

Masterclass : WiFi



<https://github.com/JulienFink/WiFi-Project>



Summary

- WiFi definition and presentation
- WiFi core mechanism
- Security issues



Summary

- WiFi definition and presentation
- WiFi core mechanism
- Security issues



WiFi definition and presentation (1/N)

- Radio waves
- Provides local network and Internet access to devices
- 2.4 GHz and/or 5.8 GHz

Designed for :	2.4 GHz	5.8 GHz
Range	✓	✗
Linkrate	✗	✓
Penetration	✓	✗



Summary

- WiFi definition and presentation
- **WiFi core mechanism**
- Security issues



WiFi core mechanism (1/N)

IEEE 802.1X

- IEEE 802.1X
- These set of standards allow you to control access to network infrastructure equipments
- Wireless Local Area Networks (WLANs)



WiFi core mechanism (1/N)

Establishing a secure communication consists of four phases

- Agreeing on the security policy
- 802.1X authentication
- Key derivation and distribution
- RSNA (Robust Security Network Association) data confidentiality and integrity



WiFi core mechanism (1/N)

Connection to a(n) router/access point - Network authentication and data encryption protocols

Network authentication and data encryption protocols

Open System Authentication

WEP

WPA/WPA2

unsafe

unsafe/depreceated

safe



WiFi core mechanism (1/N)

Open System Authentication (OSA)

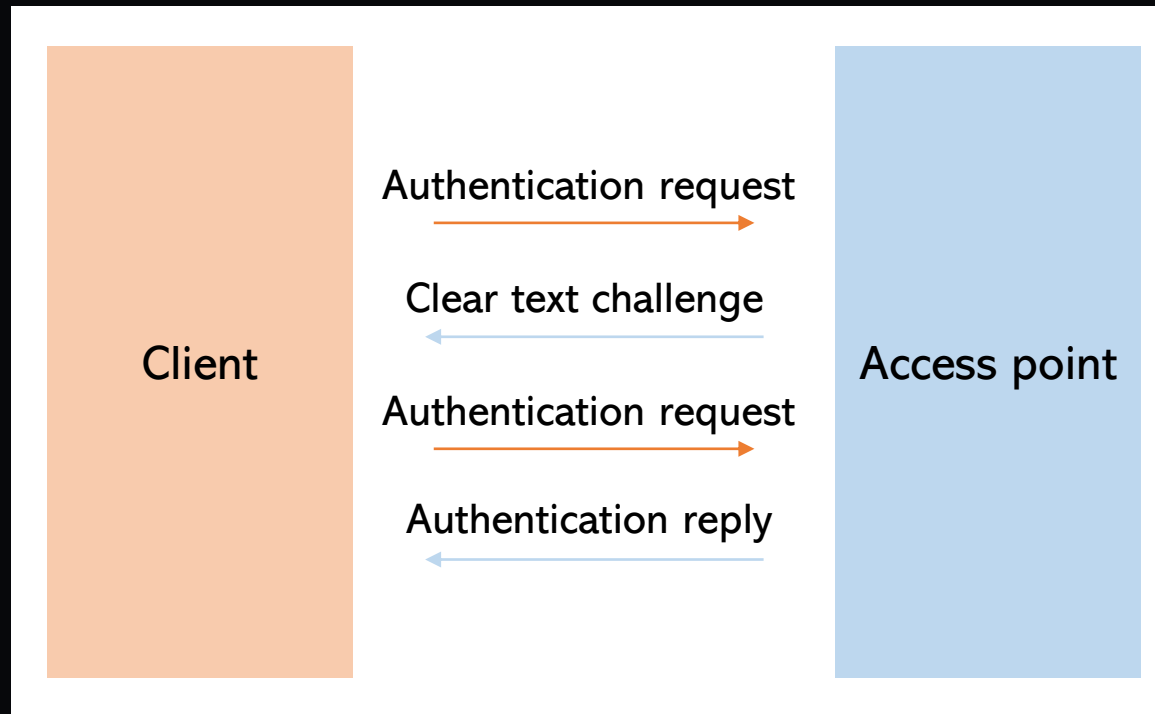
- In Open System authentication, the WLAN client does not provide its credentials to the Access Point during authentication.
- Any client can authenticate and associate with the Access Point
- Data travels in a clear format, except if other protocols perform encryption (e.g. TLS)



