Network (in)security

Thierry Sans

How many of you …

- have programmed with **sockets** ?
- have taken a **networking course** ?
- have used tools like ?
  `ping, traceroute, ipconfig/ifconfig, nslookup`
  `netstat, netcat, nmap, wireshark`
- know what is :
  IP address, port, a canonical hostname
  client, server, router
  switch (or hub), gateway
- can explain with a fair amount of details :
  Ethernet, WiFi
  IP, TCP
  ARP, BGP, DNS

The Internet

1980's - few hosts connected : government institutions and universities

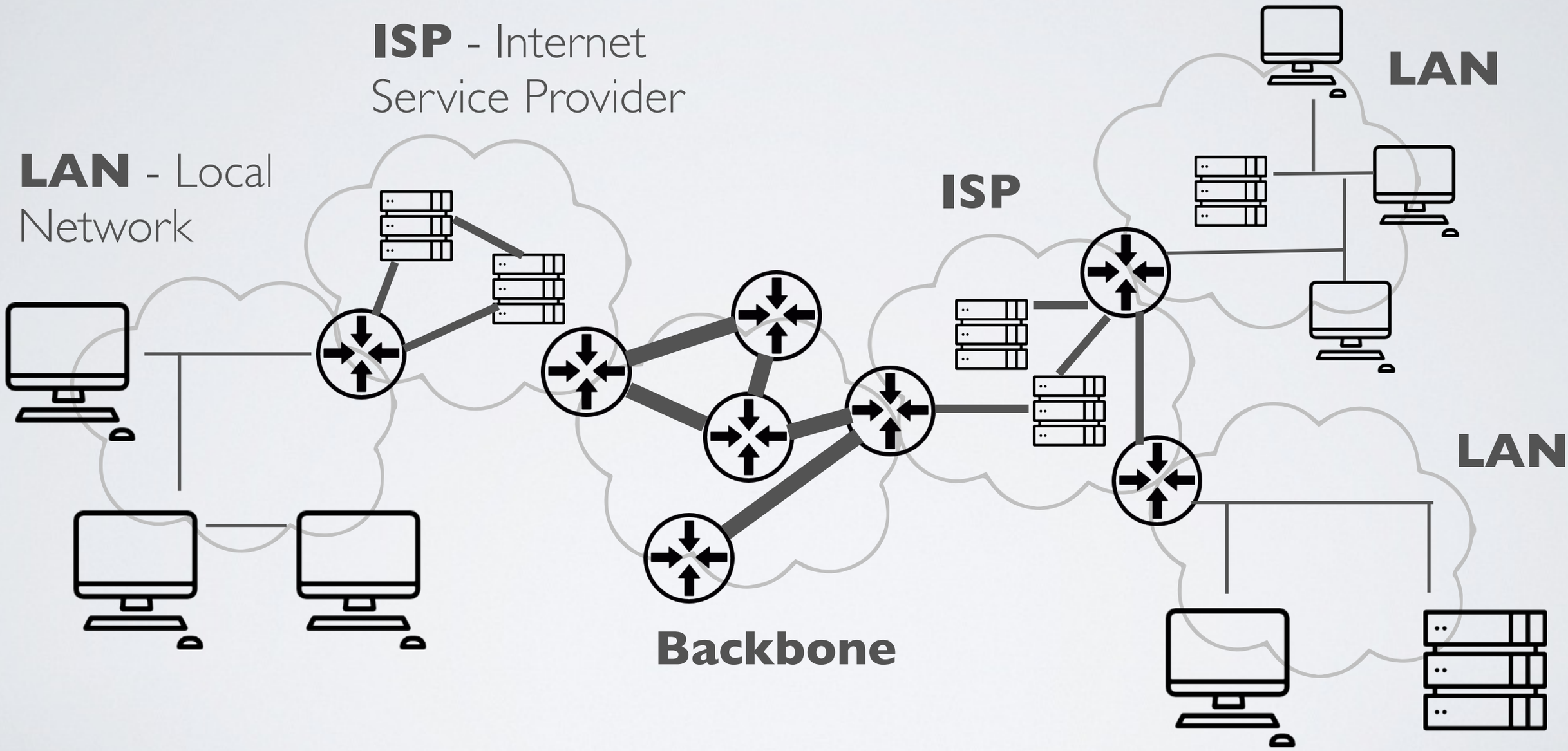
➡ Trustworthy environment

2016 - ~ 6 billion hosts connected : network of networks

➡ Untrustworthy environment

