ECE 435 – Network Engineering
Lecture 14

Vince Weaver

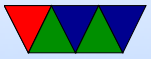
https://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

7 March 2025

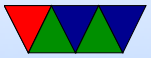
Announcements

- HW#6 due
- Will try to grade HW#5 and HW#6 before midterm
- HW#7 will be posted
- Midterm exam on Wednesday (the 12th)



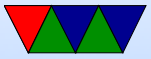
Midterm Preview (More details on Monday)

- Can have one page (8.5" x 11") of notes if you want, otherwise closed everything. I do not think you should need a calculator.
- Mostly short answer questions. No long coding exercises or protocol memorization.
- There might be some sockets code, but analyzing it not writing it.

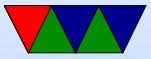


Midterm Preview – Topics

- Know the OSI layers and what each one is for.
- Be aware of socket programming in C, and what the common syscalls do (bind(), listen(), accept(), read(), write(), etc.)
- Know at a high level the following protocols:
  - WWW/http
  - e-mail
  - DNS
- Encryption (at a high level)

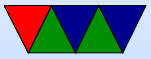


- UDP + TCP
- IPv4



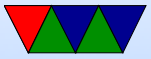
Carrier Grade NAT (CGN, CGNAT, LSN)

- Internal network uses private IP range
- Public facing server channels these through a set of external IP addresses
- NAT444 – potentially traverse 4 different IP (private in home, private in ISP, external IP)
- RFC6598 – allocate 100.64.0.0/10 for this, to avoid complications where internal/external collisions of the RFC1918 ranges



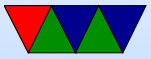
CGNAT Downsides

- Breaks end-to-end connections
- Stateful
- Doesn't fully solve IPv4 exhaustion problem cases where need a visible IP address (SSL web server?)
- Lots of devices behind a few IPs, what if get banned for spamming/security?
- Breaks port-forwarding for users, as you're in a NAT inside a NAT (port control protocol (PCP) RFC 6887 tries to work around this)



The Internet Protocol v6

- RFC2460 - RFC2466
- Started work in 1991
- Many problems with IPv4. Most notable shortage of addresses.
- IPng. (IPv5 was an experimental stream protocol)
- Migration happening, a large amount of web traffic, especially that from phones, is already switched.
- *not* backwards compatible

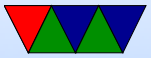


IPv6 uptake

- As of July 2016 12.5% of traffic is IPv6
- According to Google connecting to network

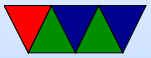
  `https://www.google.com/intl/en/ipv6/statistics.html`

  - March 2022: 34%
  - March 2024: 43%
  - March 2025: 43% (leveling off?)
- This worldwide, some countries higher (US 48%, India/France 75%)



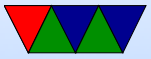
The Internet Protocol v6 Goals

- Support billions of hosts
- Reduce size of routing tables
- Simplify the protocol (so routers can be faster)
- Better security
- Pay more attention to type of service
- Aid multicasting
- Allow roaming w/o changing address
- Co-exist with existing protocols

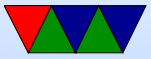


The Internet Protocol v6 features

- Address size 128 bits
  a lot of addresses. 7×10^{23} for ever square meter
- Simpler fixed length header (speeds up processing)
  Many fields not really used in IPv4 dropped (or made optional)
- Better support for options
- Better security support
  IPSEC. Originally mandatory, made optional
  Can encrypt packets at the network layer

