More Networking

Where do these standards come from?

- IETF = Internet Engineering Task Force
- RFC = Request for Comments
  - MUST, MUST NOT, SHOULD, SHOULD NOT, MAY (RFC 2119)
- “The only laws on the Internet are assembly and RFCs” --Phrack 65
  - Assembly is an abstraction
  - RFCs are not always followed
    - Often ambiguous

OSI model

- Layer 1: Physical (think Ethernet, 802.11)
- Layer 2: Data Link (think ARP)
- Layer 3: Network (think IP)
- Layer 4: Transport (think TCP)
- Layer 5: Session (think NetBIOS, SOCKS)
- Layer 6: Presentation (think SSL/TLS)
- Layer 7: Application (think HTTP)

Some Wireshark stuff (http.pcap)

- You should poke around the GUI
- You should also check out tcpdump, tshark, and Python dpkt
- View::Name Resolution
- Right Click->Follow TCP Stream
- Can look in, *e.g.*, IP header for, *e.g.*, TTL (Time-to-live), or, *e.g.*, TCP header for, *e.g.*, ports
- Never completely trust abstractions
  - Can you trust the wireshark GUI?
  - Can you trust tshark raw text output?
  - Can you trust raw bits off the wire?

TCP 3-way handshake

- TCP header has flags
  - SYN is “Synchronize”, it means the sequence number has a special meaning
  - ACK is “Acknowledge”, it means the acknowledgment number has meaning
  - RST: “I have no record of such a connection”
  - Also, FIN, CWR, ECN, URG, PUSH

TCP 3-way handshake

- SYN: I'd like to open a connection with you, here's my initial sequence number (ISN)
- SYN/ACK: Okay, I acknowledge your ISN and here's mine
- I ACK your ISN