➡ Internet (and its protocols) was
not designed for untrustworthy environment

A network of networks



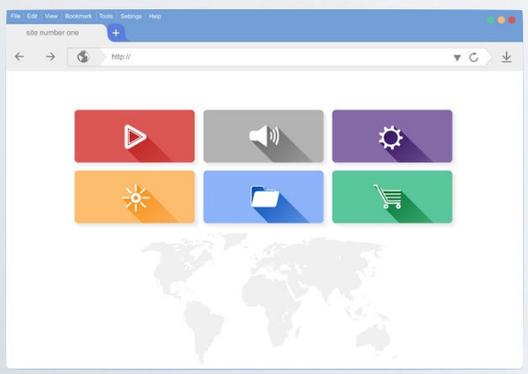
What is a protocol

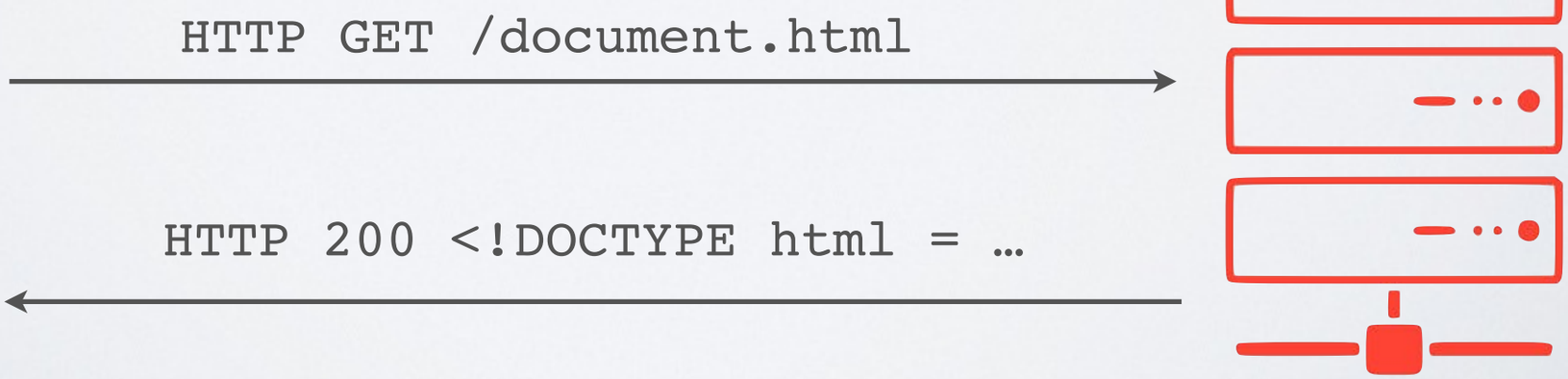
Communication protocol

is an agreement on how communication should take place

- defines the data encoding and/or format
- defines the message sequence

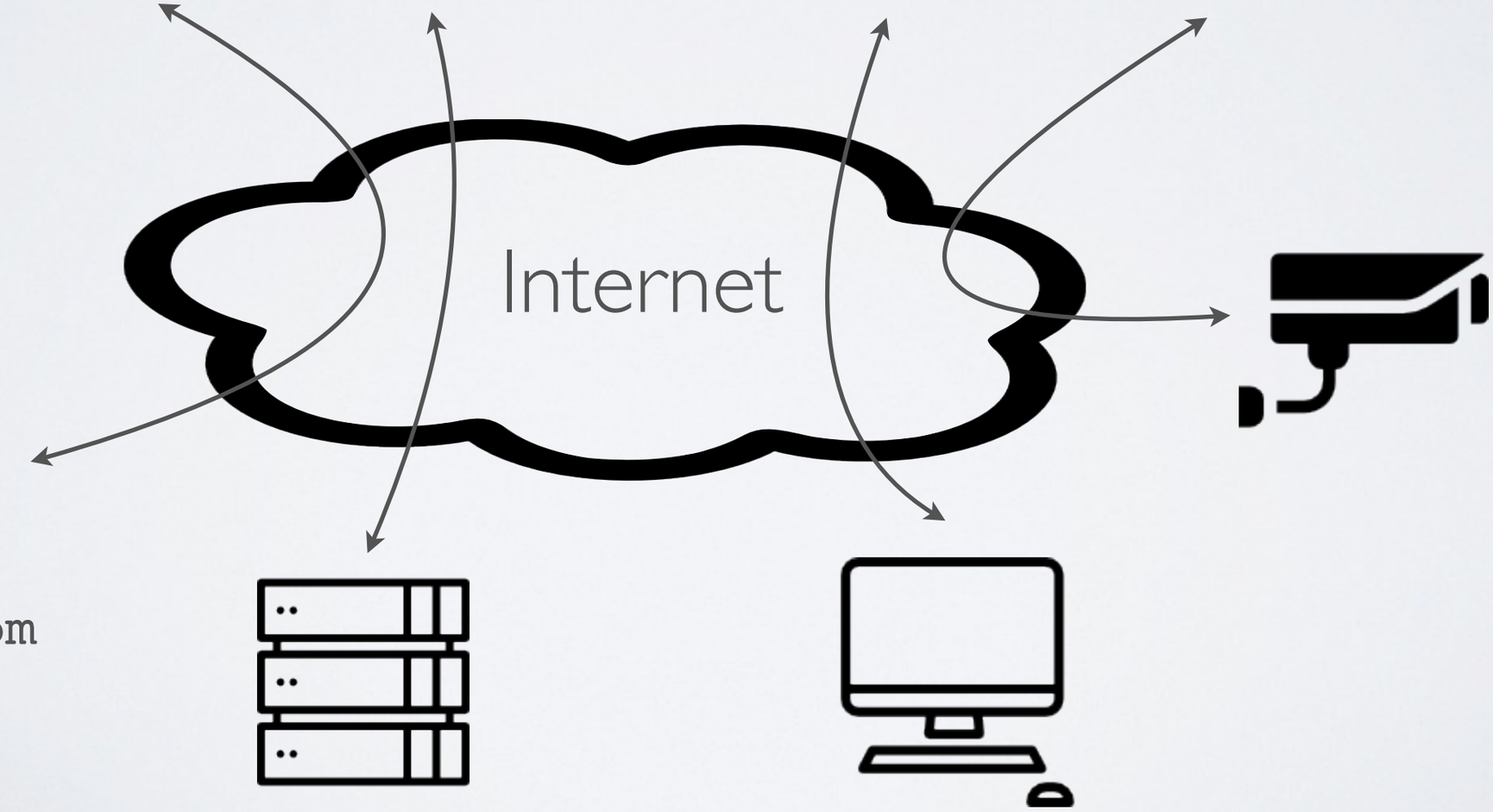
➡ (most) protocols are standards defined by the IETF - The Internet Engineering Task Force





Internet Applications

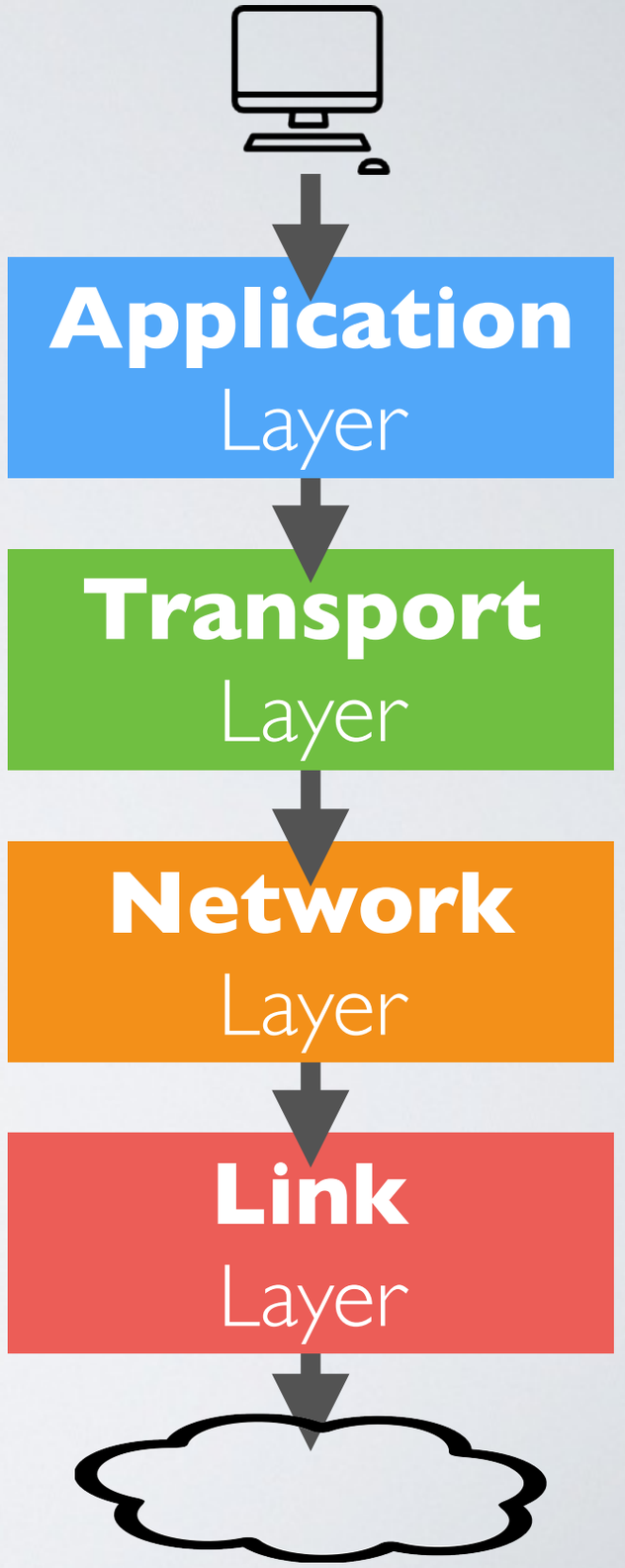
Web	Mail	File Exchange	Remote Shell	...
`http`	`smtp imap pop3 exchange`	`BiTorrent`	`ssh`	



The Internet Protocol Suite (a.k.a the network stack)

