Masterclass : Wi-Fi

GitHub

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

ESILV
ENGINEERING SCHOOL
DE VINCI PARIS

Julien Fink
A5 ESILV Student

Summary

- Wi-Fi definition and presentation
- Core mechanism - protocols overview
- Security issues

ESILV
ENGINEERING SCHOOL
DE VINCI PARIS

Julien Fink
A5 ESILV Student

Summary

- Wi-Fi definition and presentation
- Core mechanism - protocols overview
- Security issues

ESILV
ENGINEERING SCHOOL
DE VINCI PARIS

Julien Fink
A5 ESILV Student

Wi-Fi definition and presentation (1/N)

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

Designed for :	2.4 GHz	5.8 GHz
Range	✔	✘
Linkrate	✘	✔
Penetration	✔	✘

ESILV
ENGINEERING SCHOOL
DE VINCI PARIS

Julien Fink
A5 ESILV Student

Summary

- Wi-Fi definition and presentation
- **Core mechanism - protocols overview**
- Security issues

ESILV
ENGINEERING SCHOOL
DE VINCI PARIS

Julien Fink
A5 ESILV Student

Wi-Fi core mechanism (1/N)

IEEE 802.11 standard

- IEEE 802.11 refers to the set of standards that define communication for wireless local area networks (WLANs)
- A 1985 decision by the U.S. Federal Commission for Communication that opened up the ISM band for unlicensed use
- Various security algorithms for IEEE 802.11 wireless networks

ESILV
ENGINEERING SCHOOL
DE VINCI PARIS

Julien Fink
A5 ESILV Student

Wi-Fi core mechanism (1/N)

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

Network authentication and data encryption		
Open System Authentication	WEP	WPA/WPA2
unsafe	unsafe/depreceated	safe

ESILV
ENGINEERING SCHOOL
DE VINCI PARIS

Julien Fink
A5 ESILV Student

Wi-Fi 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)

