

OSI 7 LAYER MODEL VS TCP/IP

Mohammad S. Hasan

Introduction – Data and Signals

2

Table 2-1

Five combinations of data and signals

Data	Signal	Common Conversion Technique	Common Devices	Common Systems
Analog	Analog	Amplitude modulation Frequency modulation	Radio tuner TV tuner	Telephone Cable TV Broadcast TV AM and FM Radio
Digital	Digital	NRZ-L NRZI Manchester Differential Manchester Bipolar-AMI 4B/5B	Digital encoder	Local area networks Telephone systems HDTV
Digital	Analog	Amplitude shift keying Frequency shift keying Phase shift keying	Modem	Dial-up Internet access DSL Cable modems
Analog	Digital	Pulse code modulation Delta modulation	Codec	Telephone systems Music systems
Analog or Digital	Analog	Spread spectrum technology	Spread spectrum encoder	Cordless telephones Wireless LANs

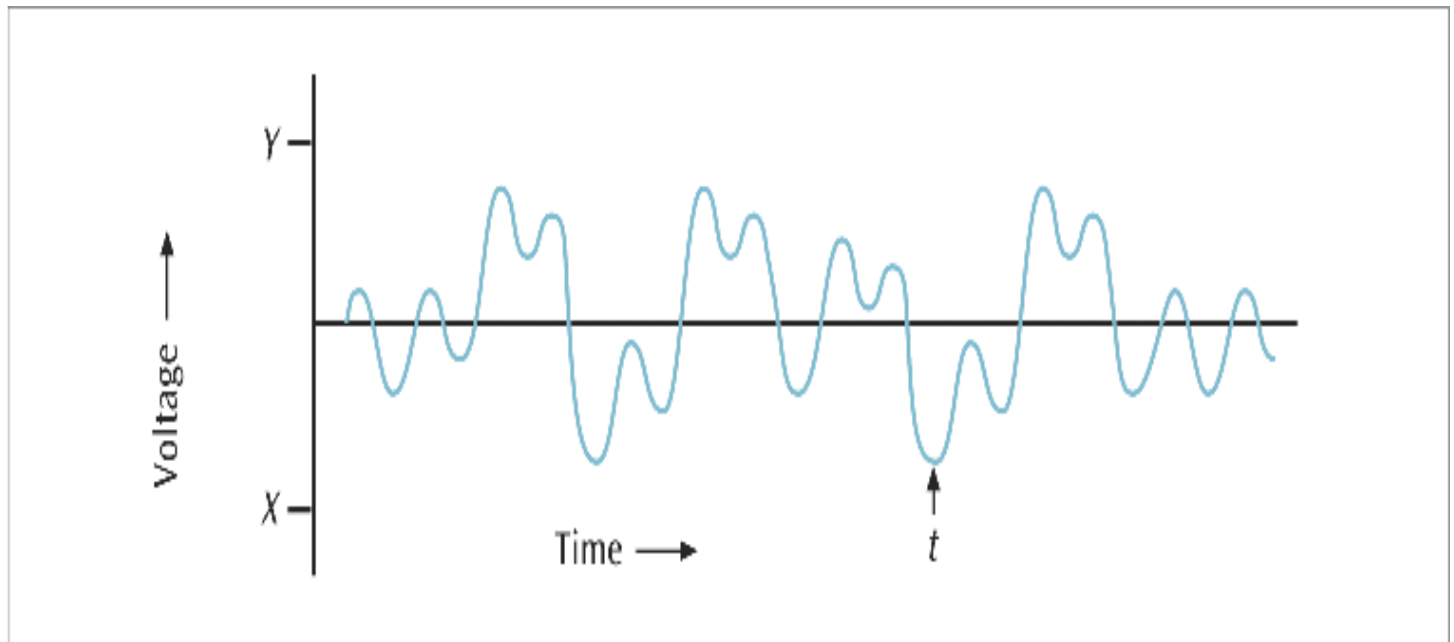
Analog versus Digital

3

- Analog - continuous waveform
- Examples: (naturally occurring) music and voice

Figure 2-1