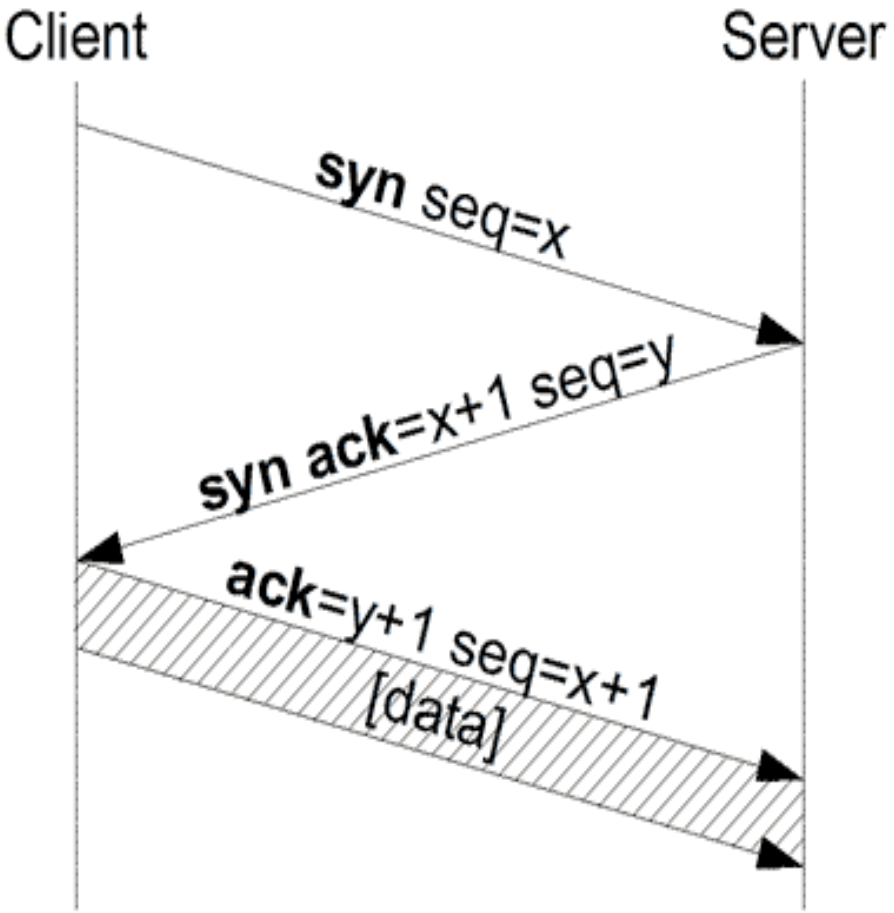
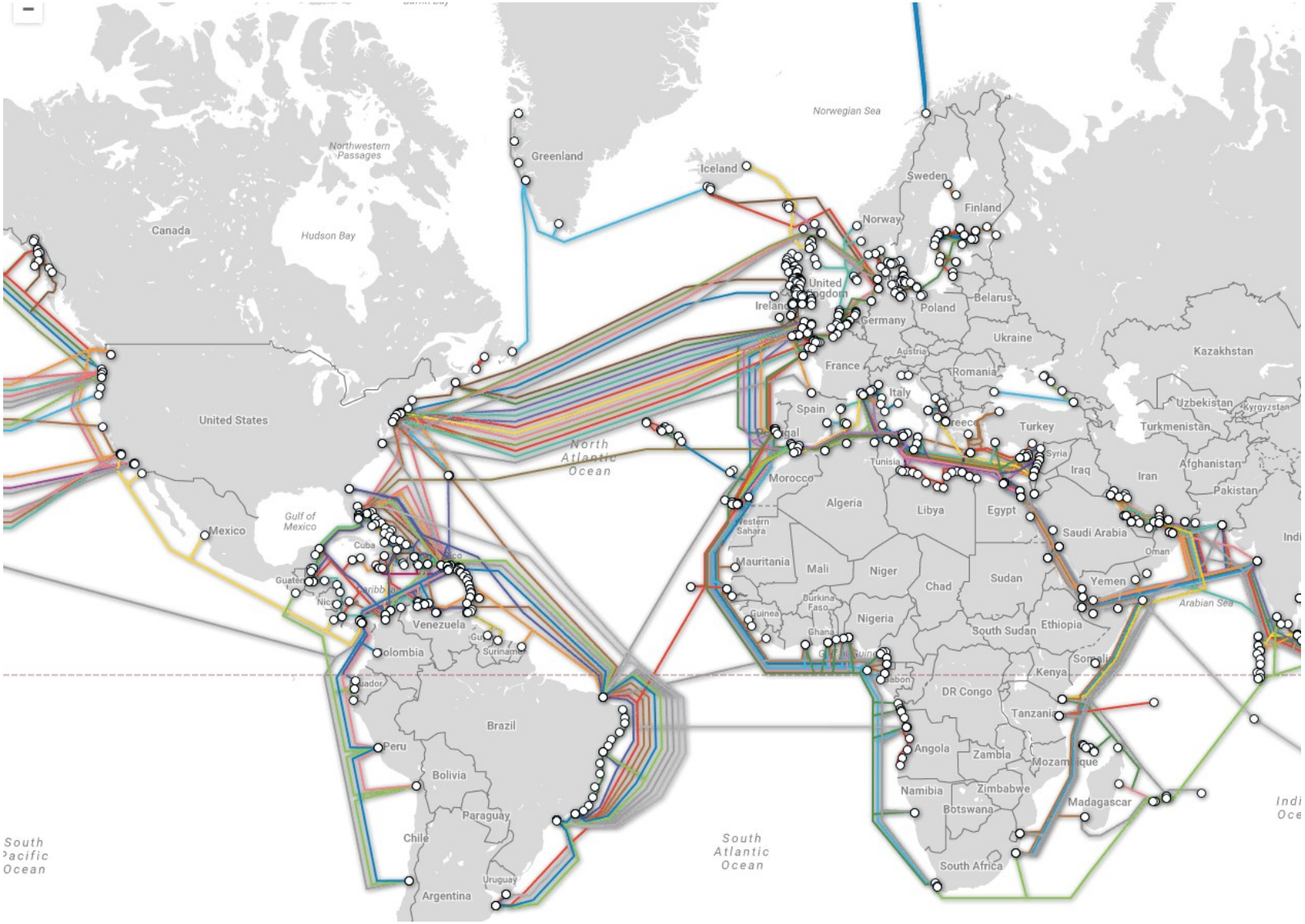