WiFi core mechanism (1/N)

WEP (Wired Equivalent Privacy) (1/2) - Shared Key authentication

In Shared Key authentication, the WEP key is used for authentication in a four-step challenge-response handshake :



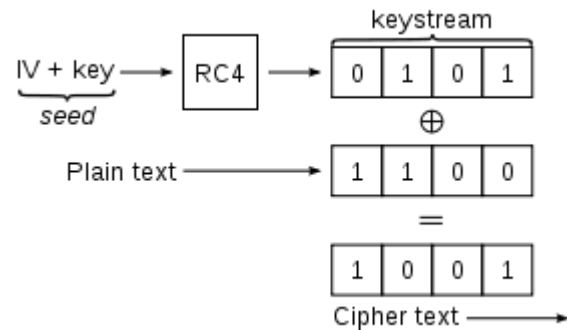
After the authentication and association, the pre-shared WEP key is also used for encrypting the data frames using RC4.



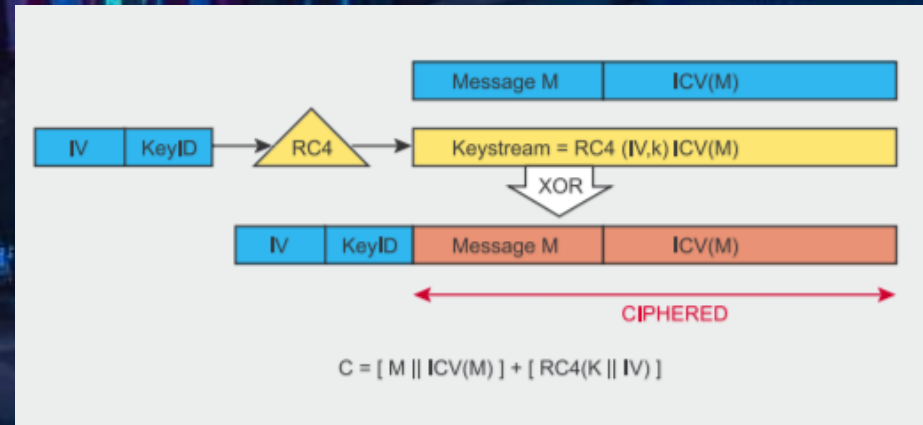
WiFi core mechanism (1/N)

WEP (2/2) - Payload encryption

- Stream cipher RC4
- 40 bits + 24 bits IV = 64-bit WEP key
- $C = [M \parallel ICV(M)] \oplus [RC4(K \parallel IV)]$