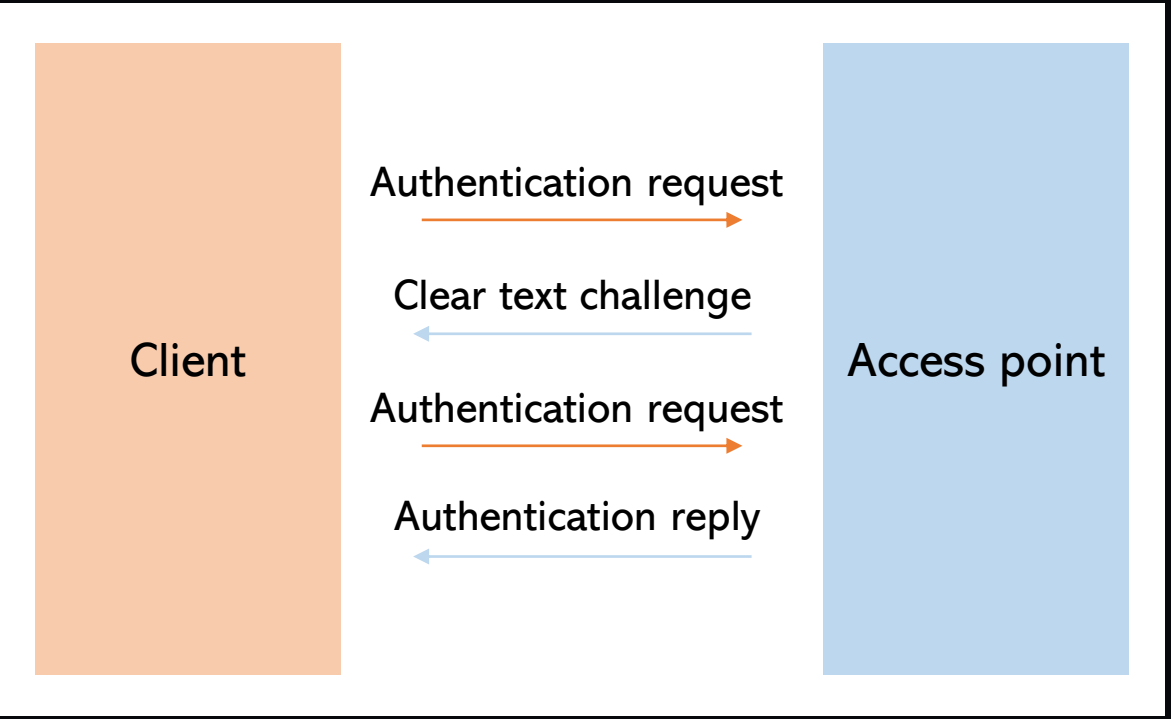
ESILV
ENGINEERING SCHOOL
DE VINCI PARIS

Julien Fink
A5 ESILV Student

Wi-Fi 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 :

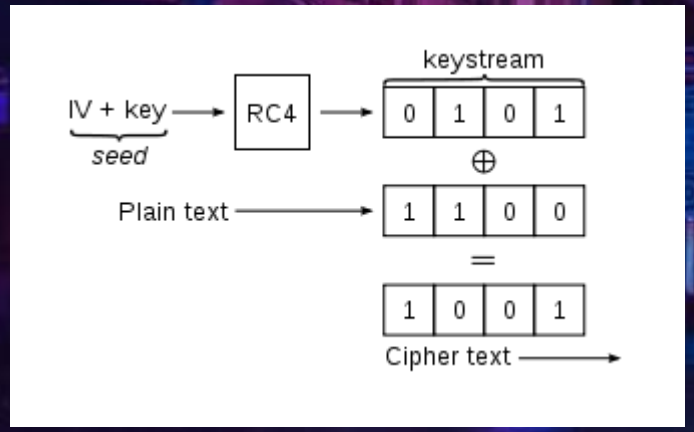


After the authentication and association, the pre-shared WEP key is also used for encrypting the data frames using RC4.

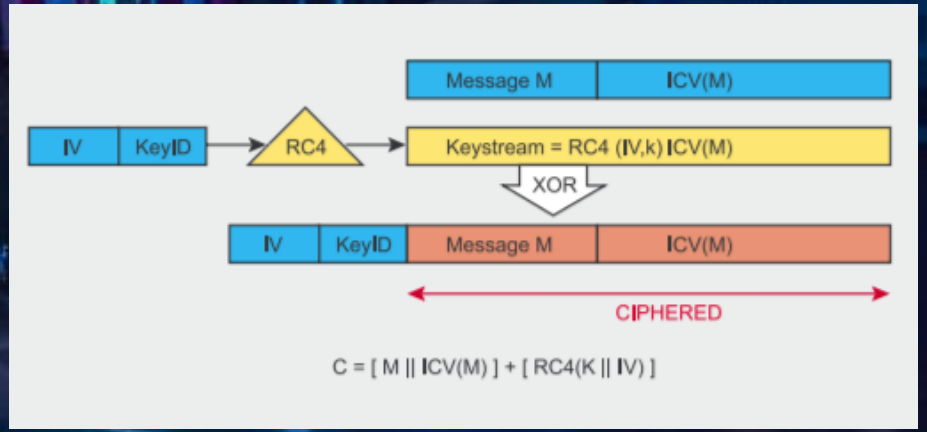
Wi-Fi core mechanism (1/N)

WEP (2/2) - Payload encryption

- Stream cipher RC4
- 40 bits + 24 bits IV = 64-bit WEP key
- C = [M || ICV(M)] ⊕ [RC4(K || IV)]



