CS326 – Systems Security

Lecture 17

Introduction to Network Security

Elias Athanasopoulos
athanasopoulos.elias@ucy.ac.cy

The Network: Game Changer

- Software exploitation over the network
  - Local vs Remote attacker
- Target resolution
  - Which hosts are good attack targets?
- Attacks at the network
  - Protocols, communication, and applications
  - Active and passive attackers
- Increased complexity
  - Different parameters interplay together

The beginning...

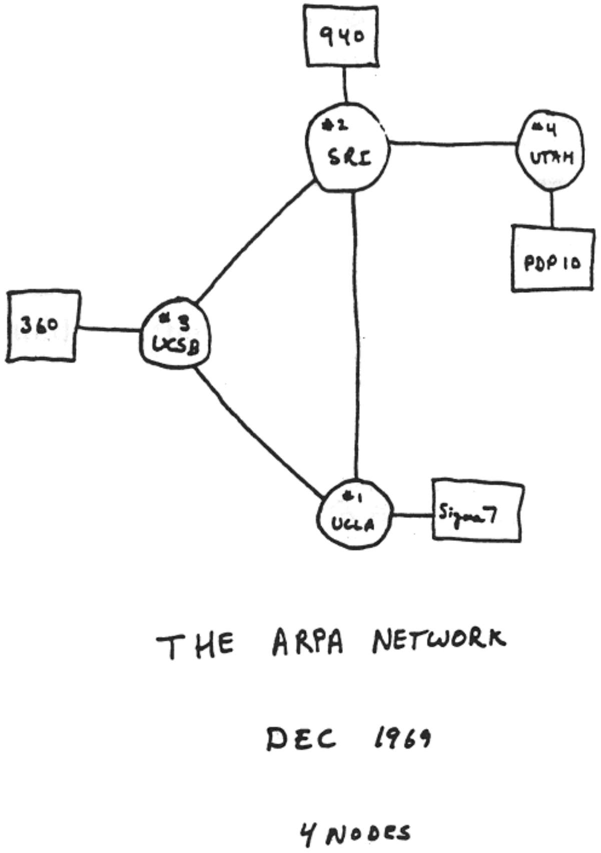


FIGURE 6.2 Drawing of 4 Node Network
(Courtesy of Alex McKenzie)