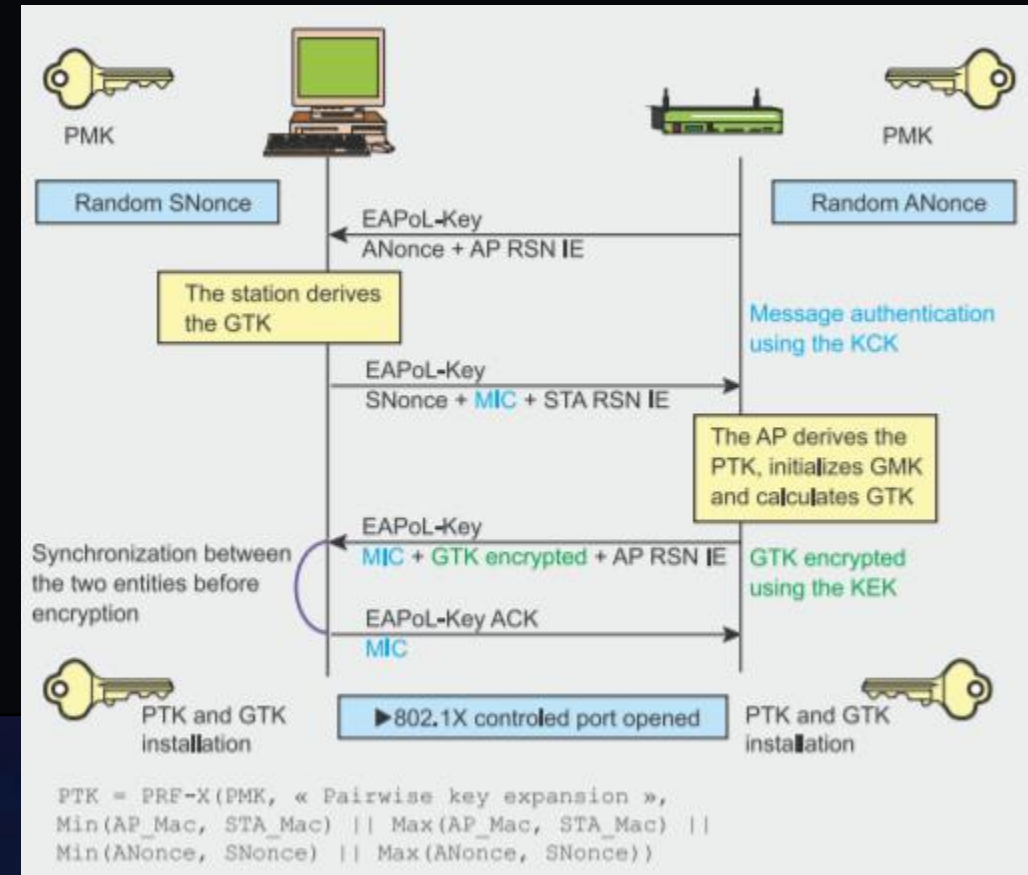
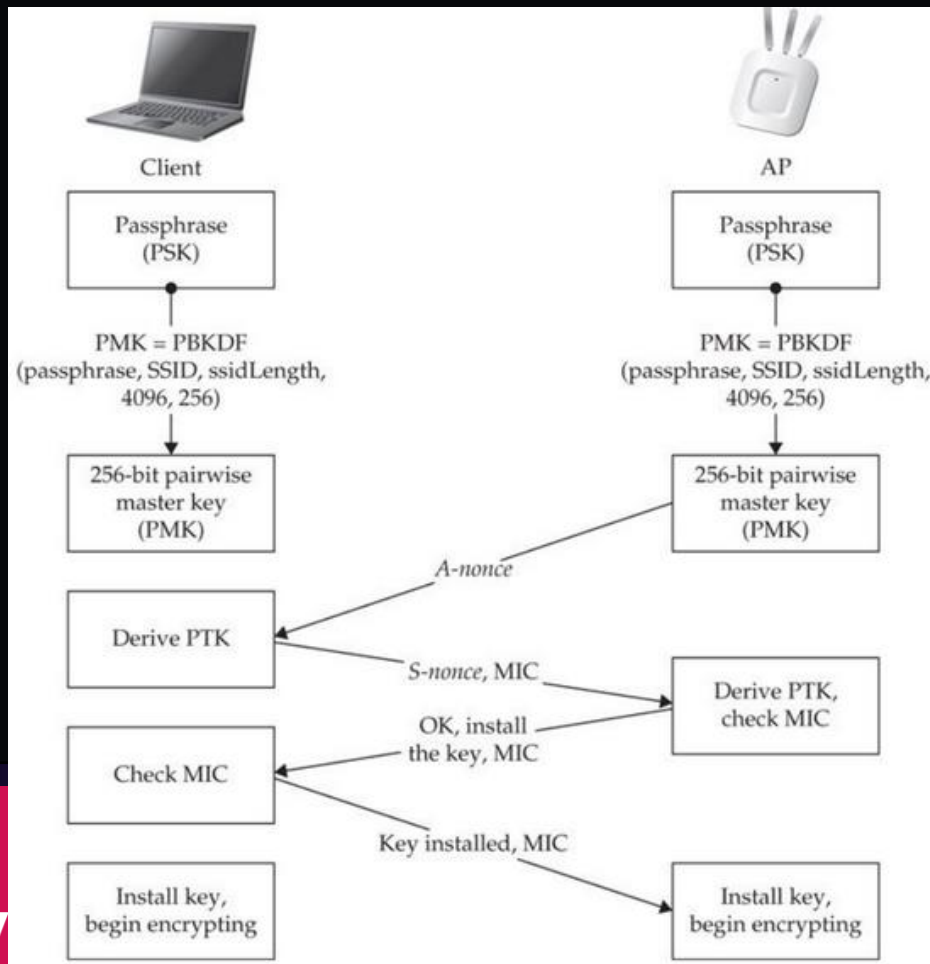
**Basic WEP
encryption: RC4
keystream XORed
with plaintext**



