail or RED routers, packet loss is inferred and used to signal that the network has become congested.

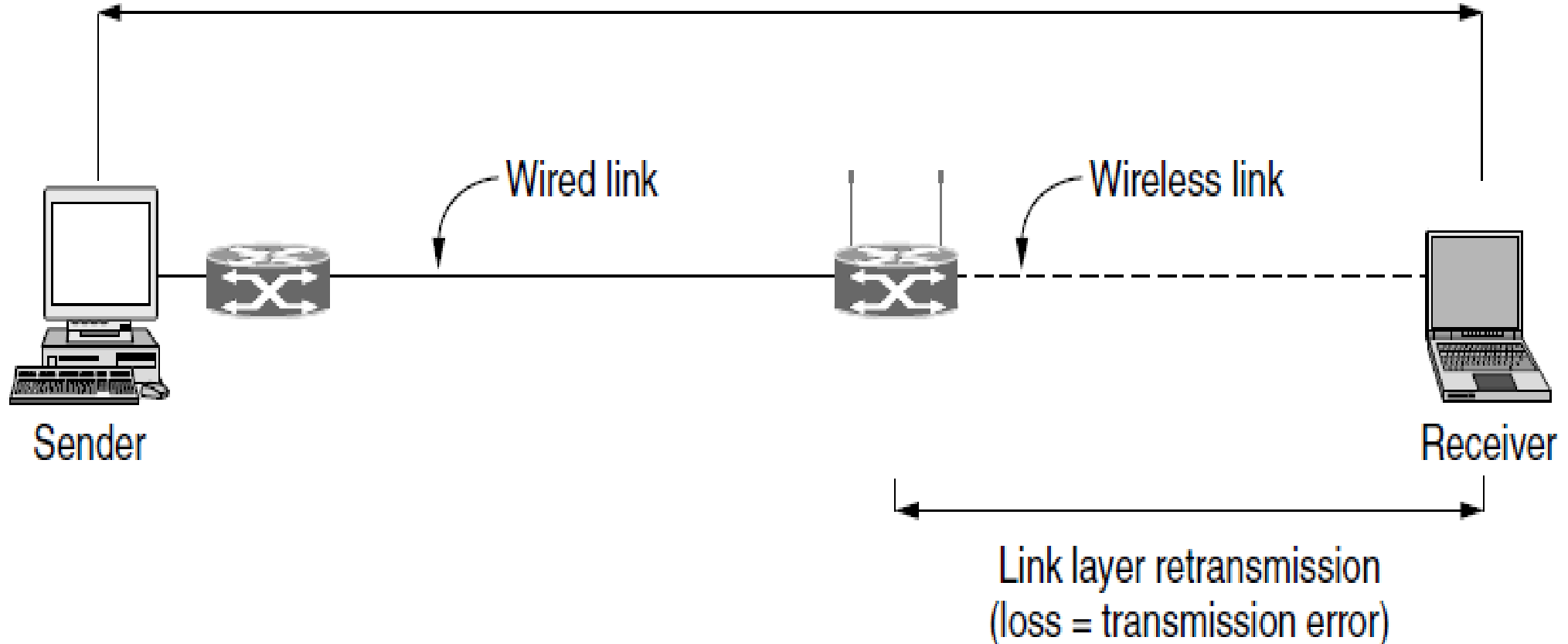
Congestion Control cont.....

Wireless Issues

- Transport protocols such as TCP that implement congestion control should be independent of the underlying network and link layer technologies.
- That is a good theory, but in practice there are issues with wireless networks.
- The main issue is that packet loss is often used as a congestion signal, including by TCP as we have just discussed. Wireless networks lose packets all the time due to transmission errors.
- One solution to this problem is to mask the wireless losses by using retransmissions over the wireless link. For example, 802.11 uses a stop-and-wait protocol to deliver each frame, retrying transmissions multiple times if need be before reporting a packet loss to the higher layer.

Congestion Control cont.....

