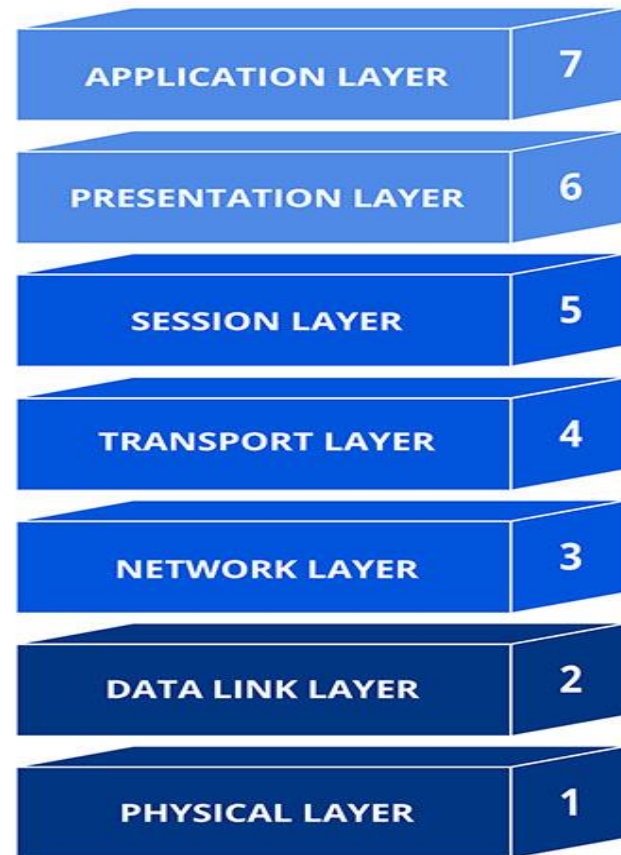


Wide Area Networks: Protocols and Services

Course Outline

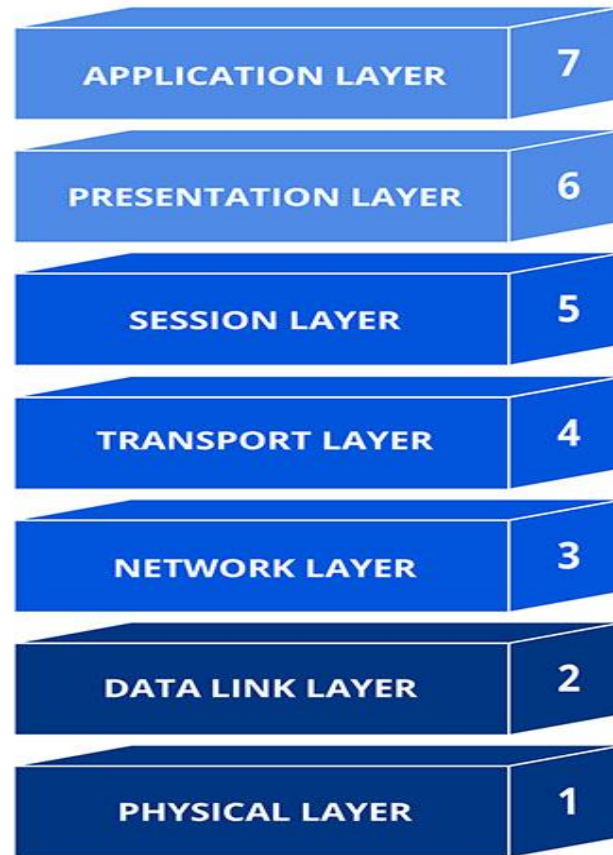
2

- Introduction to OSI
- Data link layer
- WAN networks
- The HDLC protocol
- The PPP protocol
- The Frame Relay protocol
- The MPLS protocol
- SD-WAN



Introduction to the OSI architecture

3



Problem statement

4

With the advent of Internet, the number and size of networks increased considerably. However, many networks were built using different hardware and software platforms. This resulted in incompatibility between many networks, making it difficult to establish communication between networks built on different specifications.

Solution

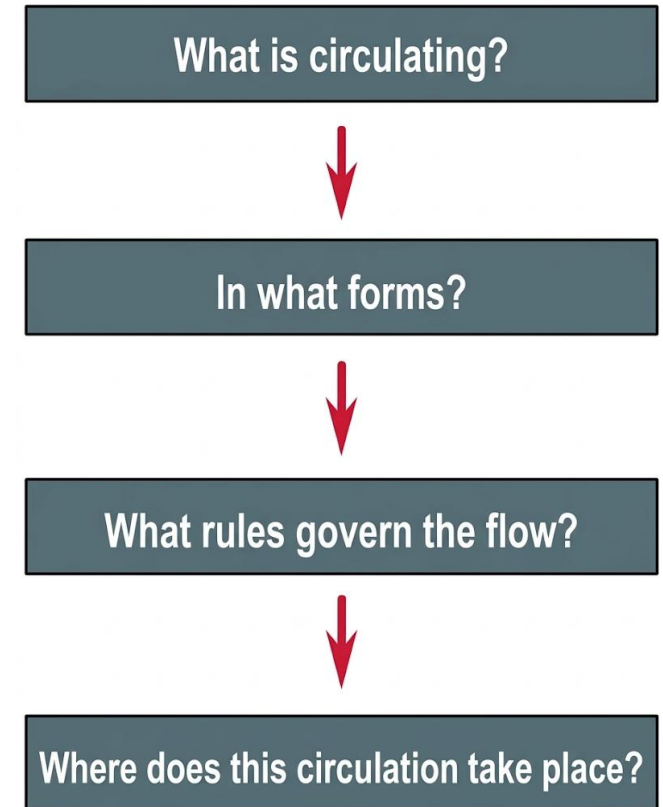
5

To solve this problem, the International Organization for Standardization (ISO) examined numerous network structures. ISO recognized the opportunity to create a network model that would help designers build networks capable of communicating and working together (interoperability). It therefore published the OSI reference model.

Analyzing a network by layer

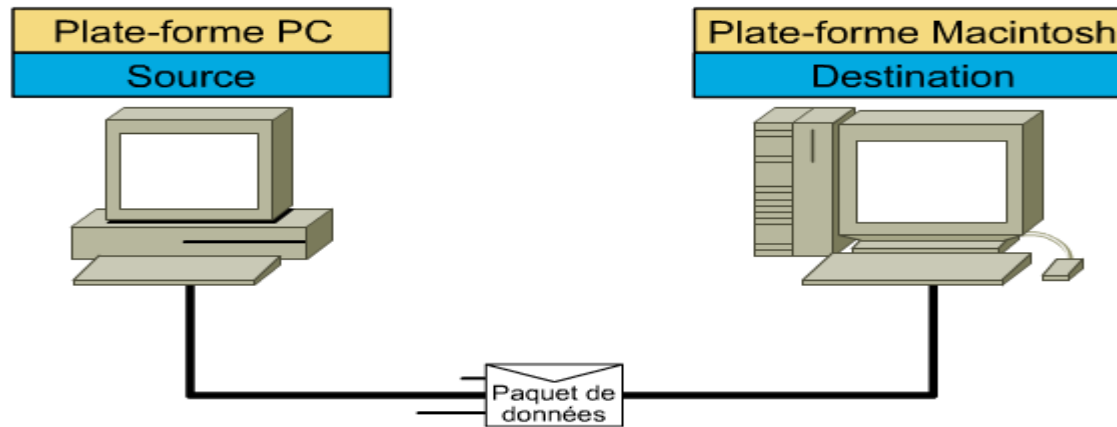
6

The concept of layers helps us understand what happens during communication between two computers. The questions shown in the figure relate to the movement of physical objects, such as road traffic, or of electronic data. This movement of objects, whether physical or logical, is called flow



Network Communication

7



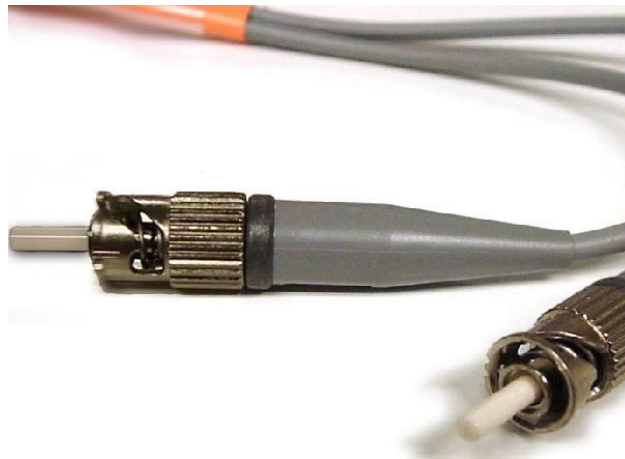
A data packet consists of a logically grouped unit of data that travels between computers. This packet includes the source information, as well as other elements needed to establish reliable communication with the destination unit.

