CSE467: Computer Security

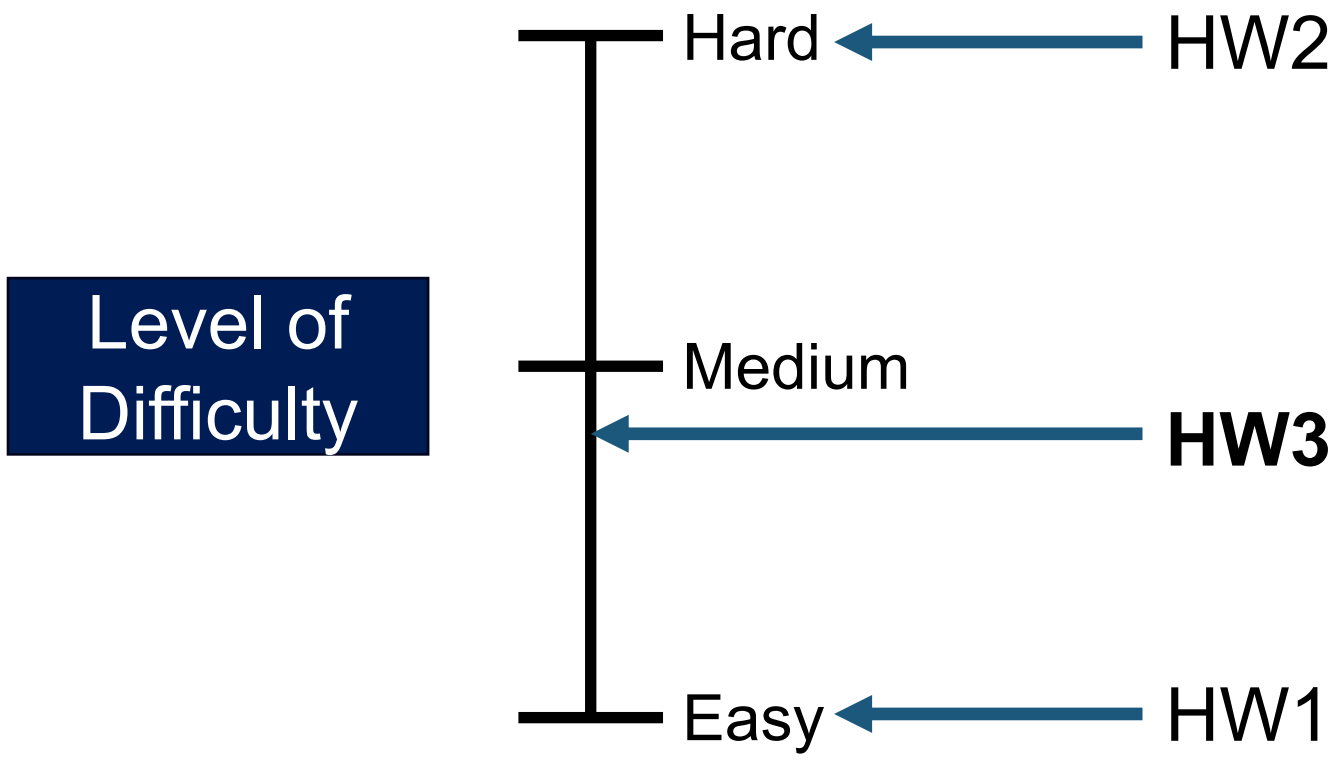
17. Introduction to Network Security

Seongil Wi

Department of Computer Science and Engineering

HW3 Will be Released

- Related to web security
- CTF-style homework (5 problems)
- **Last homework!** ☺



Network Overview

Computer Network

- A telecommunications network that allows **computers** to **exchange data**

Computer Network

- A telecommunications network that allows **computers** to **exchange data**
- Networked computing devices pass data to each other along data connections

Why is it Important?

Everything is connected!

Image from https://medium.com/@bridgettevdz/global-networks-7437c9bc7949

Internet

- An inter-net: a network of networks
  - The interconnected set of networks of the Internet Service Providers (ISPs) – e.g., KT, SKT, or LGU+
- Networks are connected using routers that support communication in a hierarchical fashion
- About 17,000 different networks make up the Internet

Protocol

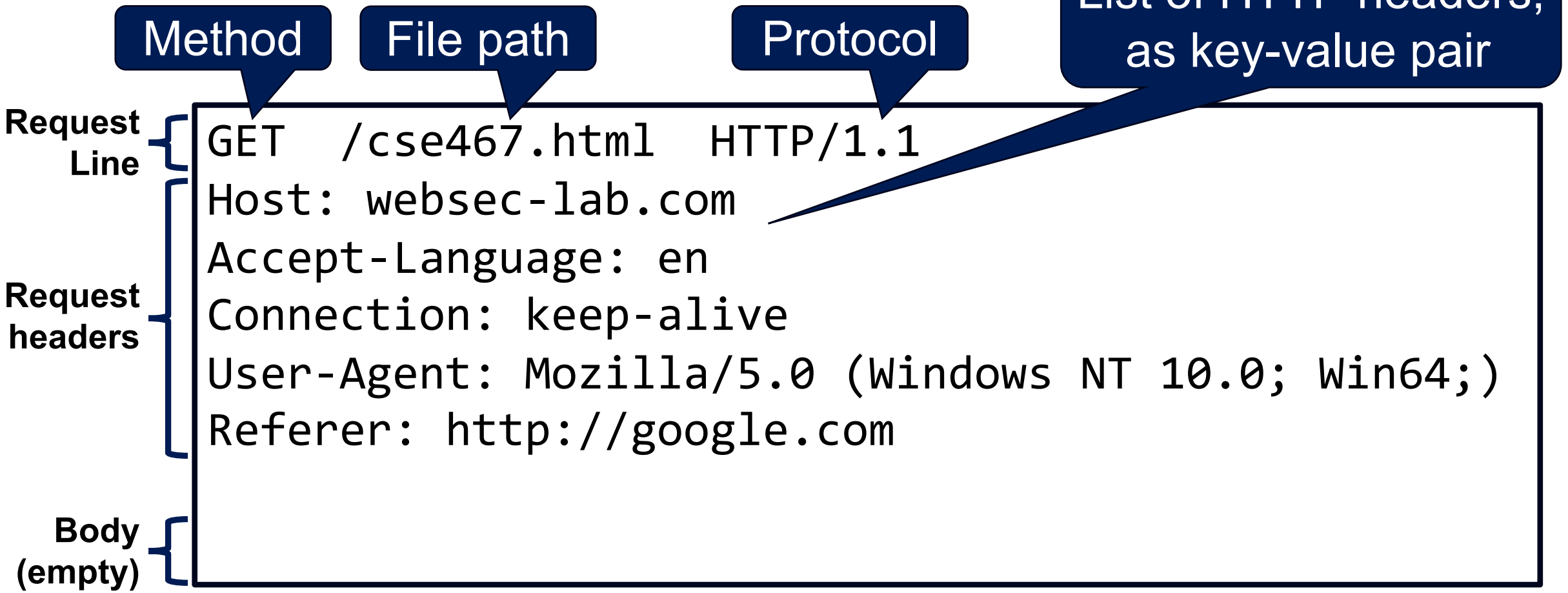
- A system of digital **rules** for data exchange between computers

Protocol

- A system of digital **rules** for data exchange between computers

RULE for Communication
- Message sequence
- Message format
- …

Recap: HTTP Request



Protocol

- A system of digital **rules** for data exchange between computers
- Many layered protocols

OSI Model

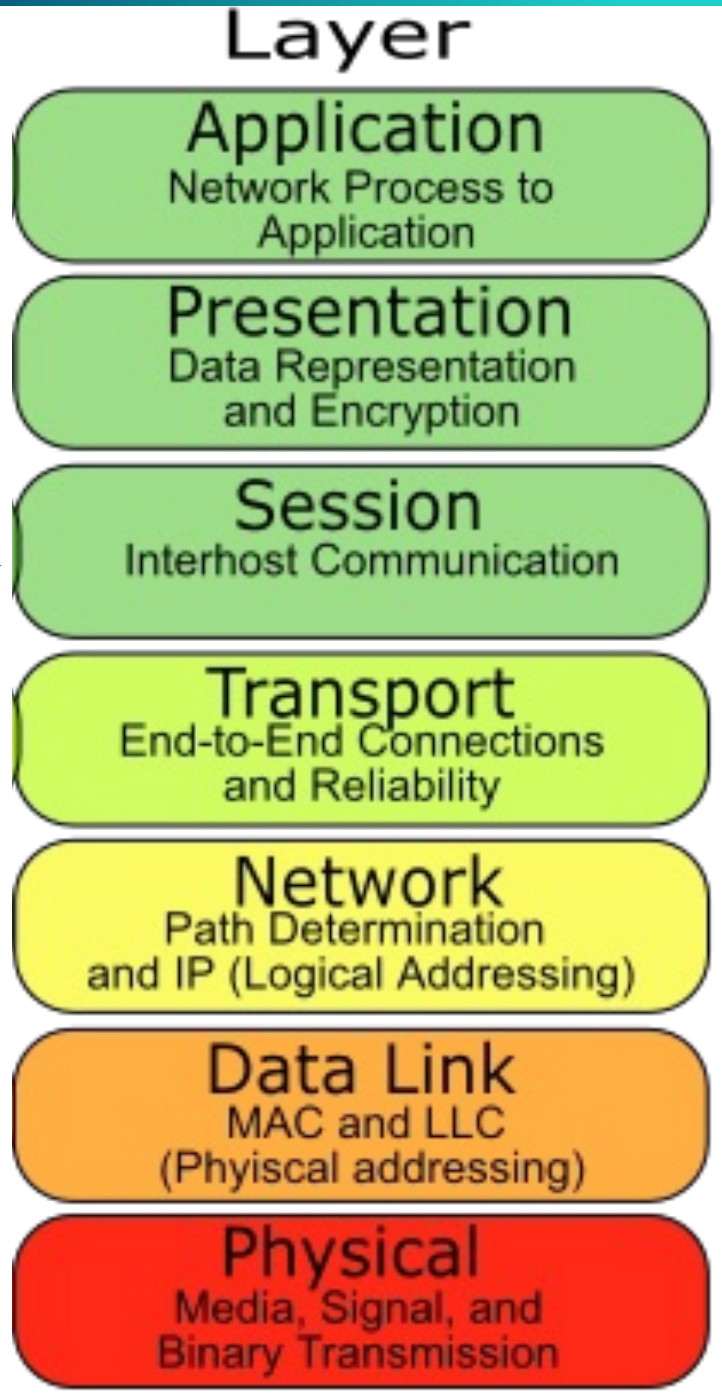
- OSI: Open System Interconnection model

- Definition
  - A conceptual model that characterizes the internal functions of a communication system by partitioning it into **abstraction layers**

OSI Model

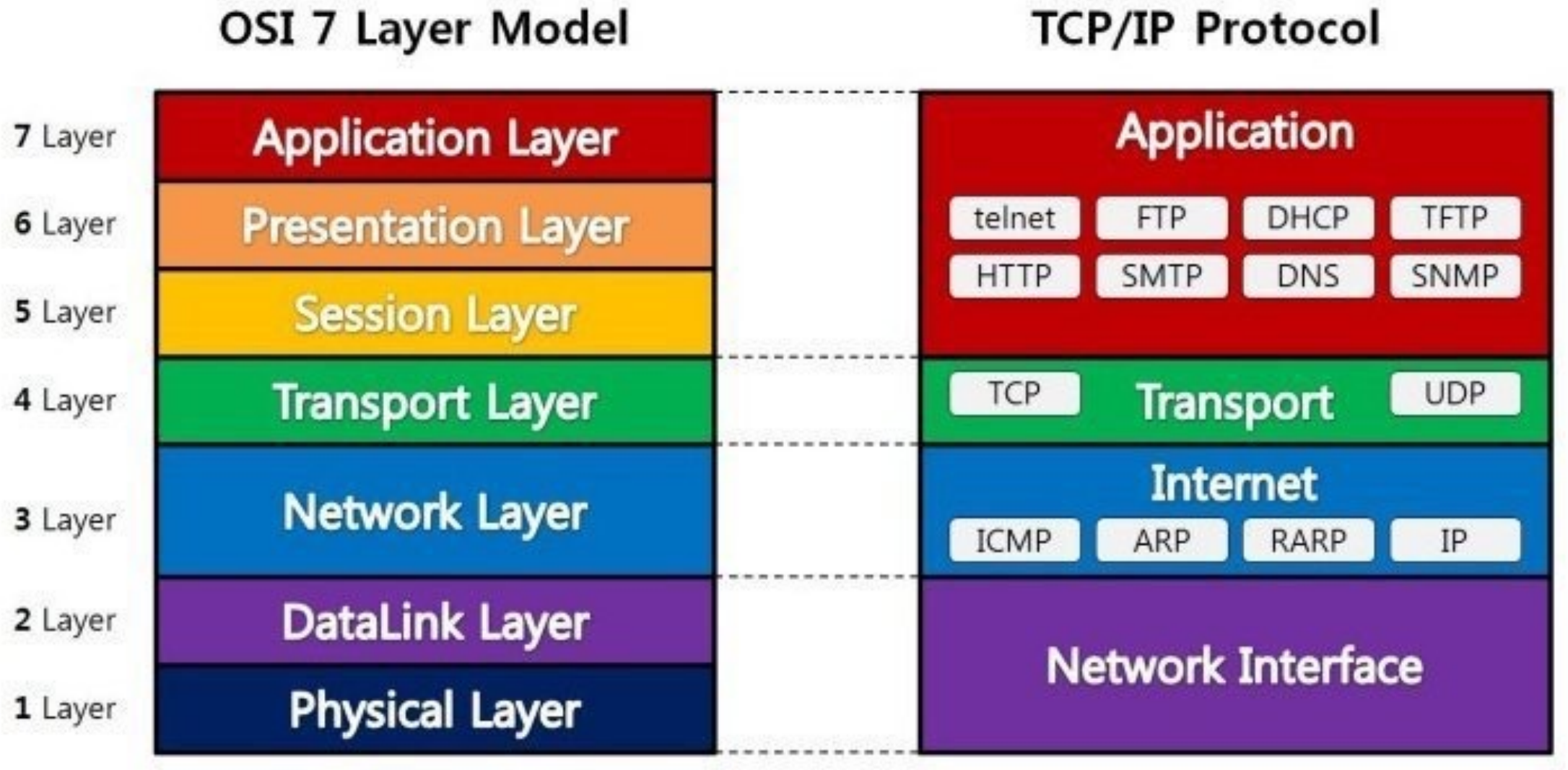
Benefits:

- Manageable
- Standardizes interfaces
- Ensures interoperability
- …



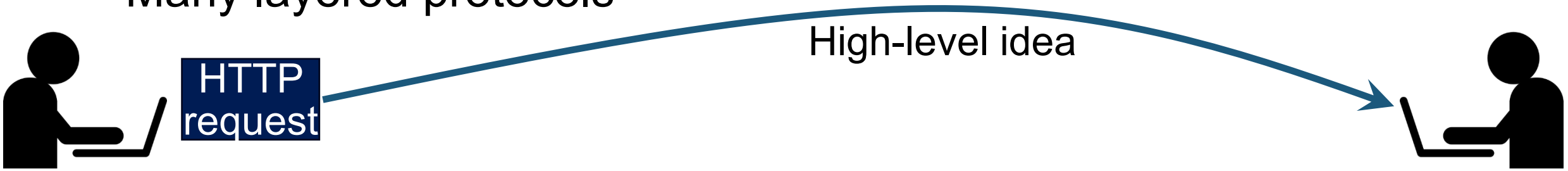
Details: take *Computer Networks* course

Protocol


OSI 7 Layer Model
TCP/IP Protocol
7 Layer
Application Layer
6 Layer
Presentation Layer
5 Layer
Session Layer
4 Layer
Transport Layer
3 Layer
Network Layer
2 Layer
DataLink Layer
1 Layer
Physical Layer
Application
telnet
FTP
DHCP
TFTP
HTTP
SMTP
DNS
SNMP
TCP
Transport
UDP
Internet
ICMP
ARP
RARP
IP
Network Interface

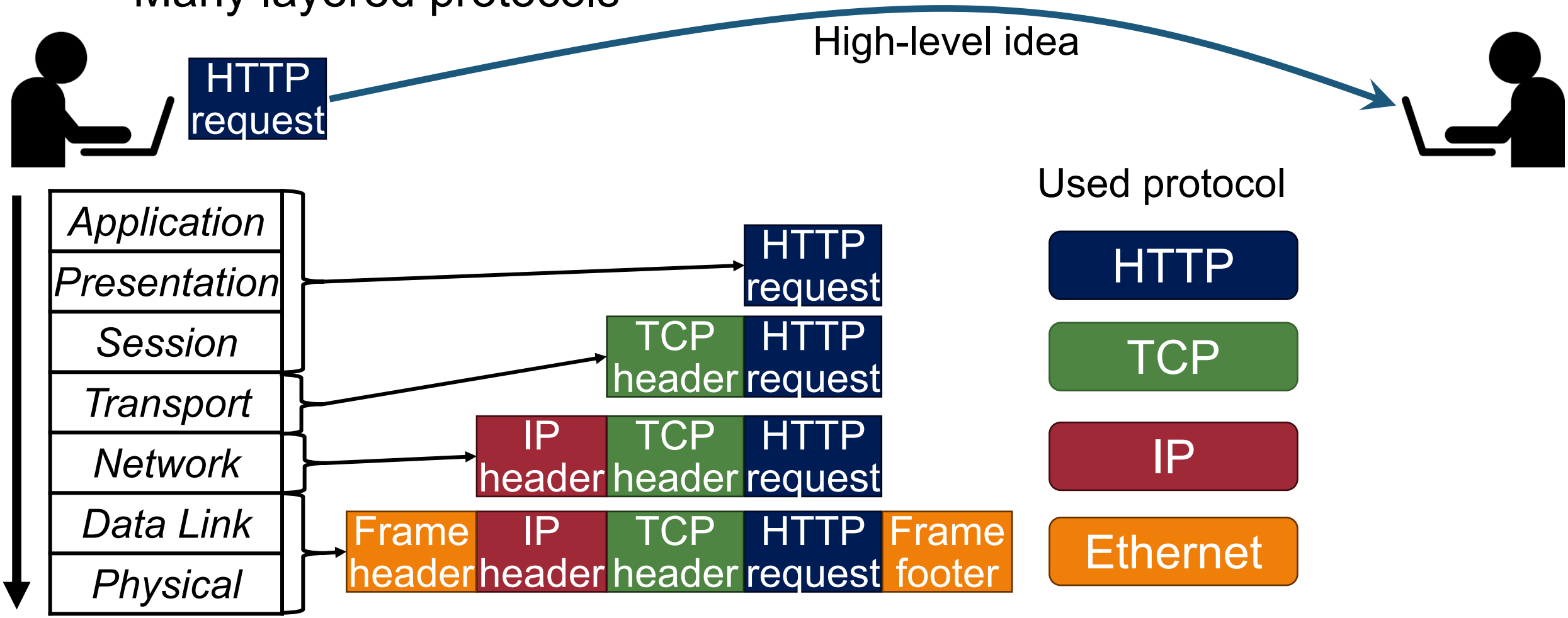
Data Encapsulation

- A system of digital **rules** for data exchange between computers
- Many layered protocols



