802.11 Security: WPA/WPA2 Cracking

Constantinos Kolias

George Mason University

kkolias@gmu.edu

Wireless Communications

- Transmission of data without the use of wires
  - Few cm to several km
- Modulation of radio waves
  - **modulation** is the process of varying one or more properties of a periodic waveform
  - with a **modulating** signal that typically contains information
- Federal Communications Commission (FCC) regulates the use of the radio specturm
  - 9kHz to 300Ghz
  - https://en.wikipedia.org/wiki/Radio_spectrum
- Parts of the radio spectrum are allocated for different applications
  - Some parts are sold or licensed to operators
  - Some parts are free

Advantages & Disadvantages

- Makes communication possible where cables don’t reach
- Convenience

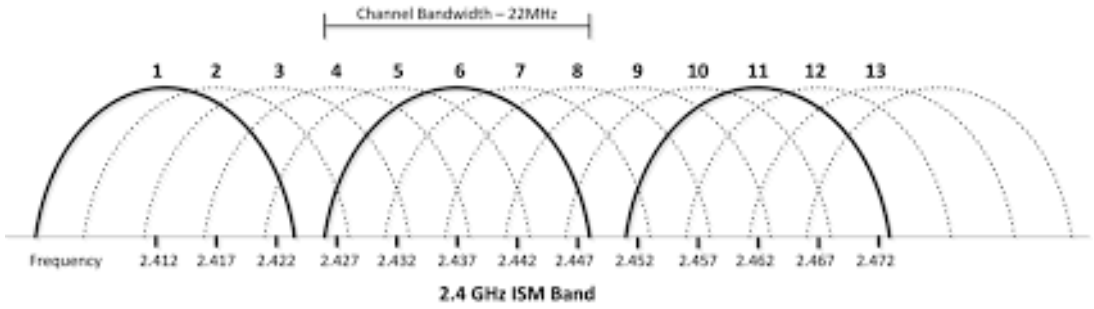
- The air medium is open to everyone
- The boundaries of a transmission cannot be confined

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



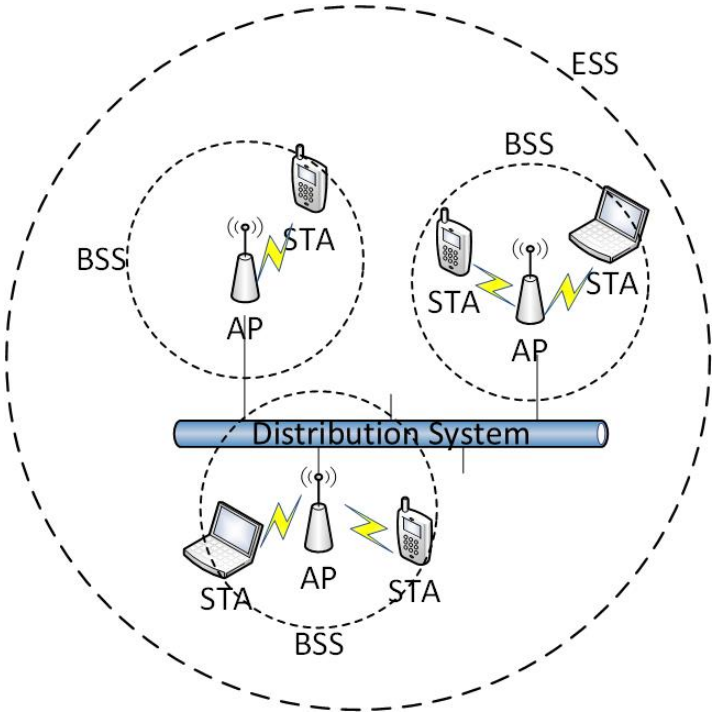
- The equipment can be set in only one channel at a time
- Each country has its own rules
  - Allowed bandwidth
  - Allowed power levels
- Stronger signal is preferred

Modes of Operation

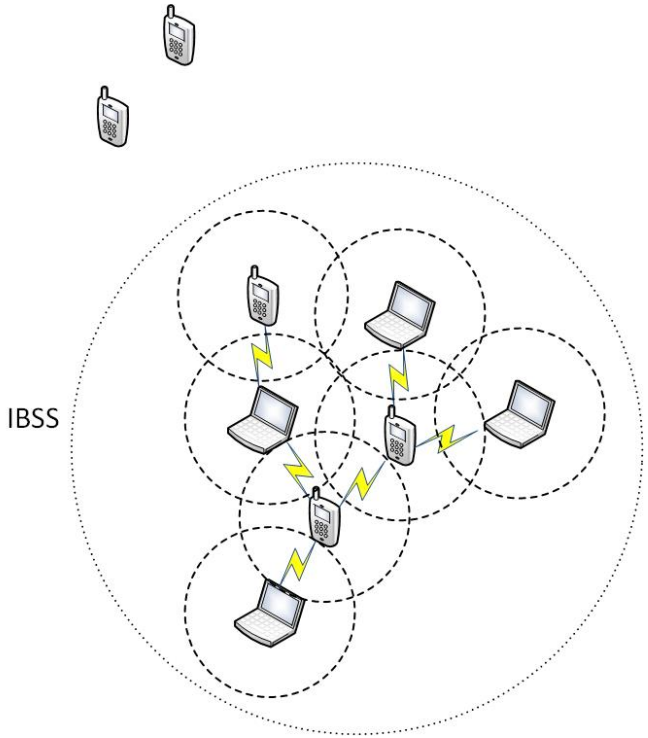
- Master
  - Acts as an AP
- Managed
  - Acts as a client, the default mode
- Ad Hoc
  - No AP, direct communication, no multi-hop
- Mesh
  - No AP, direct communication, multi-hop
- Repeater
  - Repeats incoming signals
- Promiscuous
  - Monitor all traffic of a network, requires association
- Monitor
  - Monitor all traffic, no association required

