


A faint, light gray background pattern consisting of a network of interconnected nodes and lines, resembling a molecular structure or a network graph. The nodes are represented by circles of varying sizes, and the lines are thin and gray, connecting the nodes in a complex, non-linear fashion.

CHAPTER 17 - NETWORK AND DISTRIBUTED SYSTEMS

OBJECTIVES

- Provide a high-level overview of distributed systems and the networks that interconnect them
- Discuss the general structure of distributed operating systems
- Explain general communication structure and communication protocols

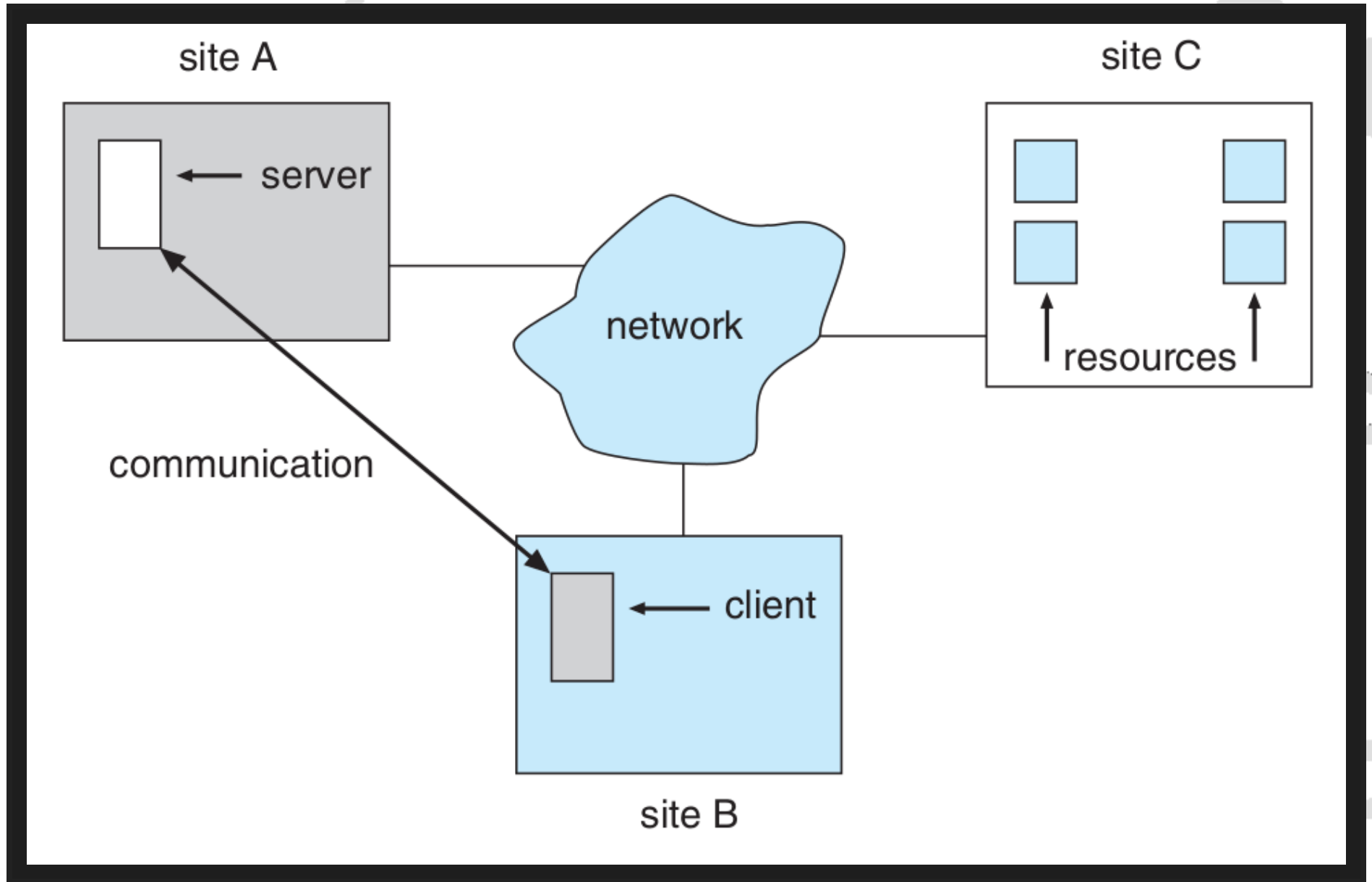
A background network diagram consisting of numerous gray circles of varying sizes connected by thin gray lines, forming a complex, interconnected web that symbolizes a distributed system.

