OSI MODEL

7 - Application — serves as the window for users and application processes to access the network services
End user layer - Program opens what was sent or creates what is to be sent.
- Resource Sharing - Remote File Access - Remote Printer Access - Directory Services - Network Management SMTP; HTTP

6 - Presentation — Formats the data to be presented to the app. layer - Network Translator
Syntax Layer - Encrypt & Decrypt if needed
- Character code translation - Data conversion - Data Compression - Data Encryption - Character Set Translation
SPEC: ASCII; GIF; PICT;

5 Session PDU-DATA — Allows session establishment between processes running on different stations.
Synch & Send to Ports (Logical Ports) Session establishment Maintenance & termination - Session support - perform security, name recognition, logging, etc. - SQL, NFS, NetBIOS services

4 Transport — Messages delivered error free, in sequence with no losses or duplication
TCP - Host to Host, Flow control - Message Segmentation
Message ACK - Message Traffic Control - Session Multiplexing - TCP - UDP - SPX - PDU-SEGMENT

3 Network — controls operations of the subnet deciding which physical path data takes
Packets - "letter" contains IP Address - Routing - Subnet Traffic Control - Frame Fragmentation - Logical - Physical Address mapping - Subnet usage accounting - IP address
- ROUTERS - IPv4; IPv6; ICMP PDU-PACKET

2 DATA LINK PDU-FRAME — Provides error free transfer of frames from one node to another over the physical layer. ARP
Frames - "envelopes", contains MAC Address - End to End
NIC - switch - NIC - Establishes & Terminates the logical link between nodes - Frame Traffic Control - Frame Sequencing
Frame Ack. - Frame Error Checking - FCS - Frame Check Seq.
Media Access Control - MAC sublayer - LLC Sublayer

1 Physical PDU-BITS — concerned with the transmission & reception of raw bit stream
Physical Structure - Cables, Hubs, etc. - Data encoding, medium attachment - Transmission technique Copper vs. Fiber

MAC ADDRESS - Unique to each NIC - Layer 2 address (OUI) 48 bits in HEX
1st 3 bytes (6 bits) are Manufacturer specific - Last 3 are NIC Spec.
- Broadcast FF:FF:FF:FF:FF:FF Multicast - 01:00:5E: Unicast 00:07:E9

COMMANDS <CMD>

- ping → to show connectivity
- arp -a → Show arp table (MAC List)
- arp -d → clear arp table (MAC List)
- ipconfig → show windows IP table & MAC Addresses
- ipconfig /release → releases your IPv4 address
- ipconfig /renew → gets a new IPv4 address
- ipconfig /flushdns → clear your DNS entries
- ipconfig /displaydns → to show your DNS entries
- WIRESHARK - filter for bootp to show DHCP discover, request, renew, & offer
- TCP - →RFC793 Transmission Control Protocol - reliable Layer 4 protocol with Flow Control & ordered data reconstruction. Connection Oriented - 3 Way Handshake
- UDP - RFC 768 User Datagram Protocol - connectionless, unreliable layer 4 protocol - NO Flow control or data reconstruction. Software Protocol HTTP - FTP - SMTP - TELNET
- DNS - Domain Name System - A Layer 7 protocol used to resolve host names to IP addresses. google.com = 173.194.43.82
- FTP - File Transfer Protocol - Layer 7 protocol used for interactive File Transfer between systems
- HTTP - Hypertext Transfer Protocol - Layer 7 protocol used to transfer Web pages (TCP)
- DHCP - Dynamic Host Configuration Protocol - Layer 7 protocol used to automatically assign an IP address, subnet mask, default gateway & DNS server address to a host - Home Router

BROADCAST IPv4 ADDRESS 0.0.0.0 255.255.255.255
MULTICAST IPv4 224.0.0.0 to 239.255.255.255
NETWORK - CIDR NOTATION IS SUBNET → /24 means 1st 24 bits are part of the network. # of hosts is value of 24th bit minus 2. Network address has all zeros - Broadcast has all 1's. 1st usable address is Network +1; last usable is Network Broadcast -1.