Deployment Architectures

Infrastructure

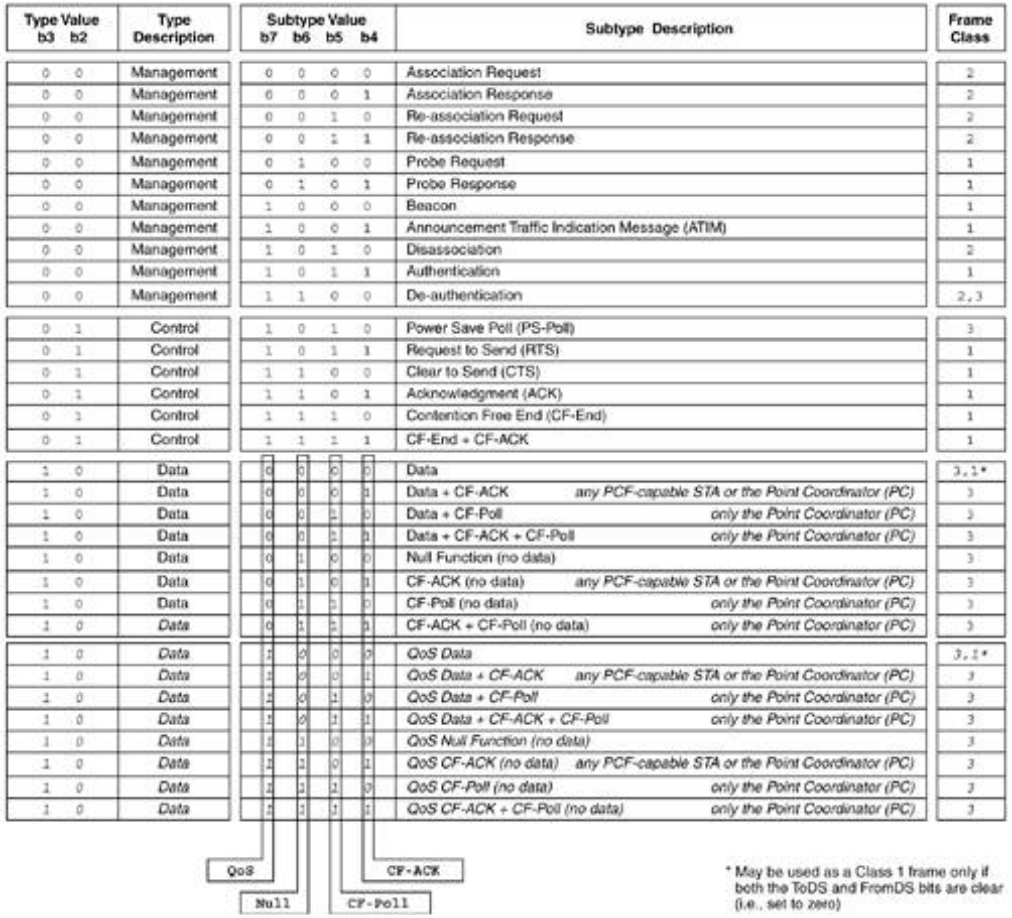


P2P/Ad-hoc



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

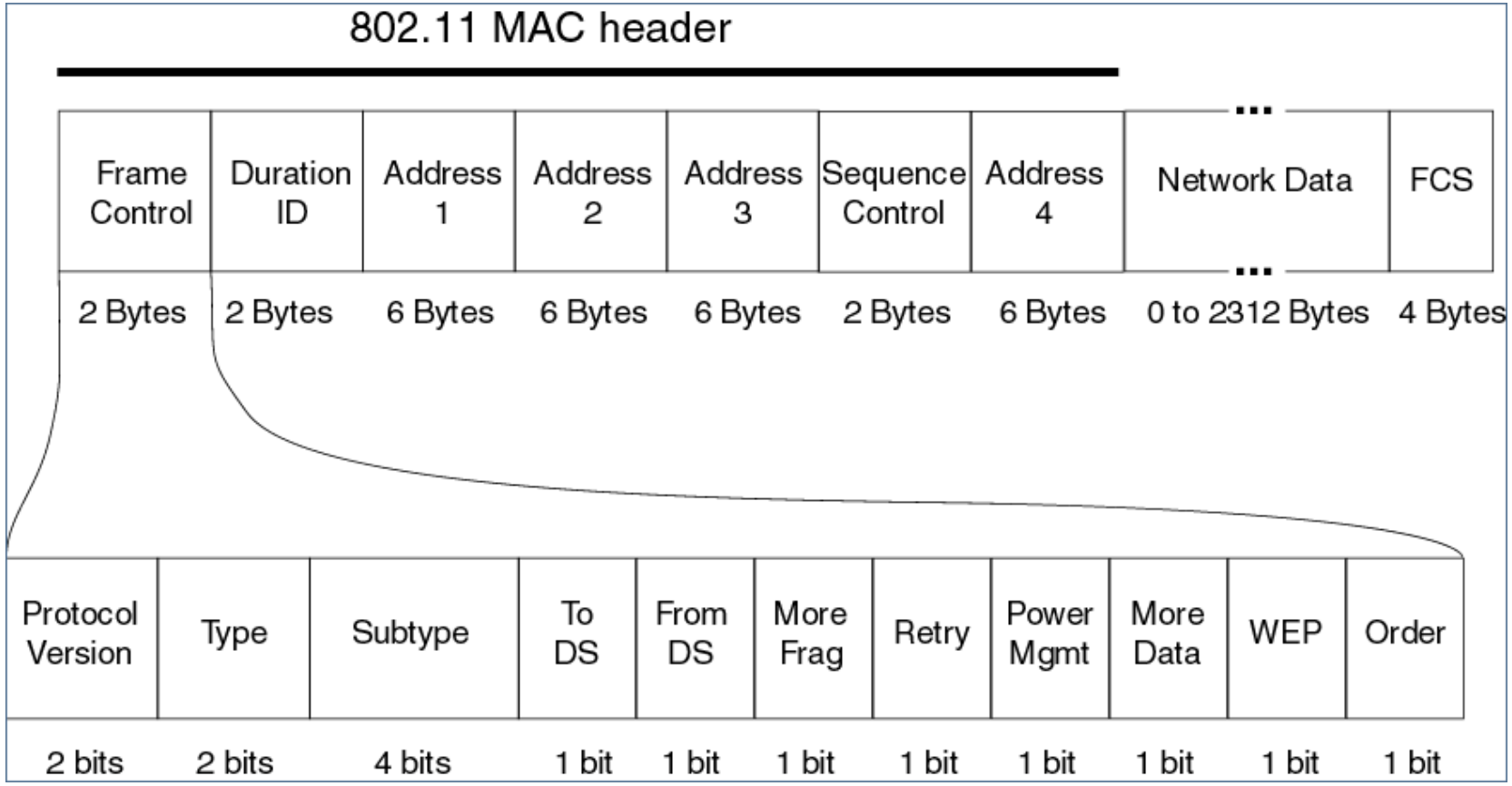


Type Value b3 b2	Type Description	Subtype Value b7 b6 b5 b4	Subtype Description	Frame Class
0 0	Management	0 0 0 0	Association Request	2
0 0	Management	0 0 0 1	Association Response	2
0 0	Management	0 0 1 0	Re-association Request	2
0 0	Management	0 0 1 1	Re-association Response	2
0 0	Management	0 1 0 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

QoS
Null
CF-ACK
CF-Poll

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

Introduction

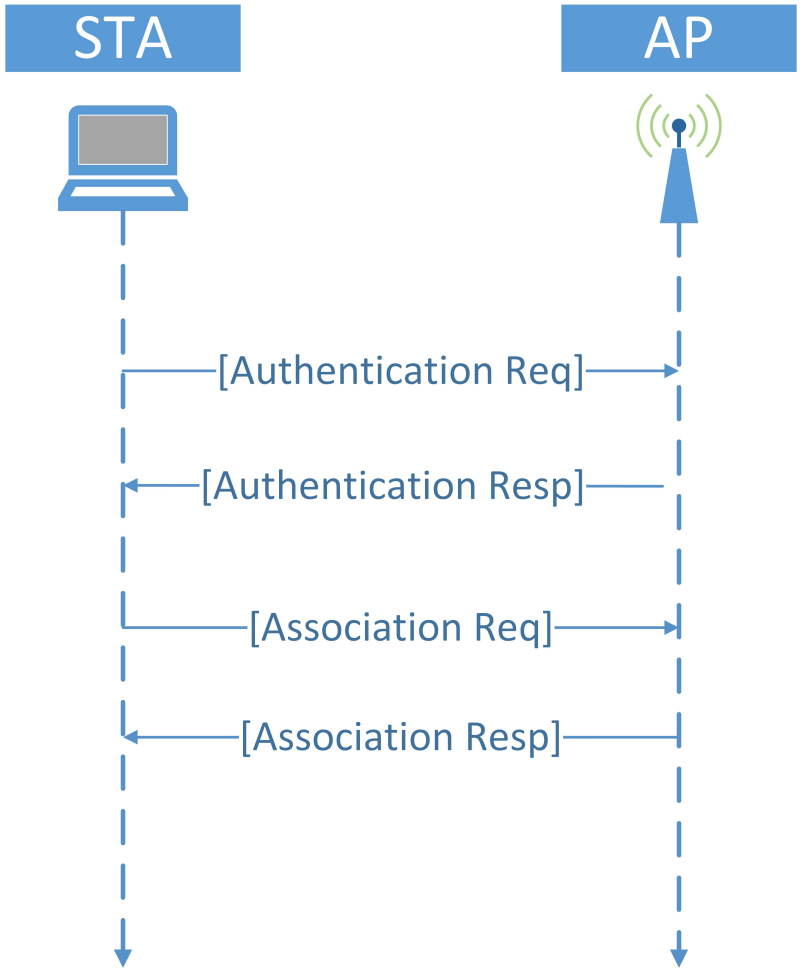


Beaconing

- The AP advertise their presence
- Once every 100ms
- They transmit a message of type Beacon
  - It contains the name of the network (SSID)
  - Capabilities