ADVANTAGES OF DISTRIBUTED SYSTEMS

OVERVIEW

- **Distributed system** is collection of loosely coupled processors interconnected by a communications network
- Processors variously called **nodes**, **computers**, **machines**, **hosts**
 - **Site** is location of the processor
 - Generally a **server** has a resource a **client** node at a different site wants to use

OVERVIEW



REASONS FOR DISTRIBUTED SYSTEMS

- **Resource sharing**
 - Sharing and printing files at remote sites
 - Shared compute power (Super computer)
 - Processing information in a distributed database
 - Using remote specialized hardware devices

REASONS FOR DISTRIBUTED SYSTEMS

- **Computation speedup**
 - Run calculations in parallel at different sites
 - load sharing or job migration

REASONS FOR DISTRIBUTED SYSTEMS

- **Reliability**
 - detect and recover from site failure, function transfer, reintegrate failed site

REASONS FOR DISTRIBUTED SYSTEMS

- **Communication** – message passing
 - All higher-level functions of a standalone system can be expanded to encompass a distributed system
- Computers can be downsized, more flexibility, better user interfaces and easier maintenance by moving from large system to multiple smaller systems performing distributed computing

A background graphic consisting of a network of interconnected nodes and lines. The nodes are represented by circles of varying sizes, some solid and some hollow, connected by thin gray lines. The overall pattern is abstract and resembles a molecular structure or a network topology.

TYPES OF NETWORK-BASED OPERATING SYSTEMS

TYPES OF NETWORK-BASED OPERATING SYSTEMS

- Network Operating Systems
- Distributed Operating Systems

NETWORK OPERATING SYSTEMS

- Users are aware of multiplicity of machines
- Access to resources of various machines is done explicitly by:
 - Remote logging into the appropriate remote machine
 - Remote Desktop (Microsoft Windows)
 - Transferring data from remote machines to local machines, via FTP mechanism
- Users must change paradigms – establish a **session**, give network-based commands

DISTRIBUTED-OPERATING SYSTEMS

- Users not aware of multiplicity of machines
 - Access to remote resources similar to access to local resources
- **Data Migration** – transfer data by transferring entire file, or transferring only those portions of the file necessary for the immediate task
- **Computation Migration** – transfer the computation, rather than the data, across the system
 - Via remote procedure calls (RPCs) or via messaging system

PROCESS MIGRATION

- **Load balancing** – distribute processes across network to even the workload
- **Computation speedup** – subprocesses can run concurrently on different sites
- **Hardware preference** – process execution may require specialized processor
- **Software preference** – required software may be available at only a particular site
- **Data access** – run process remotely, rather than transfer all data locally

A background network diagram consisting of various nodes (circles) of different sizes and colors (white, gray, black) connected by lines, forming a complex web structure. The nodes are distributed across the entire slide, with some clusters and some isolated nodes.

NETWORK STRUCTURE

A background graphic consisting of a network of interconnected nodes and lines. The nodes are represented by circles of varying sizes, some solid and some hollow, connected by thin gray lines. The overall pattern is abstract and resembles a molecular structure or a network topology.

NETWORK STRUCTURE

- Local-area networks (LAN)
- Wide-area networks (WAN)

