CSE 461 Notes

Contents

1 Networks **4**
1.1 Network Components . . . 4
1.2 Types of Links . . . 4
1.3 Network Scales . . . 4
1.4 Network Layers . . . 4
1.5 Protocols . . . 5
1.6 Encapsulation . . . 5

2 Transport Layer **6**
2.1 UDP . . . 6
2.2 TCP . . . 6
2.3 TCP Establishment . . . 6
2.4 TCP Release . . . 6
2.5 TCP Flow Control . . . 7
2.6 Stop-and-Wait . . . 7
2.7 Sliding Window . . . 7
2.8 Go-Back-N . . . 7
2.9 Selective Repeat . . . 7
2.10 ACK Clocking . . . 8
2.11 Network Congestion . . . 8
2.12 Bandwidth Allocation . . . 8
2.13 Max-Min Fairness . . . 8
2.14 TCP Congestion Control . . . 8
2.15 AIMD . . . 9
2.16 Slow Start . . . 9
2.17 Fast Retransmit . . . 9
2.18 Fast Recovery . . . 9
2.19 TCP Variants . . . 10
2.20 TCP Congestion Avoidance . . . 10
2.21 ECN . . . 10

3 Network Layer **11**
3.1 Network Layer . . . 11
3.2 Datagram Forwarding Model . . . 11
3.3 Virtual Circuit Forwarding Model . . . 11
3.4 Datagram vs. Virtual Circuit . . . 11
3.5 DHCP . . . 12
3.6 ARP . . . 12
3.7 ICMP . . . 12
3.8 Traceroute . . . 12
3.9 NAT . . . 13
3.10 IPv6 . . . 13
3.11 Routing Algorithms . . . 13
3.12 Rules of Distributed Routing . . . 13
3.13 Hierarchical Routing . . . 14
3.14 Longest Prefix Matching . . . 14

4 Application Layer **15**
4.1 Session Layer . . . 15
4.2 Presentation Layer . . . 15
4.3 Name and Address Resolution . . . 15
4.4 DNS . . . 15
4.5 DNS Namespace . . . 15
4.6 DNS Zones . . . 15
4.7 DNS Nameservers . . . 16
4.8 DNS Protocol . . . 16
4.9 Recursive Queries . . . 16
4.10 Iterative Queries . . . 16
4.11 DNS Query Process . . . 17
4.12 DNS Resource Types . . . 17

5 HTTP **18**
5.1 HTTP . . . 18
5.2 HTTP Commands . . . 18
5.3 HTTP Responses . . . 18
5.4 HTTP Fetch Process . . . 18
5.5 DOM . . . 19
5.6 PLT . . . 19
5.7 Parallel Connections . . . 19
5.8 Persistent Connections . . . 19
5.9 Web Caching . . . 20

6 Network Security **21**
6.1 Message Confidentiality . . . 21
6.2 Symmetric Encryption . . . 21
6.3 Asymmetric Encryption . . . 21
6.4 Hybrid Encryption . . . 21
6.5 Message Integrity . . . 21
6.6 Message Authenticity . . . 21
6.7 Message Authentication Codes . . . 22
6.8 Digital Signatures . . . 22
6.9 Message Digest . . . 22
6.10 Message Freshness . . . 22
6.11 Message Replay Attacks . . . 22

7 Web Security **23**
7.1 HTTPS . . . 23
7.2 SSL/TLS . . . 23
7.3 Certificates . . . 23
7.4 Certificate Authorities . . . 23
7.5 VPN . . . 23
7.6 Tunneling . . . 23
7.7 IPSEC . . . 24
7.8 VPN Connection Process . . . 24
7.9 DDoS . . . 24
7.10 Ingress Filtering . . . 24

8 Physical Layer **25**
8.1 Physical Layer . . . 25
8.2 Twisted Pair Cables . . . 25
8.3 Coaxial Cables . . . 25
8.4 Fiber Optic Cables . . . 25
8.5 Wireless Media . . . 25
8.6 Multipath . . . 25
8.7 Coding . . . 25

8.8 Clock Recovery . . . 26
8.9 Non-Return to Zero . . . 26
8.10 Return to Zero . . . 26
8.11 4B/5B . . . 26
8.12 Modulation . . . 26
8.13 Nyquist Sampling Theorem . . . 26
8.14 Shannon Capacity Theorem . . . 27
8.15 Nyquist Sampling Theorem vs. Shannon Capacity Theorem . . . 27

9 Link Layer **28**
9.1 Link Layer . . . 28
9.2 Framing . . . 28
9.3 Fixed-Size Framing . . . 28
9.4 Byte Count Framing . . . 28
9.5 Byte Stuffing . . . 28
9.6 Error Detection and Correction . . . 28
9.7 Error Detection vs. Correction . . . 29
9.8 Check Bits . . . 29
9.9 Hamming Distances . . . 29
9.10 Hamming Codes . . . 29
9.11 Parity Bits . . . 29
9.12 Checksums . . . 30
9.13 Multiplexing . . . 30
9.14 Time Division Multiplexing . . . 30
9.15 Frequency Division Multiplexing . . . 30
9.16 Statistical Multiplexing . . . 30
9.17 Multiple Access Control Protocols . . . 30
9.18 ALOHA Protocol . . . 31
9.19 CSMA Protocol . . . 31
9.20 CSMA/CD Protocol . . . 31
9.21 Binary Exponential Backoff . . . 31
9.22 Wireless Network Complications . . . 31

