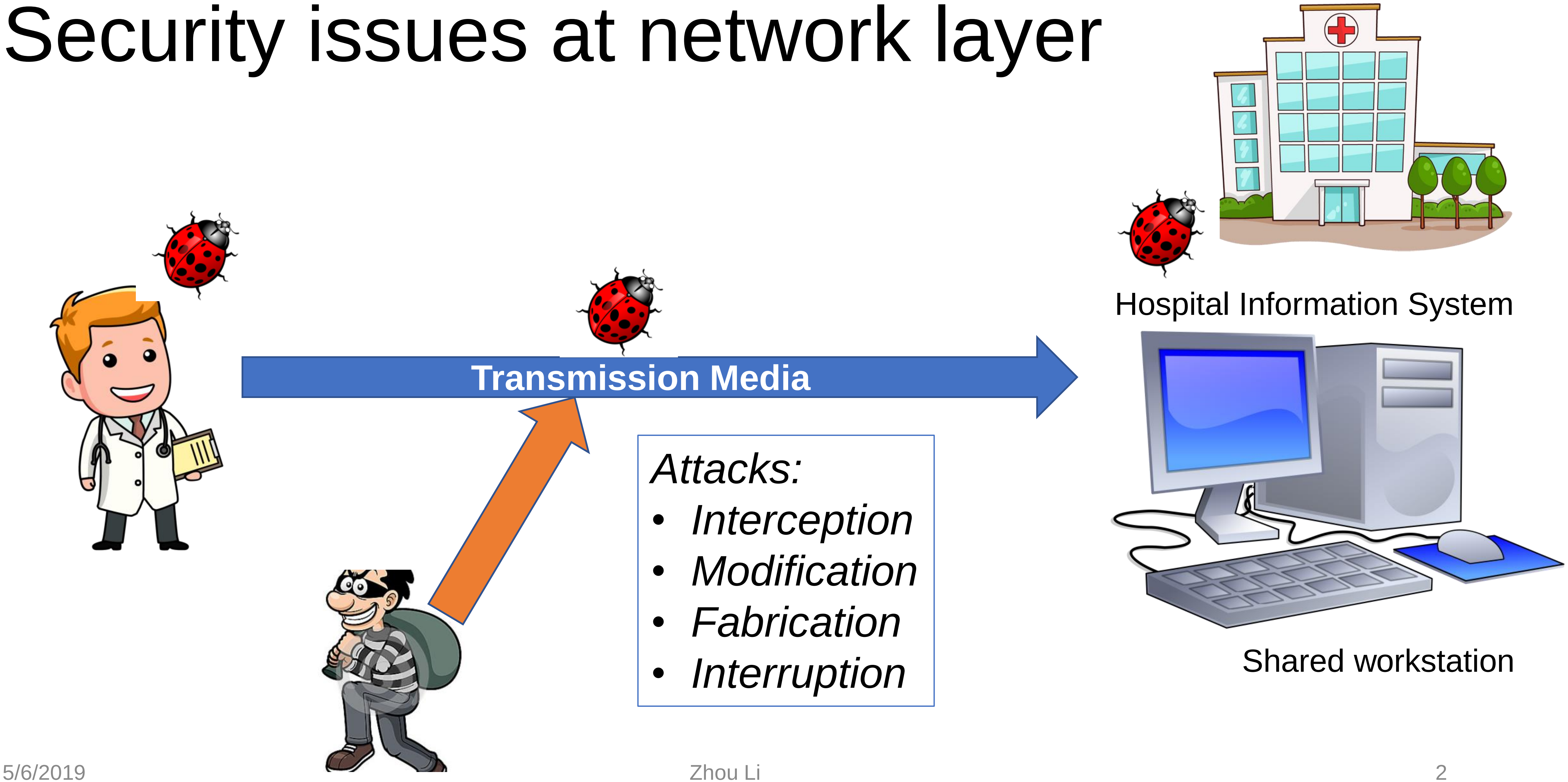
Network Security

EECS 195

Spring 2019

Zhou Li

Security issues at network layer



Attacks:
- *Interception*
- *Modification*
- *Fabrication*
- *Interruption*

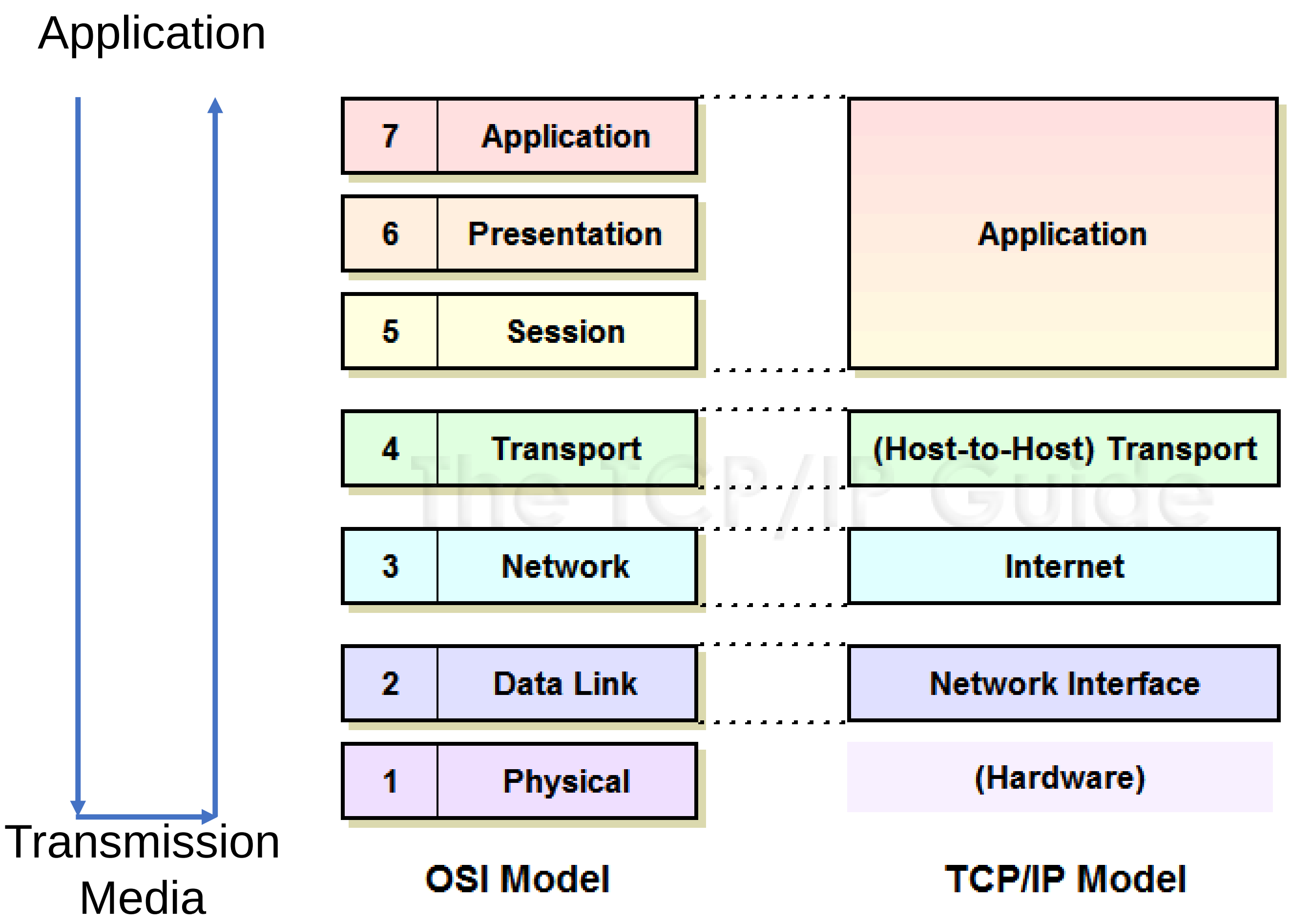
Objectives

- Networking basics
- Network threats and vulnerabilities
- WiFi security
- Denial-of-service attacks
- Network encryption concepts and tools
- Types of firewalls and what they do
- Intrusion detection and prevention systems

Network Transmission

- Transmission Media
  - Cable, Optical fiber, Microwave, WiFi, Satellite communication
- Attack vectors
  - Packet sniffing, emanation, cable splicing
- Wireless media is more vulnerable to wiretapping