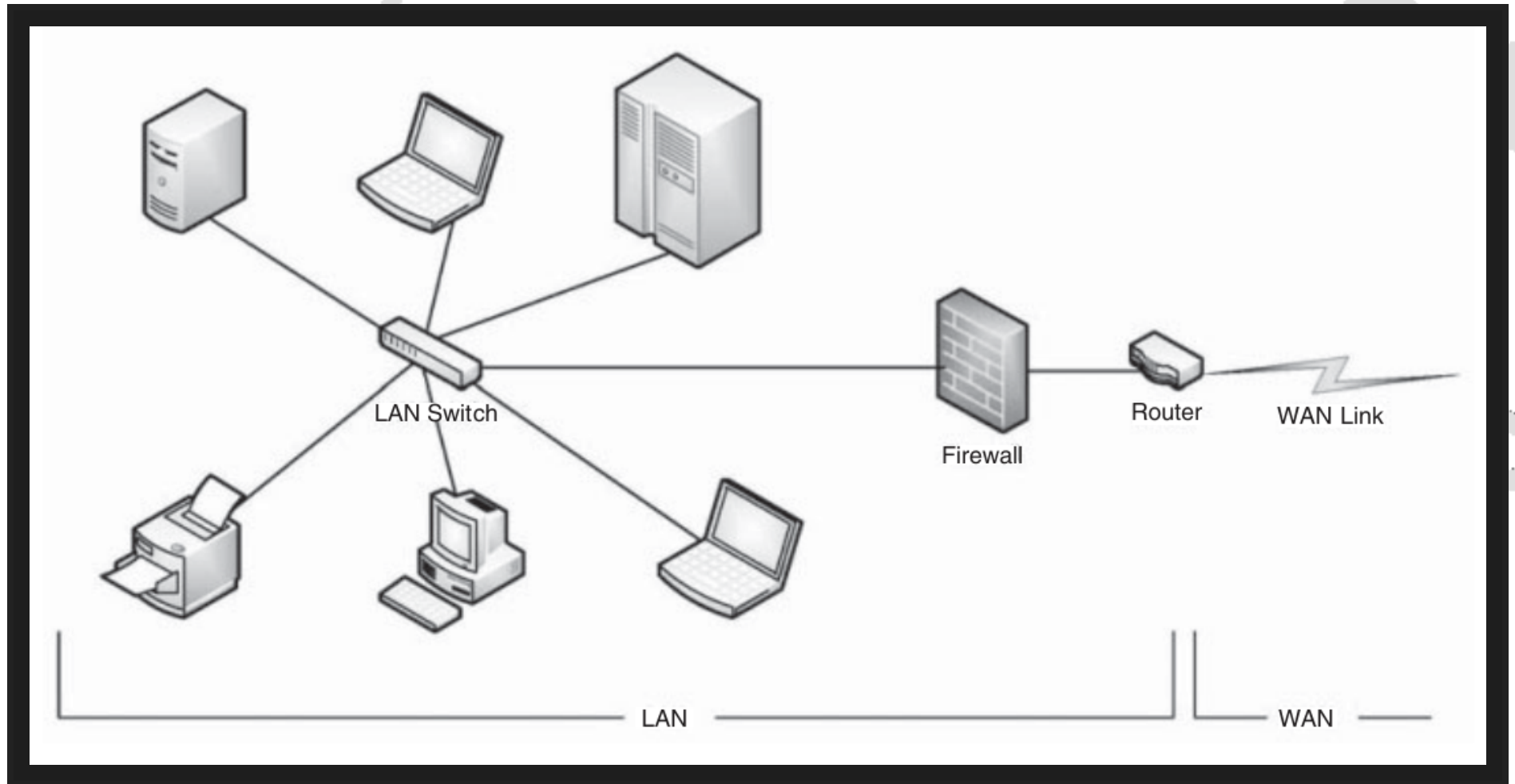
LOCAL-AREA NETWORK

- Designed to cover small geographical area
 - Multiple topologies like star or ring
 - Speeds from 1Mb per second (Appletalk, bluetooth) to 40 Gbps for fastest Ethernet over twisted pair copper or optical fibre
 - Consists of multiple computers (mainframes through mobile devices), peripherals (printers, storage arrays), routers (specialized network communication processors) providing access to other networks

LOCAL-AREA NETWORK

- Ethernet most common way to construct LANs
 - Multiaccess bus-based
 - Defined by standard IEEE 802.3
 - Wireless spectrum (WiFi) increasingly used for networking
- I.e. IEEE 802.11g standard implemented at 54 Mbps

