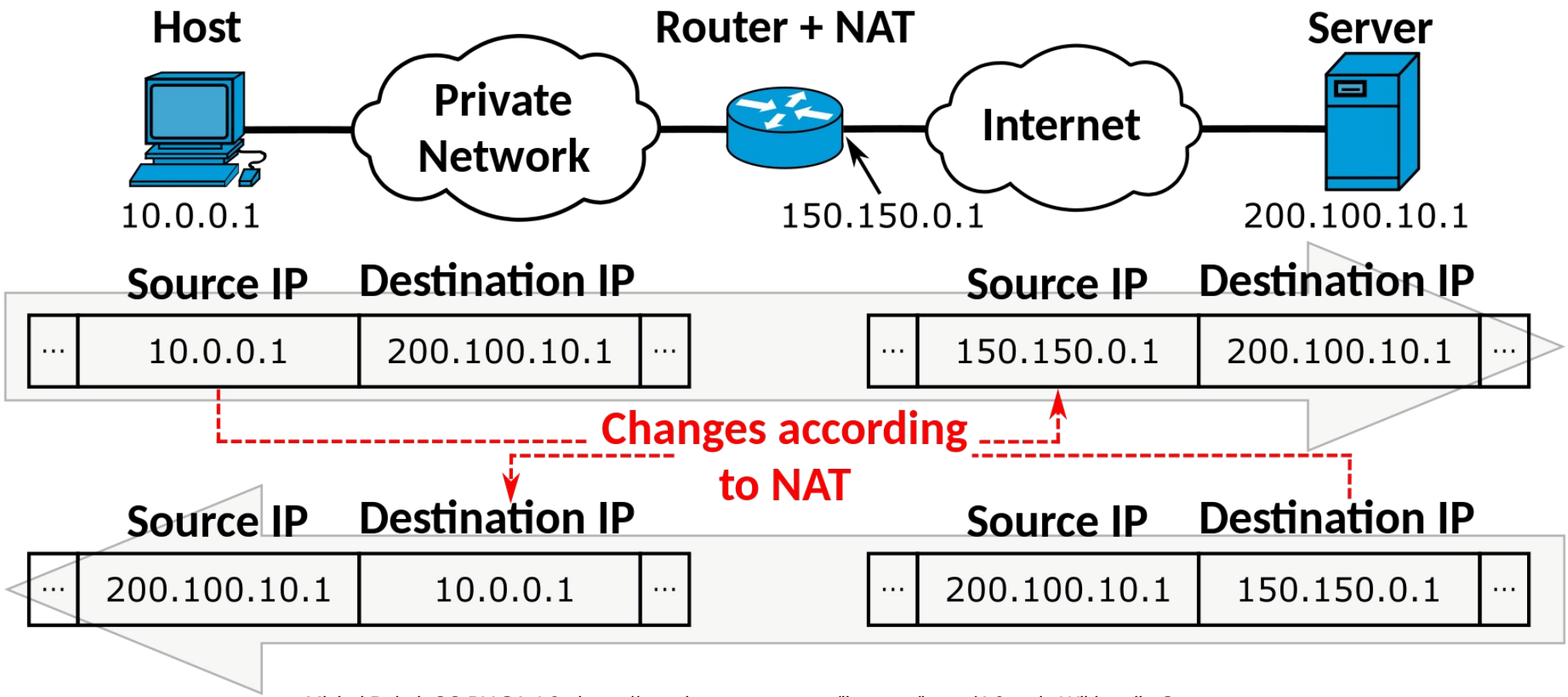
NAT, VPNs, and TCP

jedimaestro@asu.edu

Network Address Translation (NAT)

- 192.168.0.0/16, 10.0.0.0/8, and 172.16.0.0/12 are private addresses, Internet routers won't route them (called bogon filtering)
- 10.153.48.224 is my IP address when I connect to eduroam (basically the same thing as ASU wifi)
- 129.219.8.164 is my IP address as seen on the Internet