Basic WEP encryption: RC4 keystream XORed with plaintext



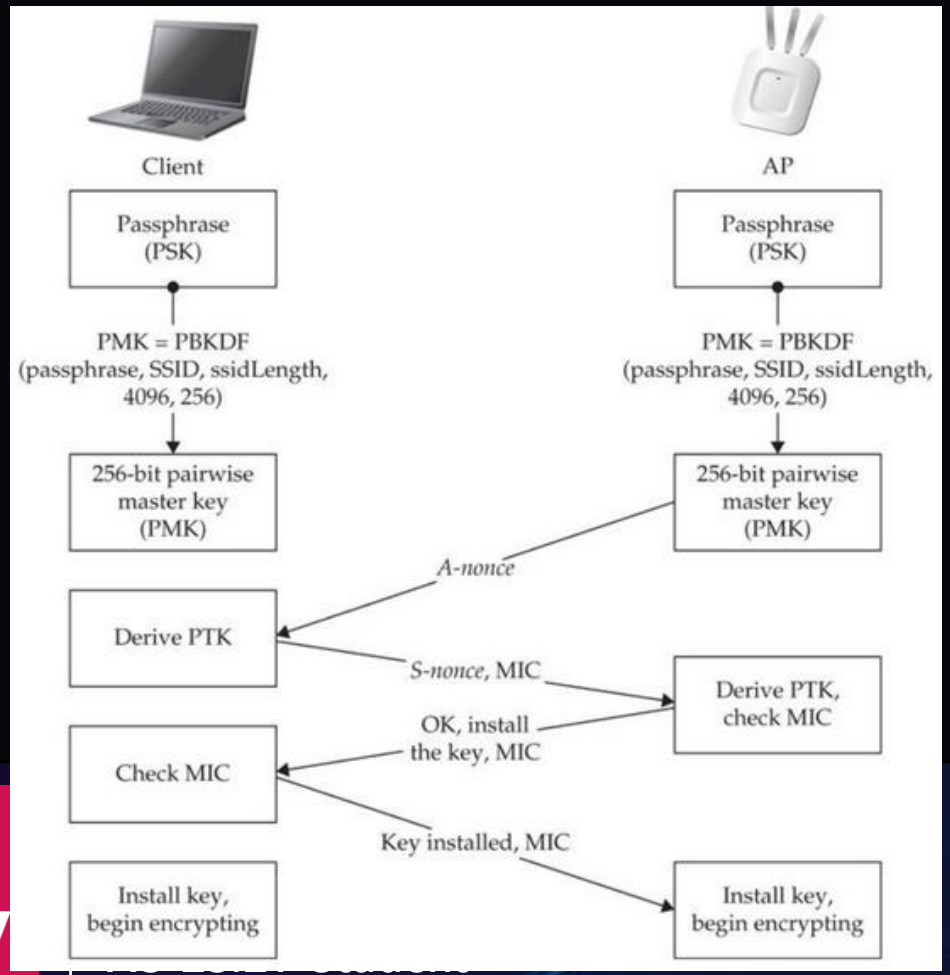
ESILV
ENGINEERING SCHOOL
DE VINCI PARIS

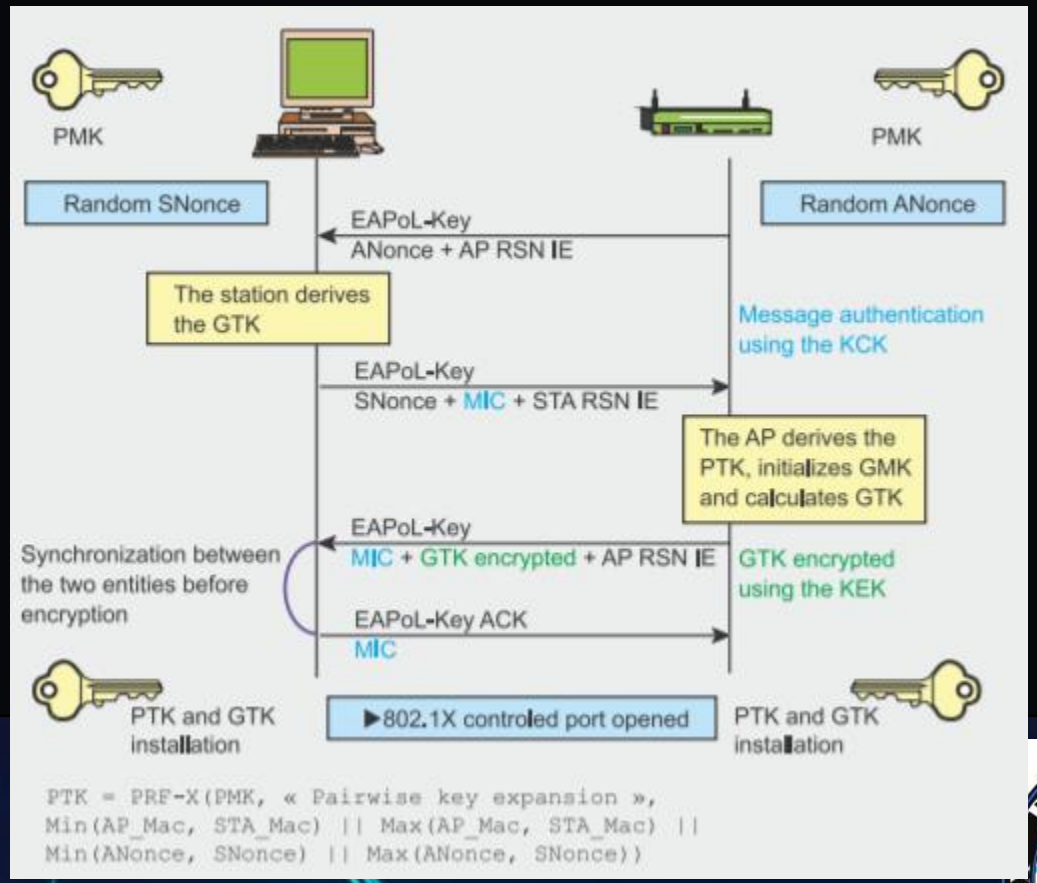
Julien Fink
A5 ESILV Student

Wi-Fi core mechanism (1/N)