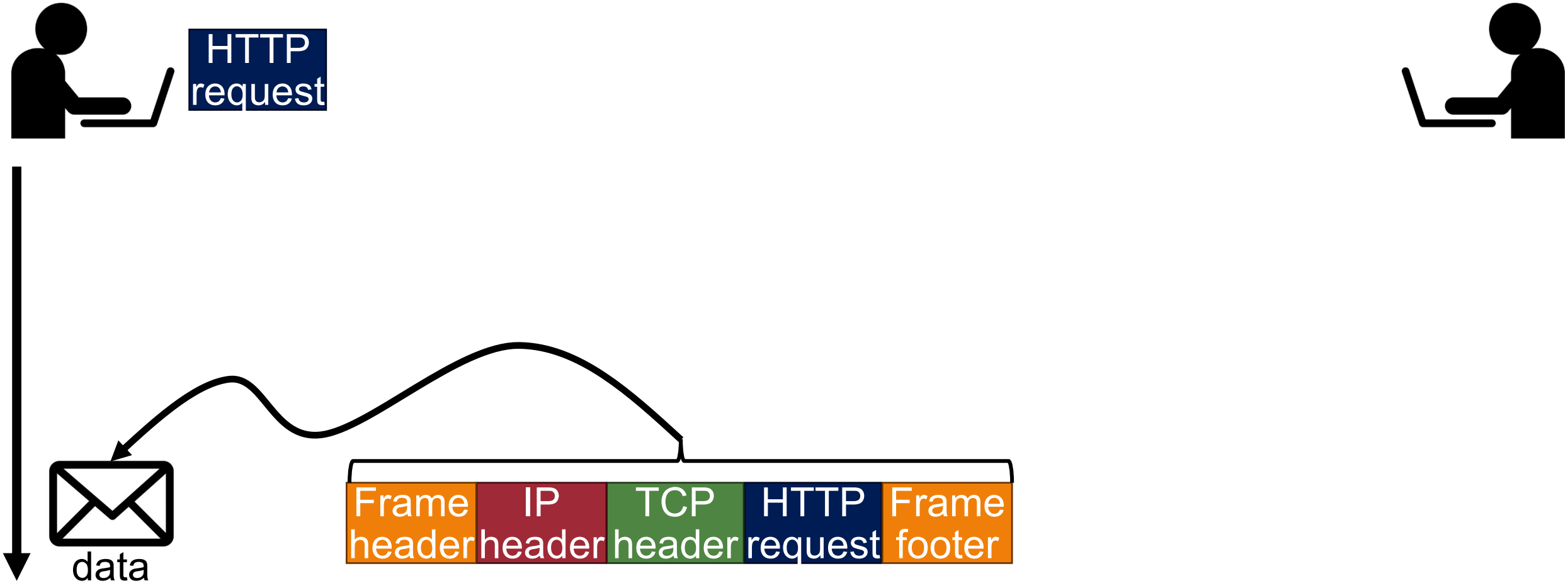
Data Encapsulation

- A system of digital **rules** for data exchange between computers
- Many layered protocols



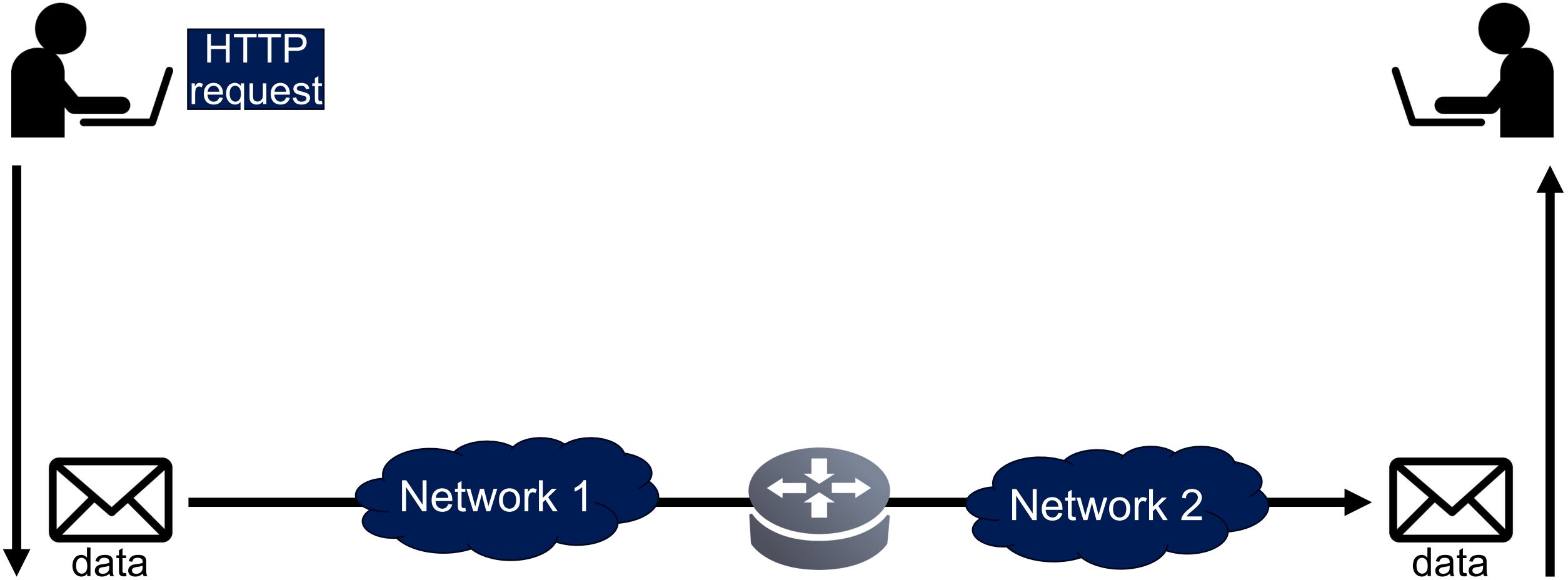
Protocol

- A system of digital **rules** for data exchange between computers
- Many layered protocols



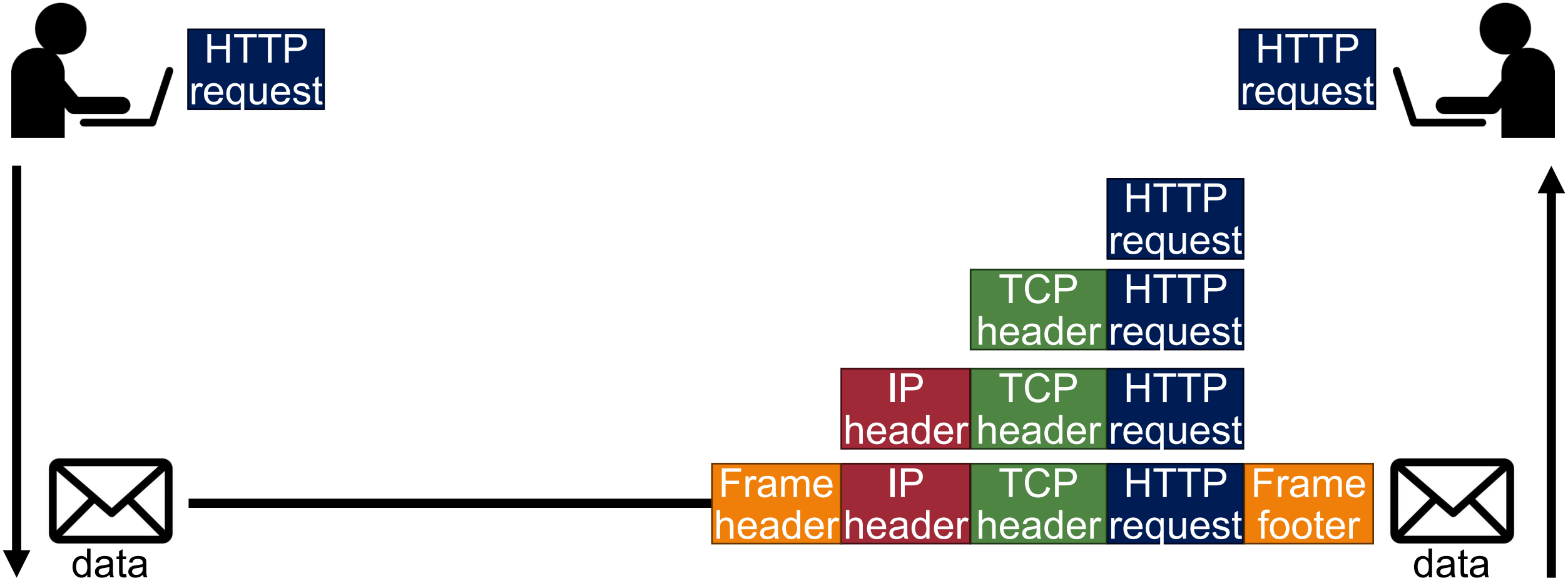
Protocol

- A system of digital **rules** for data exchange between computers
- Many layered protocols



Data De-Encapsulation

- A system of digital **rules** for data exchange between computers
- Many layered protocols

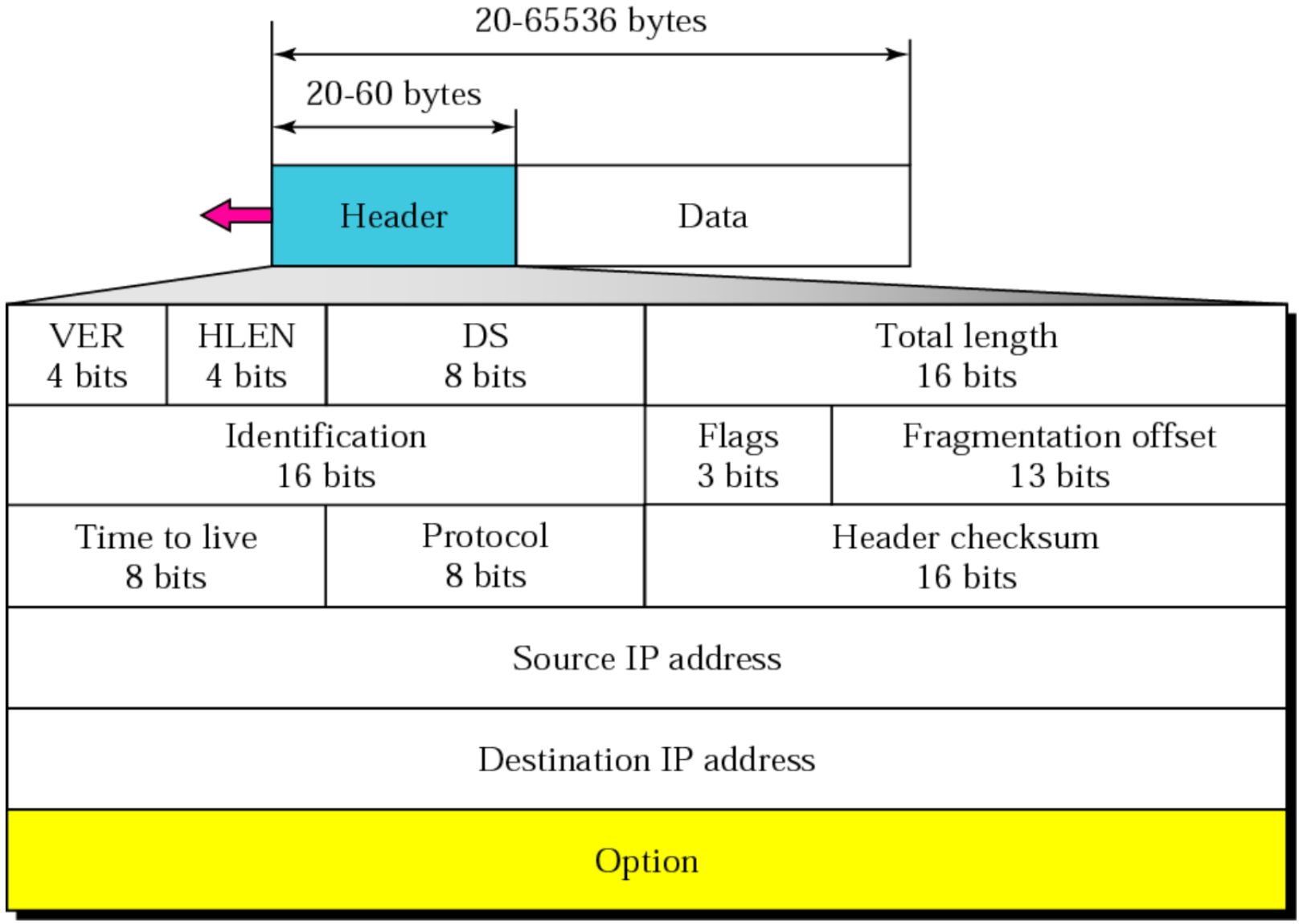


Protocol Example: Internet Protocol (IP)

- The principal communications protocol

- Characteristics of IP
  - **Connectionless**: mis-sequencing
  - **Unreliable**: may drop packets…
  - **Best effort**: … but only if necessary
  - **Datagram**: individually routed

IP Datagram


20-65536 bytes
20-60 bytes
Header
Data
VER
4 bits
HLEN
4 bits
DS
8 bits
Total length
16 bits
Identification
16 bits
Flags
3 bits
Fragmentation offset
13 bits
Time to live
8 bits
Protocol
8 bits
Header checksum
16 bits
Source IP address
Destination IP address
Option

Protocol Example: ICMP

- Internet Control Message Protocol (ICMP)
  - Used by a router/end-host to report some types of error
    - E.g., `Destination Unreachable`: packet can't be forwarded to its destination
    - E.g., `Time Exceeded`: Time To Live (TTL) reached zero, or fragment didn't arrive in time
- Encapsulated in the IP packet

```
$ ping google.com
PING google.com (142.250.206.238): 56 data bytes
64 bytes from 142.250.206.238: icmp_seq=0 ttl=115 time=31.598 ms
64 bytes from 142.250.206.238: icmp_seq=1 ttl=115 time=35.777 ms
64 bytes from 142.250.206.238: icmp_seq=2 ttl=115 time=40.632 ms
64 bytes from 142.250.206.238: icmp_seq=3 ttl=115 time=35.873 ms
...
```

Protocol Example: TCP and UDP

- TCP and UDP
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)
- Core protocols of the Internet

TCP Segment Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Sequence Number			
64	Acknowledgment Number			
96	Data Offset	Res	Flags	Window Size
128	Header and Data Checksum		Urgent Pointer	
160...	Options			

UDP Datagram Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Length		Header and Data Checksum	

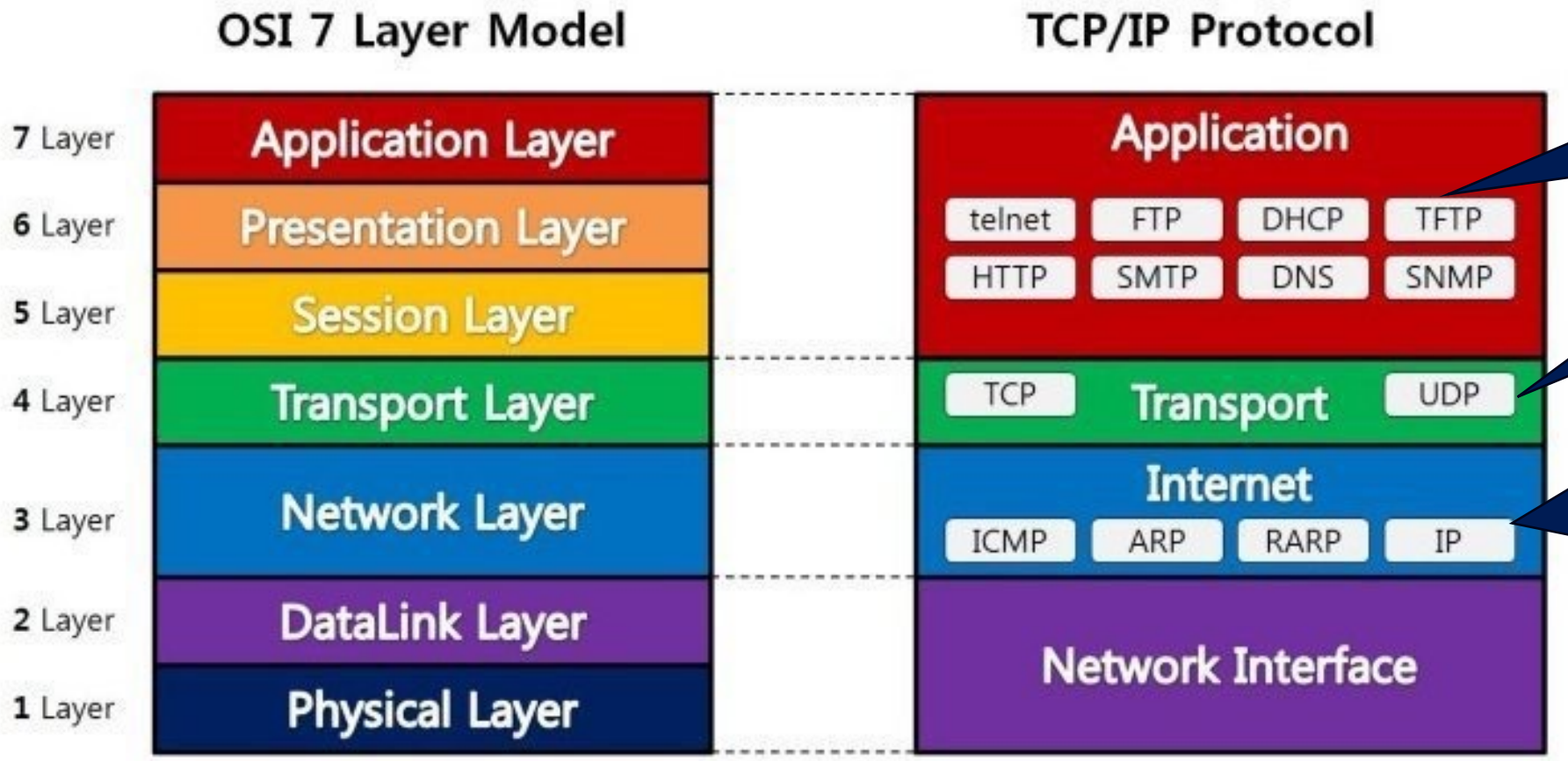
Transmission Control Protocol (TCP)

- Key features
  - Connection oriented: How?
  - Reliable: How?
  - Ordered: How?
  - Traffic (congestion) control: How?