1 Networks

1.1 Network Components

- Application: generates messages (i.e. browser, video-conferencing software)
- Host: runs the application (i.e. laptops, phones)
- Router: relays messages across links (i.e. access point, cable modems)
- Link: carries messages (i.e. wires, wireless connections)

1.2 Types of Links

- Full-duplex: bidirectional, both directions simultaneously
- Half-duplex: bidirectional, one way at a time
- Simplex: unidirectional

1.3 Network Scales

- Personal Area Network (PAN)
  - Immediate vicinity (i.e. Bluetooth)
- Local Area Network (LAN) & Data Center Network (DCN)
  - Building-wide (i.e. WiFi, Ethernet)
- Metropolitan Area Network (MAN)
  - City-wide (i.e. Cable, DSL)
- Wide Area Network (WAN)
  - Country-wide (i.e. Large ISP)
- Internet:
  - Planet-wide

1.4 Network Layers

Network layers represent levels of abstraction. The most complex layers are at the bottom and the most abstract layers are at the top

- Application layer: programs that make use of networks
- Transport layer: provides end-to-end data delivery
- Network layer: sends packets over multiple networks
- Link layer: sends frames over one or more links
- Physical layer: sends bits using signals

1.5 Protocols

Protocols are a set of rules and procedures that implement the functionality of their corresponding layer. A set of protocols in use is called a protocol stack

- Protocol instances only use the services of the lower layer
- Protocol instances virtually communicate to other instances of the same protocol

1.6 Encapsulation

Encapsulation is the process of adding protocol-specific headers and trailers to packets of data as it flows down the network layers

- Identifies the protocols used by the data
- Provides information about the data, such as source and destination addresses, the length of the data, and any error checking information

2 Transport Layer

2.1 UDP

User Datagram Protocol (UDP) is a lightweight transport layer protocol

- Connectionless datagram oriented protocol
- Provides unreliable, unordered delivery of data
- Data may be duplicated or lost
- Does not implement flow control and congestion control mechanisms

2.2 TCP

Transmission Control Protocol (TCP) is a byte-stream-oriented transport layer protocol

- Connection oriented protocol
- Provides a reliable, ordered delivery of data
- Data is delivered exactly once
- Implements flow control and congestion control mechanisms to ensure that data is transmitted at an optimal rate

2.3 TCP Establishment

A TCP connection is established via a three-way handshake

1. Client sends $\mathrm{SYN}(\mathrm{x})$
2. Server replies with $\mathrm{SYN}(\mathrm{y}) + \mathrm{ACK}(\mathrm{x}+1)$
   - Once the client receives this, it can start sending to the server
3. Client replies with $\mathrm{ACK}(\mathrm{y}+1)$
   - Once the server receives this, it can start sending to the client

2.4 TCP Release

A TCP connection is released via the following steps

1. First party sends $\mathrm{FIN}(\mathrm{x})$
   - This indicates that the first party is done with the connection
2. Second party sends $\mathrm{ACK}(x+1)$
3. Second party sends $\mathrm{FIN}(\mathrm{y})$
   - This indicates that the second party is done with the connection
4. First party sends $\mathrm{ACK}(\mathrm{y}+1)$

2.5 TCP Flow Control

A TCP connection matches transmission speed to the receiver's reception capacity using flow control

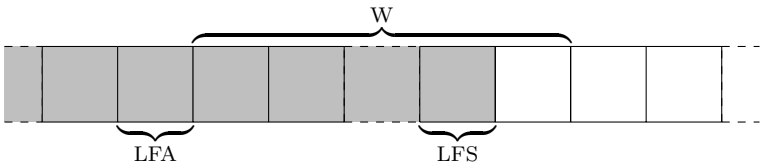
- Prevents a fast sender from overwhelming a slow receiver

2.6 Stop-and-Wait

Stop-and-Wait is a flow control method where only one packet is sent at a time

- Sender sends one packet at a time
- Sender can only send the next packet after receiving an acknowledgment for the previous one

2.7 Sliding Window



Sliding window is a flow control method where W outstanding packets are allowed at a time

- Sender keeps track of $\mathrm{Last\ Frame\ Sent}$ (LFS) and $\mathrm{Last\ Frame\ Acknowledged}$ (LFA)
- Sender sends packets while $\mathrm{LFS} - \mathrm{LFA} \leq \mathrm{W}$
- If $\mathrm{LFA} + 1$ is acknowledged, then LFA is incremented and the window advances

The sliding window is also called the congestion window (cwnd) in congestion control

2.8 Go-Back-N

Go-Back-N is a protocol that retransmits data in the event of a packet loss

- The receiver sends cumulative acknowledgments
  - i.e. if the receiver acknowledges packet 5, then it also acknowledges packets $1, 2, 3, 4$
- If the sender does not receive an acknowledgment within a timeout period, then it retransmits all the packets that have not been acknowledged
  - i.e. if the sender sends packets $5, 6, 7, 8, 9$, but only packet 5 is acknowledged, then the sender assumes that packets $6, 7, 8, 9$ are lost and retransmits them

2.9 Selective Repeat

Selective repeat is a protocol that retransmits data in the event of a packet loss

- The receiver sends cumulative and selective acknowledgments
  - i.e. if the sender sends packets $5, 6, 7, 8, 9$ and packet 6 is lost, then the receiver cumulatively acknowledges packet 5 and selectively acknowledges packets $7, 8, 9$
- If the sender does not receive an acknowledgment within a timeout period, then it retransmits all the packets that have not been acknowledged

