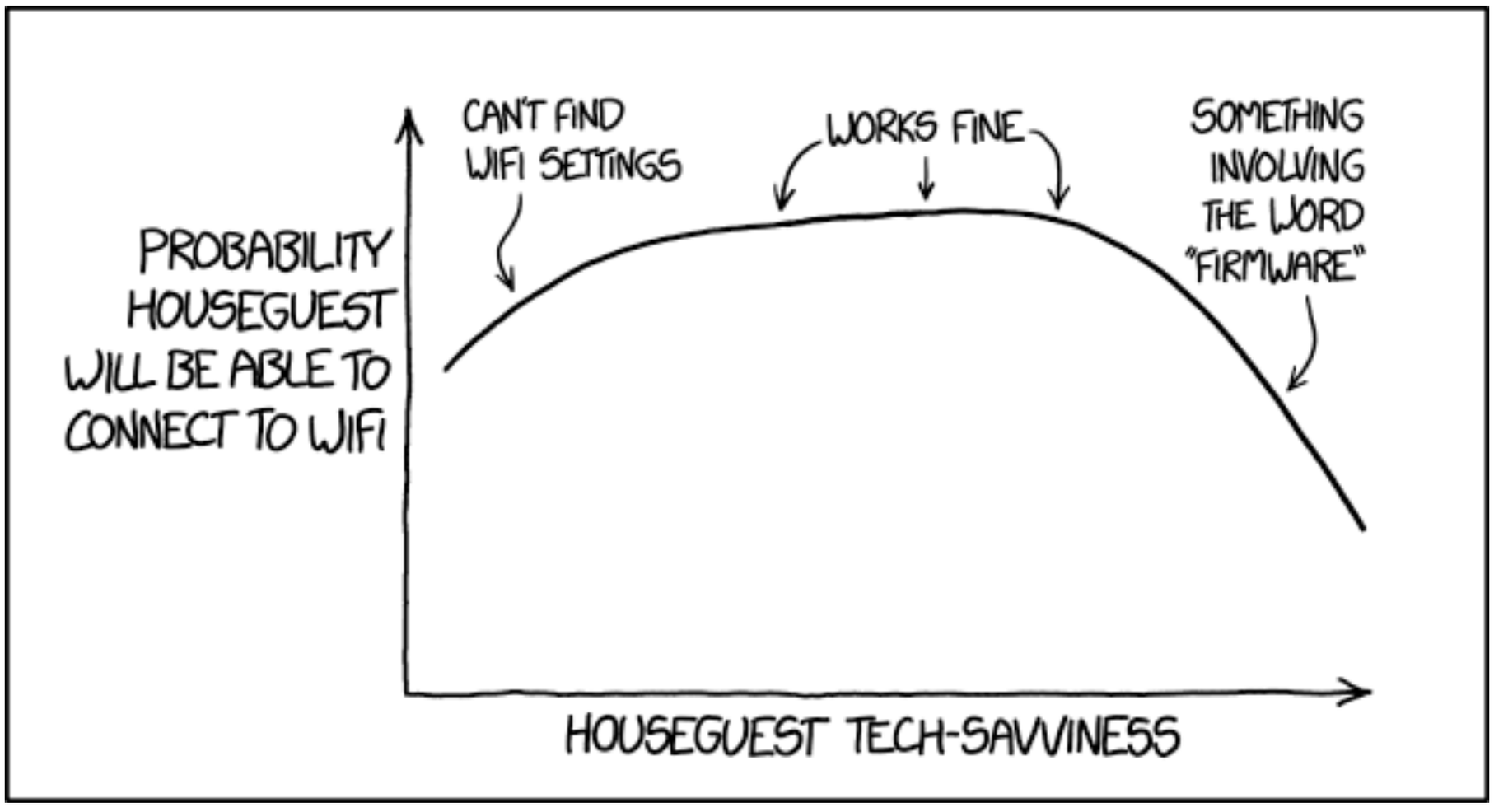
WiFi Security

February 22, 2022



Midterm Exam and Today

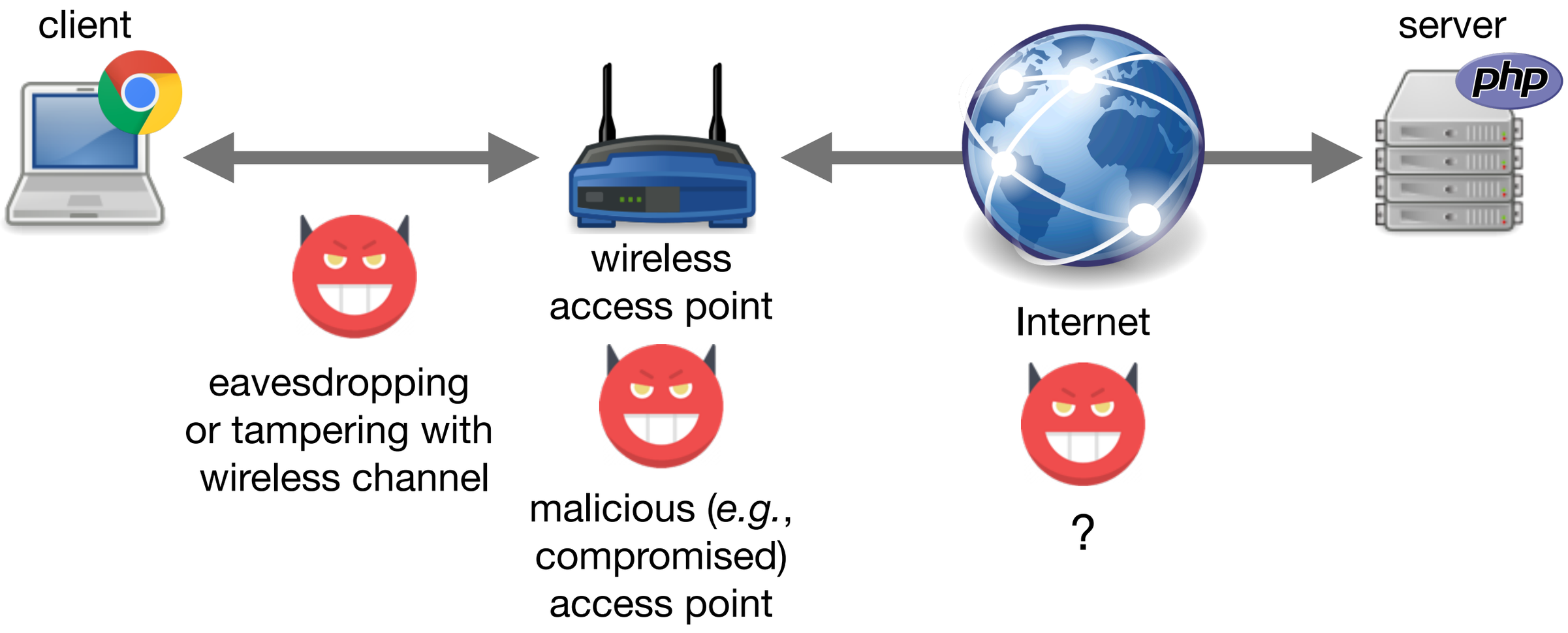
- **Midterm exam**: on **March 1st** (next Tuesday)
  - detailed list of topics and sample midterm is available on Blackboard
  - in person, during class
  - closed book, based on first five weeks of classes

- Today
  - introduction to security protocols
  - **WiFi security**: WEP, WPA, WPA2, WPA3