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

- PSK (Pre-Shared Key) authentication



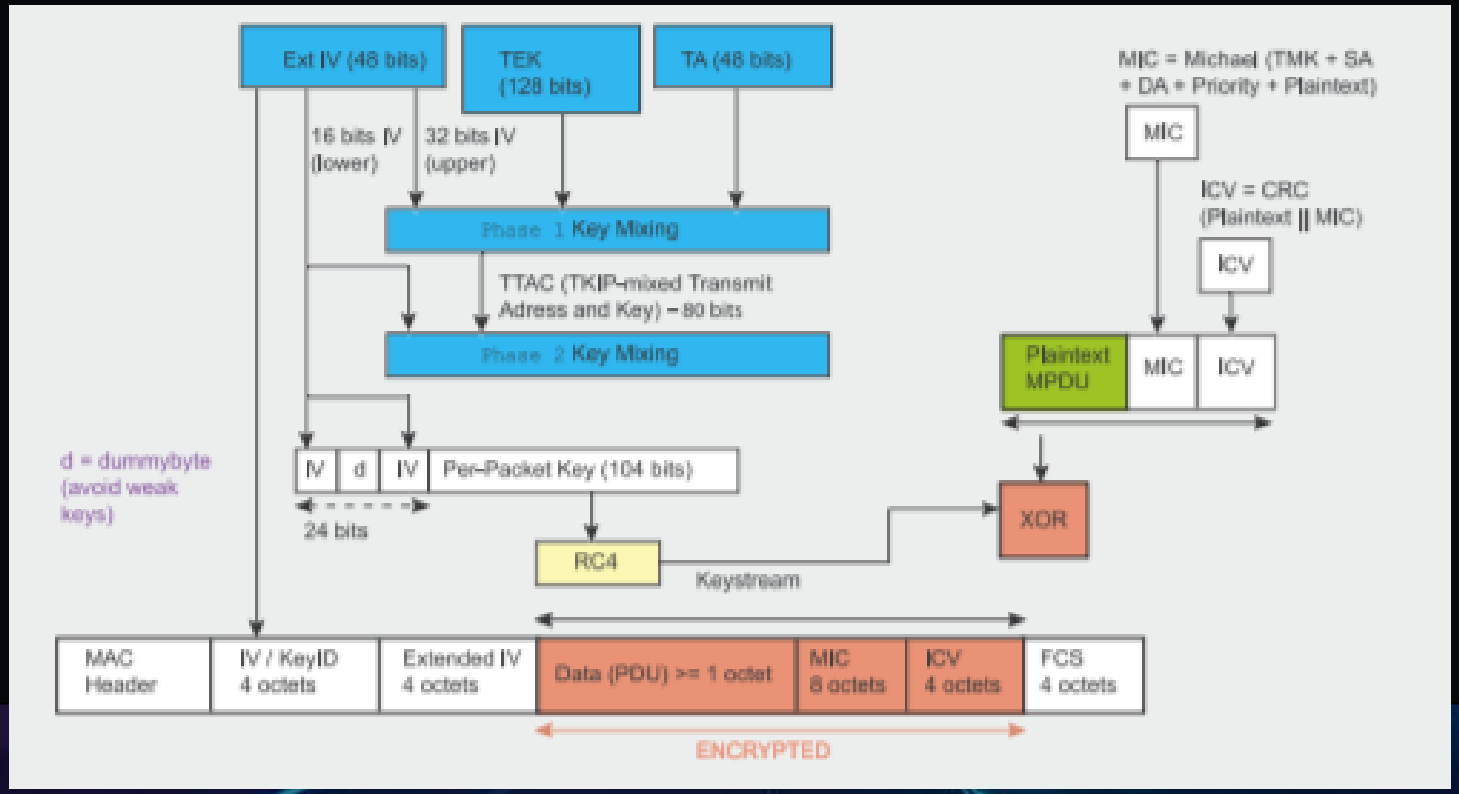


ESILV
ENGINEERING SCHOOL
DE VINCI PARIS

Wi-Fi core mechanism (1/N)

