Standards

→ set of rules allowing devices from different companies work together

Ex:
- ISO (International organization for standardization
- ANSI
- IEEE

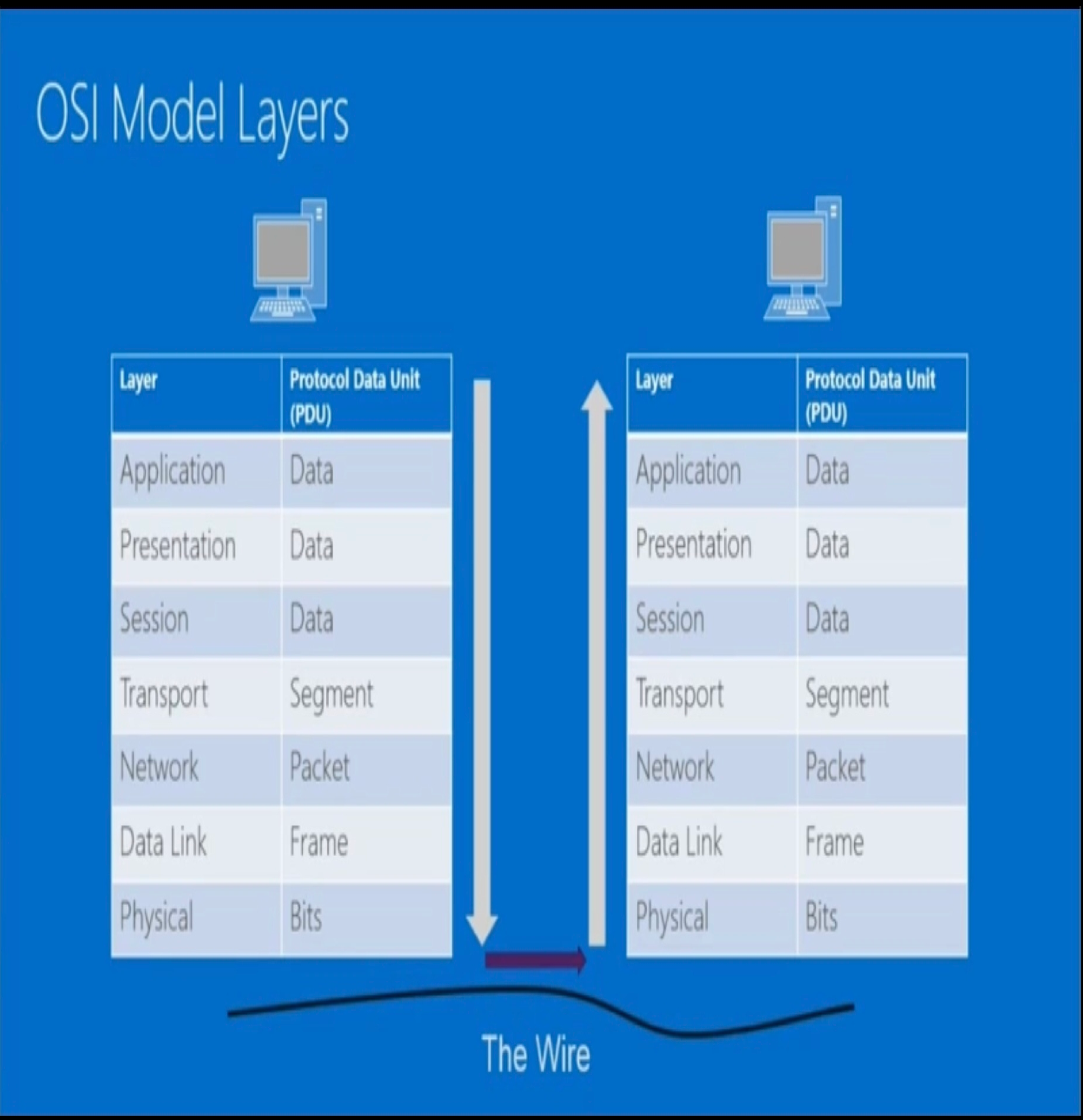
Open System Interconnection (OSI)

→ defines how data communication occurs b/w devices

→ Divided into 7 layers, each layer providing services to layers above and below

Layer	Defines
Layer 7 – Application Layer	Enables users and applications to access network services
Layer 6 – Presentation Layer	Translates data into a common format
Layer 5 – Session Layer	Establishes a communication session between devices
Layer 4 – Transport Layer	Manages message fragmentation and reassembly
Layer 3 – Network Layer	Manages data routing and creating sub networks
Layer 2 – Data Link Layer	Provides error-free transfer of data frames
Layer 1 – Physical Layer	Physical network media and signal methods