Transmission Control Protocol (TCP)

- Key features
  - Connection oriented: How? → **Three-way handshake**
  - Reliable: How? → **Retransmission with ACK**
  - Ordered: How? → **Sequence number with SEQ**
  - Traffic (congestion) control: How? → **Congestion control with window size**

Introduction to Network Security



Application-level attacks

TCP attacks

- Routing attacks
- ICMP attacks
- IP attacks

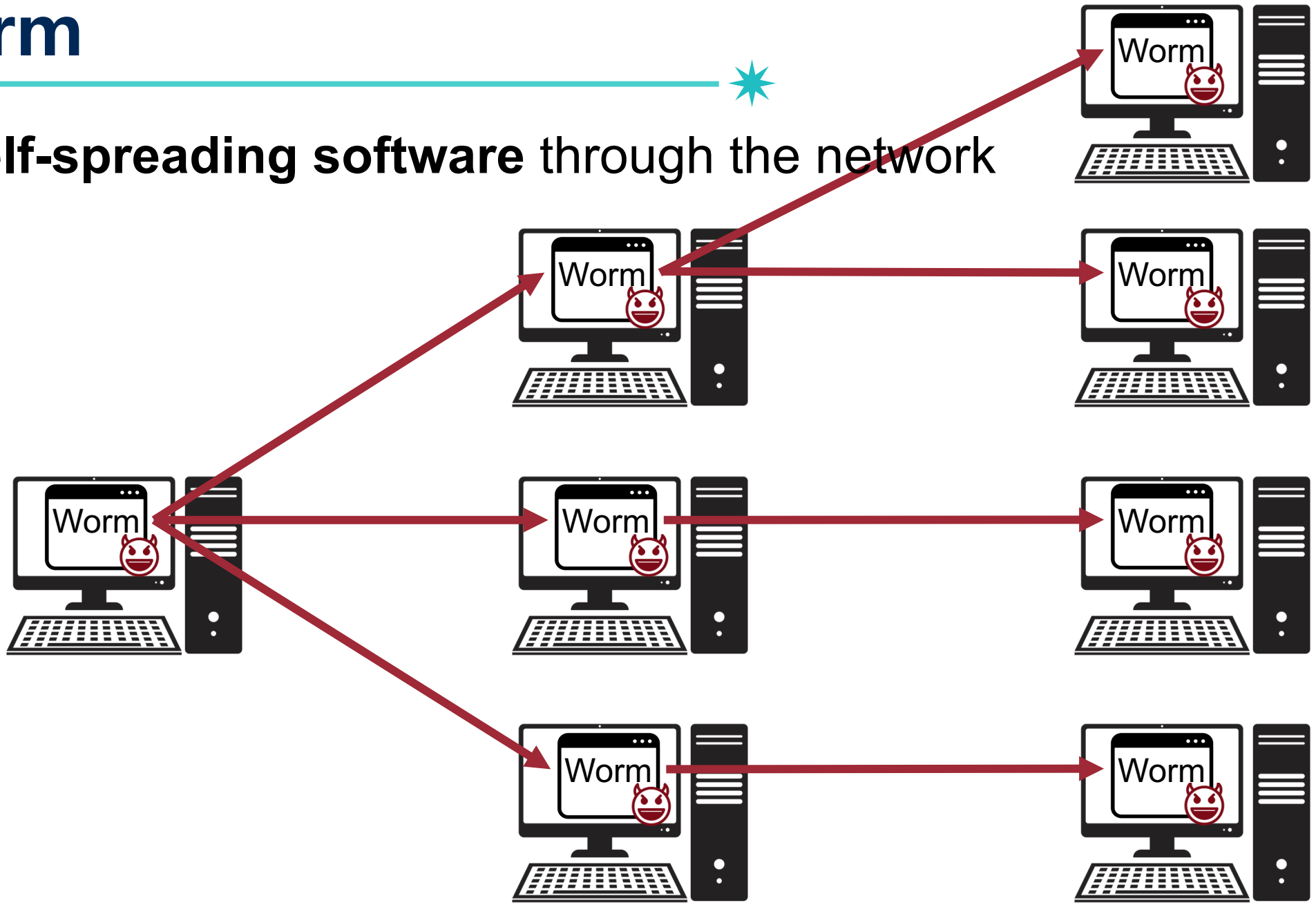
Introduction to Network Security

- Attacks 
  - Old days (First network attack, 1980s)
    - Worm
  - Advanced
    - Network attacks via web: Drive-by-download
    - Network attacks via Bot: Control victim
    - Network attacks via Denial-of-Service (DoS): flood a victim
    - Others: spoofing, flooding, …
- Defenses 
  - Firewalls
  - Intrusion Detection System (IDS)
  - Intrusion Prevention System (IDS)
  - Secure Protocols (IPSec, SSL/TLS)

Worm 

Worm

- A **self-spreading software** through the network

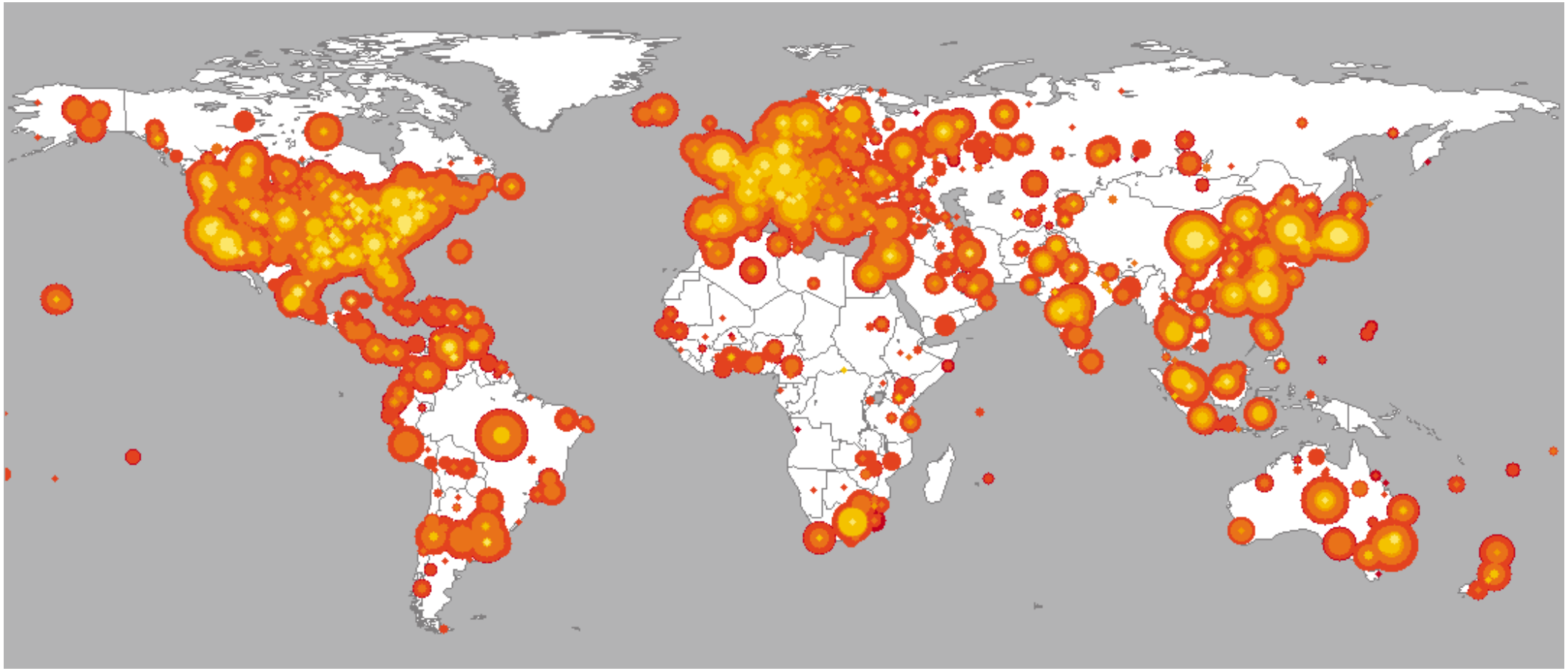


Worm – History

- Morris worm, 1988
  - Infected approximately 6,000 machines (10% of the whole computers)
  - Cost ~ $10 million in downtime and cleanup
- CodeRed worm, 2001
  - Direct descendant of Morris' worm
  - Infected more than 500,000 servers
  - Caused ~ $2.6 Billion in damages
- …

CodeRed Case

- On July 19, 2001 more than 359,000 computers were infected with the CodeRed worm in less than 14 hours



CodeRed Case

- How it works?
  - Attacking IIS web servers
    - Buffer overflow
  - Send the following packet any open 80

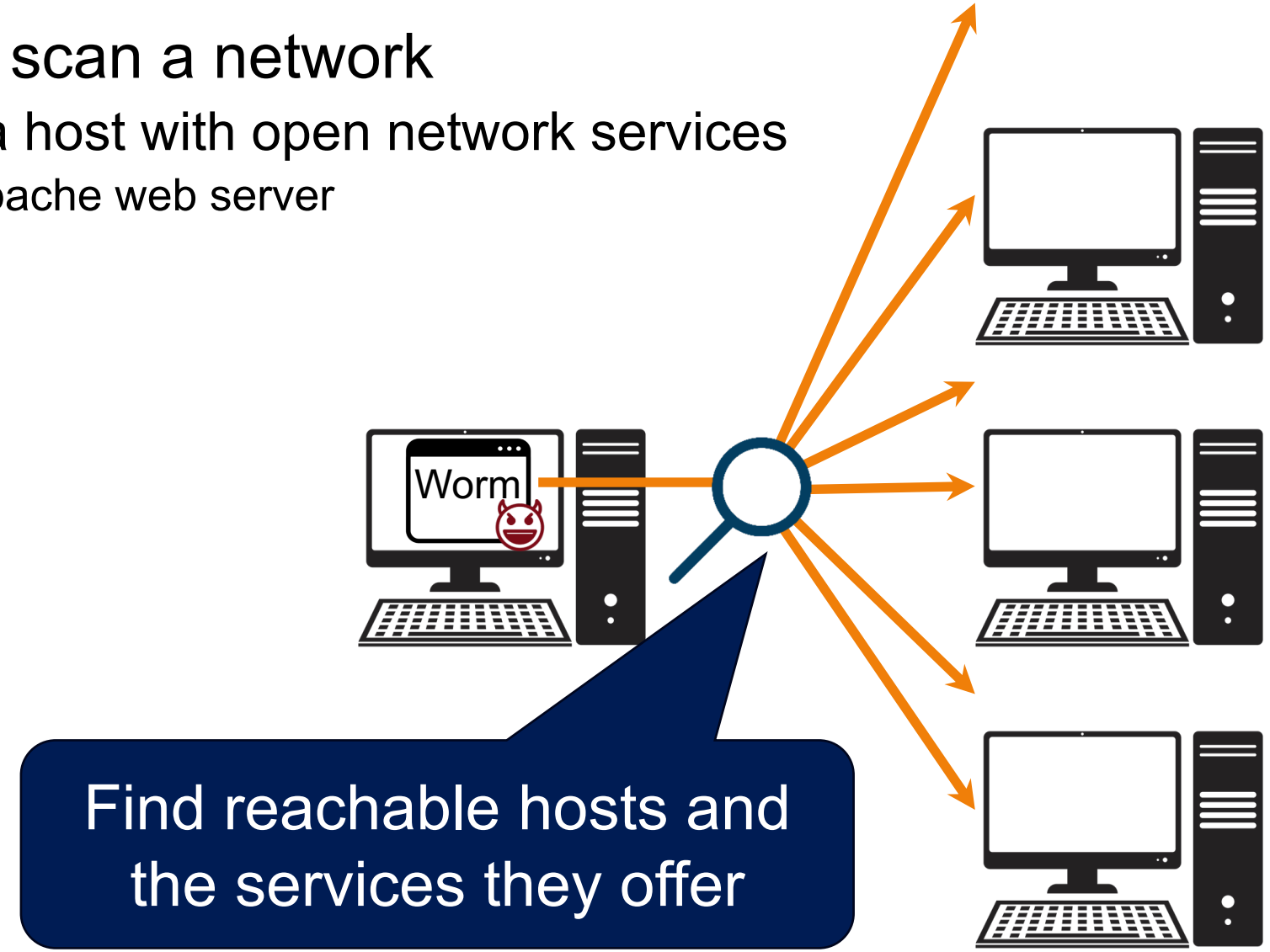
```
GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801
%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8
b00%u531b%u53ff%u0078%u0000%u00=a  HTTP/1.0
```

Worm – Process

1. **Scan**: find a victim
2. **Infect**: deliver a malicious payload

1. Scan: Find a Victim

- How to find a victim?: scan a network
  - Send packets to find a host with open network services
    - E.g., a host serving Apache web server



1. Scan: Find a Victim

- Use a protocol
  - TCP: SYN scan
    - Check if a recipient returns a SYN/ACK packet
  - UDP: Send a UDP packet to a random port
    - If a port is open: no response
    - If a port is closed: ICMP port unreachable
  - ICMP: ping scan
    - Check if a host is reachable

Nmap

- Popular network scanning tool
- Used to discover hosts and services on a computer network by sending packets and analyzing the responses

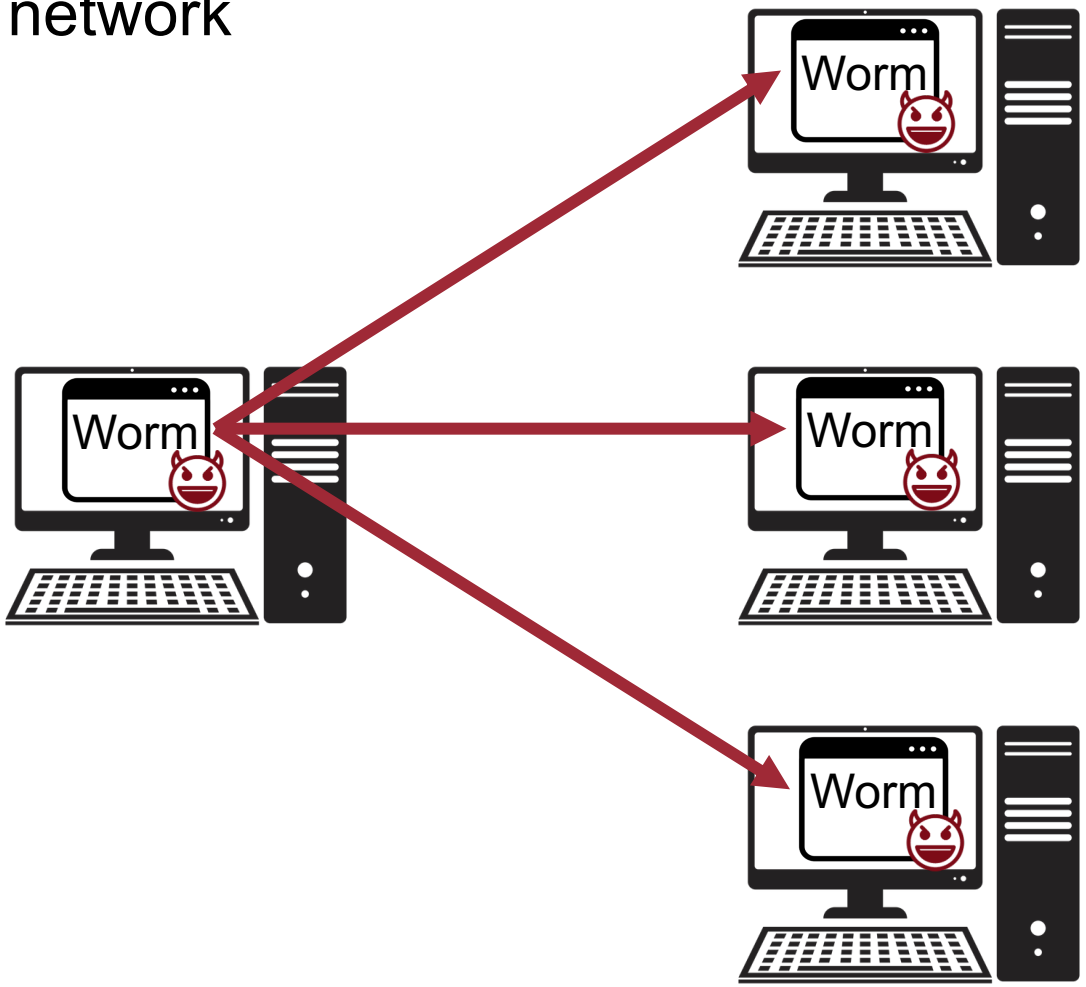
Nmap Example


```
┌──[✗]─[ucihamadara@parrot]─[~]
└──╼ $sudo nmap 192.168.1.22
[sudo] password for ucihamadara:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-17 14:56 EDT
Nmap scan report for basicpentest (192.168.1.22)
Host is up (0.0068s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
MAC Address: 08:00:27:66:44:4C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.53 seconds
```

2. Infect: Deliver a Malicious Payload

- How to deliver ?
  - Data payload (with binary) through a network
- How to infect a host?
  - Usually buffer overflow
  - Heap-based attacks



Denial of Service (DoS) 