LOCAL-AREA NETWORK



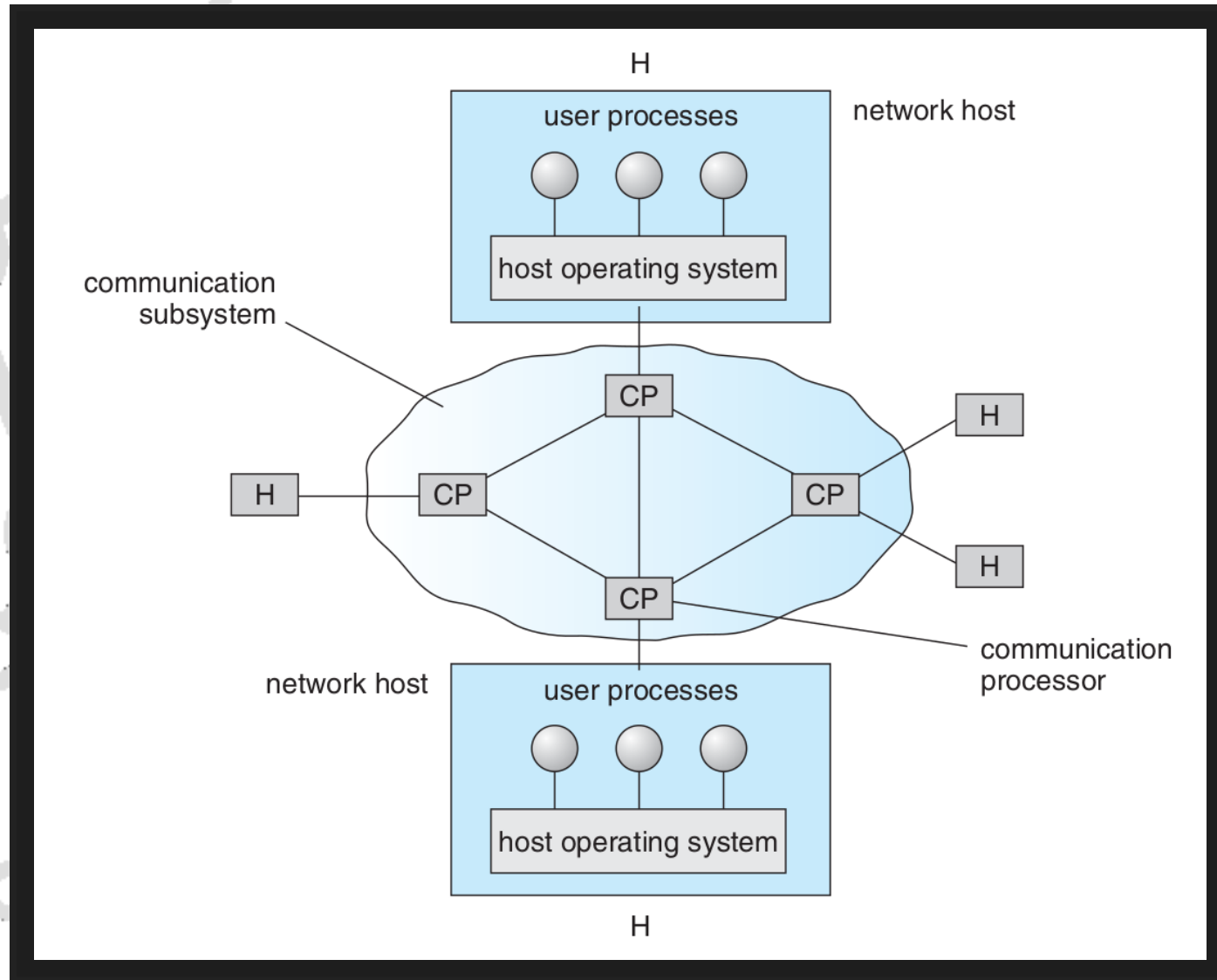
WIDE-AREA NETWORKS

- Links geographically separated sites
 - Point-to-point connections over long-haul lines (often leased from a phone company)
 - Implemented via connection processors known as routers
 - Internet WAN enables hosts world wide to communicate
 - Hosts differ in all dimensions but WAN allows communications

WIDE-AREA NETWORKS

- Speeds
 - T1 link is 1.544 Megabits per second
 - T3 is $28 \times \text{T1s} = 45 \text{ Mbps}$
 - OC-12 is 622 Mbps
- WANs and LANs interconnect, similar to cell phone network:
 - Cell phones use radio waves to cell towers
 - Towers connect to other towers and hubs

WIDE-AREA NETWORKS



A background network diagram consisting of various sized gray circles (nodes) connected by thin gray lines (edges). The nodes are distributed across the slide, with some forming small clusters and others being isolated. The overall pattern suggests a complex, interconnected communication structure.

COMMUNICATION STRUCTURE

COMMUNICATION STRUCTURE

The design of a communication network must address four basic issues:

- **Naming and name resolution** - How do two processes locate each other to communicate?
- **Routing strategies** - How are messages sent through the network?
- **Connection strategies** - How do two processes send a sequence of messages?
- **Contention** - The network is a shared resource, so how do we resolve conflicting demands for its use?

NAMING AND NAME RESOLUTION

- Name systems in the network
- Address messages with the process-id
- Identify processes on remote systems by `<host - name, identifier>` pair
- **Domain name system (DNS)** – specifies the naming structure of the hosts, as well as name to address resolution (Internet)

ROUTING STRATEGIES

A faint, light gray background network diagram consisting of numerous circular nodes of varying sizes connected by thin lines, forming a complex web-like structure.

- Fixed routing
- Virtual routing
- Dynamic routing

FIXED ROUTING

- A path from A to B is specified in advance; path changes only if a hardware failure disables it
 - Since the shortest path is usually chosen, communication costs are minimized
 - Fixed routing cannot adapt to load changes
 - Ensures that messages will be delivered in the order in which they were sent

VIRTUAL ROUTING

- A path from A to B is fixed for the duration of one session. Different sessions involving messages from A to B may have different paths
 - Partial remedy to adapting to load changes
 - Ensures that messages will be delivered in the order in which they were sent

DYNAMIC ROUTING

- The path used to send a message from site A to site B is chosen only when a message is sent
 - Usually a site sends a message to another site on the link least used at that particular time
 - Adapts to load changes by avoiding routing messages on heavily used path
 - Messages may arrive out of order
 - This problem can be remedied by appending a sequence number to each message
 - Most complex to set up

ROUTING STRATEGIES

- Tradeoffs mean all methods are used
- UNIX provides ability to mix fixed and dynamic
- Hosts may have fixed routes and gateways connecting networks together may have dynamic routes