WiFi core mechanism (1/N)

WPA & WPA2 (Wi-Fi Protected Access) - PSK authentication

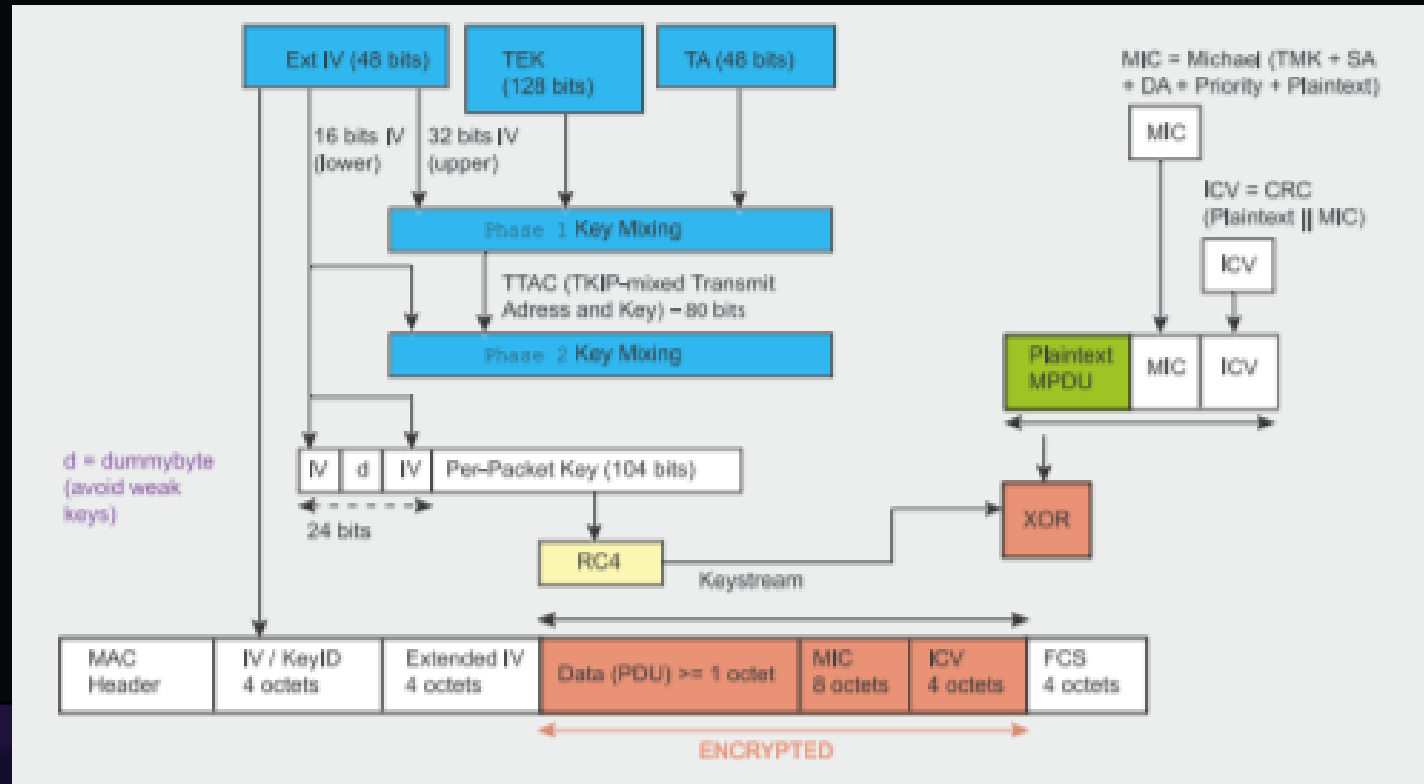
- PSK (Pre-Shared Key) authentication