Image from Wikipedia

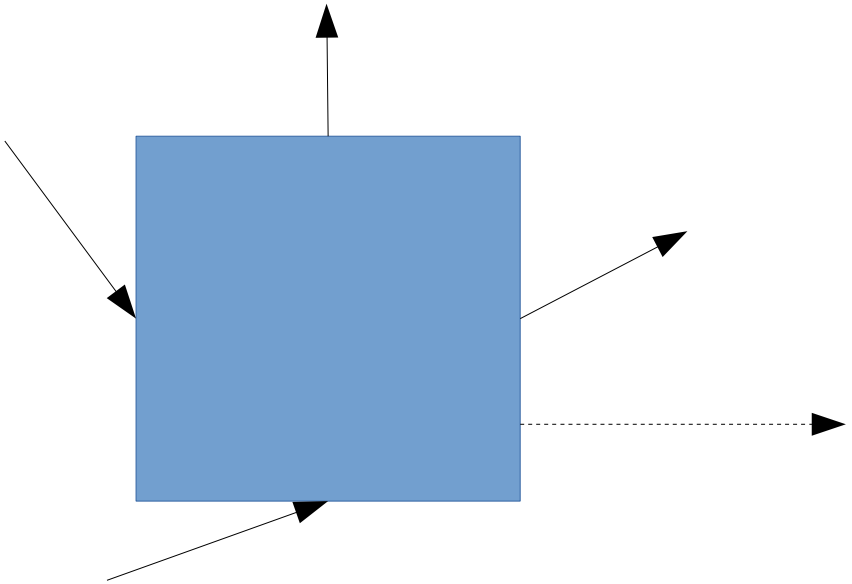
Attacks in Layer 1



From submarinecablemap.com

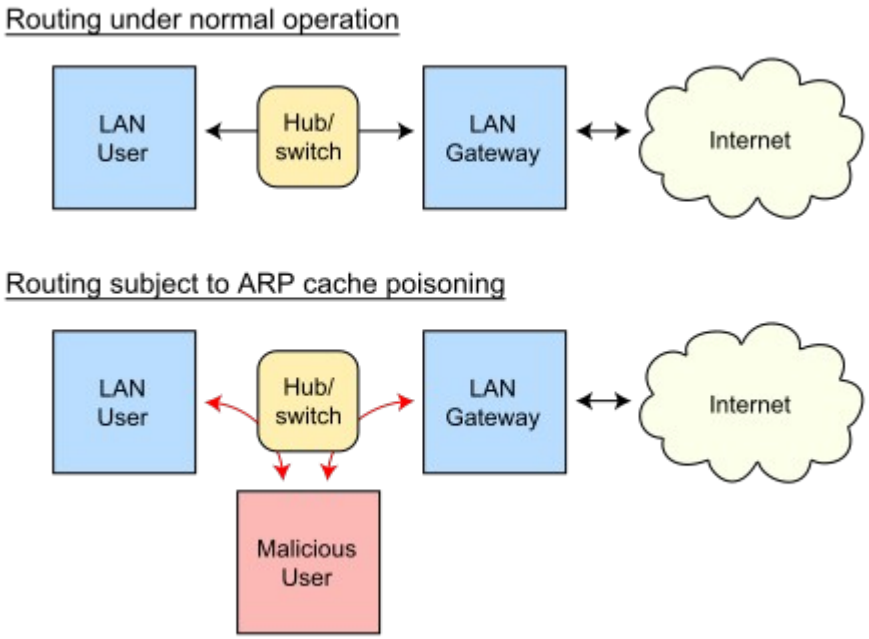
Attacks in Layer 1

- Taps are easy
  - Port mirrors on backbone routers literally split light
  - Port is the physical hole in a router, can mirror any of them to get a copy of the traffic
- 802.11 suite of wifi protocols has various issues