WPA - Payload encryption

- TKIP (Temporal Key Integrity Protocol) encryption



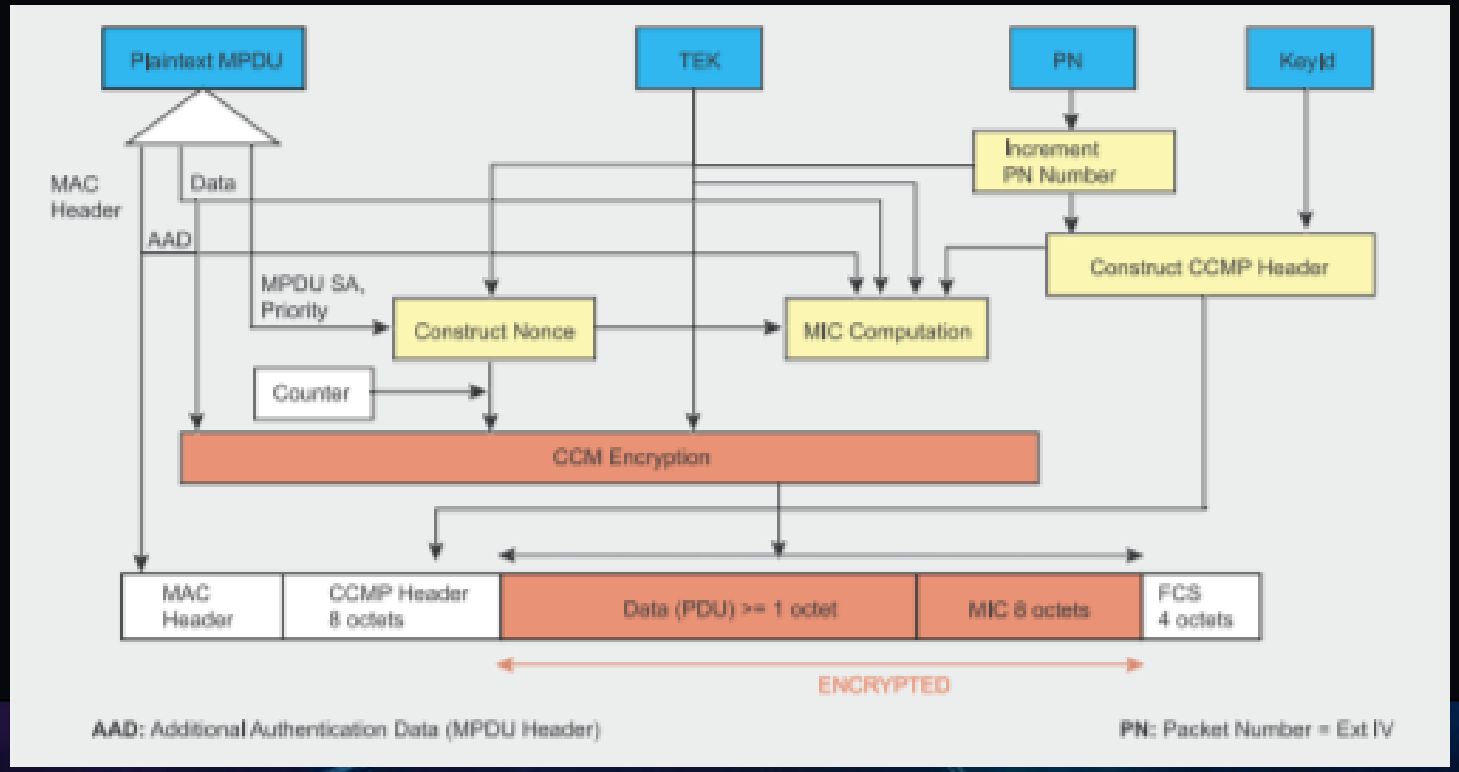
ESILV
ENGINEERING SCHOOL DE VINCI PARIS

Julien Fink
A5 ESILV Student

Wi-Fi core mechanism (1/N)