Protocols are built on top of each as layers (modularity and encapsulation)

- How two programs can send messages to each other ?
- How to make sure that messages have been well transmitted ?
- How to route messages through the network ?
- How to encode messages to go through copper, fiber or air ?



confidentiality
integrity
availability

The attacker is capable of …

Scanning - survey the network and its hosts

Eavesdropping - read messages

Spoofing - forge illegitimate messages

DOS (Denial of Service) - disrupt the communications

➡ The attacker can target any layer in the network stack

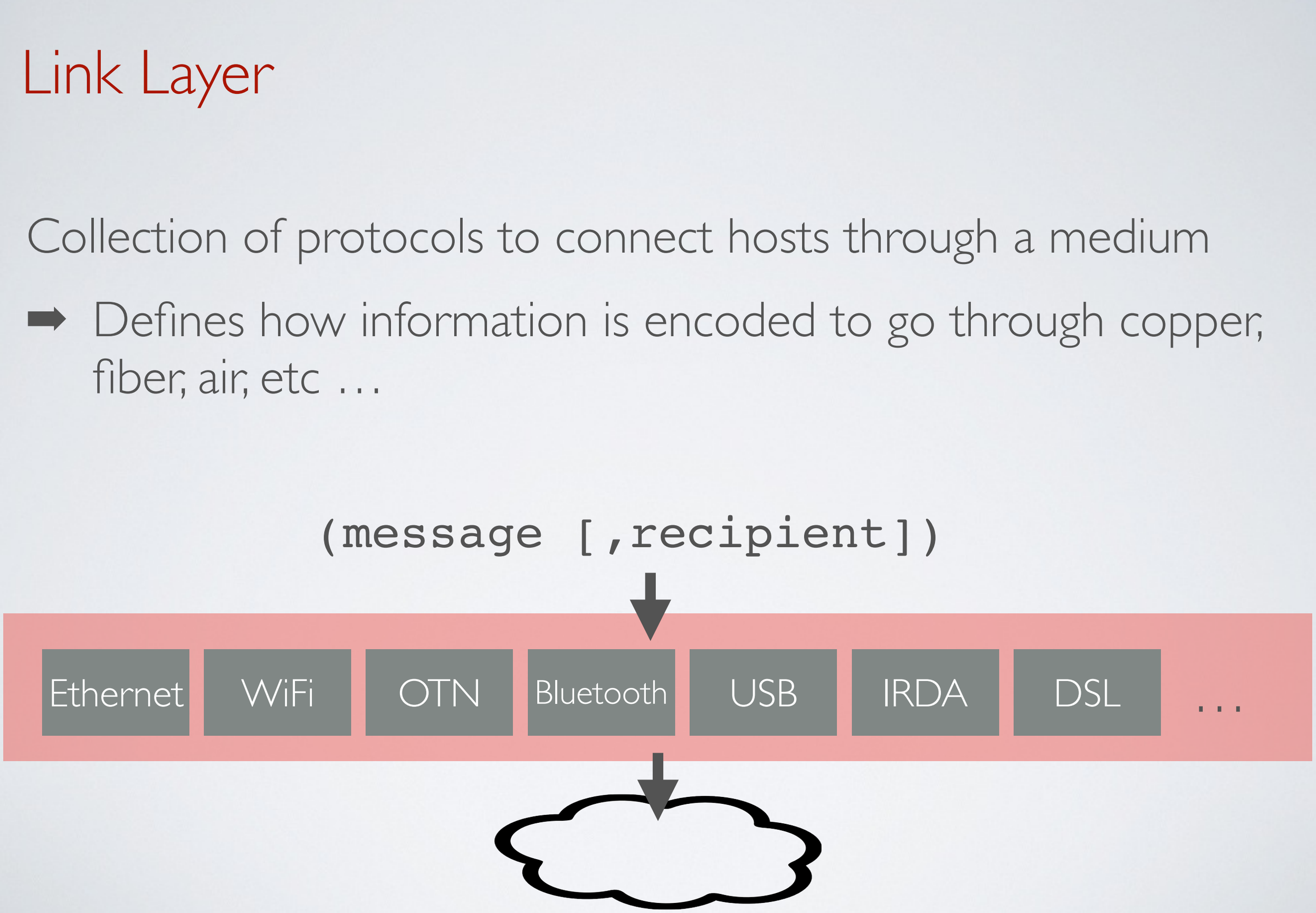
Link Layer

connecting machines together

Link Layer

Collection of protocols to connect hosts through a medium

➡ Defines how information is encoded to go through copper, fiber, air, etc …



Multiple Interfaces

A host can be connected to several hosts or networks through **multiple interfaces**

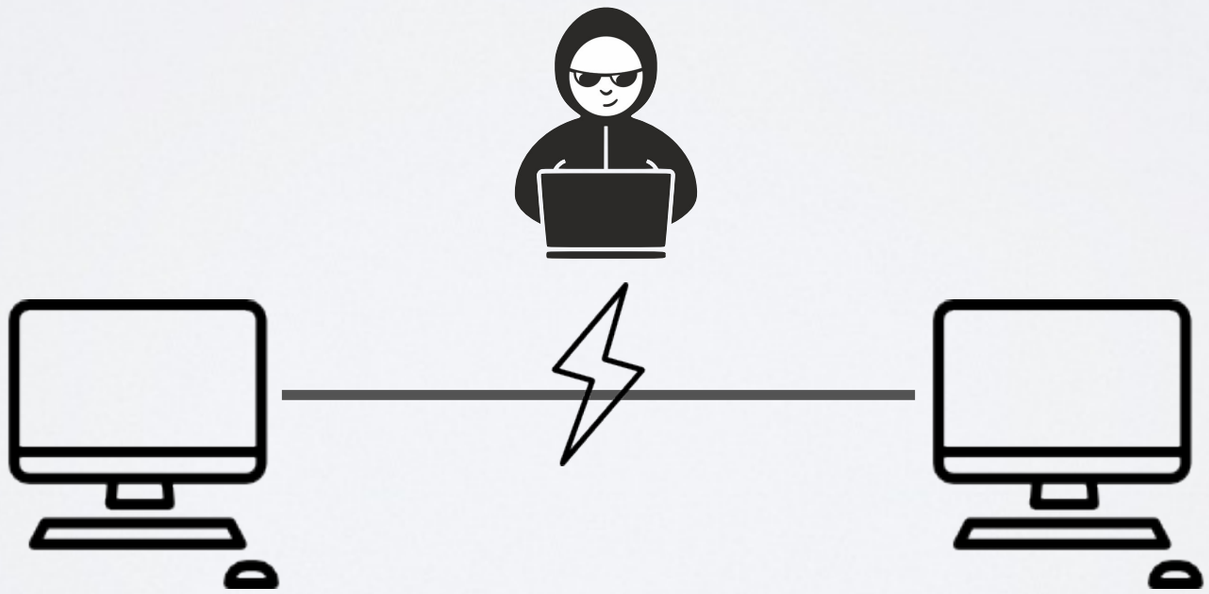
- Some are connected to a single host only (Point-to-Point)
- Others are connected to a entire network (BUS)