Couple of years ago…

Many apps

amazon

twitter

YouTube

reddit

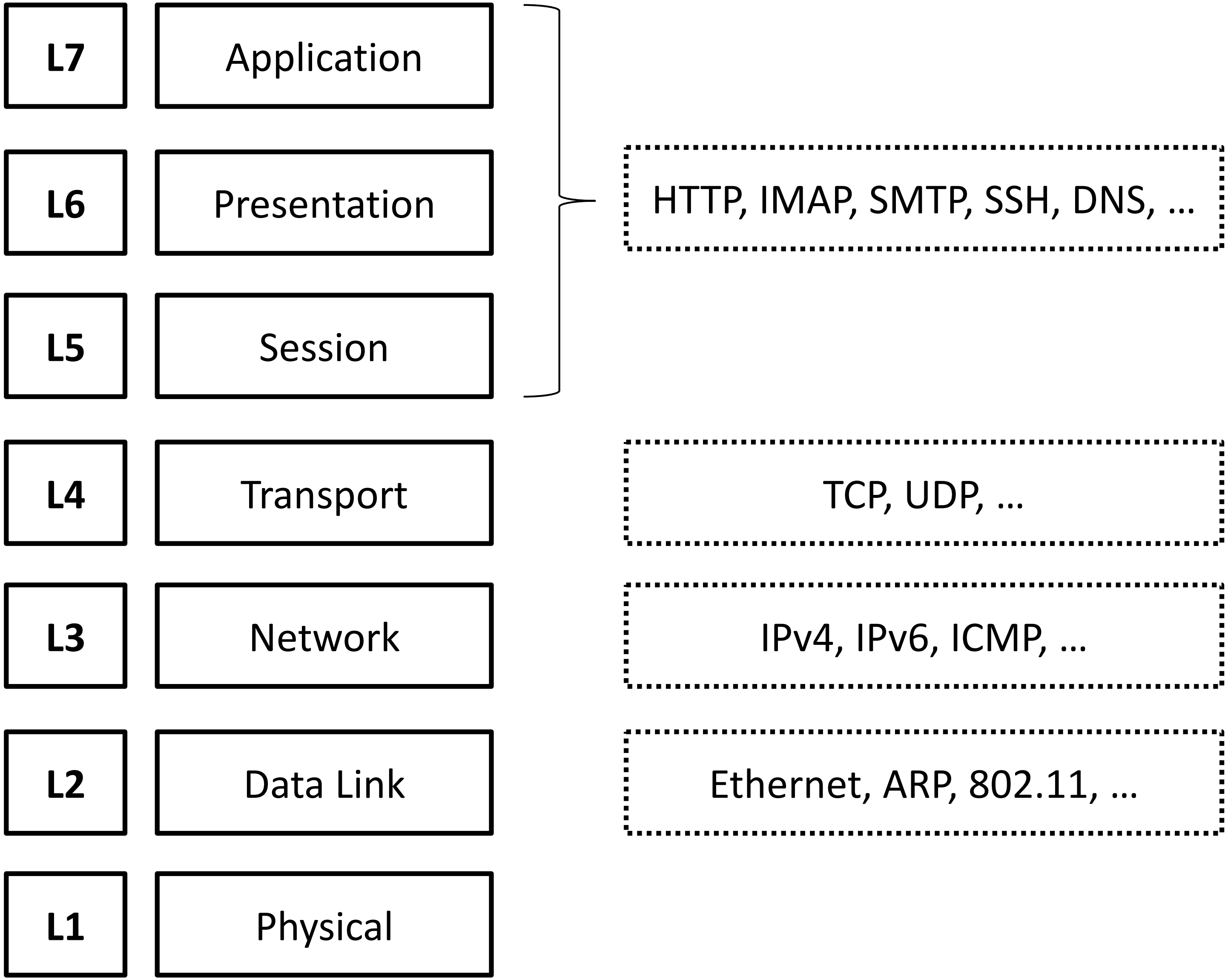
Gmail

foursquare

Insta
Instagram

Internet of Things (IoT)

Network Layers (OSI Model)