The OSI Model and TCP/IP Stack



Attacks

HTTP hijacking, …

DNS poisoning, …

SYN flooding, …

IP flooding, …

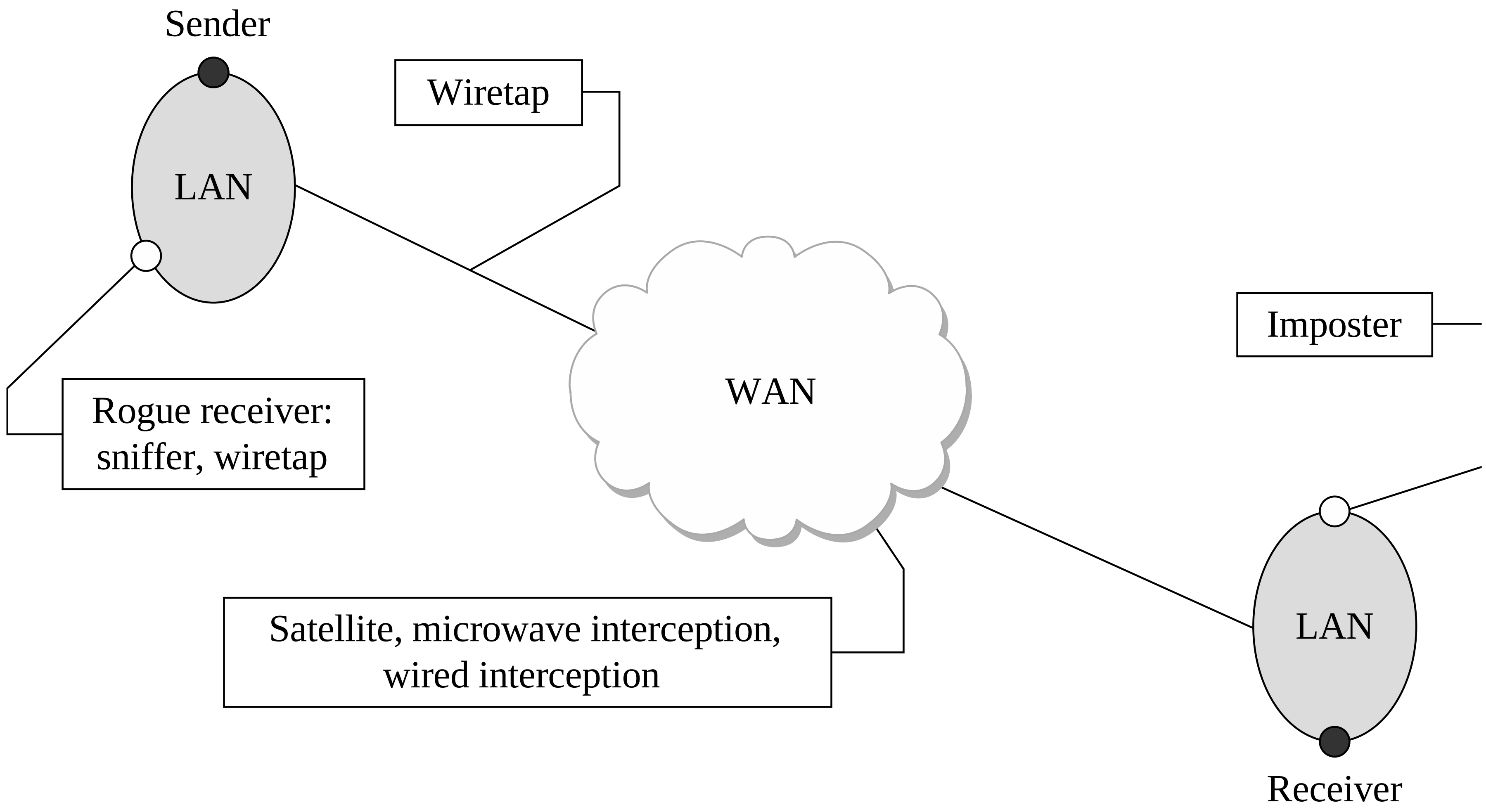
WEP key cracking, …

Addressing and routing

- For data going from A to B
  - Indirect connection for most cases, relays are needed
- Addressing
  - Network layer: router sends packet (destination IP address, source IP address and data)
  - Data-link layer: MAC addresses of your computer's and router's NIC are added to packet to create a frame
- Routing
  - Directs traffic on a path leading to a destination
- Ports
  - Number associated with an application program that serves or monitors for a network service