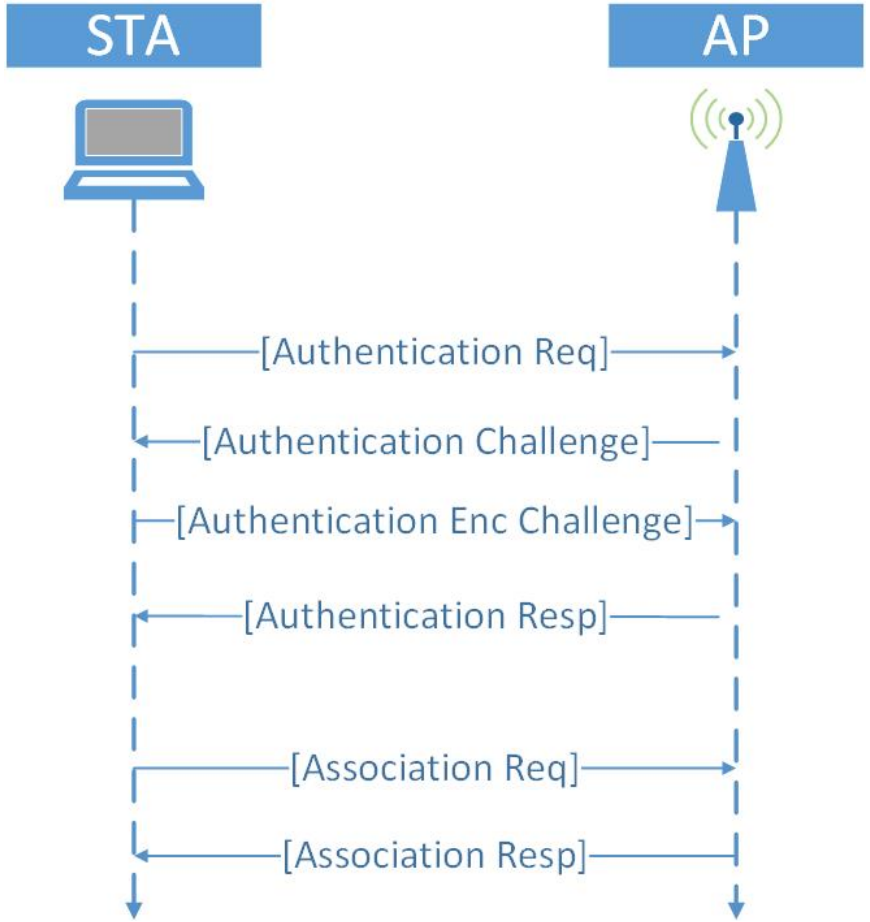
802.11 Security Modes: Open Access

- Open Access
  - No protection (whitelists)