WPA2 - Payload encryption

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



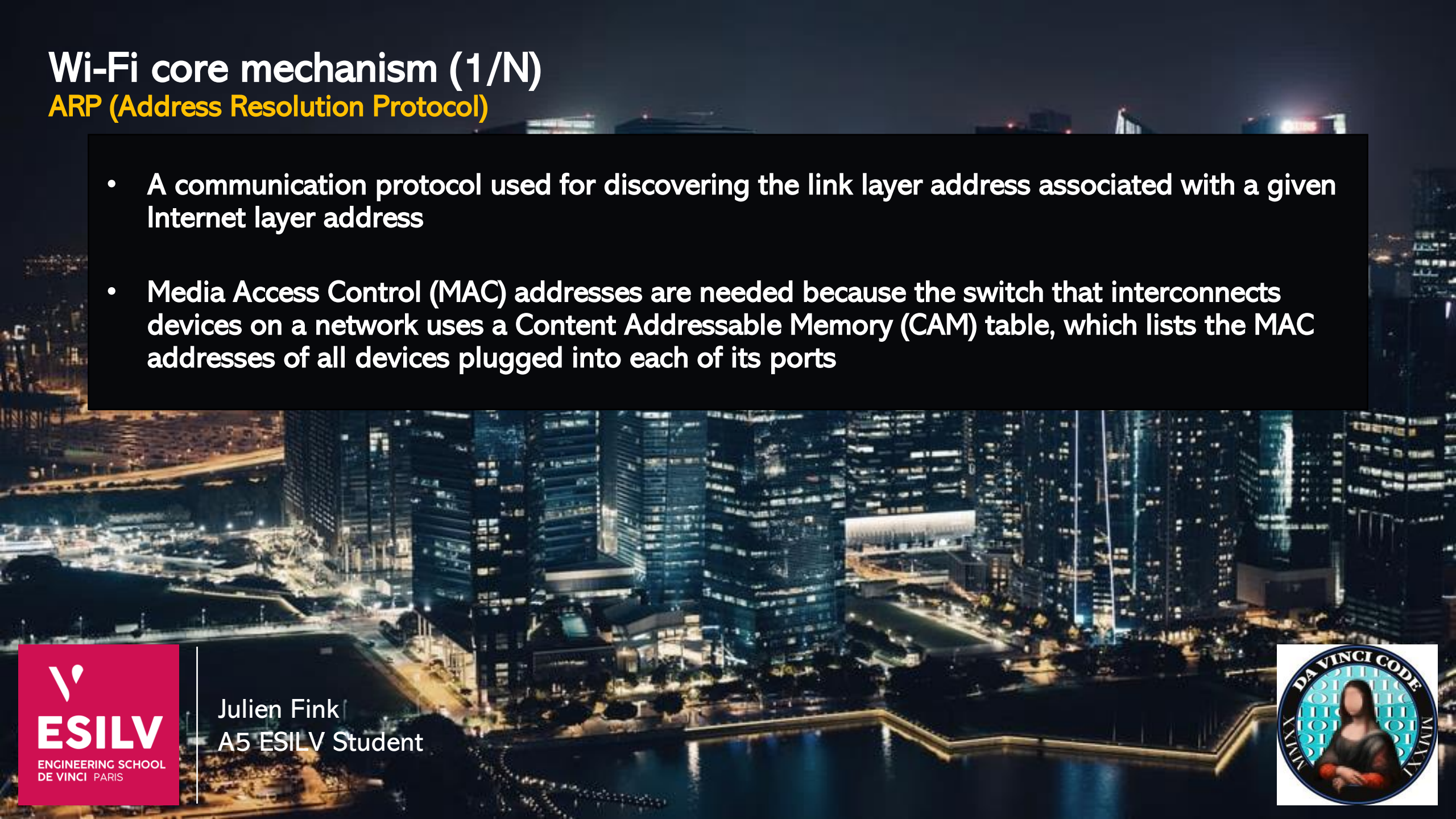
ESILV
ENGINEERING SCHOOL
DE VINCI PARIS

Julien Fink
A5 ESILV Student