Transport with end-to-end congestion control (loss = congestion)

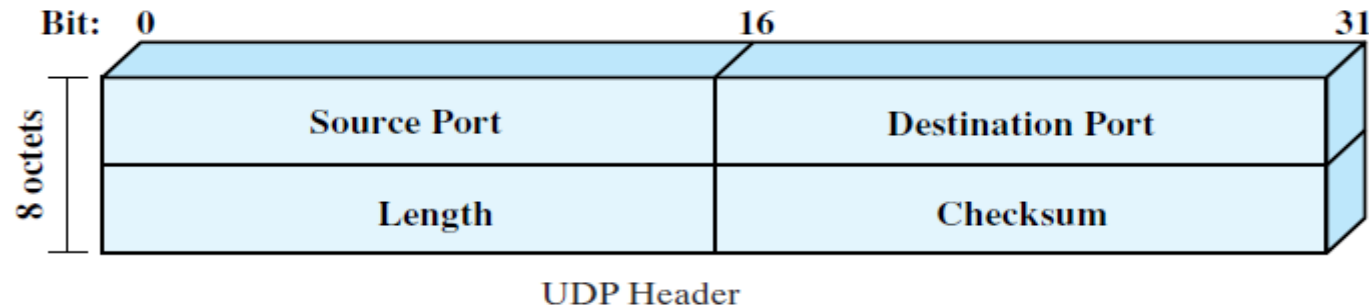


Congestion control over a path with a wireless link.

Connectionless Transport: UDP

- The **User Datagram Protocol (UDP)** is a connectionless, unreliable transport protocol. It does not add anything to the services of IP except for providing process-to-process communication instead of host-to-host communication.
- Process-to-process communication service can be provided by UDP using socket addresses, a combination of IP addresses and port numbers.
- UDP is a very simple protocol using a minimum of overhead. If a process wants to send a small message and does not care much about reliability, it can use UDP.
- UDP is a connectionless protocol, it does not provide error, flow and congestion control services for application layer protocols.

UDP cont.....



- Essentially, it adds a port addressing capability to IP. The header includes a source port and destination port. The Length field contains the length of the entire UDP segment, including header and data.
- The checksum is the same algorithm used for TCP and IP. For UDP, the checksum applies to the entire UDP segment plus a pseudo-header prefixed to the UDP header at the time of calculation and which is the same pseudo-header used for TCP.
- If an error is detected, the segment is discarded and no further action is taken.

UDP application areas

- The following shows some typical applications that can benefit more from the services of UDP than from those of TCP:
 - UDP is suitable for a process that requires **simple request-response communication** with little concern for flow and error control. **Example:** DNS, and DHCP
 - UDP is **suitable for a process with internal flow and error control mechanisms.** **For example,** the Trivial File Transfer Protocol (TFTP) process includes flow and error control.
 - UDP is a suitable for **multicasting**. Multicasting capability is embedded in the UDP software.
 - UDP is used for management processes such as SNMP.
 - UDP is used for some **route updating protocols** such as Routing Information Protocol (RIP).
 - UDP is normally used for interactive **real-time applications** that cannot tolerate uneven delay between sections of a received message.
 - UDP is suitable for inward data collection (involves the periodic active or passive sampling of data sources, such as sensors).