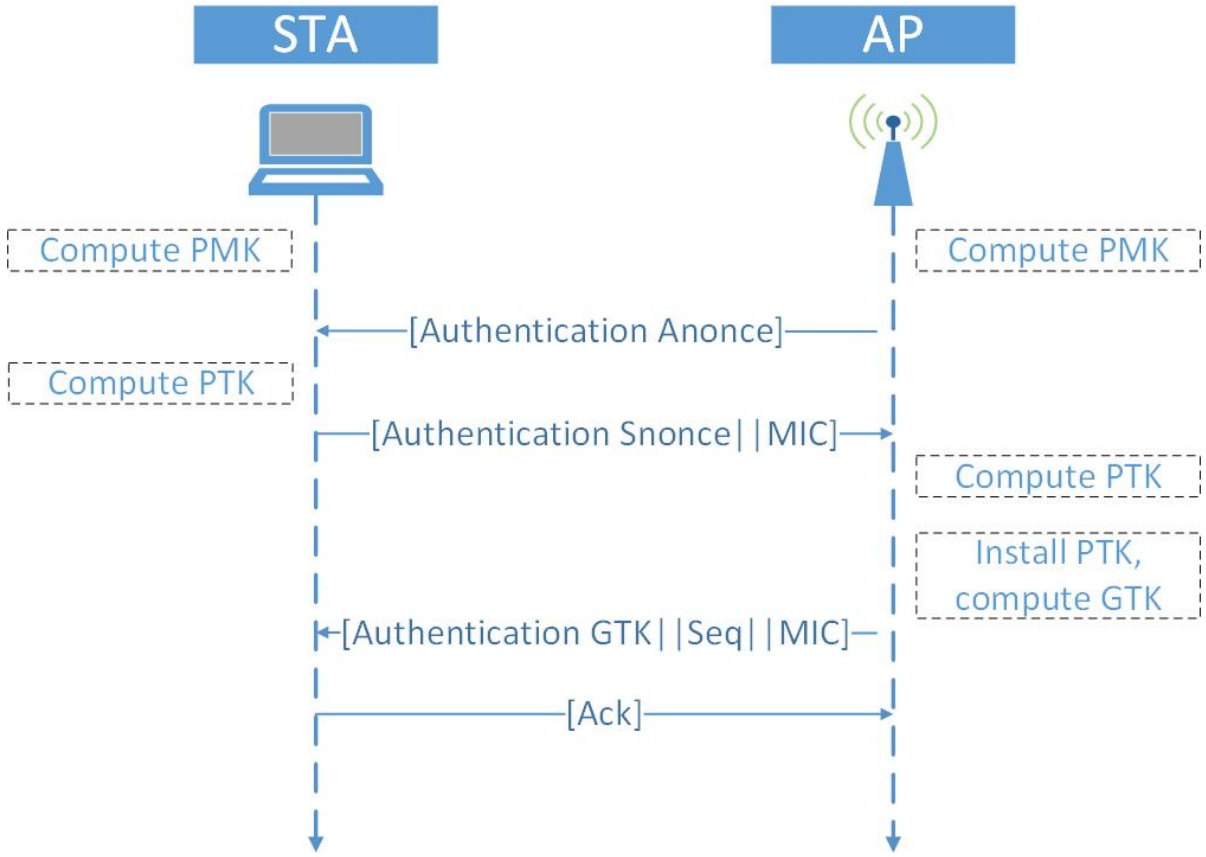
802.11 Security Modes:WEP

- Based on RC4 Encryption
- Broken

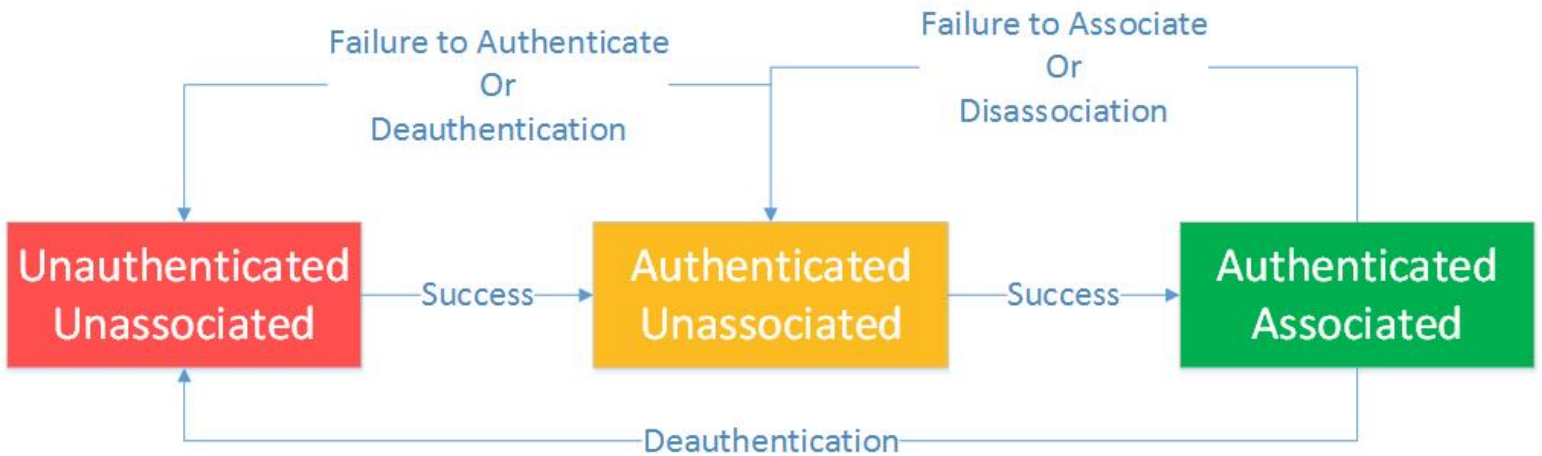


802.11 Security Modes: WPA/WPA2

- Based on AES
- Much more secure
- Current standard

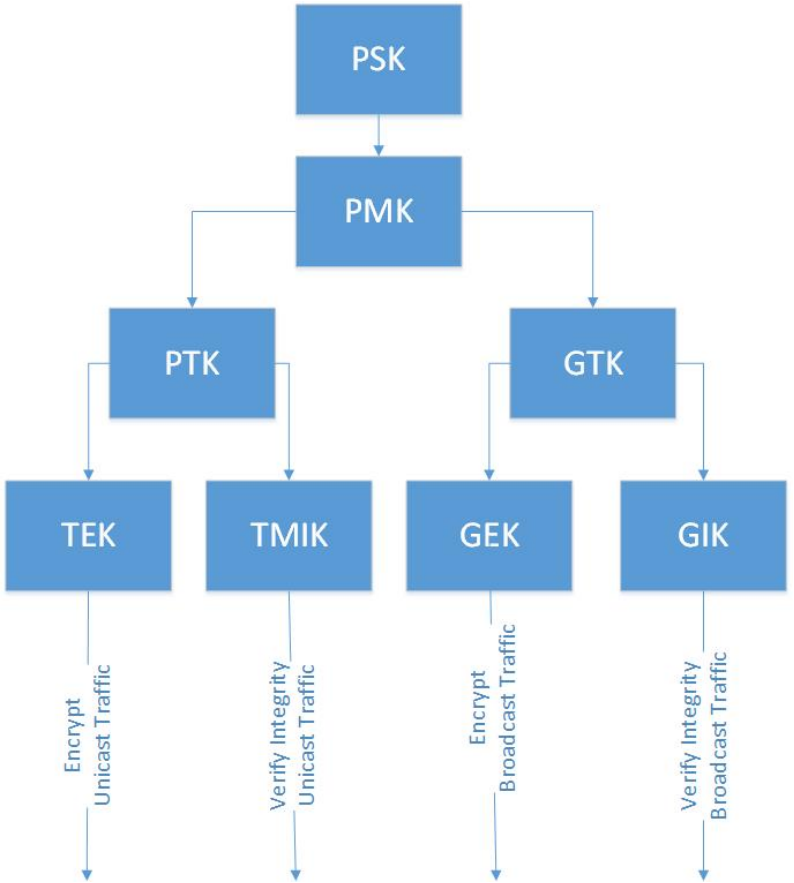


States of a Client