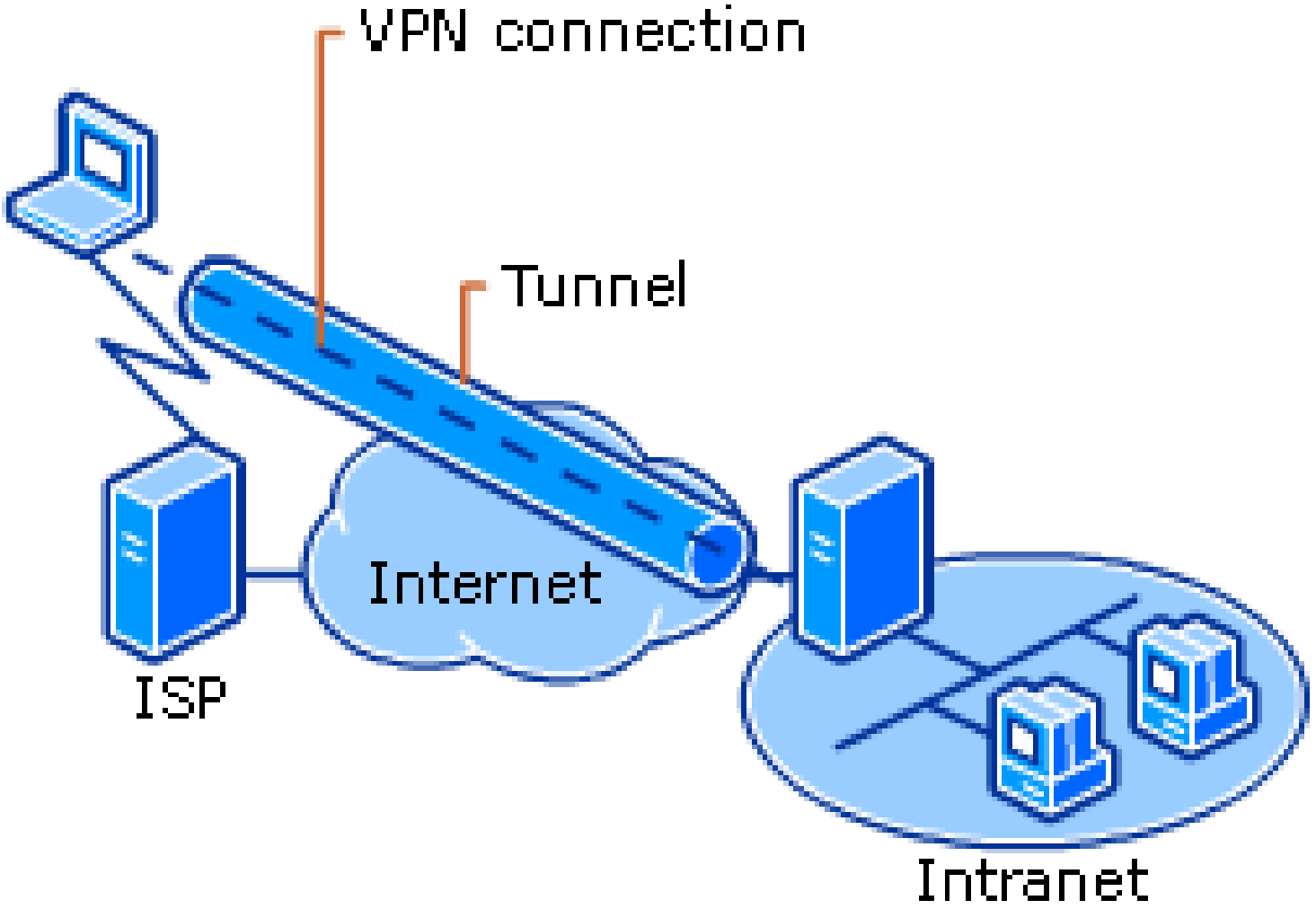


Michel Bakni, CC BY-SA 4.0 <https://creativecommons.org/licenses/by-sa/4.0>, via Wikimedia Commons

