OSI Model Concepts

The standard model for networking protocols and distributed applications is the International Standard Organization's Open System Interconnect (ISO/OSI) model. It defines seven network layers.

Short for **Open System Interconnection**, an ISO standard for worldwide communications that defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

At one time, most vendors agreed to support OSI in one form or another, but OSI was too loosely defined and proprietary standards were too entrenched. Except for the OSI-compliant X.400 and X.500 e-mail and directory standards, which are widely used, what was once thought to become the universal communications standard now serves as the teaching model for all other protocols.

Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

Layer 1 - Physical

Physical layer defines the cable or physical medium itself, e.g., thinnet, thicknet, unshielded twisted pairs (UTP). All media are functionally equivalent. The main difference is in convenience and cost of installation and maintenance. Converters from one media to another operate at this level.

Layer 2 - Data Link

Data Link layer defines the format of data on the network. A network data frame, aka packet, includes checksum, source and destination address, and data. The largest packet that can be sent through a data link layer defines the Maximum Transmission Unit (MTU). The data link layer handles the physical and logical connections to the packet's destination, using a network interface. A host connected to an Ethernet would have an Ethernet interface to handle connections to the outside world, and a loopback interface to send packets to itself.

Ethernet addresses a host using a unique, 48-bit address called its Ethernet address or Media Access Control (MAC) address. MAC addresses are usually represented as six colon-separated pairs of hex digits, e.g., 8:0:20:11:ac:85. This number is unique and is associated with a particular Ethernet device. Hosts with multiple network interfaces should use the same MAC address on each. The data link layer's protocol-specific header specifies the MAC address of the packet's source and destination. When a packet is sent to all hosts (broadcast), a special MAC address (ff:ff:ff:ff:ff:ff) is used.

Layer 3 - Network

NFS uses Internetwork Protocol (IP) as its network layer interface. IP is responsible for routing, directing datagrams from one network to another. The network layer may have to break large datagrams, larger than MTU, into smaller packets and host receiving the packet will have to reassemble the fragmented datagram. The Internetwork Protocol identifies each host with a 32-bit IP address. IP addresses are written as four dot-separated decimal numbers between 0 and 255, e.g., 129.79.16.40. The leading 1-3 bytes of the IP identify the network and the remaining bytes identifies the host on that network. The network portion of the IP is assigned by InterNIC Registration Services, under the contract to the National Science Foundation, and the host portion of the IP is assigned by the local network administrators. For large sites, the first two bytes represents the network portion of the IP, and the third and fourth bytes identify the subnet and host respectively.

Even though IP packets are addressed using IP addresses, hardware addresses must be used to actually transport data from one host to another. The Address Resolution Protocol (ARP) is used to map the IP address to it hardware address.

Layer 4 - Transport

Transport layer subdivides user-buffer into network-buffer sized datagrams and enforces desired transmission control. Two transport protocols, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), sits at the transport layer. Reliability and speed are the primary difference between these two protocols. TCP establishes connections between two hosts on the network through 'sockets' which are determined by the IP address and port number. TCP keeps track of the packet delivery order and the packets that must be resent. Maintaining this information for each connection makes TCP a stateful protocol. UDP on the other hand provides a low overhead transmission service, but with less error checking. NFS is built on top of UDP because of its speed and statelessness. Statelessness simplifies the crash recovery.

Layer 5 - Session

The session protocol defines the format of the data sent over the connections. The NFS uses the Remote Procedure Call (RPC) for its session protocol. RPC may be built on either TCP or UDP. Login sessions uses TCP whereas NFS and broadcast use UDP.

Layer 6 - Presentation

External Data Representation (XDR) sits at the presentation level. It converts local representation of data to its canonical form and vice versa. The canonical uses a standard byte ordering and structure packing convention, independent of the host.

Layer 7 - Application

Provides network services to the end-users. Mail, ftp, telnet, DNS, NIS, NFS are examples of network applications.