Feedback: `https://forms.gle/JGbNCmCsU69iWaTv8`

Security Protocols

Communication Threats in Practice

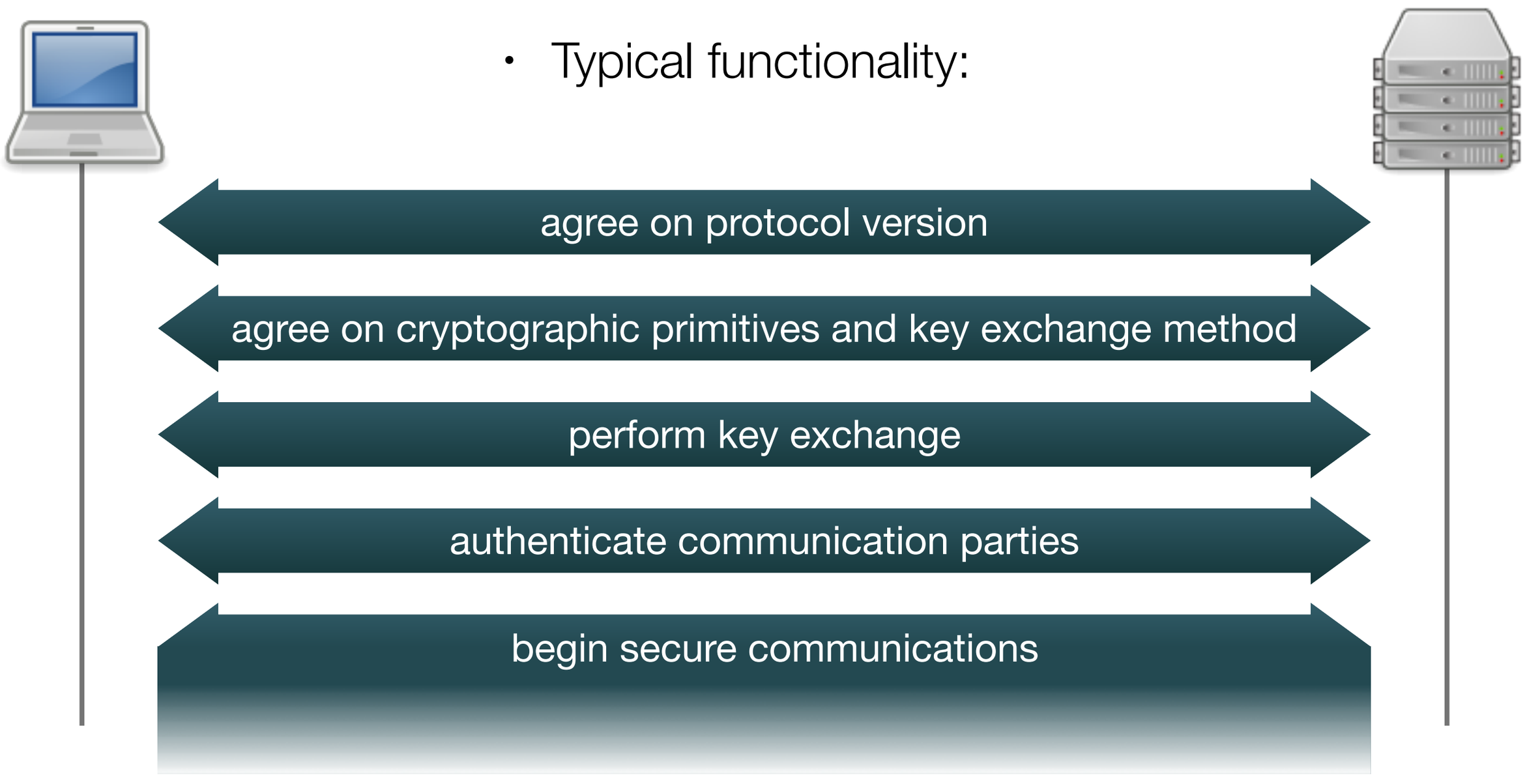


Security

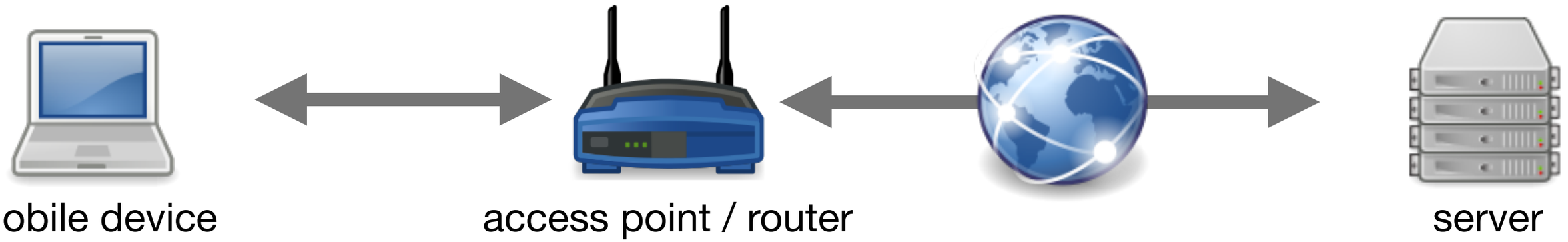
How can devices, software products, etc.
from different vendors, manufacturers, etc.
communicate with each other?