ROUTING STRATEGIES

- **Router** is communications processor responsible for routing messages
- Must have at least 2 network connections
- Maybe special purpose or just function running on host
- Checks its tables to determine where destination host is, where to send messages
 - Static routing – table only changed manually
 - Dynamic routing – table changed via **routing protocol**

PACKET STRATEGIES

- Messages vary in length – simplified design breaks them into **packets** (or **frames**, or **datagrams**)
- **Connectionless message** is just one packet
 - Otherwise need a connection to get a multi-packet message from source to destination

CONNECTION STRATEGIES

- **Circuit switching** - A permanent physical link is established for the duration of the communication
- **Message switching** - A temporary link is established for the duration of one message transfer
- **Packet switching** - Messages of variable length are divided into fixed-length packets → sent to the destination
 - Each packet may take a different path through the network
 - The packets must be reassembled into messages as they arrive

CONNECTION STRATEGIES

- Circuit switching requires setup time, but incurs less overhead for shipping each message, and may waste network bandwidth
- Message and packet switching require less setup time, but incur more overhead per message

The background of the slide features a complex, abstract network diagram. It consists of numerous circular nodes of varying sizes, some solid and some hollow, connected by thin, light gray lines. These lines form a web-like structure that spans the entire page, with some clusters being denser than others. The overall effect is a sense of interconnectedness and data flow.

COMMUNICATION PROTOCOL

COMMUNICATION PROTOCOL

The communication network is partitioned into the following multiple layers:

- **Layer 1: Physical layer** – handles the mechanical and electrical details of the physical transmission of a bit stream
- **Layer 2: Data-link layer** – handles the frames, or fixed-length parts of packets, including any error detection and recovery that occurred in the physical layer