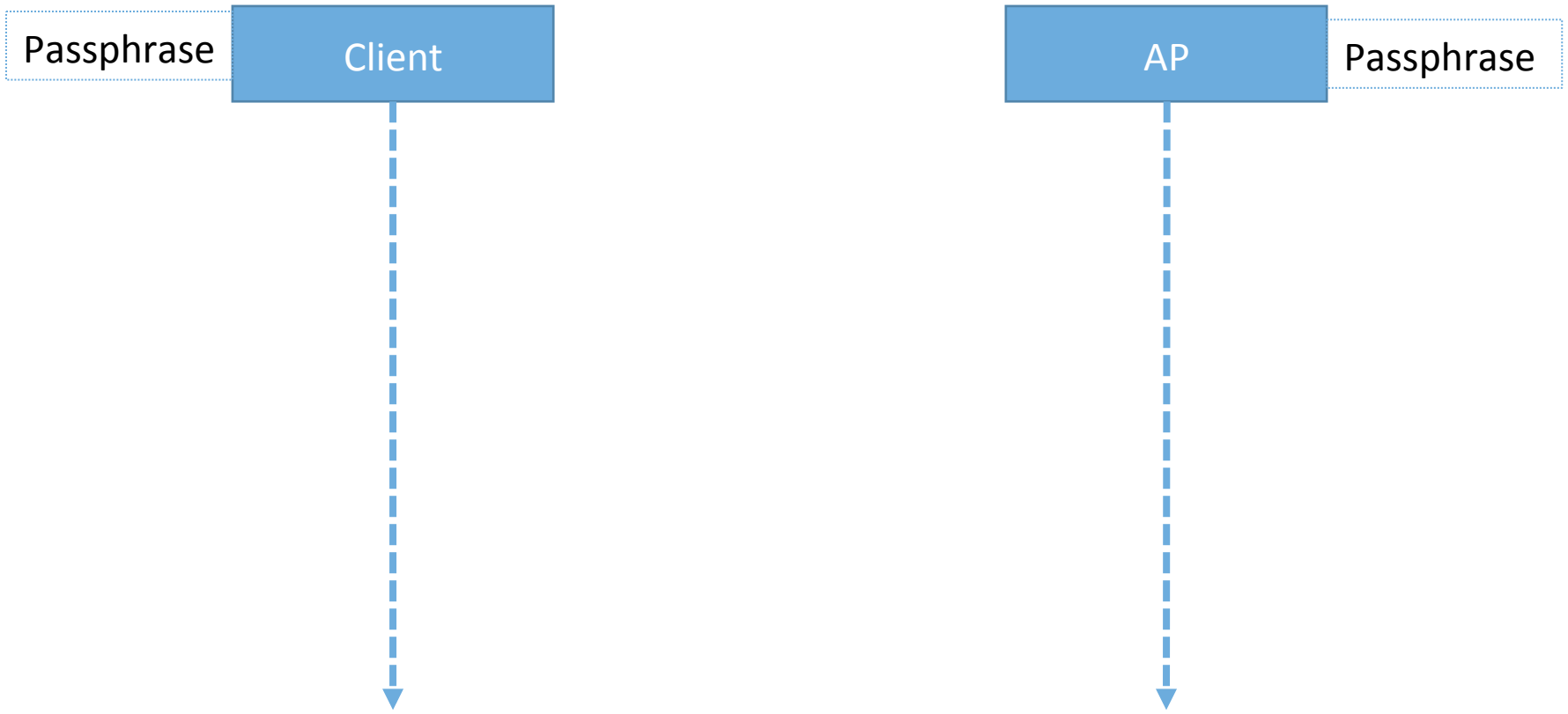


WPA2

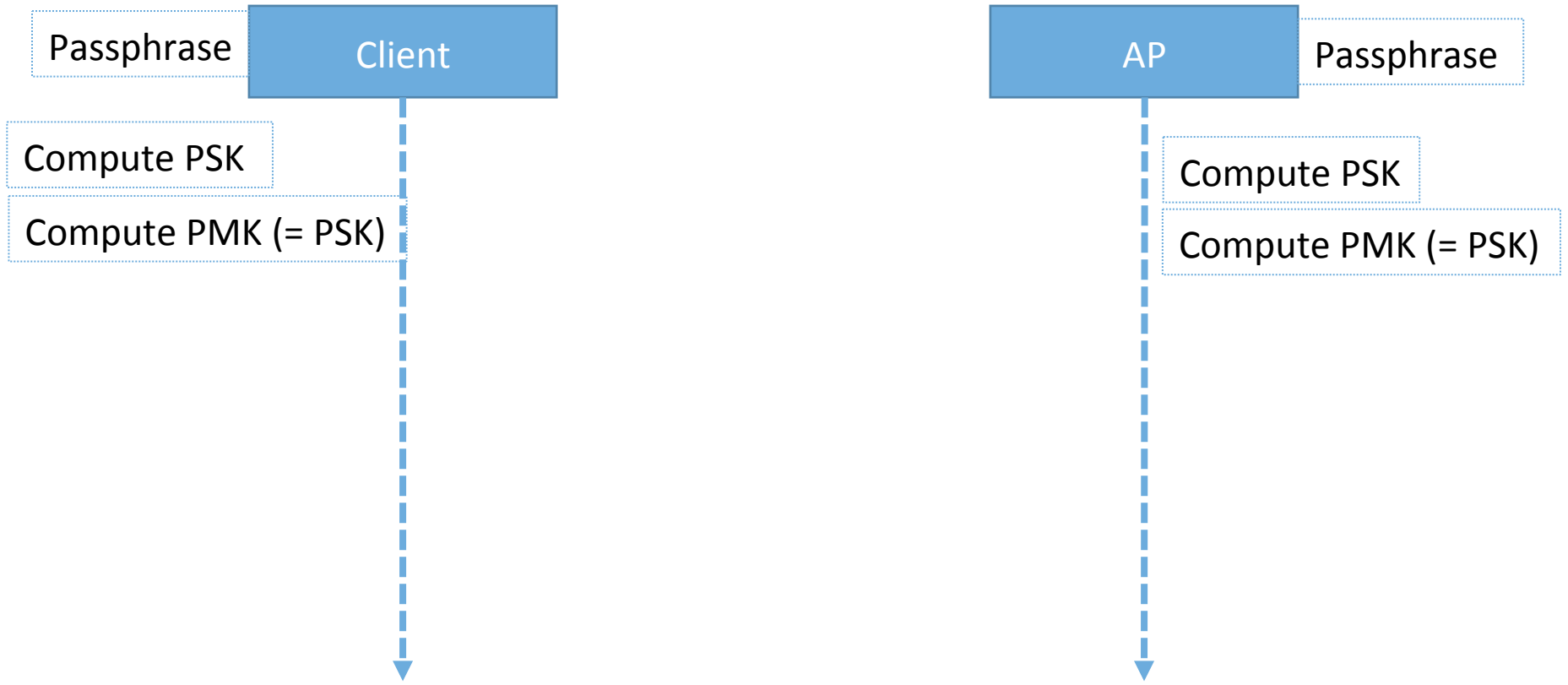
Key Hierarchy



WPA/WPA2 Four Way Handshake

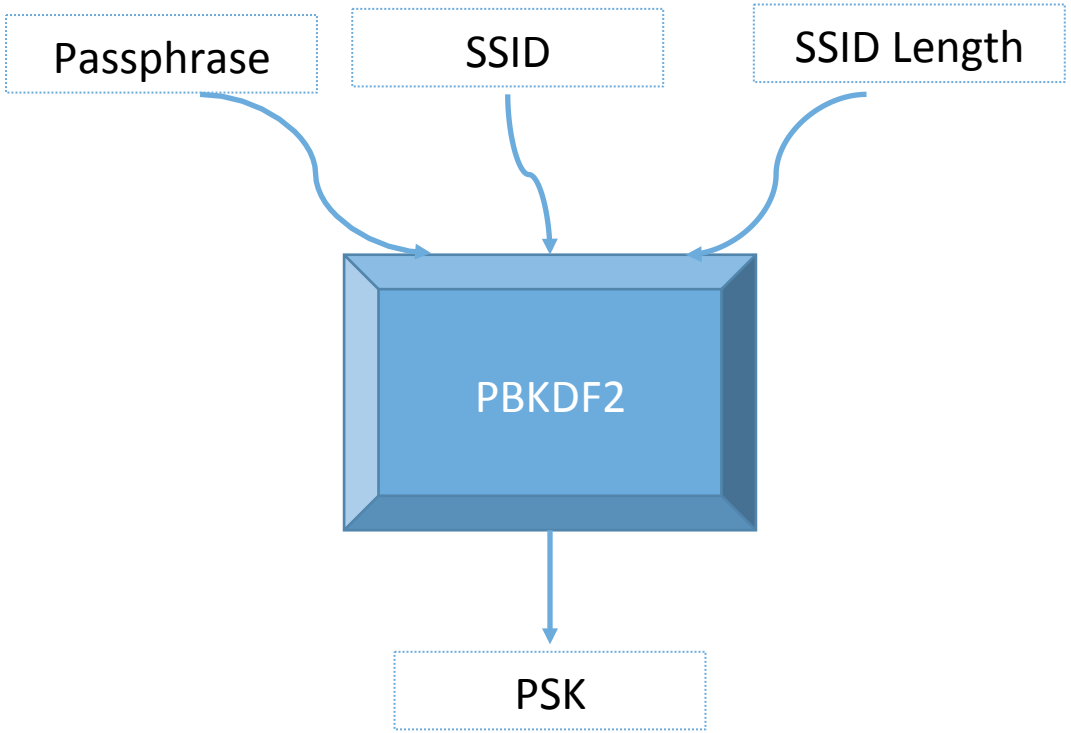


WPA/WPA2 Four Way Handshake

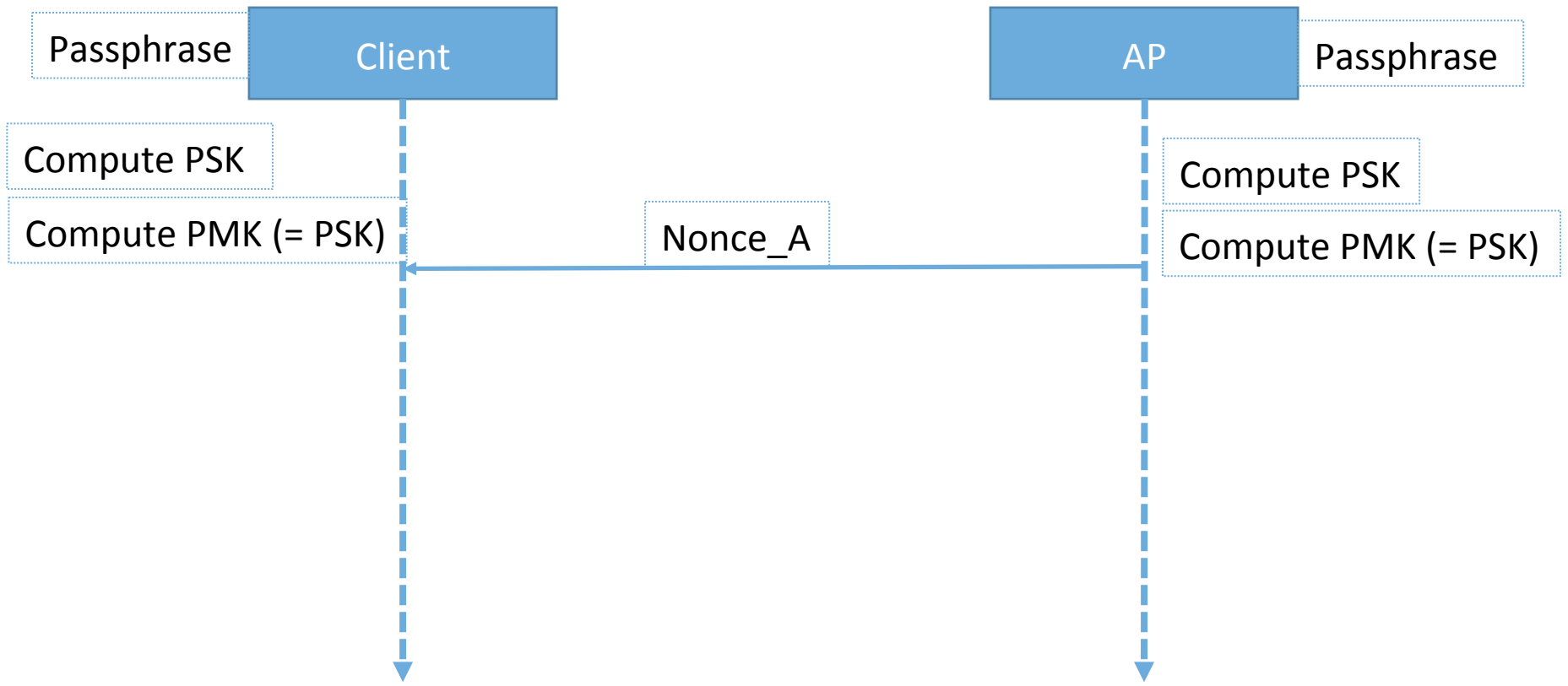


Computation of PSK