Point-to-Point Link

Only two hosts are connected at each end of the medium

e.g. OTN, IRDA, DSL …

➡ Harder for an attacker to intercept messages

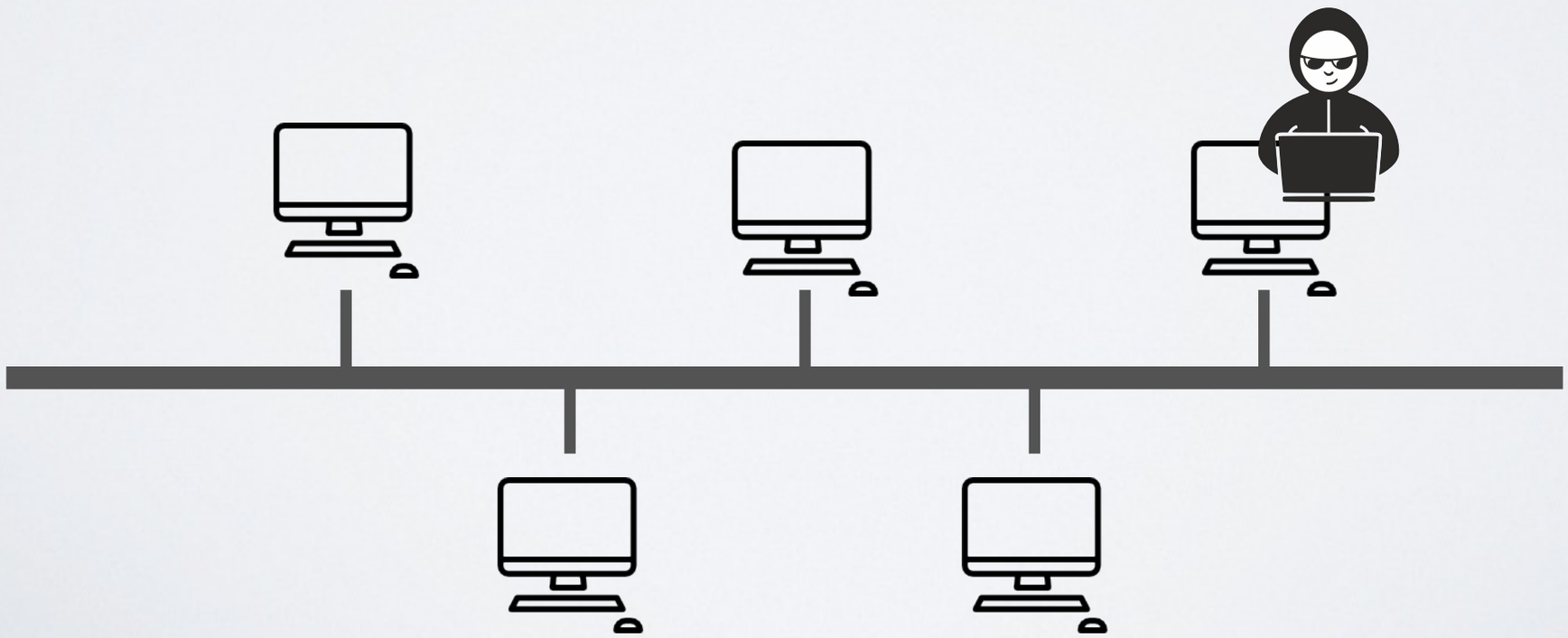


Bus Link (a.k.a LAN - Local Area Network)

Several hosts are connected to the same medium with a unique physical address called

e.g. Ethernet and WiFi uses MAC Media Access Control addresses

➡ Easier for the attacker to intercept messages since they are all broadcasted to the same medium



confidentiality

Packet Sniffing over Ethernet or WiFi

- All messages are transmitted on the medium with the MAC address of the recipient

- Each network interface only picks messages that correspond to its MAC address

➡ An attacker can set its network interface in ***promiscuous mode*** to capture (sniff) all traffic

e.g. Wireshark

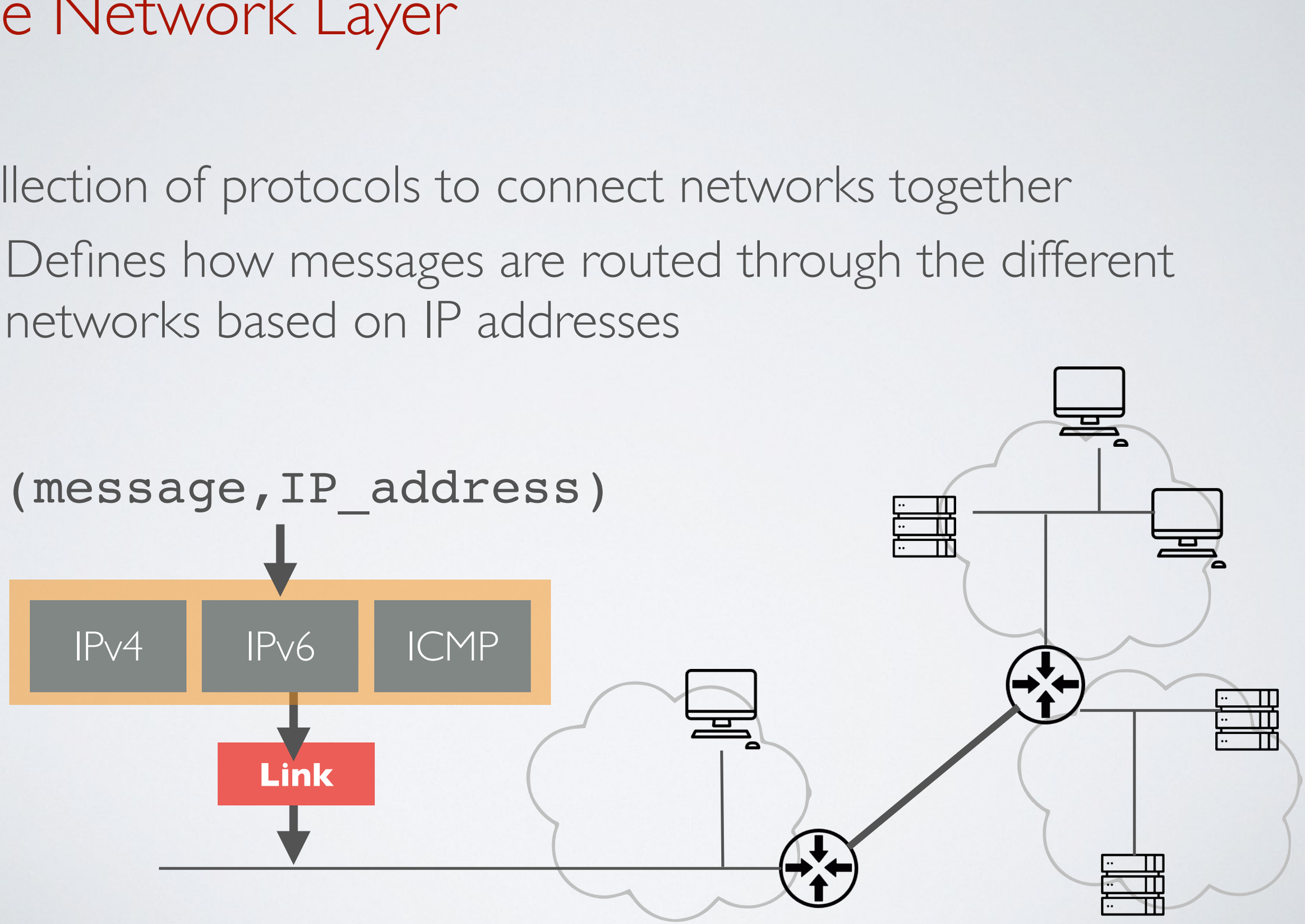
Network Layer

connecting networks together

The Network Layer

Collection of protocols to connect networks together

➡ Defines how messages are routed through the different networks based on IP addresses