CISCO COMMANDS

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#banner motd #....
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
  → service password-encryption
R1(config)#interface gigabitethernet 0/0
  or interface fastethernet 0/0
R1(config-if)#ip address 192.. 255...
R1(config-if)#no shutdown
```

Configure Default Gateway on Switch
→ While in Vlan

```
S1(config)#interface vlan 1
S1(config-if)#ip address 192.. 255...
S1(config-if)#no shutdown
S1(config-if)#description LINK TO...
S1(config-if)#exit
S1(config)#ip default-gateway ...
R1(config)#ip route 200.. 255.. 192...
R1(config)#copy running-config startup
```

CHAPTER 5 - ETHERNET Layer 1 & 2

- IEEE 802.2 & 802.3
- speeds up to 100 Gbps
- LLC & MAC Sublayers
  - Handles communication between upper & lower layers. MAC → lower sublayer of Data Link layer - Implemented by hardware - usually by NIC - responsible for Data Encapsulation & Media Access Control
  - adds a header & trailer to PDU
  - → Frame delimiting; MAC Addressing; error check (CRC)
- LLC → Carrier Sense Multiple Access (CSMA)
  - Ethernet - CSMA/CD - detection
- 802.11 → WiFi - CSMA/CA - avoidance

SIZE	8	6	6	2	46-1500	4
ETHERNET II	Preamble	Destination Address	Source Address MAC	TYPE	802.2 Header & DATA	FCS

MINIMUM SIZE = 64 BYTES ← contained in FCS
MAXIMUM SIZE = 1518 BYTES — If FCS doesn't match or if size is < 64 or > 1518 frame is dropped

ARP Table - used to find addresses (IP & MAC)
ARP REQUEST - Layer 2 broadcast to all devices on LAN - if no device responds packet is dropped

LOCAL NETWORK - Uses MAC Address. Otherwise Default Gateway IPv4 address is used.
IF SWITCH receives ARP it sends request out all ports except one received on
- SWITCH saves info to its address table

SWITCH → Store & Forward - checks CRC
- Cut THROUGH - reads destination address & sends PDU frame
Fast Forward / Fragment Free - stores 1st 64 bytes & sends
→ Most errors occur in 1st 64 Bytes.

Layer 2 Switch vs. Layer 3 Switch
- Switching only ← also acts as router
- Switched Virtual Interface SVI (associated w/ LAN)
- ROUTED PORT - use no switchport cmd.
- ETHER CHANNEL - bundle of routed ports.

CHAPTER 6 - NETWORK LAYER

- End 2 End transport processes - addressing end devices; encapsulation; routing; de-encap
- IPv4 & IPv6 are Network/Layer 3 Protocols
- → OUTDATED/LEGACY → IPX; AppleTalk; CLNS/DECNet
- IP is Connectionless ⇒ packets are just sent
  - → Nothing in header to establish or keep connection
  - → LESS OVERHEAD; Best Effort Delivery

IPv4 headers → TTL → HOP Count / Time to Live (bytes)
- → Version; Length; Services; Total Length; 4
- → ID; Flag; Fragment offset; 4
- → Time to Live; Protocol; Header Checksum; 4
- → SOURCE IP ADDRESS → 4
- → DESTINATION IP ADDRESS → 4
- → Options; padding; 4

IPv6 → 128 BIT ADDRESS vs. 32 BIT IN IPv4
- → improved packet handling (simple header)
- → eliminates the need for NAT
- → Integrated security (Built in support for IPsec)
- → 4 Billion IPv4 addresses vs. 000 000 000 000
- → 340 UNDECILLION IPv6 → 340,000 000 000 000 000 000 000 000
- → IPv6 header is still only 4 bytes wide
- → Version; Traffic Class; Flow Label
- → Payload Length; Next Header; Hop Limit
- → Source IPv6 Address
- → Destination IPv6 Address

<CMD> netstat -r → shows routing table
- → ON ROUTING TABLE - METRIC is Distance to something. lower = use that first
Router examines L3 header for destination network address; if there is a match in the routing table, packet is forwarded; if not - dropped