L7 Application

L6 Presentation

L5 Session

HTTP, IMAP, SMTP, SSH, DNS, …

L4 Transport

TCP, UDP, …

L3 Network

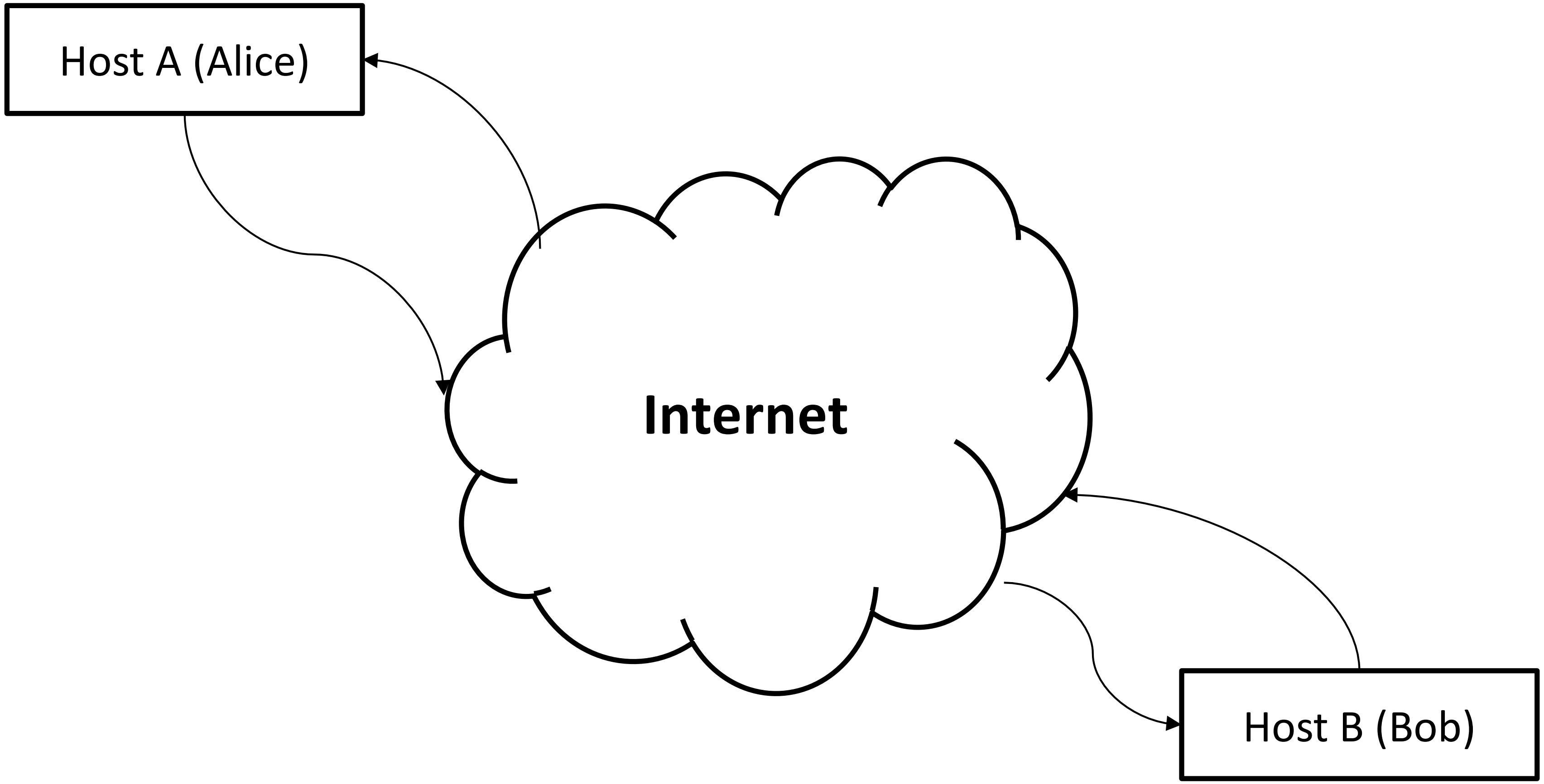
IPv4, IPv6, ICMP, …

L2 Data Link

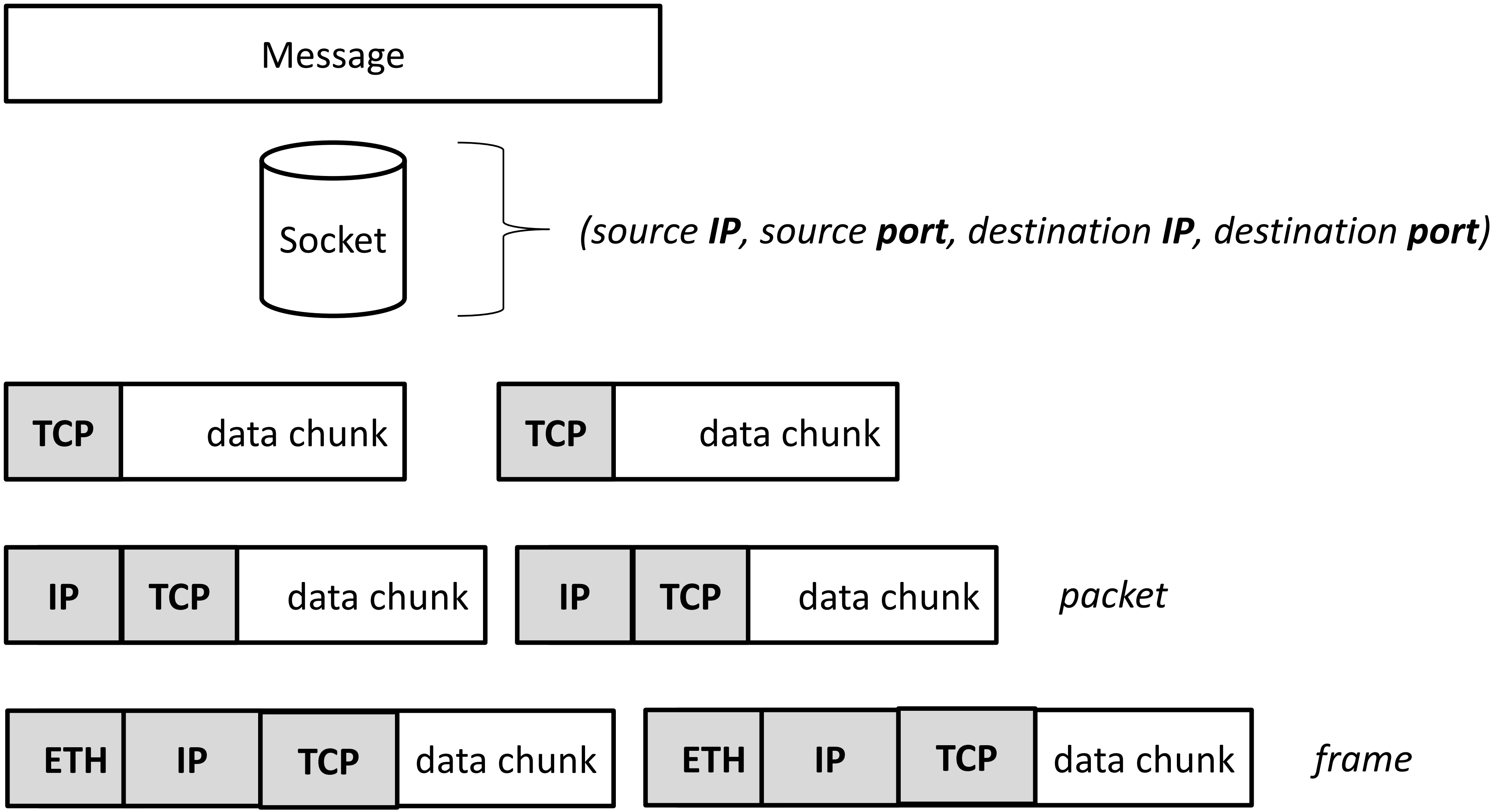
Ethernet, ARP, 802.11, …

L1 Physical

Network Communication



Sending Messages



Message

Socket

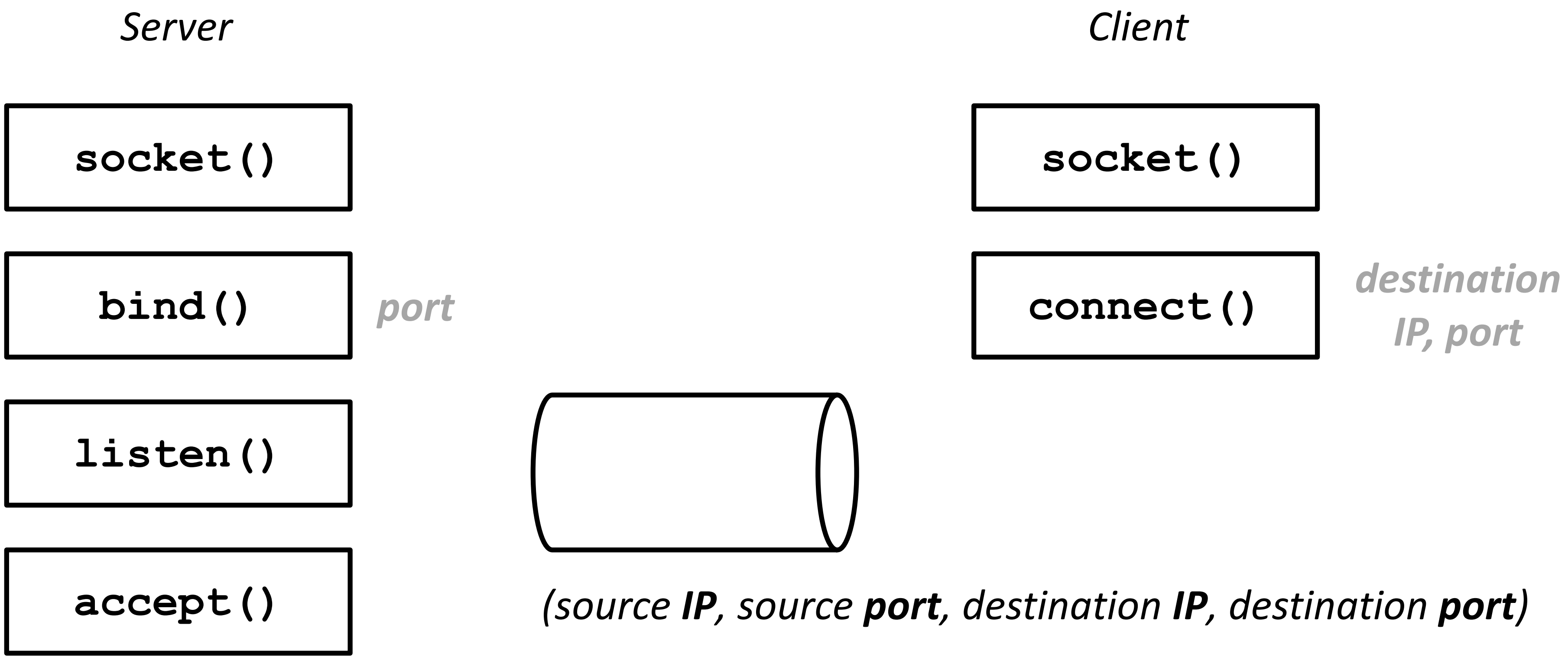
*(source **IP**, source **port**, destination **IP**, destination **port**)*

TCP | data chunk   TCP | data chunk

IP | TCP | data chunk   IP | TCP | data chunk   *packet*

ETH | IP | TCP | data chunk   ETH | IP | TCP | data chunk   *frame*

Creating Sockets



Server

`socket()`

`bind()`

port

`listen()`

`accept()`

Client

`socket()`

`connect()`

destination IP, port

*(source **IP**, source **port**, destination **IP**, destination **port**)*

IP Address

- Devices joining a network need to be addressable
  - IPv4 and IPv6 addresses
- IPV4 address
  - 4 bytes, a.b.c.d
  - E.g., 54.32.128.23
- Not all routable
  - Private addresses

IPv4 Private Addresses

	IP address range	number of addresses
24-bit block	10.0.0.0 – 10.255.255.255	16,777,216
20-bit block	172.16.0.0 – 172.31.255.255	1,048,576
16-bit block	192.168.0.0 – 192.168.255.255	65,536

Address Resolution Protocol (ARP)

- Associates Ethernet devices with IP addresses
  - A MAC address is paired with an IP address
- IP packets are sent over Ethernet frames
- Each Ethernet frame has a 48-bit address
- ARP broadcasts an IP address
  - Host with the IP address responds with an IP/Ethernet address pair

Ethernet Frame

Link Layer

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
| 48 bits                       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Destination Address           |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ 48 bits                       |
|                                 Source Address                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type (16 bits)                |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               |
|                                                               |
|                     Payload (46-1500 bytes)                   |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         32 bits CRC                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

ARP Spoofing

- ARP has no authentication
- A malicious host may *claim* to have several IP addresses
  - A malicious host that *poisons* the router with a fake IP address/MAC mapping, intercepts the traffic towards this IP address
- Defense
  - Static ARP mappings for critical services
  - Heuristic-based, e.g., a MAC address that is associated with several IP addresses indicates a possible attack

Internet Protocol

- Hosts that have acquired an IP address can send IP packets to other hosts
- A packet may cross several routers until the destination is reached
- The forward path may be different with the return path
- Packets can be lost or re-ordered
- Packets can be split in smaller packets
  - They are reassembled by the receiving router

Internet Protocol (IPv4) Packet
Network Layer

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|         Total Length          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Identification                |Flags|         Fragment Offset |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |        Header Checksum        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Source Address                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Destination Address                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Options                     | Padding       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Internet Control Message Protocol (ICMP)

- Protocol for sending error messages and operational information
  - E.g., host is down
- Used in `ping` and `traceroute`
  - `ping`: sends `ICMP ECHO_REQUEST` packets to network hosts
  - `traceroute`: prints the route packets take to network host