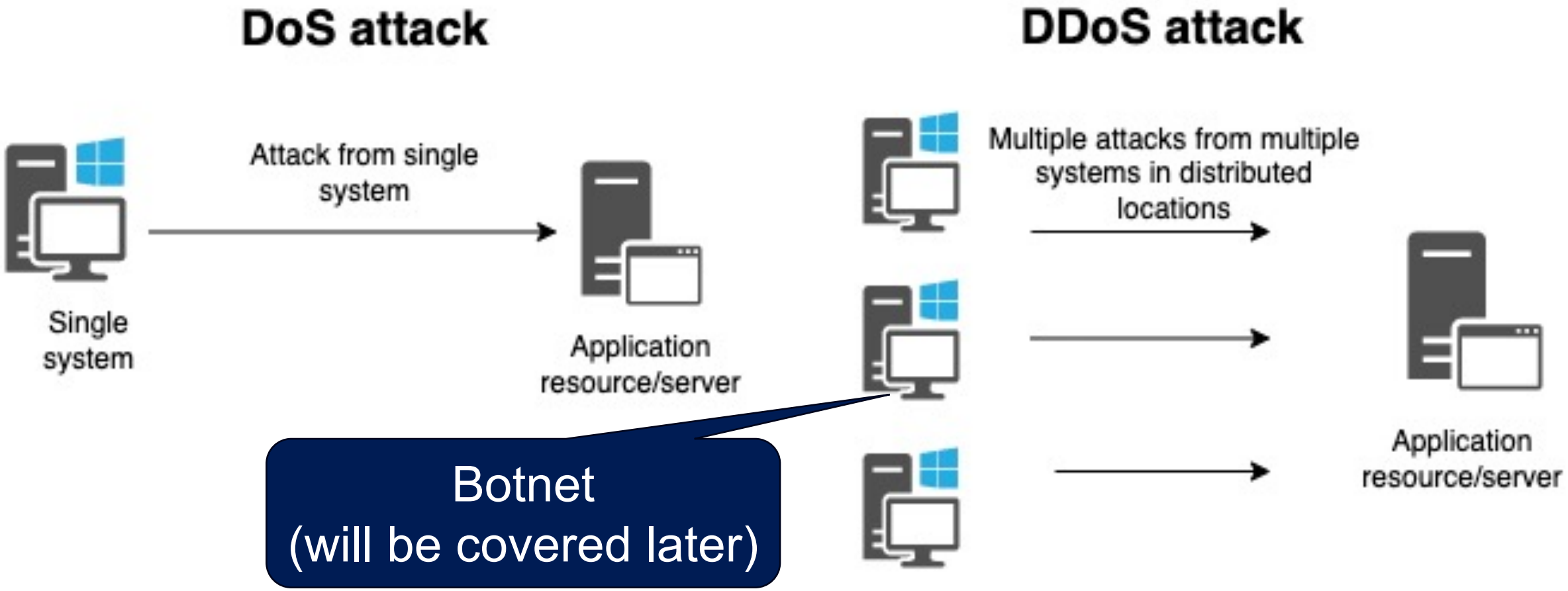
Denial of Service (DoS)

- Disrupting **the use** of networks, systems, or applications (availability)

- How to do?
  - By sending large number of network flows exhausting service provider's resources

Distributed Denial-of-Service (DDoS)

- Employ **multiple (compromised) computers** to perform a coordinated and widely distributed DoS attack



(D)DoS Attack Surface

- Any part of your network or services that is vulnerable to an attack
  - Network interfaces
  - Infrastructure
  - Firewall/IPS
  - Servers
  - Protocols
  - Applications
  - Databases

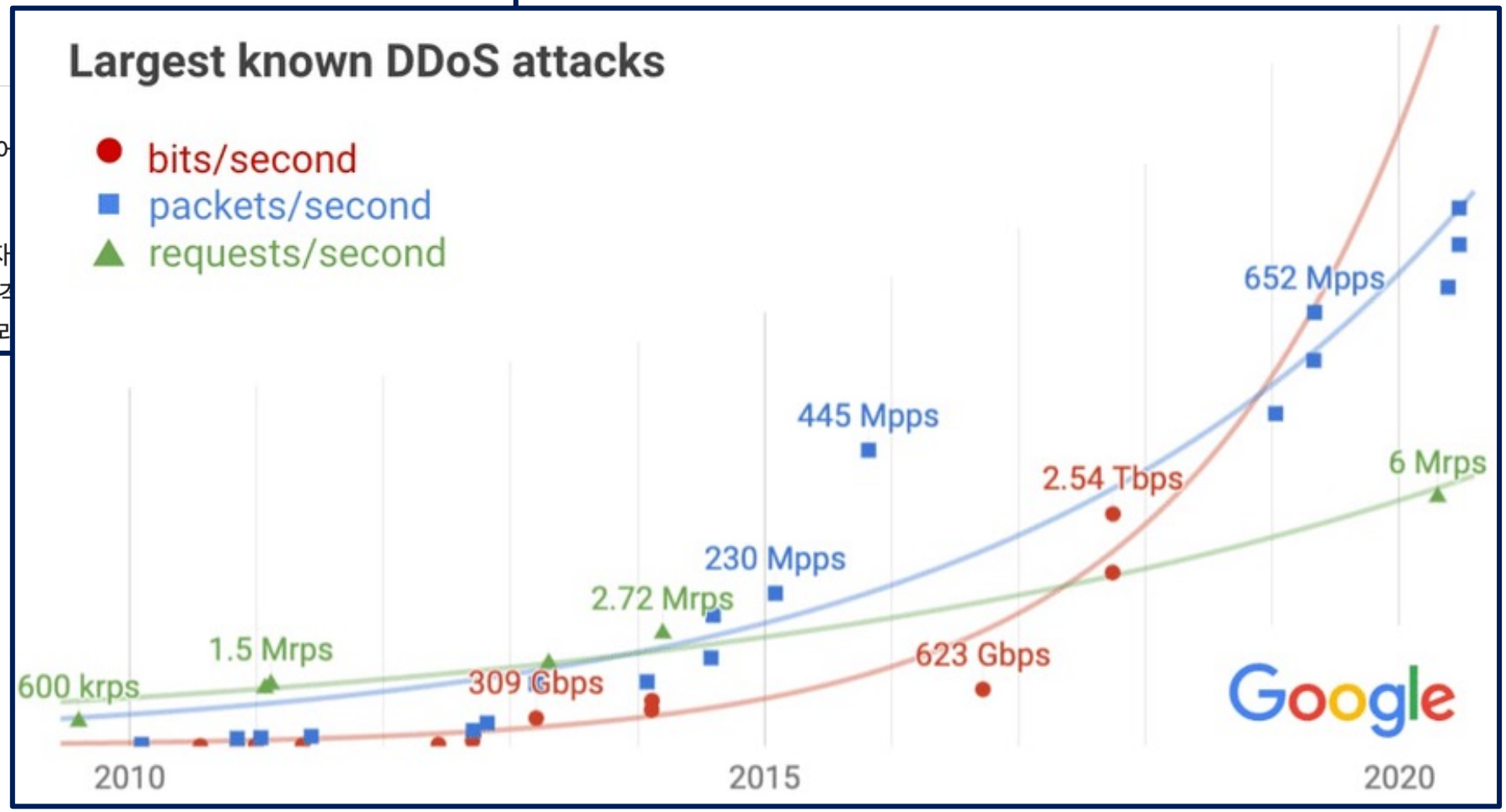
DDoS Trend

구글·아마존, 전례 없는 강도의 디도스 공격 당해

기사입력 : 2023년10월12일 11:15 | 최종수정 : 2023년10월12일 11:16

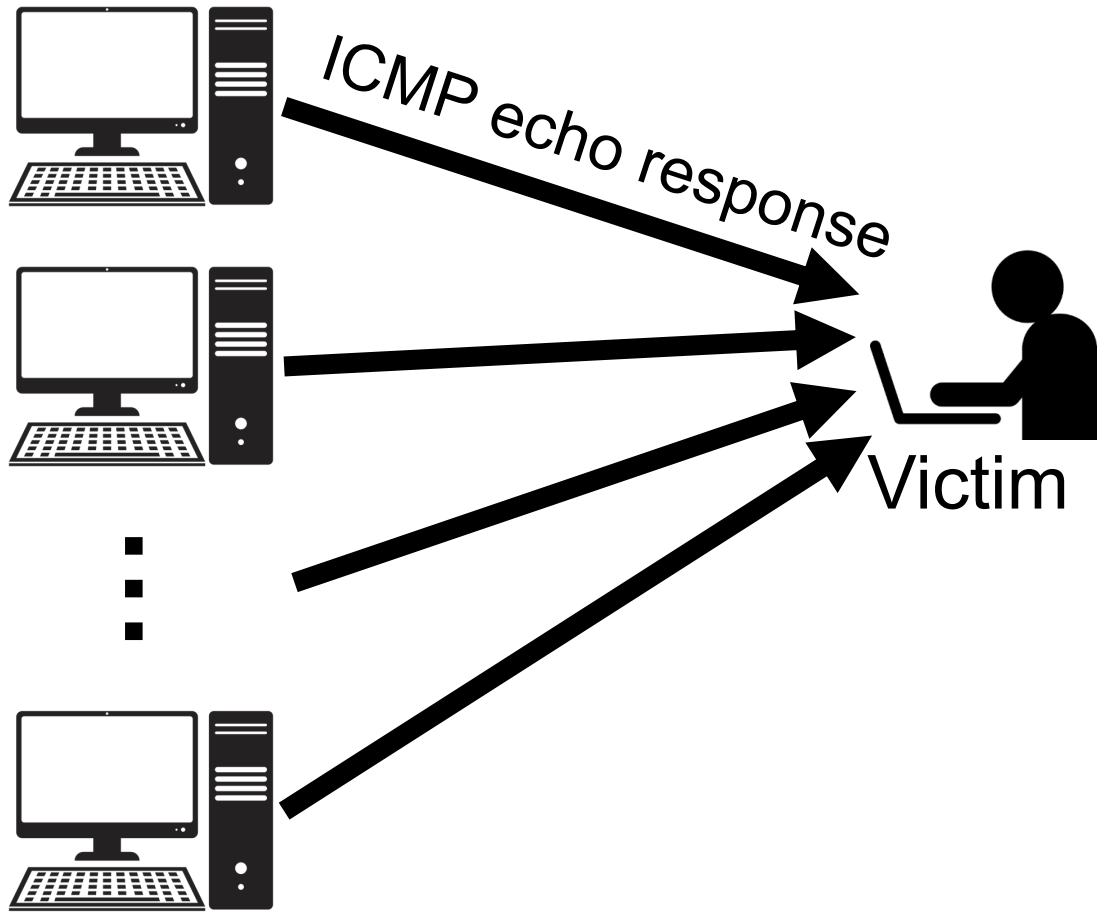
[서울=뉴스핌]박공식 기자 = 구글, 아마존, 클라우드플레어
을 당한 것으로 알려졌다.

알파벳 소유의 구글은 10일(현지시간) 블로그 포스트에 자
었던 사상 최대의 공격보다 7배 이상 많은 악성 트래픽 공격
키피디아의 9월 한 달 자료 요청 건수를 능가하는 악성 트래



Ping Flood Attack

- The computing device is flooded with tons of Internet Control Message Protocol (ICMP) ping response



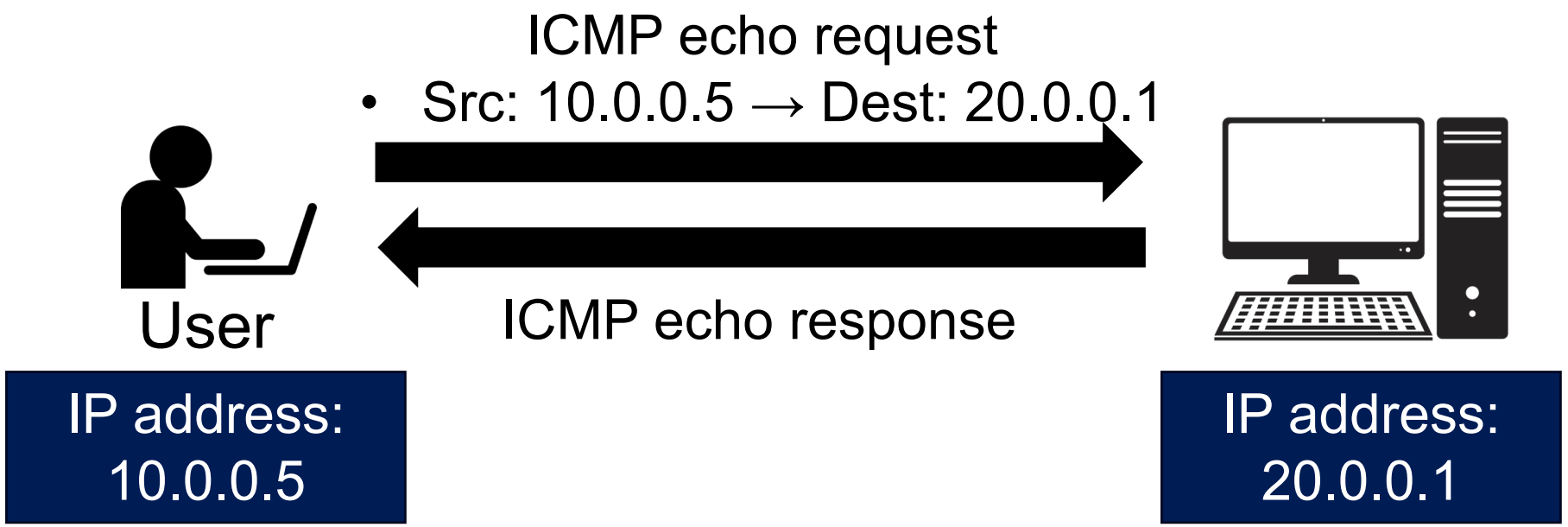
Recap: ICMP

- Internet Control Message Protocol (ICMP)
  - Used by a router/end-host to report some types of error
    - E.g., `Destination Unreachable`: packet can't be forwarded to its destination
    - E.g., `Time Exceeded`: Time To Live (TTL) reached zero, or fragment didn't arrive in time
- Encapsulated in the IP packet

```
$ ping google.com
PING google.com (142.250.206.238): 56 data bytes
64 bytes from 142.250.206.238: icmp_seq=0 ttl=115 time=31.598 ms
64 bytes from 142.250.206.238: icmp_seq=1 ttl=115 time=35.777 ms
64 bytes from 142.250.206.238: icmp_seq=2 ttl=115 time=40.632 ms
64 bytes from 142.250.206.238: icmp_seq=3 ttl=115 time=35.873 ms
...
```

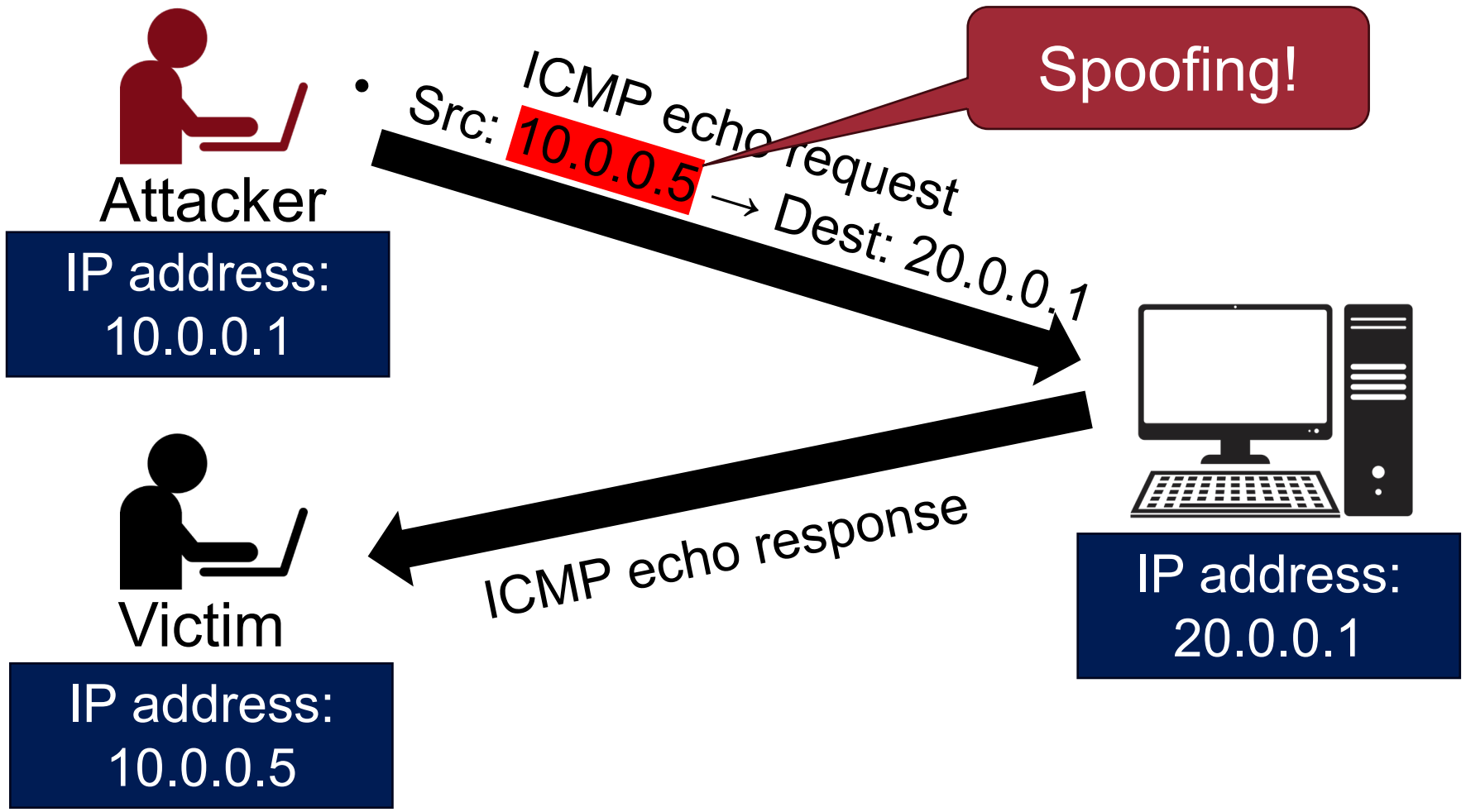
Recap: ICMP

- Internet Control Message Protocol (ICMP)
  - Used by a router/end-host to report some types of error
    - E.g., `Destination Unreachable`: packet can't be forwarded to its destination
    - E.g., `Time Exceeded`: Time To Live (TTL) reached zero, or fragment didn't arrive in time