A simple example of an analog waveform



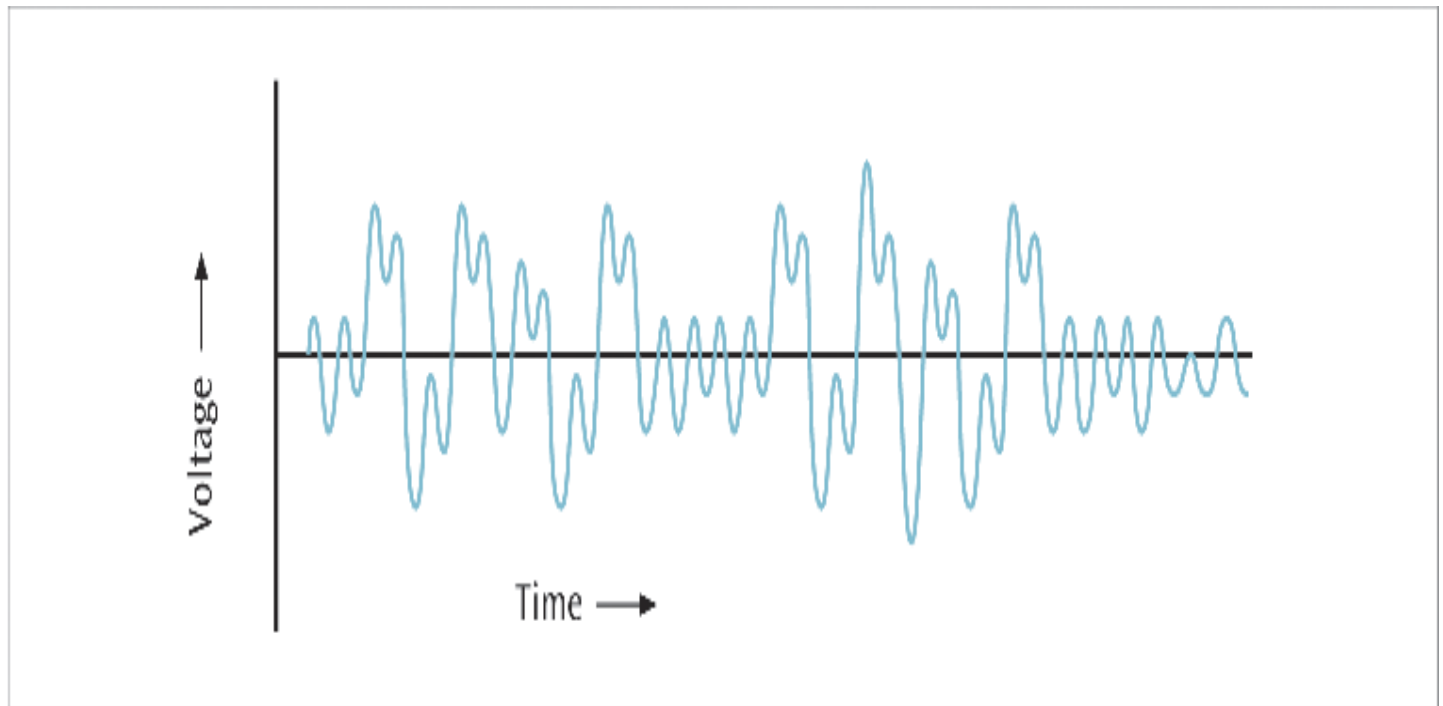
Analog versus Digital

4

- Harder to separate noise from an analog signal than from a digital signal

Figure 2-2

*The waveform of a
symphonic overture
with noise*



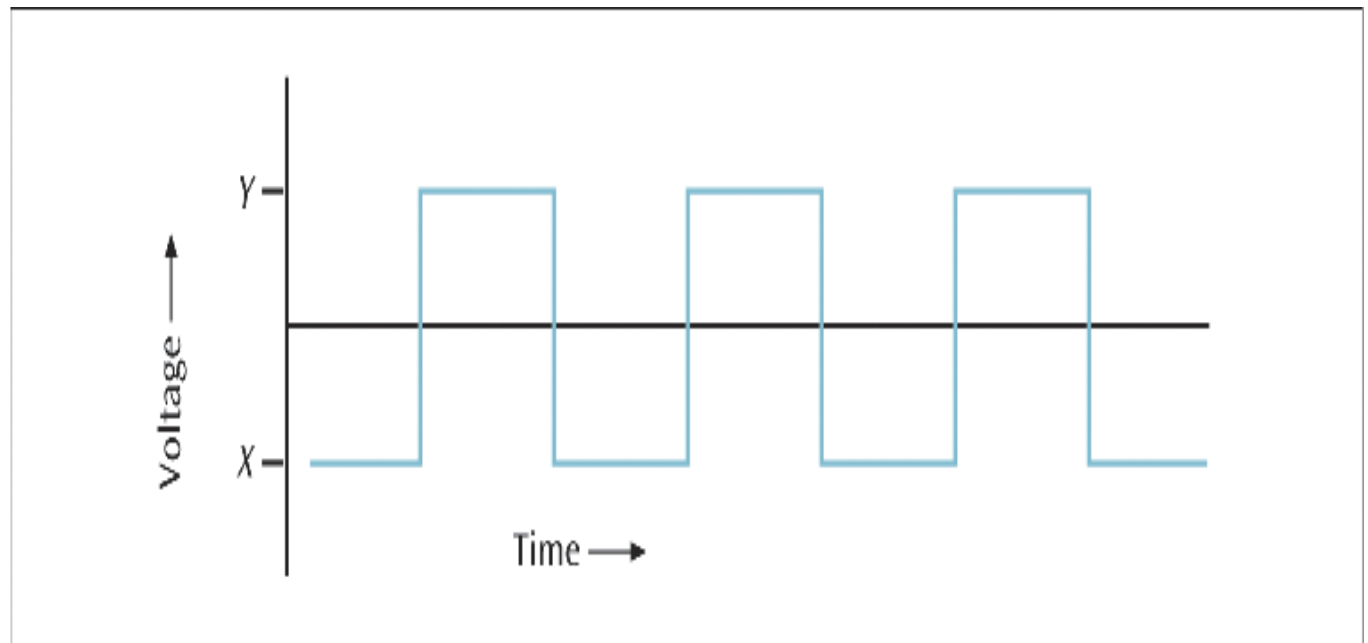
Analog versus Digital

5

- Digital - discrete or non-continuous waveform
- Examples: computer 1s and 0s

Figure 2-3

A simple example of a digital waveform



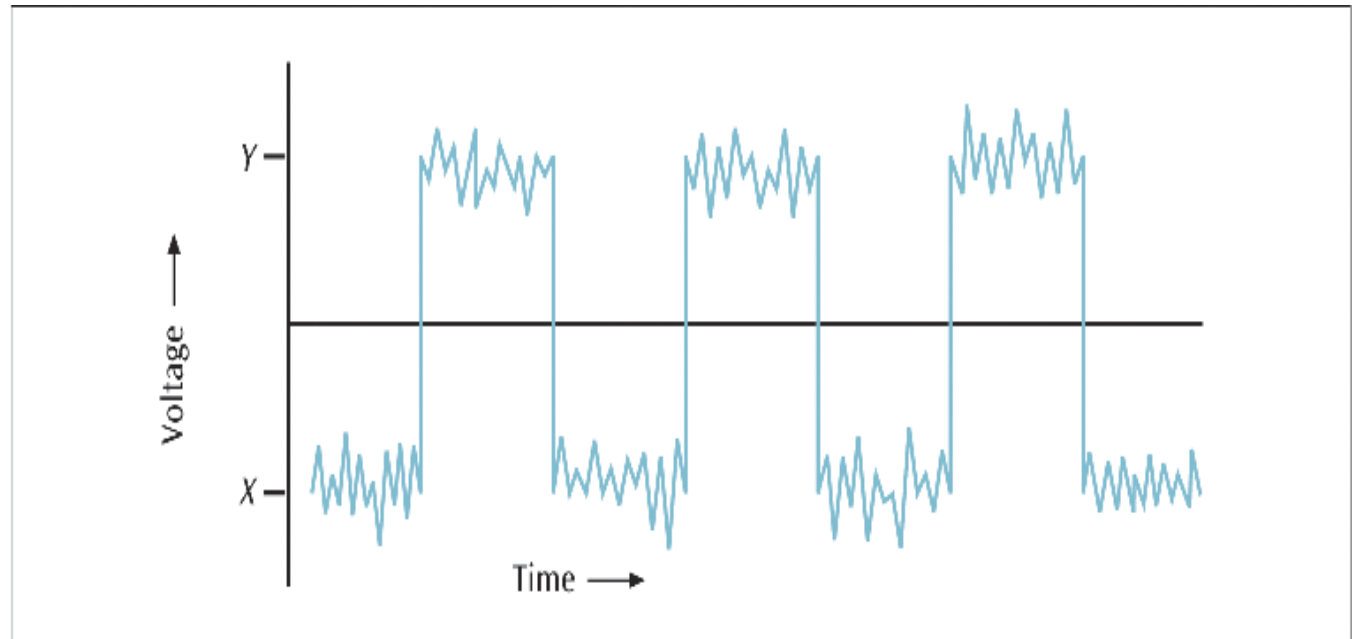
Analog versus Digital

6

- Despite noise in this digital signal
- You can still differentiate a high voltage from a low voltage

Figure 2-4

A digital signal with some noise introduced



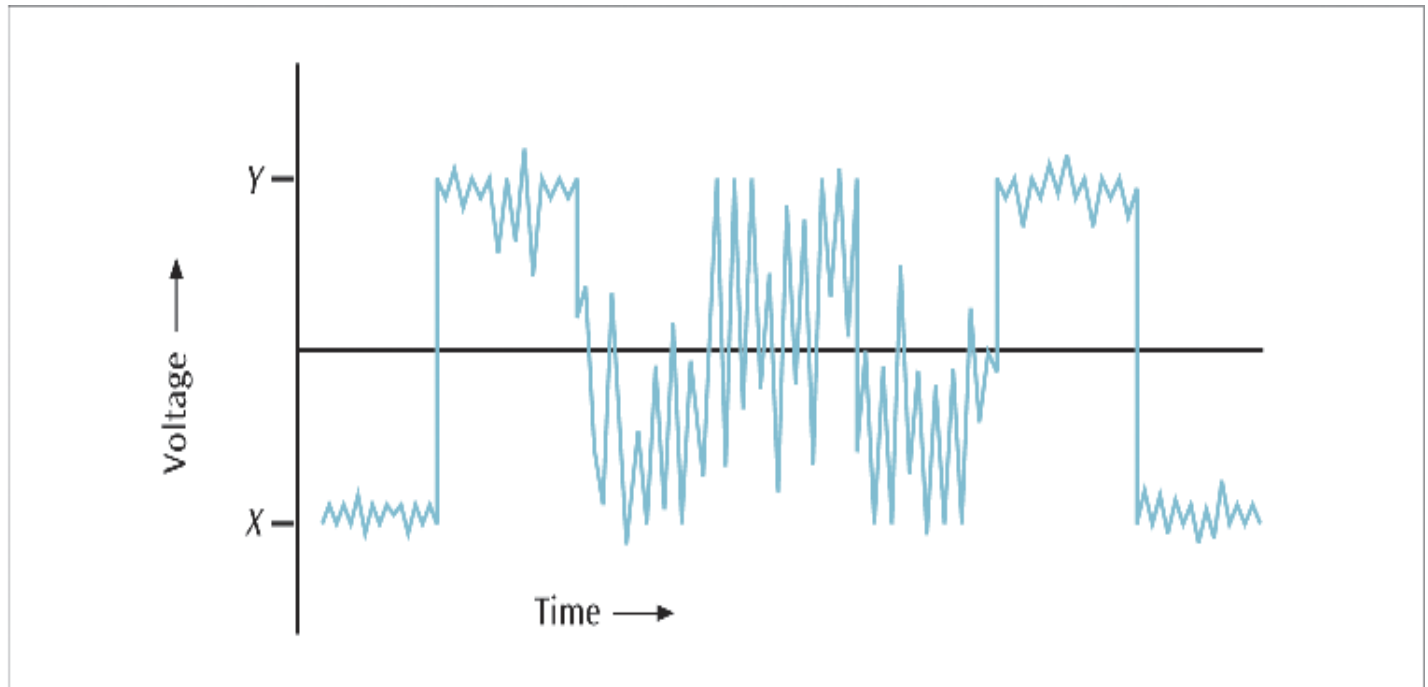
Analog versus Digital

7

- If there is too much noise
- Hard to identify a high voltage and a low voltage

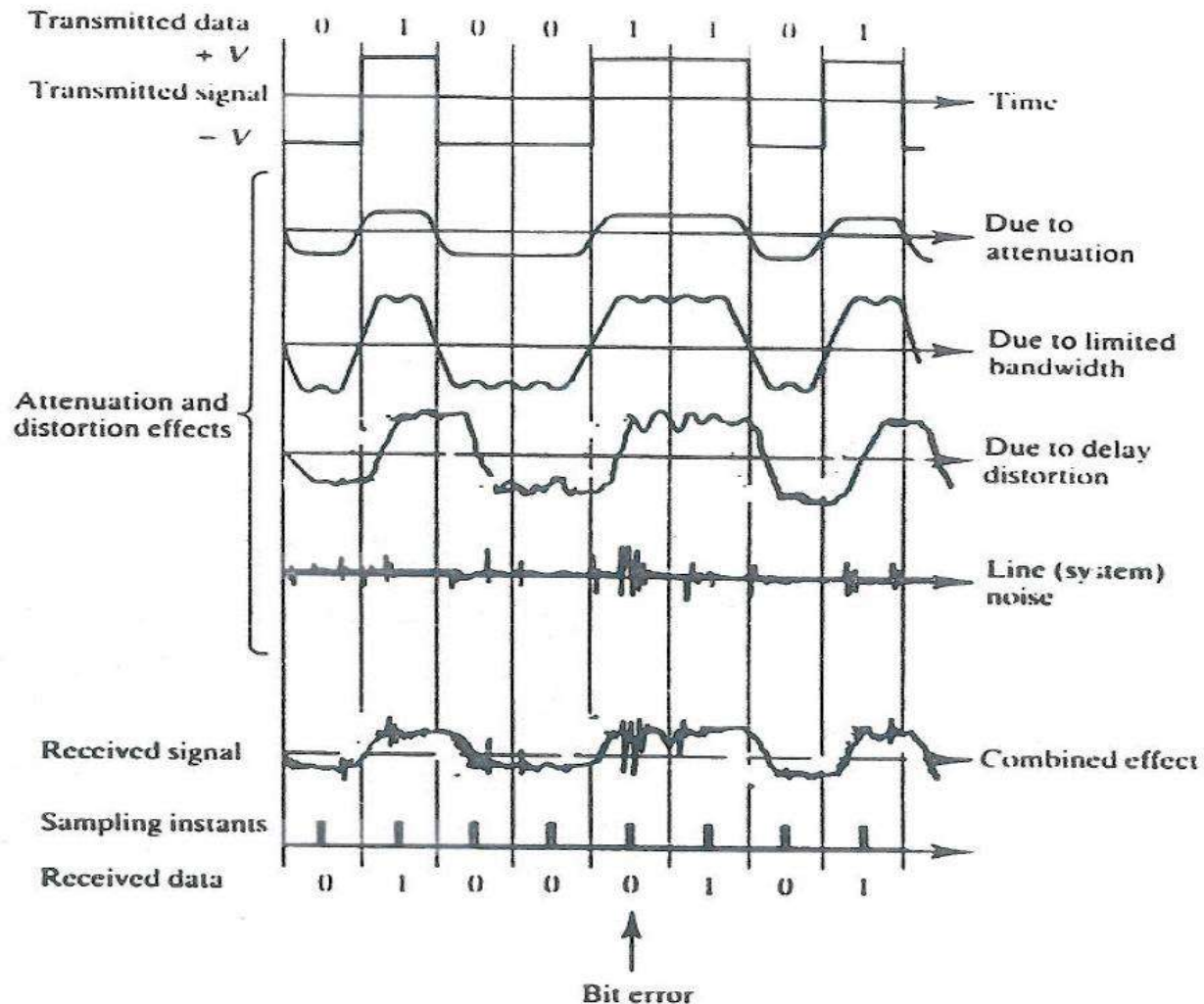
Figure 2-5

A digital waveform with noise so great that you can no longer recognize the original waveform