Media

8

The medium provides the transmission support for data packets:

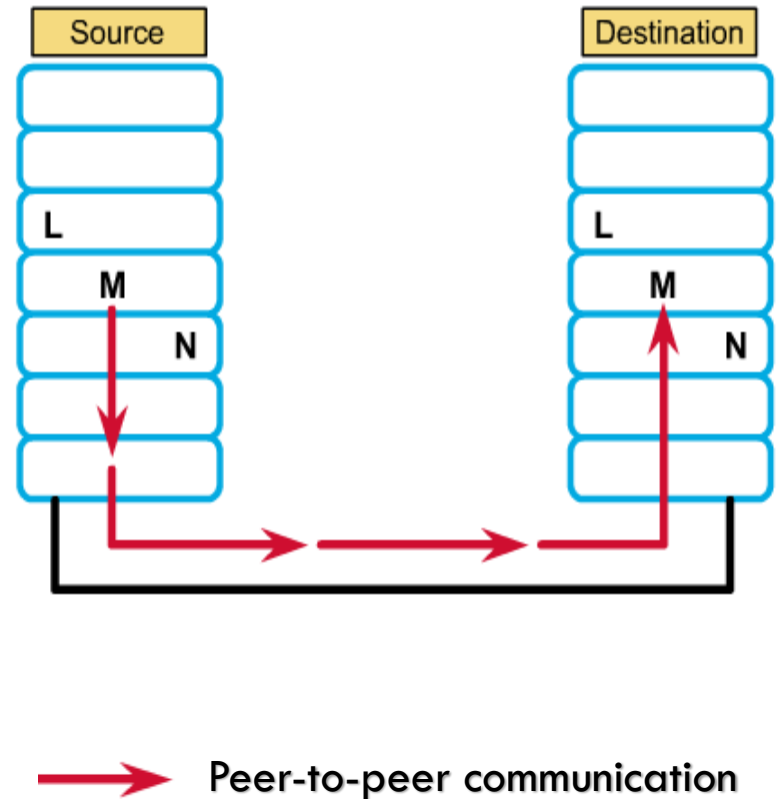
- ❖ A telephone wire
- ❖ An RJ45 cable
- ❖ A coaxial cable
- ❖ Fiber optics
- ❖ RADIO



Computer Protocol

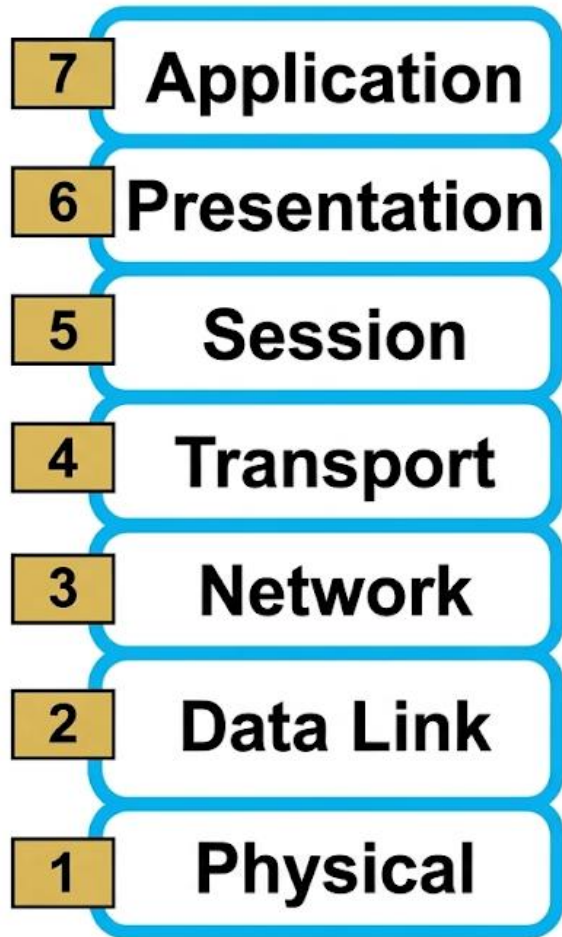
9

For data packets to travel from a source to a destination on a network, it is important that all network units speak the same language, or protocol. A protocol consists of a set of rules that improve the efficiency of communications within a network.



Why a layered network model

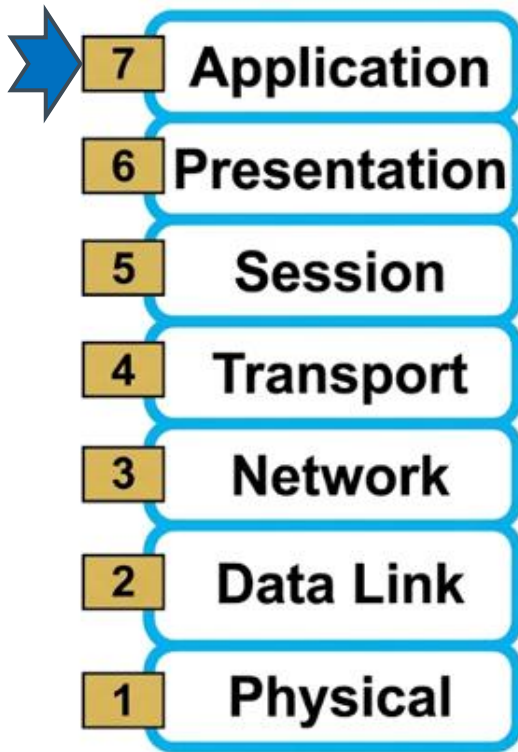
10



- ◆ It reduces complexity.
- ◆ It standardizes interfaces.
- ◆ It facilitates modular design.
- ◆ It ensures technology interoperability.
- ◆ It accelerates evolution.
- ◆ It simplifies teaching and knowledge acquisition.

The 7 layers of the OSI model

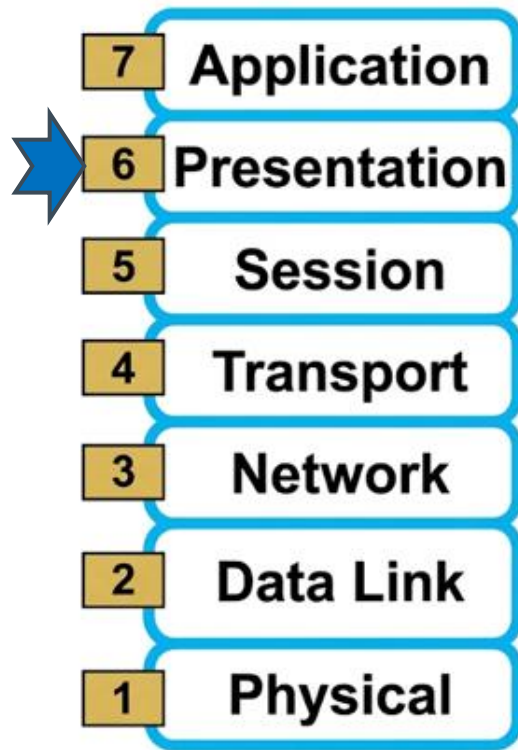
11



The application layer is the OSI layer closest to the user. It provides network services to the user's applications. (e.g., web browser)

The 7 layers of the OSI model

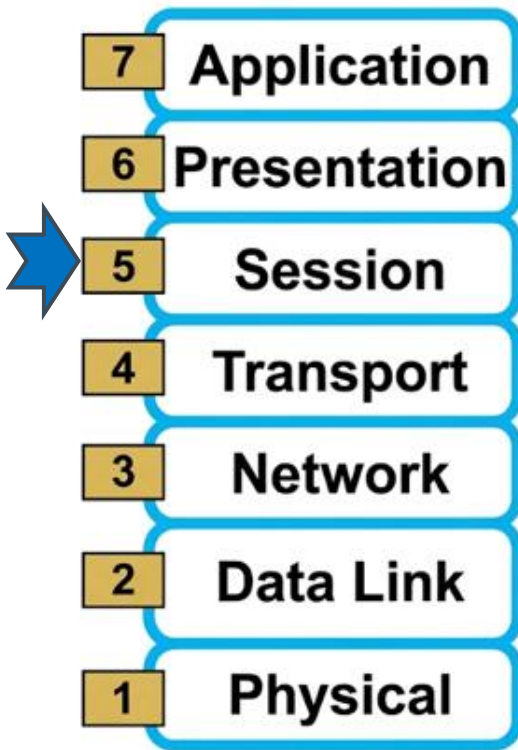
12



The presentation layer ensures that information sent by the application layer of one system is readable by the application layer of another system.