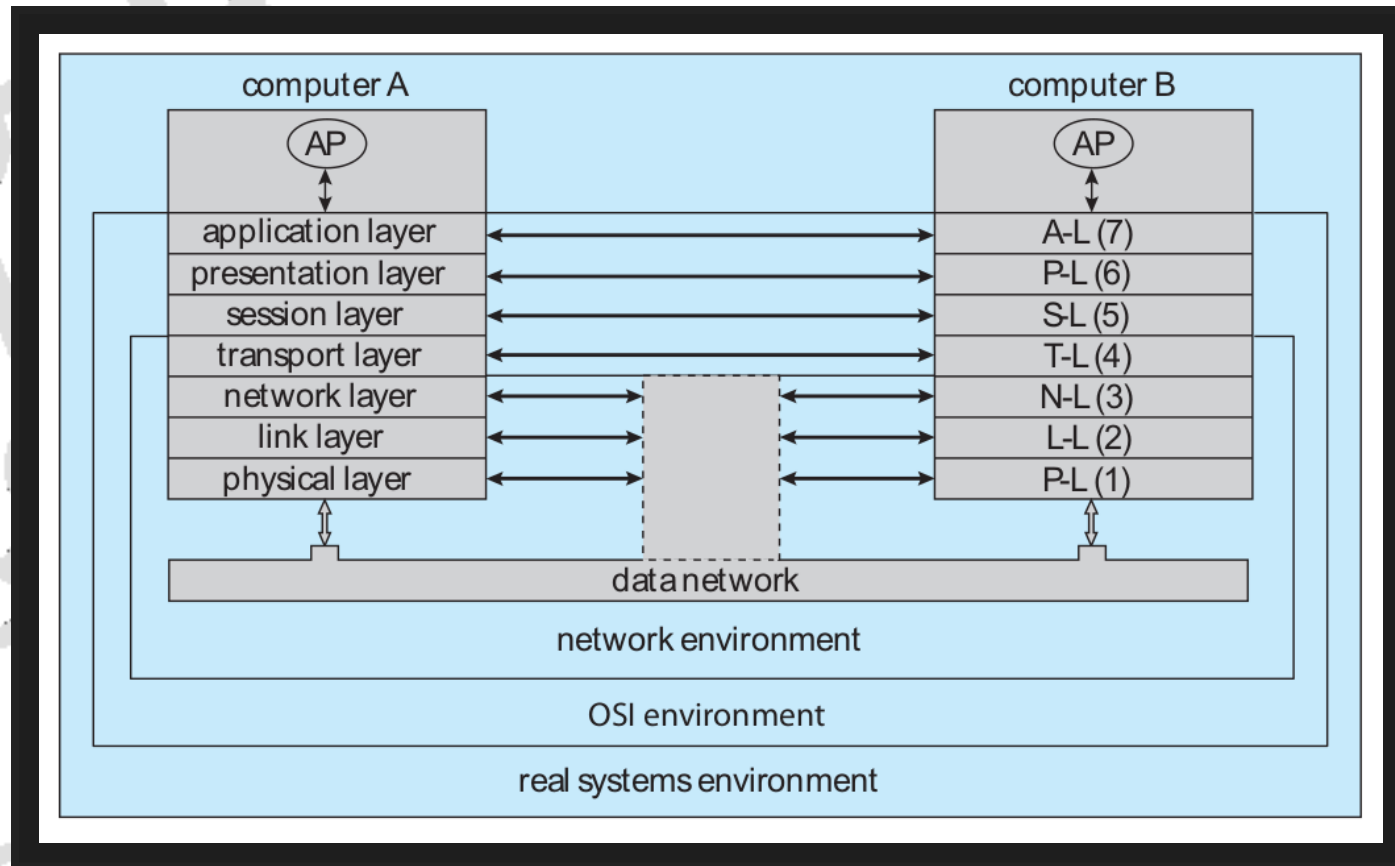
COMMUNICATION PROTOCOL

- **Layer 3: Network layer** – provides connections and routes packets in the communication network, including handling the address of outgoing packets, decoding the address of incoming packets, and maintaining routing information for proper response to changing load levels
- **Layer 4: Transport layer** – responsible for low-level network access and for message transfer between clients, including partitioning messages into packets, maintaining packet order, controlling flow, and generating physical addresses

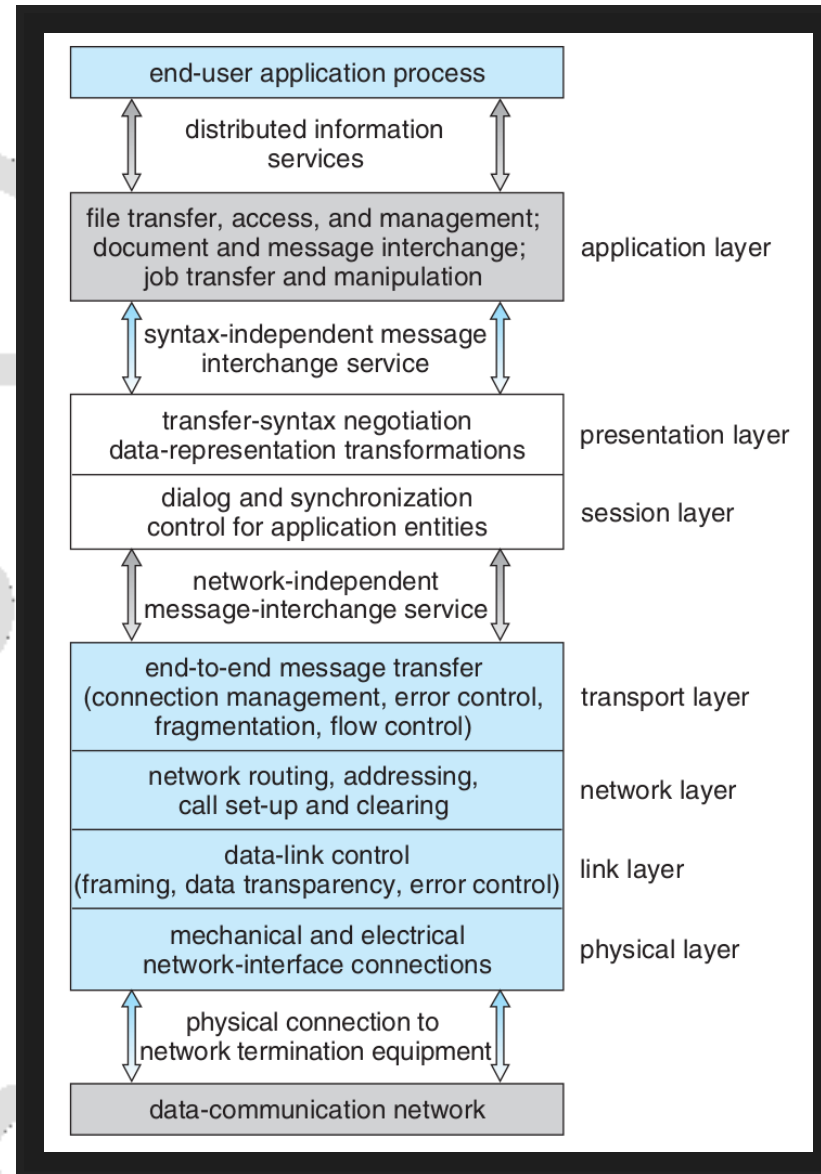
COMMUNICATION PROTOCOL

- **Layer 5: Session layer** – implements sessions, or process-to-process communications protocols
- **Layer 6: Presentation layer** – resolves the differences in formats among the various sites in the network, including character conversions, and half duplex/full duplex (echoing)
- **Layer 7: Application layer** – interacts directly with the users, deals with file transfer, remote-login protocols and electronic mail, as well as schemas for distributed databases