Network Threats and Attacks

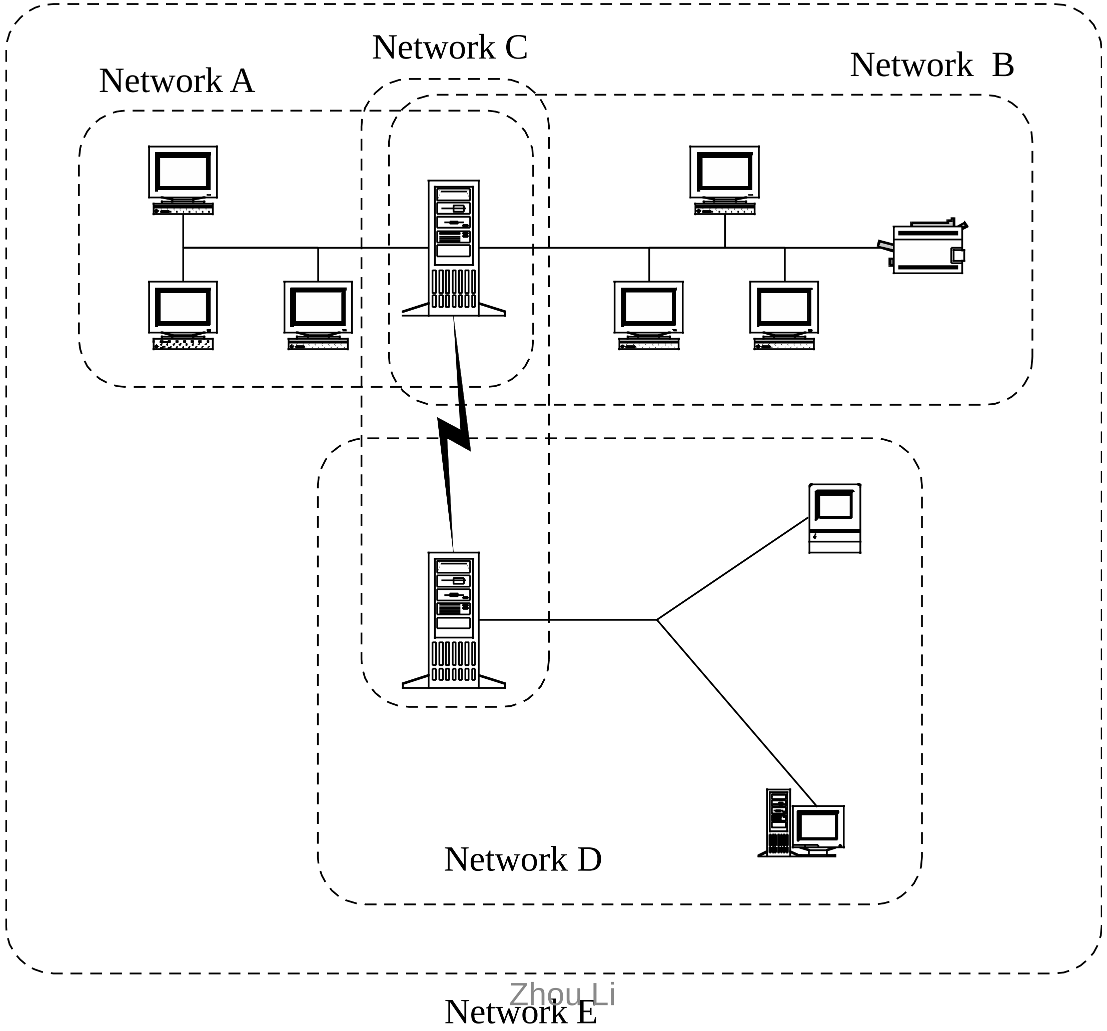
Adversary Model



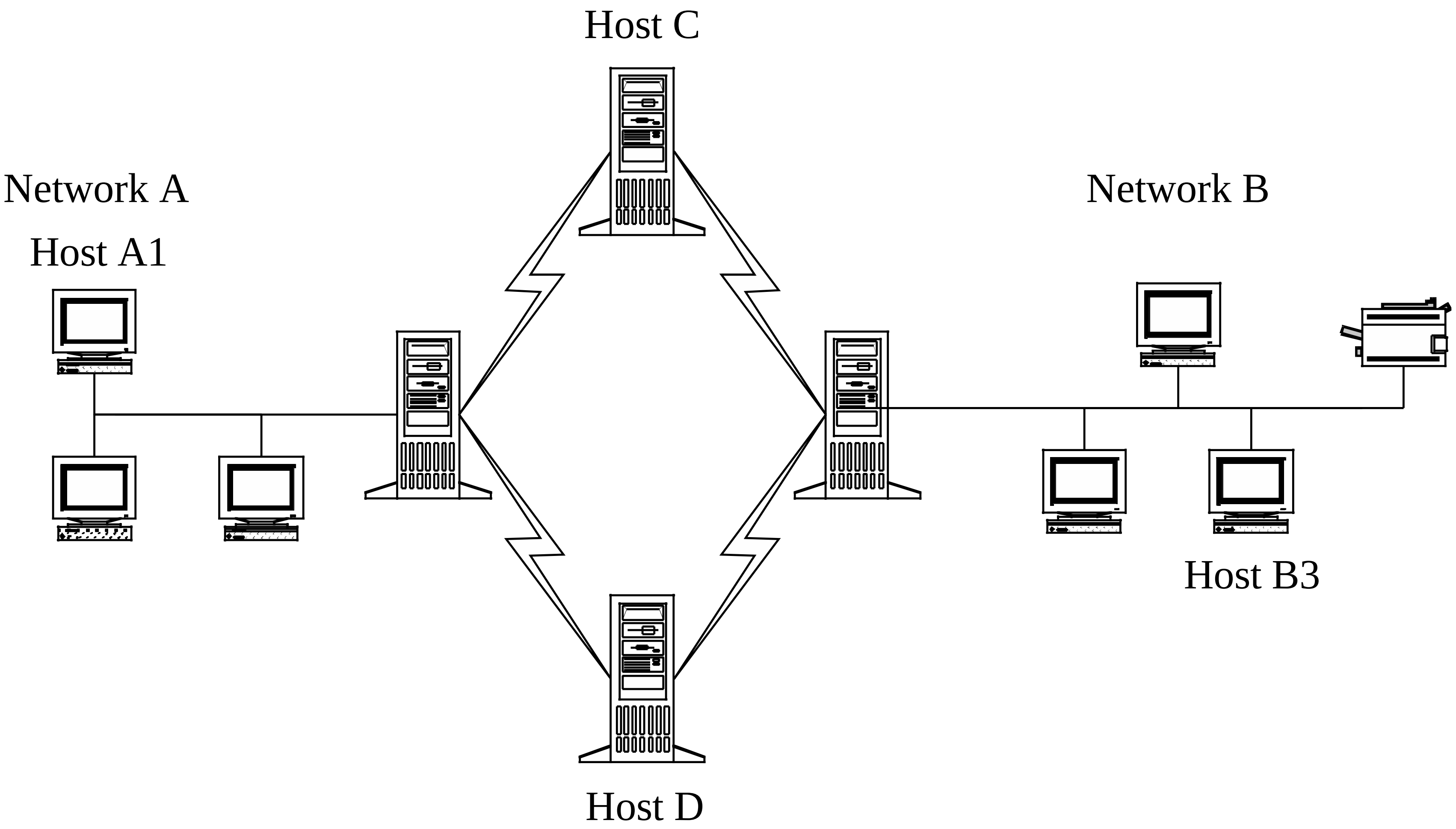
What Makes a Network Vulnerable to Interception?