Chapter V

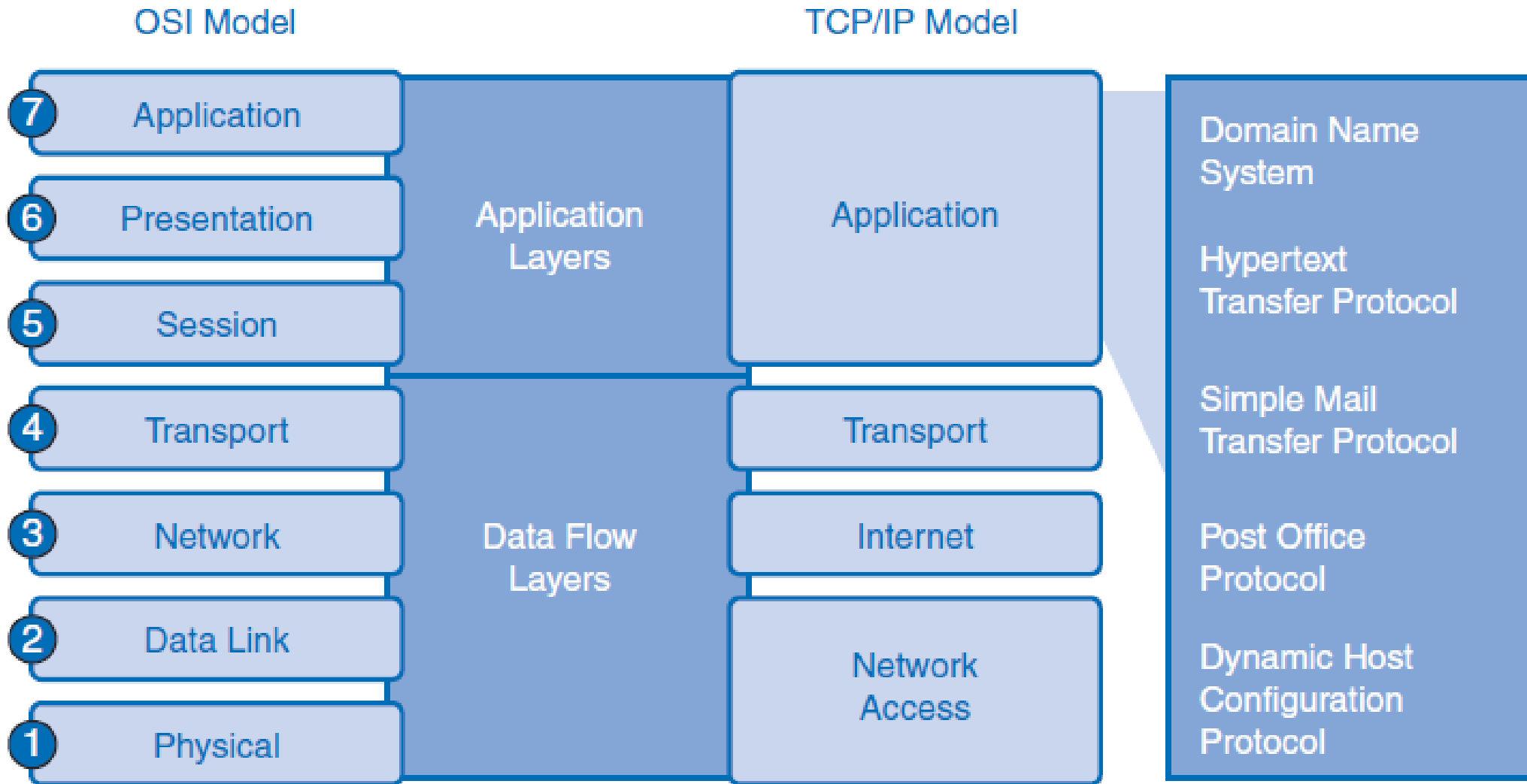
Application Layer

Data Communication and Computer Networks

(CSE 3204)

Contents

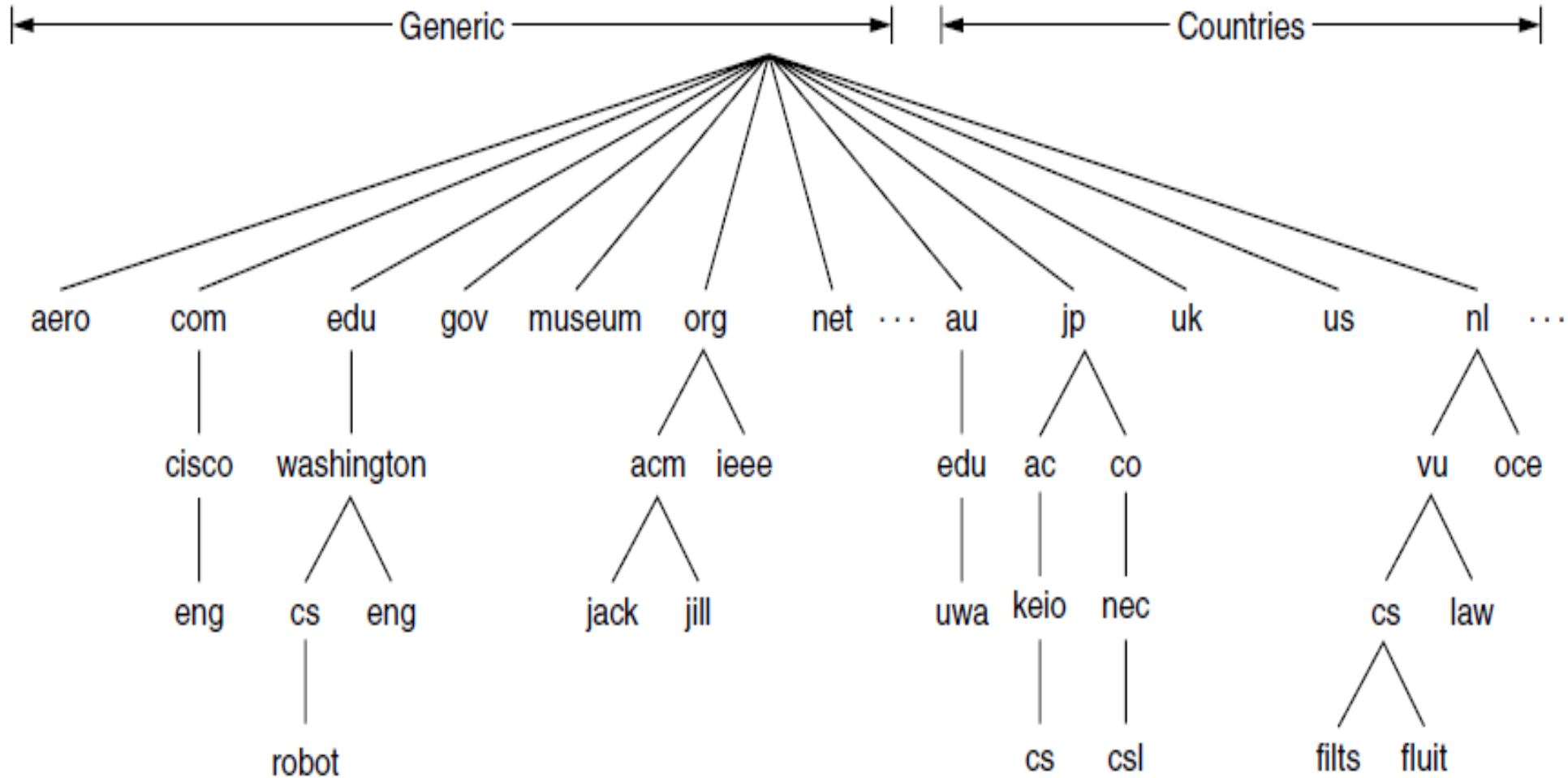
- Domain name system (DNS)
- Web access (HTTP)
- Electronic Mail (SMTP and MIME)
- Network Management (SNMP)
- Voice Over IP and Multimedia Support: SIP