Reliable Communication

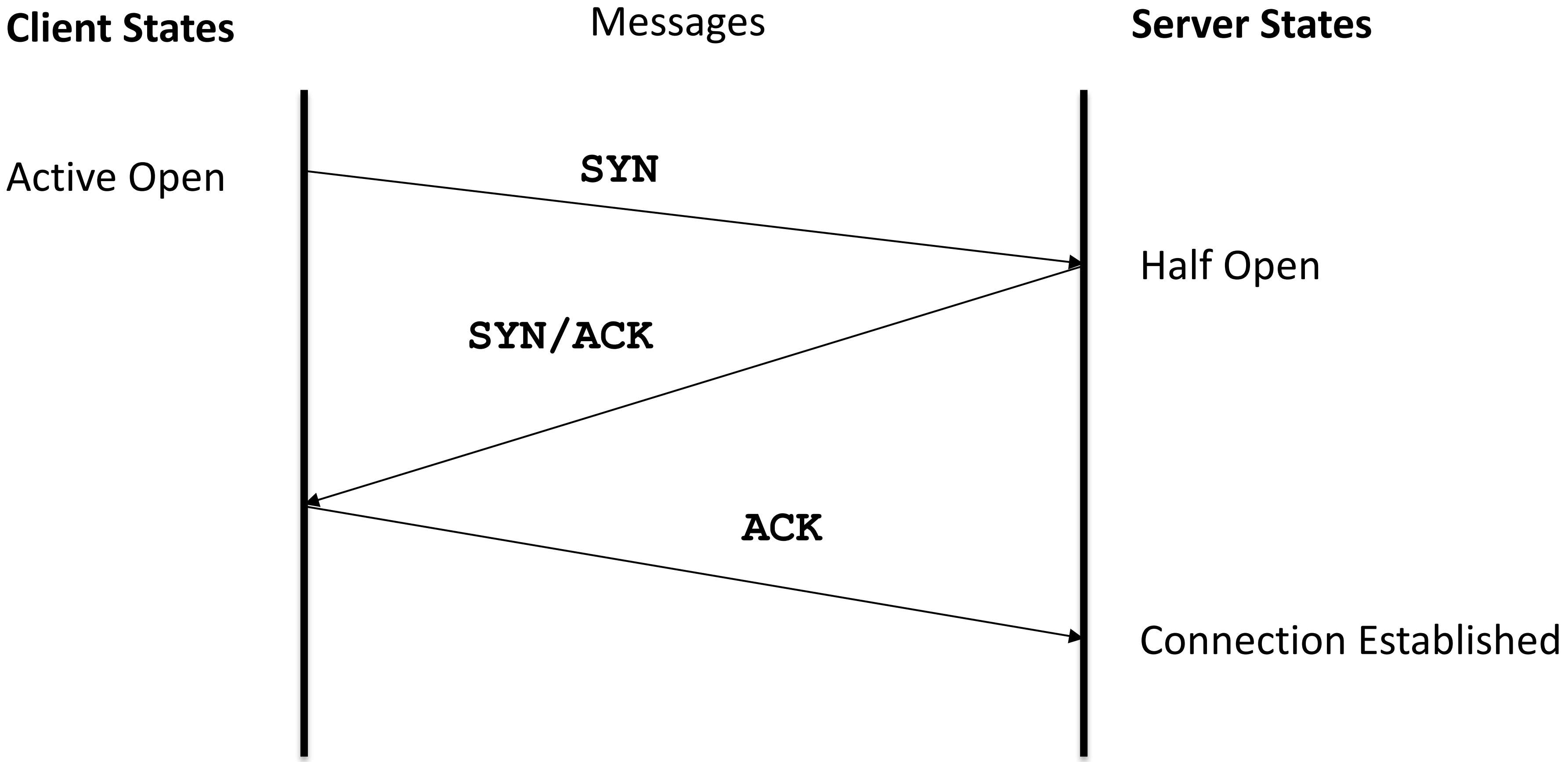
- Applications may need some logic for dealing with
  - Lost packets, re-ordering, acknowledging of received packets
- TCP implements all these features
- TCP allows reliable communication between two end points

Transmission Control Protocol (TCP)