Ping Flood Attack – Method: Spoofing

- Use of forged source IP address

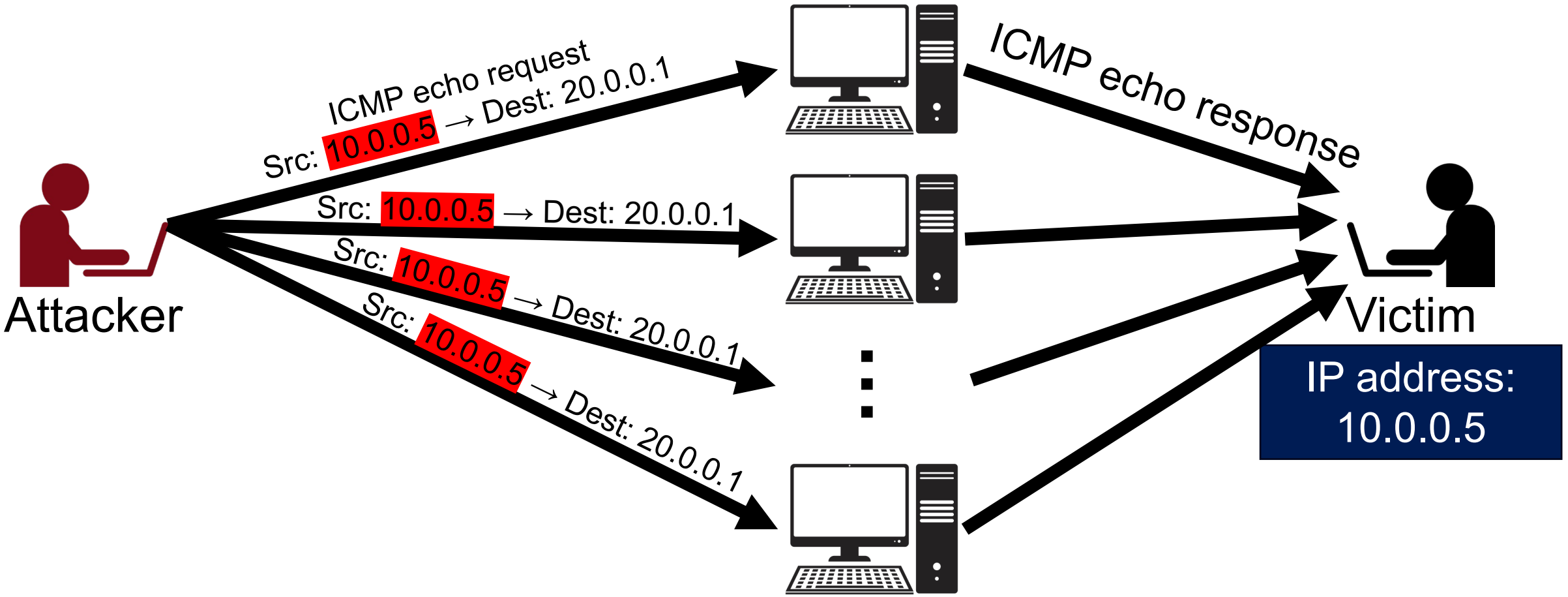


Method: Spoofing

- How to
  - Network RAW socket programming
  - Nmap
    - My own IP address is 10.0.0.1
    - `$ nmap -e eth0 -S 10.0.0.5 20.0.0.1`
    - Use the network interface eth0 to send a spoofed packet (10.0.0.5) to 20.0.0.1
  - …

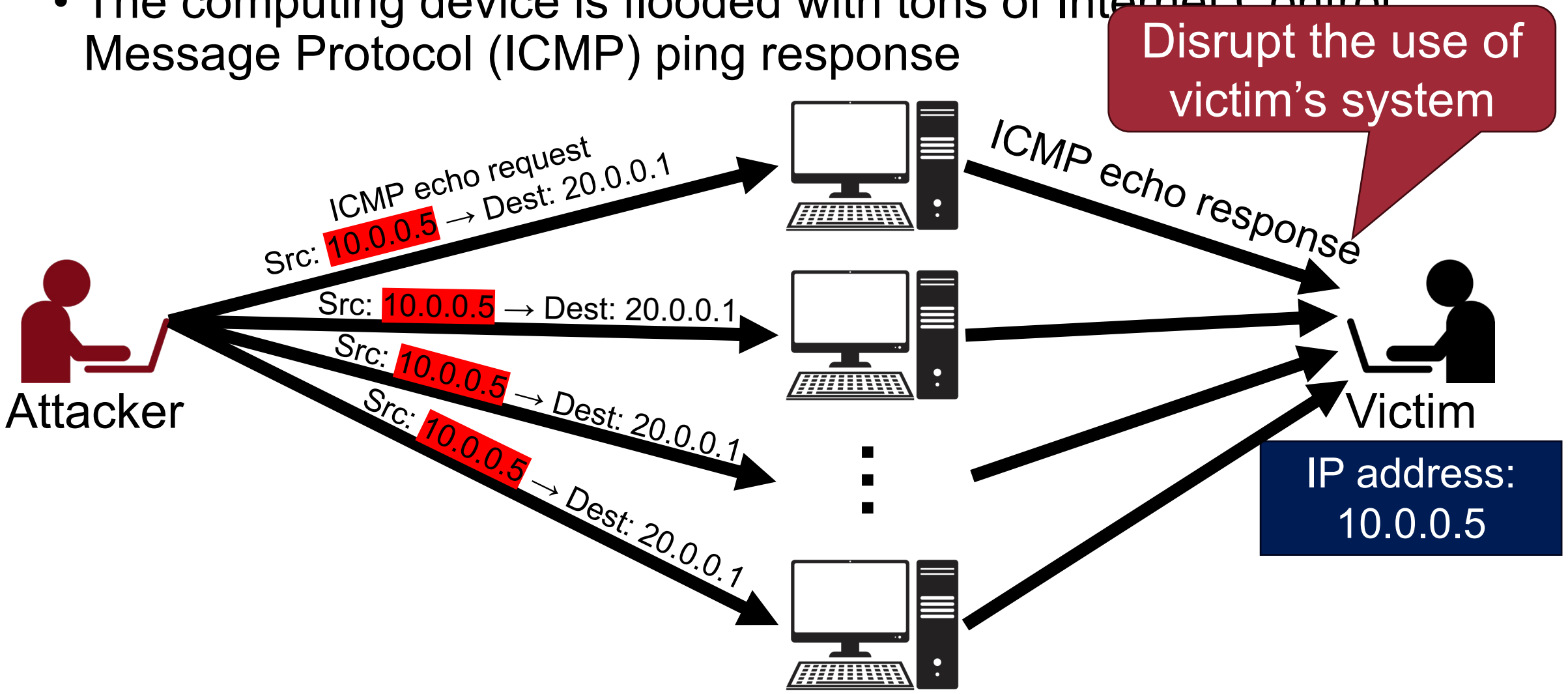
Ping Flood Attack

- The computing device is flooded with tons of Internet Control Message Protocol (ICMP) ping response



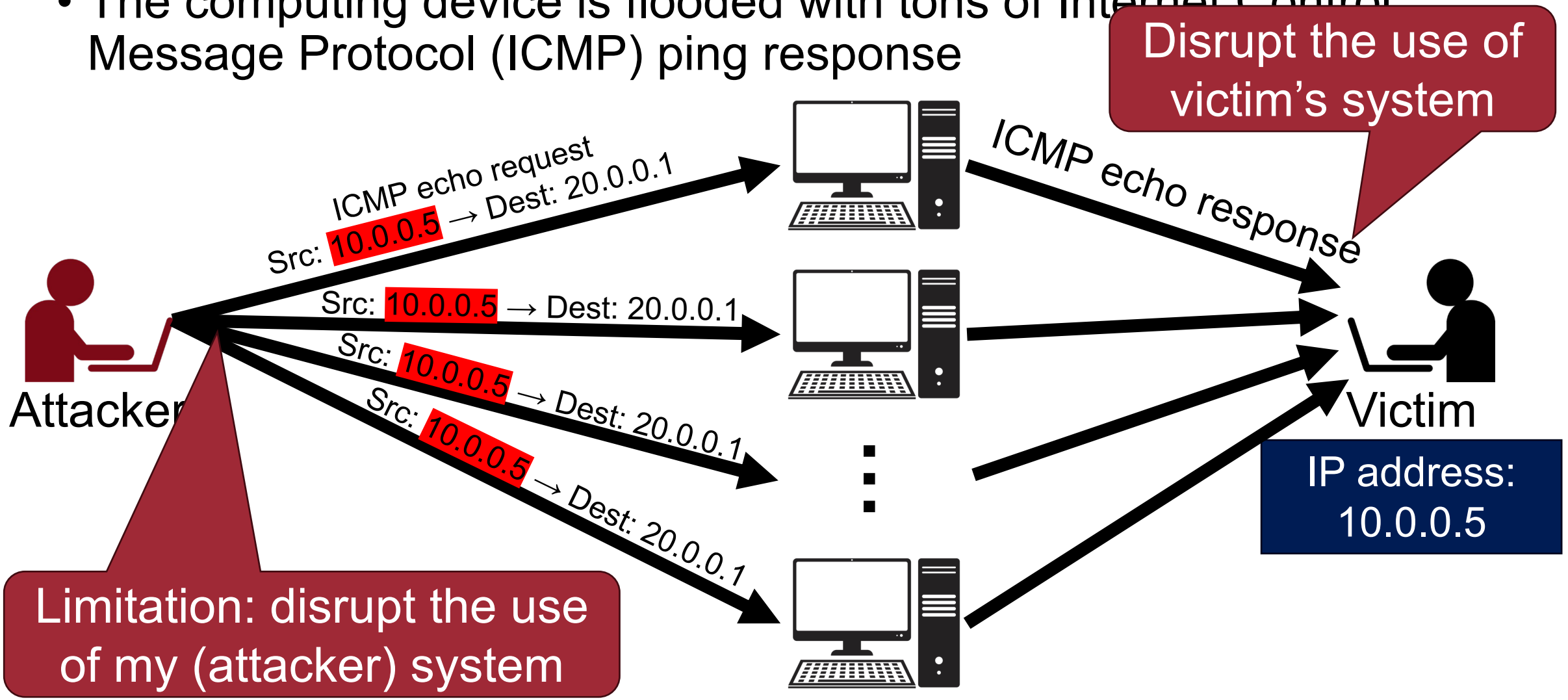
Ping Flood Attack

- The computing device is flooded with tons of Internet Control Message Protocol (ICMP) ping response



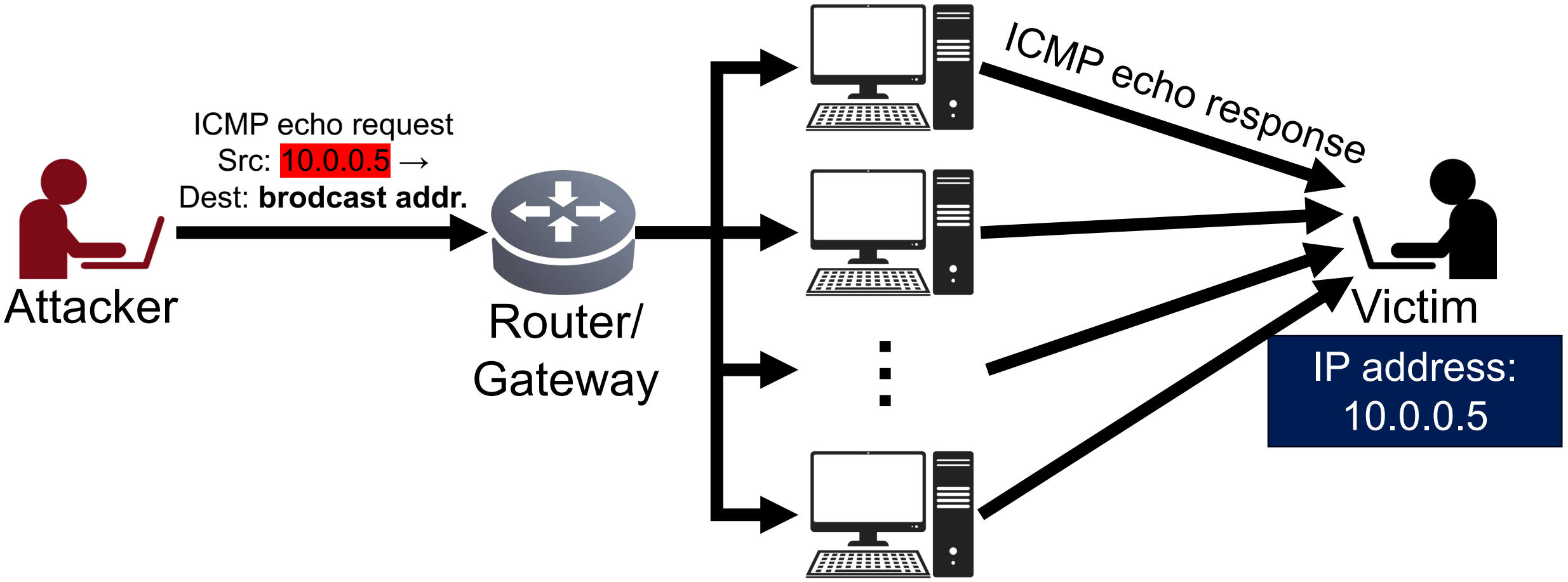
Problem?

- The computing device is flooded with tons of Internet Control Message Protocol (ICMP) ping response



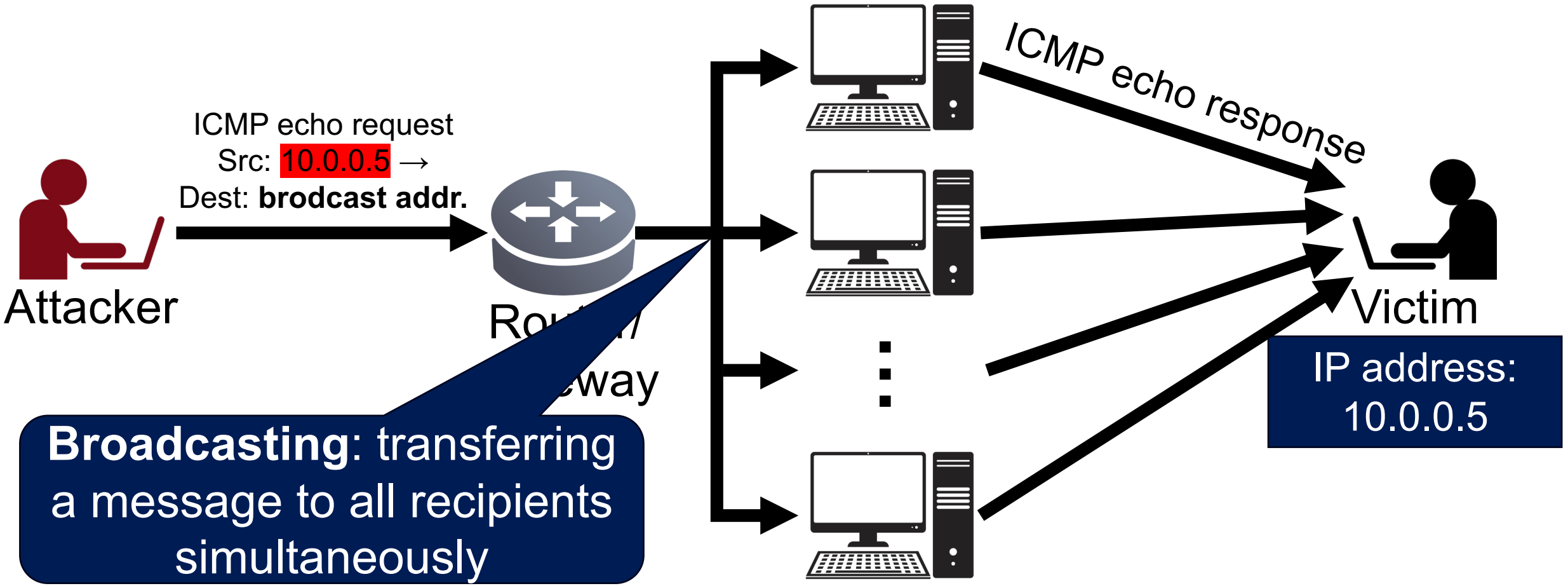
Smurf Attack

- Idea: sending ping request to **broadcast address**



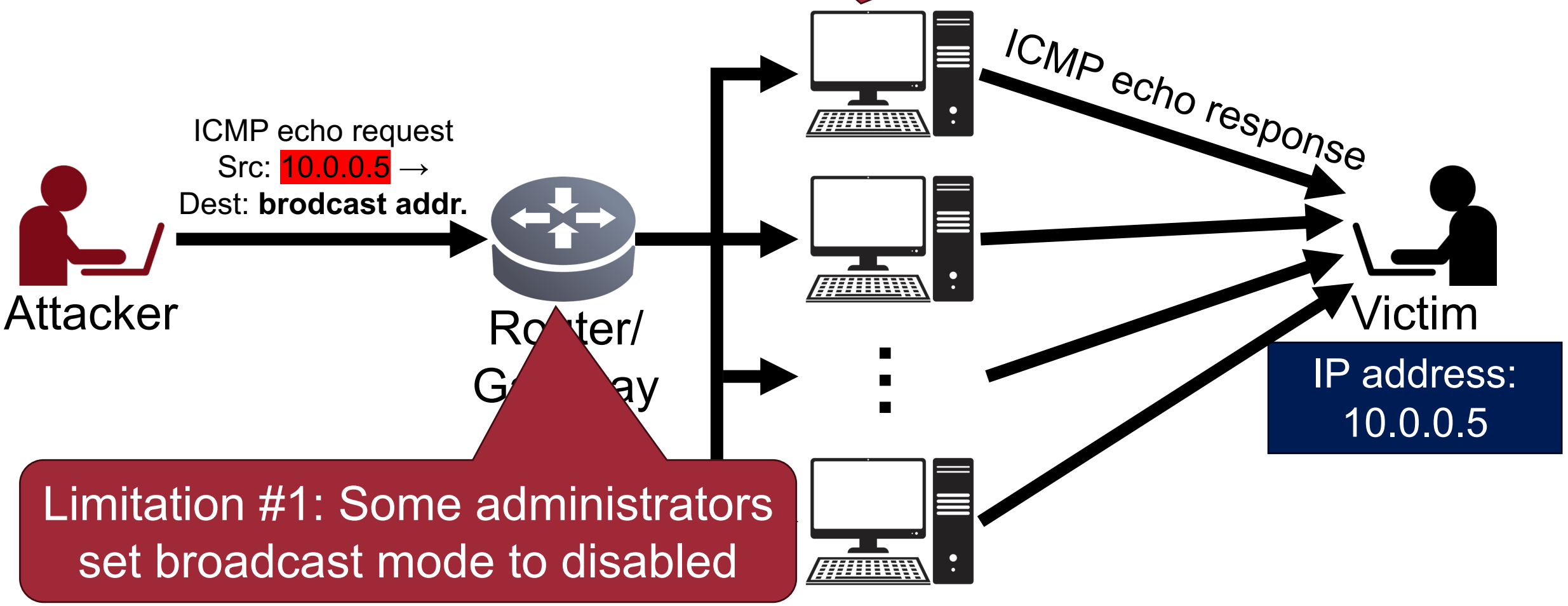
Smurf Attack

- Idea: sending ping request to **broadcast address**



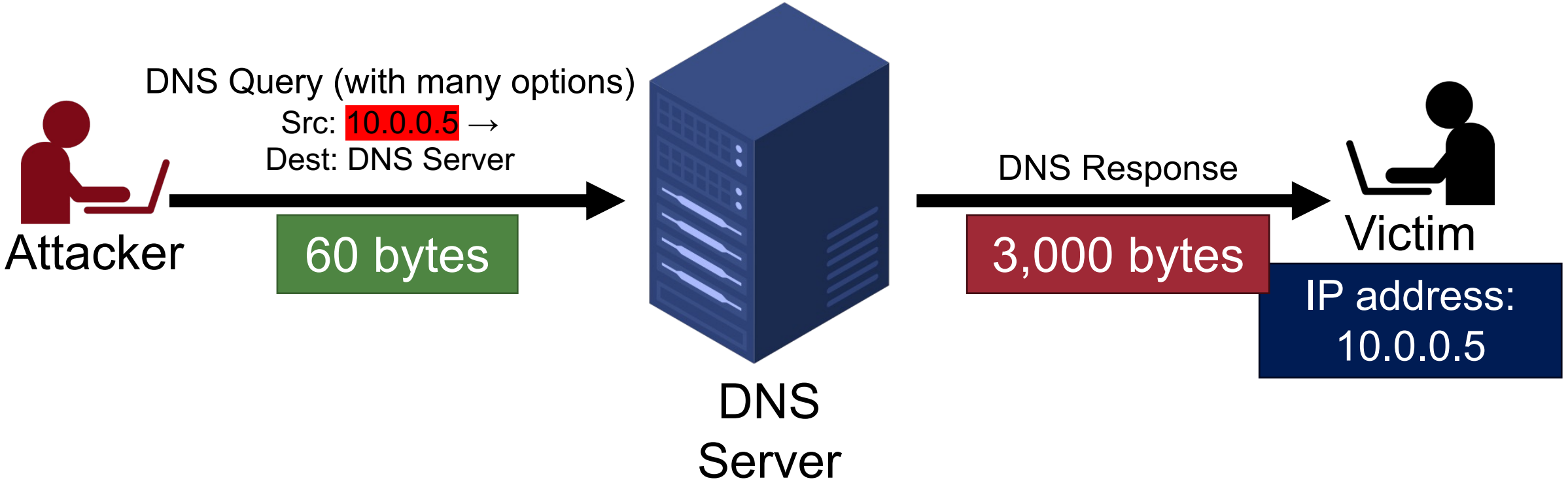
Problem?