Domain Name System (DNS)

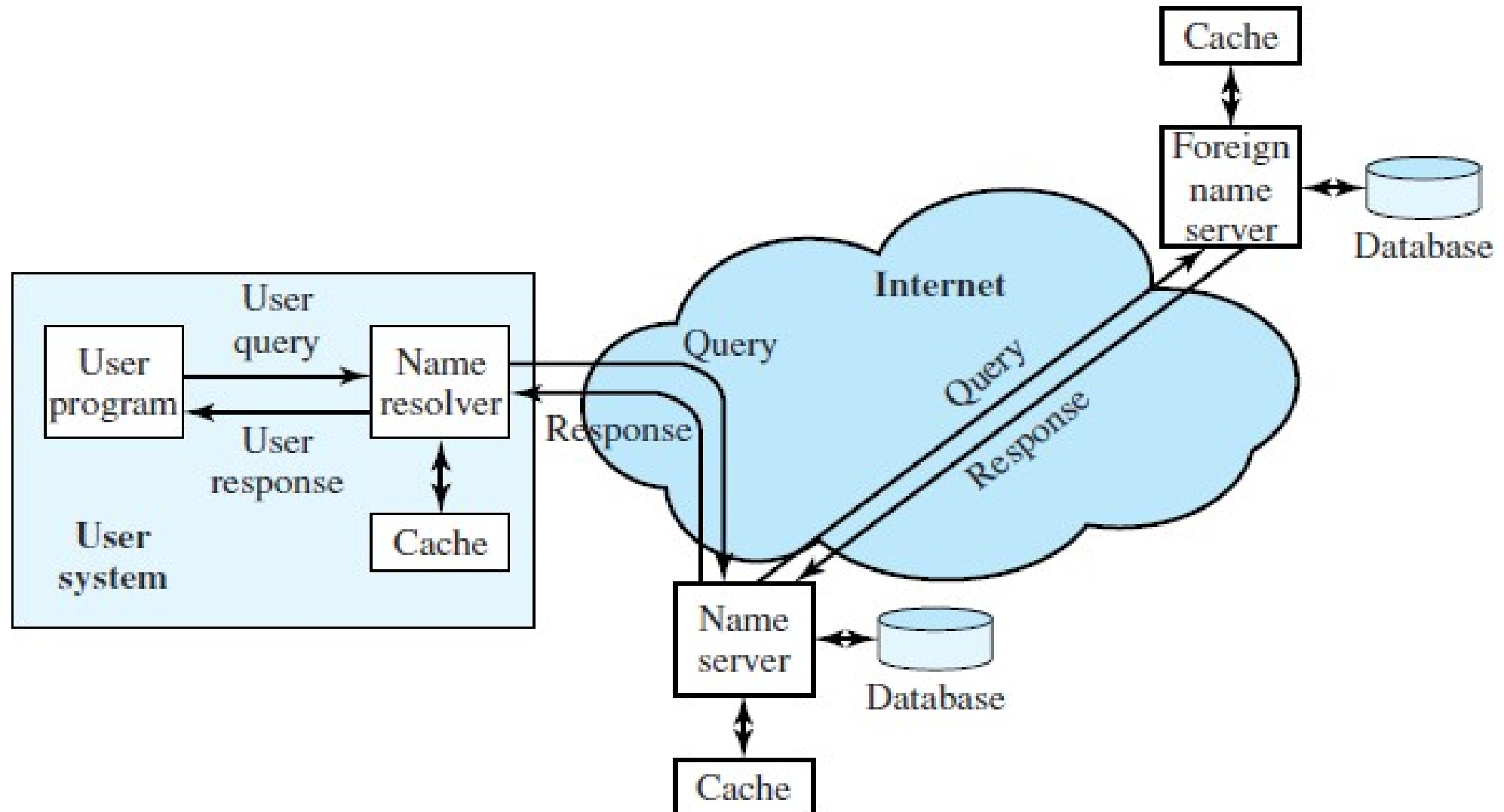
- The essence of DNS is the invention of a **hierarchical, domain-based naming** scheme and a distributed database system for implementing this naming scheme.
- It is primarily used for mapping **host names to IP addresses** but can also be used for other purposes.
- **Four elements comprise the DNS:**
 - **Domain name space:** DNS uses a tree-structured name space to **identify resources** on the Internet.
 - **DNS database:** Conceptually, each node and leaf in the name space tree structure names a set of information (e.g., IP address, type of resource) that is contained in a **resource record (RR)**. The collection of all RRs is organized into a distributed database.
 - **Name servers:** These are server programs that hold information about a portion of the domain name **tree structure and the associated RRs**.
 - **Resolvers:** These are programs that **extract information from name servers** in response to client requests. A typical client request is for an IP address corresponding to a given domain name.