WiFi core mechanism (1/N)

WPA - Payload encryption

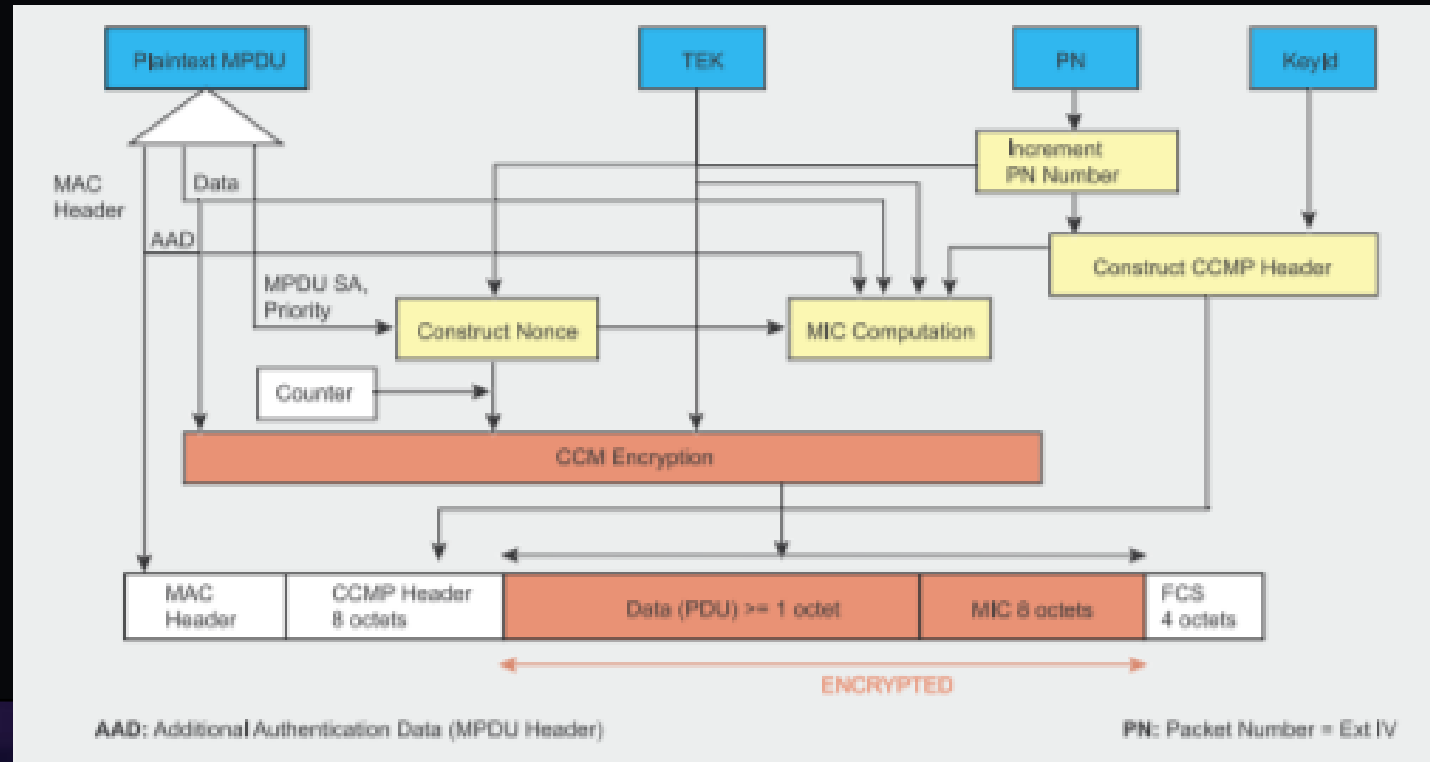
- TKIP (Temporal Key Integrity Protocol) encryption