- Idea: sending ping reques



Amplification Attack

- Idea: controlling the **size of responses**, not the number of responses
- Example: DNS Amplification Attack



Amplification Attack

- Idea: controlling the **size of responses**, not the number of responses
- We can leverage many protocols (which give long responses compared to short requests)
  - DNS: Domain Name Server
  - NTP: Network Time Protocol
  - SSDP: Simple Service Discovery Protocol
  - CHARGEN:
  - …

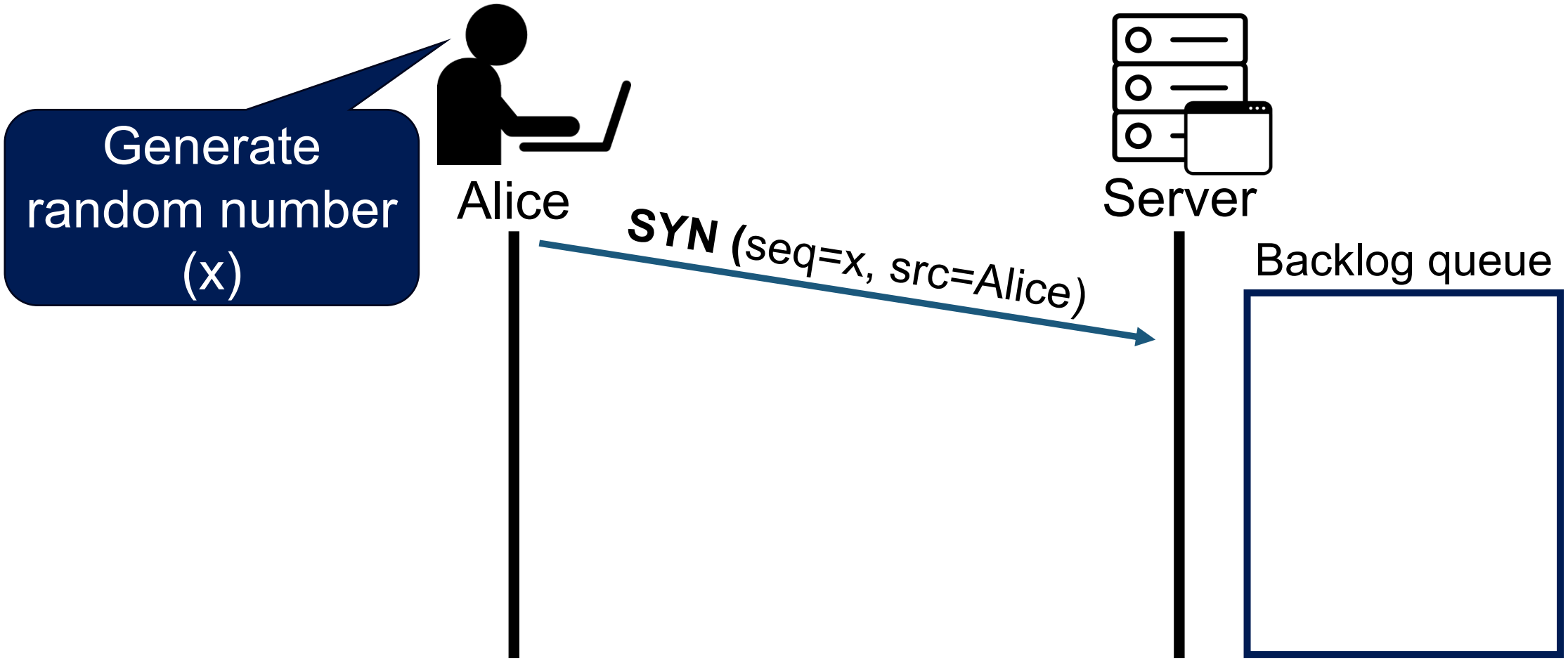
SYN Flooding Attack 

TCP SYN Flooding Attack

- Floods the server with **SYN Packets**

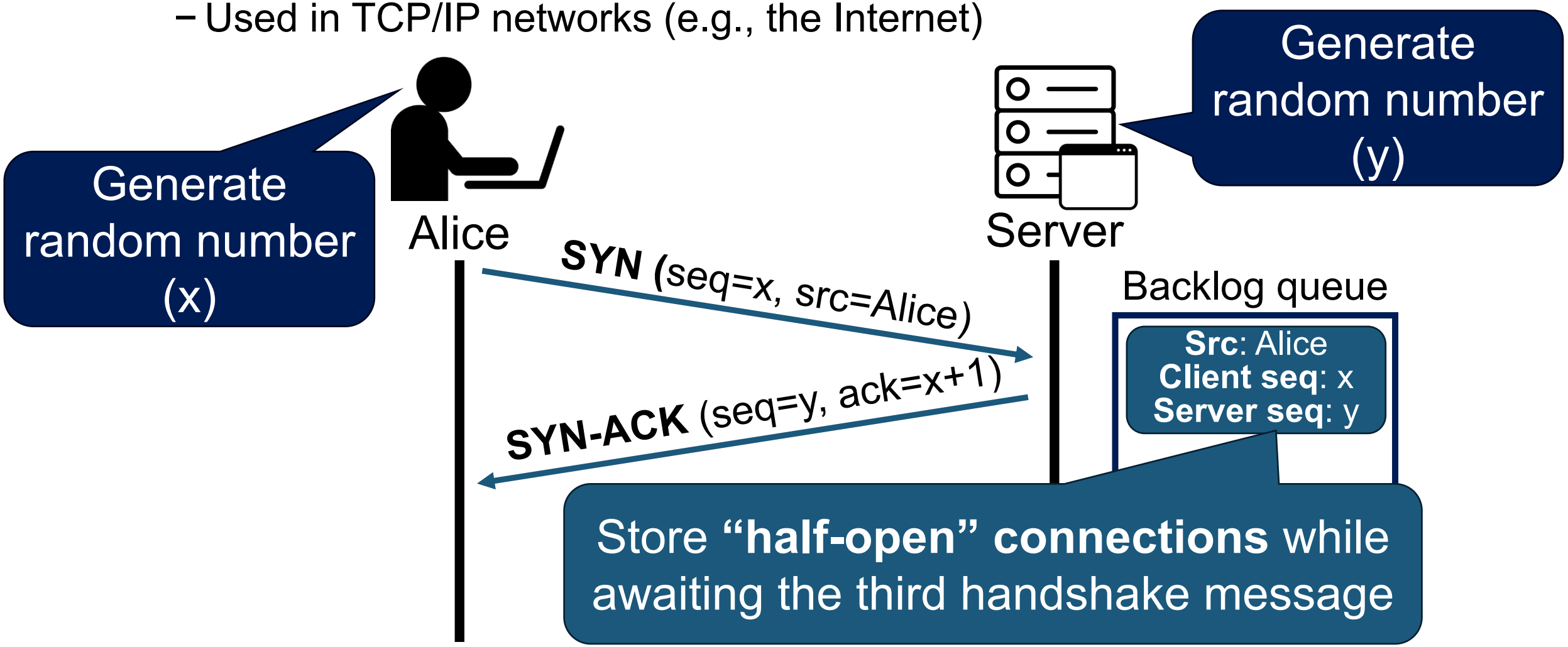
TCP Three-way Handshake

- Establish a connection between the server and the client
  - Used in TCP/IP networks (e.g., the Internet)



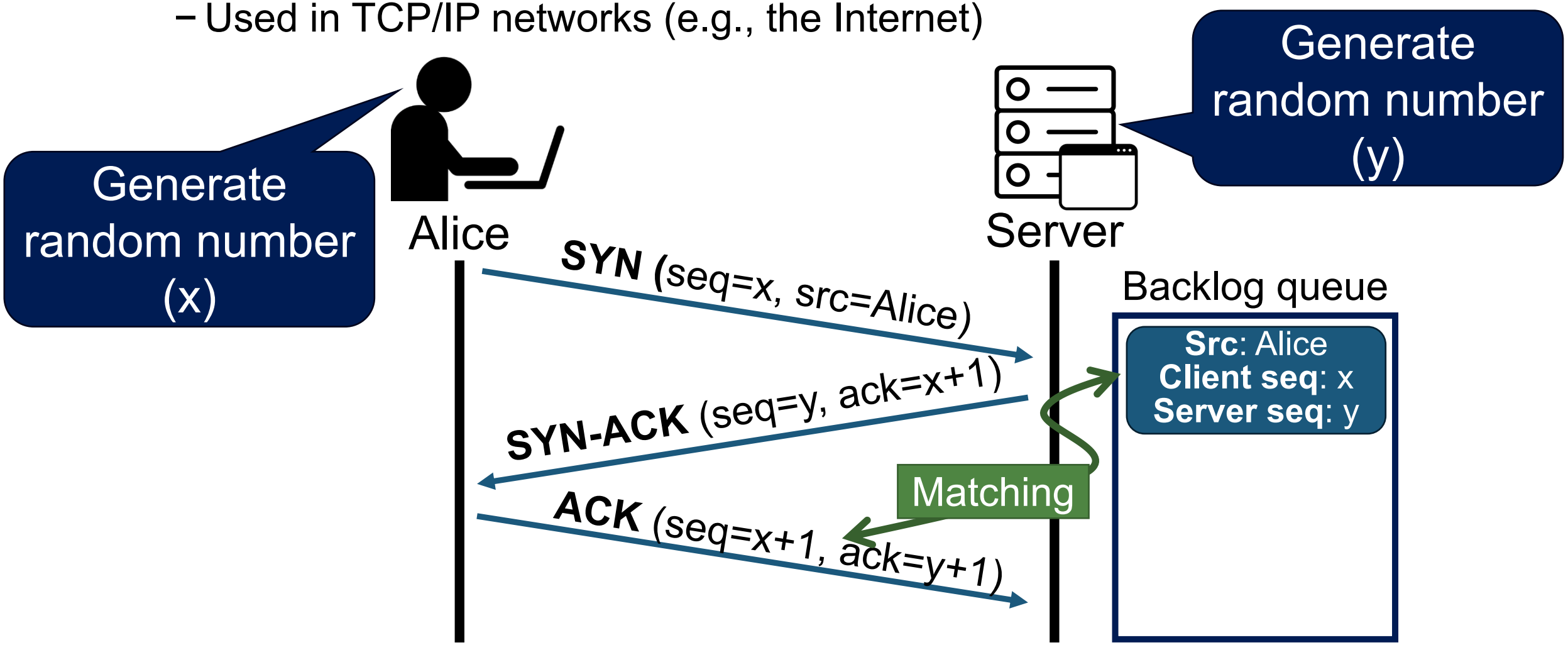
TCP Three-way Handshake

- Establish a connection between the server and the client
  - Used in TCP/IP networks (e.g., the Internet)



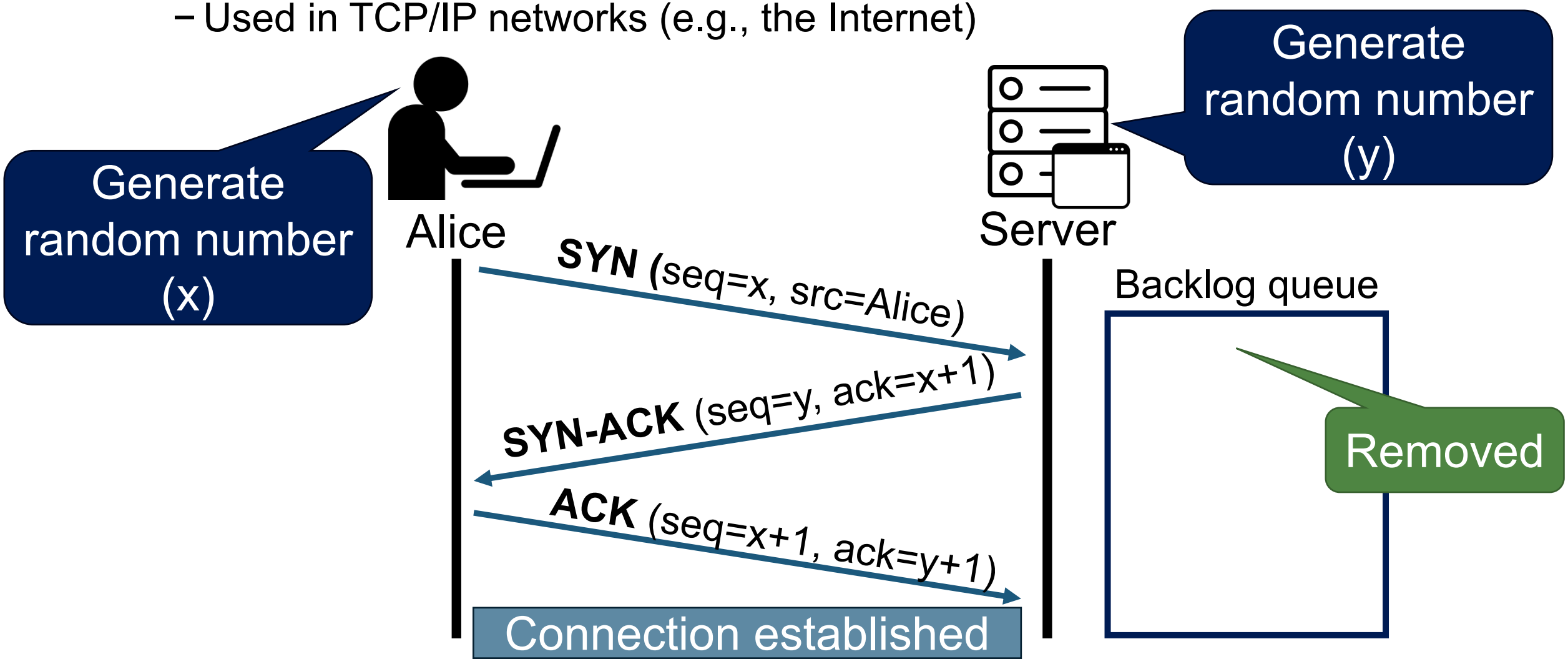
TCP Three-way Handshake

- Establish a connection between the server and the client
  - Used in TCP/IP networks (e.g., the Internet)



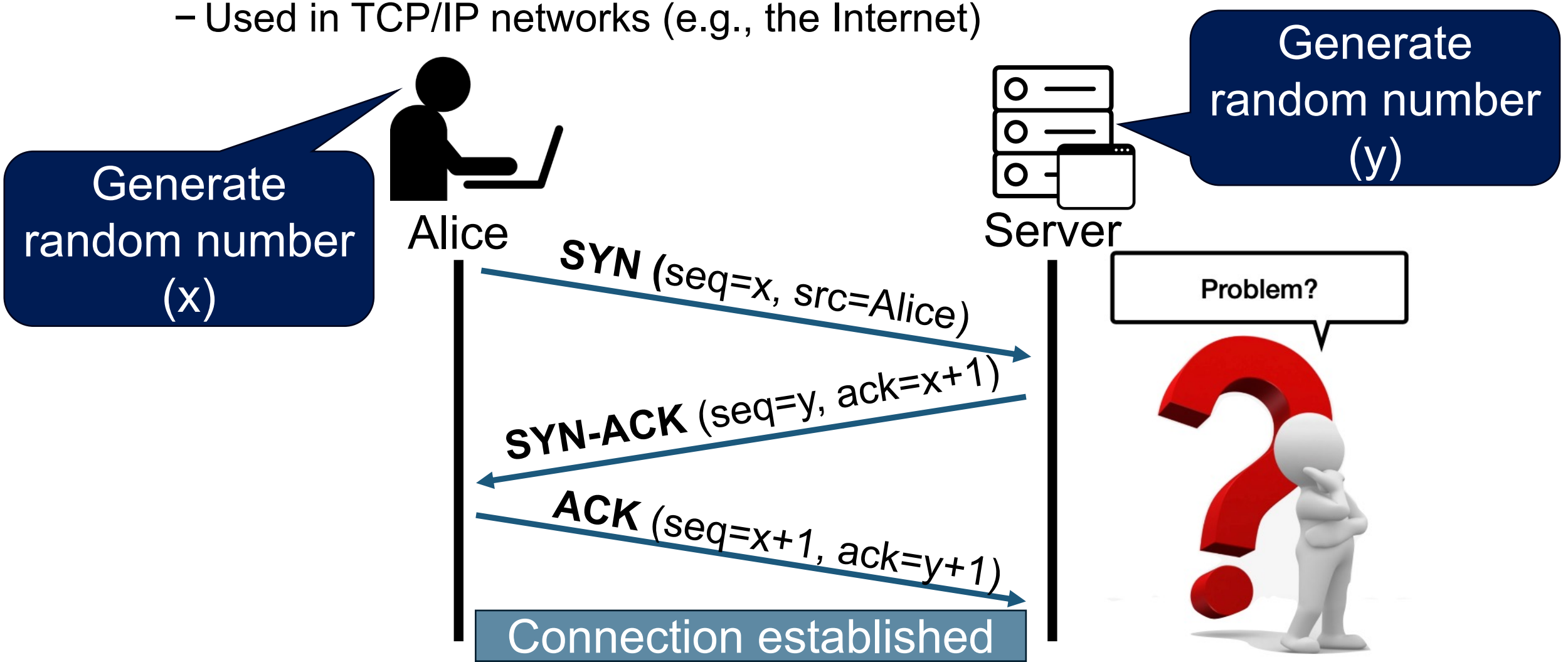
TCP Three-way Handshake

- Establish a connection between the server and the client
  - Used in TCP/IP networks (e.g., the Internet)