Security Protocols

- Standard security protocols specify messages, data structures, and the usage of cryptographic primitives to provide interoperability



Communication in Practice

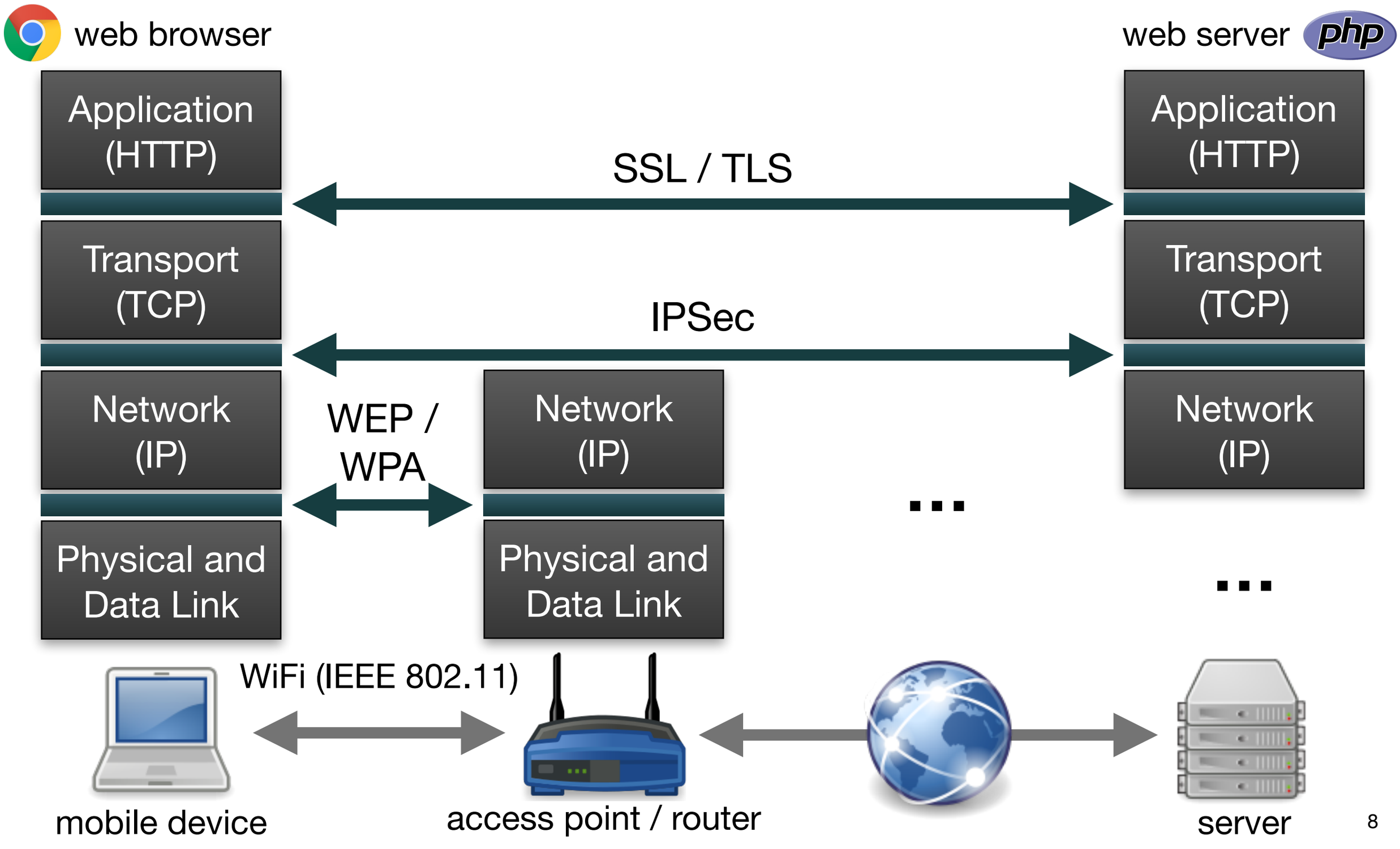


mobile device