IP - Internet Protocol

- Each message has the IP address of the issuer and recipient
- Routers route packet based on their routing table and a default route

➡ Best effort protocol

ICMP - Internet Control Message Protocol

Exchange information about the network

e.g. error reporting, congestion control, network reachability

➡ `ping, traceroute`

Host Discovery

~ confidentiality

By default, hosts answer to ICMP echo request messages

➡ An attacker scan an entire network to find IP addresses of active hosts

e.g. **`nmap`** (does that among other things)

IP Spoofing

integrity
availability

- Routers do not validate the source
- Receiver cannot tell that the source has been spoofed

➡ An attacker can generate raw IP packets with custom IP source fields

e.g. DOS (blackhole) and MITM attacks

ICMP ping of death (before 1997)

availability

Any host receiving a 64K ICMP payload would crash or reboot

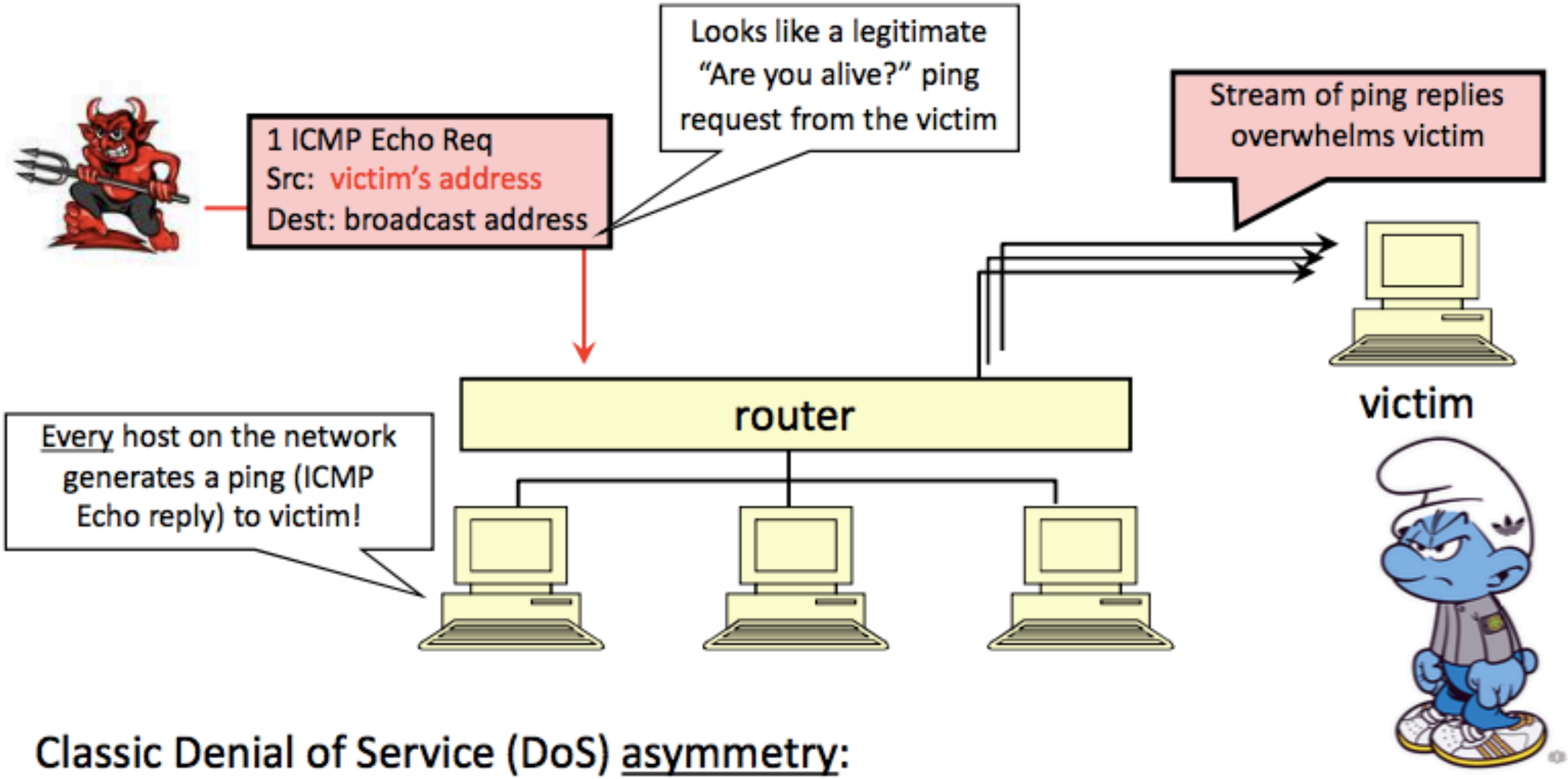
- 64K bytes payload were assumed to be invalid by programmers
- An attacker could split a 64K payload, transmit it and would be reassembled by the receiver overflowing a buffer

ICMP Ping Flood

availability

- An attacker can overwhelm a host by sending multiples ICMP echo requests

ICMP Smurf Attack - an elaborated ping flood attack



Classic Denial of Service (DoS) asymmetry:
cheap for attacker, expensive for victim, due to protocol amplification