VPN = NAT + encrypted tunnel

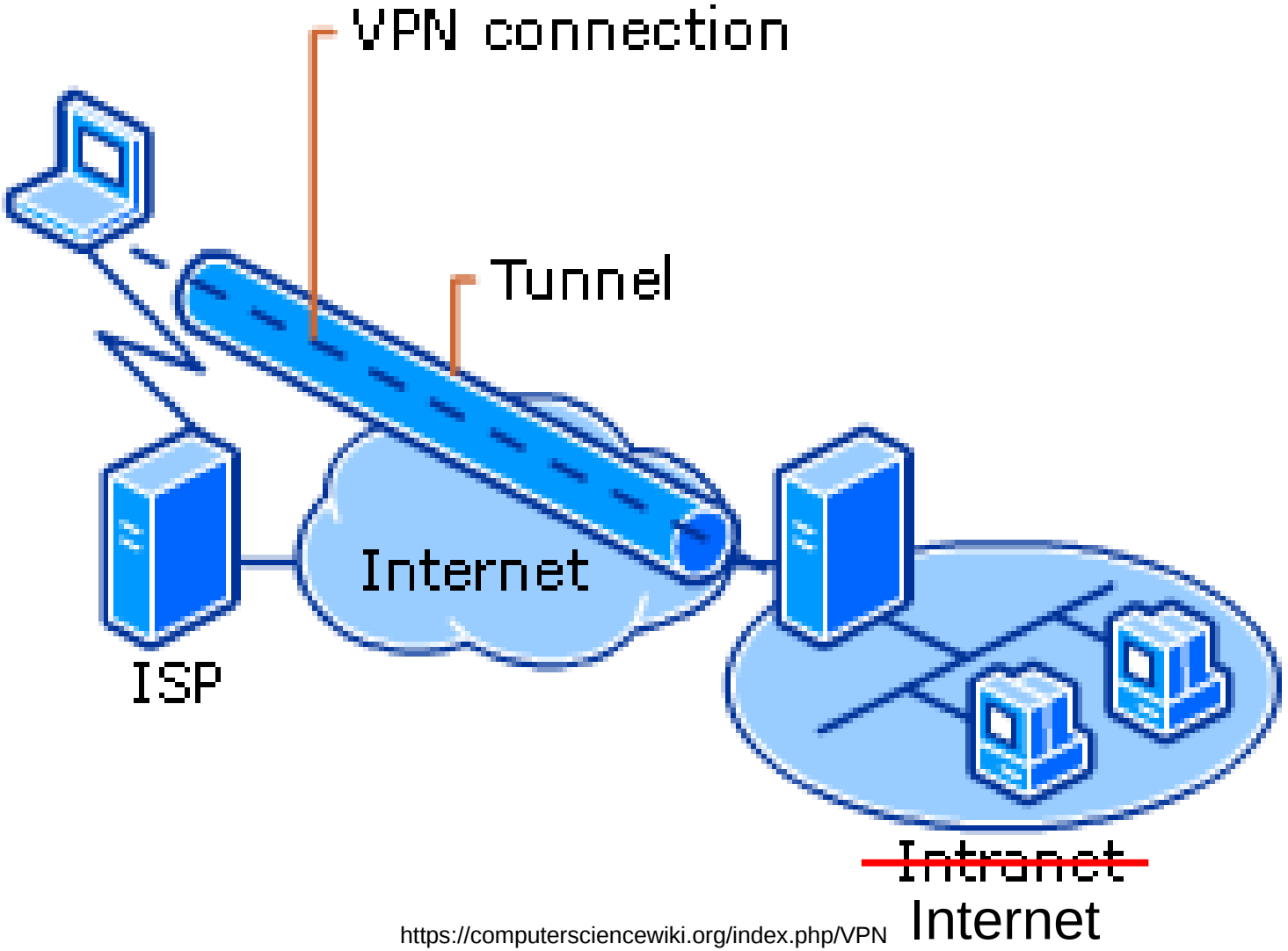
(Virtual Private Network)

What a VPN is supposed to be...