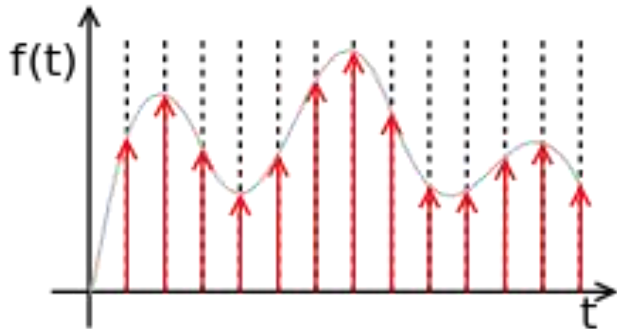
Signal distortion and bit error

8

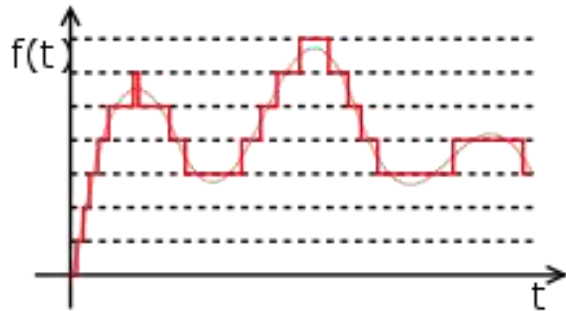


Quantization

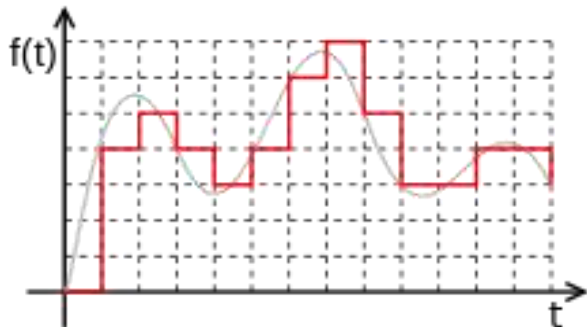
9



Sampled signal (discrete signal): discrete time, continuous values.



Quantized signal: continuous time, discrete values.



Digital signal (sampled, quantized): discrete time, discrete values.

Open Systems Interconnect (OSI) Vs TCP/IP

10

OSI 7 layer model

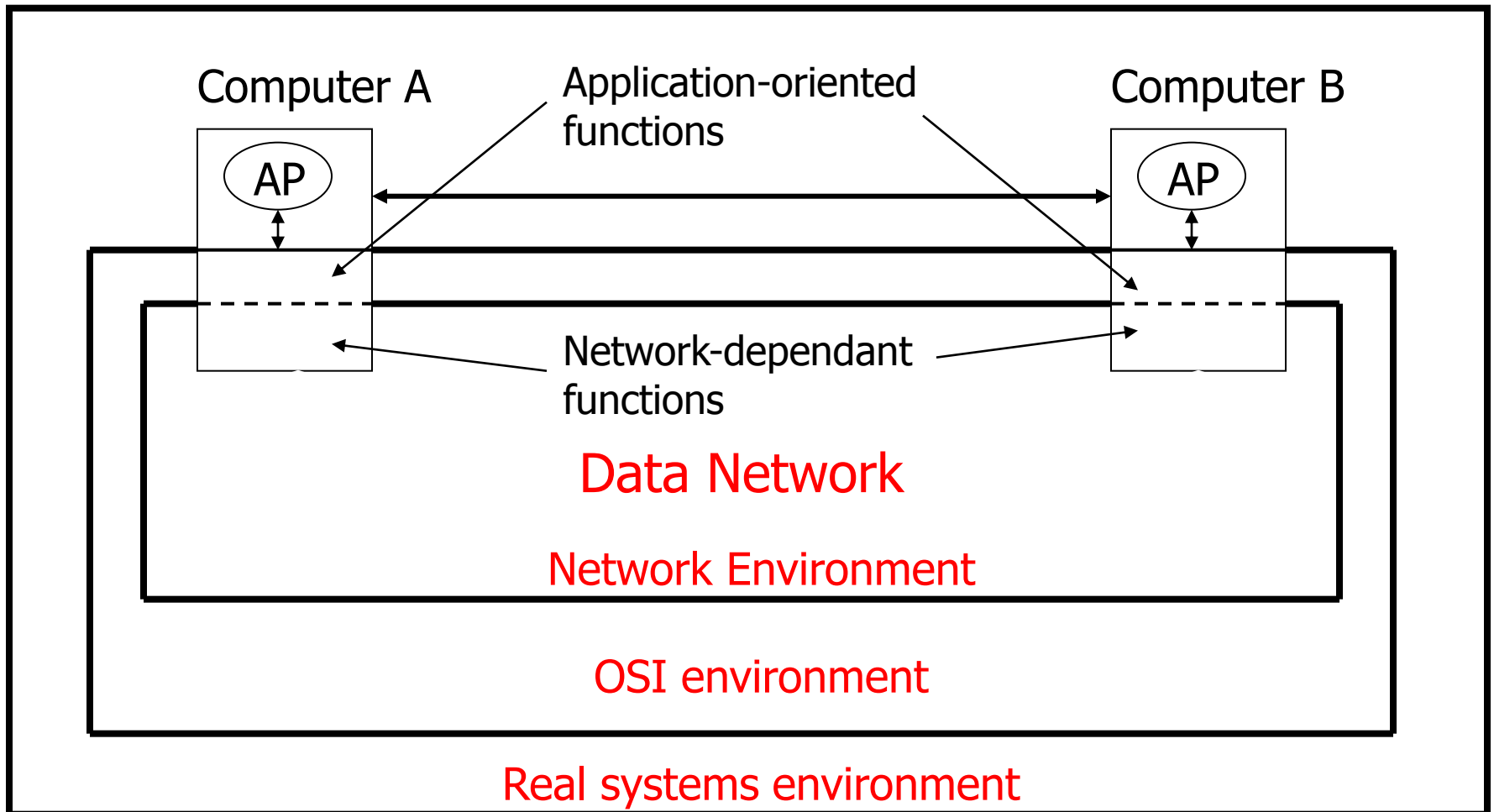
Application	Application Layers
Presentation	
Session	
Transport	Data Flow Layers
Network	
Data Link	
Physical	