- Anonymity
  - An attacker can attempt many attacks, anonymously, from thousands of miles away
- Many points of attack
  - Large networks mean many points of potential entry
- Sharing
- Network complexity
  - One system is very complex and hard to protect; networks of many different systems, with disparate OSs, vulnerabilities, and purposes are that much more complex
- Unknown perimeter
  - Networks, especially large ones, change all the time, so it can be hard to tell which systems belong and ed systems open up potential access to more users than do single computers
- System are behaving, and impossible to tell which systems bridge networks
- Unknown path
  - There may be many paths, including untrustworthy ones, from one host to another

Unknown Perimeter



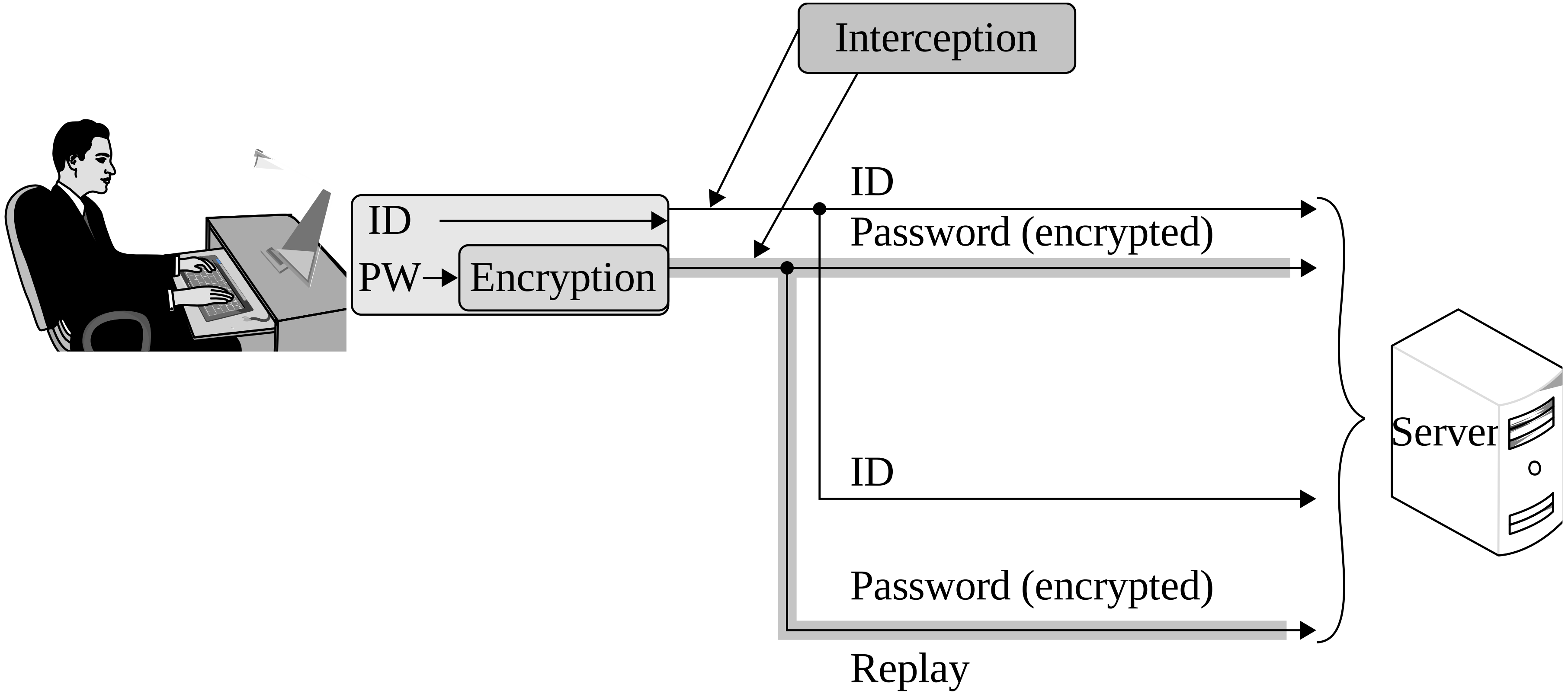
Unknown Path



Modification and Fabrication

- Data corruption