The 7 layers of the OSI model

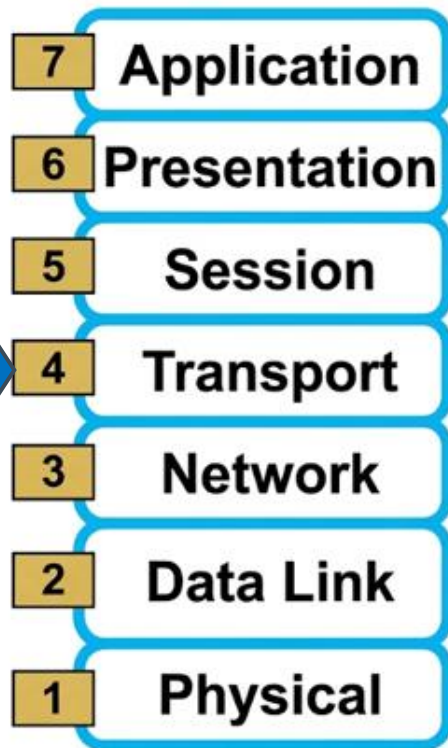
13



As its name suggests, the session layer opens, manages, and closes sessions between two communicating host systems.

The 7 layers of the OSI model

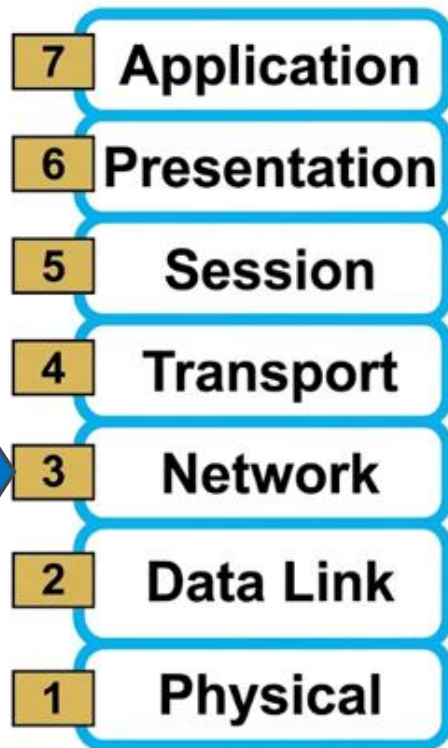
14



The transport layer segments the data sent by the sending host system and reassembles it into a data stream on the receiving host system.

The 7 layers of the OSI model

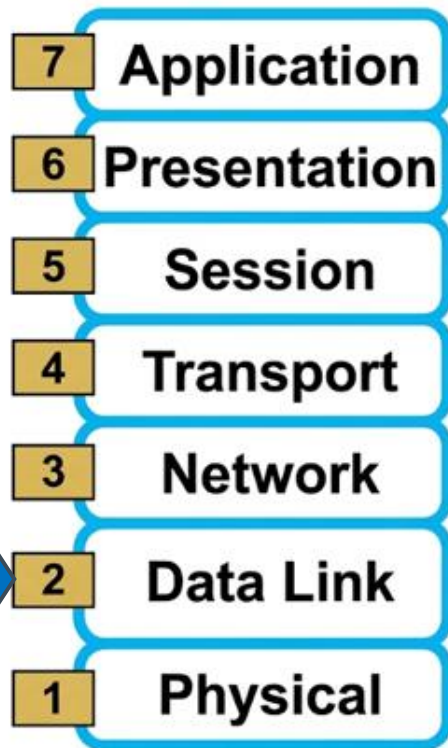
15



The network layer is a complex layer that provides connectivity and path selection between two host systems that may be located on geographically distant networks.

The 7 layers of the OSI model

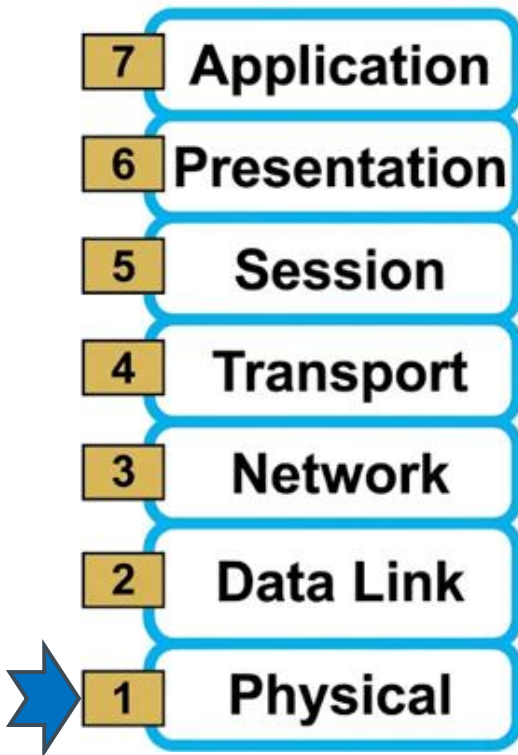
16



The data link layer provides reliable transit of data across a physical link. As such, the data link layer handles physical addressing, network access, error notification, ordered delivery of frames, and flow control.

The 7 layers of the OSI model

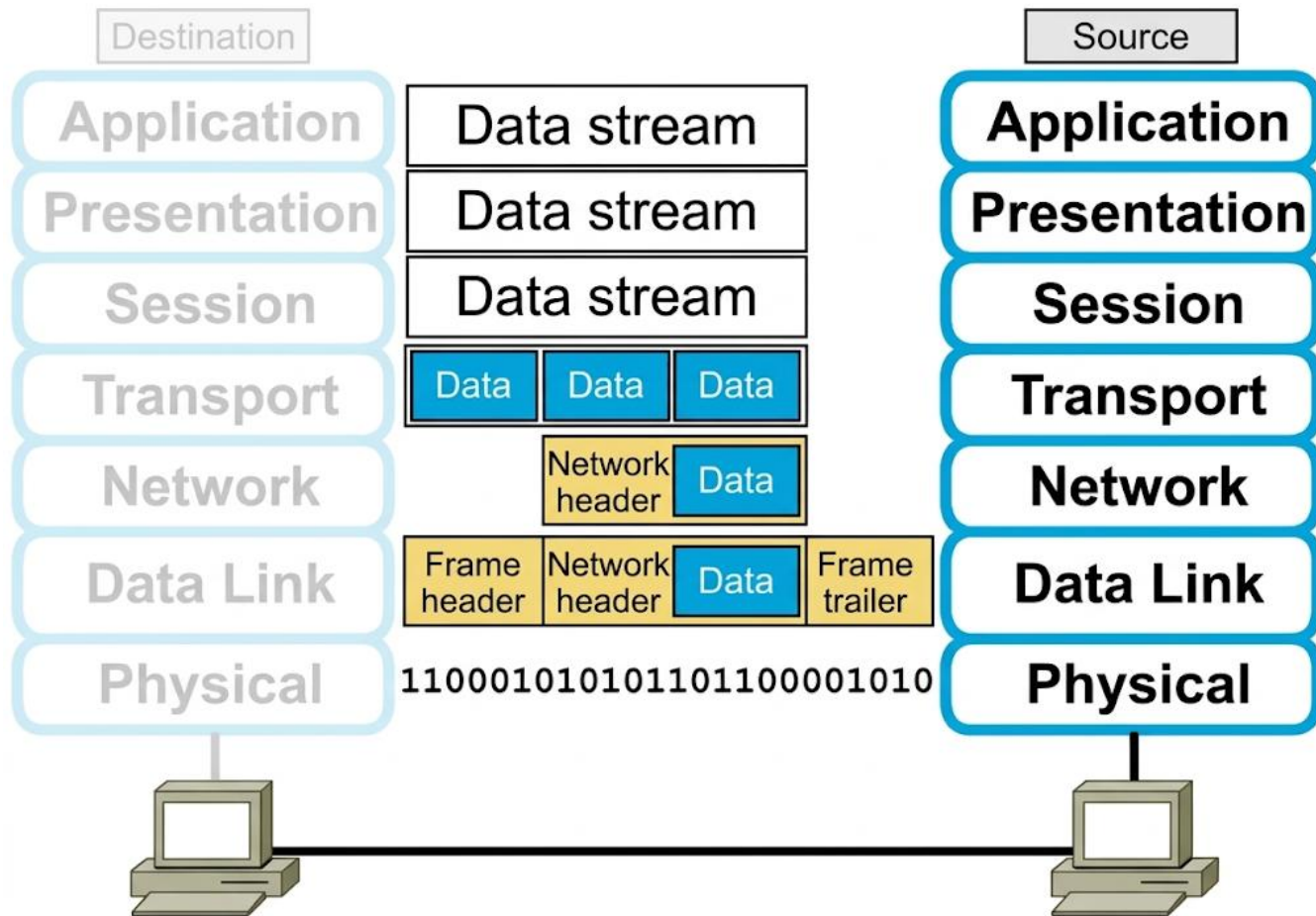
17



Defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between end systems.