→ OSI is a protocol to access internet



Layer 1: Physical layer

- Defines the physical and electrical medium for data transfer
- Physical layer components: cables, jacks, patch panels, punch blocks, hubs, and MAUs
- Physical layer concepts: topologies, analog versus digital/encoding, bit synchronization, baseband versus broadband, multiplexing, and serial data transfer
- Unit of measurement: Bits

Ethernet Standards

Ethernet Standards

- LAN standard providing a communication method for high speed data exchange among devices
- Defined Physical and Data Link Layer
- 100BASE-T
  - 100 for 100 Mbps
  - BASE for baseband
  - T for twisted-pair cabling
- Baseband refers to the fact that devices on the network use digital signaling over a single frequency
- Broadband systems use analog signaling over a range of frequencies enabling multiple channels over the same physical medium

→ It has frame type - how data is packaged and sent over internet

Layer 2: Data Link Layer

- Establishes, maintains, and decides how transfer is accomplished over the physical layer and ensures error-free transmission over the physical layer
- Physical addresses (the hexadecimal address that is burned into the ROM of the NIC), known as the MAC address uniquely identify each hardware device work at the Data Link Layer
- Data Link Layer components: network interface cards and bridges
- Unit of measurement: frames

MAC Address

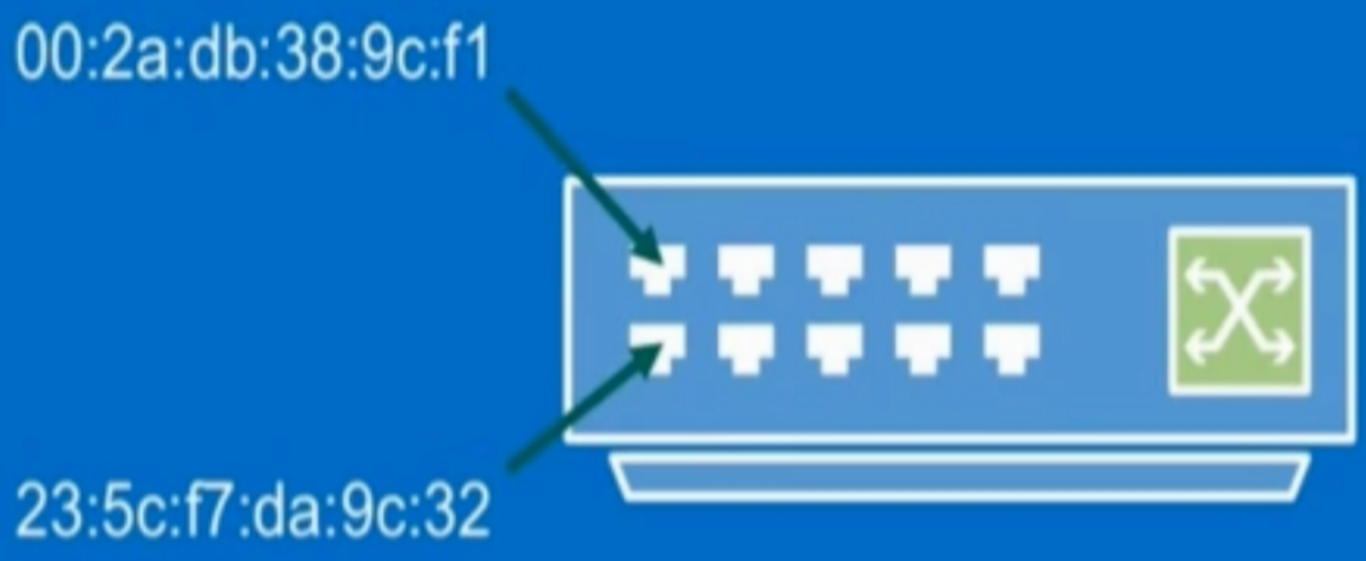
- Media Access Control
- Unique hardware identified assigned to a network interface card (NIC)
- Format: twelve character hexadecimal numbers split in two's separated by a colons (separatoss)

-> First six characters represent the company that made Network interface, and last six is a unique number

★ MAC address can be faked or spoofed in a process called spoofing.

