NYU TANDON SCHOOL OF ENGINEERING

# *Network Security*

## 802.11 Security

Phillip Mak
pmak@nyu.edu

# Objectives

- Overview of Wireless 802.11
- Describe how WEP is flawed and work out various methods to attack it
- Understand how WPA and WPA2 improves upon WEP
- Describe methods to attack any wireless network
- Understand Wi-Fi-Protected Setup

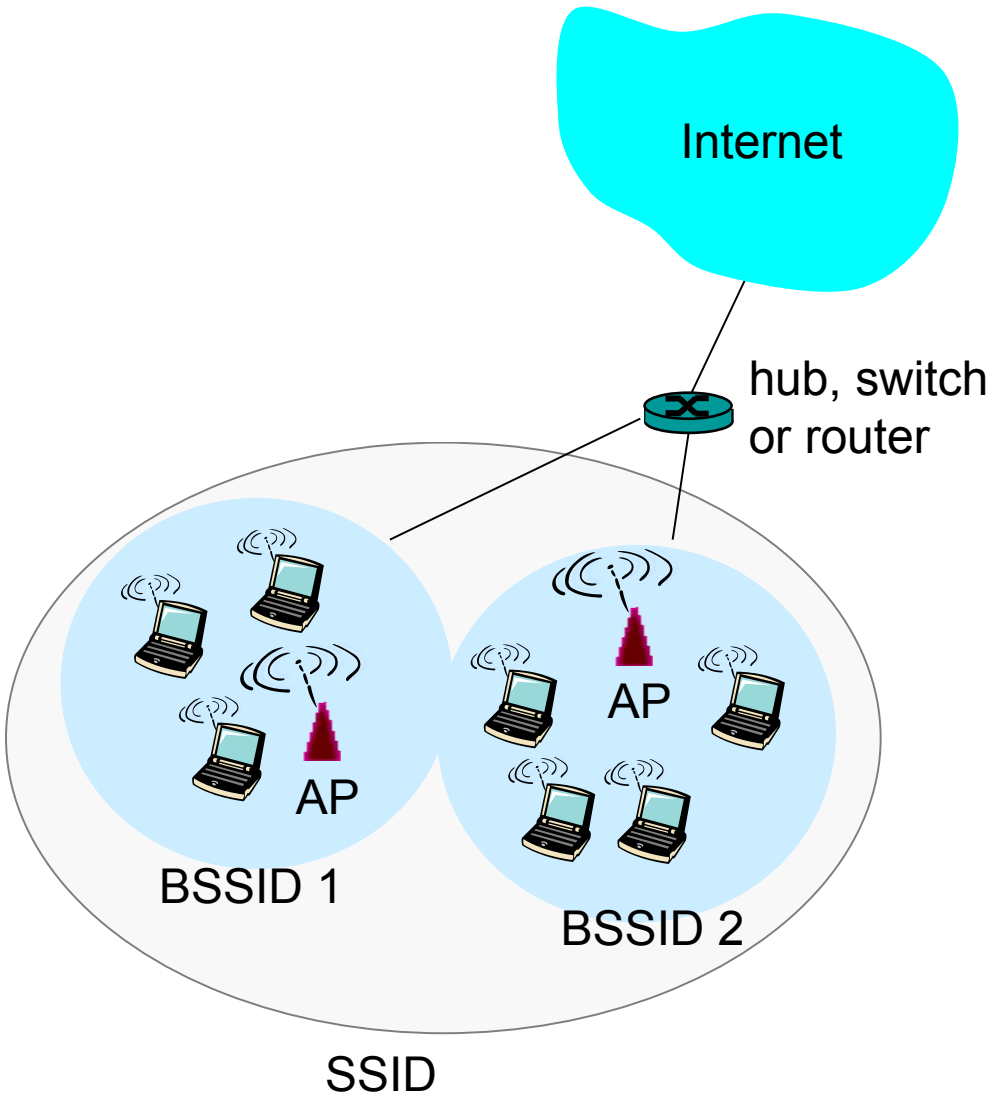
# IEEE 802.11 Wireless LAN

- 802.11b (Wi-Fi 1)
- 2.4-2.495 GHz unlicensed radio spectrum
- up to 11 Mbps
- direct sequence spread spectrum (DSSS) in physical layer: all hosts use same chipping code
- Deprecated in 2004
- 802.11a (Wi-Fi 2)
- 5 GHz range (4915-5815MHz)
- up to 54 Mbps
- Physical layer: orthogonal frequency division multiplexing (OFDM)
  - Used for encoding data on multiple frequencies
- 802.11g (Wi-Fi 3)
- 2.4-2.495 GHz range
- up to 54 Mbps
- 802.11n (Wi-Fi 4)
- 2.4-2.495 GHz & 4.915-5.825 GHz
- 4x40 MHz channel size
- up to 600 Mbps
- 802.11ac (Wi-Fi 5)
- 4.915-5.825 GHz
- 8x160 MHz channel size
- up to 3.5 Gbps
- 802.11ax (Wi-Fi 6)
- 2.4-2.495 GHz & 4.915-5.825 GHz
- up to 9.6 Gbps
- WPA3
- 802.11ax (Wi-Fi 6E)
- With 6GHz (5.925–7.125 GHz)

- Next: 802.11be (Wi-Fi 7)

- **All have collusion avoidance using CSMA/CA**
- **All have base-station and ad-hoc versions**
- **All allow for reducing bit rate for longer range**

