ECE 435 – Network Engineering
Lecture 13

Vince Weaver

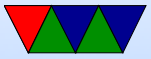
http://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

23 October 2018

Announcements

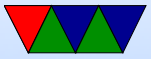
- Fire Alarm went off
- HW#6 was posted
- Recent news:
  RFC 8484 "DNS over https" was approved
  Some minor controversy.
  Mostly from the DoT (DNS over TLS RFC 7857) people



HW#5 Review

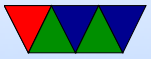
- Header length was the most trouble, top 4 bits of nibble (0x8)

- It's a web request
- Size: 0x46 = 70 bytes, 4/70 = 5.7%
- 3-way handshake SYN/SYN+ACK/ACK
- Sends hi / ack / sends back HI / ack. Note PSH sent so that it doesn't wait and piggyback
- Closing connection. FIN/ACK+FIN/ACK

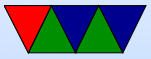


- Network connections
  - CLOSE-WAIT: received a FIN and ACKed it, waiting to close

    Only a few, https and imap
  - ESTAB: established, a few ssh, https, imap connections
  - SYN-RECV: way too many, SYN flood
  - TIME-WAIT: connection closed, waiting a bit before re-using port
  - UNCONN – UDP listening. 789? ipp, mdns (multi-cast DNS, bonjour, can find names on network w/o

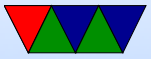


running DNS), lsof -i udp:789, rpcbind
  - LISTEN – listening. Can see ipp (CUPS printing), netbios/microsoft, apparently have SAMBA running,
- Synflood, by default Linux uses SYN cookies to defend against this



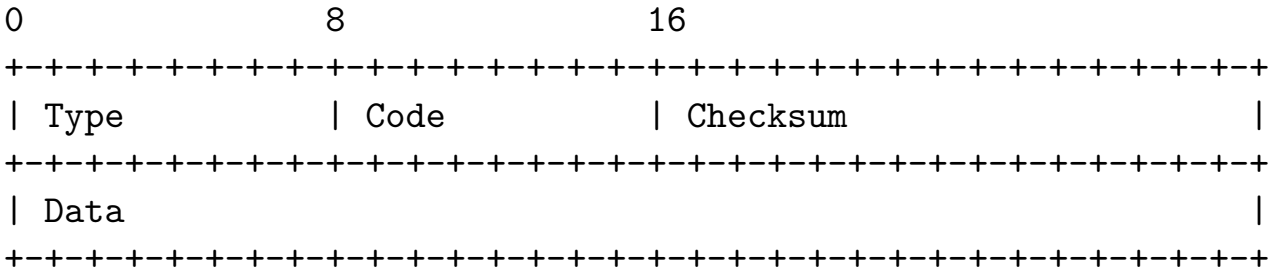
Errors

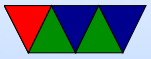
- What happens when something goes wrong with your packet?
- Does a router just drop it?
- Or does it try to let the sender know?



ICMP

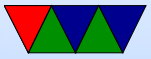
- Internet Control Message Protocol
- Carried as a payload in an IP packet
- IP header type 1
- Some sysadmins block ICMP. Why?





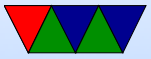
A Selection of ICMP Types/Codes

- `DESTINATION UNREACHABLE`, Also if MTU is too small but do-not-fragment set
- `SOURCE QUENCH` – should slow transmission rate (congestion), This is now usually done in transport layer
- `REDIRECT` – try the other router path
- `TIME EXCEEDED` – exceeded TTL, traceroute uses this
- `PARAMETER PROBLEM` – illegal value in header
- `ECHO`, `ECHO_REPLY` – see if machine is up
- `TIMESTAMP`, `TIMESTAMP_REPLY` – performance debug



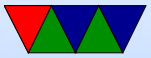
ping

- Mike Muuss in 1983
  `http://ftp.arl.army.mil/~mike/ping.html`
- Like sonar ping (Hunt for Red October), not any of the backronyms you might find.
- Ping the duck
- ICMP ECHO packet, waits for ECHO reply. Prints timing info, etc.
- Used to just say "host is alive". People would make machines called elvis.

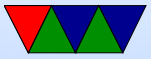


Malicious pings

- Ping of death – crash any machine on network (late 90s)
  - Technically not a ping bug, but fragmentation
  - Ping typically 56 bytes, but can be 64k
  - Technically not valid, but most will try anyway
  - 64k ping broken into 8 fragments
  - Maximum can specify is 65528, add in 20 for header, 65548
  - This is bigger than 65536, buffer overflow on reassemble

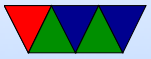


- Ping flood
- Broadcast ping to x.x.x.255 (no longer works)



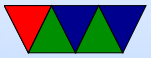
traceroute

- Van Jacobson in 1987 (also wrote tcpdump)
- Uses ICMP
- *not* tracer-t
- Send packet with TTL=1, when sends ICMP error message know where first hop is
- Send packet with TTL=2, find next
- Linux traceroute sends UDP packets as originally ICMP requests weren't supposed to generate ICMP errors
- Sends 3 packets, lists all 3 results

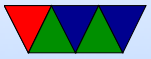


Dynamic Host Configuration Protocol (DHCP)

- RFC2131
- To get on network need IP, subnet mask, default router
- Can we automatically get this?
- Broadcasts, asking for address
- Server can respond with a fixed one (setup in config file) or handle out dynamically from range
- To avoid need for server on each subnet, can pass through



- Broadcast DHCPDISCOVER on UDP port 67.
- All servers send DHCPOFFER on port 68
- Send DHCPREQUEST, respond with DHCPACK
- Timer, needs to re-request before timer is out or server might give to someone else
- Get a “lease” from the server. Why short vs long lease/
- Can see this all inaction with `dhclient -v`
- DHCP format based on BOOTP



Setting up DHCP server

- Static vs Dynamic (how hand out static addresses?)
- Be careful to not hand out on network you don't own