OSI Model Reference Table

Layer	Function	Protocols	Network Components
Application User Interface	• Used for applications specifically written to run over the network • Allows access to network services that support applications; • Directly represents the services that directly support user applications • Handles network access, flow control and error recovery • Example apps are file transfer,e-mail, NetBIOS-based applications	DNS; FTP; TFTP; BOOTP; SNMP;RLOGIN; SMTP; MIME; NFS; FINGER; TELNET; NCP; APPC; AFP; SMB	Gateway
Presentation Translation	• Translates from application to network format and vice-versa • All different formats from all sources are made into a common uniform format that the rest of the OSI model can understand • Responsible for protocol conversion, character conversion,data encryption / decryption, expanding graphics commands, data compression • Sets standards for different systems to provide seamless communication from multiple protocol stacks • Not always implemented in a network protocol		Gateway Redirector
Session Syncs and Sessions	• Establishes, maintains and ends sessions across the network • Responsible for name recognition (identification) so only the designated parties can	NetBIOS Names Pipes Mail Slots	Gateway

	participate in the session • Provides synchronization services by planning check points in the data stream => if session fails, only data after the most recent checkpoint need be transmitted • Manages who can transmit data at a certain time and for how long • Examples are interactive login and file transfer connections, the session would connect and re-connect if there was an interruption; recognize names in sessions and register names in history	RPC	
Transport Packets; Flow control & Error-handling	• Additional connection below the session layer • Manages the flow control of data between parties across the network • Divides streams of data into chunks or packets; the transport layer of the receiving computer reassembles the message from packets • A train is a good analogy => the data is divided into identical units • Provides error-checking to guarantee error-free data delivery, with on losses or duplications • Provides acknowledgment of successful transmissions; requests retransmission if some packets don't arrive error-free • Provides flow control and error-handling	TCP, ARP, RARP; SPX NWLink NetBIOS / NetBEUI ATP	Gateway Advanced Cable Tester Brouter
Network Addressing; Routing	• Translates logical network address and names to their physical address (e.g. computername ==> MAC address)	IP; ARP; RARP, ICMP; RIP; OSFP;	Brouter Router

	• Responsible for
	  ○ addressing
	  ○ determining routes for sending
	  ○ managing network problems such as packet switching, data congestion and routing
	• If router can’t send data frame as large as the source computer sends, the network layer compensates by breaking the data into smaller units. At the receiving end, the network layer reassembles the data
	• Think of this layer stamping the addresses on each train car
		IGMP;
		
		IPX
		
		NWLink
		
		NetBEUI
		
		OSI
		
		DDP
		
		DECnet
			Frame Relay Device
			
			ATM Switch
			
			Advanced Cable Tester

Data Link Data frames to bits	• Turns packets into raw bits 100101 and at the receiving end turns bits into packets. • Handles data frames between the Network and Physical layers • The receiving end packages raw data from the Physical layer into data frames for delivery to the Network layer • Responsible for error-free transfer of frames to other computer via the Physical Layer • This layer defines the methods used to transmit and receive data on the network. It consists of the wiring, the devices use to connect the NIC to the wiring, the signaling involved to transmit / receive data and the ability to detect signaling errors on the network media	Logical Link Control • error correction and flow control • manages link control and defines SAPs 802.1 OSI Model 802.2 Logical Link Control — Media Access Control • communicates with the adapter card • controls the type of media being used: 802.3 CSMA/CD (Ethernet) 802.4 Token Bus (ARCnet)	Bridge Switch ISDN Router Intelligent Hub NIC Advanced Cable Tester

		802.5 Token Ring 802.12 Demand Priority	
Physical Hardware; Raw bit stream	• Transmits raw bit stream over physical cable • Defines cables, cards, and physical aspects • Defines NIC attachments to hardware, how cable is attached to NIC • Defines techniques to transfer bit stream to cable	IEEE 802 IEEE 802.2 ISO 2110 ISDN	Repeater Multiplexer Hubs • Passive • Active TDR Oscilloscope Amplifier