access point / router

server

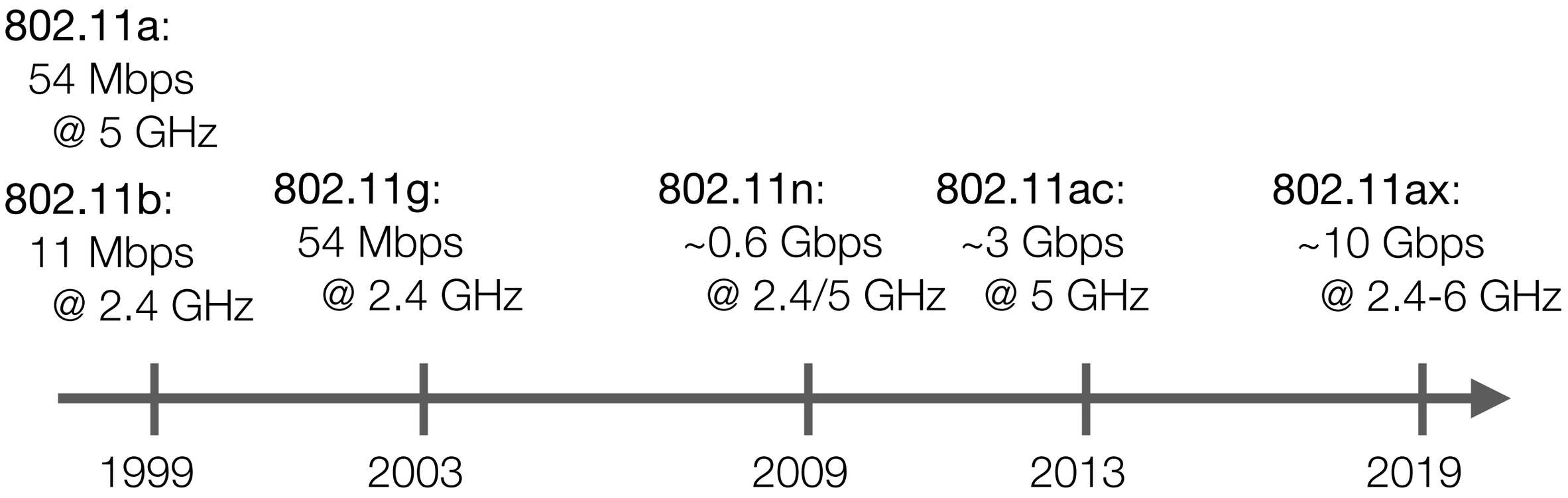
Protocol Stack in Practice



IEEE 802.11

IEEE 802.11 Standards

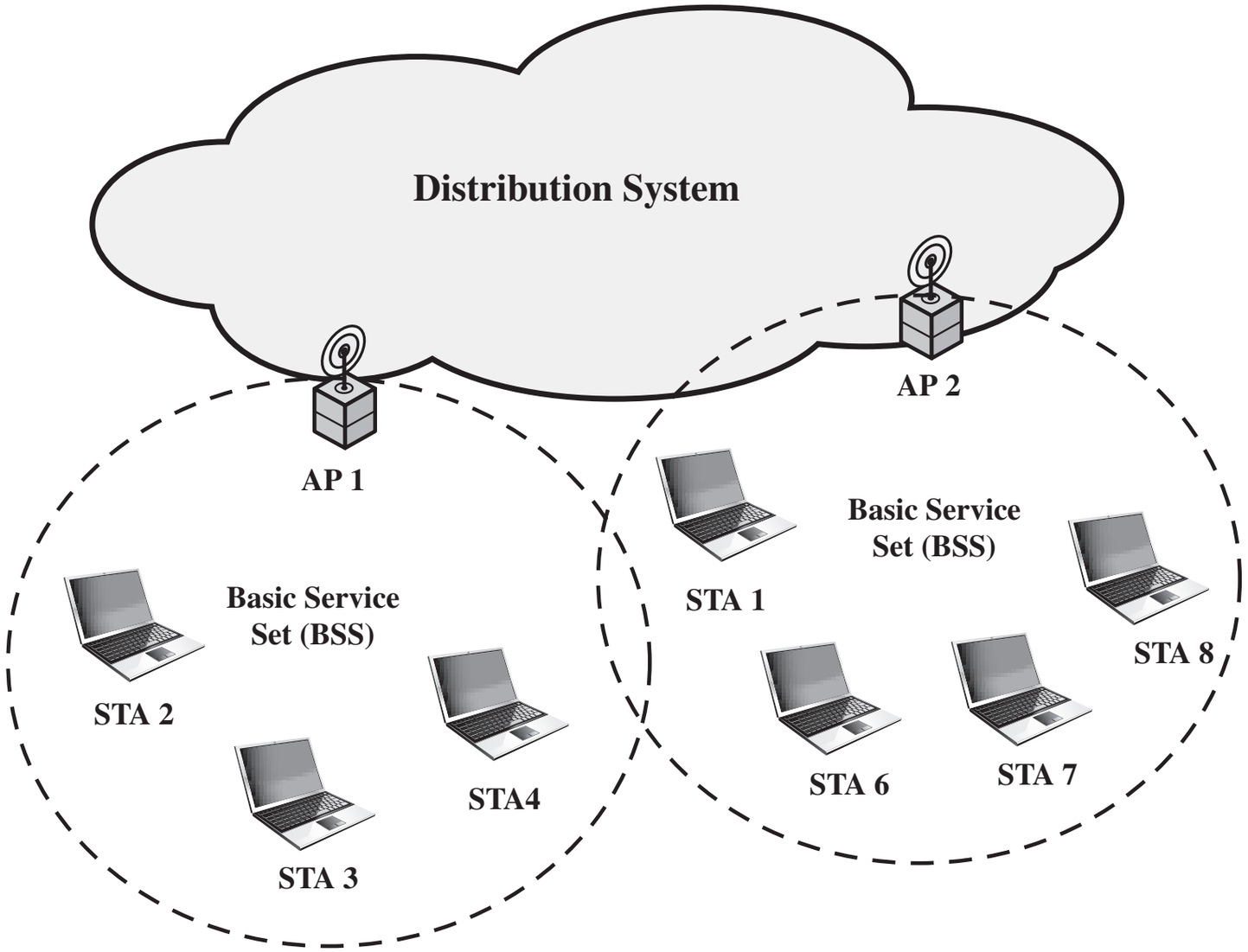
- **802.11**: set of standards for wireless local area networks (WLANs)