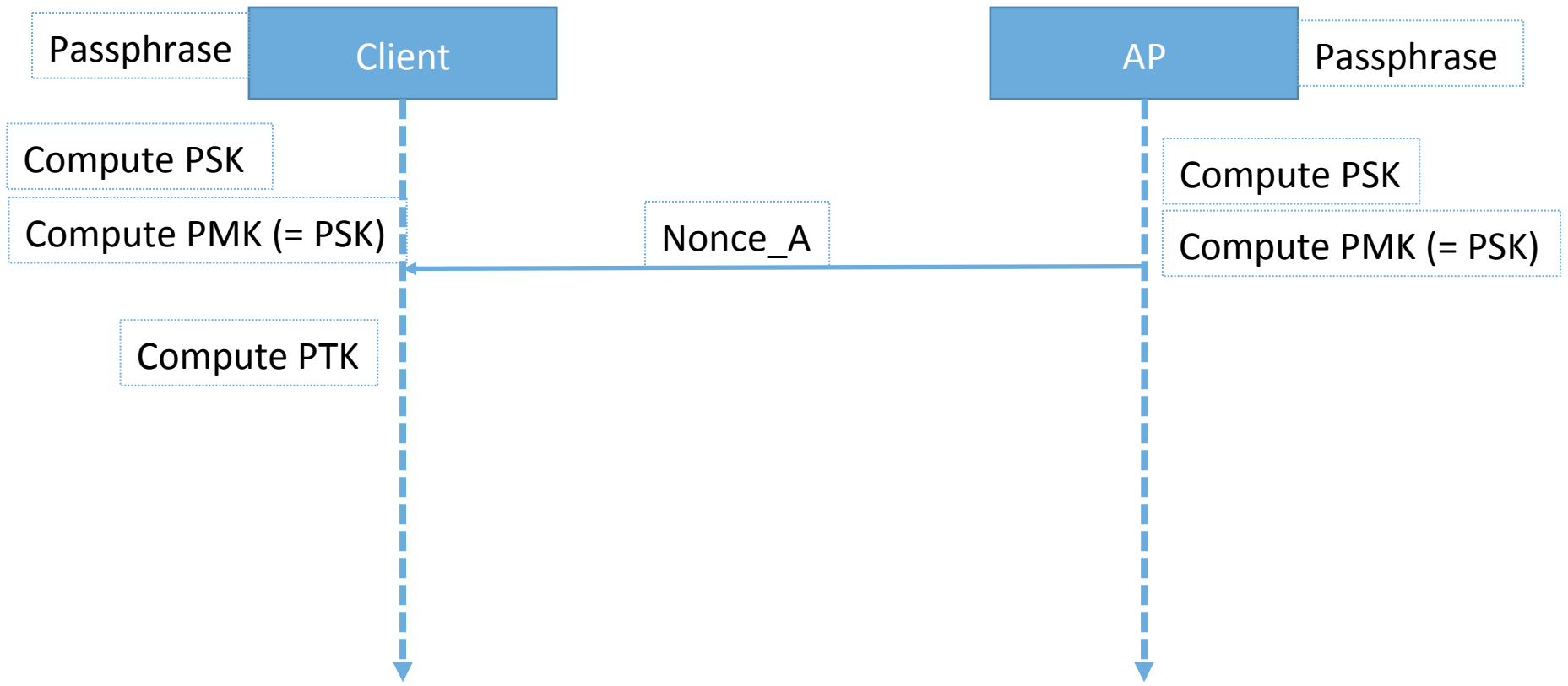
- Passphrase is a secret “phrase” you choose during the AP configuration
  - 8-63 characters long
- It is also the secret you insert in your device when you connect to a network
- SSID is the name of network
- PBKDF2 hashes 3 components 4096 times
- Heavy computation