# 802.11 LAN architecture

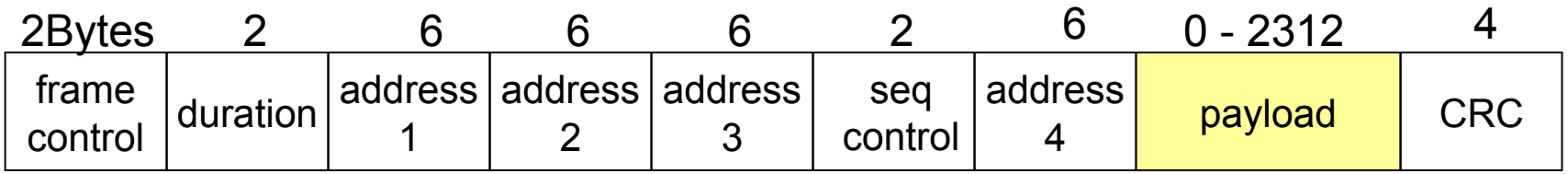



- wireless host communicates with base station
  - Access Point (AP) = base station
  - Basic Service Set (BSS) is the set of AP and STAs communicating with each other
  - All AP/BSS are named by their BSSID, or MAC Address
- Infrastructure mode contains:
  - Stations (STA): Hosts
  - Access Points (AP): Base Stations
- ad hoc mode
  - Hosts only
  - No AP

# Channels, beacon frames & association

- 802.11b/g/n
  - 2.4GHz-2.495GHz spectrum divided into 13 channels (14 in Japan) at different frequencies; 3 non-overlapping (4 in Japan)
  - AP admin chooses frequency for AP
  - Interference possible: channel can be same as that chosen by neighboring AP! 2.4 GHz is also popular for other appliances such as wireless telephones and microwaves
- AP regularly sends beacon frame
  - Includes SSID (Network Name), BSSID (AP MAC), beacon interval (often 0.1 sec)
- host: must associate with an AP
  - scans channels, listening for beacon frames or sends a probe request
  - selects AP to authenticate and associate with
  - Authentication may be Open, WEP, WPA, WPA2
  - Association is to join the network
  - After joining, host will typically run DHCP to get IP address in SSID or Network subnet
  - Host will keep IP if it travels from one AP to another within the same SSID/Network