- **Wi-Fi** Alliance
  - non-profit organization of companies, certifies devices for interoperability
  - WiFi = WLAN based on 802.11 standard

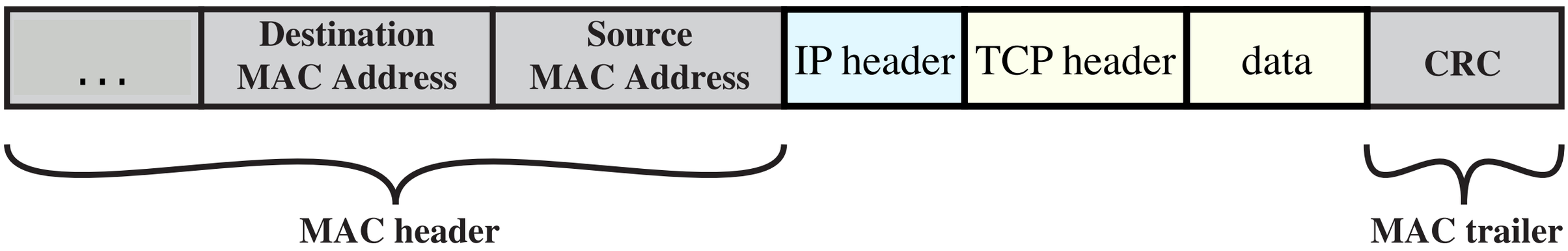
IEEE 802.11 Network Components

- **Station** (STA)
  - any device using IEEE 802.11
  - interface identified by a **MAC address**
- Basic Service Set
  - set of stations executing the same medium access control protocol
  - identified by a **service set identifier (SSID)**



- **Access Point** (AP)
  - has station functionality and provides access to the distribution system

IEEE 802 Frame



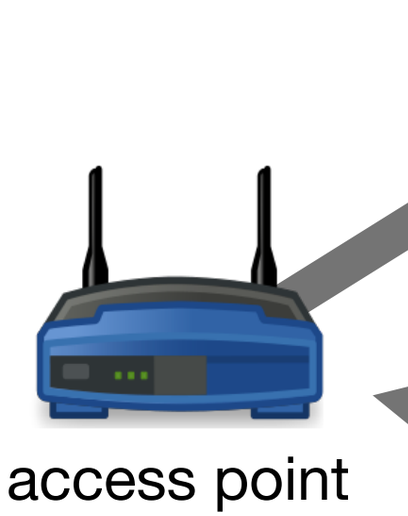
Medium Access Control (MAC) frame format:

- **Destination MAC address**: destination's physical address on the LAN
- **Source MAC address**: source's physical address on the LAN
- **MAC Service Data Unit**: data from higher layer
- **CRC**: cyclic redundancy check field, for transmission error detection

IEEE 802.11 Beacons and Association

Beacon:

- broadcast periodically to announce the WLAN
- contains information about the network, including the SSID



access point

station

- listens for beacons

1. Association Request
(contains SSID)

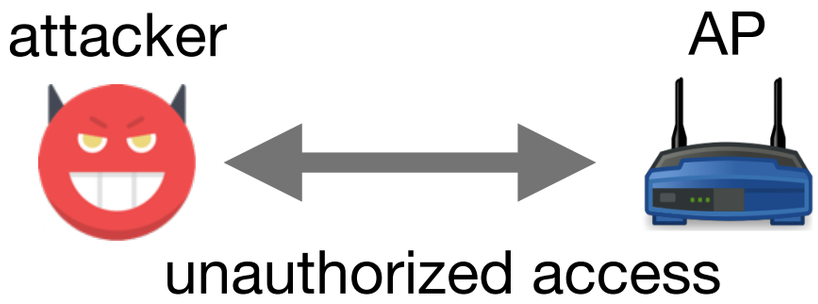
2. Association Response

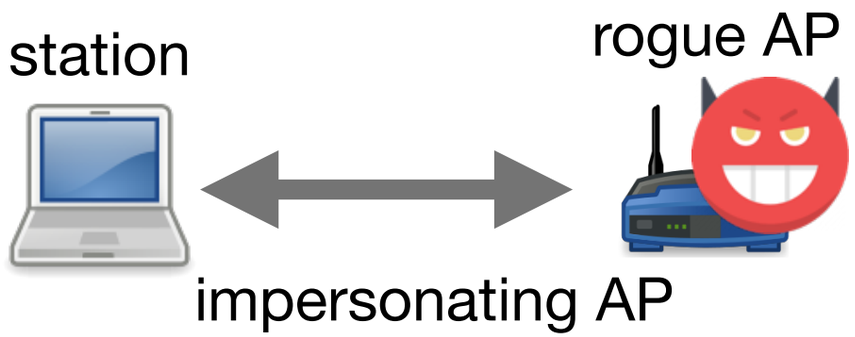
Wireless Security

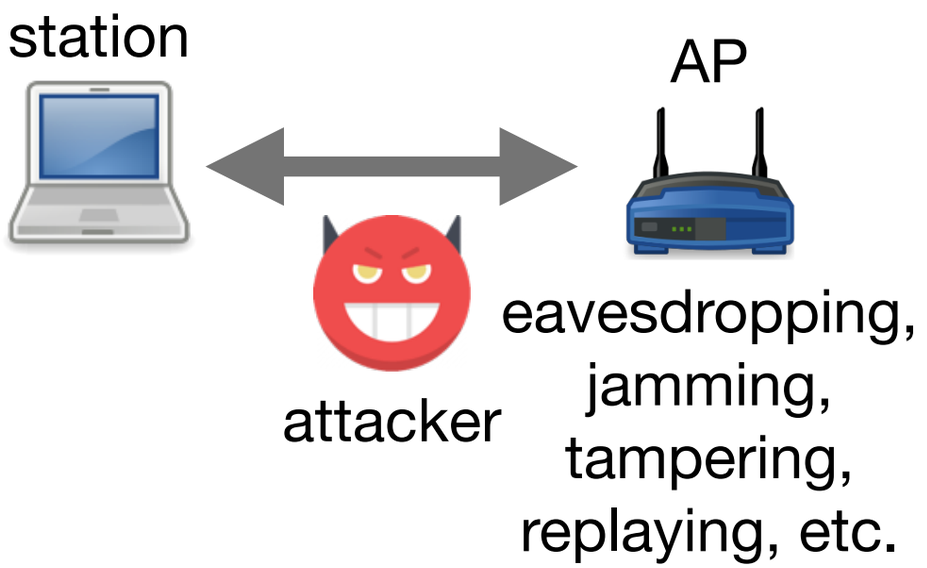
Security Challenge

Problem: no inherent physical protection

- **joining** a network does not require physical access
- radio transmissions are broadcast
  → anyone in range can **eavesdrop**
- **injecting** new messages or **replaying** old messages is possible
- **jamming** attacks against availability
- jamming and injecting messages can be combined into **tampering** attacks







Simple “Solutions” for Access Control
Hidden SSID

- Association request must contain the SSID of the network
  - by default, the AP broadcasts it periodically in the beacon
- AP may be configured to **stop announcing the SSID**
  → SSID may be be used as a “password”
- However,
  - SSID must be hard to guess
  - every authorized user must know the SSID
  - **SSID can be easily eavesdropped** whenever an authorized station connects to the network
    → does not provide any security
- Tools are available for eavesdropping (*e.g.*, AIRCRACK-NG)

Simple “Solutions” for Access Control
MAC Address Based Filtering

- AP may be configured to **allow only devices with certain MAC addresses** to connect
  - MAC addresses of all authorized devices must be registered in advance
- However,
  - **MAC address is sent in plaintext** in every packet
  - many WLAN devices allow their MAC addresses to be changed
    → attacker can easily impersonate an authorized user
- *Example*: changing MAC address of macOS

```
$ sudo ifconfig en0 ether 6c:40:aa:11:22:33
```