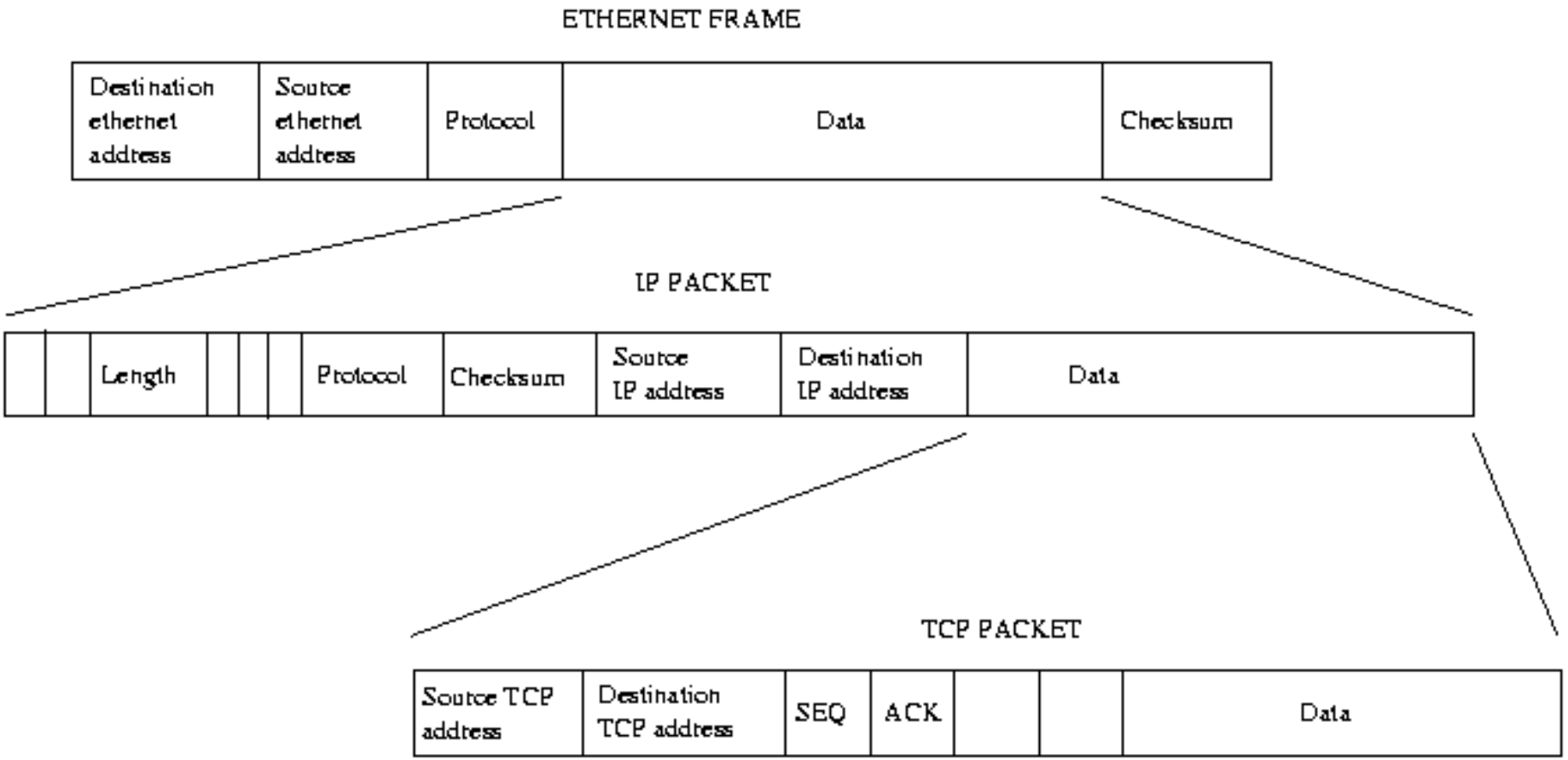
https://computersciencewiki.org/index.php/VPN