# 802.11 frame: addressing



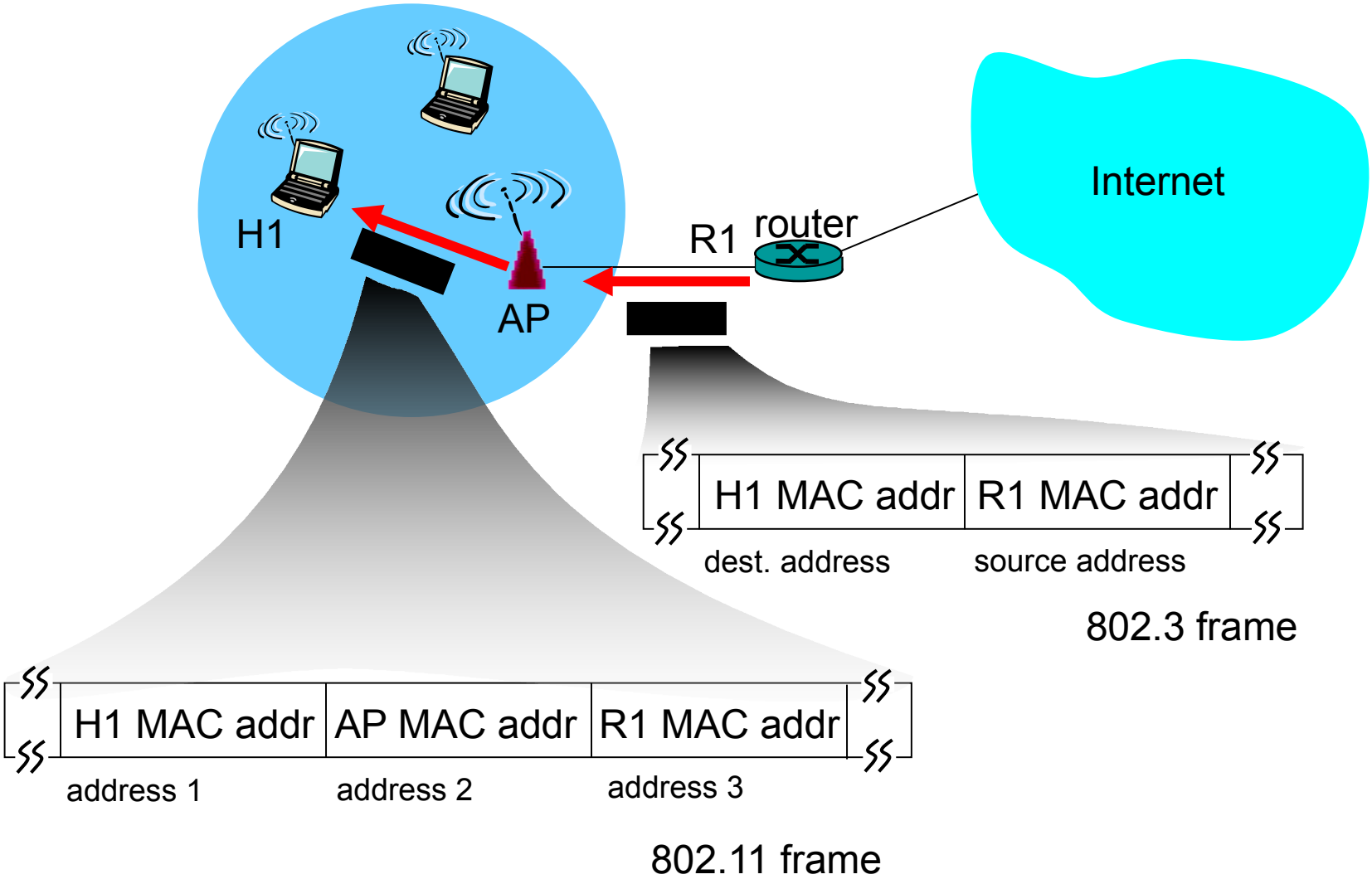

Address 1: Destination. MAC address of wireless host or AP to receive this frame

Address 2: Source. MAC address of wireless host or AP transmitting this frame

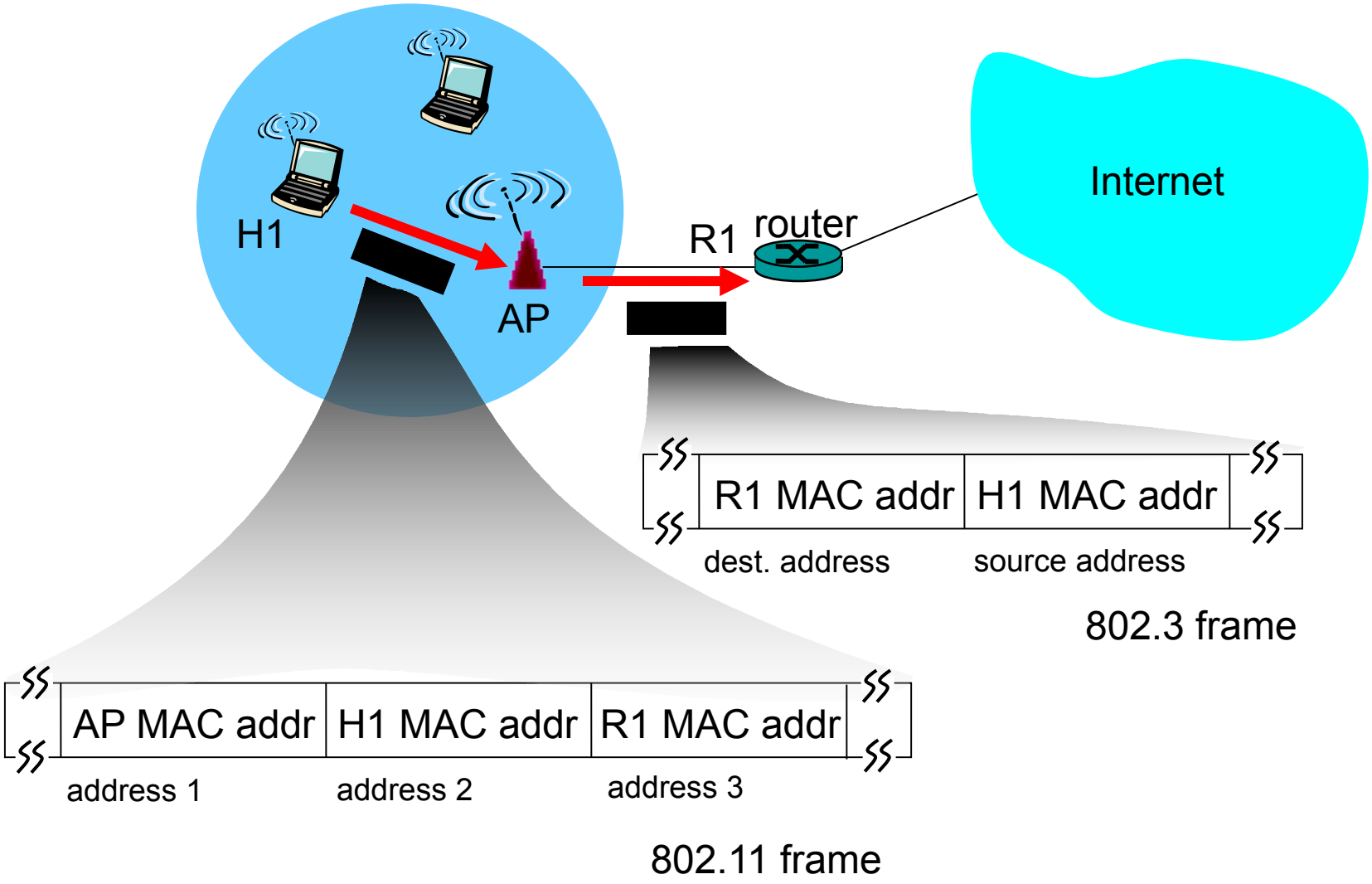
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

# 802.11 frame: addressing to STA



# 802.11 frame: addressing to AP



# 802.11 frame (more)

frame:

| 2 Bytes | 2 | 6 | 6 | 6 | 2 | 6 | 0 - 2312 | 4 |
|---|---|---|---|---|---|---|---|---|
| frame control | duration | address 1 | address 2 | address 3 | seq control | address 4 | payload | CRC |

| 2 Bits | 2 | 4 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|
| Protocol version | Type | Subtype | To AP | From AP | More frag | Retry | Power mgt | More data | WEP | Rsvd |

*frame control field expanded*

- Protocol version: Always zero
- Type/subtype distinguishes beacon, association, ACK, RTS, CTS, etc frames.
- To/From AP defines meaning of address fields
- 802.11 allows for fragmentation at the link layer but is almost only ever used during an attack since 802.3 (Ethernet) frames are smaller
- Retry identifies retransmitted frames (e.g., when ACK lost)
- 802.11 allows stations to enter sleep mode
- WEP = 1 if WEP encryption is used

# 802.11 Sniffing

- Requires wireless card that supports raw monitoring mode (rfmon)
  - Grabs all frames including management frames
- Tools:
  - There are many. Dump packets into Wireshark; interfaces with GPS devices, storing physical location
- Access control lists based on MAC addresses
  - Do they work?
    - Attacker sniffs channel, obtains valid MAC address
    - Attacker modifies its MAC address to valid address
- DEFCON Wi-Fi Shootout
  - Read Wi-Fi traffic from 125 miles away
  - They had to adjust for the curvature of the earth
  - FCC max allowable transmit powers are 1watt indoors, 4 watt outside