  - i.e. if the sender sends packets $5, 6, 7, 8, 9$ and packet 6 is lost, then the receiver cumulatively acknowledges packet 5 and selectively acknowledges packets $7, 8, 9$. The sender only retransmits packet 6

2.10 ACK Clocking

ACK clocking is an emergent packet transmission control/clocking mechanism induced by the network

- If there is a slow link in the network, then transmitted packets become spread out and arrive at greater intervals
- The acknowledgments to these packets are transmitted and are received at greater intervals
- The sliding window advances more slowly such that the transmission rate decreases

2.11 Network Congestion

Network congestion occurs when there are more packets in the network than it can handle

- Transmission delay increases since more packets are buffered
- Drop rate increases since buffers cannot absorb all incoming packets
- Goodput rate drops since retransmitted packets clog up the network

2.12 Bandwidth Allocation

The network must allocate its bandwidth such that its resources are utilized efficiently, while still fairly distributed among senders

- Efficiency: the network's resources should be utilized as much as possible while still avoiding congestion
- Fair: the network's resources should be allocated as evenly as possible to ensure equal access to the network

2.13 Max-Min Fairness

Max-min fair allocation is a method of allocating network resources such that increasing the rate of any flow will decrease the rate of a smaller flow

- In effect, this maximizes the minimum flow

2.14 TCP Congestion Control

A TCP connection matches transmission speed to the network's capacity using congestion control

- Prevents a fast sender from overwhelming a slow network
- Unlike congestion avoidance, congestion control manages network traffic once congestion is detected

2.15 AIMD

Additive Increase Multiplicative Decrease (AIMD) is a congestion control protocol to achieve max-min fair allocation

- If the network is not congested, then senders additively increase transmission rates
- If the network is congested, then senders multiplicatively decrease transmission rates
- Senders converge to max-min fair allocation

2.16 Slow Start

Slow start is an algorithm used by TCP to quickly increase the transmission rate when establishing a new connection or when recovering from packet loss

- Slow start phase
  - Start with cwnd set to the initial window size and $\mathrm{ssthresh}$ set to infinity
  - Double cwnd with each $\mathrm{round\ trip\ time\ (RTT)}$
  - Achieved by incrementing cwnd with each received acknowledgment
  - Switch to the additive increase phase once cwnd exceeds $\mathrm{ssthresh}$
- Additive increase phase
  - Increment cwnd with each RTT
  - Achieved by adding $\frac{1}{\mathrm{cwnd}}$ to cwnd with each received acknowledgment
  - The current congestion window size is given by $\lfloor \mathrm{cwnd} \rfloor$
  - Set $\mathrm{ssthresh}$ to $\frac{\mathrm{cwnd}}{2}$, reset cwnd to the initial window size, and switch to the slow start phase once packet loss occurs

2.17 Fast Retransmit

Fast retransmit is a mechanism used by TCP to quickly detect and retransmit lost packets without waiting for a timeout to expire

- If the sender receives three duplicate acknowledgments, then it considers the next unacknowledged packet as lost and retransmits all packets that have not been acknowledged
- i.e. if the sender sends packets $5, 6, 7, 8, 9$ and receives acknowledgments $5, 5, 5, 5$, then the sender retransmits packets $6, 7, 8, 9$

2.18 Fast Recovery

Fast recovery is a mechanism used by TCP which enables fast retransmit to retransmit lost packets while still maintaining a high transmission rate

- If the sender receives three duplicate acknowledgments, then the sender performs fast retransmit and multiplicatively decreases cwnd
- The sender uses the duplicate acknowledgments to infer which packet was lost and which packets were received
- This allows the sender to advance the congestion window and transmit more packets without waiting for the lost packet to be acknowledged
- i.e. if the sender sends packets $5, 6, 7, 8, 9$ and receives acknowledgments $5, 5, 5, 5$, then it can infer that packet 6 was lost and packets $7, 8, 9$ were received. The sender can then retransmit packet 6 and send packets $10, 11, 12, 13$

2.19 TCP Variants

- TCP Tahoe
  - Makes use of slow start
  - In the event of a packet loss, it sets $\mathrm{ssthresh}$ to $\frac{\mathrm{cwnd}}{2}$, resets cwnd to the initial window size, and switches to the slow start phase
- TCP Reno
  - Makes use of slow start, fast retransmit, and fast recovery
  - In the event of a packet loss, it sets $\mathrm{ssthresh}$ and cwnd to $\frac{\mathrm{cwnd}}{2}$, and switches to the additive increase phase

2.20 TCP Congestion Avoidance

A TCP connection avoids congesting the network using congestion avoidance

- Unlike congestion control, congestion avoidance manages network traffic even before congestion is detected

2.21 ECN

Explicit Congestion Notification (ECN) is a congestion avoidance protocol that provides an early indication of network congestion before packet loss occurs

- If a router detects that its buffers are starting to fill up, it marks a flag in the IP header of packets
- When the receiver receives a marked packet, it includes this mark in its acknowledgment to the sender
- The sender becomes aware that the network is starting to get congested and slows down
- Advantages
  - Congestion is detected early before packet loss occurs
  - No extra packets need to be sent
- Disadvantages
  - Routers and hosts must be upgraded to support ECN
  - Additional processing may introduce overhead and result in increased latency

3 Network Layer

3.1 Network Layer

The network layer serves three purposes

- Inter-networking: connects different link layer networks together
- Addressing: provides a globally unique way to address hosts
- Routing and forwarding: finds and traverses paths between hosts
  - Routing: the process of deciding the direction in which to send packets
  - Forwarding: the process of moving packets across the network