How commercial VPNs and many privacy/anti-censorship tools work…

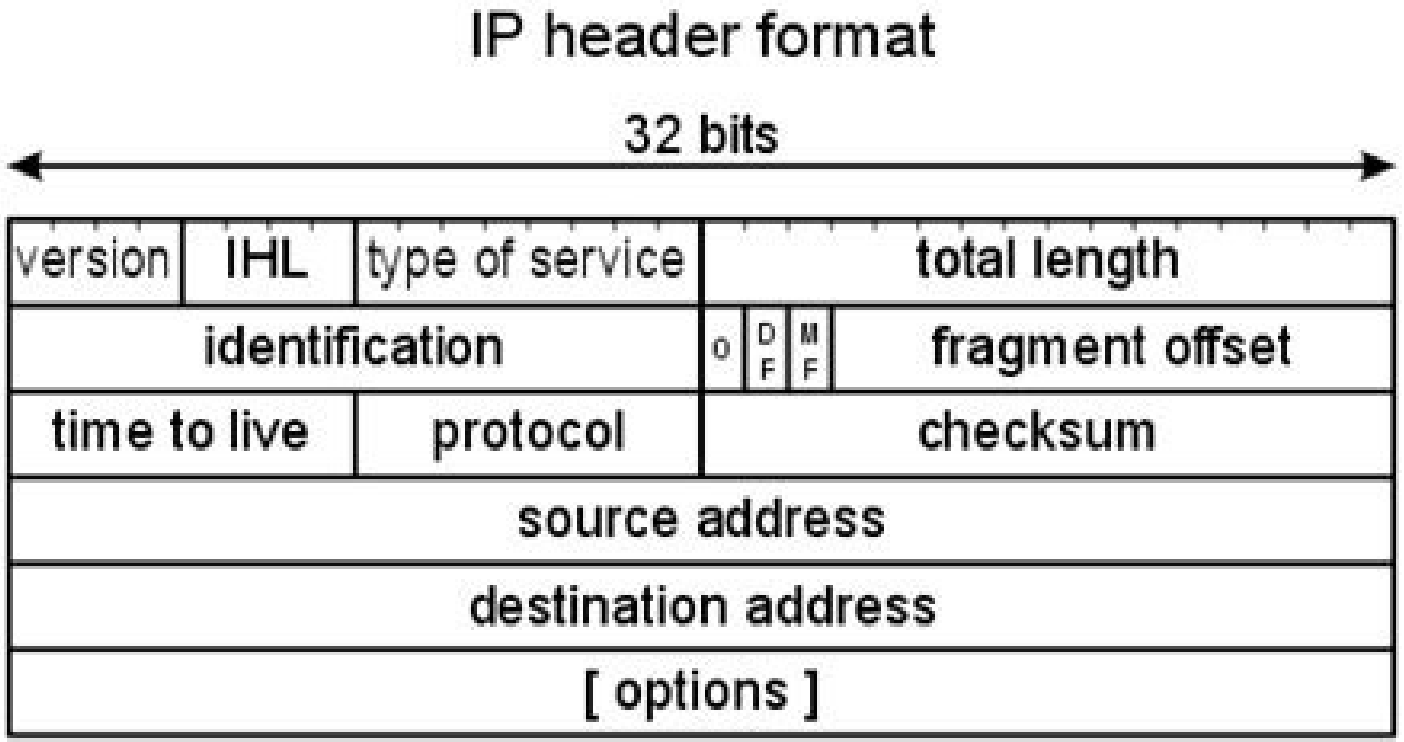