# Sniffing Encrypted 802.11 traffic

Suppose:

- Traffic encrypted with symmetric crypto
- Attacker can sniff but can't break crypto

Information is still leaked:

- SSID, Mac addresses
- Manufacturers of cards from MAC addrs
- Count # of devices
- Management frames are sent in the clear
- 802.11w protects management frames, but is not widely implemented

- Traffic analysis reveals:

-Size of packets

-Timing of messages

-Determine apps being used

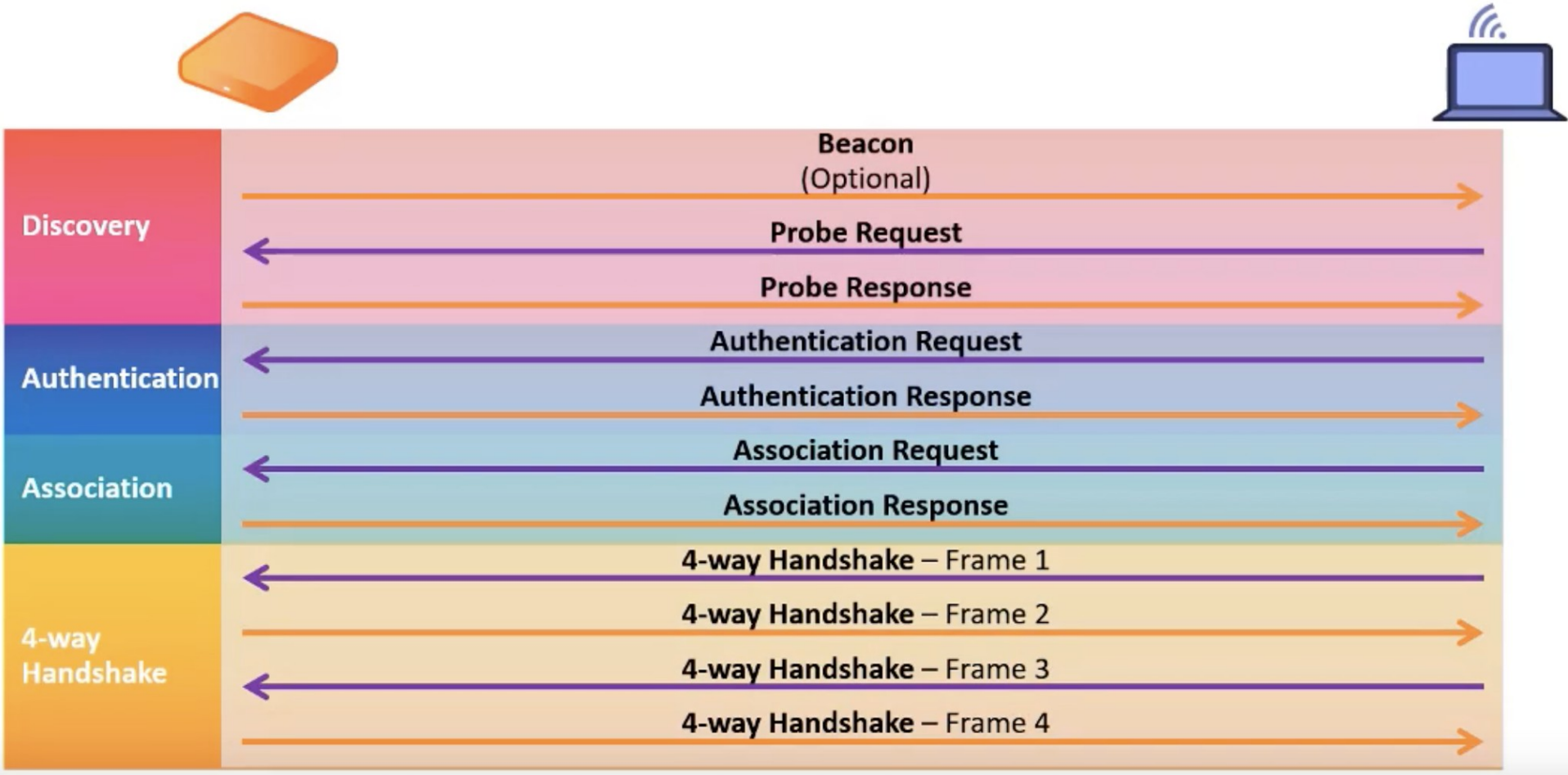
- But cannot see anything really useful
- Attacker needs the keys!