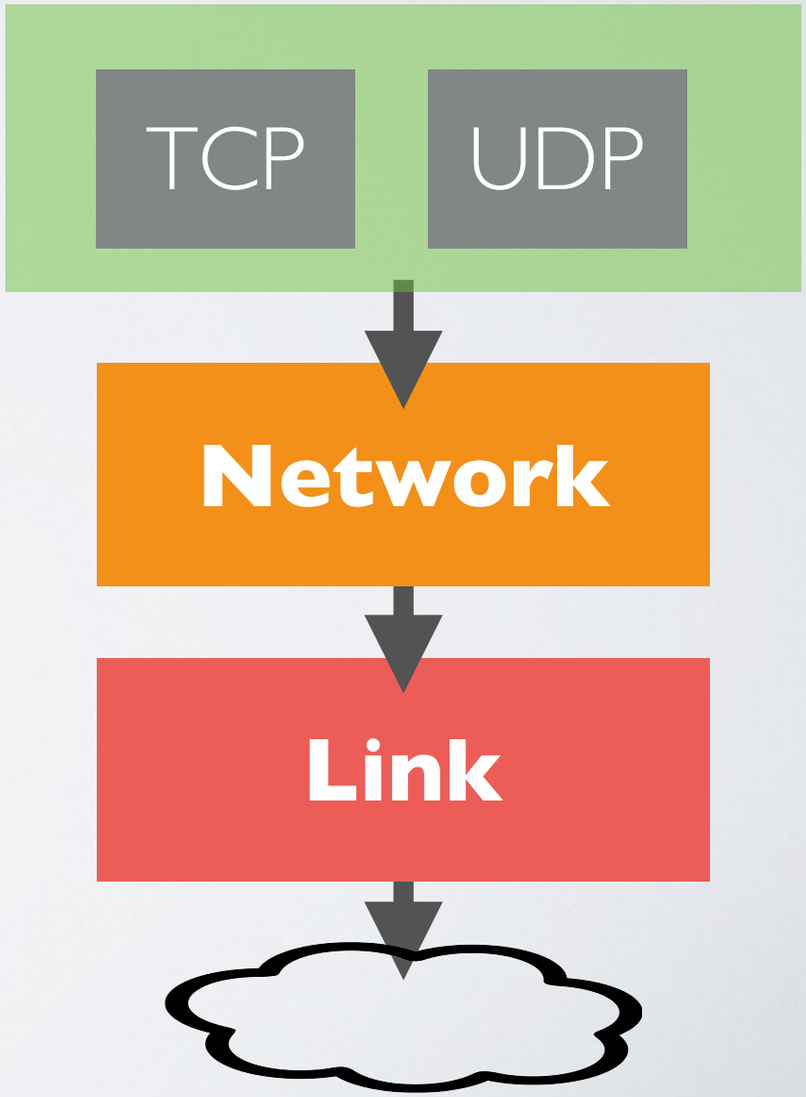
Transport Layer

end-to-end connection

The Transport Layer

Collection of protocols to ensure end-to-end connections

- ➡ Allows hosts to have multiple connections through **ports**
- ➡ Allows messages to be **fragmented** into small IP packets
- ➡ Make sure that all packets are received

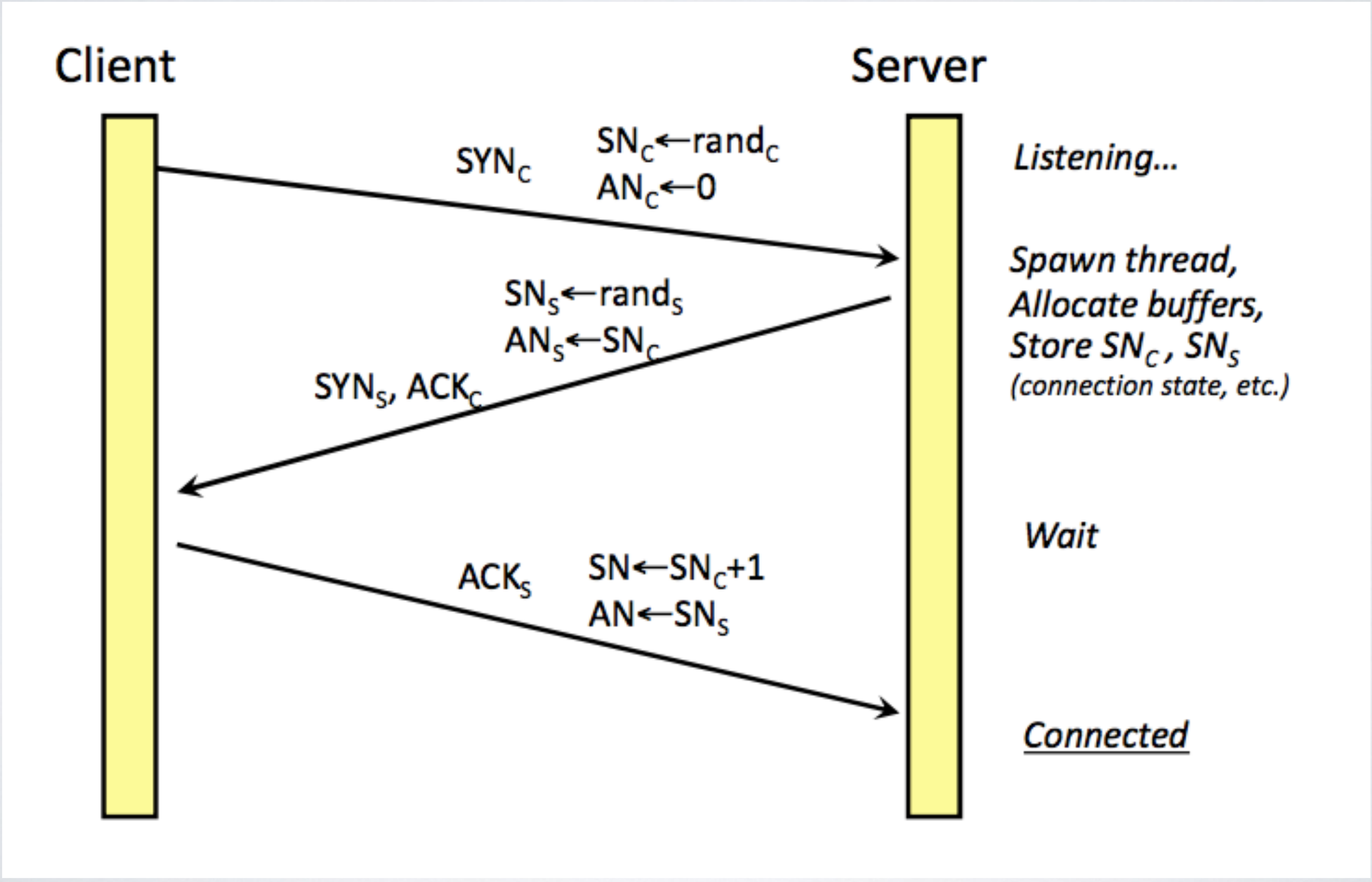


TCP - Transmission Control Protocol

- The sender divides data-stream into packets sequence number is attached to every packet
- The receiver checks for packets errors, reassembles packets in correct order to recreate stream
- ACK (acknowledgements) are sent when packets are well received and lost/corrupt packets are re-sent

➡ Connection state maintained on both ends

TCP "3-way" handshake



Port scanning

~ confidentiality

- Using the "3-way" handshake, an attacker can scan for all open ports for a given host

  e.g. **`nmap`**

availability

TCP-syn flooding

Client

Server

SYN_{C1}

SYN_{C2}

SYN_{C3}

SYN_{C4}

SYN_{C5}

Listening…

Spawn a new thread, Allocate buffers

… and more

… and more

… and more

… and more

… and more

Hold on, won't 3-way handshake cause Client to receive it's own "syn flood" as server responds to all it's SYN's with SYN-ACK's?

Note asymmetric effort between attacker client and victim server

TCP Connection Reset (DOS)

availability

Each TCP connection (i.e each port) has an associated state sequence number

- An attacker can guess (sniff) the current sequence number for an existing connection and send packet with reset flag set, which will close the connection

UDP - User Datagram Protocol

UDP is a connectionless transport-layer protocol

➡ No acknowledgement, no flow control, no message continuation, no reliability guarantees

e.g. media streaming (VoIP, video broadcasting)