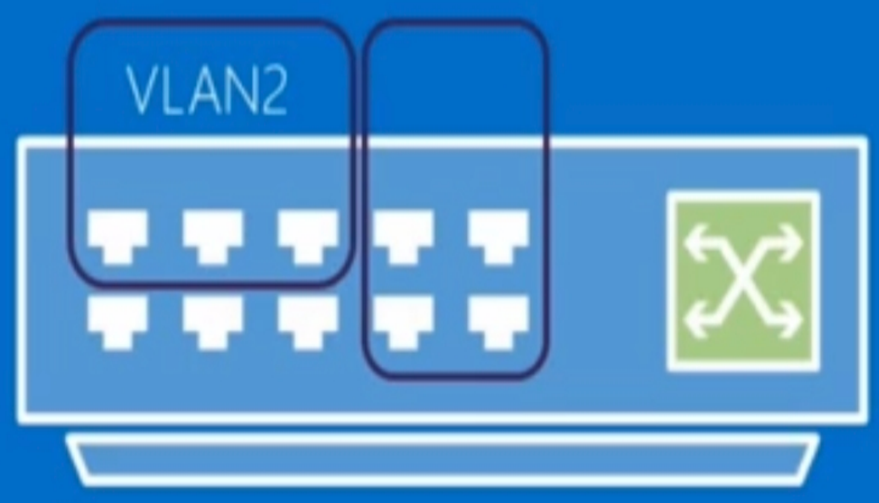
Switches

- Layer 2 switches are hardware-based and use the MAC address of each host computer's network adapter when deciding where to direct data frames
- Ports on the switch are mapped to the specific MAC address of the device attached



VLAN

- Layer 2 switching can also allow for a virtual LAN (VLAN) to be implemented.
- A VLAN is implemented to segment and organize the network, to reduce collisions, boost performance
- IEEE 802.1Q is the standard that supports VLANs
- A tag is added to the data frame to identify the VLAN

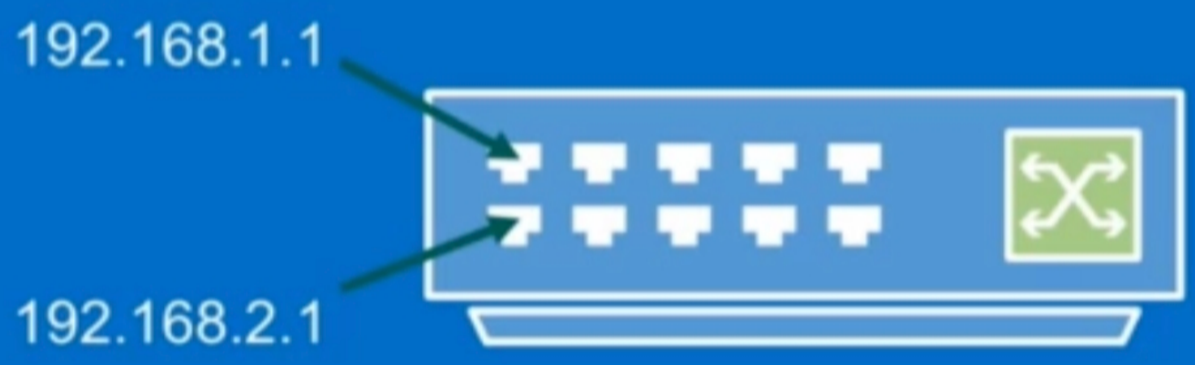


Layer 3 - Network Layer

- Controls the operations of routing and switching information to different networks
- Translates logical addresses or names to physical addresses
- Internet Protocol (IP) is a Network Layer protocol
- Devices that work at the network layer are routers and IP switches
- Network Layer components: IP addresses, subnets
- Unit of measurement: packets

Switches

- Switches can also reside on the network layer
- A layer 3 switch determines paths for data using logical addressing (IP addresses) instead of physical addressing (MAC addresses for a layer 2 switch)
- Layer 3 switches forward packets, whereas layer 2 switches forward frames



Layer 4 - Transport Layer

- This layer ensures messages are delivered error-free, in sequence and with no losses or duplications
- Protocols that work at this layer segment messages, ensure correct reassembly at the receiving end, perform message acknowledgement and message traffic control
- The Transport Layer contains both connection-oriented and connectionless protocols
- Unit of measurement used: segments or messages

Connection Oriented Communications

- Require both devices involved in the communication establish an end-to-end logical connection before data can be sent
- These communications are considered reliable network services
- Packets not received by the destination device can be resent by the sender