# MAC Address Randomization

- As MAC Addresses are sent in the clear, MAC Address Randomization is used as protection from tracking
- Supported by most operating systems
  - iOS 14, Windows 10, Android 10
  - Not MacOS

- Network service considerations
  - Wi-Fi ACL using MAC Addresses
  - DHCP Leases
  - Network logs

# Client Association

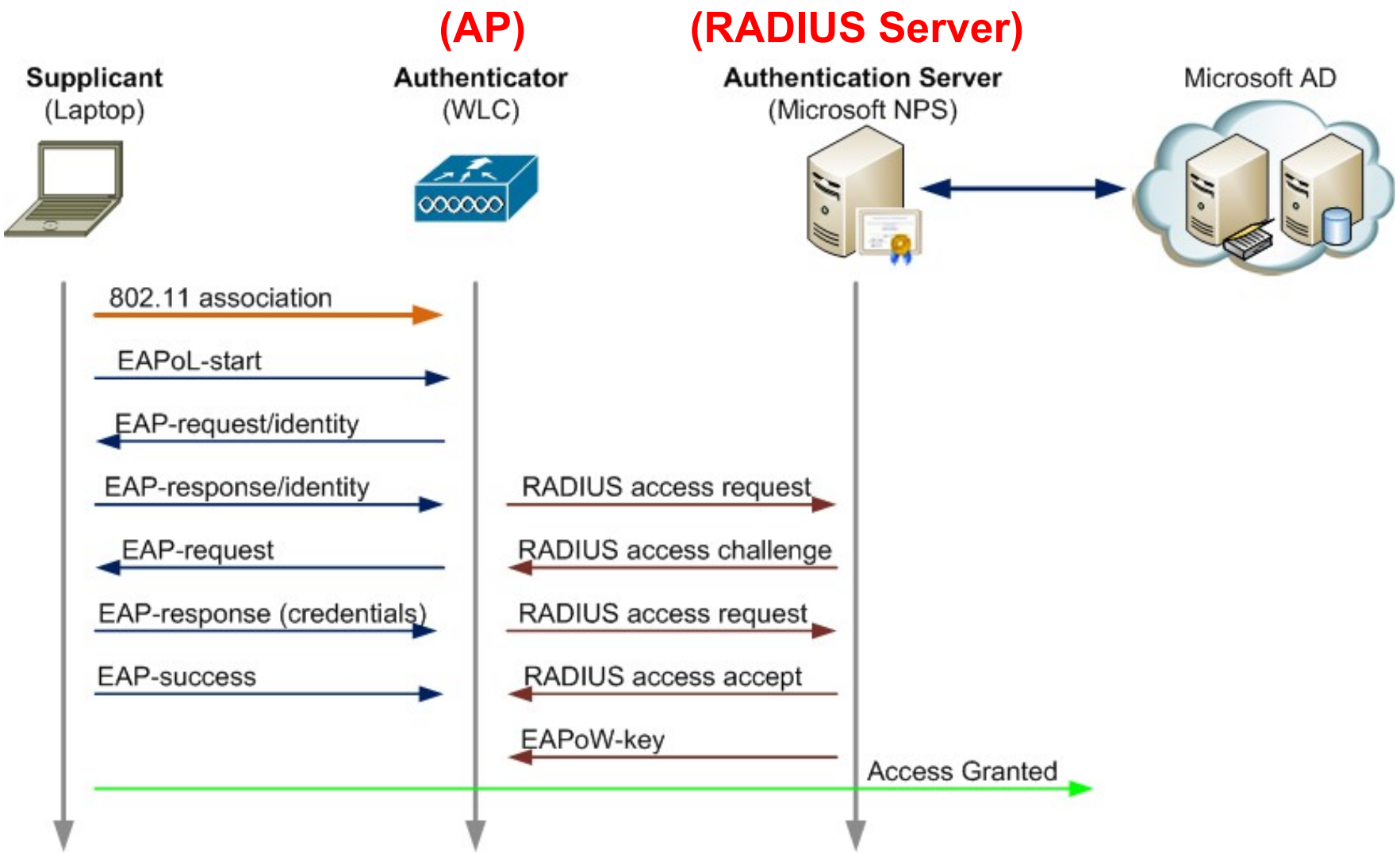



Source: Ruckus Wireless

# Client Association

- In WPA (1/2/3), there are two ways to associate:
  - Personal Mode (Pre-shared Key)
    - WPA1/WPA2 – pre-shared keys susceptible to brute force attacks
    - WPA3 – cannot perform an offline brute-force attack
  - Enterprise Mode (various methods)