  - May be intentional or unintentional, malicious or nonmalicious, directed or random
- Sequencing
  - Permuting the order of data, such as packets arriving in sequence
- Substitution
  - Replacement of one piece of a data stream with another
- Insertion
  - A form of substitution in which data values are inserted into a stream
- Replay
  - Legitimate data are intercepted and reused

Simple Replay Attack



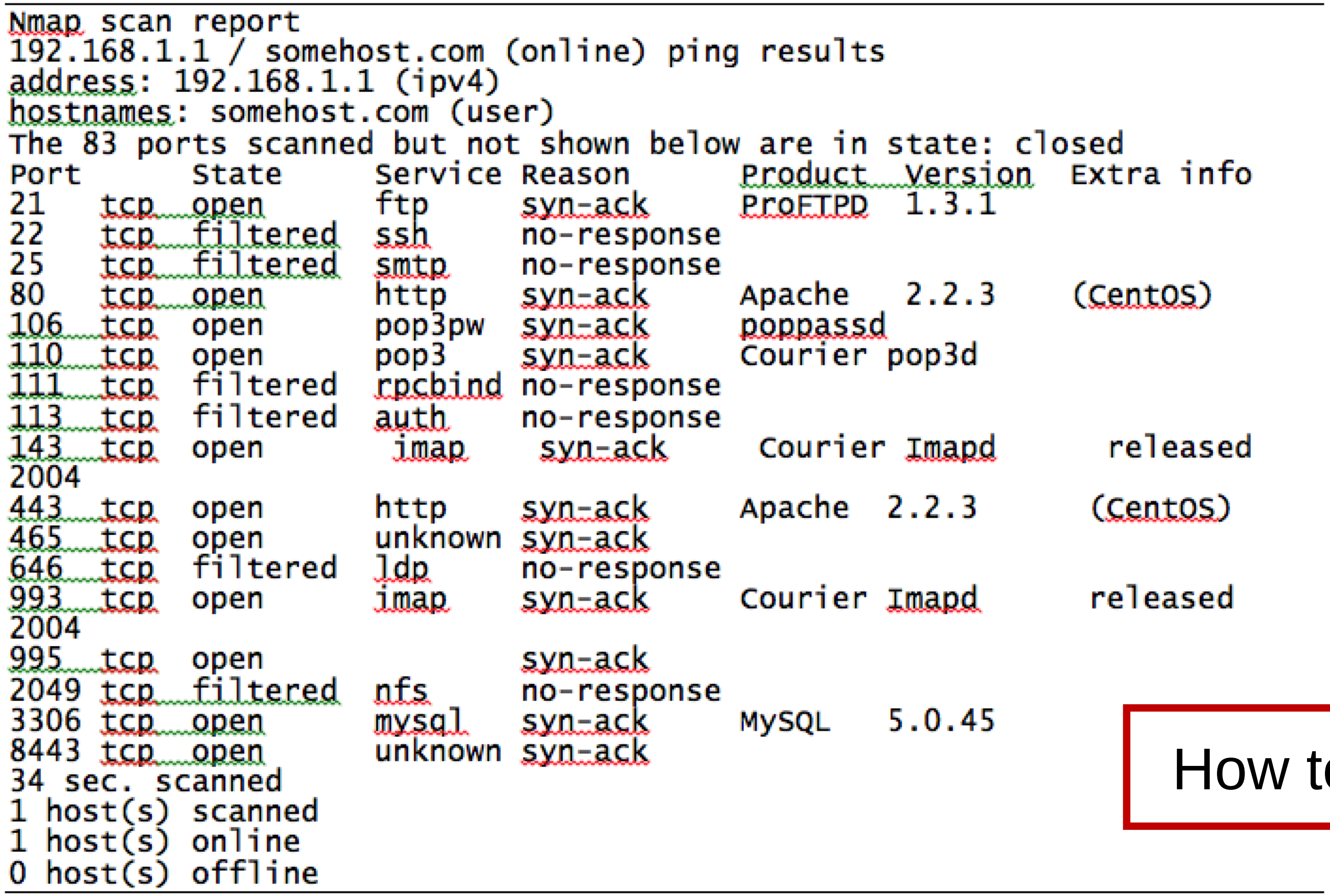
Interruption: Loss of Service

- Routing
  - Internet routing protocols are complicated, and one misconfiguration can poison the data of many routers
- Excessive demand
  - Network capacity is finite and can be exhausted; an attacker can generate enough demand to overwhelm a critical part of a network
- Component failure
  - Component failures tend to be sporadic and unpredictable, and will cause loss of service if not planned for