The DNS Name Space



A portion of the Internet domain name space.

DNS Operation



Web Access HTTP

- The Hypertext Transfer Protocol (HTTP) is the **foundation protocol** of the World Wide Web (WWW) and can be used in any client/server application involving hypertext.
- It is a protocol for transmitting information with the efficiency necessary for making hypertext jumps.
- The data transferred by the protocol can be **plaintext, hypertext, audio, images, or any Internet-accessible information**.
- HTTP is a transaction-oriented client/server protocol.
- The most typical use of HTTP is between a **Web browser and a Web server**.
- To provide reliability, HTTP makes use of TCP

Web Access HTTP cont.....

- HTTP is a “**stateless**” **protocol**: Each transaction is treated independently.
- Accordingly, a typical implementation will create a new TCP connection between client and server for each transaction and then terminate the connection as soon as the transaction completes, although the specification does not dictate this one-to-one relationship between transaction and connection lifetimes.
- The stateless nature of HTTP is well suited to its typical application.
- A normal session of a user with a Web browser involves retrieving a sequence of Web pages and documents.
- Another important feature of HTTP is that it is flexible in the formats that it can handle.

Electronic Mail: SMTP and MIME

Simple Mail Transfer Protocol (SMTP)

- SMTP is the standard protocol for **transferring mail** between hosts in the TCP/IP suite.
- SMTP has traditionally been limited to the delivery of simple text messages.
- SMTP is not concerned with the format or content of messages themselves, with two exceptions.
 1. SMTP standardizes the message character set as **7-bit ASCII**.
 2. SMTP adds **log information** to the start of the delivered message that indicates the path the message took.

SMTP cont.....

- To begin, mail is created by a user agent program in response to user input.
- Each created message consists of a header that includes the recipient's e-mail address and other information, and a body containing the message to be sent.
- These messages are then queued in some fashion and provided as input to an SMTP Sender program, which is typically an always-present server program on the host.
- Although the structure of the outgoing mail queue will differ depending on the host's operating system, each queued message conceptually has two parts:
 1. The message text, consisting of
 2. A list of mail destinations.