Connectionless Communications

- End-to-end connection is not necessary before data is sent
- Every packet that is sent has the destination address in the header
- Sufficient to move independent packets, such as in streaming media
- Datagram delivery is not guaranteed and lost packets cannot be resent

Connection-based Protocols

- The Transport Layer contains both connection-oriented and connectionless protocols
- Transmission Control Protocol (TCP) provides a connection-based, reliable, byte-stream service to programs
- User Datagram Protocol (UDP) provides a connectionless, unreliable transport service

TCP and UDP

- TCP transport is used for logging on, file and print sharing, replication of information between domain controllers, transfer of browse lists, and other common functions. TCP can only be used for one-to-one communications.
- UDP is often used for one-to-many communications, using broadcast or multicast IP datagrams

Protocol	Type	Example
Transmission Control Protocol (TCP)	Connection-oriented	Web browser
User Datagram Protocol (UDP)	Connectionless	Streaming media

—> TCP used for logging in and print sharing replication so basically

when you need acknowledgement

→ UDP is used in situations where packets can't be reset, one to many communications (broadcast), video streaming etc

Ports

- Ports are a Layer 4 protocol that a computer uses for data transmission
- Ports act as logical communications endpoint for specific program on computers for delivery of data sent
- There are a total of 65,536 ports, numbering between 0 and 65,535
- Ports are defined by the Internet Assigned Numbers Authority or IANA and divided into categories

Ports

Port Number	*Associated Protocol*	*Full Name*
21	FTP	File Transfer Protocol
22	SSH	Secure Shell
23	Telnet	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name System
80	HTTP	Hypertext Transfer Protocol
88	Kerberos	Kerberos
110	POP3	Post Office Protocol Version 3
119	NNTP	Network News Transfer Protocol
137–139	NetBIOS	NetBIOS Name, Datagram, and Session Services, respectively
143	IMAP	Internet Access Message Protocol
161	SNMP	Simple Network Management Protocol
389	LDAP	Lightweight Directory Access Protocol
443	HTTPS	Hypertext Transfer Protocol Secure (uses TLS or SSL)
445	SMB	Server Message Block
1701	L2TP	Layer 2 Tunneling Protocol
1723	PPTP	Point-to-Point Tunneling Protocol
3389	RDP	Remote Desktop Protocol (Microsoft Terminal Server)

→ A port number is added to IP address to access specific webpage or server

->A port number is 16-bits

0-65535

Layer 5- Session Layer

- The Session Layer manages session establishment, maintenance and termination between network devices
- Example: when you log on and log off
- This layer controls the name and address database for the OS
- NetBIOS (Network Basic Input Output System) is a protocol that works at this layer for associating names to computers

Layer 6- Presentation Layer

Layer 6 – Presentation Layer

- This layer translates the data format from sender to receiver in the various OSes that may be used
- Presentation Layer concepts include: character code conversion, data compression, and data encryption
- Redirectors work on this layer, such as mapped network drives that enable a computer to access file shares on a remote computer

Layer 7 - Application Layer

Layer 7 – Application Layer

- Serves as a the window for users and application processes to access network services
- This layer is where message creation begins
- End-user protocols such as FTP, SMTP, Telnet, and RAS work at this layer
- This layer is not the application itself, but the protocols that are initiated by this layer

→ The program itself is not application layer, it hooks into this layer

OSI Model Revisited

Layer	Protocol	Device
7 – Application	FTP, HTTP, POP3, SMTP	Gateway
6 – Presentation	Compression, Encryption	N/A
5 – Session	Logon/Logoff	N/A
4 – Transport	TCP, UDP	N/A
3 – Network	IP, ICMP, ARP, RIP	Routers
2 – Data Link	802.3, 803.5	NICs, Switches, Bridges, WAPs
1 – Physical	100BASE-T, 1000BASE-X	Hubs, Patch Panels, RJ45 Jacks

TCP Model

- The TCP/IP model is similar to the OSI model
- This model is composed of only four layers

Layer	Description	Protocols
Application Layer	Defines TCP/IP application protocols	HTTP, Telnet, FTP, SMNP, DNS
Transport Layer	Provides communication session management	TCP, UDP, RTP
Internet Layer	Packages and routes data	IP, ICMP, ARP, RARP
Network Interface	Details how data is physically sent through the network	Ethernet, Token Ring, Frame Relay

→ OSI physical layer is skipped altogether on TCP model