TCP/IP model

Application	Protocols
Transport	
Internet	Networks
Network Access	

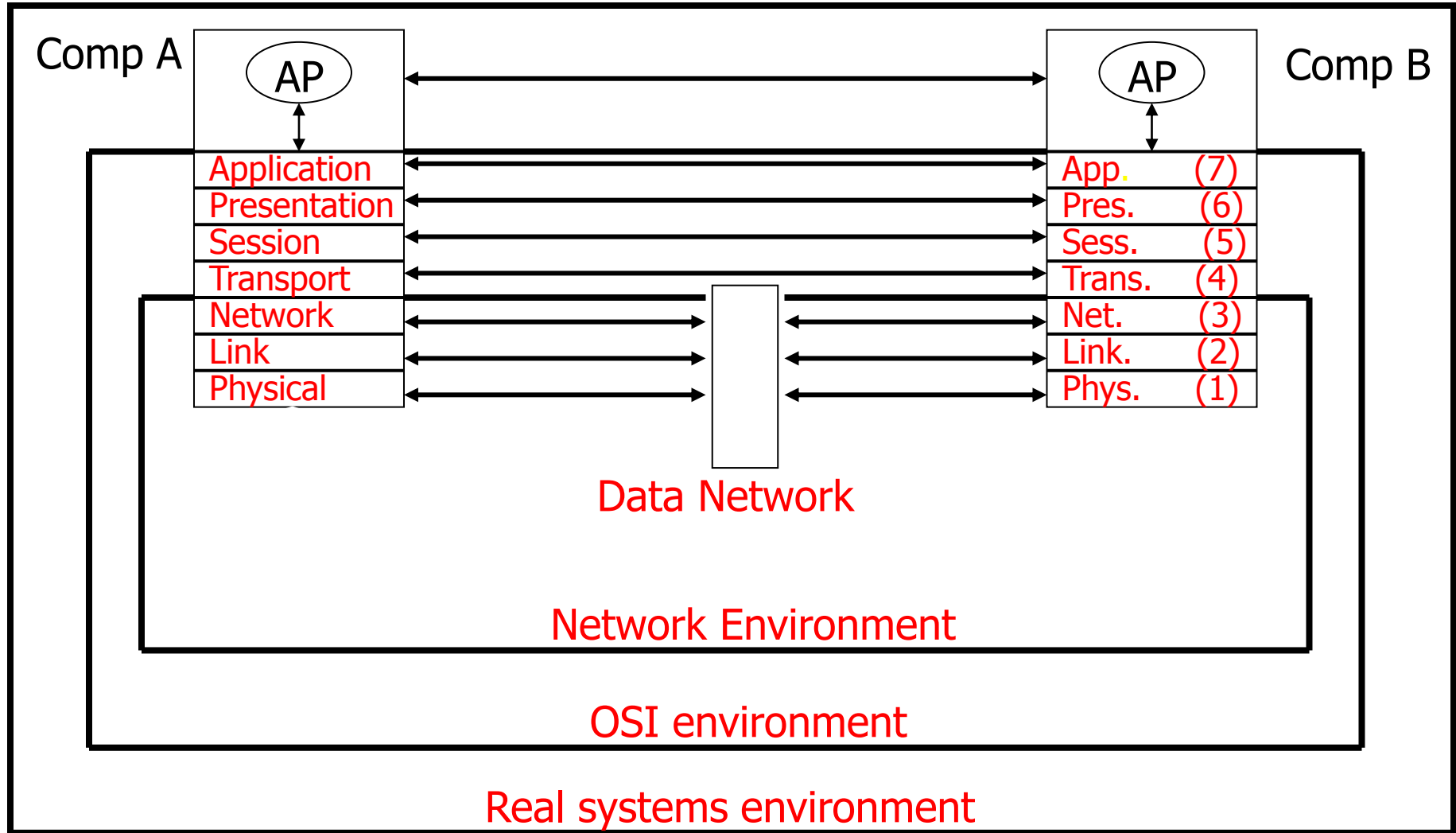
ISO basic model

11



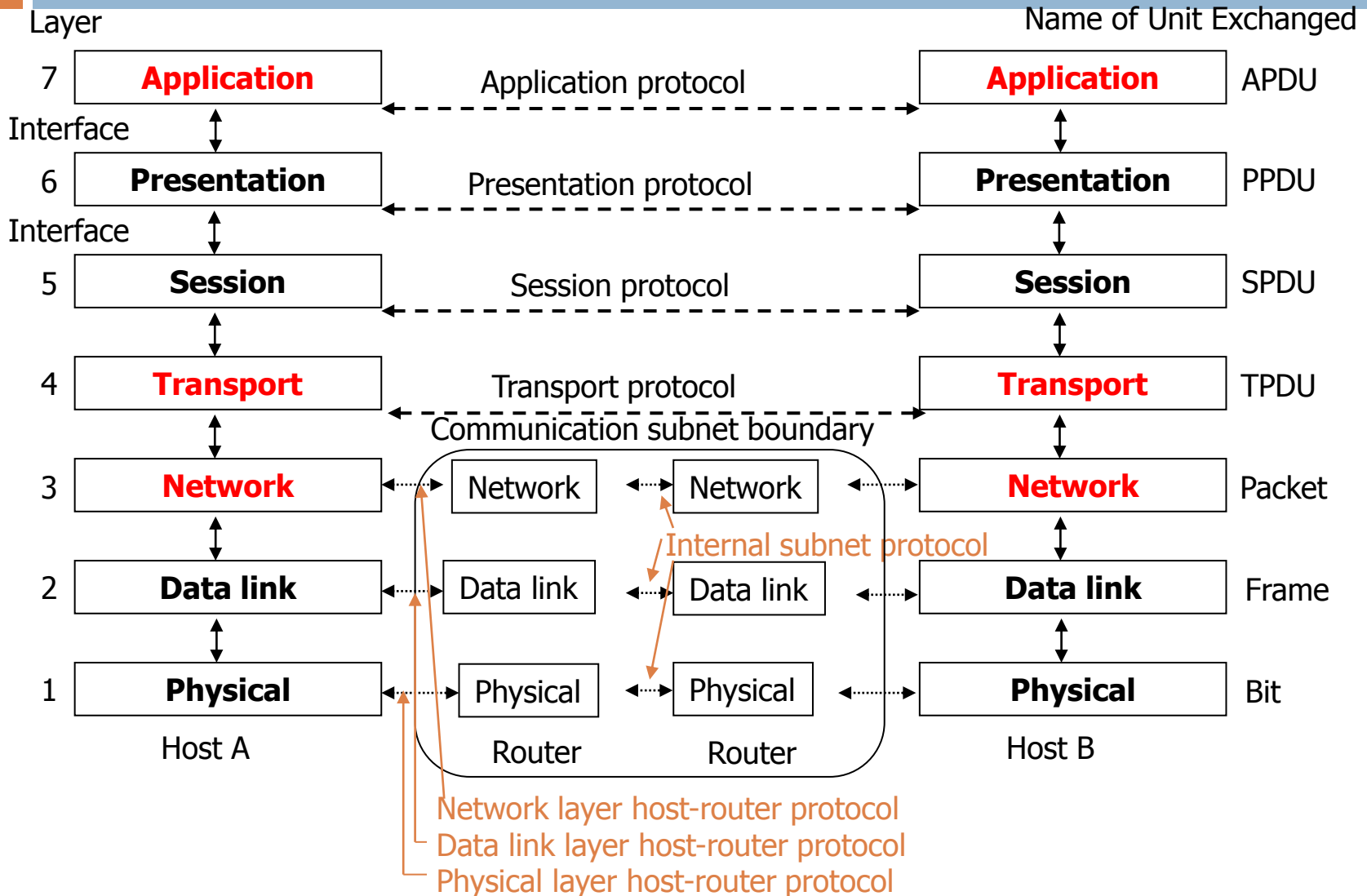
ISO 7 layer model

12



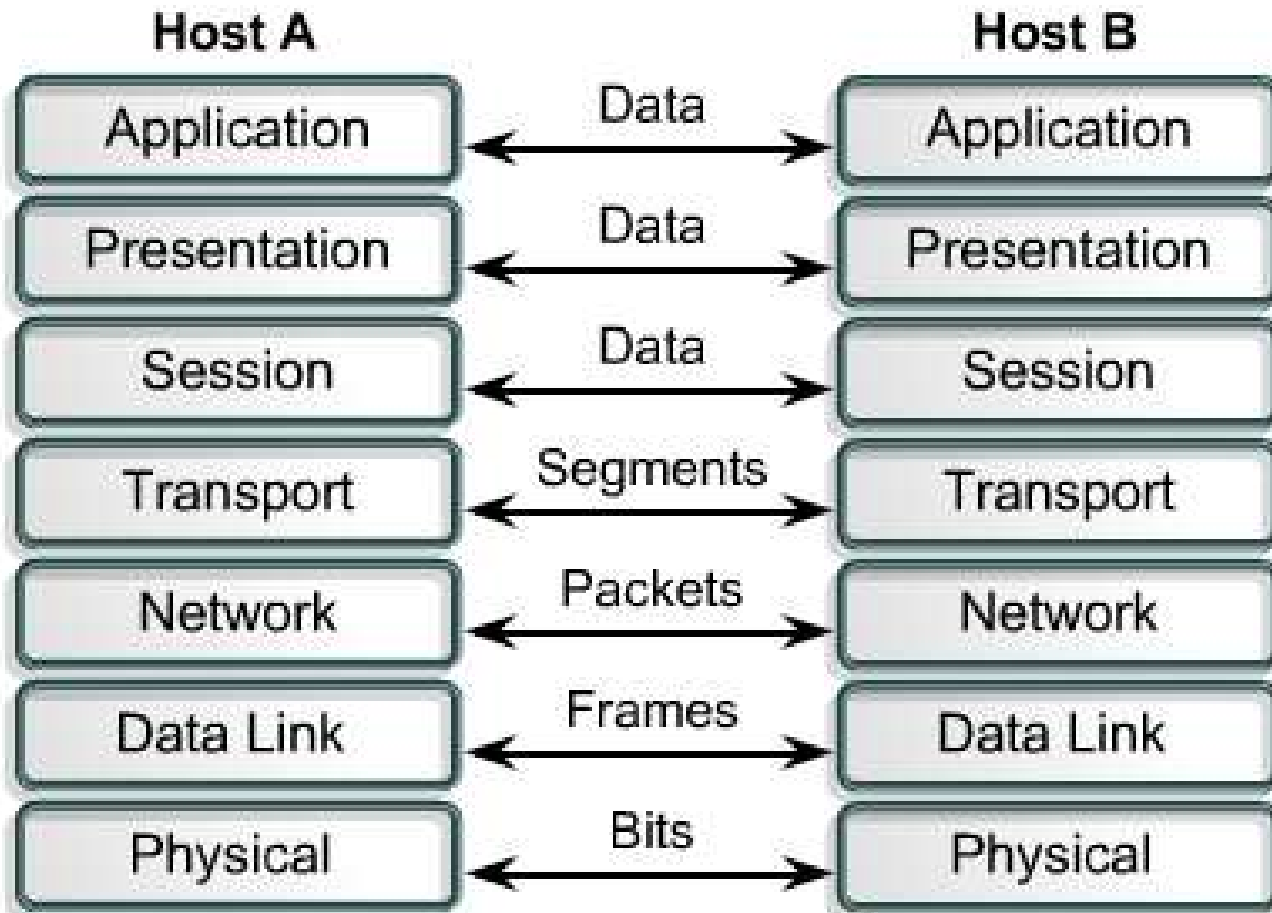
The OSI Reference Model

13



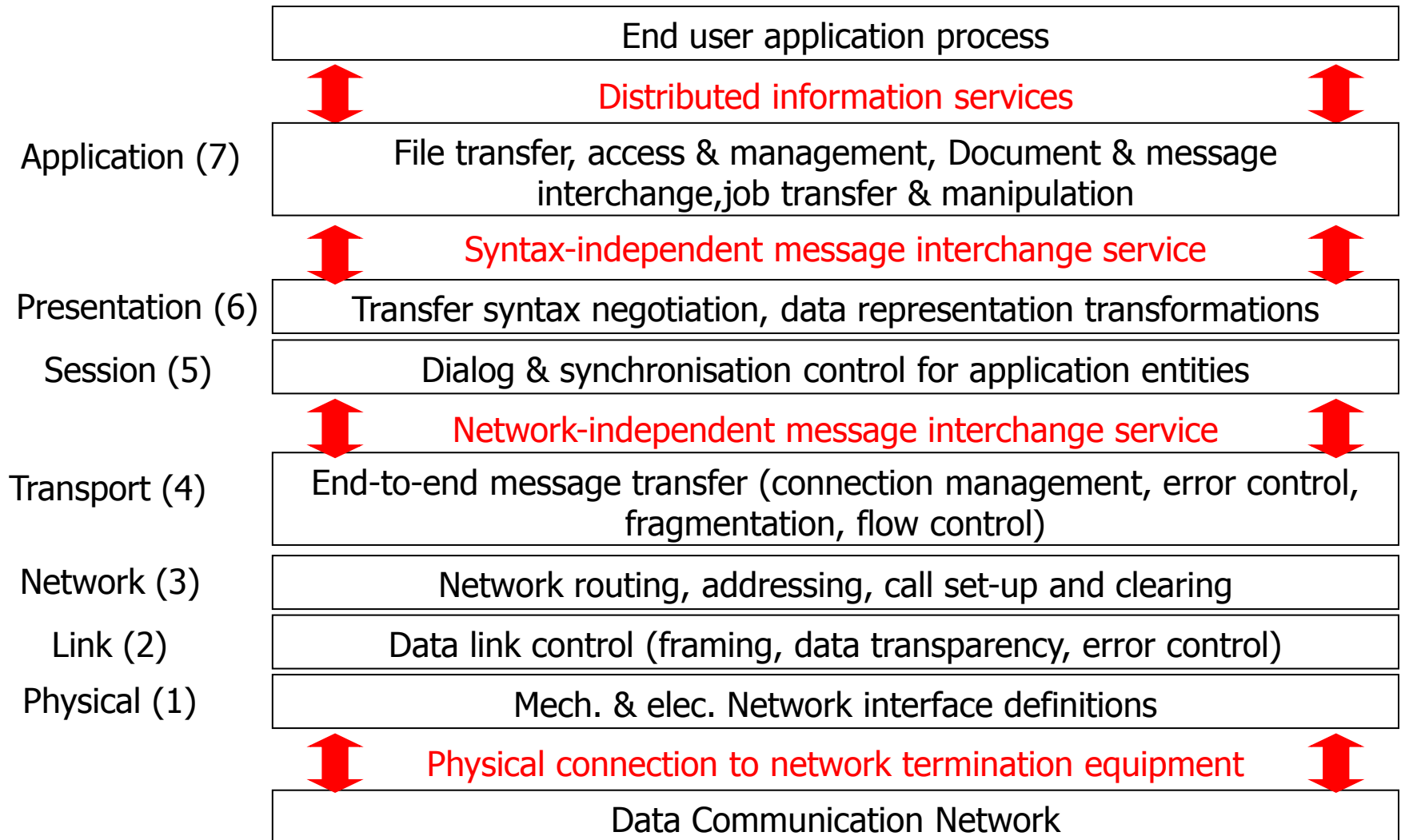
Encapsulation

14



Protocol layer overview

15



7 Layer model summary

16

Application	FTP, TFTP, HTTP, SMTP, DNS, TELNET, SNMP
Presentation	
Session	
Transport	TCP (the internet)
Network	IP (the internet)
Data Link	Ethernet (common LAN technology)
Physical	