# Client Association – 802.1x (Enterprise)



# Wireless Security Protocols

- WEP
- WPA
- WPA2
- WPA3

# Attacks on Pre-Shared Keys (PSK)

- Attacker can get keys from disgruntled employee or sloppy administration.
- Possible solution: put key in hardware or software & don't make key visible to humans.
- Problems:
- Attacker gets access to equipment with key
- With good technical skills, attacker can extract key
- Ex: large corporation puts key in flash memory of all its devices
- Someone clever extracts key, publishes it on Web, destroying corporate security solution

# WEP Design Goals

- Symmetric key crypto
  - Confidentiality
  - Station authorization
  - Data integrity
- Self synchronizing: each packet separately encrypted
  - Given encrypted packet and key, can decrypt; can continue to decrypt packets when preceding packet was lost
  - Unlike Cipher Block Chaining (CBC) in block ciphers
- Efficient
  - Can be implemented in hardware or software
  - Older APs implemented WEP in hardware

# WEP is flawed. Summary of flaws

One common shared key

- If any device is stolen or compromised, must change shared key in all devices
- No key distribution mechanism
- Infeasible for large organization as approach doesn't scale

Crypto is flawed

- Early 2001: Integrity and authentication attacks published
- August 2001 (weak-key attack): can deduce RC4 key after observing several million packets
- AirSnort application allows casual user to decrypt WEP traffic

Crypto problems

- 24 bit IV to short
- Same key for encryption and message integrity
- ICV flawed, does not prevent adversarial modification of intercepted packets
- Cryptanalytic attack allows eavesdroppers to learn key after observing several millions of packets

# IEEE 802.11i draft - WPA

- Much stronger encryption
  - TKIP (temporal key integrity protocol)
  - Intended for compatibility with existing WEP Hardware
    - Still uses RC4 stream cipher
  - Depreciated in 2012
- Extensible set of authentication mechanisms
  - Employs 802.1X authentication
- Key distribution mechanism
  - Typically public key cryptography
  - RADIUS authentication server
    - distributes different keys to each user
    - also there's a less secure pre-shared key mode
- WPA: Wi-Fi Protected Access
  - Pre-standard subset of 802.11i

# IEEE 802.11i WPA2

- Non-draft version of 802.11i is called WPA2
- Strongest encryption to date
- Uses AES, strong block cipher
- Longer key, 4-way handshake between STA and AP
  - Both AP and STA are authenticated
- No known weaknesses with the algorithm
  - Aside from bruteforcing passwords
- Pre-Shared Key is still vulnerable to weak passphrase dictionary attacks and stolen client

# IEEE 802.11w – Protected Management Frames (PMF)

- Management frames were still unencrypted after WPA2 in 2004
- 802.11w ratified in 2009
- 2014: Implemented in Linux and BSD drivers used by some wireless cards. Also implemented in Windows 8. Compatibility issues can exist with older clients (Windows 7, older APs)
- Mitigates an attacker from injecting malformed management frames into the network and causing a self-DOS
- Protects:
  - Deauthentcation, Disassociation
  - Authentication handshake frames
  - QoS (802.11e) frames

# Securing 802.11

- Use WPA2-AES with a strong passphrase
  - Better yet, use a RADIUS server
- Disable backwards compatibility with WEP and TKIP
- Protect the physical network
- Implement a robust PKI and EAP implementation
  - TTLS, PEAP-EAP-TLS, EAP-FAST
- Update client trusted certificates, do not use OS defaults
- Run latest vendor firmware

# WPA3 Security Improvements

- Perfect Forward Secrecy
- Protect Managements Frames
- No more offline dictionary attacks on passphase
- “Wi-Fi” Easy Connect – improved Wi-Fi Protected Setup