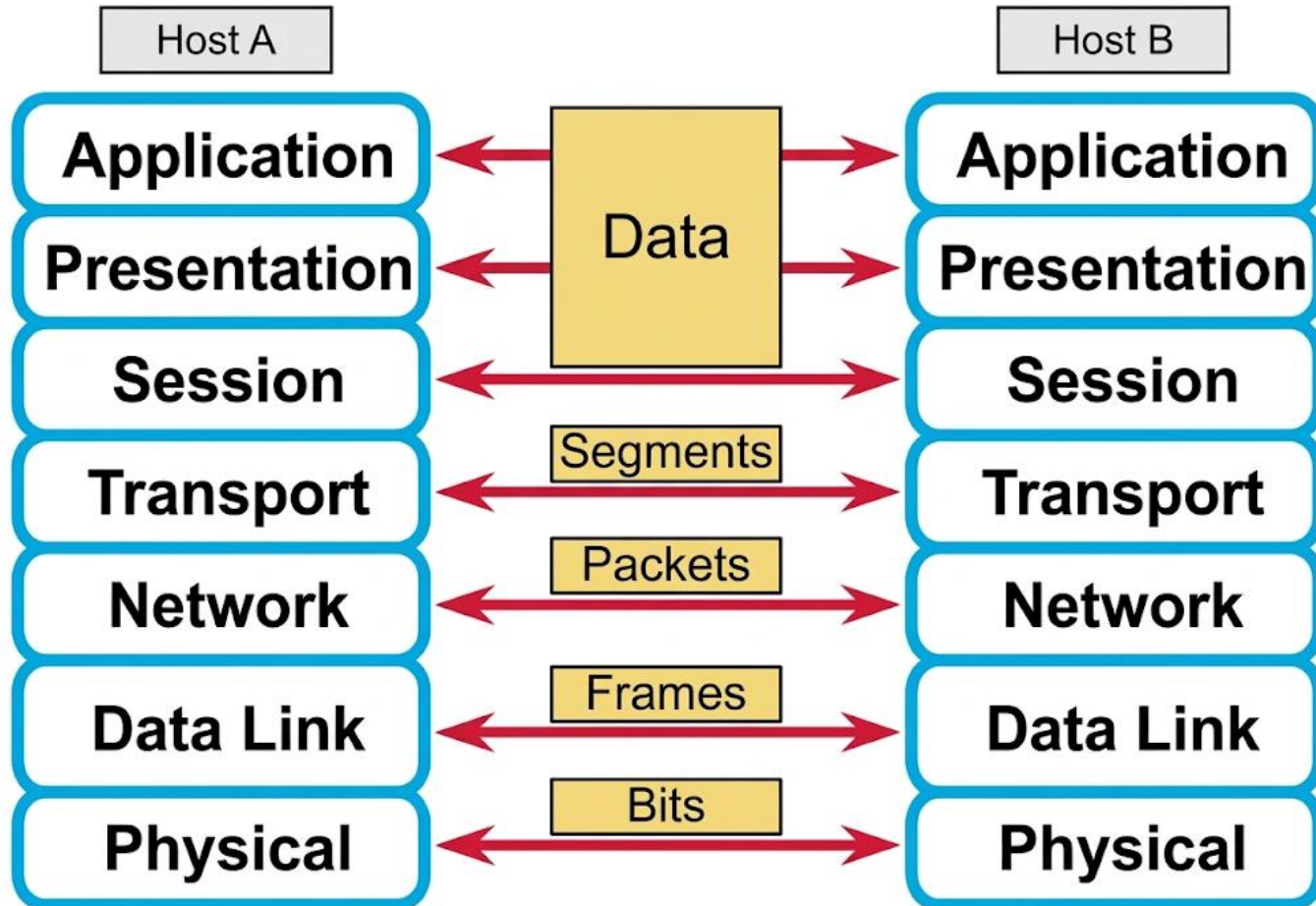
Data encapsulation

18



Peer-to-peer communication

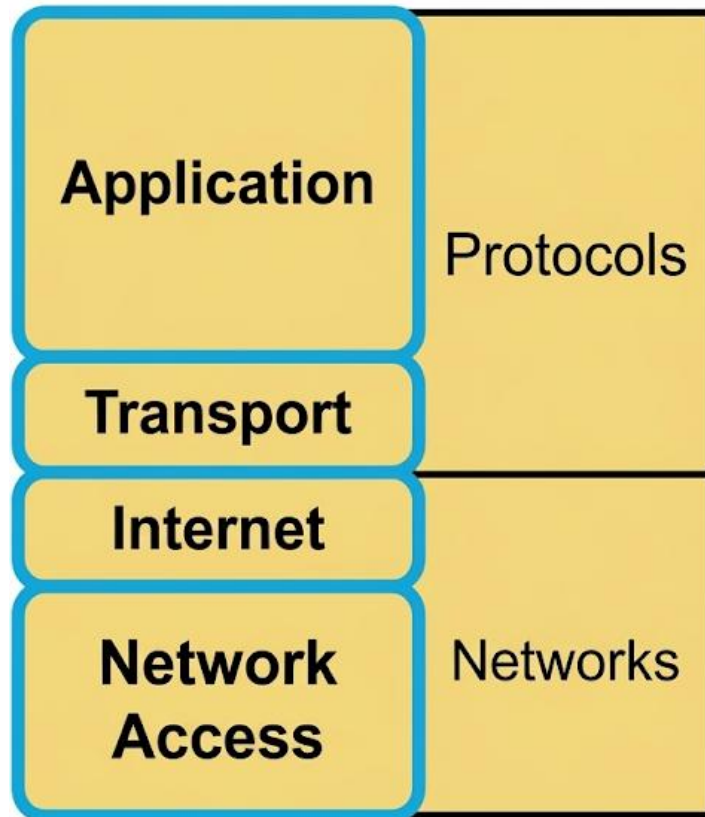
19



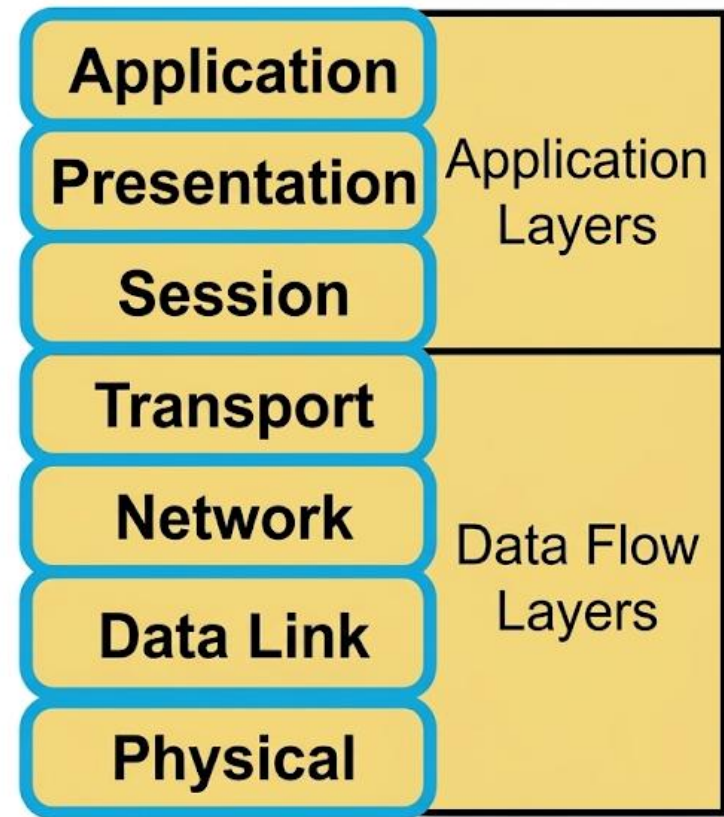
TCP/IP Model

20

TCP/IP Model



OSI Model



TCP/IP Model

21

Network Access layer

- ❑ This layer combines the functions of the two lowest layers of the OSI model (physical + data link).
- ❑ It provides the means to deliver data to systems attached to the network.