The OSI Model

17

- Application layer - where the application using the network resides
 - ▣ Common network applications include remote login, file transfer, e-mail, and web page browsing
- Presentation layer - performs series of miscellaneous functions necessary for presenting the data package properly to the sender or receiver

The OSI Model

18

- Session layer - responsible for establishing sessions between users
- Transport layer - provides end-to-end error-free network connection
 - ▣ Makes sure data arrives at destination exactly as it left the source
- Network layer - responsible for creating, maintaining and ending network connections
 - ▣ Transfers a data packet from node to node within the network

The OSI Model

19

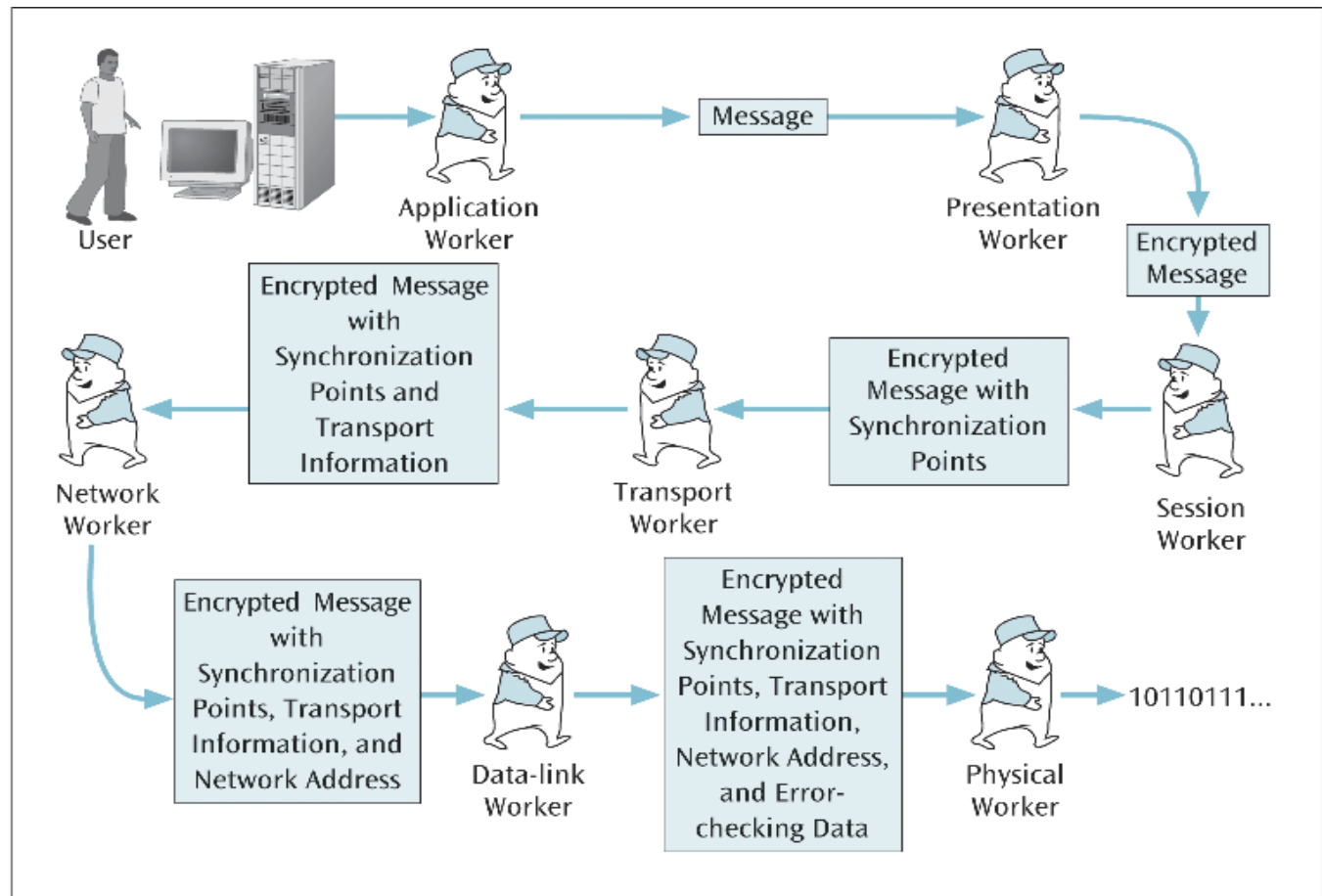
- Data link layer - responsible for taking data and transforming it into a frame with header, control and address information, as well as error detection code
- Physical layer - handles the transmission of bits over a communications channel
 - Includes voltage levels, connectors, media choice, modulation techniques

The OSI Model

20

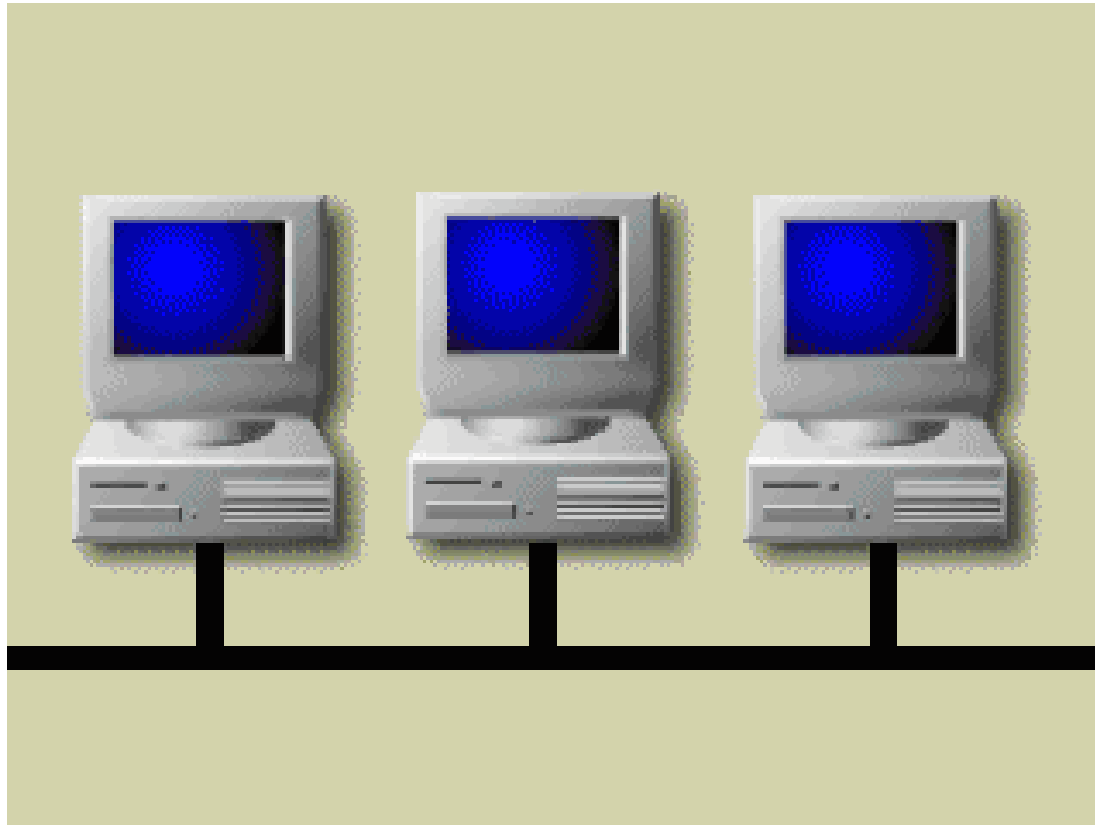
Figure 1-13

Network workers perform their job duties at each layer in the model



7 Layer protocol

21



7 layer operation

22

7. APPLICATION LAYER

6. PRESENTATION LAYER

5. SESSION LAYER

4. TRANSPORT LAYER

3. NETWORK LAYER

2. DATA LINK LAYER

1. PHYSICAL LAYER

What is TCP/IP?

23

- ❑ Industry standard suite of Protocols
- ❑ Routable enterprise networking protocol
- ❑ Technology for connecting dissimilar systems
- ❑ Robust, scaleable, cross-platform client/server framework
- ❑ Method for gaining access to the internet

Transmission Control Protocol (TCP)

24

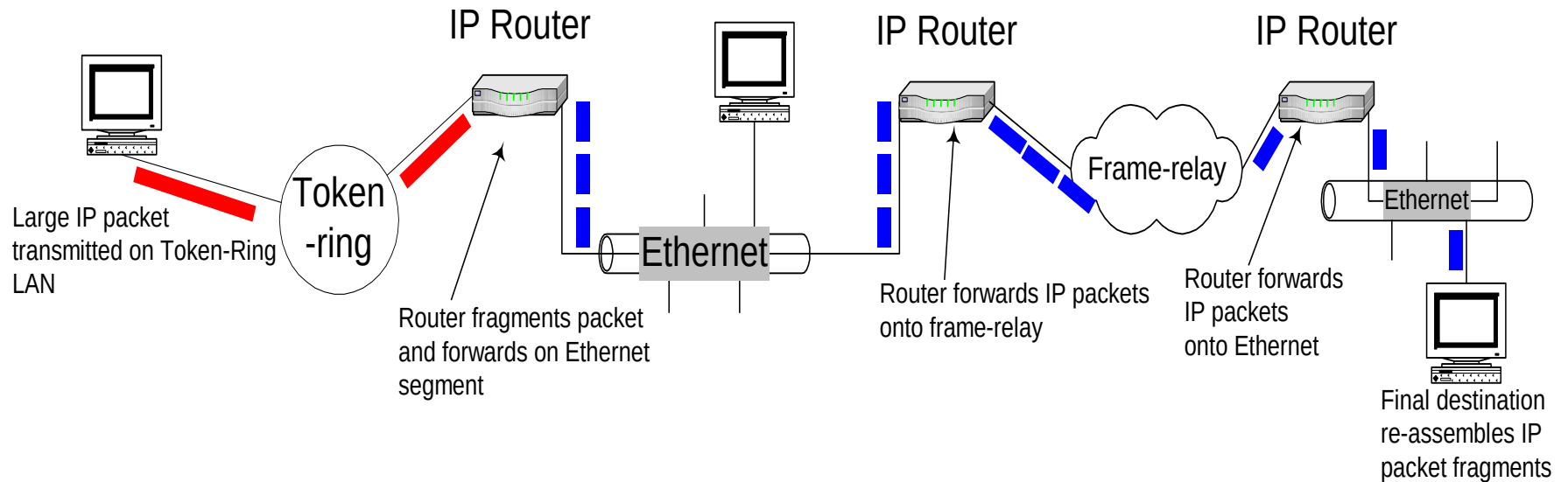
□ Service

- Guarantees end to end delivery of packets, re-sends anything not received
- Controls the flow of data from host to host and host into the network
- Multiplexing, the TCP header has a port number which is used to determine which application should receive the packet
- Connection-orientated, reliable
- Divides outgoing messages into segments, reassembles at destination