3.2 Datagram Forwarding Model

In the datagram forwarding model, each packet is treated as an independent entity and is forwarded by the routers based on the destination address in the packet header

- Routers maintain forwarding tables that map destination addresses to the next router to which packets should be forwarded

3.3 Virtual Circuit Forwarding Model

In the virtual circuit forwarding model, packets are transmitted over a virtual circuit that is established between the source and destination devices. Transmission involves the following phases

- Setup phase
  - The connection is established and the circuit is set up
  - A path is chosen and the forwarding information is stored in the routers
- Data transfer phase
  - Packets are transmitted along the virtual circuit
  - Routers maintain forwarding tables that map circuit numbers to the next router to which packets should be forwarded
- Teardown phase
  - The circuit is deleted and the connection is closed
  - Forwarding information is removed from routers

3.4 Datagram vs. Virtual Circuit

- In the datagram model, there is no setup phase
- In the datagram model, routers maintain state for each destination address while in the virtual circuit model, routers maintain state for each connection
- In the datagram model, packets carry the full destination address while in the virtual circuit model, packets carry short labels

3.5 DHCP

Dynamic Host Configuration Protocol (DHCP) is a broadcast protocol that enables nodes to obtain IP addresses and other network parameters from a DHCP server

- When a node wants to join a network, it broadcasts a DHCP request message to all nodes on the link-layer network
- The DHCP server receives this request and sends a DHCP response message with the necessary network parameters offering an available IP address
- The node requests this IP address and the DHCP server acknowledges
- To renew the lease on the IP address, the node requests the IP address and the DHCP server acknowledges

3.6 ARP

Address Resolution Protocol (ARP) is a broadcast protocol that maps network-layer IP addresses to link-layer MAC addresses

- When a node wants to send packets to another node on the local network, it needs the MAC address of the destination
- The sender checks its ARP cache for the appropriate IP-to-MAC address mapping
- If the destination IP address is not in the cache, the sender broadcasts an ARP request message to all nodes on the local network
- The node with the requested IP address receives this request and sends an ARP response message containing its MAC address
- The sender adds this IP-to-MAC address mapping to its ARP cache

3.7 ICMP

Internet Control Message Protocol (ICMP) is a companion protocol to IP used to report errors and provide diagnostic information related to IP packet delivery

- When a router encounters an error while forwarding, it sends an ICMP error report back to the IP source

3.8 Traceroute

Traceroute is a network diagnostic tool used to trace the path of an IP packet from the source node to the destination node

- Traceroute sends probe packets with increasing $\mathrm{time\ to\ live}$ (TTL), starting with one
- When the TTL on the packet reaches 0, a time exceeded ICMP error message is reported back to the source
- These ICMP error messages identify routers on the path

3.9 NAT

Network Address Translation (NAT) is a technique used to allow multiple hosts on a private network to share a single public IP address

- A NAT box maintains an internal/external translation table that maps each private IP address to a public IP address and port
- The NAT box intercepts packets and rewrites the source or destination IP address and port according to the translation table
- Advantages
  - Conserves IP addresses and alleviates address scarcity
  - Provides security by hiding the private IP addresses of hosts in the network
- Disadvantages
  - Can break applications that rely on IP address information
  - Can break peer-to-peer applications which rely on direct connections between hosts

3.10 IPv6

IPv6 is a version of IP developed to address the limitations of IPv4

- IPv6 uses a 128-bit address space
- Addresses are written as 8 groups of 4 hex digits
- IPv6 only has public addresses with no need for NAT boxes
- IPv6 has a simpler header format reducing the amount of header processing required
- IPv6 supports IPsec by default

3.11 Routing Algorithms

Routing algorithms must satisfy the following properties

- Correctness: paths must work
- Efficiency: paths must utilize network bandwidth efficiently
- Fair: paths must not starve any nodes
- Fast convergence: algorithm must recover quickly after changes
- Scalability: algorithm must work well as network scales

3.12 Rules of Distributed Routing

- All nodes are alike. There is no controller
- Nodes learn by exchanging messages with neighbors
- Nodes operate concurrently
- There may be node, link, and message failures

3.13 Hierarchical Routing

Hierarchical routing is a technique used to improve the scalability and efficiency of routing algorithms in large-scale networks

- The network is divided into a number of regions/domains each corresponding to an IP prefix
- Regions/domains are connected to one another through gateway routers
- Packets are first routed to a region/domain, and then to the appropriate subregion/subdomain

3.14 Longest Prefix Matching

Longest prefix matching is a technique used to determine the most specific matching route for a given destination IP address

- Nodes maintain forwarding tables that map IP address prefixes to routes
- The route associated with the longest prefix matching the destination IP address is selected
- Advantages
  - Works well with the hierarchical nature of IP addresses
  - Flexible as it can provide both default behavior and special case behavior
- Disadvantages
  - Forwarding tables can be very large
  - Lookup is complex and can increase latency

4 Application Layer

4.1 Session Layer

The session layer maintains a series of related network connections in support of an application task

- i.e. a Skype call requires individual connections for audio, video, and chat

4.2 Presentation Layer

The presentation layer formats, encrypts, compresses, and encodes data such that it can be exchanged and identified by networked devices

- i.e. media types (MIME) identify content type such as image/jpeg

4.3 Name and Address Resolution

- Resolution: the process of mapping a name to an address
- Names: higher-level identifiers for resources
- Addresses: lower-level locators for resources