Reconnaissance: Port Scanning

- Port scan maps the topology and hardware and software components of a network segment
  - Reports which ports respond to queries and which of several known vulnerabilities are presented on an IP
  - Scan a small network and identify the active IPs and their connectivities
- Tools: nmap, telnet, …

Port Scanning (cond.)

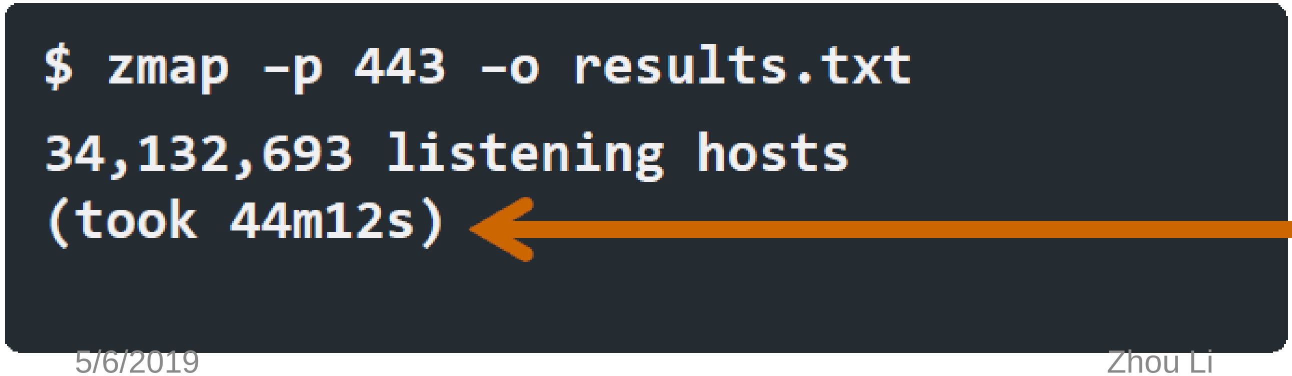


```
Nmap scan report
192.168.1.1 / somehost.com (online) ping results
address: 192.168.1.1 (ipv4)
hostnames: somehost.com (user)
The 83 ports scanned but not shown below are in state: closed
Port      State     Service Reason      Product  Version  Extra info
21   tcp  open      ftp     syn-ack     ProFTPD  1.3.1
22   tcp  filtered  ssh     no-response
25   tcp  filtered  smtp    no-response
80   tcp  open      http    syn-ack     Apache   2.2.3    (CentOS)
106  tcp  open      pop3pw  syn-ack     poppassd
110  tcp  open      pop3    syn-ack     Courier pop3d
111  tcp  filtered  rpcbind no-response
113  tcp  filtered  auth    no-response
143  tcp  open       imap    syn-ack     Courier Imapd      released
2004
443  tcp  open      http    syn-ack     Apache  2.2.3      (CentOS)
465  tcp  open      unknown syn-ack
646  tcp  filtered  ldp     no-response
993  tcp  open      imap    syn-ack     Courier Imapd      released
2004
995  tcp  open              syn-ack
2049 tcp  filtered  nfs     no-response
3306 tcp  open      mysql   syn-ack     MySQL   5.0.45
8443 tcp  open      unknown syn-ack
34 sec. scanned
1 host(s) scanned
1 host(s) online
0 host(s) offline
```

How to defend?

ZMap

- https://zmap.io/
- An open-source tool that can port scan **the entire IPv4 address space** from just one machine in under 45 minutes with 98% coverage
- With Zmap, an Internet-wide TCP SYN scan on port 443 is as easy as:



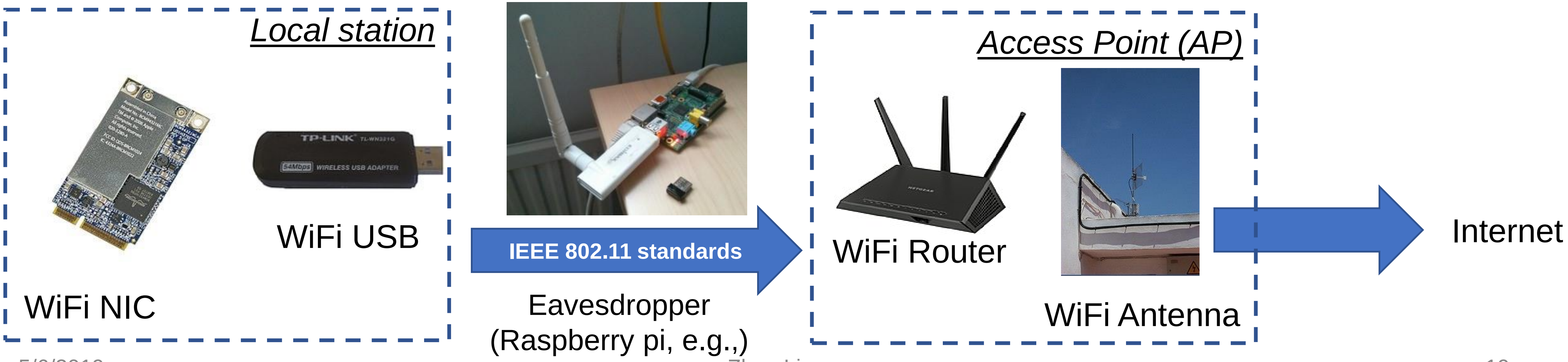
```
$ zmap -p 443 -o results.txt
34,132,693 listening hosts
(took 44m12s)
```

97% of gigabit Ethernet linespeed

Data-link layer: WiFi Security

Background about WiFi

- Data-link layer protocol (layer 2)
- Wi-Fi is technology for radio wireless local area networking of devices based on the IEEE 802.11 standards.
- Communicated in 2.4GHz radio signal band.
- The band is divided into 14 channels/subranges (often 1,6, and 11 are used)
- Wireless signal can travel up to 100 meters (300 feet) (802.11b, g)
- Wi-Fi is more vulnerable to eavesdropping than wired networks.



Local station

WiFi NIC

WiFi USB

IEEE 802.11 standards

Eavesdropper
(Raspberry pi, e.g.,)

Access Point (AP)

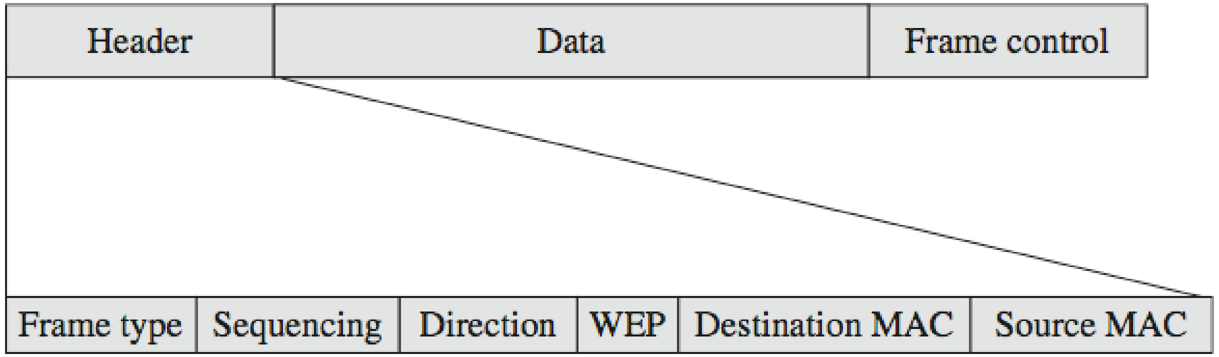
WiFi Router

WiFi Antenna

Internet

WiFi Frames

- Each WiFi data unit is a frame
  - Contains MAC header, payload (data), and FCS (frame check sequence)
  - MAC: 48-bit or 64-bit unique (?) hardware address (e.g., 01af3c4c8a21)
  - **MAC header:** frame type (control/management/data), sequencing (fragmentation & order control), direction (to or from AP), WEP (1-bit about encryption or not), up to 4 MAC addresses (sender & receiver, plus 2 optional for traffic filtering points).
  - **Payload:** 0-2304 bytes
  - **FCS:** integrity check for entire frame



Format of a WiFi frame

Management Frames

- Controlling the establishment and handling of a series of data flows
- Frame types:
  - **Beacon:** AP (Access Point) periodically sends a beacon frame to announce its presence and relay info, such as timestamp, identifier and other params.
  - **Authentication:** NIC responds to beacon with its identity (e.g., your computer responds to coffee shop’s beacon by returning MAC addr). To terminate an established connection: deauthentication frame
  - **Association request and response:** following authentication, a NIC requests AP to establish a session (NIC and AP agree on some parameters, e.g., encryption algorithms), to terminate a session: deassociation request

SSID (Service Set Identifier)

- Used by wireless device to distinguish AP
- A string of up to 32 characters (e.g., Starbucks-WiFi)
- Contained in beacon frame
- It’s not designed to be unique and private!

Question: *how do I know Starbucks-WiFi belongs to Starbucks?*