IP network

25

- The Internet protocol (IP) is not dependent on any particular hardware and is ideally suited to integrate LANs and WANs into 1 network



IP (Internet Protocol)

26

□ Service

- responsible for moving packets from source to destination across the network
 - fragmentation and re-assembly of packets across small packet sub-nets
- ## □ IP is a Datagram protocol, it does not
- guarantee delivery
 - guarantee sequence of delivery
 - control flow of packets into network

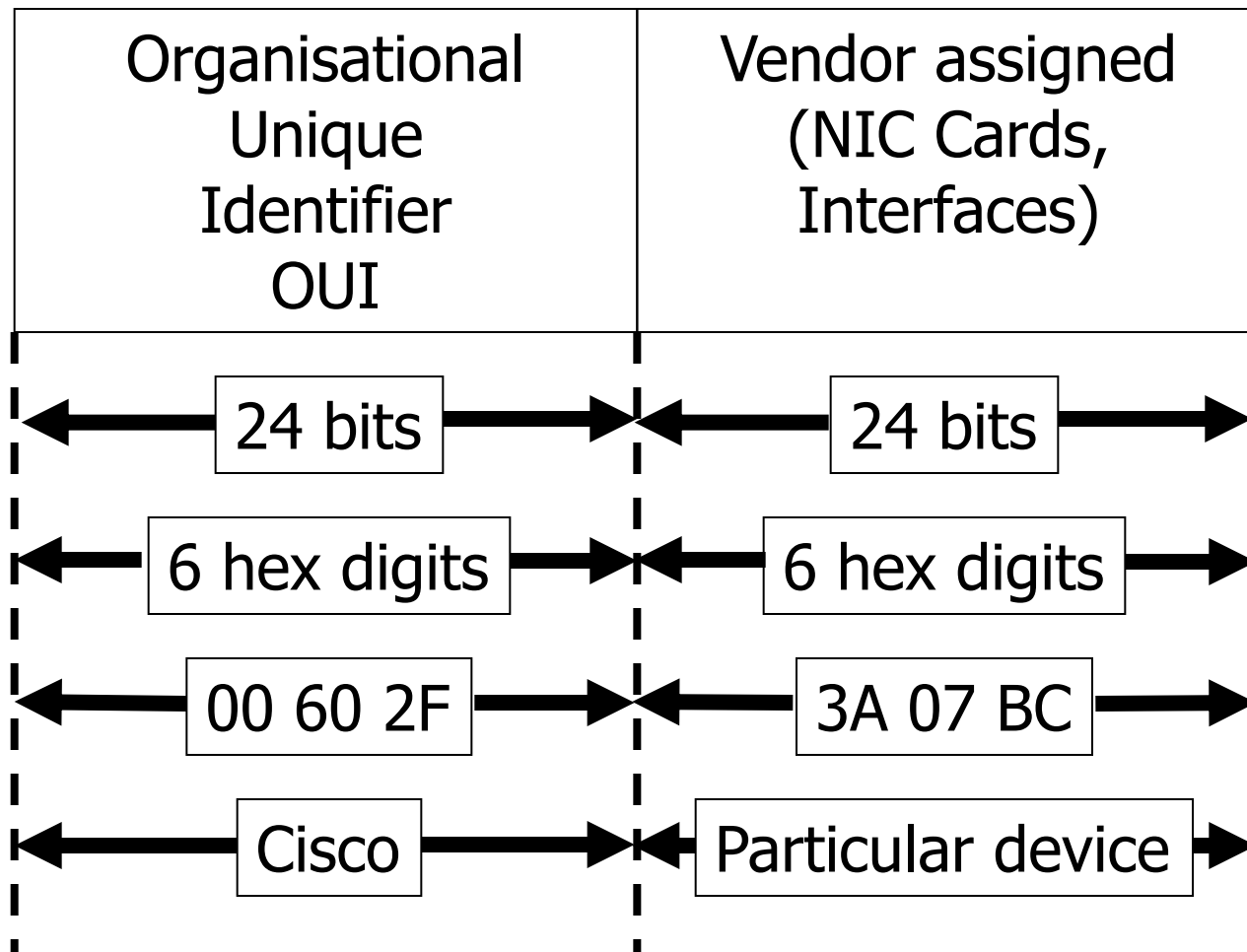
MAC Addressing

27

- ❑ Without a name computers cannot be accessed
- ❑ At the data link layer, a header, and possibly a trailer, is added to upper layer data.
- ❑ Header and trailer contain control information intended for the data link layer entity in the destination system.
- ❑ Data from upper layer entities is encapsulated in the data link layer header and trailer.

MAC Address

28



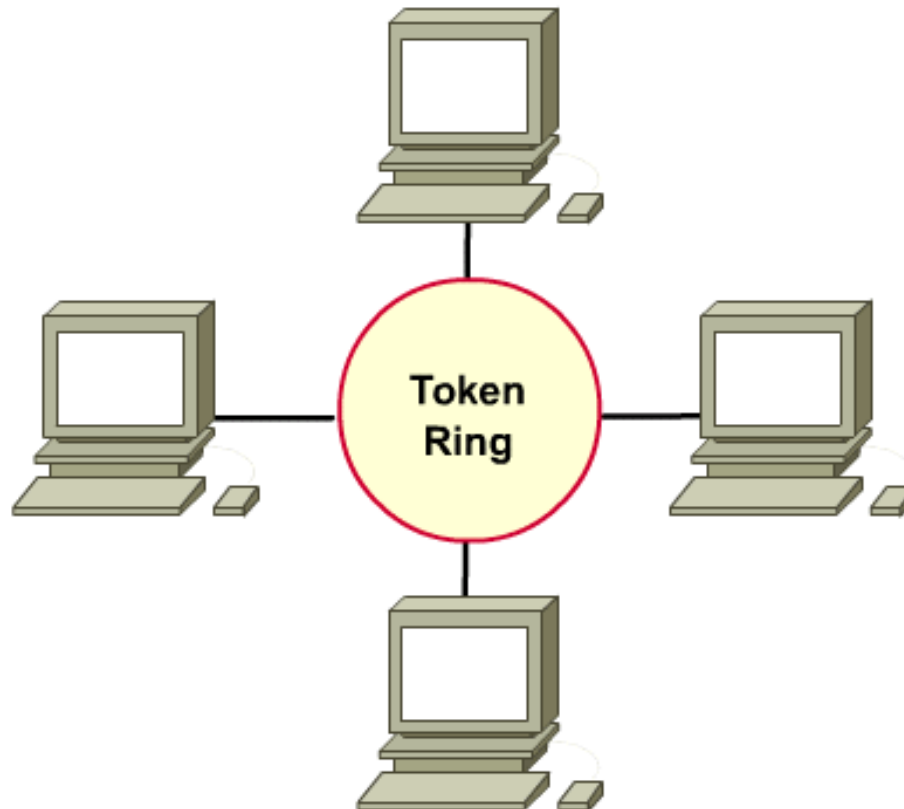
Flat structure

29

- ❑ MAC addresses provide a way for computers to identify themselves.
- ❑ They give hosts a permanent, unique name.
- ❑ The number of possible addresses is extremely large 2^{48} (over 2 trillion!) possible MAC addresses.
- ❑ One major disadvantage, they have no structure, and are considered flat address spaces.
- ❑ Different vendors have different OUIs, but they're like personal identification numbers.
- ❑ As your network grows to more than a few computers, this disadvantage becomes a real problem.