Multipurpose Internet Mail Extensions (MIME)

- MIME is an extension to address some of the problems and limitations of the use of SMTP electronic mail. Lists the following limitations of the SMTP scheme:
 1. SMTP cannot transmit executable files or other binary objects.
 2. SMTP cannot transmit text data that includes national language characters because these are represented by 8-bit codes with values of 128 decimal or higher, and SMTP is limited to 7-bit ASCII.
 3. SMTP servers may reject mail messages over a certain size.
 4. SMTP gateways that translate between the character codes ASCII and EBCDIC do not use a consistent set of mappings, resulting in translation problems.
 5. SMTP gateways to X.400 electronic mail networks cannot handle non textual data included in X.400 messages.

MIME cont....

- The MIME specification includes the following elements:
 1. New message header fields are defined, which may be included in an RFC 822 header. These fields provide information about the body of the message.
 2. A number of content formats are defined, thus standardizing representations that support multimedia electronic mail.
 3. Transfer encodings are defined that enable the conversion of any content format into a form that is protected from alteration by the mail system.

Network Management: Simple Network Management Protocol (SNMP)

- As networks grow in scale, two facts become painfully evident:
 - The network and its associated resources and distributed applications become indispensable (vital) to the organization.
 - More things can go wrong, disabling the network or a portion of the network or degrading performance to an unacceptable level.
- A large, reliable network cannot be put together and managed by human effort alone.
- The complexity of such a system dictates the use of **automated network management tools**.

SNMP cont.....

- A network management system is a collection of tools for network monitoring and control that is integrated in the following senses:
 - A single operator interface with a powerful but user-friendly set of commands for performing most or all network management tasks.
 - A minimal amount of additional equipment. That is, most of the hardware and software required for network management is incorporated into the existing user equipment.
- The software used in accomplishing the network management tasks resides in the host computers and communications processors (e.g., networks switches, routers).
- A NMS is designed to view the entire network as a unified architecture, with addresses and labels assigned to each point.
- The active elements of the network provide regular feedback of status information to the network control center.

SNMP cont.....

- SNMP was developed for use as a network management tool for networks and internetworks operating TCP/IP.
- The term SNMP is actually used to refer to a collection of specifications for network management that include the protocol itself, the definition of a database, and associated concepts.
- The model of network management that is used for **SNMP includes the following key elements:**
 - Management station, or manager
 - Agent
 - Management information base
 - Network management protocol

SNMP cont.....

- The **management station** is typically a standalone device, but may be a capability implemented on a shared system. The management station serves as the interface for the human network manager into the network management system. The management station will have:
 - A set of management applications for **data analysis, fault recovery**, and so on.
 - An interface by which the network manager may monitor and control the network.
 - The capability of translating the network manager's requirements into the actual monitoring and control of remote elements in the network.
 - A database of network management information extracted from the databases of all the managed entities in the network.

SNMP cont.....

- **Agents** such as **hosts, bridges, routers, and hubs**, may be equipped with agent software so that they may be managed from a management station.
- The agent responds to requests for information from a management station, responds to requests for actions from the management station, and may asynchronously provide the management station with important but unsolicited information.
- The collection of objects is referred to as a **management information base (MIB)**. The MIB functions as a collection of access points at the agent for the management station.

SNMP cont....

- The management station and agents are linked by a **network management protocol**.
- The protocol used for the management of TCP/IP networks is the SNMP. An enhanced version of SNMP, known as SNMPv2, is intended for both TCP/IP- and OSI-based networks. Each of these protocols includes the following key capabilities:
 - **Get**: Enables the management station to retrieve the value of objects at the agent.
 - **Set**: Enables the management station to set the value of objects at the agent.
 - **Notify**: Enables an agent to send unsolicited notifications to the management station of significant events.

Voice Over IP and Multimedia Support: SIP

- The Session Initiation Protocol (SIP) is an application level control protocol for setting up, modifying, and terminating real-time sessions between participants over an IP data network.
- The key driving force behind SIP is to enable Internet telephony, also referred to as **voice over IP (VoIP)**.
- SIP can support any type of **single media or multimedia session**, including teleconferencing.
- SIP supports five facets of establishing and terminating multimedia communications:
 - **User location:** Users can move to other locations and access their telephony or other application features from remote locations.

SIP cont.....

- **User availability:** Determination of the willingness of the called party to engage in communications.
- **User capabilities:** Determination of the media and media parameters to be used.
- **Session setup:** Setup up point-to-point and multiparty calls, with agreed session parameters.
- **Session management:** Including transfer and termination of sessions, modifying session parameters, and invoking services.

End of the Course!!!

Thank
You for Your
Attention