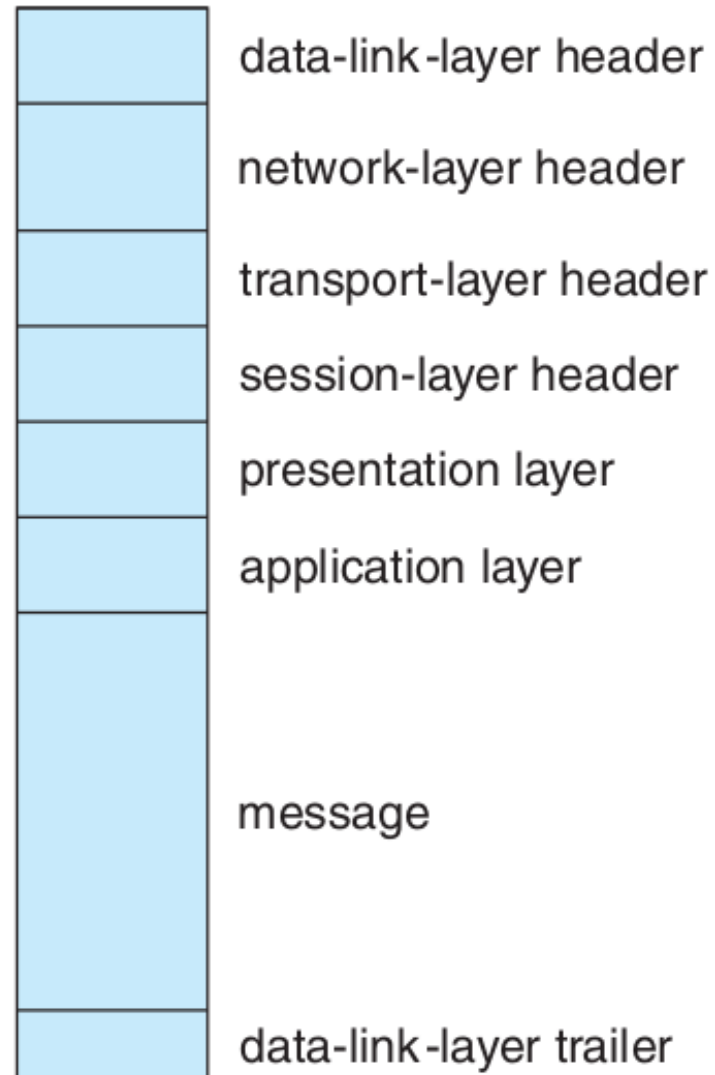
COMMUNICATION VIA ISO NETWORK MODEL



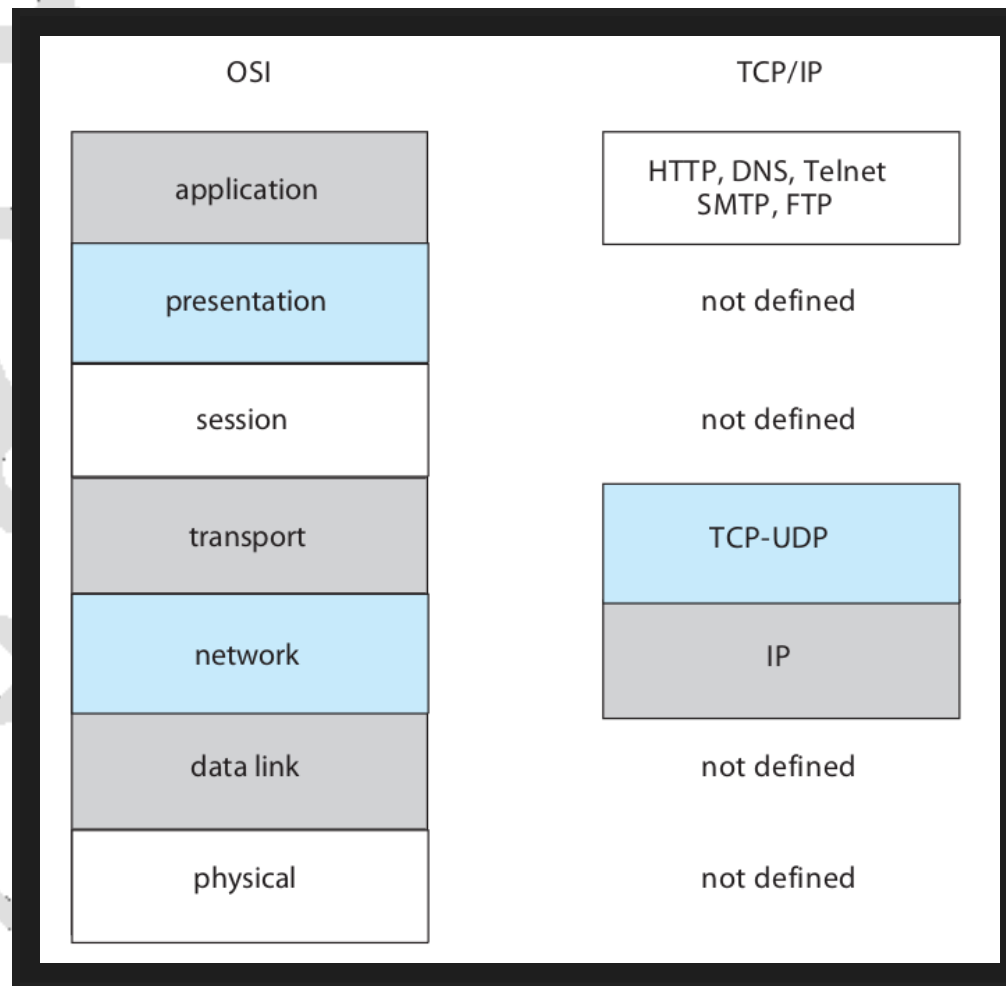
THE OSI PROTOCOL STACK



AN OSI NETWORK MESSAGE



THE OSI AND TCP/IP PROTOCOL STACKS



A background network diagram consisting of a complex web of interconnected nodes and edges. The nodes are represented by circles of varying sizes, some of which are solid gray, while others are hollow with a gray outline. The edges are thin gray lines connecting the nodes, creating a dense, organic-looking structure that fills the entire slide.

EXAMPLE: TCP/IP

TCP/IP

- The transmission of a network packet between hosts on an Ethernet network
- Every host has a unique **IP address** and a corresponding Ethernet **Media Access Control (MAC)** address
- Communication requires both addresses
- Domain Name Service (DNS) can be used to acquire IP addresses

TCP/IP

- **Address Resolution Protocol (ARP)** is used to map MAC addresses to IP addresses
 - **Broadcast** to all other systems on the Ethernet network
- If the hosts are on the same network, ARP can be used
- If the hosts are on different networks, the sending host will send the packet to a router which routes the packet to the destination network

AN ETHERNET PACKET

bytes

7	preamble—start of packet	each byte pattern 10101010
1	start of frame delimiter	pattern 10101011
2 or 6	destination address	Ethernet address or broadcast
2 or 6	source address	Ethernet address
2	length of data section	length in bytes
0–1500	data	message data
0–46	pad (optional)	message must be > 63 bytes long
4	frame checksum	for error detection

A background network diagram consisting of numerous nodes (circles) of varying sizes connected by thin lines. Some nodes are solid gray, while others are hollow. The connections form a complex, interconnected web across the entire slide.

ROBUSTNESS

A background network diagram consisting of a complex web of interconnected nodes and edges. The nodes are represented by circles of varying sizes, some of which are solid gray, while others are hollow with a gray outline. The edges are thin gray lines connecting the nodes, forming a dense, non-linear structure that fills the entire slide.