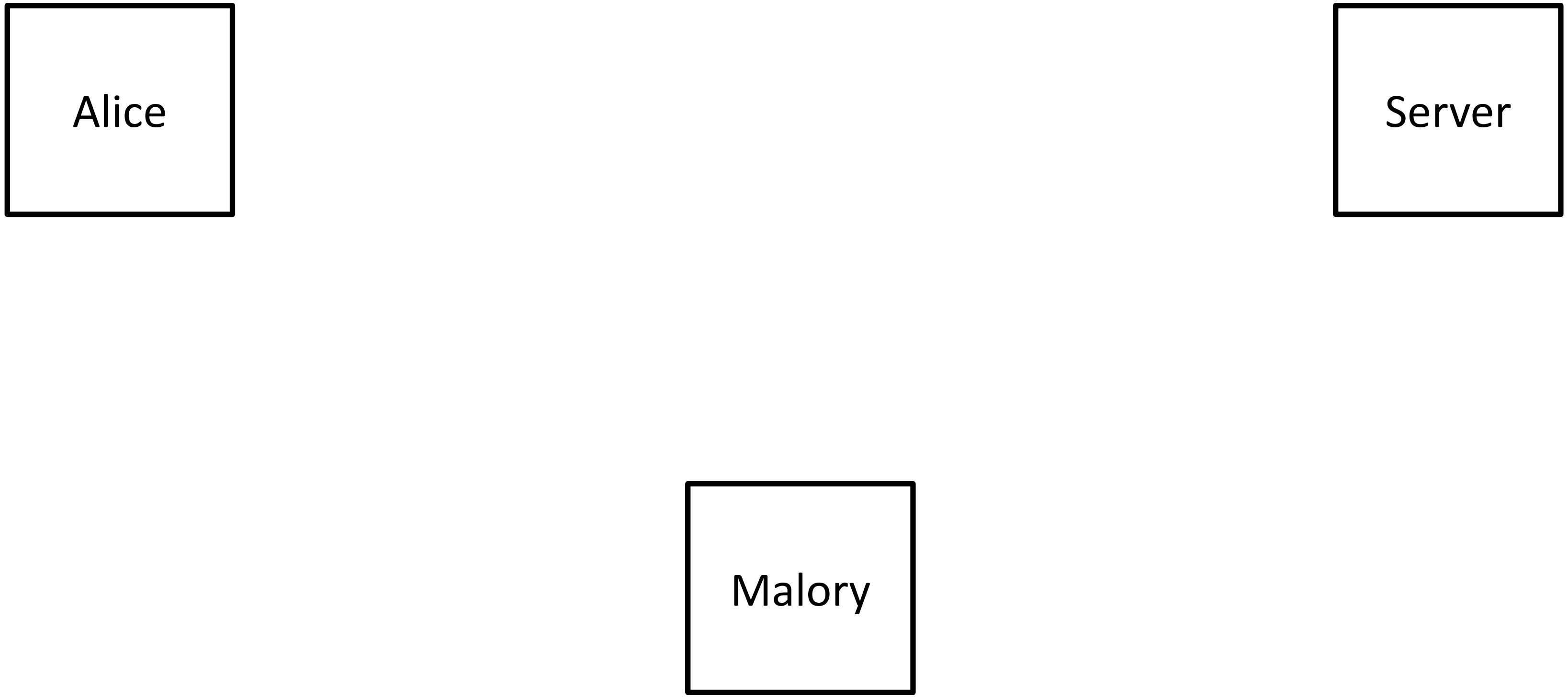
Transport Layer

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Source Port           |       Destination Port       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Sequence Number                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Acknowledgment Number                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Data   |           |U|A|P|R|S|F|                              |
| Offset | Reserved  |R|C|S|S|Y|I|          Window              |
|        |           |G|K|H|T|N|N|                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Checksum              | Urgent Pointer               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Options                          |    Padding     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        .... data ....                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