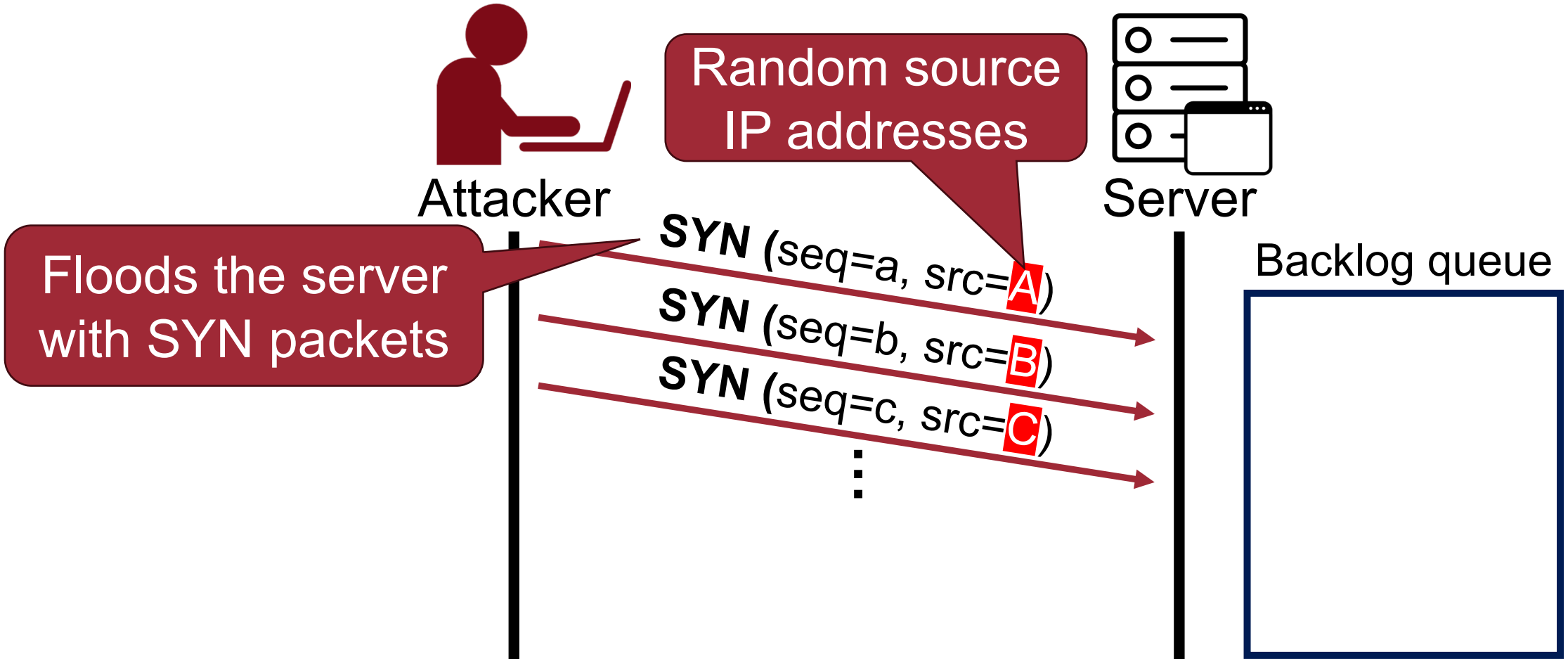
TCP Three-way Handshake

- Establish a connection between the server and the client
  - Used in TCP/IP networks (e.g., the Internet)



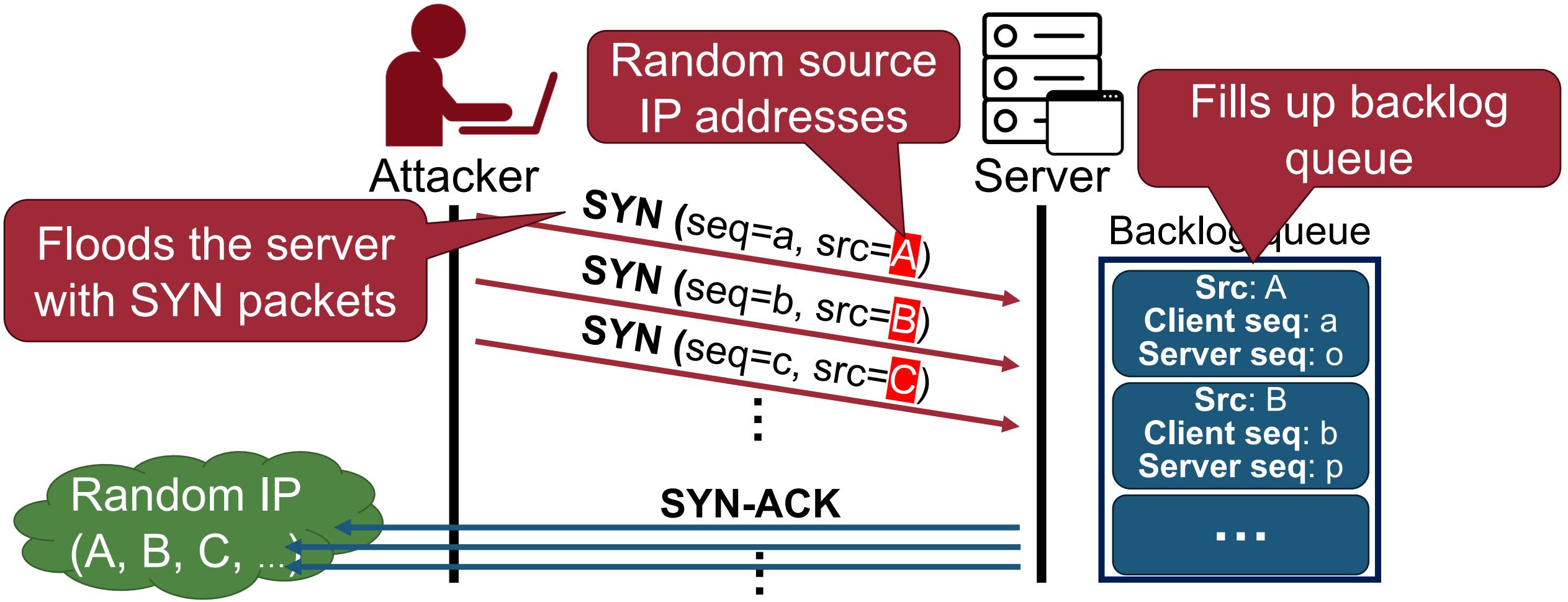
TCP SYN Flooding Attack

- Floods the server with SYN Packets



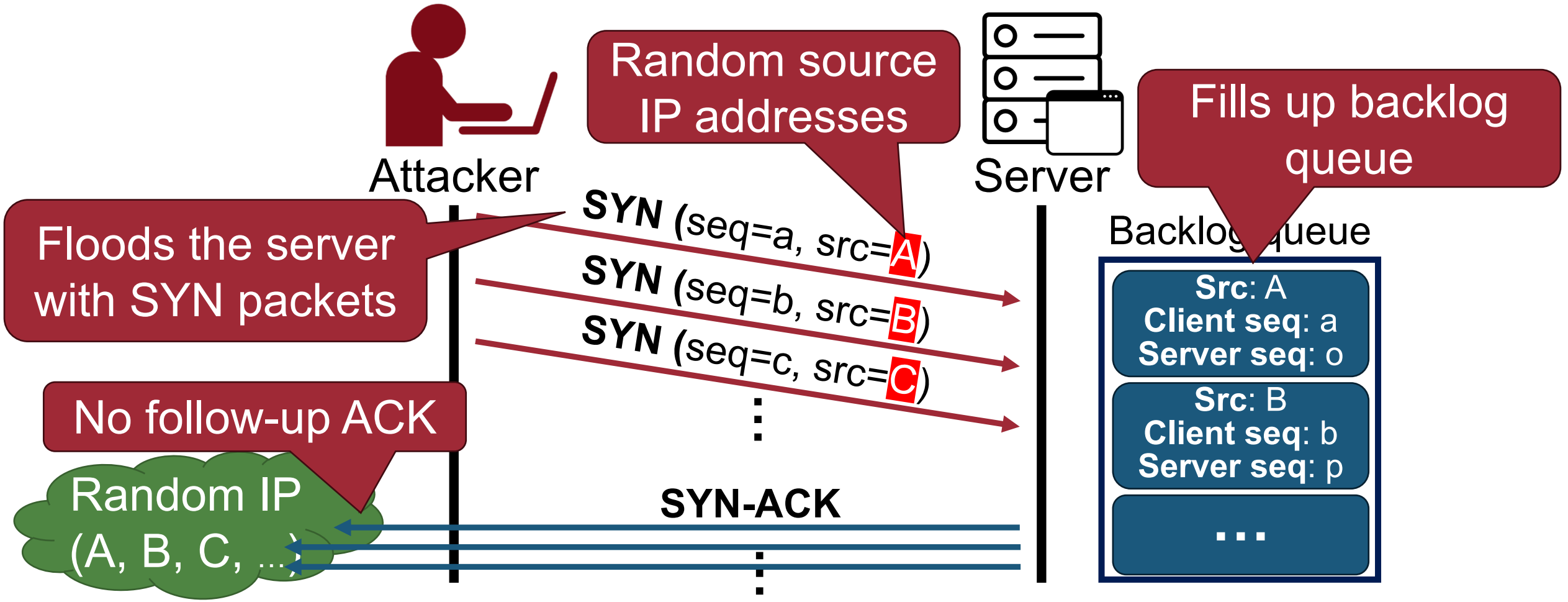
TCP SYN Flooding Attack

- Floods the server with SYN Packets



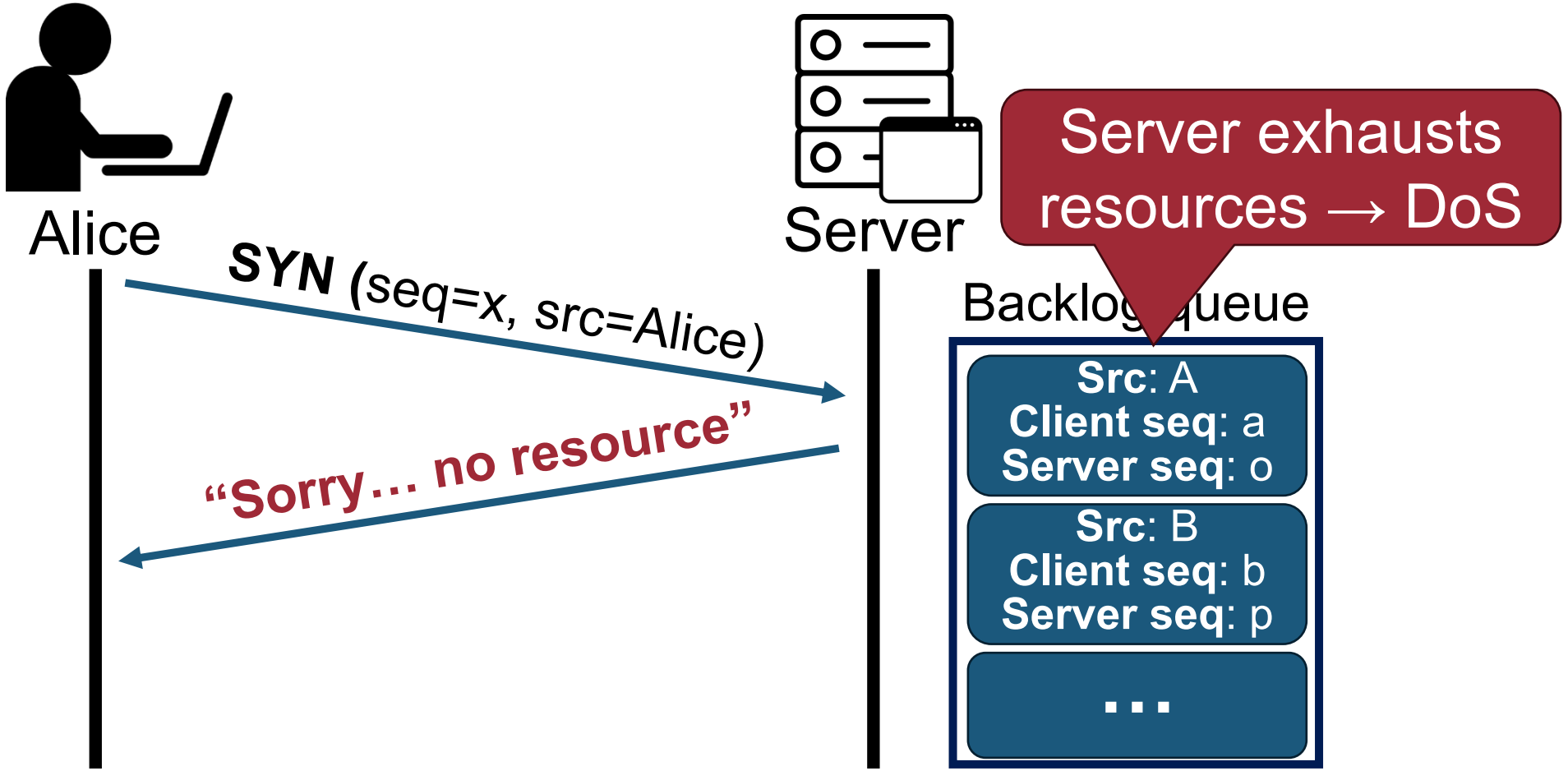
TCP SYN Flooding Attack

- Floods the server with SYN Packets



TCP SYN Flooding Attack

- Floods the server with SYN Packets
  - No further connections



Why is it Vulnerable?

- TCP backlog issue - Limited size

OS	Backlog queue size
Linux 1.2.x	10
FreeBSD 2.1.5	128
WinNT 4.0	6

  - Backlog timeout: 3 minutes
  - Attacker need only send 128 SYN packets every 3 minutes

How to Mitigate SYN Flooding Attack?

- Set the Queue Size for TCP Backlog

```
$ sysctl -w net.ipv4.tcp_max_syn_backlog=1024
```

✓ Limitation: Arms race! Attackers can easily win

- Set the Firewalls
  - E.g., Blocks if similar packets exceed 10 per second

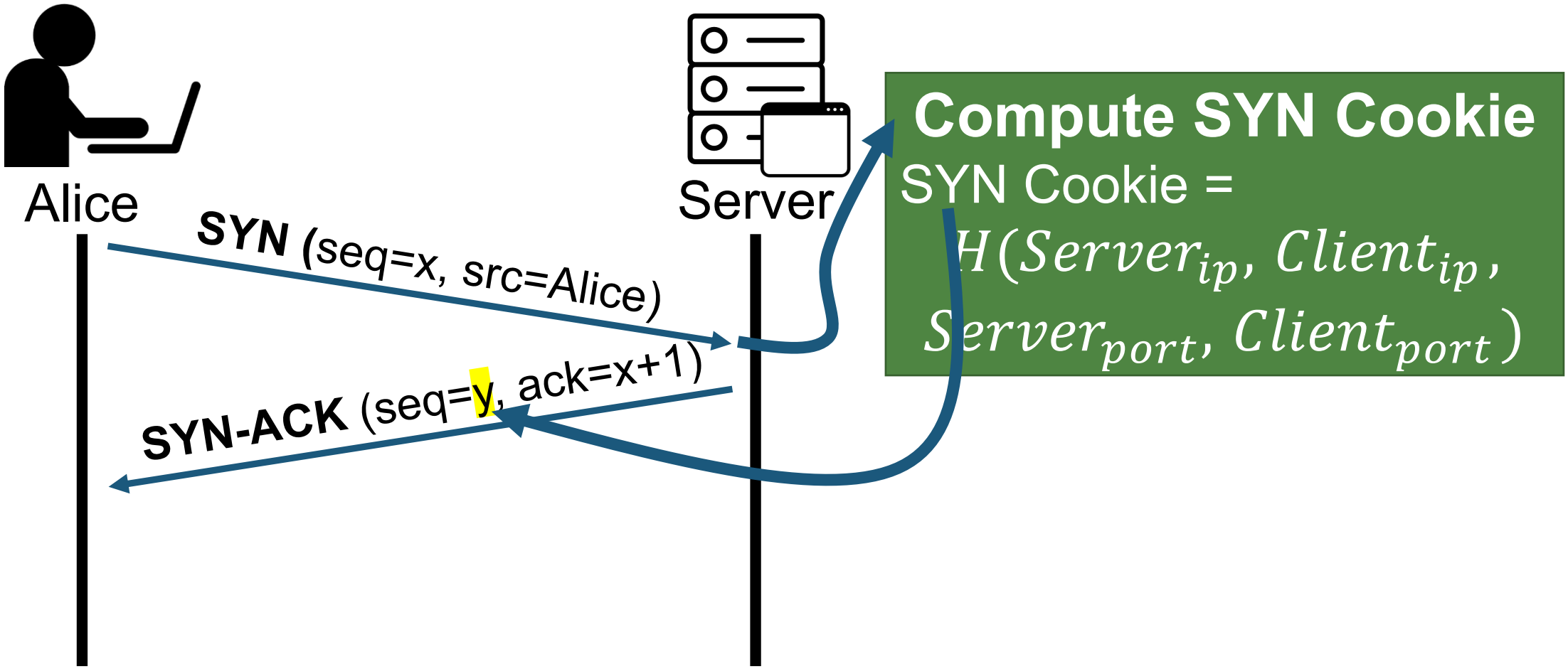
```
$ iptables -A INPUT -p TCP --dport 80 --syn -m limit 10/second -j ACCEPT
$ iptables -A INPUT -p TCP --dport 80 --syn -j DROP
```