TCP/IP Model

22

Internet layer

- ❑ Corresponds to layer 3 (network) of the OSI model.
- ❑ Provides connectionless interconnection of remote networks.
- ❑ Based on the IP (Internet Protocol) protocol.
- ❑ IP's purpose is to route packets (datagrams) to their destination independently of one another.

TCP/IP Model

23

Internet layer

- ❑ individual packet routing, packets may arrive out of order.
- ❑ The IP protocol supports neither lost-packet detection nor error recovery.

TCP/IP Model

24

Transport layer

- Provides the mechanisms needed to know the state of the transmission.
- Ensures the reliability of exchanges,
- Ensures that data arrives in the correct order,
- Determines which application the packets should be delivered to.
- Includes 2 protocols: **UDP** (User Datagram Protocol) & **TCP** (Transmission Control Protocol)

TCP/IP Model

25

What is the difference between

TCP and **UDP** ???

TCP/IP Model

26

Application layer

Hosts most network programs and applications. These programs generally run just above the TCP and UDP protocols and are often associated with well-defined ports. It is the richest layer in terms of the number of network applications and associated services. It covers the entire set of {session + presentation + application} layers of the OSI model.

Transport protocols: TCP and UDP

27

The IP network provides unreliable (best-effort) data transfer; under these conditions, application programs must account for any possible network failures, and in particular:

- Error detection and recovery.
- Data loss.
- Data being delivered out of sequence.

This role falls to the transport layer.

Transport protocols: TCP and UDP

28

TCP: handles splitting the message into datagrams, reassembling them on arrival in the correct order, and retransmitting anything that was lost. Unlike UDP, TCP makes it possible to:

- provide reliable transmission.
- detect and correct packet loss or duplication.
- define how to establish a connection and how to terminate it.

Transport protocols: TCP and UDP

29

UDP: a simple protocol, whose advantage is offering a short execution time, which makes it possible to accommodate real-time constraints.

The drawback of this protocol is its unreliability:

- provides a service with no error recovery and uses no ACKs.
- does not resequence messages and performs no flow control.

UDP messages can be lost, duplicated, or delivered out of sequence.

Transport protocols: TCP and UDP

30

The concept of a transport connection

A transport connection makes it possible to view the network as a virtual link between two applications running on the end systems.

A transport connection is fully defined by the combination of several identifiers:

- ☐ The identifier of the end systems, or **IP addresses**
- ☐ The identifier of the transport **protocol** used
- ☐ The identifier of the end processes, or **port**

Transport protocols: TCP and UDP

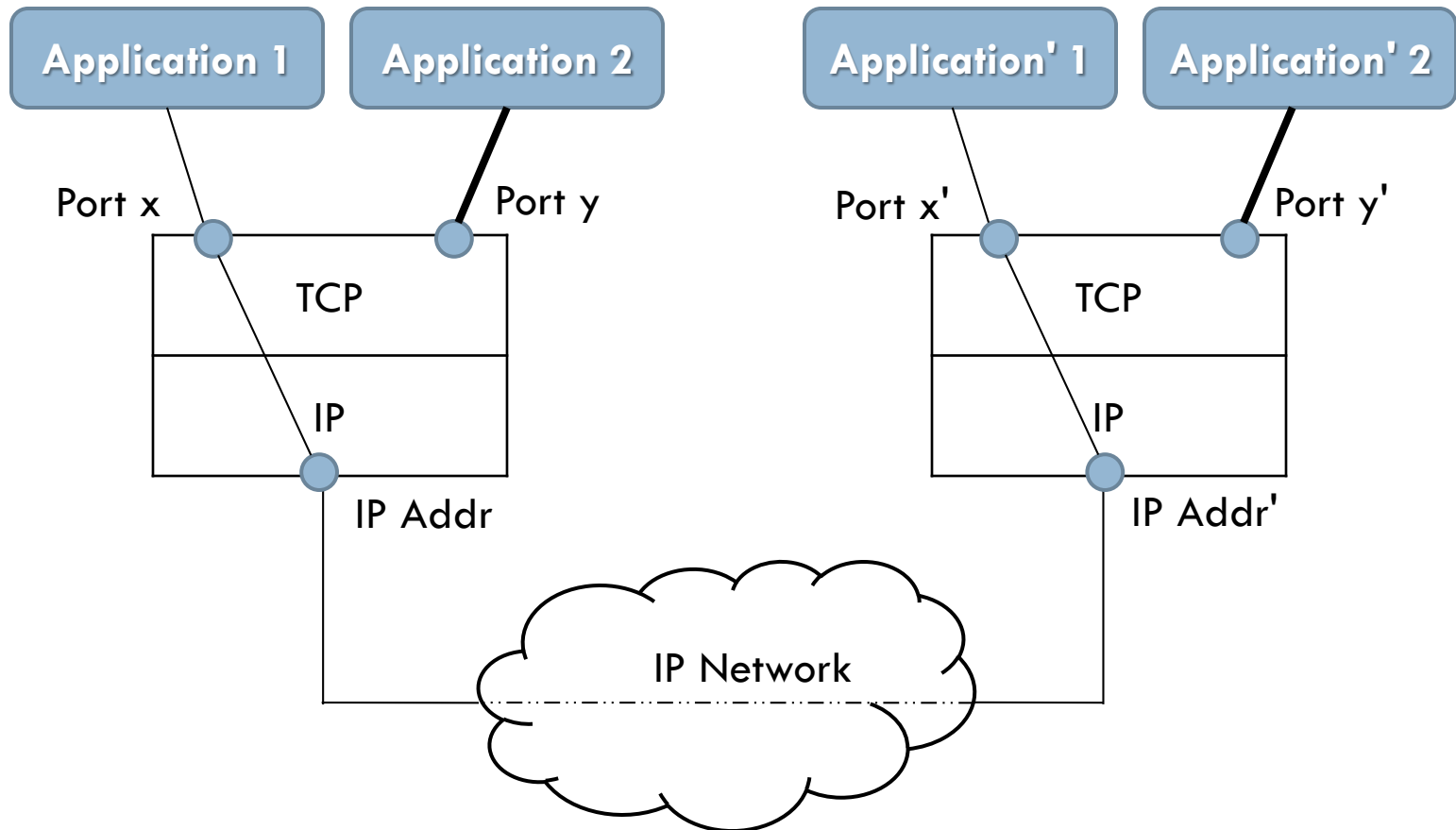
31

The concept of transport connection multiplexing

A single system can run several applications, so it must be able to establish and distinguish between multiple transport connections. It is the concept of a **port** that allows transport connections to be multiplexed; a port identifies one end of the connection.

Transport protocols: TCP and UDP

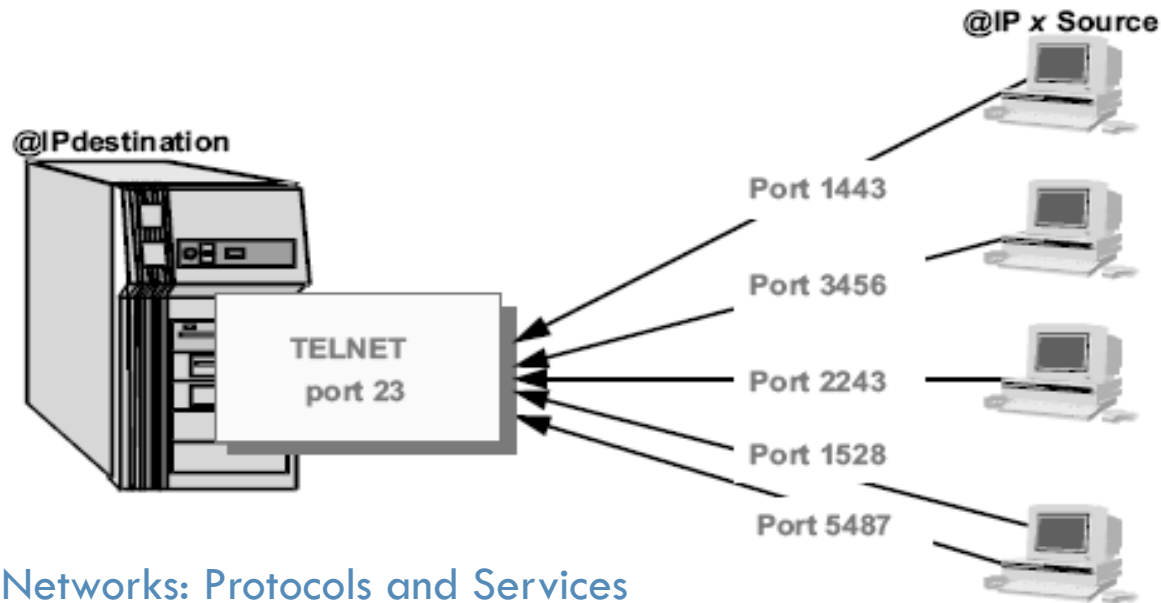
32



Transport protocols: TCP and UDP

33

The virtual terminal application (Telnet) is identified by port number 23. A client wishing to establish a Telnet session calls on remote port 23, while locally it assigns some arbitrary, unique port number on that machine ($> 1,024$).