Attacks in Layer 2

- ARP spoofing
- ARP cache poisoning



From Wikipedia

Attacks in Layer 3

- Man-in-the-middle
  - Great Cannon is an example (in-path)
- Man-on-the-side
  - Great Firewall of China (GFW, on-path) and NSA QUANTUM are examples
- TTL is a clue, but is easy to hide

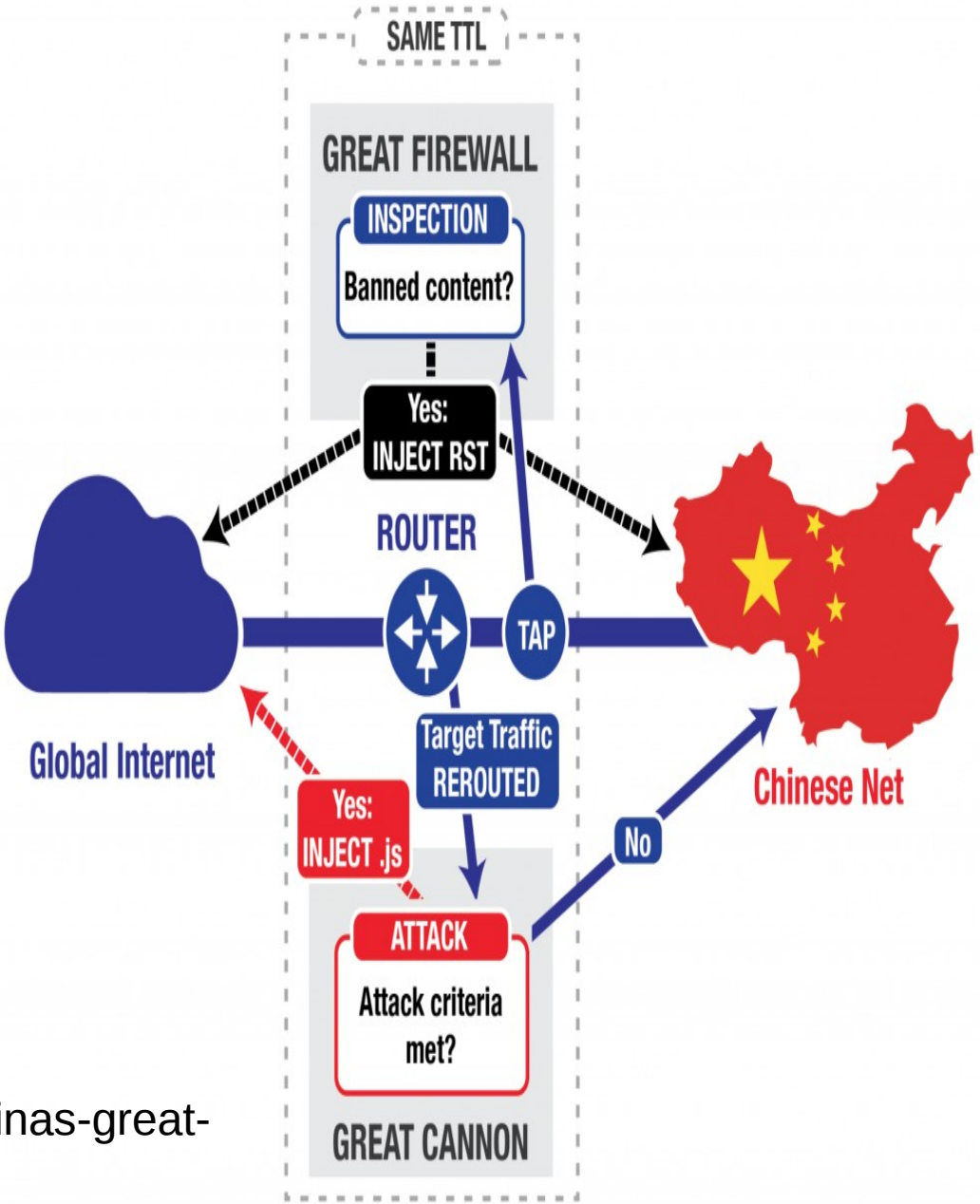


Image from https://citizenlab.org/2015/04/chinas-great-cannon/

Other IP-layer attacks

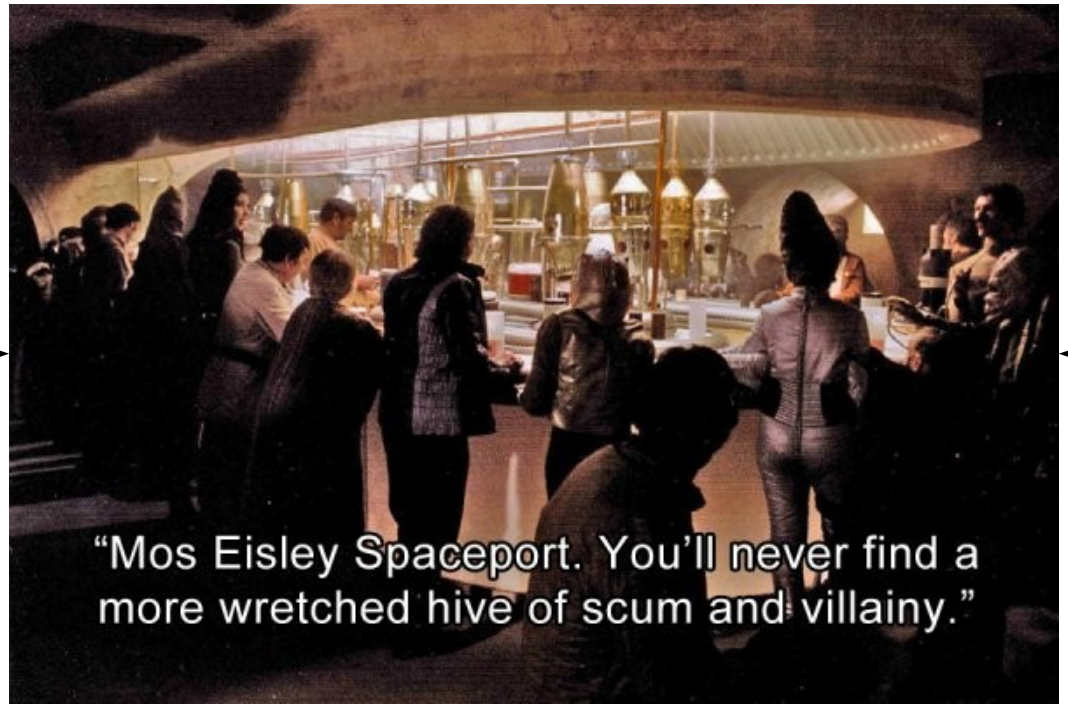
- BGP prefix attack
  - BGP routers prefer more specific announcements, meaning you can steal a /25 by announcing two /24s
- BGP announcements that are duplicated
  - Should get about half the traffic
- Announce a whole /8
  - Spammers can use whole chunks of unused (*i.e.*, unannounced) IP address space

Off-path attacks in layer 4

- If you can guess the initial sequence numbers of a TCP connection, you can hijack it off-path
  - See “Off-Path TCP Exploits...” by Cao *et al.* at USENIX Security 2016 as an example
- There are also off-path threats to privacy
  - See “Counting Packets Sent Between Arbitrary Internet Hosts” by Knockel and Crandall at USENIX FOCI 2014

Where is all this going?

- All layers have lots of attacks, can't talk about them all
- Lab 1 is about port scanning, Lab 2 involves sockets
- Later in the semester we'll talk about Internet censorship and surveillance at various times
- There are different threat models to consider
- After network security, we'll start talking about cryptography which can add security properties (like confidentiality, integrity, and authentication) end-to-end


“Mos Eisley Spaceport. You’ll never find a
more wretched hive of scum and villainy.”