IEEE 802.11 Security Standards

- **WEP** (Wired Equivalent Privacy)
  - introduced in 1997 as part of the original 802.11 standard
  - shown to be insecure in 2001

- **WPA** (WiFi Protected Access)
  - introduced in 2003, as a quick fix to WEP
  - subset of draft IEEE 802.11i
- WPA-2 (IEEE 802.11i)
  - standardized in 2004
- WPA-3
  - announced in 2018
  - very similar to WPA-2

WEP

How <u>not</u> to design a security protocol…

Wired Equivalent Privacy (WEP)

Security mechanism defined in IEEE 802.11

- Goal: make WiFi **at least as secure as wired networks**
  - not a very ambitious goal, but fell short of even this goal…
- Design overview
  - security is based on a 40 or 104-bit secret key
    - WiFi “password” shared by all users
  - **confidentiality**: RC4 stream cipher
    - key is extended by a 24-bit IV, which is changed for each message
      → used as nonce to prevent key reuse problems
  - **integrity**: encrypted CRC32 (Cyclic Redundancy Check) checksum
  - **access control**: challenge-response between AP and station

WEP Design Flaws

- Authentication
  - **one-way authentication** (only for station) → AP can be impersonated
- Integrity protection
  - based on **error-detection code** (CRC32) instead of cryptographic hash
    → forging authentication tags is trivial
  - **no message replay protection**
- Key usage
  - **no session key**: long-term key used for all purposes
    (authentication, encryption, integrity protection)
  - **short nonce** (i.e., 24-bit IV) → danger of key reuse for stream cipher
    - busy network with 1000 packets per second reuses in less than 5 hours

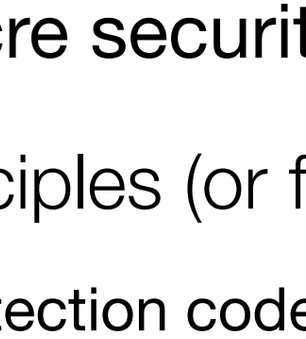
Fluhrer-Mantin-Shamir Attack (2001)

- Attacker knows the first three bytes of RC4 key (i.e., the 24-bit IV)
- Due to RC4 weaknesses, attacker can guess the 4th key byte (i.e., 1st secret byte) correctly with probability ≈ **0.58%** using a single ciphertext-plaintext pair
  - random guess should be correct only with probability = 1 / 256 ≈ 0.39%
- With enough ciphertext-plaintext pairs, attacker can discover the 4th key byte (with probability ≈ 100%)
- Then, the attacker can discover the 5th, 6th, … bytes using the same approach (i.e., 2nd, 3rd, … secret bytes)
- In practice, WEP keys can be broken in a matter of minutes (or less)
  → WEP is **not secure**
  - easy to use tools for breaking WEP are available

Lessons Learned from WEP

- Aiming for mediocre security will likely result in no security
- Follow design principles (or face the consequences)
  - do not use error-detection codes for message authentication
  - use session keys for data encryption and authentication
  - ...
- Do not use WEP
- Problem:

  WEP needed to be replaced very quickly in 2001



- existing devices (*e.g.*, access points, wireless interface cards) had **hardware support only for WEP** (*e.g.*, for RC4)
- many networking devices had **low computational performance**

IEEE 802.11 Security Standards

- **WEP** (Wired Equivalent Privacy)
  - introduced in 1997 as part of the original 802.11 standard
  - shown to be insecure in 2001
- **WPA** (WiFi Protected Access)
  - introduced in 2003, as a quick fix to WEP
  - subset of draft IEEE 802.11i
- **WPA-2** (IEEE 802.11i)
  - standardized in 2004

WiFi Protected Access (WPA)

Standard: 802.11i TKIP (Temporal Key Integrity Protocol)

- Design goals:
  fix the flaws of WEP and be **compatible with legacy hardware**
- Overview
  - key usage: **session key** is established during a secure two-way authentication
  - confidentiality: RC4 encryption, but with **48-bit IV**, which is **mixed thoroughly** with the session key and source MAC address
    - prevents key reuse and the Fluhrer-Mantin-Shamir attack
  - integrity: 64-bit message integrity codes computed using Michael, which is **computationally very efficient** but provides only ~20 bits of effective security
    - after wrong code, station is banned for a minute and needs to re-authenticate
- Deprecated in later revisions of the standard

Next lecture:

Midterm Preparation