https://computersciencewiki.org/index.php/VPN

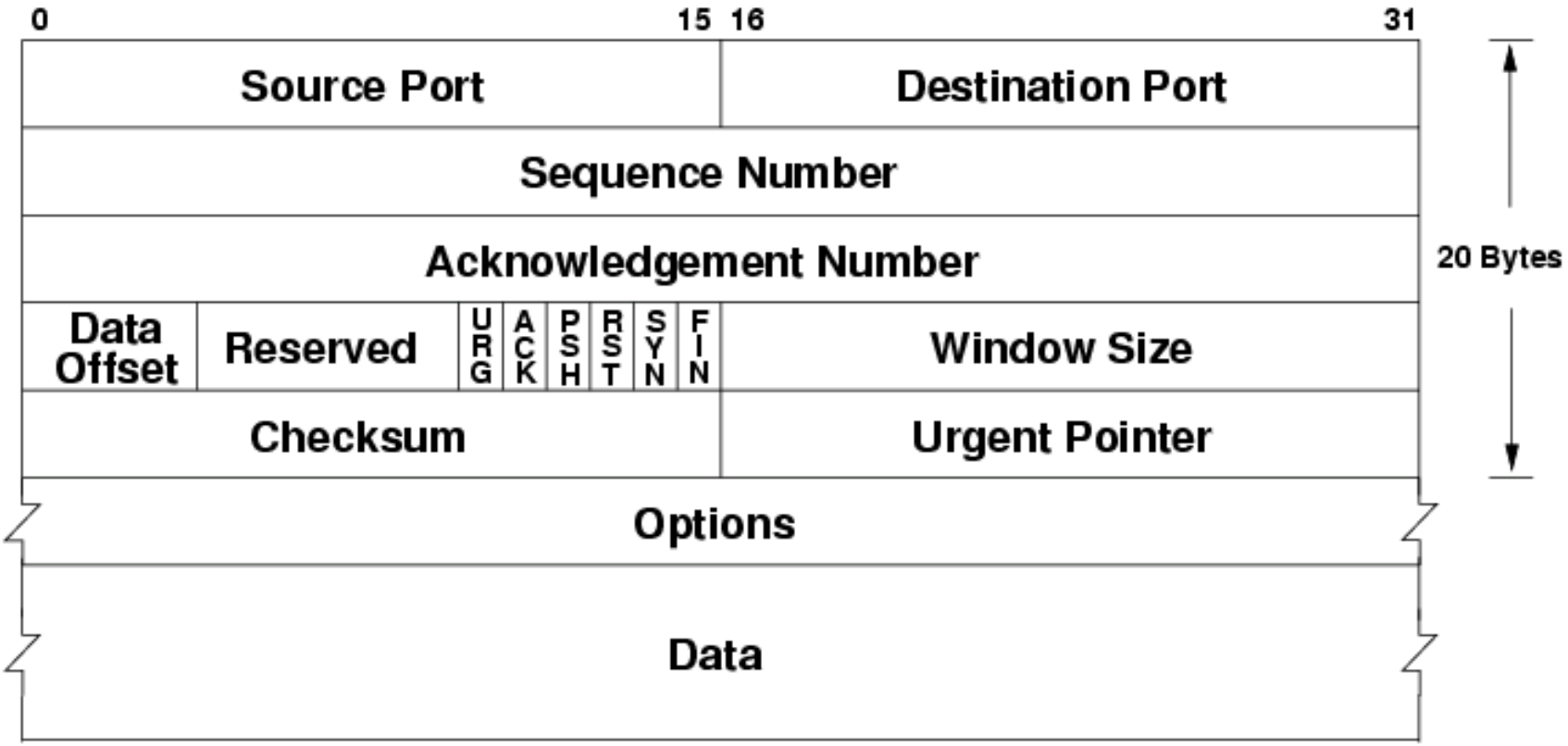
TCP in a nutshell...