4.4 DNS

The Domain Name System (DNS) is a system of naming servers that maps host names to their IP address

- Uses a distributed directory based on a hierarchical namespace
- Uses an automated protocol to merge updates
- Efficient and easy to manage on a large scale

4.5 DNS Namespace

The DNS namespace refers to the hierarchical structure of domain names within the DNS system

- Structured in a tree-like format, with each level of the hierarchy separated by dots
- The root of the tree is known as the root domain, represented by a single dot
- Below the root domain are the top-level domains (TLDs) such as .com, .org, .edu, .gov, etc
- Below the TLDs are the second-level domains (SLDs) which can be registered and owned by individuals, organizations, or entities

4.6 DNS Zones

A DNS zone refers to a portion of the DNS namespace that is managed by a specific entity

- Any subtree within the DNS hierarchy represents a DNS zone

4.7 DNS Nameservers

A DNS nameserver is the root of a DNS zone. It is authoritative for the zone and is responsible for handling DNS queries related to the domain and its subdomains

4.8 DNS Protocol

The DNS protocol is an application that operates in a client-server model, where DNS resolvers (clients) send queries to DNS servers

- Uses UDP messages to enable fast delivery of data
- Operates on port 53
- Uses ARQ for reliability
- DNS servers are stateless
- Queries and responses are linked by a 16-bit ID field

4.9 Recursive Queries

In a recursive query, the DNS resolver (typically operated by the client) sends a query to the DNS server and expects the server to provide a complete answer

- If the DNS server has the information in its cache or is authoritative for the zone, it will respond with the IP address of the requested resource
- If the DNS server does not have the information, it will initiate its own queries to resolve the query further
- The DNS server recursively queries other DNS servers until it obtains a complete answer

Advantages

- The DNS resolver offloads the burden to the DNS server
- The DNS server can cache results for a pool of DNS resolvers

4.10 Iterative Queries

In an iterative query, the DNS resolver sends a query to DNS server and expects the server to provide the best possible answer it can, even if it does not have the complete information

- If the DNS server does not have the complete information, it will provide a referral to another DNS server that may have more information
- The DNS resolver iteratively contacts different DNS servers, following the chain of referrals, until it obtains a complete answer or determines that the domain does not exist

Advantages

- Server can quickly respond with what it knows instead of initiating its own queries
- Easy to build high load servers

4.11 DNS Query Process

Suppose a client wants to resolve the domain name `cs.washington.edu`. Assume that no information is currently cached

1. The client sends a recursive query to a DNS resolver, often the local nameserver
2. The local nameserver sends an iterative query to the root DNS server for the IP address of the `.edu` server
3. The local nameserver sends an iterative query to the `.edu` server for the IP address of the `washington.edu` server
4. The local nameserver sends an iterative query to the `washington.edu` server for the IP address of the `cs.washington.edu` server
5. The local nameserver receives the IP address for `cs.washington.edu` and sends it back to the client

4.12 DNS Resource Types

- SOA: indicates start of authority and contains key zone parameters
- A: indicates the IPv4 address of a host
- AAAA: indicates the IPv6 address of a host
- CNAME: indicates the canonical name for an alias
- MX: indicates the mail exchanger for the domain
- NS: indicates the nameserver of the domain or delegated subdomain

5 HTTP

5.1 HTTP

Hypertext Transfer Protocol (HTTP) is a request/response protocol that operates in a client-server model, where client (typically web browsers) send requests to servers

- Uses TCP messages to enable reliable, ordered delivery of data
- Operates on port 80

5.2 HTTP Commands

- GET: read a web page
- HEAD: read a web page's header
- POST: append to a web page
- PUT: store a web page
- DELETE: remove the web page
- TRACE: echo the incoming request
- CONNECT: connect through a proxy
- OPTIONS: query options for a page

5.3 HTTP Responses

- 1xx: information
- 2xx: success
- 3xx: redirection
- 4xx: client error
- 5xx: server error

5.4 HTTP Fetch Process

1. Send a DNS query to resolve the server to IP address
2. Set up a TCP connection to the server
3. Send an HTTP request for the page
4. Await an HTTP response for the page
5. Execute and fetch embedded resources and render the page
6. Clean up any idle TCP connections

5.5 DOM

The Document Object Model (DOM) represents the structure and content of an HTML document as a tree-like structure

- Embedded JavaScript modifies the DOM based on user actions, asynchronous functions, or other server-side actions

5.6 PLT

Page Load Time (PLT) refers to the amount of time it takes for a web page to fully load and become visible to the user in a web browser from the initial page request. Depends on a variety of factors such as

- Sizes of the files that make up the web page
- Network latency and bandwidth
- Server response time

5.7 Parallel Connections

Parallel connections enable the client to run multiple parallel HTTP instances simultaneously

- Advantages
  - Server remains unchanged
  - Each parallel connection is only slightly slower than the single connection
- Disadvantages
  - Parallel connections compete with each other for network resources
  - Exacerbates network bursts and loss

5.8 Persistent Connections

Persistent connections enable the client to reuse HTTP instances for multiple requests

- Advantages
  - Removes the cost of setting up and tearing down connections
  - Enables the use of request pipelining where multiple requests can be sent to the server simultaneously
- Disadvantages
  - Increased client and server complexity
  - Keeping connections open for an extended period can tie up server resources

5.9 Web Caching

Web caching enables the client to temporarily store copies of web resources

- Advantages
  - Improved performance
  - Reduced network traffic
- Disadvantages
  - Cached content may become stale
  - Increased storage requirements