Deterministic MAC

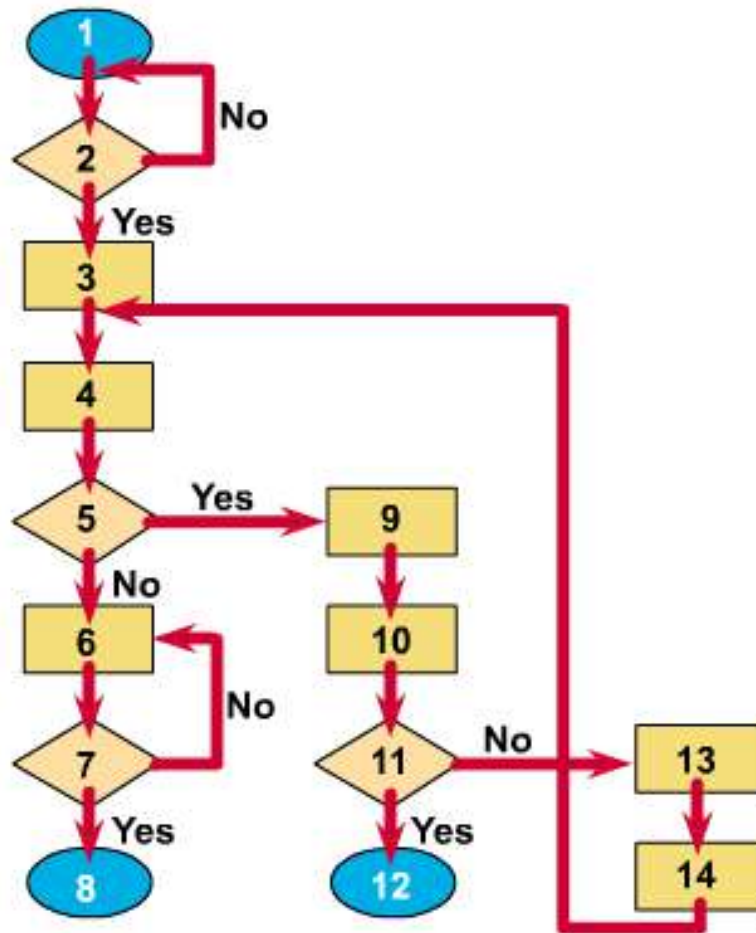
30



Non-Deterministic MAC

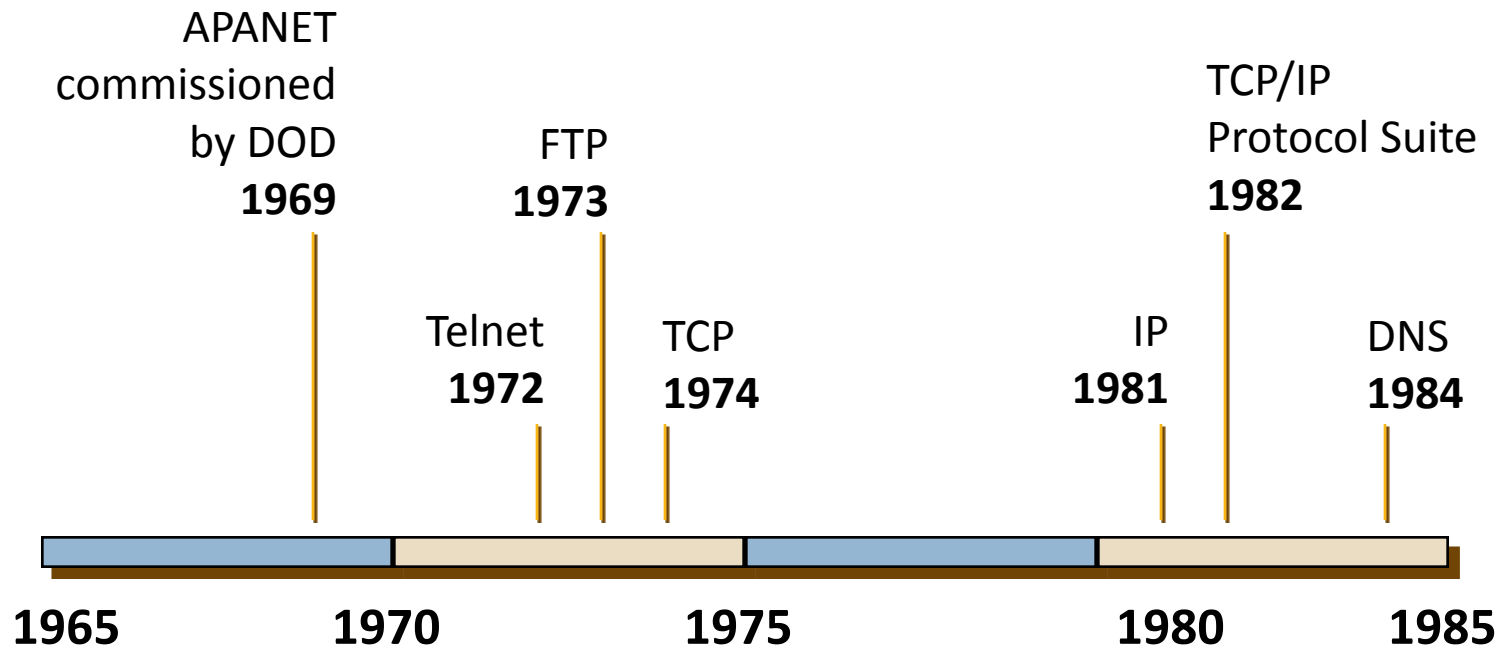
31

1. Host wants to transmit
2. Is carrier sensed?
3. Assemble frame
4. Start transmitting
5. Is a collision detected?
6. Keep transmitting
7. Is the transmission done?
8. Transmission completed
9. Broadcast jam signal
10. $\text{attempts} = \text{attempts} + 1$
11. $\text{attempts} > \text{too many?}$
12. Too many collisions;
abort transmission
13. Algorithm calculates backoff
14. Wait for t seconds