WiFi core mechanism (1/N)

WPA2 - Payload encryption

- CCMP (Counter-Mode/CBC-Mac protocol) encryption



WiFi core mechanism (1/N)

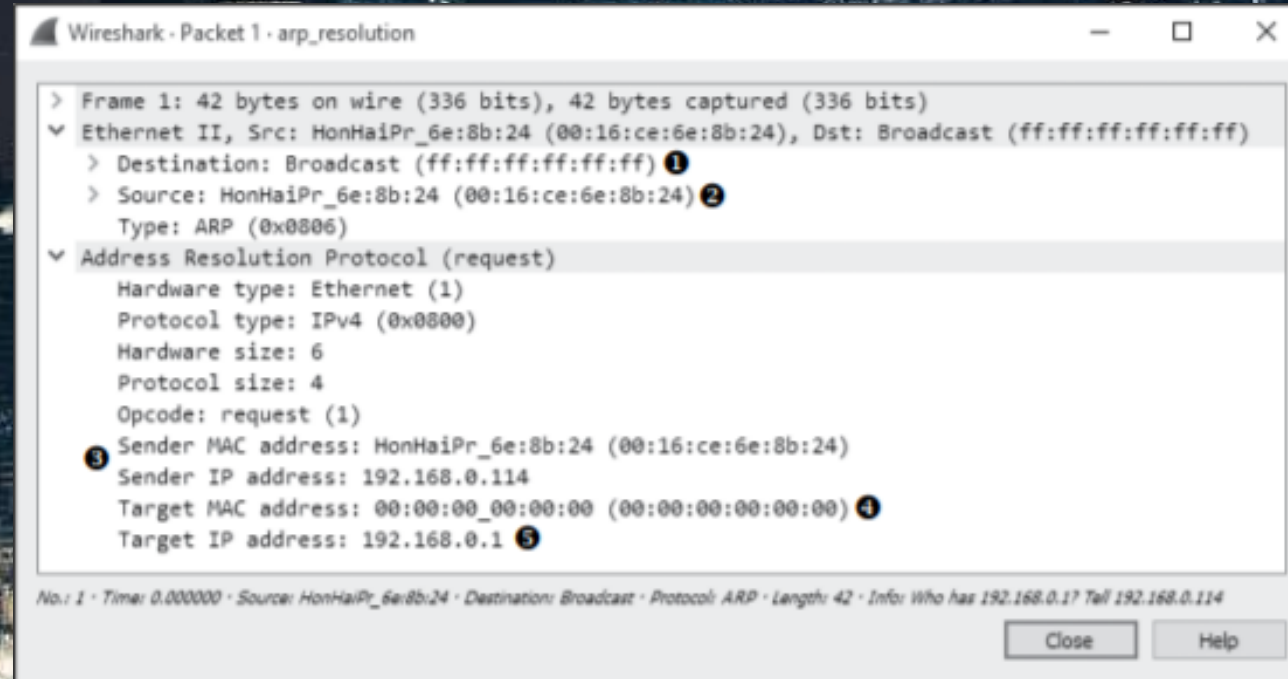
ARP (Address Resolution Protocol)

- A communication protocol used for discovering the link layer address associated with a given Internet layer address
- Media Access Control (MAC) addresses are needed because the switch that interconnects devices on a network uses a Content Addressable Memory (CAM) table, which lists the MAC addresses of all devices plugged into each of its ports