NO ROUTE = ICMP destination host unreachable

ROUTER is a computer
- RAM (Volatile) - Running IOS; Running configuration file; IP routing & arp tables; Packet buffer
- ROM (Non-Vol) - Bootup instructions; Basic diagnostic software; Limited IOS
- NVRAM (Non-Vol) - Startup Config File
- Flash (Non-Vol) - IOS; Other System files

CHAPTER 7 - Transport Layer Protocols

- → Transport Layer moves data between apps on host
- → The transport layer tracks each conversation flowing between a source application & destination application separately - so you can have many app running
- → Transport layer segments the data for transport
- TCP - reliable acknowledged delivery
- UDP - just sends; unreliable - less overhead. Used by DNS; VoIP; Video Streaming; DHCP

PORT Numbers are used by TCP & UDP for each app.
- 0-1023 → Well Known Contact Ports
- 1024-49151 - Registered Ports
- 49152-65535 - Private and/or Dynamic Ports

Well known Ports - reserved for specific apps
- 21 → FTP; 23 → Telnet; 25 SMTP; 80 HTTP
- 110 → POP3; 194 → IRC; 443 HTTPS (Secure HTTP)
- 69 → TFTP; 520 → RIP ← UDP - TCP ← COMMON
- 53 - DNS; 161 SNMP; 531 AOL IM, IRC

REGISTERED PORTS: TCP - 1863 - MSN Messenger
2000 Cisco SCCP (VoIP); 8008 & 8080 → Alternate HTTP
UDP → 1812 - RADIUS Authentication Protocol;
5004 RTP (Voice & Video Transport Protocol)
5060 SIP (VoIP) COMMON → 1433 - MS SQL;
2948 WAP (MMS)
<CMD> netstat → used to see TCP connections that are open & running

TCP Three Way handshake
- establish that the destination device is present
- verifies device has active service & is accepting requests on that port number that client will use
- informs the destination device that the source client intends to establish a connection on that port #

HOST A → SEND SYN → SEND SYN ACK → SYN RECD ← RECD ← CTL=SYN,ACK ← HOST B
ESTABLISHED CTL=ACK
CTL → Which control bits are set to 1. SYN - Sequence Number
Host A sends ACK response to B
The window size determines the number of bytes sent before an acknowledgement is expected.
The acknowledgement number is the number of the next expected byte.

PORTS provide a "tunnel" for data to get from the Transport Layer to the appropriate application at the destination.

MASK	128	64	32	16	8	4	2	1	CIDR	# OF NET
255	1	1	1	1	1	1	1	1		
254	1	1	1	1	1	1	1	0	/31	128
252	1 2	1	1	1	1	1 2	0	0	/30	64
248	1 6	1	1	1	1 6	0	0	0	/29	32
240	1 14	1	1	1 14	0	0	0	0	/28	16
224	1 30	1	1 30	0	0	0	0	0	/27	8
192	1 62	1 62	0	0	0	0	0	0	/26	4
128	1 126	0	0	0	0	0	0	0	/25	2
254 0	0 254	0	0	0	0	0	0	0	/24	1

PRIVATE IPv4 Address Blocks
- → hosts that do not require internet access
- → 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
- → 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
- → 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)

SHARED ADDRESS SPACE
- not globally routable
- used by ISP's → 100.64.0.0/10

LOOPBACK ADDRESS → 127.0.0.1 (127.0.0.0/8) reserved
LINK-LOCAL ADDRESS → 169.254.0.0/16 can be auto assigned locally
TEST-NET → 192.0.2.0/24 → teaching & learning reserved
EXPERIMENTAL 240.0.0.0 to 255.255.255.254 are reserved.
FORMAL NAME CIDR - Classless Interdomain Routing

TO ADD A STATIC ROUTE TO CISCO ROUTER
<Command><option><Remote Network Address><Subnet Mask><Next hop IP address>
ip route 192.168.200.0 255.255.255.0 205.211.30.2
- this means to get to network 192.168.200.0/24 forward the packets to 205.211.30.2 ← Default gateway