TCP/IP development

32



TCP/IP Utilities

33

FTP

TFTP

RCP

Telnet

RSH

REXEC

LPR

LPQ

LPD

PING

IPCONFIG

NSLOOKUP

HOSTNAME

NETSTAT

NBTSTAT

ROUTE

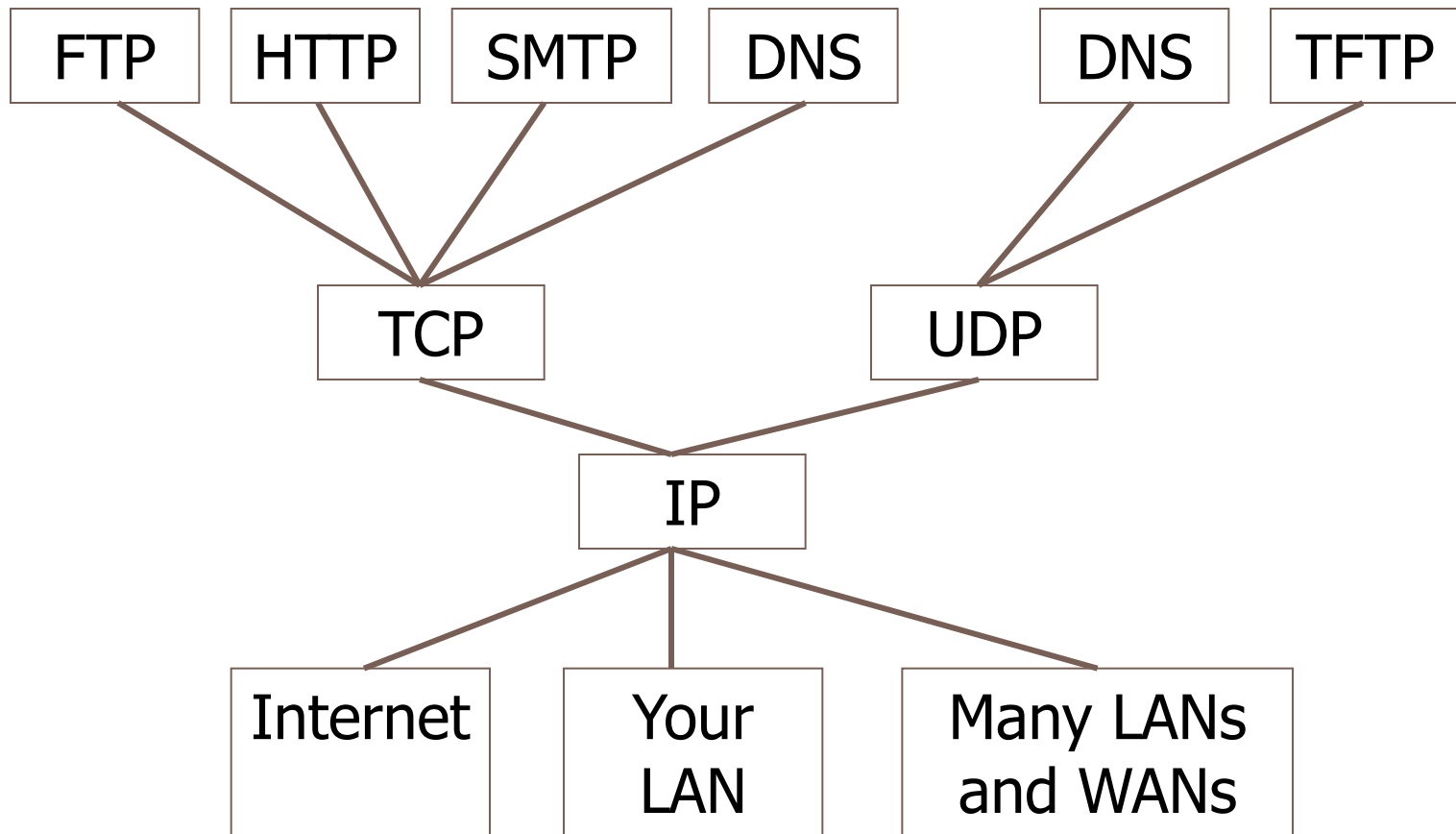
TRACERT

ARP

Finger

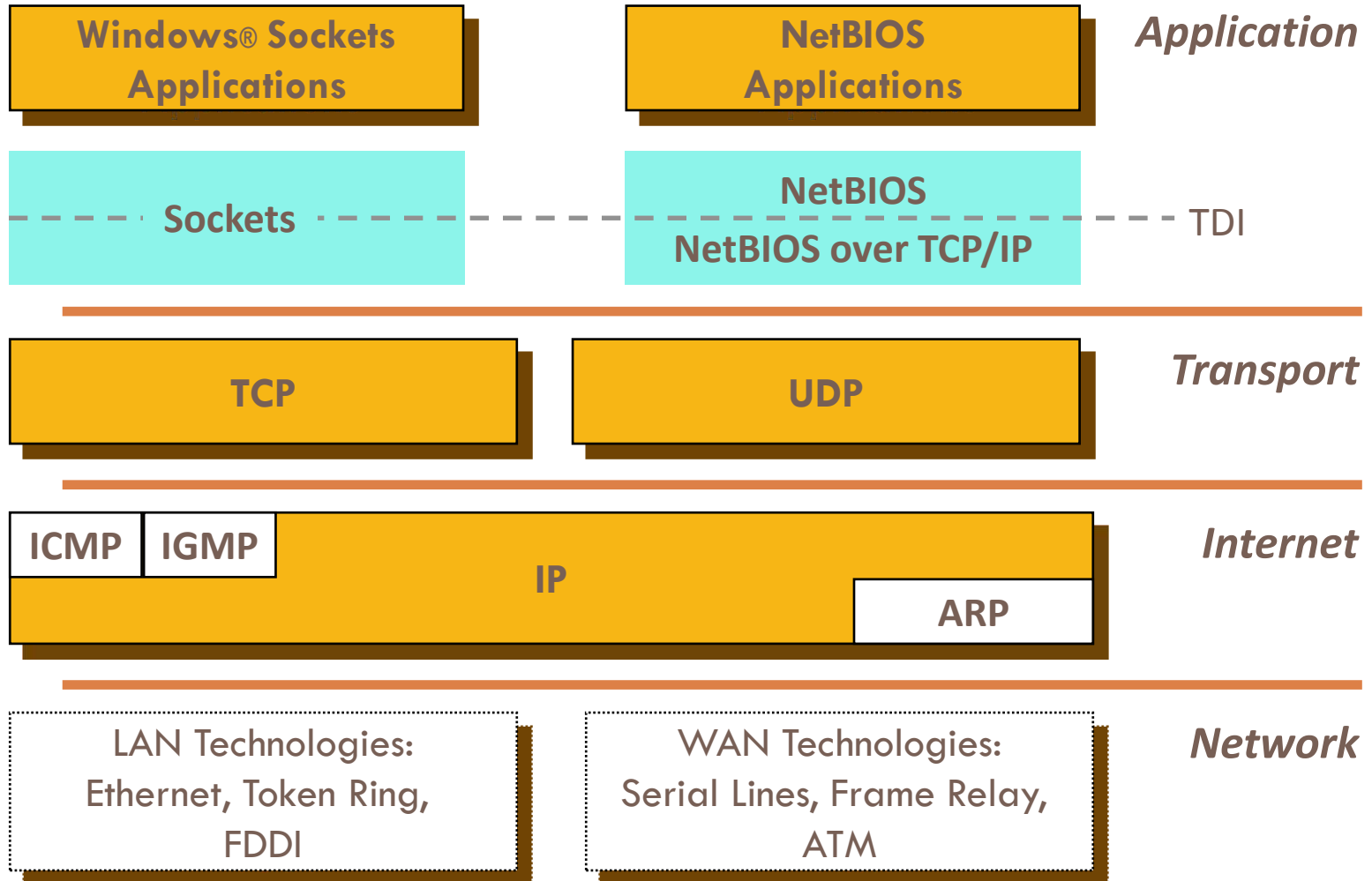
Protocol Graph

34



TCP/IP protocol suite

35

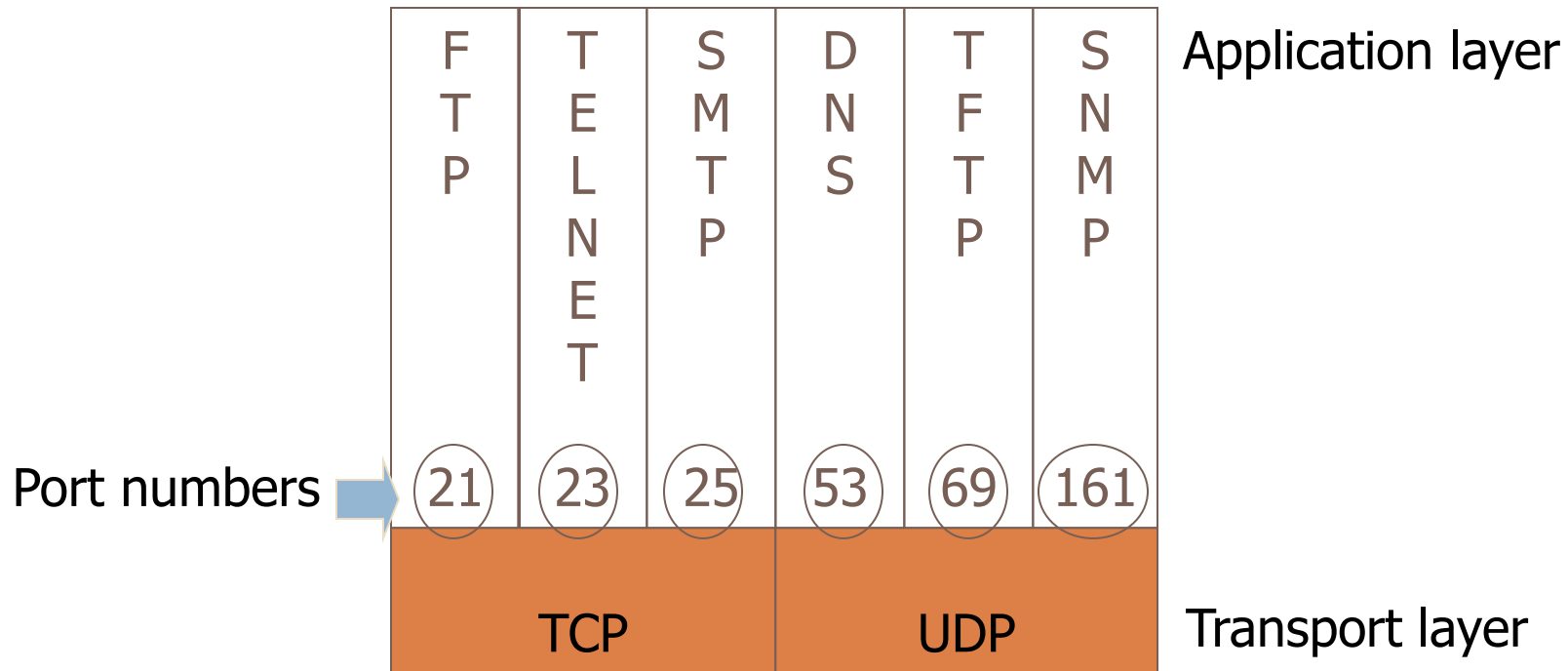


36

Source Port				Destination Port				
Sequence number								
Acknowldgment number								
TCP header length	reserved	URG	ACK	PUSH	RESET	SYN	FIN	Window Size
Checksum				Urgent Pointer				
Options								
Data								

Protocols & port numbers

37



TCP client ports

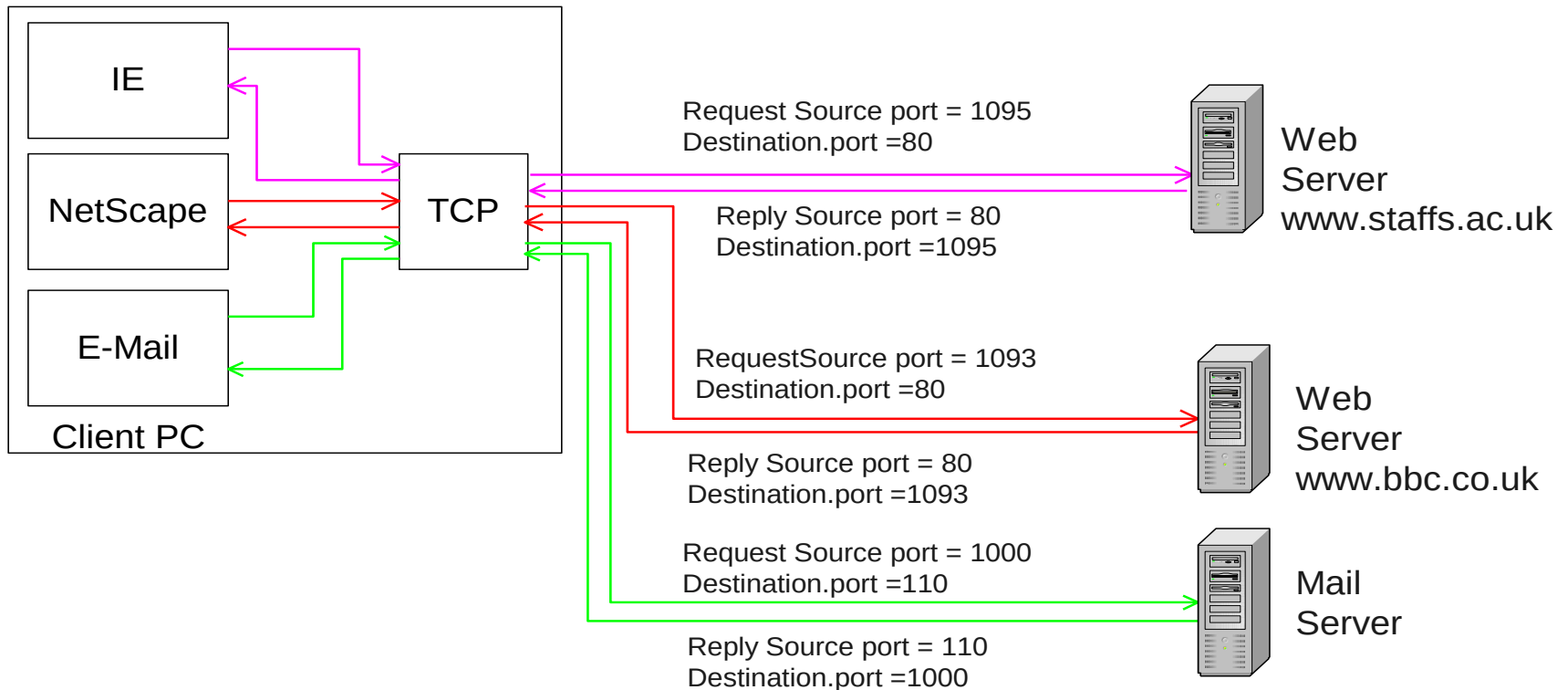
38

- Q. If you have a computer running an e-mail package, 2 web browsers (Netscape and IE) how does the computer know, when a TCP/IP packet arrives which application should receive the packet ?
- A. Each application sets up its connection using a different port number, when the replies come back from the server the port number is used to send the packet to the correct connection.

TCP ports (cont.)

39

- Note : Each application is allocated a different port number by the TCP software



TCP server ports

40

- The server must respond to client requests
- Q. How does the client know which port to send its request to ?
- A. “Well known port numbers” are assigned to particular services.

Port no.	Protocol	Service
80	HTTP	Web Access
110	POP3	retrieving e-mail
25	SMTP	e-mail transfer

TCP Error control

41

- The acknowledgment and sequence number fields are used to guarantee delivery of packets to the destination.
- For each packet sent out an acknowledgment must be sent back.
- If no acknowledgment is sent back within a certain time the packet is sent again.
- Each new packet to be transmitted is allocated a new sequence no., the returning acknowledgment no. informs the sender of the next expected sequence no.
- The sequence no. is used to keep the packets in order.

TCP flow control

42

- The window size field is used by the receiver to control the flow of packets from the sender.
- If the receiver sets the window size to 400 the sender is only allowed to send 400 bytes before stopping.
- The receiver can stop the sender by setting the window size to 0.

UDP (User Datagram Protocol)

43

□ Service

- connectionless
- provides port allocations the same as TCP
- Unreliable, does NOT guarantee delivery
- does not guarantee sequencing
- useful when speed is more important than reliability e.g. Internet telephony
- Transmits messages called datagrams
- Does not reassemble incoming messages
- No flow control
- uses not acknowledgments

UDP segment format

44

# of bits	16	16	16	16	n
	Source Port	Destination Port	Length	Check Sum	Data...

IP network and host id.

45

- An example with Class A addressing
- First digit is network id , last 3 digits host id
- Note the routers use the network id to route the packets across the internet