Transport protocols: TCP and UDP

34

The first 1,024 values are reserved. Ports identified by these values are called well-known, or registered, ports; these ports are tied to specific applications.

Service name	Port number	Protocol
FTP	20-21	TCP
TELNET	23	TCP
DNS	53	UDP
TFTP	69	UDP
HTTP	80	TCP
POP3	110	TCP

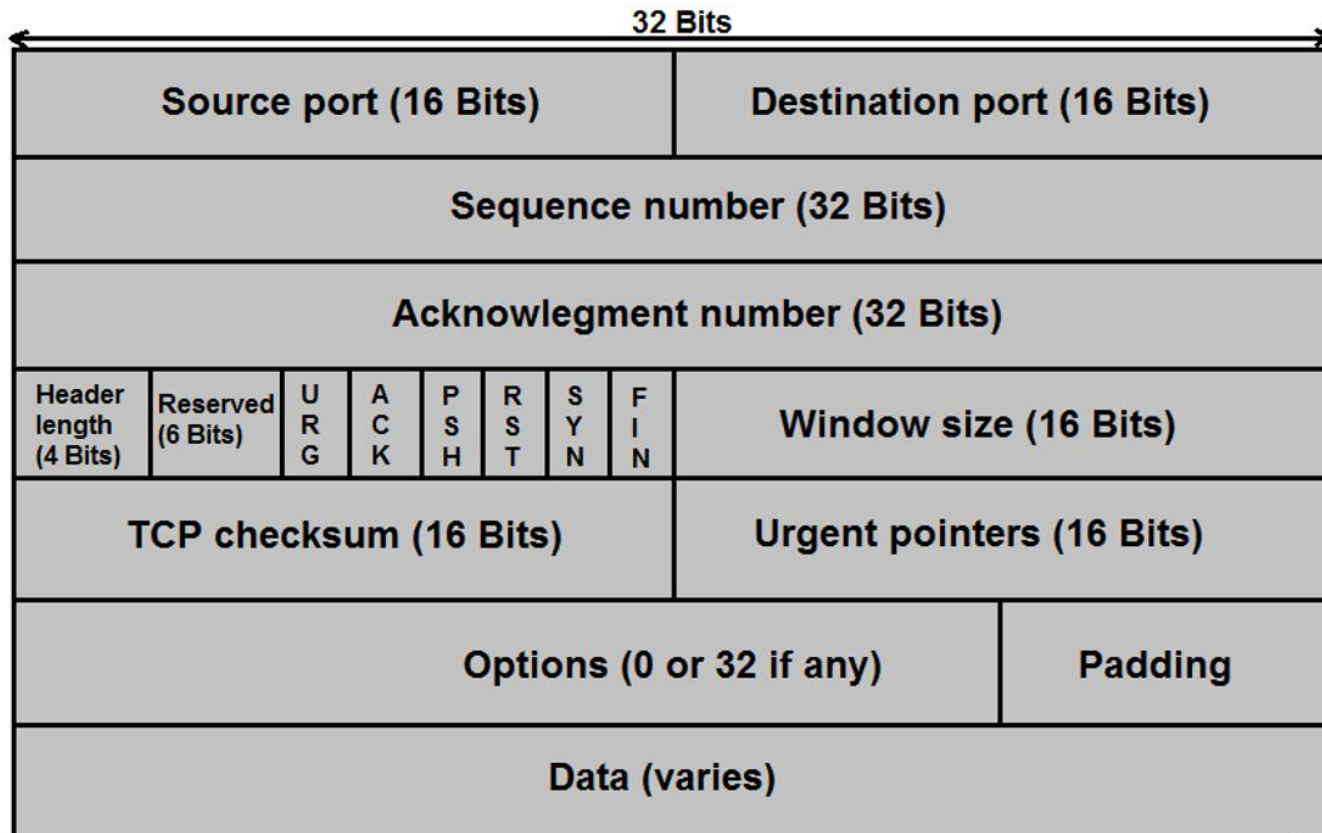
Transport protocols: TCP and UDP

35

Well-known ports allow a client application to identify an application on the remote system. The client end of the connection is identified by a port number assigned dynamically by the calling process. This port number is called a dynamic port.

Transport protocols: TCP and UDP

36



TCP segment format

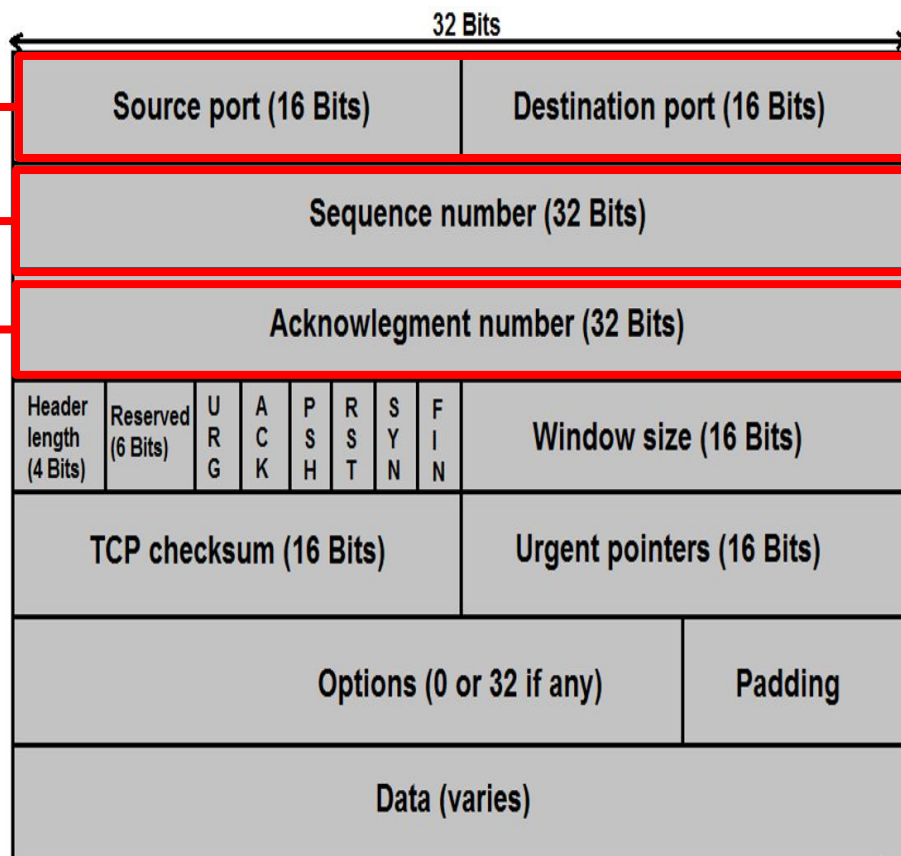
Transport protocols: TCP and UDP

37

Port → 16 bits

32-bit field indicating the number of the first byte carried by the segment

32-bit field; the ACK value indicates the number of the first expected byte, i.e., the number of the last byte received + 1



