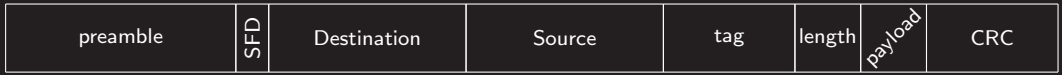
CS356: More Networking

W. Michael Petullo

University of Wisconsin–La Crosse

As of October 18, 2021

Firewalls: Ethernet Frames



Preamble (7 bytes) Alternating 0s and 1s; allows for synchronization

Start of frame delimiter (1 byte) Indicates upcoming bits start frame

Destination adderess (6 bytes) MAC address of destination

Source address (6 bytes) MAC address of source

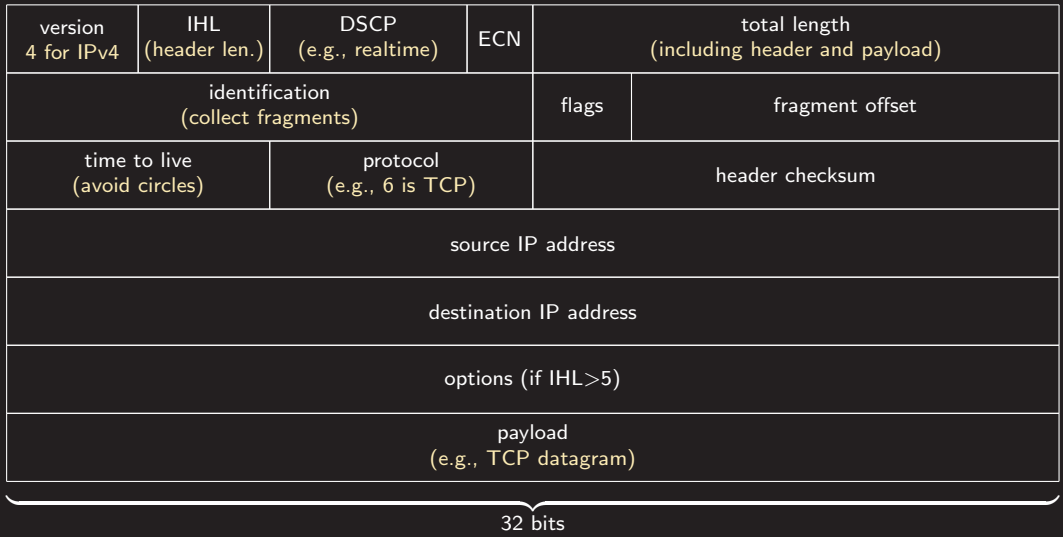
Tag (4 bytes) An optional tag

Length (2 bytes) Length of entire Ethernet frame

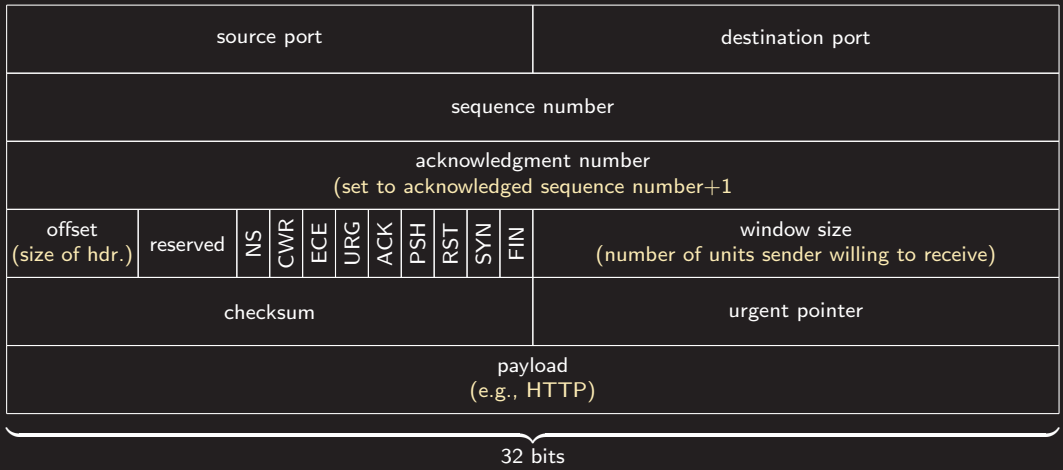
Payload (46–1500 bytes) Data carried by frame (e.g., IP packet)