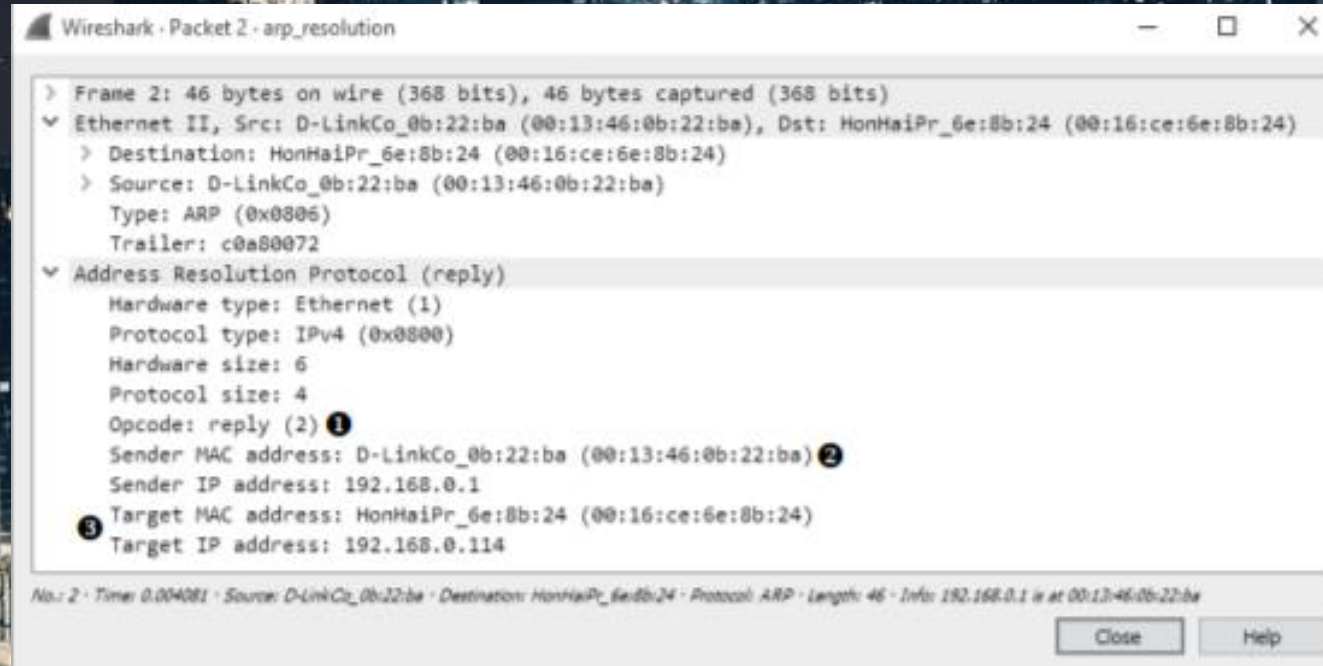
WiFi core mechanism (1/N)

ARP (Address Resolution Protocol) - ARP request



WiFi core mechanism (1/N)

ARP (Address Resolution Protocol) - ARP reply



Summary

- WiFi definition and presentation
- WiFi core mechanism
- **Security issues**



Security issues (1/N)

For radio communications in general

- Eavesdropping
- RF Denial of Service (DoS)
- Media Access Control (MAC) address spoofing
- Hijacking
- Man-in-the-Middle attacks
- Encryption cracking



Useful links

- <https://repository.root-me.org/R%C3%A9seau/EN%20-%20Hacking%20wifi.pdf>
- [https://github.com/koutto/pi-pwnbox-rogueap/wiki/O5.-WPA-WPA2-Personal-\(PSK\)-Authentication](https://github.com/koutto/pi-pwnbox-rogueap/wiki/O5.-WPA-WPA2-Personal-(PSK)-Authentication)
- <http://www.c-jump.com/bcc/common/Talk/WIFIconfig/index.html>
- <https://cylab.be/blog/32/how-does-wpawpa2-wifi-security-work-and-how-to-crack-it>
- <https://wifi.pressbooks.com/chapter/securite/>