6 Network Security

6.1 Message Confidentiality

Confidentiality ensures that only authorized individuals or entities can access and view the message

6.2 Symmetric Encryption

In symmetric encryption, both parties share a secret key which is used for both the encryption and decryption of data

- Advantages
  - Symmetric encryption algorithms are faster and more efficient
- Disadvantages
  - Secret key must be securely distributed

6.3 Asymmetric Encryption

In asymmetric encryption, a public key is used for the encryption of data and a private key is used for the decryption of data

- Advantages
  - Eliminates the need for secure key distribution
- Disadvantages
  - Asymmetric encryption algorithms are more computationally intensive

6.4 Hybrid Encryption

Hybrid encryption combines both symmetric and asymmetric encryption to leverage the strengths of both encryption methods

- Asymmetric encryption is used for secure key exchange
- Once the shared secret key is established, both parties switch to symmetric encryption for the actual data transmission

6.5 Message Integrity

Integrity ensures that the information received is the same as the information sent, without any unauthorized modifications

6.6 Message Authenticity

Authenticity ensures that the information is genuine and originates from the expected sender

6.7 Message Authentication Codes

A message authentication code (MAC) is a small token appended to the message that validates its integrity and authenticity

- Generating and validating the MAC is a symmetric process
- Both parties share a secret key which is used to generate and verify the MAC

6.8 Digital Signatures

A digital signature is a small token appended to the message that validates its integrity and authenticity

- Generating and validating the signature is an asymmetric process
- The sender generates the signature using a private key, and the receiver verifies the signature using a public key

6.9 Message Digest

A message digest is a secure fixed-length checksum appended to the message that validates its integrity, but not its authenticity

- A cryptographic hash function is used to generate the checksum

6.10 Message Freshness

Freshness ensures that the message is current and has not been replayed or reused from a previous instance

6.11 Message Replay Attacks

In a message replay attack, an attacker intercepts and retransmits previously recorded messages to deceive the recipient or gain unauthorized access

- Sequence numbers and nonces (numbers-used-once) can be used to identify duplicate messages

7 Web Security

7.1 HTTPS

HTTPS is the secure version of HTTP, ensuring that the data transmitted between the browser and the website is encrypted and secure

- Uses HTTP over SSL/TLS

7.2 SSL/TLS

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are cryptographic protocols that provide secure communication over a network

- TLS is the newer and more widely adopted successor to SSL
- Verifies the identity of the server
- Maintains message confidentiality, integrity, authenticity, and freshness

7.3 Certificates

Certificates are digital documents that binds an entity's public keys to an identity, vouching that the public key contained in the certificate belongs to the entity

7.4 Certificate Authorities

A certificate authority (CA) is a trusted third-party entity that verifies the identity and authenticity of entities and issues certificates

- CAs maintain a certificate revocation list that contains revoked certificates

7.5 VPN

A virtual private network (VPN) creates a private network connection between a user's device and a remote server, allowing users to securely access and transmit data

- Operates at the network layer
- Logically separate from the Internet

7.6 Tunneling

Tunneling allows data from one network to be transported over another network, creating a virtual tunnel for the data

- Tunneling encapsulates IP packets within an IP packet
- The original packet is the payload of the encapsulating packet
- The outer IP header has tunnel endpoints as source/destination
- The inner IP header has private network IP addresses as source/destination
- Does not guarantee confidentiality, integrity, or authenticity

7.7 IPSEC

IP security (IPSEC) is a set of mechanisms for ensuring confidentiality, integrity, and authenticity

- Often used to secure VPN tunnels

7.8 VPN Connection Process

1. Client and VPN server establish an encrypted connection
2. VPN software creates a logical network interface on the client
3. Applications send traffic through this interface
4. VPN software tunnels the traffic to the VPN server
5. The VPN server unwraps the traffic, NATs the packet, and sends it to the destination
    - The destination only sees the VPN server's IP address

7.9 DDoS

Distributed Denial of Service (DDoS) is a type of cyber attack in which compromised computers are used to overwhelm a targeted system or network with a flood of malicious traffic

- Attackers can spoof their IP addresses to make it appear as if the flood of malicious traffic is originating from multiple legitimate sources

7.10 Ingress Filtering

Ingress filtering is a network security measure that examines incoming network traffic at the network boundary to filter out potentially malicious or unauthorized traffic

- Helps prevent IP spoofing by verifying the source IP addresses of incoming packets against legitimate address ranges assigned to the network

8 Physical Layer

8.1 Physical Layer

The physical layer is responsible for transmitting digital bits over a physical medium using analog signals

8.2 Twisted Pair Cables

Twisted pair cables consist of pairs of insulated copper wires twisted together

- Widely used in Ethernet networks and telephone systems

8.3 Coaxial Cables

Coaxial cables have a central conductor surrounded by an insulating layer, a metallic shield, and an outer insulating layer

- Provides better shielding against electromagnetic interference compared to twisted pair cables

8.4 Fiber Optic Cables

Fiber optic cables use thin strands of glass or plastic fibers to transmit data using light signals

- Offers high bandwidth, low attenuation, and high resistance to electromagnetic interference

8.5 Wireless Media

Wireless media allow for flexible connectivity without the need for physical cables

- Includes various media such as radio waves, microwaves, and infrared signals
- Sender radiates signal over a region, essentially broadcasting to all nearby receivers
- Wireless signals at similar frequencies can interfere