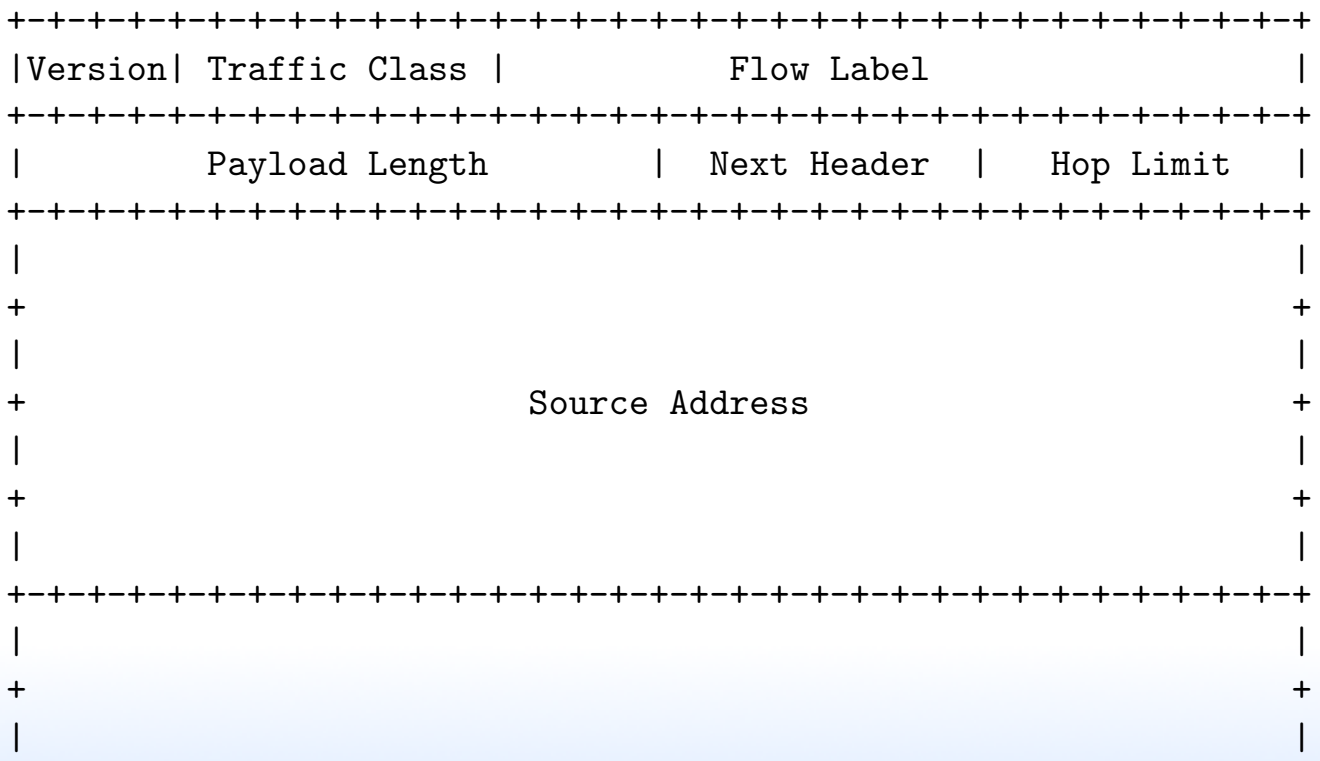


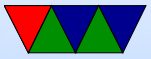
- Quality of service (???)
- Anycast (see end of slides)
- Autoconfiguration (like DHCP)
- Minimum fragment size 1280 (up from 576)
- No checksum – was slow and recalculated often

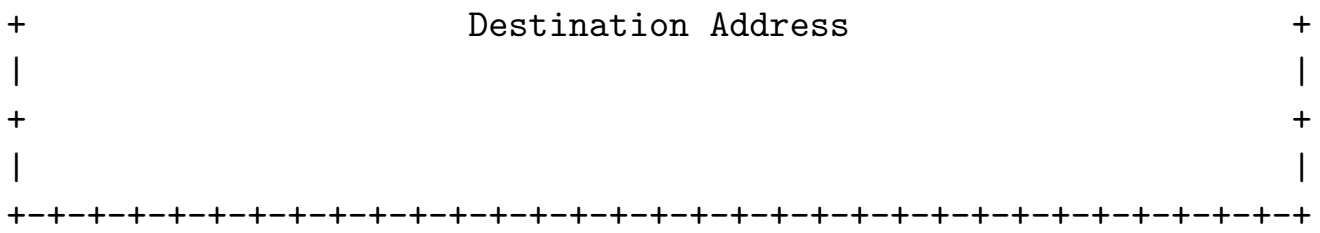


IPv6 header

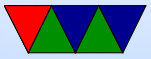
- Header fixed length of 40 bytes, with Extension headers
- ASCII art from RFC 2460





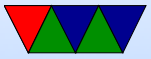


- **Version Number** (1 nibble [4-bits]) = 6
- **Differential Services/Traffic Class** (8-bits) (QoS/congesti
  6-bit differential services, 2 bits ECN (sort of like recent IPv4?)
- **Flow label** (20-bits) (for streaming?) (Recently for ECMP (Equal Cost Multipath) Line sharing. Sending packets different router paths can be bad with TCP as packets more likely to arrive late/out-of-order. Instead

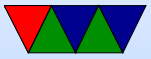


send all packets with same flow label same path, but balance different paths)

- **Payload Length** (16-bits) 64k (header bytes not counted anymore) (if you want longer, extension for Jumbograms (up to 4GB))
- **Next header** (8-bits) If nothing special identifies TCP or UDP If special options (fragmentation, security) indicated
  (TCP=0x6, UDP=0x11)
- **Hop Limit** (8-bits) TTL, big debate about whether 8-bits was enough

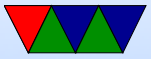


- **Source Address** (128-bits)
- **Destination Address** (128-bits)
- Why not 64-bit addresses?
- No checksum, link or transport catches issues
  What does this mean for UDP?