TCP segment format

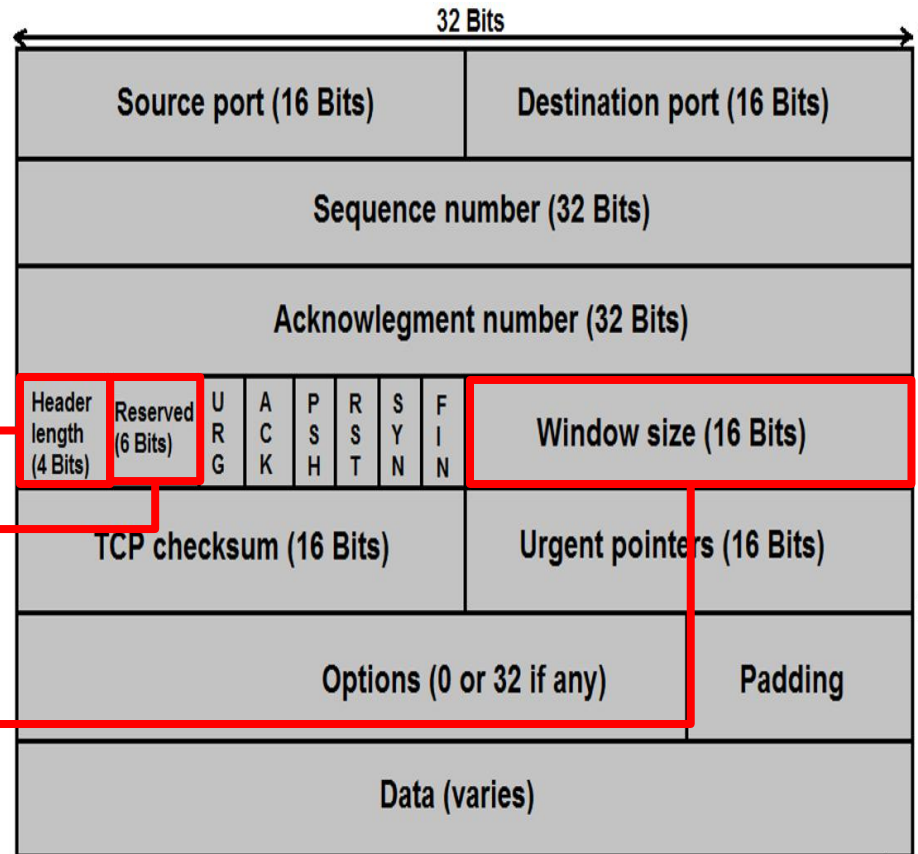
Transport protocols: TCP and UDP

38

4-bit field indicating the header length as a multiple of 32 bits

Area reserved for future use. This field must be filled with 0.

16-bit field indicating the number of bytes the receiver agrees to accept.



TCP segment format

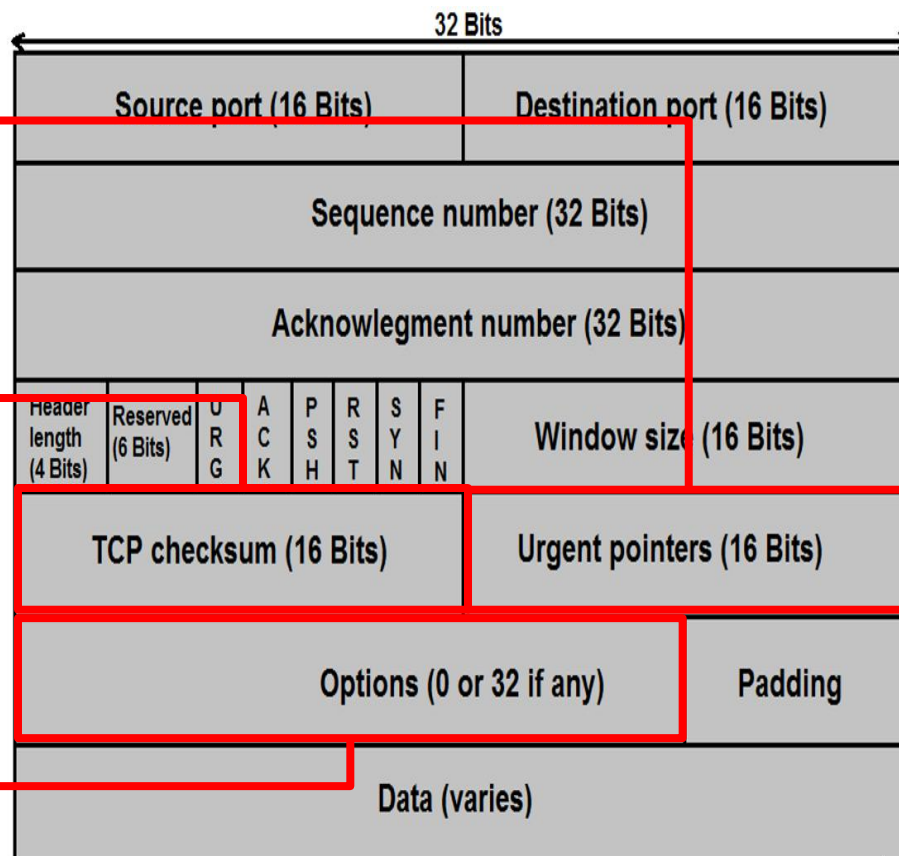
Transport protocols: TCP and UDP

39

16-bit field specifying the last byte of an urgent message.

16-bit field used to detect errors in the segment's header and body.

Area containing the various TCP protocol options



TCP segment format

Transport protocols: TCP and UDP

40

-URG: Indicates that the Urgent Pointer field is valid and the segment contains urgent data.

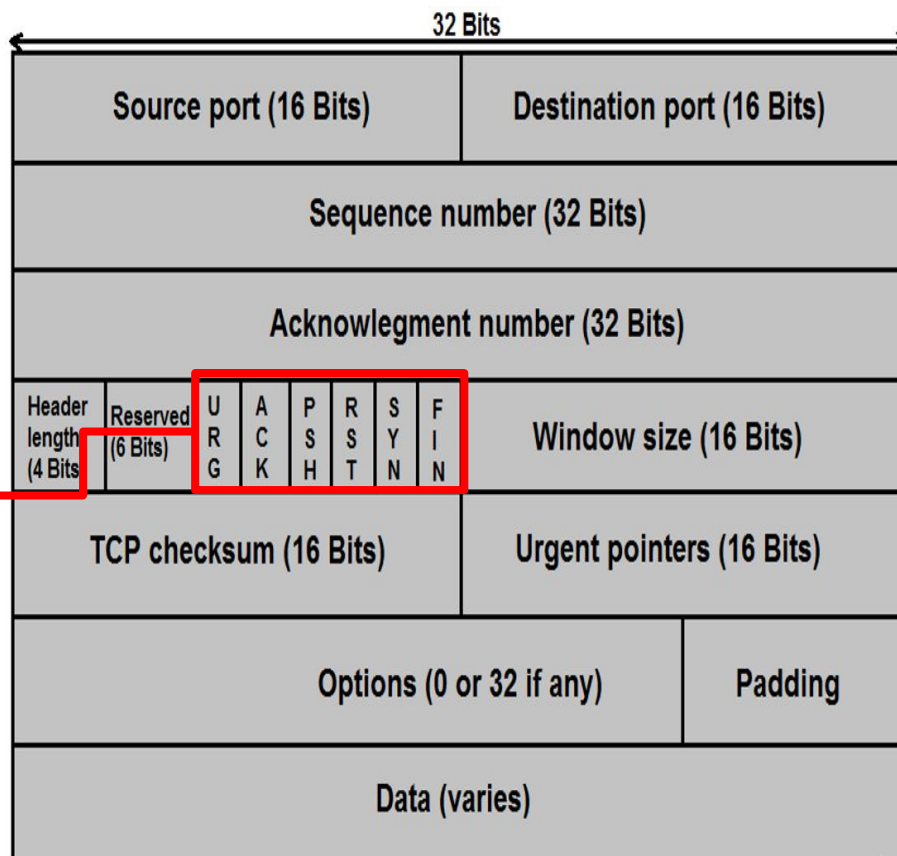
-ACK: Indicates that the Acknowledgment Number field is valid.

-PSH: Requests the receiving TCP to push data to the application immediately without buffering.

-RST: Abruptly resets/terminates the connection due to an error or rejection.

-SYN: when set to 1, this bit corresponds to a connection request

-FIN: this flag corresponds to a disconnection request.