8.6 Multipath

Multipath is the phenomenon where a transmitted signal takes multiple paths to reach the receiver

- Occurs when the transmitted signal encounters obstacles, causing the signal to reflect, scatter, and arrive at the receiver through different paths
- Multiple paths result in multiple signals, each with different delays, attenuations, and phase shifts

8.7 Coding

Coding is the process of representing information or data in a specific format before transmission over a physical medium

- Helps to define the electrical or optical characteristics of the transmitted signal, including signal levels, timing, and synchronization
- Examples of line coding schemes include Non-Return to Zero (NRZ), Return to Zero (RZ), 4B/5B,

8.8 Clock Recovery

Clock recovery is the process of extracting timing information from a received data stream

- Synchronizes the transmitter and receiver with a common clock to ensure accurate transmission and reception of data

8.9 Non-Return to Zero

In Non-Return to Zero (NRZ), each bit is represented by a voltage level for the entire duration of the bit time

- A high voltage ($+\mathrm{V}$) represents a 1 and a low voltage ($-\mathrm{V}$) represents a 0
- There is no neutral/rest voltage, hence the name

8.10 Return to Zero

In Return to Zero (RZ), each bit is represented by a voltage level and separated by a transition voltage level

- A high voltage ($+\mathrm{V}$) represents a 1, a low voltage ($-\mathrm{V}$) represents a 0, and a neutral voltage ($0\mathrm{V}$) represents a transition

8.11 4B/5B

In 4B/5B, each 4-bit group is replaced with a corresponding 5-bit symbol determined by a predefined lookup table

- Ensures a balanced distribution of 1s and 0s in the transmitted data stream to maintain a reasonable number of transitions and aid in clock recovery
- Provides some level of error detection capability
- Often used in high-bandwidth applications such as Ethernet

8.12 Modulation

Modulation is the process of modifying a carrier signal to efficiently convey information for transmission over a physical medium

- Carrier signals can be modulated by changing its amplitude, frequency, or phase

8.13 Nyquist Sampling Theorem

Let B be the bandwidth of the signal in hertz (Hz), and V be the number of signal levels. Then the Nyquist sampling theorem states that

$$R = 2B \log_2 V$$

where R is the maximum sampling rate in $\mathrm{bits/sec}$

- The sampling rate represents the number of samples needed to accurately reconstruct a continuous signal from its discrete samples
- To sample a waveform accurately, we need to capture both the positive and negative peaks of each cycle. Therefore we must record two samples for each cycle
- Confusingly, we use the units $\mathrm{bits/sec}$ to describe the *sampling* rate. Therefore it is important to understand that R is <u>not</u> the data transmission rate

8.14 Shannon Capacity Theorem

Let B be the bandwidth of the signal in hertz (Hz), V be the number of signal levels, S be the total voltage range in volts (V), and N be the total noise value in volts (V). Then the Shannon capacity theorem states that

$$V = 1 + \frac{S}{N}$$
$$C = B \log_2 \left(1 + \frac{S}{N}\right)$$

where C is the maximum data transmission rate in $\mathrm{bits/sec}$

- The data transmission rate represents the number of information bits that can be transmitted
- If the voltage ranges from $-s$ to $+s$, then the total voltage is $2s$
- If the noise is guaranteed to be at most n, then the total noise value is $2n$

8.15 Nyquist Sampling Theorem vs. Shannon Capacity Theorem

- The Nyquist sampling theorem provides an upper bound on the maximum number of discrete samples we can modulate onto a carrier signal
- The Shannon capacity theorem provides an upper bound on the maximum number of bits we can transmit
- It takes two samples to identify each bit. Hence the Nyquist sampling theorem and Shannon capacity theorem differ by a factor of 2

9 Link Layer

9.1 Link Layer

The link layer is responsible for transferring frames over one or more connected physical links

- Provides services such as framing, error detection/correction, multiplexing, and switching

9.2 Framing

Framing is the process of dividing a stream of data into discrete frames

- Involves adding special characters or bit patterns to mark the beginning and end of each frame
- Allows the receiving device to identify and extract individual frames from the data stream

9.3 Fixed-Size Framing

In fixed-size framing, all frames consist of a predetermined and constant number of bits, regardless of the amount of data being transmitted

- Disadvantage: if the payload being transmitted is much smaller than the fixed frame size, a significant portion of the frame is occupied by padding

9.4 Byte Count Framing

In byte count framing, the length of each frame is indicated using a fixed-length field within the frame header

- Disadvantage: if synchronization is lost due to errors or misalignment in the data stream, the receiver may misinterpret the byte count and extract incorrect frame boundaries

9.5 Byte Stuffing

In byte stuffing, flag bytes and escape bytes are inserted/stuffed into the data stream

- A flag byte indicates the start or end of the frame
- If the flag byte is encountered within the data stream, then the escape byte is inserted to indicate that the following byte is not a flag but part of the actual data
- If the escape byte is encountered within the data stream, then another escape byte is inserted to indicate that the following byte is not an escape but part of the actual data
- Disadvantage: introduces additional overhead in terms of extra bytes inserted

9.6 Error Detection and Correction

Error detection and correction is the process of detecting and correct errors in transmitted data to ensure data integrity and reliability

- Involves adding additional information to the transmitted data to allow the receiving device to identify and correct errors if possible or request retransmission of the erroneous data

9.7 Error Detection vs. Correction

- Error detection is more efficient when errors are not expected, or errors involve many bits when they occur
  - Used in the link layer and above
- Error correction is more efficient when errors are expected, or there is no time for retransmission
  - Heavily used in the physical layer and also used in the application layer