http://www.elec-intro.com/cms/plus/view.php?aid=10377



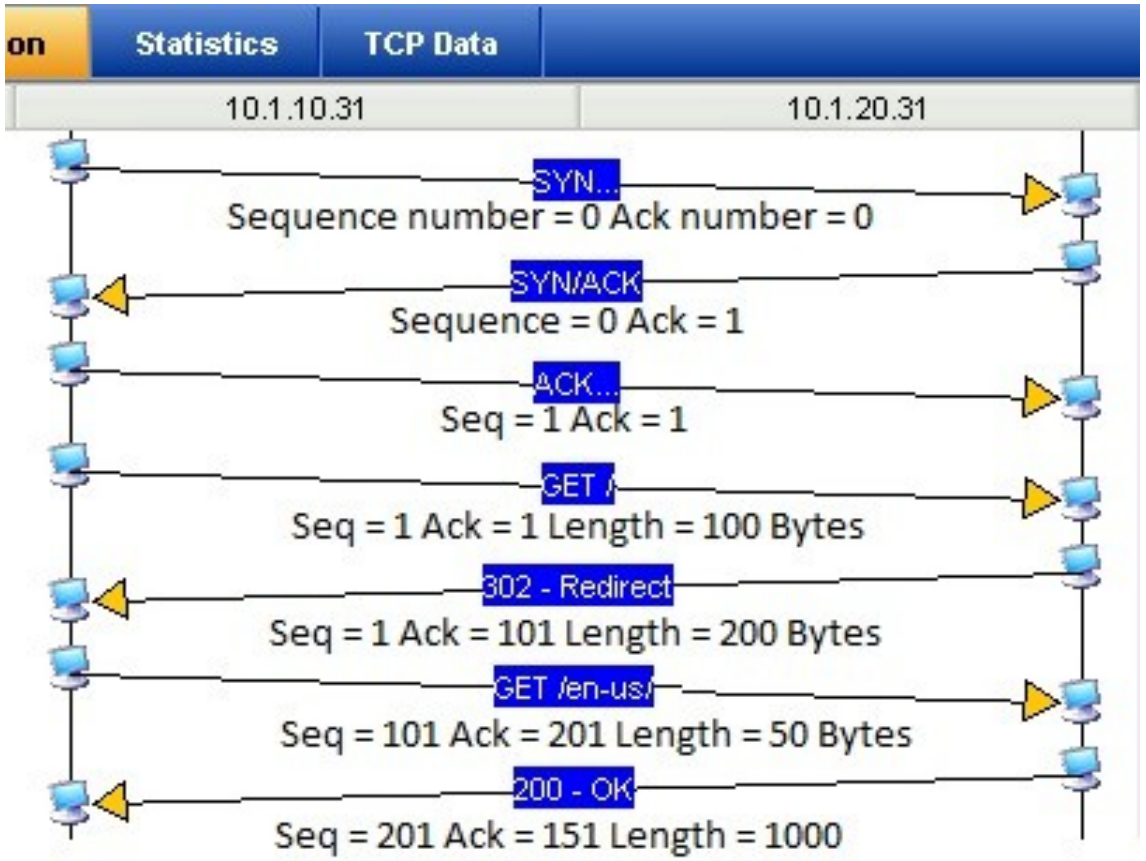
https://networkengineering.stackexchange.com/questions/40506/in-ipv4-does-the-identification-field-in-a-tcp-packet-change-for-fragmented-pack