✓Limitation: Performance

- SYN Cookie

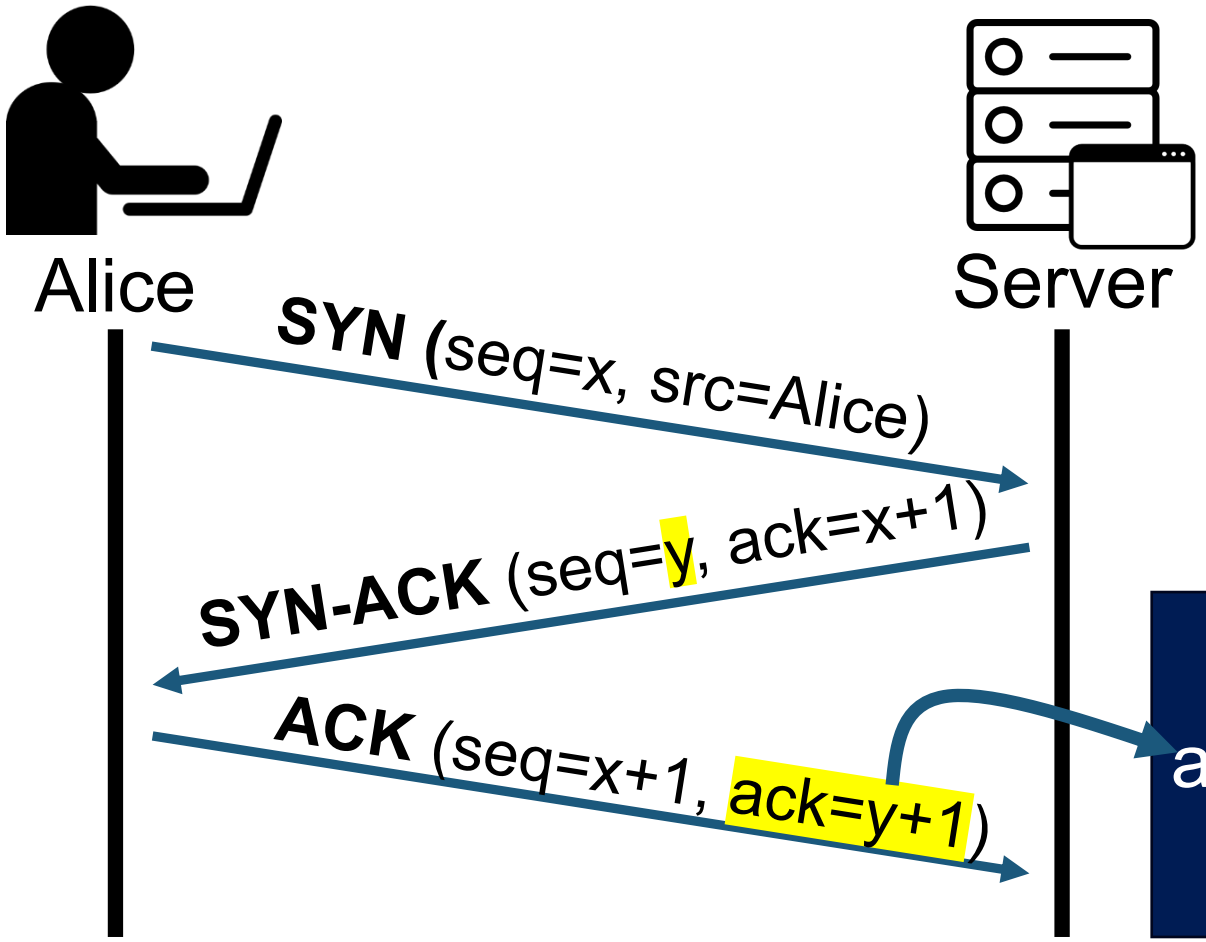
SYN Cookie

- Idea: DO NOT store! DO **recompute**!



SYN Cookie

- Idea: DO NOT store! DO **recompute**!



Compute SYN Cookie

SYN Cookie =

$H(Server_{ip}, Client_{ip}, Server_{port}, Client_{port})$

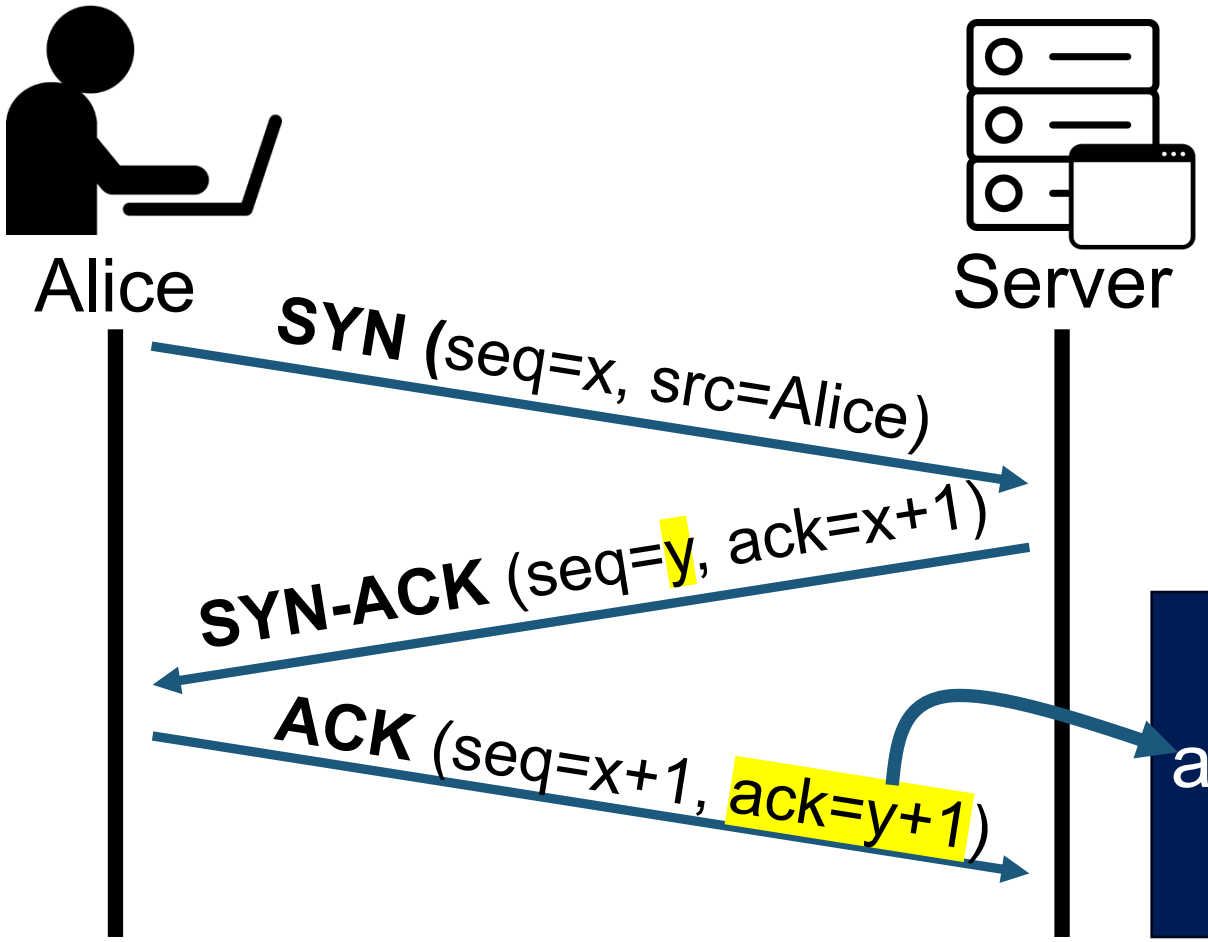
Verify (Recompute)

ack == 1+$H(Server_{ip}, Client_{ip}, Server_{port}, Client_{port})$

SYN Cookie

- Idea: DO NOT store! DO **recompute**!

```
$ sysctl -w net.ipv4.tcp_syncookies=1
```



Compute SYN Cookie

SYN Cookie =

$$H(Server_{ip}, Client_{ip}, Server_{port}, Client_{port})$$

Verify (Recompute)

ack == 1+$H(Server_{ip}, Client_{ip}, Server_{port}, Client_{port})$

SYN Cookie

- Idea: DO NOT store! DO **recompute**!
- SYN Cookie = $H(Server_{ip}, Client_{ip}, Server_{port}, Client_{port})$

SYN Cookie

- Idea: DO NOT store! DO **recompute**!
- SYN Cookie = $H(Server_{ip}, Client_{ip}, Server_{port}, Client_{port})$
- Limitation: SYN cookie value is **public** because: $H, Server_{ip}, Client_{ip}, Server_{port}, Client_{port}$ are all public
  - Attackers can send massive valid SYN cookie!
- Idea: $H(Server_{ip}, Client_{ip}, Server_{port}, Client_{port}, \boldsymbol{Secret})$ where $\boldsymbol{Secret}$ is randomly generated by the server

Botnet

Definition: Bot

- Bot (Zombie):
  - A software application that runs automated tasks over the Internet
  - Compromised computer controlled by malware (bot-code) without owner consent/knowledge

Definition: Botnet

- Botnet:
  - A **collection of bots** communicating with other similar programs in order to perform tasks

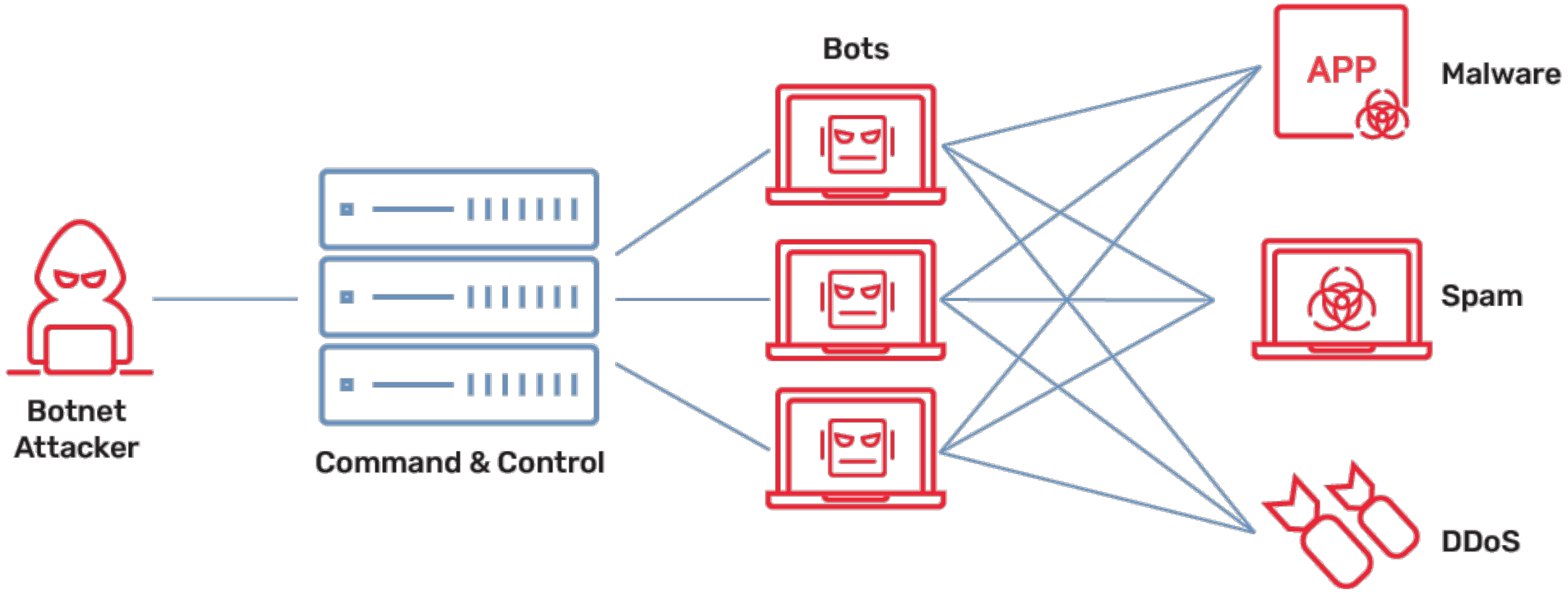


Image from https://www.a10networks.com/glossary/what-is-a-botnet-iot-botnet/

Botnet Threat

- Infects huge amount of computers
- Infected computers are under control of botnet attacker

- They can make profit for botnet attacker
  - Infect new hosts
  - Send spam/phishing email
  - Perform DDoS attacks for some rewards
  - …

Command and Control (C&C) Server

- Essential for operation and support of botnet
- Two styles
  - Centralized
  - P2P

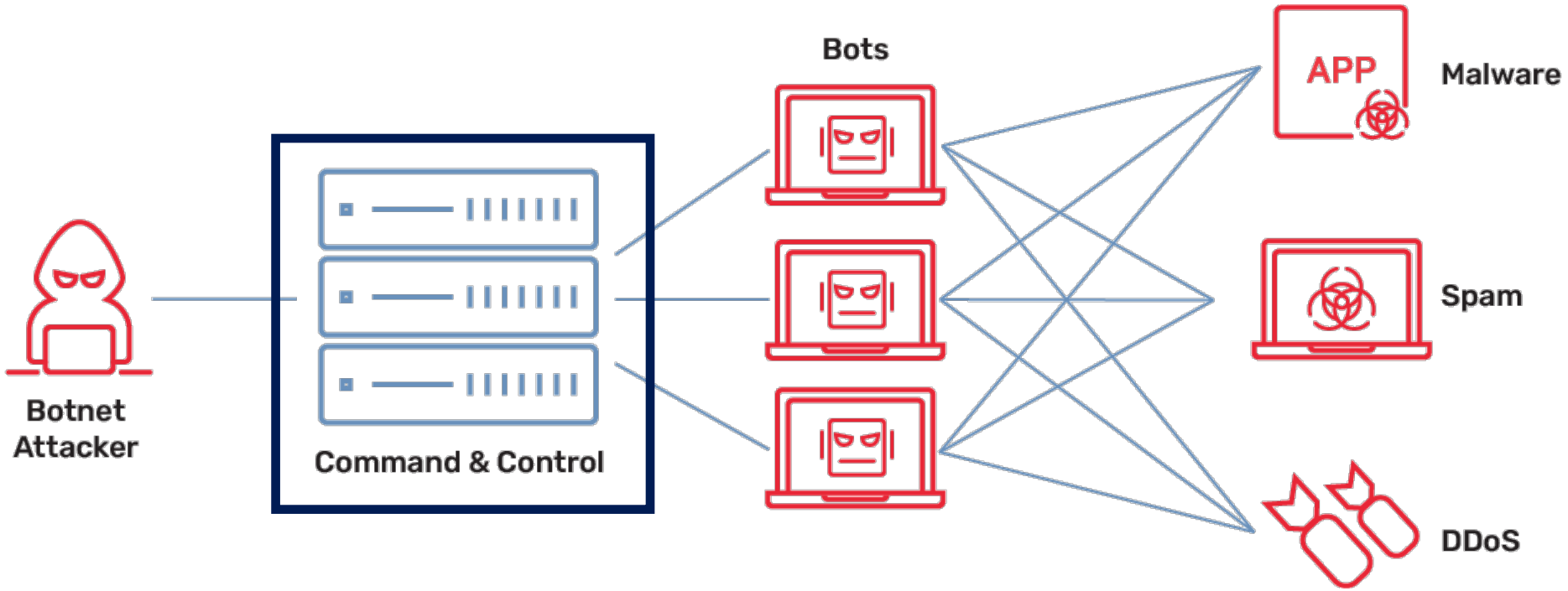
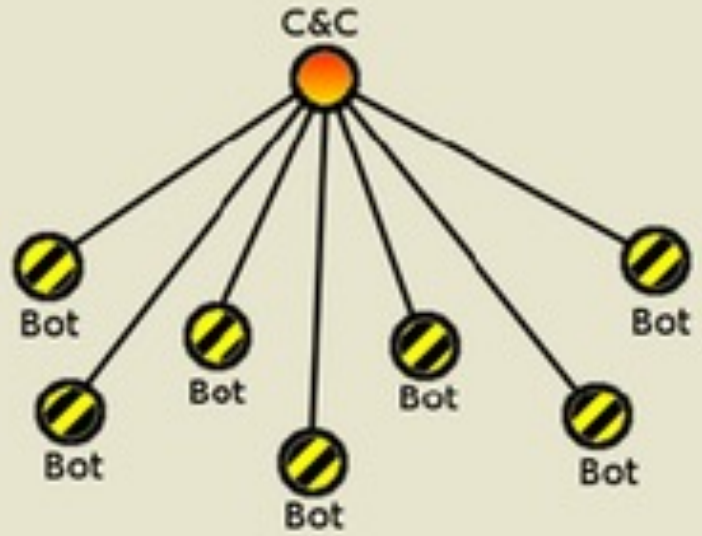


Image from https://www.a10networks.com/glossary/what-is-a-botnet-iot-botnet/

Centralized C&C

- **Pros**: Simple to deploy, cheap, short latency for large scale attacks
- **Cons**: Easiest to eliminate

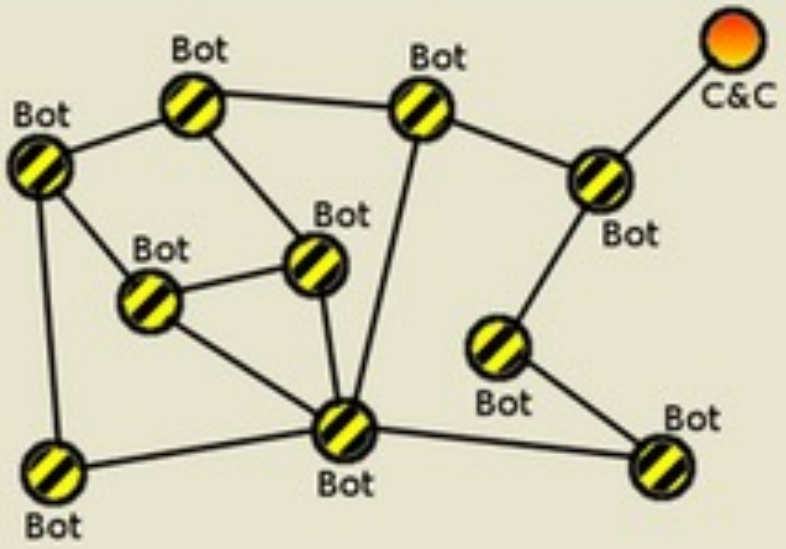
Centralized Botnet



P2P C&C

- **Pros**: Resilient to failures, hard to discover, hard to defend
- **Cons**: Hard to launch large scale attacks
  - Because P2P technologies (Napster, Gnutella…) are currently only capable of supporting very small groups (<50 peers)

Peer-to-Peer Botnet



Summary

- Worm: first network attack
- Denial of Service (DoS)
  - Distributed DoS (DDoS)
  - Ping Flood Attack
  - Smurf Attack
  - Amplification Attack
  - SYN Flooding Attack
- SYN Flooding Attack
- Botnet

Question?