Cyclic redundancy check (4 bytes) Hash of addresses, length, and data

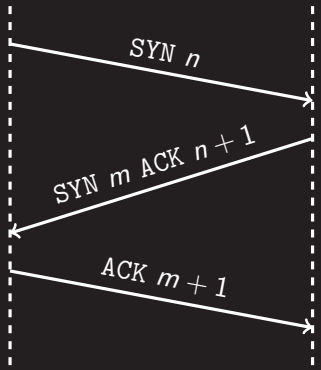
Firewalls: Internet Protocol Packets



Firewalls: Transmission Control Protocol Segments



More Networking: TCP Details



- Three-way handshake establishes initial sequence number, providing weak authenticator and preparing for reliability (`connect` system call).
- Subsequent segments contain `SYN` and `ACK` values (`recv`/`send`/`read`/`write`).
- Sender will at some point stop sending to allow `ACK` s to catch up (window size; transparent buffering).
- `FIN` flag indicates connection should close (`close`/`shutdown`).
- `RST` flag indicates something went wrong.

Wireshark demo: HTTPS (filter: `tcp.port==443`)

More Networking: Attacks on TCP

- Send `SYN` but never `ACK`.
- Guess of observe sequence number.
  - Sent `FIN` segments.
  - Sent `RST` segments.
  - Inject data segments.

Protection: `SYN` cookies (DJB, 1996)

t:	timestamp
m:	maximum segment size normally stored in `SYN` queue
F:	server-selected secret function
s:	$F(l_1, P_1, l_2, P_2, t)$
ISN:	$t \bmod 32 \parallel m \parallel s$

1. Check freshness of t
2. Recompute s and compare
3. Decode m

`https://cr.yp.to/syncookies.html`

More Networking: How Fast Can We Go?

source port	destination port
length	(optional) checksum

- DNS
- Real-time audio streams
- Real-time video streams

Wireshark demo: DNS (filter: `dns`)

More Networking: Port Scanning

TCP (nmap's `-sT`) Complete connection, but slow and noisy

SYN (nmap's `-sS`) Send `SYN` watch for `SYN-ACK`

UDP (nmap's `-sU`) Send datagram, watch for ICMP port unreachable

FIN (nmap's `-sF`) Send spurious `FIN`; might traverse firewall; closed ports send `RST`, open ports ignore

See `nmap` man page.

More Networking: UDP Programming

1. `connect` has a different meaning: the protocol itself does not have the concept of a connection, so `connect` simply indicates the host to which subsequent `write`/`send` operations will transmit or from where `read`/`recv` will accept datagrams. Alternatively, skip `connect` and use `sendto`/`recvfrom`.
2. `getattrinfo` will produce translations relevant for UDP if you set the hint parameter's `ai_socktype` field to `SOCK_DGRAM`.
3. We have sometimes relied on the end-of-file condition as a protocol terminator. With no connection, there is no end-of-file. Instead, the structure of the message must indicate when a protocol is complete. Common approaches include a special delimiter or a known length.

Complete networkudp in C on Aquinas.

More Networking: UDP Exercise

Complete networkudp in C on Aquinas.

- Consolidate and reorganize network in C.
- Refine error handling.
- Provide clear usage message, e.g., "Usage: %s HOST PORT\n", argv[0].
- Set `ai_socktype` field to `SOCK_DGRAM` in `hint` parameter to `getattrinfo`.
- Rethink `read`/`recv` loop.

More Networking: Assignments

Graded Homework Aquinas: udpscan

Reading Read 0x400–0x433

https://www.flyn.org/courses/cs356/schedule