ROBUSTNESS

- Failure detection
- Reconfiguration

FAILURE DETECTION

Detecting hardware failure is difficult

- To detect a link failure, a heartbeat protocol can be used
- Assume Site A and Site B have established a link
 - At fixed intervals, each site will exchange an I-am-up message indicating that they are up and running
- If Site A does not receive a message within the fixed interval, it assumes either
 1. the other site is not up or
 2. the message was lost

FAILURE DETECTION

- Site A can now send an Are-you-up? message to Site B
- If Site A does not receive a reply, it can repeat the message or try an alternate route to Site B
- If Site A does not ultimately receive a reply from Site B, it concludes some type of failure has occurred

FAILURE DETECTION

- Types of failures:
 - Site B is down
 - The direct link between A and B is down
 - The alternate link from A to B is down
 - The message has been lost
- However, Site A cannot determine exactly **why** the failure has occurred

RECONFIGURATION

- When Site A determines a failure has occurred, it must reconfigure the system:
 1. If the link from A to B has failed, this must be broadcast to every site in the system
 2. If a site has failed, every other site must also be notified indicating that the services offered by the failed site are no longer available
- When the link or the site becomes available again, this information must again be broadcast to all other sites

The background of the slide is a light gray network of interconnected circles and lines, resembling a molecular structure or a complex web. The circles vary in size and are connected by thin gray lines. The word "QUESTIONS" is centered in the middle of the slide in a bold, black, sans-serif font.

QUESTIONS

The background of the slide features a light gray network diagram. It consists of numerous circular nodes of varying sizes connected by thin, straight lines. Some nodes are solid gray, while others are hollow. The connections form a complex, interconnected web across the entire slide.

BONUS

- 💡 Exam question number 13: **Network and Distributed Systems**