UDP Flood

availability

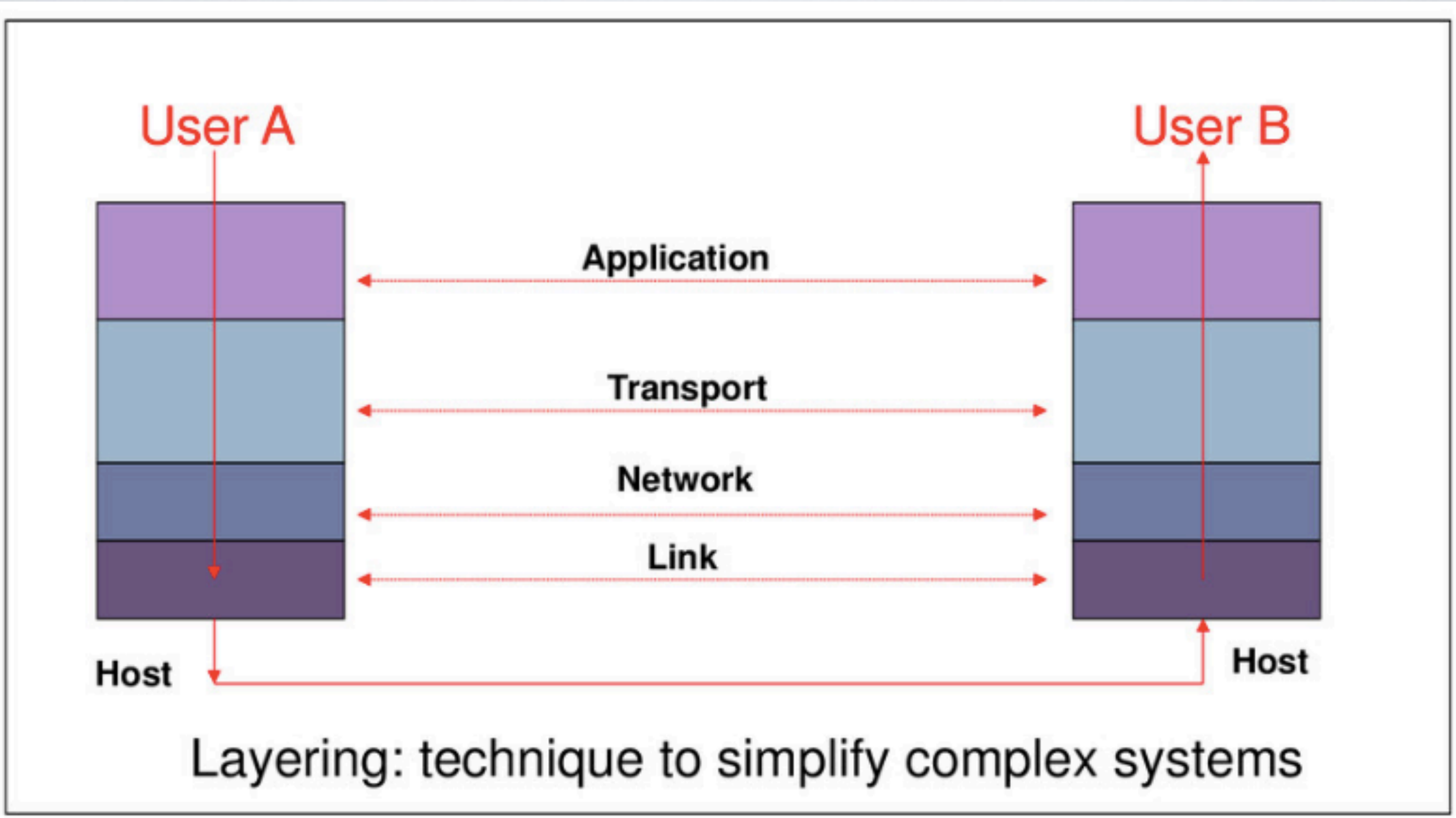
When a UDP packet is received on a non-opened port, the host replies with an `ICMP Destination Unreachable`

➡ An attacker can send a large number of UDP packets to all ports of a target host

