Computer Networking

1. TCP/IP 5 layer n/w model
    1. physical → cables, connectors → bits
    2. data link → ethernet, wifi → frames → MAC addr
    3. network → IP → datagram → IP addr
    4. transport → tcp/udp → segment → ports
    5. application → http, smtp, messages
2. Networking devices:
    1. hub (physical layer, only 1 m/c can send data at a time → collision domain)
    2. switch (data link layer)
    3. router (network layer → BGP(border gateway protocol) → tells optimal path to the router for routing)
    4. servers-clients
3. DHCP - dynamic host configuration protocol
    1. gives dynamic IP address
    2. configures subnet mask, gateway for a host
    3. assigns NTP server → keeps all computers on a n/w synchronized in time
    4. DHCP discovery process
        1. dhcp client on the host sends dhcp discover broadcast msg
        2. dhcp lease
4. NAT - n/w address translation
    1. security safeguards → IP masquerading (hiding IP of a computer from

others)
    1. one-to-many NAT
2. preserving limited amounts of available IPv4 space
3. technique that allows a gateway(router/firewall) to rewrite the source IP of an outgoing datagram while retaining the original IP in order to rewrite it in the response
4. port preservation
5. port forwarding (sender only needs to know the IP of the receiver)

5. IP address classes
    1. class A,B,C
    2. cidr → classless inter-domain routing
6. Firewall → at transport layer
7. Configurations for a host to operate on a n/w
    1. IP addr
    2. subnet mask
    3. gateway for a host
    4. DNS server
8. FQDN - fully qualified domain name
    1. 255 chars
    2. hostname/subdomain.domain.topLevelDomain
    3. host.sub.sub.subdomain.domain.topLevelDomain
9. DNS server
    1. caching name server
    2. recursive name server
    3. root name server
    4. TLD name server (top level domain) → ICANN (Internet corporation for assigned names and numbers)
    5. Authoritative name server (dns zones, ns records - name servers responsible for the zone)
    6. resource record types:
        1. A record (domain name → IPv4 addr)
            1. a single domain name can have multiple IPs (round robin)

    2. AAAA - Quad A record (IPv6)
    3. cname record (domain name1 → domain name2)
    4. MX - mail exchange record (email server)
    5. SRV - service record
    6. TXT - text record (additional notes/config/data)
    7. PTR - pointer resource record (resolves IP to name/fqdn → reverse lookup)
10. IANA - in-charge of distributing IP addresses
11. TCP connection
    1. 3-way handshake (1syn, 2syn/ack, 1ack)
    2. 1req, 2ack
    3. 2resp, 1ack
    4. 4-way handshake (2fin, 1ack, 1fin, 2ack)
12. sockets
    1. tcp
    2. udp → streaming video, VPNs
    3. raw → ping uses raw socket to send ICMP packets
    4. unix → to talk to programs on the same computer
13. SSL → newer version is TSL
14. VPN
    1. vpn tunnel
    2. 2-factor authentication
    3. remote client → vpn tunnel → (router → VPN server)
    4. tunneling protocol
15. proxies
    1. server that acts on behalf of a client
    2. web proxy
    3. gateway
    4. reverse proxy → single frontend for many servers behind it
    5. encryption/decryption

16. Protocols:
    1. ARP - address resolution protocol
        1. used to discover h/w addr (MAC addr) of a node with a certain IP addr
        2. n/w devices maintain a local ARP table (IP addr: MAC addr)
        3. ARP broadcast
        4. `arp -na` cmd to see the mappings of arp table
17. Ports
    1. 53 - dns udp
    2. 80 - http
    3. 443 - https
    4. 67 - dhcp server
    5. 68 - dhcp client
    6. 20 - ftp
    7. 25 - smtp
18. Verifying connectivity:
    1. ping
        1. icmp (internet control message protocol) → protocol used to communicate network errors
        2. destination unreachable → host/port
        3. time exceeded
    2. traceroute/mtr
    3. netcat/nc → testing port connectivity
        1. nc <host> <port>
19. Digging into dns:
    1. nslookup → set debug
    2. nslookup <domain>
    3. /etc/hosts → loopback addr → 127.0.0.1 localhost

Resources:

1. Coursera: Bit and bytes of networking
2. https://jvns.ca/networking-zine.pdf