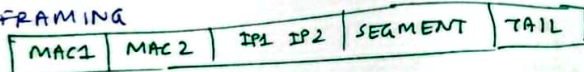

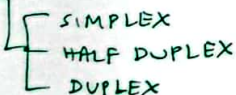


THE OSI MODEL					
LAYER	PROTOCOL DATA UNIT (PDU)	PURPOSES	PROTOCOLS SUPPORTED	DEVICES/SERVICES	ATTACKS
APPLICATION ⑦ <i>How application uses network</i>	DATA	<ul style="list-style-type: none"> - Resource sharing - Remote file access - Remote resource access - Directory services - Network management - Emails - Virtual terminals 	HTTP/S FTP SMTP POP3 Telnet LPD (Linux)	DNS server	<u>EXPLOIT</u> Malware SMTP attack FTP Bounce Data attack Ransomware
PRESENTATION ⑥ <i>Represent and display data</i>	DATA	(a) Translation → characters & numbers to binary format (0's and 1's) (b) Bit reduction/compression → lossless } Data conversion and compression (c) Encryption	ASCII UNICODE TIFF JPEG SSL		<u>PHISHING</u>
SESSION ⑤ <i>Establish communication</i>	DATA	DIALOG CONTROLLER: (a) Full duplex - 2 way communication between 2 devices at the same time (b) Half duplex - 1 way communication at a time SESSION MANAGEMENT - establish session - maintenance - terminate - support Authentication, authorization, tracking of files downloaded.	SQL NFS RPC	APIs Net BIOS	<u>HITACKING</u> - Cross site scripting - session side jacking - Malware cookie hijacking
TRANSPORT ④ <i>Provide reliable delivery</i>	SEGMENTS	SEGMENTATION - source and destination portnos. - sequencing FLOW CONTROL ERROR CONTROL - checksums CONNECTION ORIENTED TRANSMISSION → TCP CONNECTION LESS TRANSMISSION → UDP	TCP UDP	WWW Email FTP TFTP DNS online streaming	→ SYN flood → SYN packets → smurf attacks <u>DDOS attacks</u> <u>Reconnaissance attacks</u>

DDoS attacks

Reconnaissance attacks

OSI MODEL (cont'd)

LAYER	PDU	PURPOSES	PROTOCOLS	DEVICES/SERVICES	ATTACKS
NETWORK ③ Address assigning and packet forwarding	Packets	LOGICAL ADDRESSING PATH DETERMINATION ROUTING	IPV4, IPV6 Masking OSPF BGP IS-IS ICMP ARP Routing protocols	ROUTERS	<u>SPOOFING</u> IP spoofing DOS and DDOS Attacks MITM attacks ICMP flooding Ping of death
DATA LINK ② organizing data and transmitting	FRAMES	FRAMING  PHYSICAL ADDRESSING - media access control ERROR CONTROL FLOW CONTROL (Address resolution)	ATM CDP ARP (IP-MAC address linking) FDDI Frame Relay IEEE 802.11 MPLS	switches Bridges NIC device drivers of host machines	<u>MAC-SPOOFING</u> MAC Flooding Misconfigured devices vulnerable old firmware ARP poisoning DNS spoofing DHCP starvation
PHYSICAL ① Transmitted bits	BITS	BIT SYNCHRONIZATION BIT RATE CONTROL PHYSICAL TOPOLOGIES  TRANSMISSION MODE  ELECTRICAL SIGNALS TO BITS Fiber optics → PHOTONS Electrical voltage → ETHERNET Radio frequencies → WIRELESS	- Digital subscriber line - Infrared data association - USB - Bluetooth - Ethernet	Hubs Repeaters Modem cables coax / fiber	<u>SNIFING ATTACKS</u> Alter data bits. Environmental & Physical threats - Dust - water - power outage - rodents Vandalism Eavesdropping SNIPPING Hub-inserting

HARDWARE LAYER