WPA/WPA2 Four Way Handshake

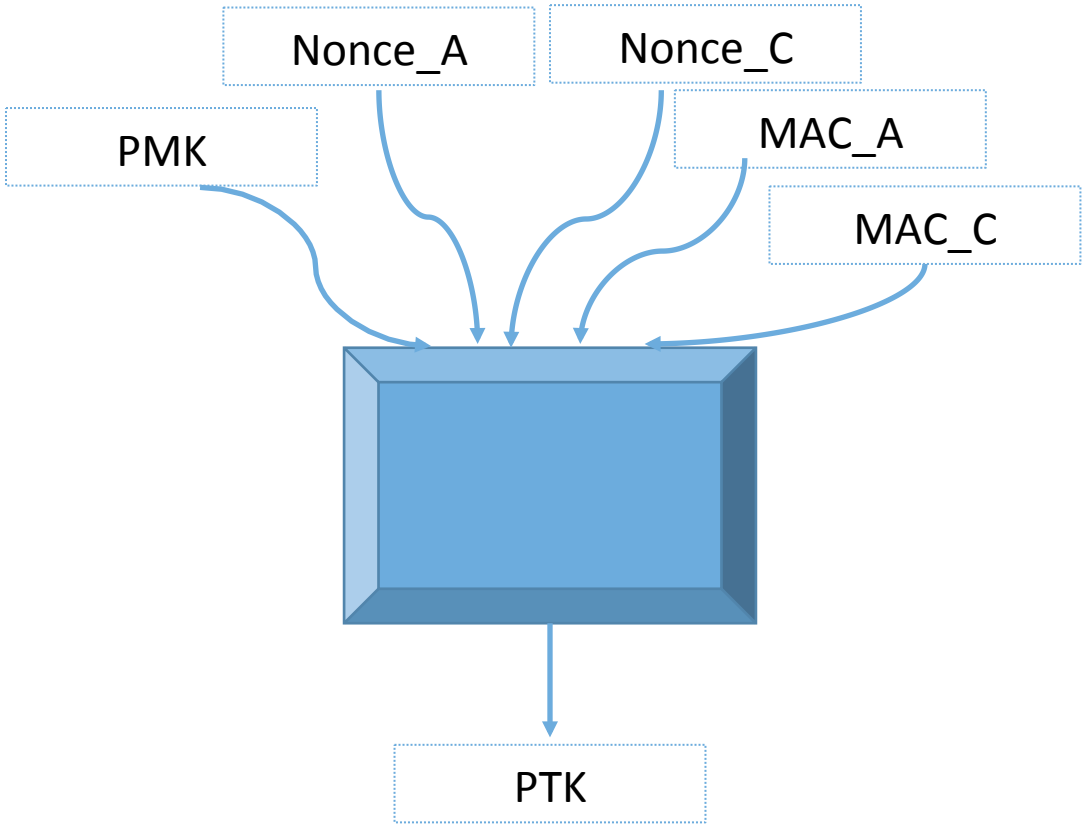


WPA/WPA2 Four Way Handshake

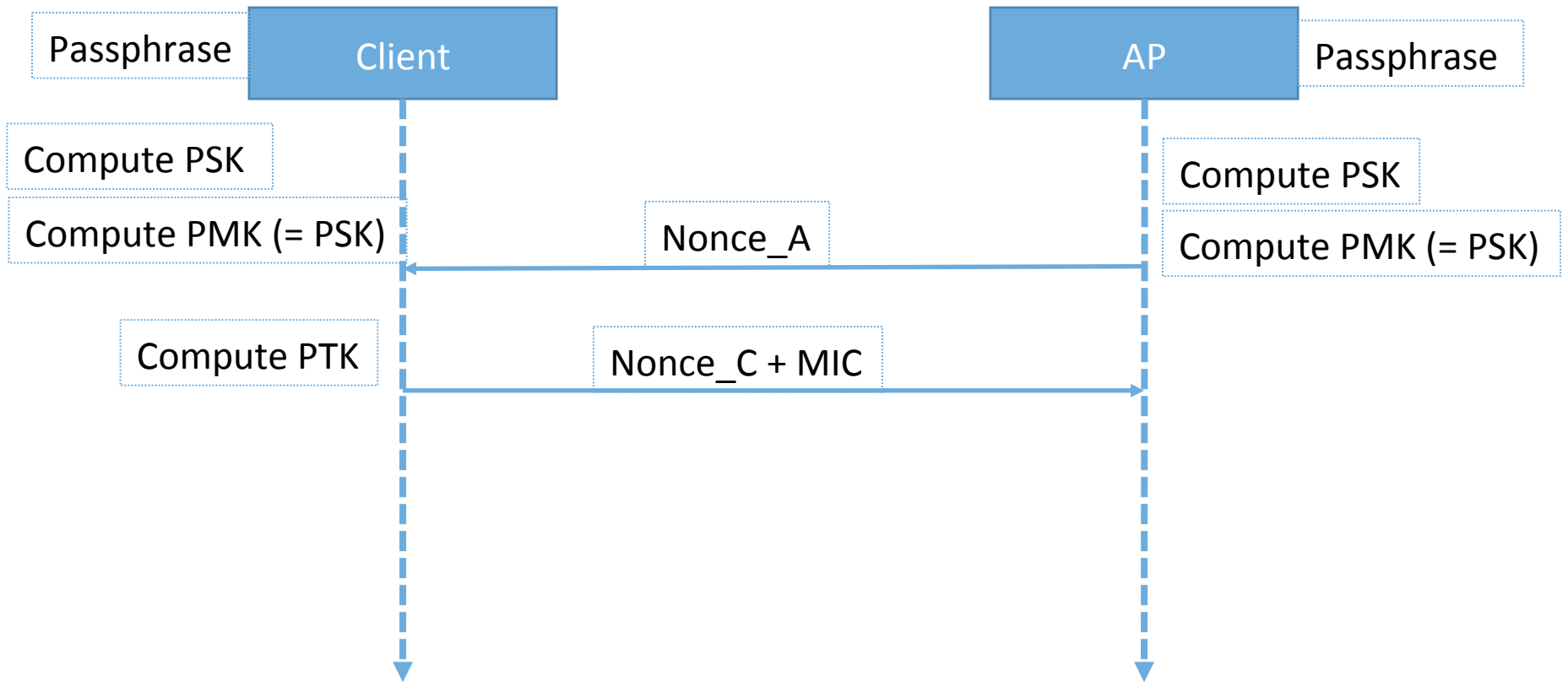


Computation of PTK

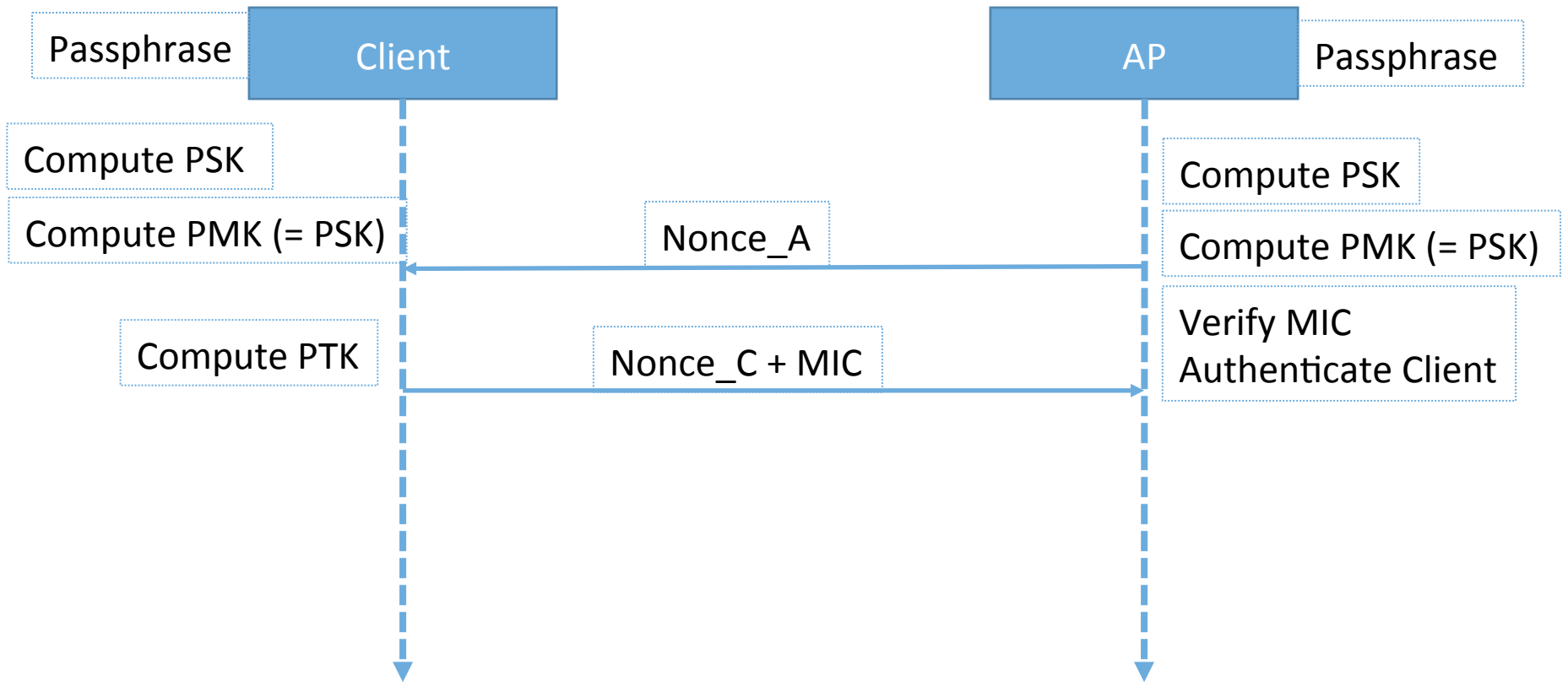
- PMK is derived from the Passphrase
- Nonce_A is a random number chosen by the AP and received through the first message
- Nonce_C is a random number chosen by the client
- MAC_A the hardware address of the AP
- MAC_C the hardware address of the client