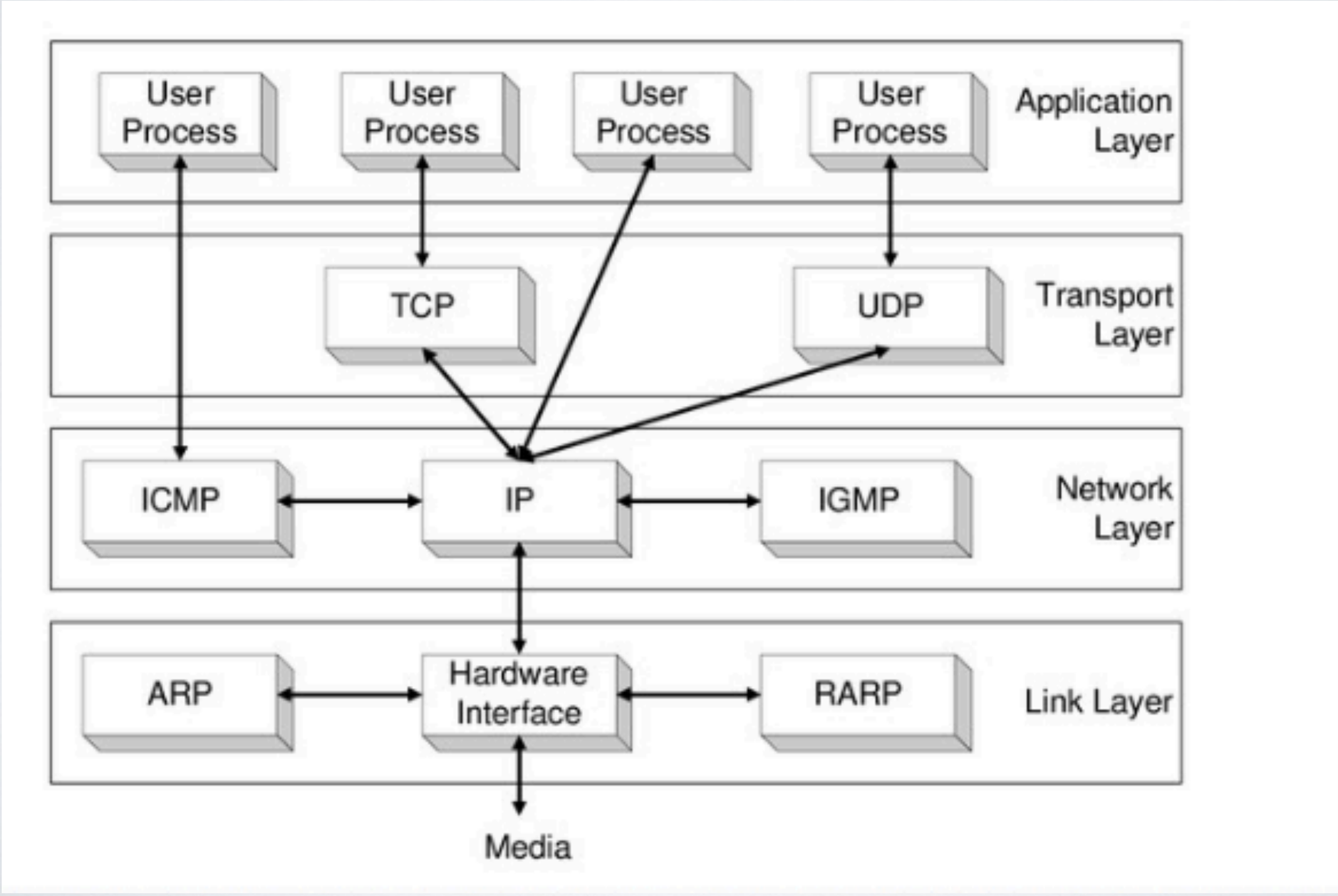
e.g *Low Orbit Ion Cannon*

The TCP/IP Stack

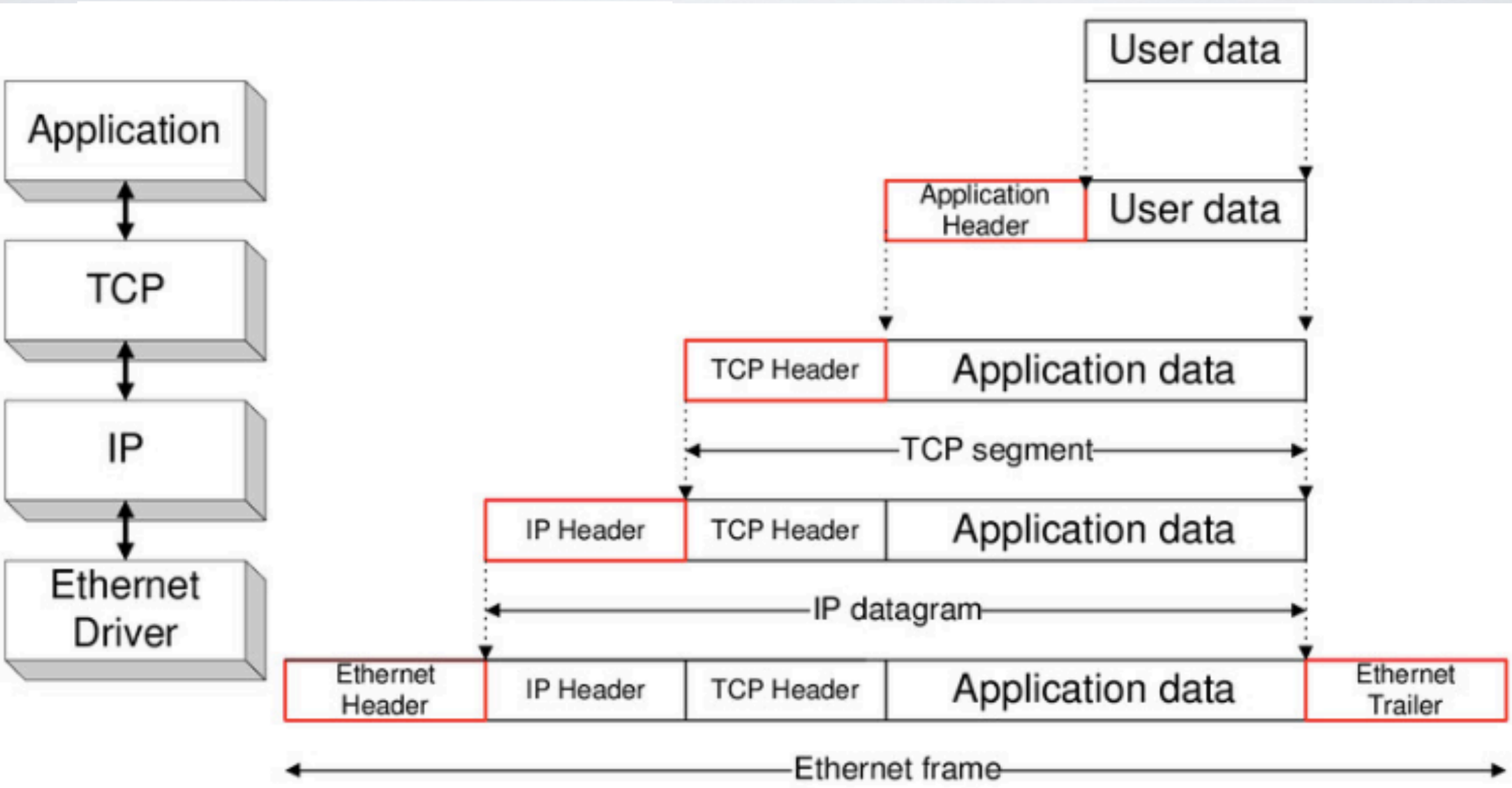
Layering


User A
User B
Application
Transport
Network
Link
Host
Host
Layering: technique to simplify complex systems

TCP/IP


User Process
User Process
User Process
User Process
Application Layer
TCP
UDP
Transport Layer
ICMP
IP
IGMP
Network Layer
ARP
Hardware Interface
RARP
Link Layer
Media

Data encapsulation

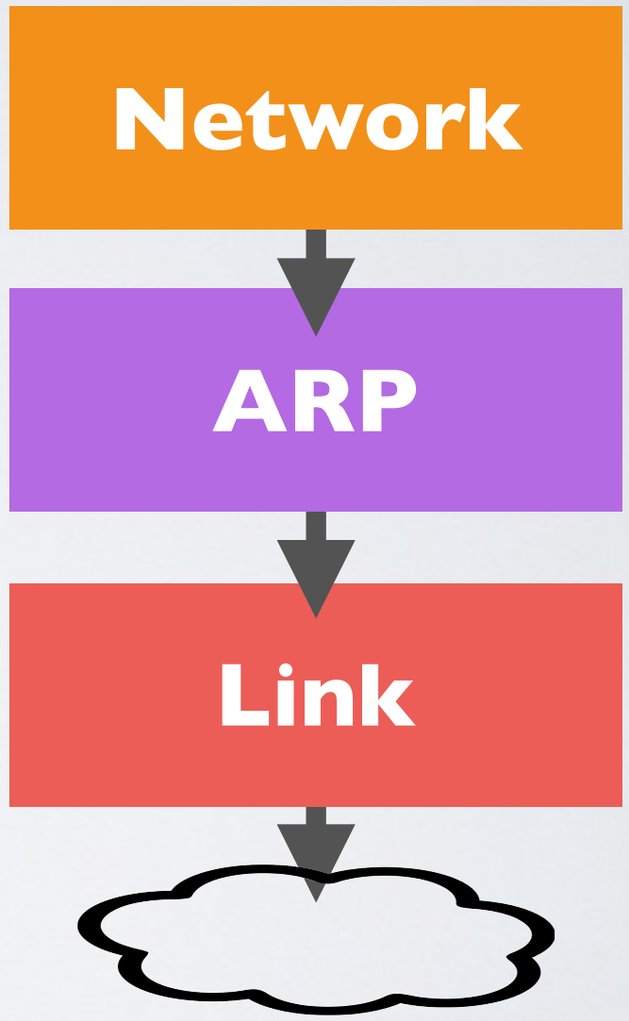


Special Protocols

ARP - Address Resolution Protocol

Each host has an ARP table that contains mapping between MAC and IP addresses

➡ Host broadcasts their own IP address and MAC address to others to build their ARP table



ARP Cache Poisoning

integrity
availability

➡ An attacker can broadcast fake IP-MAC mappings to the other hosts on the network

e.g. DOS and MITM attacks

BGP - Border Gateway Protocol (a.k.a routing)

Each router has a routing table to IP messages

BGP is the protocol for establishing routes

➡ Routers advertise the best route to other nearby routers depending on the state of the network

Route hijacking

confidentiality

availability

➡ An attacker can advertise fake routes

e.g. DOS (blackhole) and MITM attacks

DNS - Domain Name Server

Internet applications relies on canonical hostname rather than IP addresses

DNS servers translates domain names into IP addresses

➡ DNS servers form a distributed directory service by exchanging information about domains and other DNS servers

DNS Cache Poisoning

confidentiality

availability

➡ An attacker can advertise fake DNS information

e.g. DOS and MITM attacks