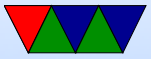
IPv6 addresses

- 2^{128} is a lot. $7x10^{23}$ per m^2 of Earth surface
- Too long for dotted decimal, use colon hexadecimal
- Why colons? .BE is a valid domain ending for one...
- X:X:X:X:X:X:X:X where X is 16 bit chunk
- F000:0123:5678:0000:0000:ABCD:0001:CAFE
- Can drop leading zeros, as well as groups of zeros
  F000:123:5678::ABCD:1:CAFE
  Note, cannot drop two sets of groups of zeros. Why? Ambiguous.



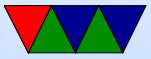
IPv6 reserved addresses

- ::1 ip6-localhost, fe00::0 ip6-localnet
- fe80:: link-local?
- 2001:: special? reserved?
- 2002:: 6to4 (deprecated)
- 64:: more 6to4 (?)
- ff00:: multicast



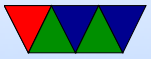
Will IPv6 addresses run out?

- Article about Huawei getting a /17 ipv6 block (a huge amount), to do that a /12 ipv6 block (even more) had to be reserved `https://www.theregister.com/2024/12/06/apnic_huawei_ipv6/`
- See `https://www.iana.org/assignments/ipv6-address-space/ipv6-addres xhtml` here for current ipv6 allocations

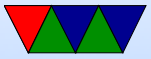


IPv6 Options

- Happen immediately after the header.
- Should occur in numerical order (though routers might be able to handle if they don't)
- Routers should inspect in order as some later might depend on earlier.
- Plain: IPV6:Next=TCP, TCP, Data
- Example: IPV6:Next=Routing, Routing:Next=TCP, TCP, Data
- Various types

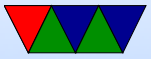


- Hop-by-hop (so far only used for jumbo frames, if that set header length is set to 0)
- Source Routing
- Fragmentation
- Authentication
- Encryption



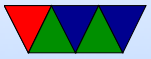
IPv6 fragmentation

- Info is in an extension header
- Routers cannot fragment, only at source
- How can this work when not know MTU?
- MTU is always greater than 1280
- Path MTU discovery protocol to discover MTU along the way (RFC 1981). (IPv4 too, set DNF and get error via ICMP) If too big, sends an error back and source needs to fragment it smaller
- Easier for source to handle than every router along way



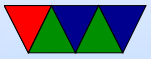
IPv6/IPv4 compat

- Dual stack – host runs both IPv4 and IPv6
  or internal is IPv6 but router converts to IPv4 before passing on
- Tunneling – encapsulate IPv6 inside of IPv4, tunnels across IPv4, split back out to IPv6 on other side of tunnel
- IPv4 mapped to IPv6 with special 96-bit prefix
  there are specs for this, not sure if really implemented

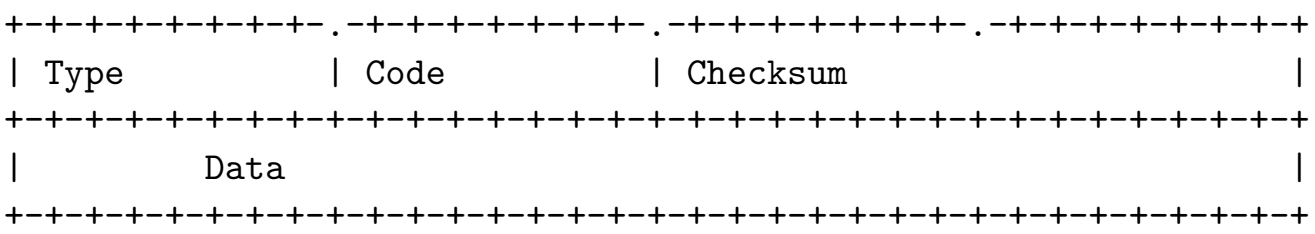


IPv6 Routing

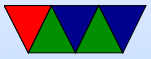
- Much like IPv4
- IPv6 network address, “prefix-length” instead of netmask
- Routing table as before



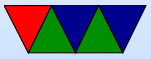
ICMP6



- Checksum: similar to TCP, also includes pseudo-header
- Type 0, Destination Uncertain
  - Various
- Type 1, Packet too big
- Time Exceeded
- Bad Parameters



- ECHO / ECHO Reply
- Neighbor Discovery Protocol (NDP)
- SEND – Secure Neighbor Discovery Protocol
- Multicast Listener Discovery (MLD)



IPv6 Anycast / Multicast

- We'll talk about this later when we talk about broadcast