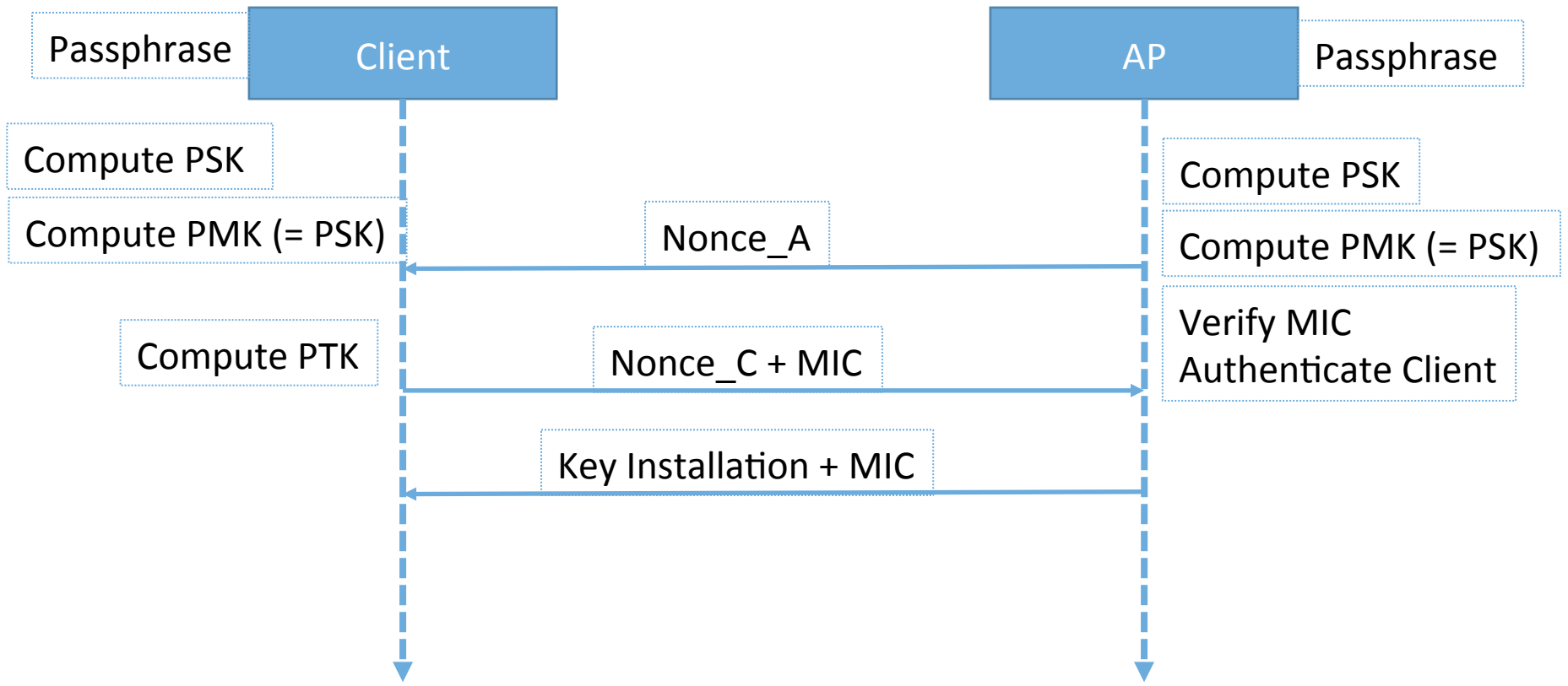
WPA/WPA2 Four Way Handshake



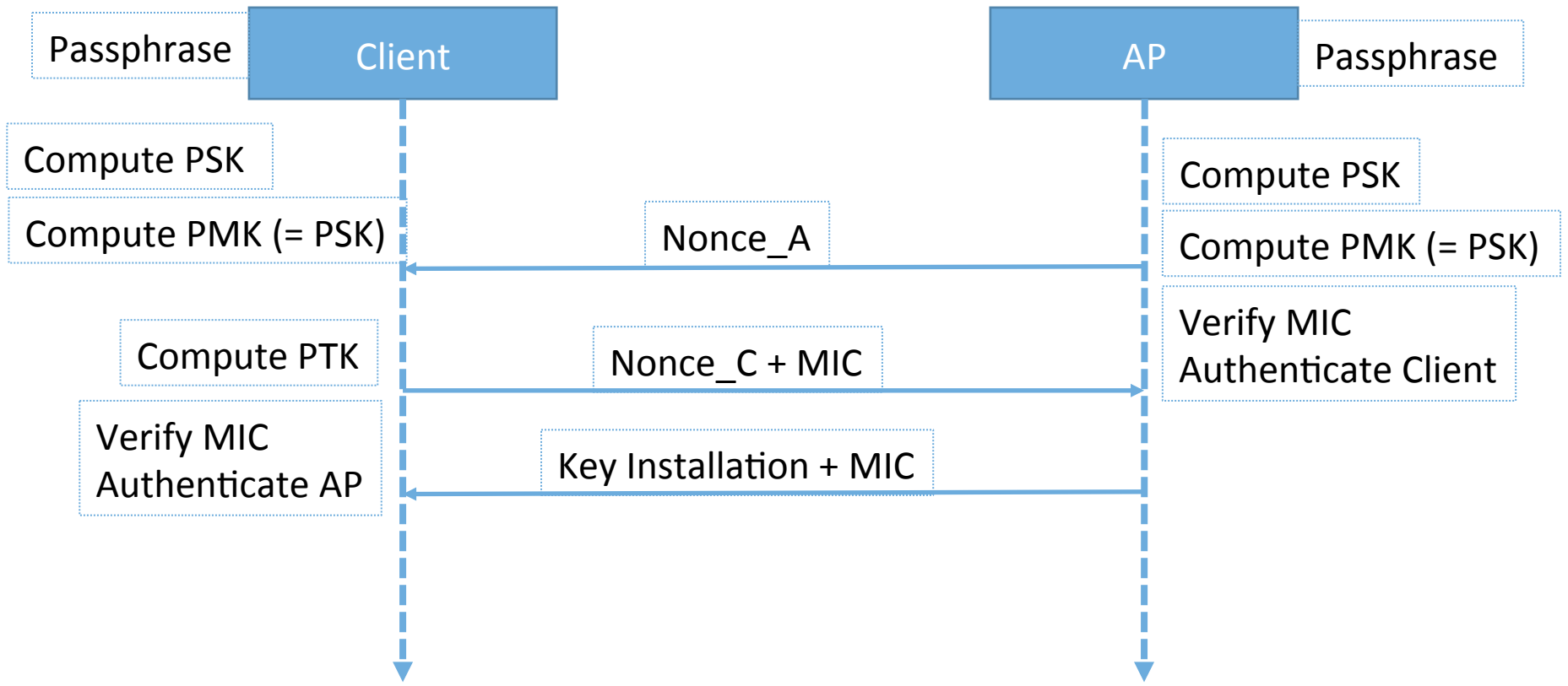
WPA/WPA2 Four Way Handshake



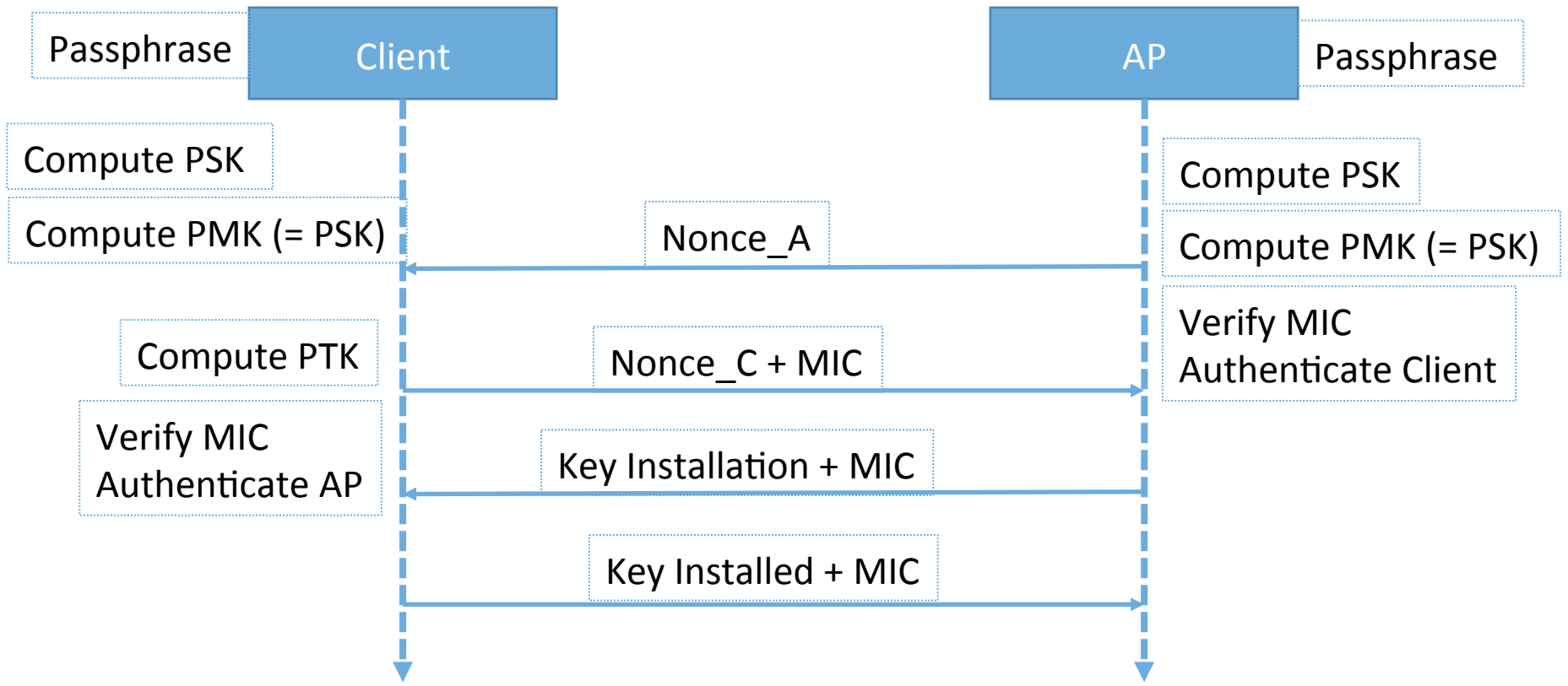
WPA/WPA2 Four Way Handshake



WPA/WPA2 Four Way Handshake



WPA/WPA2 Four Way Handshake



Cracking WPA/WPA2

- If attacker is present at a 4-way handshake
  - Nonce_A
  - Nonce_C
  - MAC_A
  - MAC_C
  - BUT NOT PMK
  - He must compute the PMK
- To compute the PMK(=PSK)
  - SSID
  - SSID length
  - BUT NOT passphrase
- What can he do???

Cracking WPA/WPA2

- Create a dictionary of possible passphrases
  - http://www.aircrack-ng.org/doku.php?id=faq#where_can_i_find_good_wordlists
- Choose a passphrase
- Create the PMK
- Use to PMK to produce PTK
- Use this key to generate the MIC of message 3
- If the MICs match the correct passphrase was used
- If not…repeat

Lab Setup

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

Other Attacks

- Deauthentication Flooding
  - Make everyone loose their connection
- Beacon Flooding
  - Flood a client with fake network names
- Authentication Request Flooding
  - Burden the AP with invalid authentication requests
- Evil Twin
  - Create a network with the same name in which the attacker can see everything
- Crack the key (WEP)