TCP Handshake



TCP Hijacking

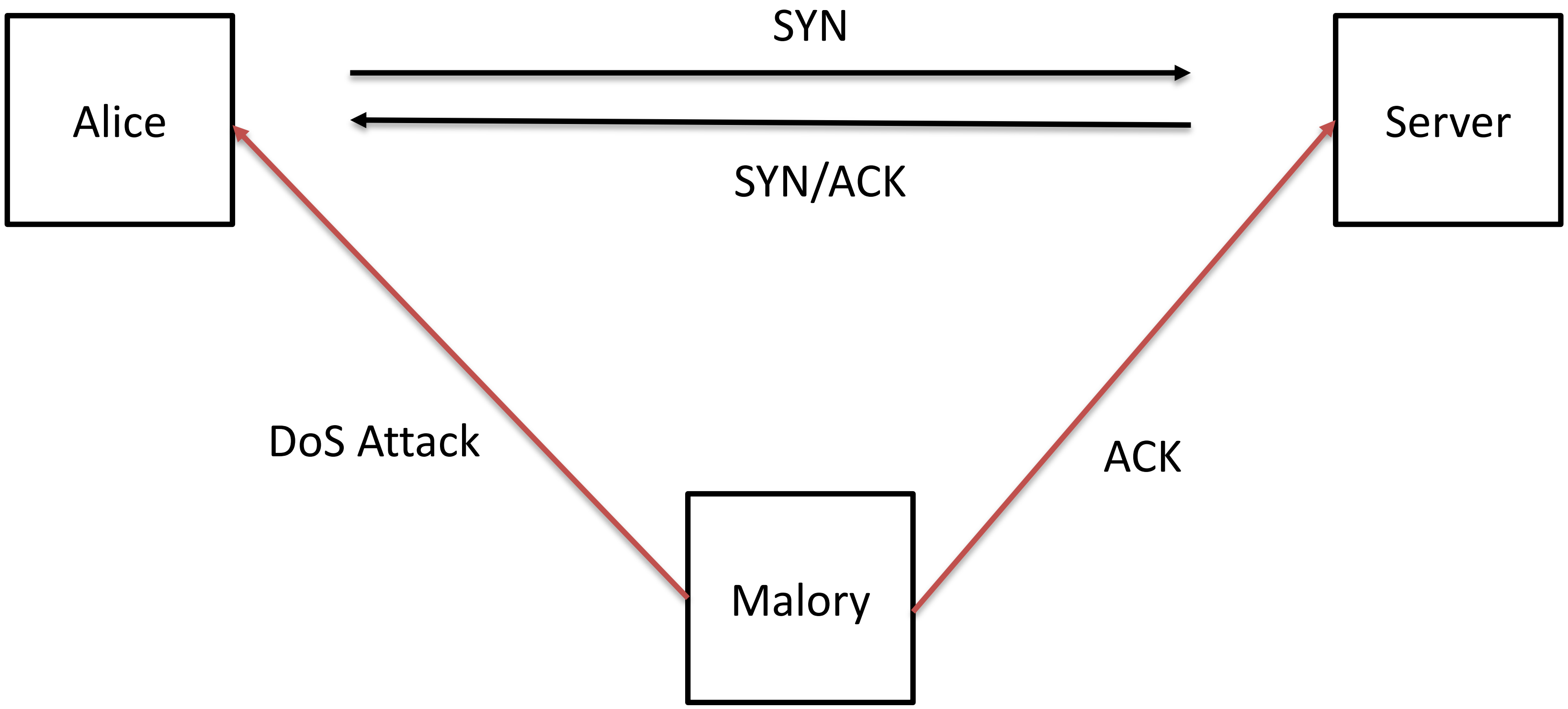


Alice

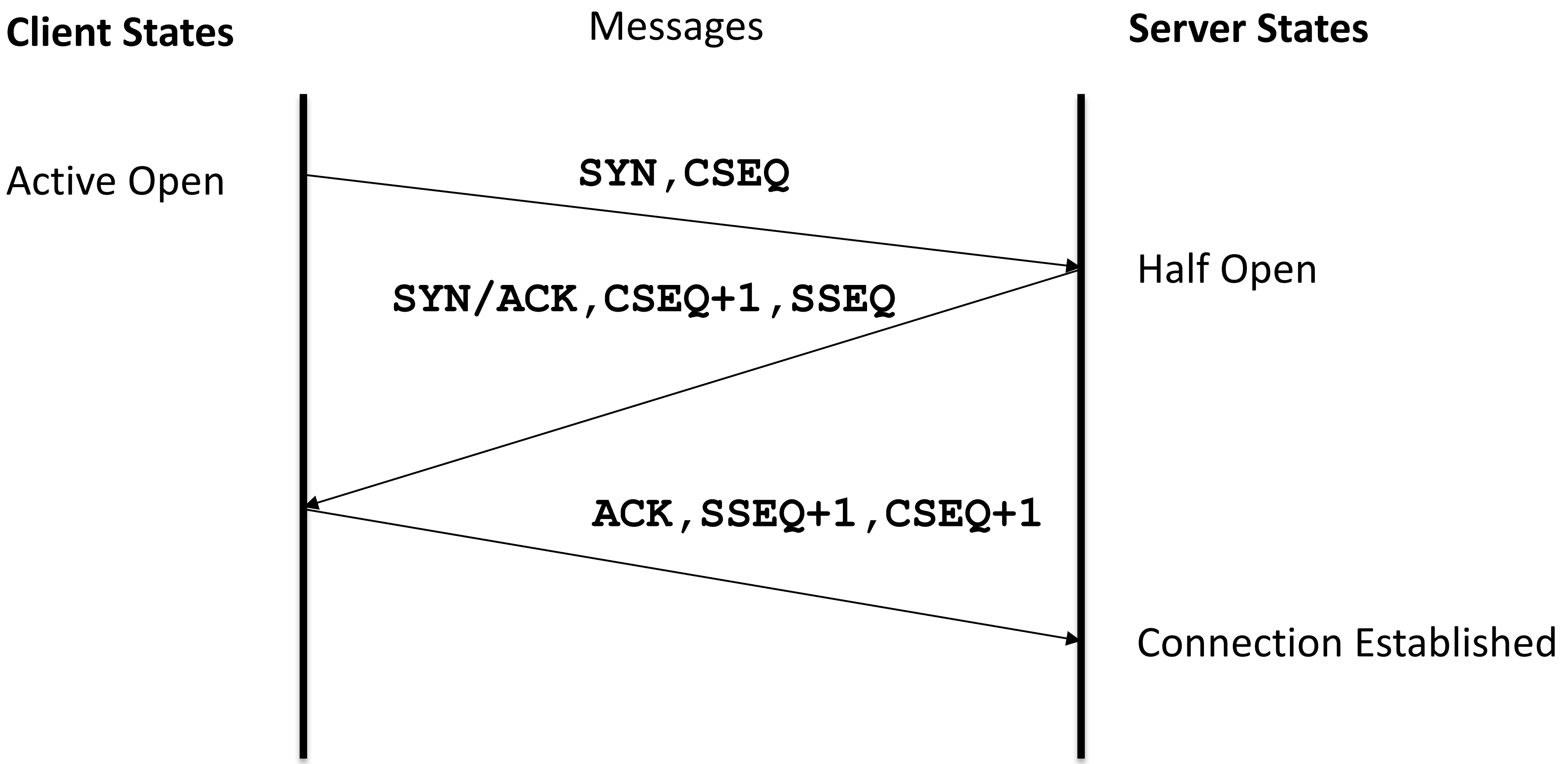
Server

Malory

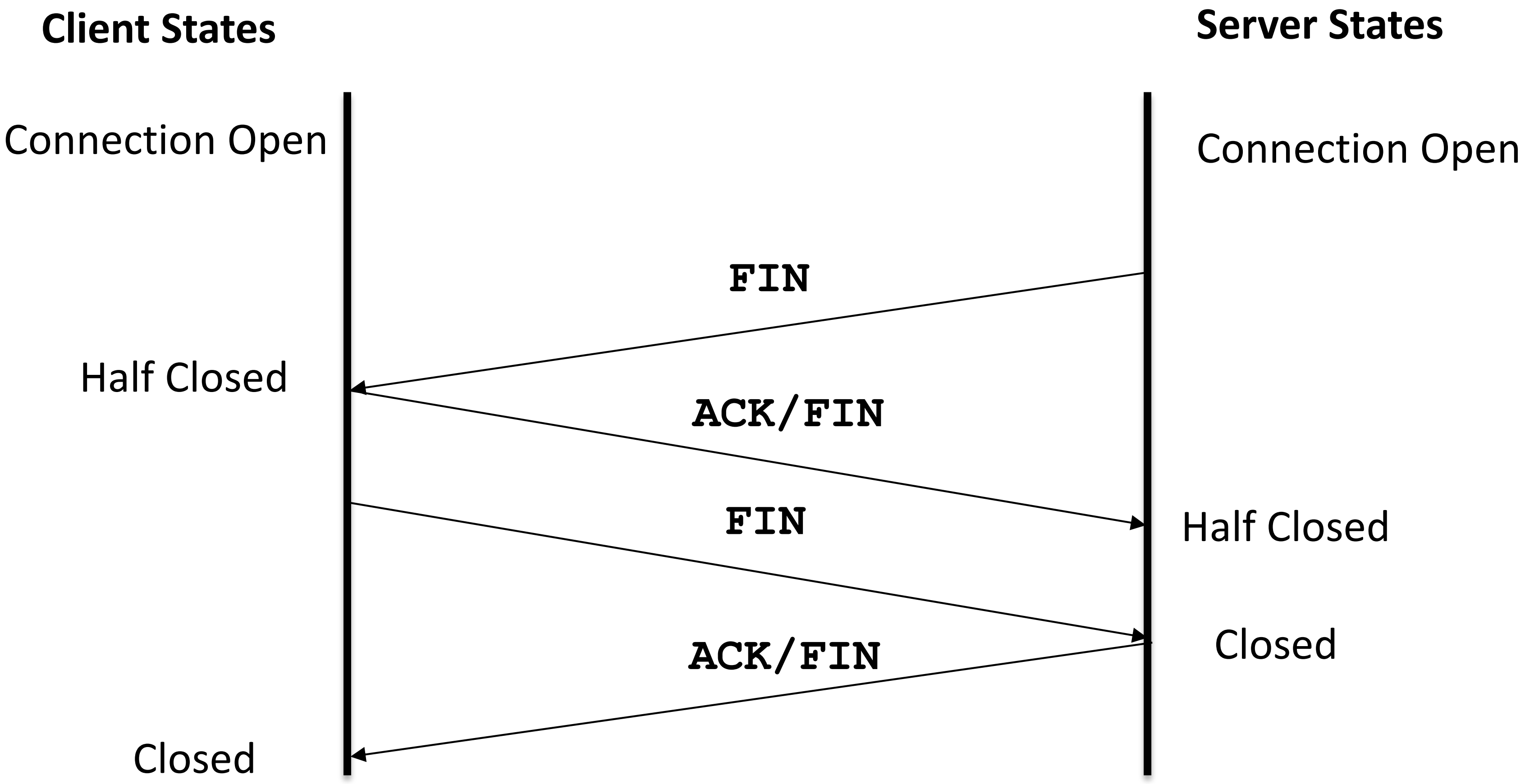
TCP Hijacking



TCP Handshake (hardened)



TCP Close


Client States
Server States
Connection Open
Connection Open
FIN
Half Closed
ACK/FIN
FIN
Half Closed
ACK/FIN
Closed
Closed

TCP Handshake Attacks

- TCP Connection Hijacking
  - **`CSEQ`** and **`SSEQ`** are random numbers
  - Predict the random numbers in the TCP handshake
  - Send packets using the predicted random numbers
- Denial of Service (DoS)
  - Send TCP SYN packets with fake IP addresses
- Backscatter traffic
  - Measure DoS attacks by monitoring SYN/ACK towards spoofed IP addresses

Domain Name System (DNS)

- Distributed tree-hierarchy with mapping names to IP addresses
  - What's the IP address of www.google.com?
- Several DNS attacks
  - The main goal of the attacks is to hijack a domain name and capture traffic
- Phishing
  - Fake web sites that look alike popular ones
  - E.g., www.bankofvvest.com and www.bankofwest.com

DNS tools

- `whois`
  - Internet domain name and network number directory service
- `dig`
  - DNS lookup utility
- `nslookup`
  - query Internet name servers interactively