9.8 Check Bits

Check bits are numerical values calculated from the transmitted data that can be used to detect errors during transmission

- The sender performs some mathematical computation on the data and appends the resulting value as check bits
- The codeword consists of the combined data and check bits
- The receiver performs the same computation on the received data and compares the received check bits with the calculated check bits

9.9 Hamming Distances

- The Hamming distance between two codewords is the number of positions at which the corresponding bits in the codewords differ
- The Hamming distance of a coding is the minimum error distance between any pair of codewords that cannot be detected
  - For a coding of distance $d + 1$, up to d errors will always be detected
  - For a coding of distance $2d + 1$, up to d errors can always be corrected by mapping to the closest valid codeword

9.10 Hamming Codes

Hamming codes are a type of error-correcting code with a distance of 3. Let n be the number of bits in the message. Then

$$n \leq 2^k - k - 1$$

where k is the number of check bits needed to protect the message

- With k check bits, we are able to detect all 2-bit errors and correct all 1-bit errors in our n-bit message

9.11 Parity Bits

A parity bit is an additional bit added to the original data such that the resulting codeword has an even number of 1s

- 1-Dimensional parity has a Hamming distance of 2

9.12 Checksums

A checksum is a value calculated from the data to detect errors

- To calculate the checksum
  1. Arrange the data in 16-bit words
  2. Add the 16-bit words together
  3. Add any carryover back to get 16 bits
  4. Take the compliment to get the checksum
- Checksum has a Hamming distance of 2
  - Still better than 1-dimensional parity
  - Very rarely unable to detect 2-bit errors

$$
\begin{array}{cccccc}
 & 0 & 0 & 0 & 1 \\
 & \mathrm{f} & 2 & 0 & 4 \\
 & \mathrm{f} & 4 & \mathrm{f} & 5 \\
+ & \mathrm{f} & 6 & \mathrm{f} & 7 \\
\hline
2 & \mathrm{d} & \mathrm{d} & \mathrm{f} & 1 \\
 & & \downarrow & & \\
 & \mathrm{d} & \mathrm{d} & \mathrm{f} & 1 \\
+ & & & & 2 \\
\hline
 & \mathrm{d} & \mathrm{d} & \mathrm{f} & 3 \\
 & & \downarrow & & \\
 & 2 & 2 & 0 & \mathrm{c}
\end{array}
$$

9.13 Multiplexing

Multiplexing is the ability for multiple devices to simultaneously access and utilize a shared link

9.14 Time Division Multiplexing

Time Division Multiplexing (TDM) divides the available time slots of a communication channel into fixed time intervals. Each device is assigned a specific time slot during which they can transmit or receive data

- In TDM, devices send data at a high rate over a short period
- Suitable for continuous traffic and a fixed number of devices

9.15 Frequency Division Multiplexing

Frequency Division Multiplexing (FDM) divides the available frequency spectrum into multiple non-overlapping frequency bands. Each device is assigned a specific frequency band for communication

- In FDM, devices send data at a low rate over a long period
- Widely used in telecommunications

9.16 Statistical Multiplexing

Statistical Multiplexing (SM) dynamically allocates bandwidth based on the data traffic needs of individual devices, optimizing the utilization of available resources

9.17 Multiple Access Control Protocols

Multiple access control (MAC) protocols are a form of statistical multiplexing that enable multiple devices to access a shared link without a centralized control mechanism

- Often used in Ethernet networks

9.18 ALOHA Protocol

The ALOHA protocol allows devices to transmit data whenever they have it, without checking for link availability. If a collision occurs, then devices wait for a random period before retrying

- Simple and works well under low load
- Not efficient under high load

9.19 CSMA Protocol

The carrier sense multiple access (CSMA) protocol improves upon the ALOHA protocol by having devices listen for link activity before transmitting data

- Carrier sense is the ability to detect the presence or absence of a carrier signal on a shared link
- Works well when link bandwidth is small

9.20 CSMA/CD Protocol

The carrier sense multiple access with collision detection (CSMA/CD) protocol improves upon the CSMA protocol by having devices immediately stop transmitting upon detecting a collision

- devices wait $2\mathrm{D}$ seconds before retrying, where D is the latency of the link
  - D is precomputed as a function of cable distance

9.21 Binary Exponential Backoff

Binary exponential backoff (BEB) is a collision resolution algorithm that determines the waiting time for retransmission when a collision is detected

- For the 1^{st} collision, wait 0 or 1 frame times
- For the 2^{nd} collision, wait 0 to 3 frame times
- For the 3^{rd} collision, wait 0 to 7 frame times
- For the n^{th} collision, wait 0 to $2^n - 1$ frame times

BEB distributes the devices' transmission attempts across a wider range of time slots, quickly reducing the probability of repeated collisions

- Often used in CSMA protocols

9.22 Wireless Network Complications

- Hidden terminals problem
  The hidden terminals problem occurs in wireless networks when two devices A and B are within range of a common device C, but are out of range from each other
  - A and B cannot coordinate their communications
  - If A and B communicate with C simultaneously, their transmissions will collide
  - Addressed by RTS/CTS
- Exposed terminals problem
  The exposed terminals problem occurs in wireless networks when two devices are within range of each other, and one device refrains from transmitting due to a perceived interference caused by the other device's transmission

- A detects B's transmission and assumes the channel is busy
- A refrains from transmitting, even if its intended recipient is out of range and not affected by B's transmission