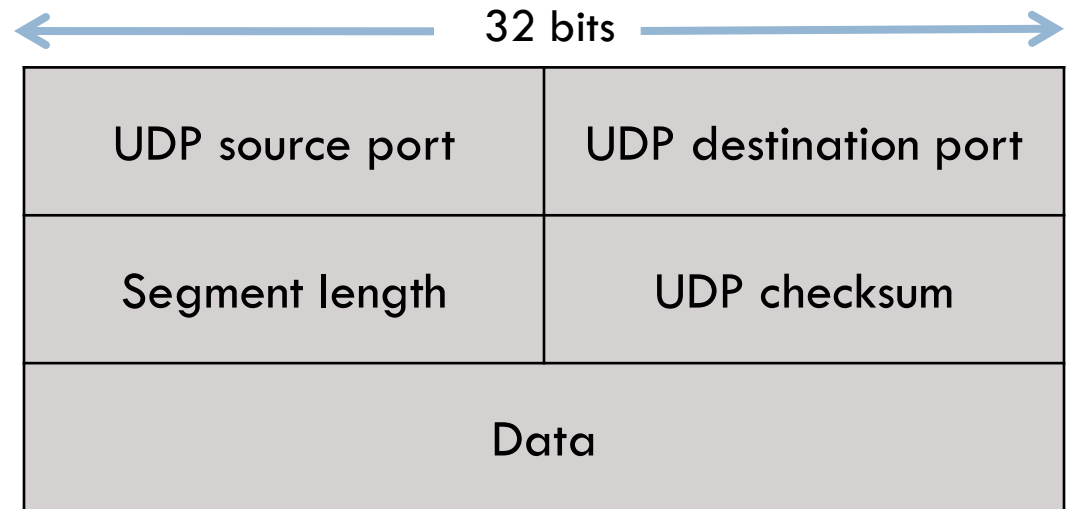


TCP segment format

Transport protocols: TCP and UDP

41

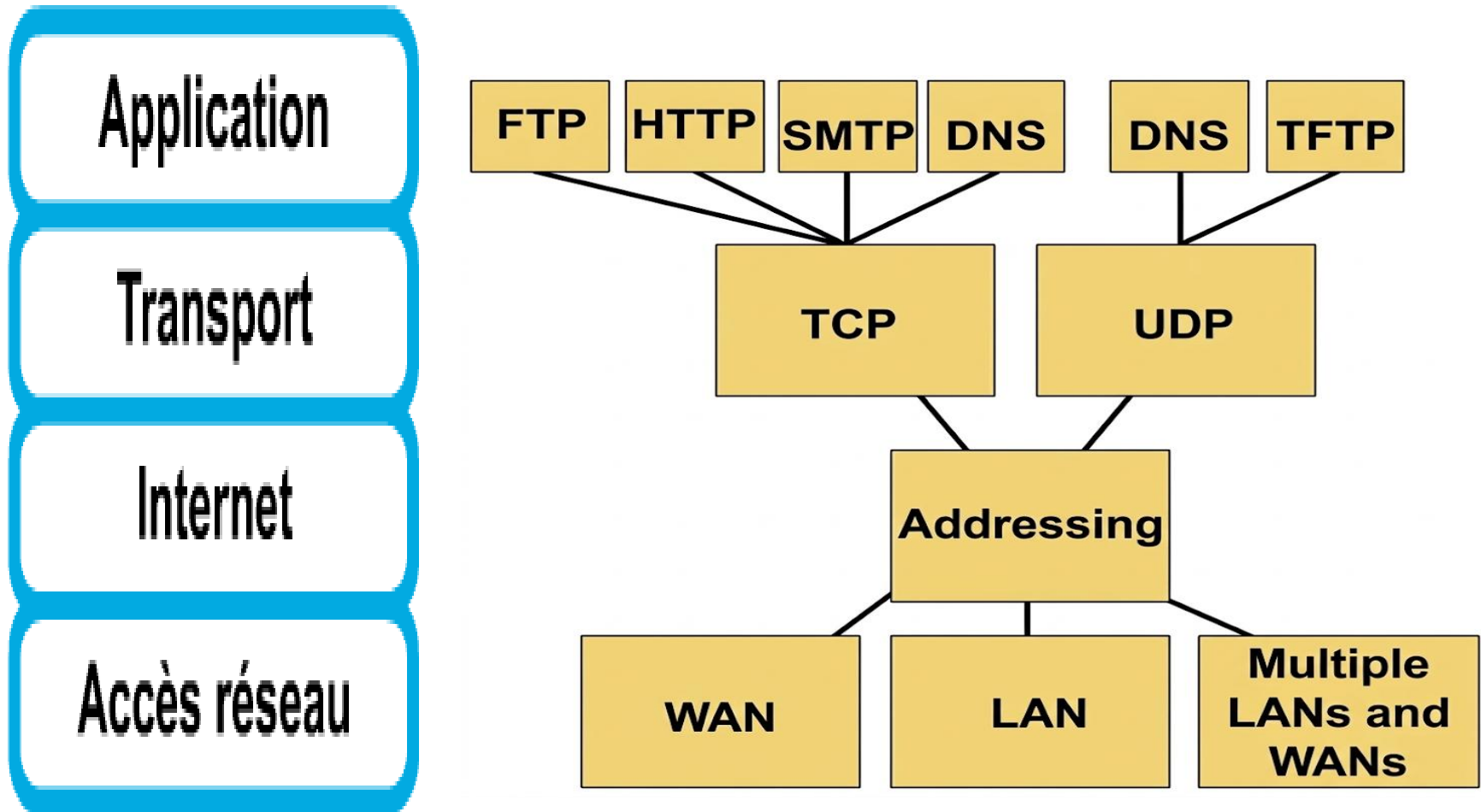
UDP segment format



- Source/destination port → 02 bytes
- Segment length → 02 bytes (header included)
- The checksum field → 02 bytes
- User data

TCP/IP protocol diagram

42



The FTP protocol

43

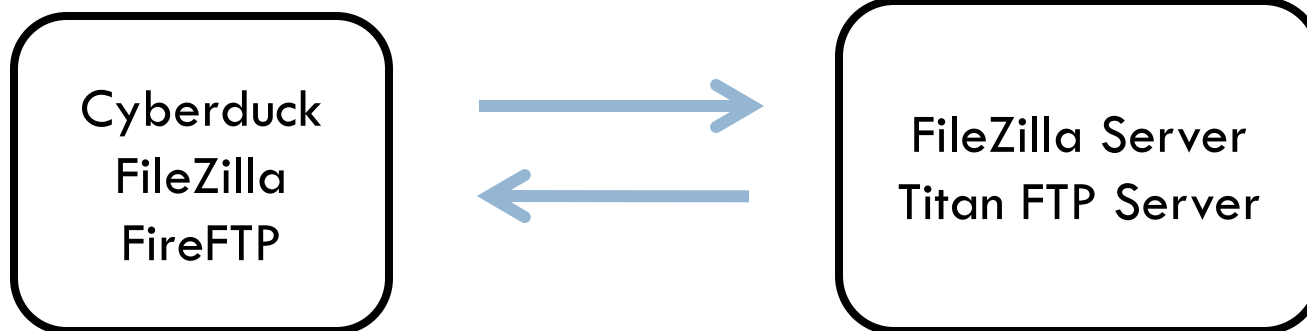
FTP, or File Transfer Protocol, is a communication protocol for exchanging files over a TCP/IP network. It lets a computer copy, delete, or modify files over the network. This mechanism is often used:

- Within companies
- On the Internet, to update a website hosted by a provider.

The FTP protocol

44

Characteristics	Follows a client-server model
	Uses a TCP connection
	Port 21 for commands
	Port 20 for data



The TFTP protocol

45

TFTP (Trivial File Transfer Protocol, or simplified file transfer protocol) is a simplified file transfer protocol.

Characteristics	Follows a client-server model
	Uses UDP / Port 69
	Unreliable / Possible packet loss
	Well suited to local area networks

The HTTP protocol

46

It is a communication protocol developed for the World Wide Web, allowing clients using web browsers to access a server containing data.

Characteristics	Follows a client-server model
	HTTP: Uses TCP / Port 80
	HTTPS: Uses TCP / Port 443

The DNS protocol

47

The Domain Name System (or DNS) is a service that translates a domain name into the IP address of the machine bearing that name.

DNS generally uses UDP on port 53. If a response exceeds the UDP size limit (originally 512 bytes, now often 4096 with EDNS0), the server sets the Truncated bit, prompting the client to retry the query over TCP on port 53.

The RDP protocol

48

Remote Desktop Protocol (RDP) is a protocol that lets a user connect to a server running Microsoft Terminal Services. By default, the server listens on TCP port 3389.

The SNMP protocol

49

Simple Network Management Protocol (SNMP) is a communication protocol that lets network administrators manage network equipment, and remotely monitor and diagnose network and hardware problems.

Characteristics	Manager / Agent / Managed device
	UDP - Port 161 for requests
	UDP - Port 162 for responses and traps

End of the chapter