The changing Internet

Networked System: A cooperating set of autonomous computing devices that exchange data to perform some application goal
Channel constraints: bound communications speed and reliability
OSI Reference Model: Application Layer, Presentation Layer, Session Layer, Transport Layer, Network Layer, Data Link Layer, Physical Layer
Note: Real networks don't follow the OSI Reference Model
Physical Layer: Transmits raw bits over a physical medium.
Baseband Data Encoding: NRZ: 0 is represented by no change in voltage, 1 is represented by a change in voltage. Easy to miscount bits if long run of same value. **Manchester:** Encoding: 0 is represented by a transition from high to low, 1 is represented by a transition from low to high.
Modulation: Allows multiple signals on a channel, modulated onto carriers of different frequency. Amplitude Modulation, Frequency Modulation, Phase Modulation.
Data Link Layer: provides framing, addressing, media access control, error detection, and flow control.
Framing: Separate the bitstream into meaningful frames of data.
Media Access Control: How devices share the channel. If another transmission is active, the device must wait until the channel is free.
Network Layer: provides routing, addressing, and packet switching. Internet Protocol (IP).
IPv4: 32-bit address space. Fragmentation difficult at high data rates.
IPv6: 128-bit address space. No in-network fragmentation. Simple header format.
Routing: Each network administered separately - an autonomous system (AS), different technologies and policies.
Inter-domain Rounting: Route advertisements are sent to the routing table of the destination. Border Gateway Protocol (BGP). Advertisements have AS-path.
Transport Layer: provides end-to-end error recovery, flow control, and multiplexing.
TCP: Connection-oriented, reliable, in-order delivery, flow control, congestion control.
UDP: Connectionless, unreliable, out-of-order delivery, no flow control, no congestion control.
Session Layer: provides session establishment, maintenance, and termination.
Managing Connections: How to find participants in a connection, how to setup and manage the connection.
Presentation Layer: provides data representation and encryption.
Application Layer: provides the interface to the application. Deliver email, stream video, etc.
Happy Eyeballs: The process of trying multiple connections to a server to find one that is available.

Connection Establishment in a Fragmented Network

TCP is a transport layer protocol, provides a reliable ordered byte stream service over the best-effort IP network. Provides congestion control. TCP segments carried as data in IP packets. IP packets carried as data in link layer frames. Link layer frames delivered over physical layer. Lost packets are retransmitted, ordering is preserved, message boundaries are not preserved. TCP follows a client-server model. The server calls the accept () function to accept incoming connections, while the client initiates a connection by calling connect (). Calls to send () and recv () are used to send and receive data. As RTT increases, benefits of increasing bandwidth reduce
Impact of TLS: HTTP sends and retrives data immediatly once the TCP connection is open. HTTPS opens a TCP connection, then negotiates secure parameters using TLS. TLS v1.3: extra 1RTT, TLS v1.2: 2RTT.
Impact of Ipv6 and dual stack deployments: Hosts support a combination of IPv4 and IPv6.
Peer-to-peer Connections You should be able to run a TCP server on any device, and TCP, UDP based peer-to-peer applications. Peer-to-peer connetion establishment is difficult due to network address translation (NAT). **NAT** is a work around for the shortage of IPv4 addresses, it allows several devices to share a single public IP address. ISP assigns new range of IP addressses to customer. Records the mapping, so the reverse changes can be made to any incoming replies as they traverse the NAT in the reverse direction
NAT Breaks Applications: Client-server applications with server behind NAT fail – need explicit port forwarding Hard-coding IP addresses, rather than DNS names, in configuration files and application is a bad idea OUTgoing connections create state in NAT, so replies can be translated to reach the correct host on the private network.