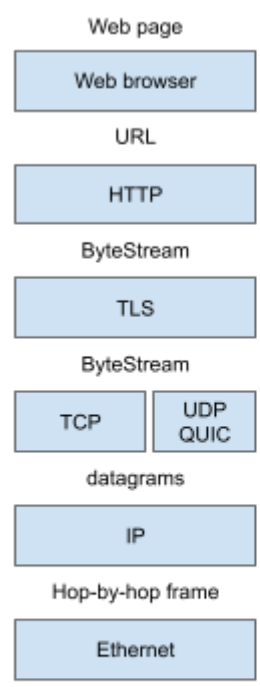
Things we talked about after midterm and some interesting questions I was asking myself when I reviewed these things:

- Naming across the Stack



Names	assigned	discovered
URL links	delegated/contextual to page author	HATEOAS
Domain names Host names	Global hierarchy/ distributed database with delegation (e.g. (e.g. edu. => mit.edu. => lamp.mid.edu.)	DNS (1 special seed - the entry point of DNS (in /etc/resolv.conf)
IP address	Global hierarchy with delegation (e.g. assigned ranges for each country/area, and then ISPs ask local authorities for ranges of IP) DHCP	Routing
MAC addresses	Global hierarchy with delegation => manufacturer (24 bits) + serial # (24 bits)	ARP (lab 5)
DNS for secure websites	Global hierarchy of trusted certification authorities	N special seeds for trusted certification authorities

For secure links (e.g. BOA)

  - How does DNS work?
  - How are IP addresses assigned?
  - How are hardware addresses assigned?

- Physical Layer
  - **Shannon theory**: the capacity of a link is C = W log(1 + PN) (P - average power, N - average noise, W - band width)
  - **Clock synchronization**: preamble, downward/upward transition for encoding 0/1
- Elasticity Buffer
  - **Why** elasticity buffer:
    - Clock synchronization
  - **How** elasticity buffer:
    - Sender: inter-packet gap and MTU
    - Receiver: start draining when B/2 buffered, stop when reach the end of a packet and starts waiting again

- History of Home Networking

Level	What's new
0	Each computer had several serial ports Each serial port is connected to a teletype machine
0.1	modem: transform between bits and telephone signal.
1: Internet at home	PCs replaced terminals, and speak TCP/IP. SLIP: IP over serial ports and routers. ISP tracks how IP addresses should be routed in its routers' routing table.
2: cable modem	modem also speaks Ethernet
3: home network	Multiple PCs are connected to the same modem via a switch
4: home subnet	A range of IP addresses is delegated to the home network, and a router in the home routes from ISP to different PCs. ISP only has an entry for getting to the router. Later, the home switch is replaced by Wi-Fi (AP)
5: home subnet	A home DHCP server for assigning IP addresses delegated to the home subnet.
6: proxy server	Each subnet has a local range of IP addresses (10/8), and a computer relays packets between two TCP Connections
7: transparent proxy	The PCs are not aware of the existence of proxy
8: network address/port translation (NAPT)	No more relaying, only change the address/port of packets.
9a: P2P over public server	A public server holds the files for two PCs behind different NAPTs.
9b: P2P via public proxy	A public server relays between two TCP Connections.
9c: P2P via explicit NAPT rules	Instantiate NAPT rules for direct connection between two PCs behind NAPTs
9d: P2P via NAPT traversal	STUN, and rendezvous server.

  - Why do we need a home subnet?
  - Why are P2P connections difficult with home subnets?
  - What are the different ways of making P2P connections possible between two ends behind different NAPTs?

- Security
    - Properties: **Integrity, Confidentiality, Authenticity**

Threat Model	Mitigations / Techniques
Accidental corruption	checksum/CRC
Adversarial modification	Secure hash Message Authentication Code (keyed hash)
Replay	Idempotence of messages
Eavesdropping	encryption (AE AD)
	Authenticated encryption requires a pre-established shared secret. For communication with strangers: AKE
	Certificates, certification authorities and TLS
Metadata Privacy	TOR
But TOR does not solve everything…	
Eavesdropper timing attack correlation	
Sybil attack	
Security holes that are not in TOR itself (e.g. the browser)	

    - What does each of the security properties mean in the context of Networking?
    - What tools of encryption we used and what issue does each of the tools solve?
    - How are certificates created?
    - What are the potential issues of certification authorities?
    - What is TOR?

- Video Streaming
    - How are audios and videos sent over the Internet?
    - What are the kinds of trade-offs we made when deciding how to send video and audio data?