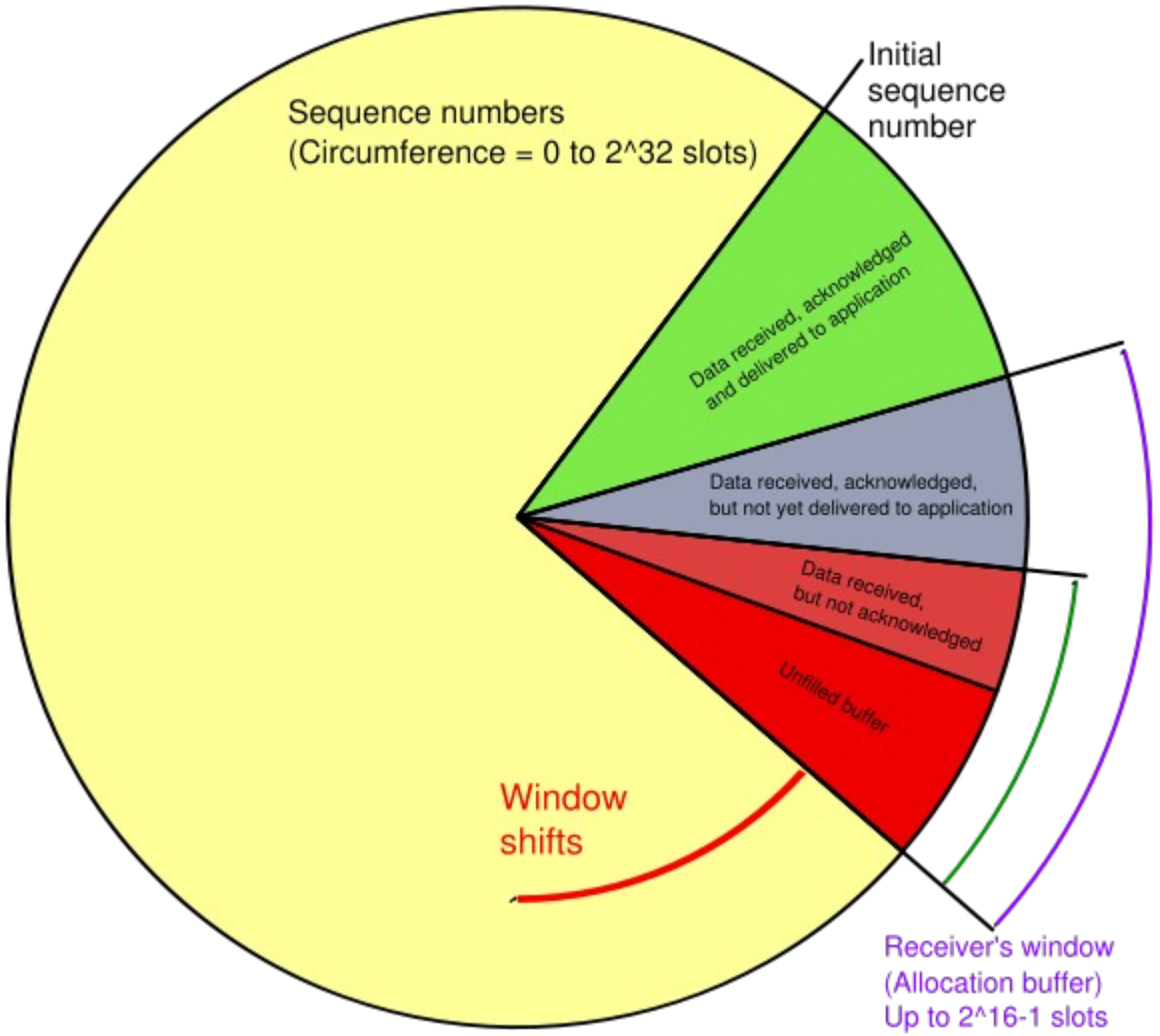
https://www.csestack.org/difference-tcp-udp-protocol/

Flags

- SYN – synchronize on a new initial sequence number
- ACK – the acknowledgment field has meaning
- RST – I have no record of a connection with the state you sent me
- FIN – this will be my last packet
- PUSH – don’t buffer things
- URG – mark things as urgent (not really used or implemented)
- NS, CWR, and ECE – explicit congestion stuff



https://www.networkdatapedia.com/post/2016/11/29/practical-tcp-series-sequence-and-acknowledgment-numbers



Mike de, CC BY-SA 3.0 <http://creativecommons.org/licenses/by-sa/3.0/>, via Wikimedia Commons

RFC 5696

- Protects against blind RSTs
- If you get a RST that is close but not exact, send a “challenge ACK”
  - Somebody who has no state for that connection will send a RST that matches exactly
  - Somebody who does have state for that connection will ignore

Videos you should watch on Tuesday 10/26...

- https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/cao
- https://www.usenix.org/conference/usenixsecurity21/presentation/tolley
- Optional (amusing) viewing if you want to understand the Fartbook reference and don't mind listening to two people (who have no idea how TCP works or what they're talking about) rambling and ranting…
  - https://twit.tv/shows/security-now/episodes/744

    (start at 1:24:12)