Wi-Fi 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

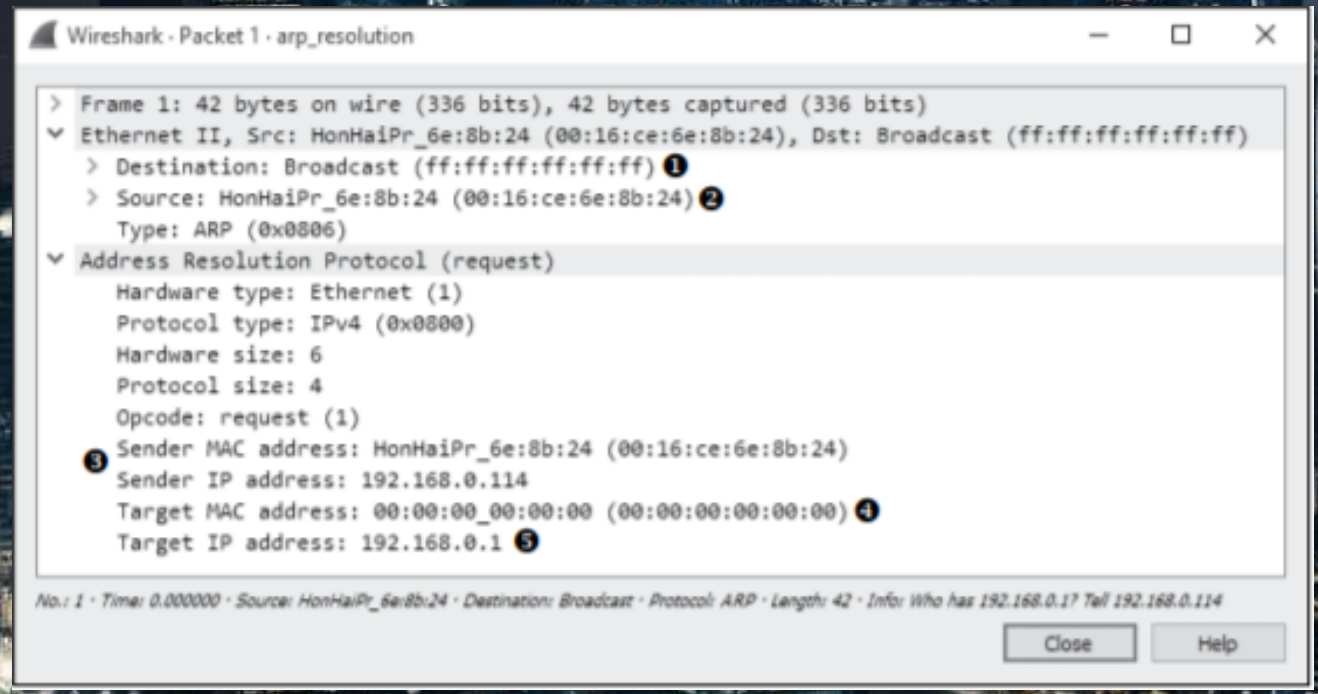


ESILV
ENGINEERING SCHOOL
DE VINCI PARIS

Julien Fink
A5 ESILV Student

Wi-Fi core mechanism (1/N)

ARP (Address Resolution Protocol) - ARP request

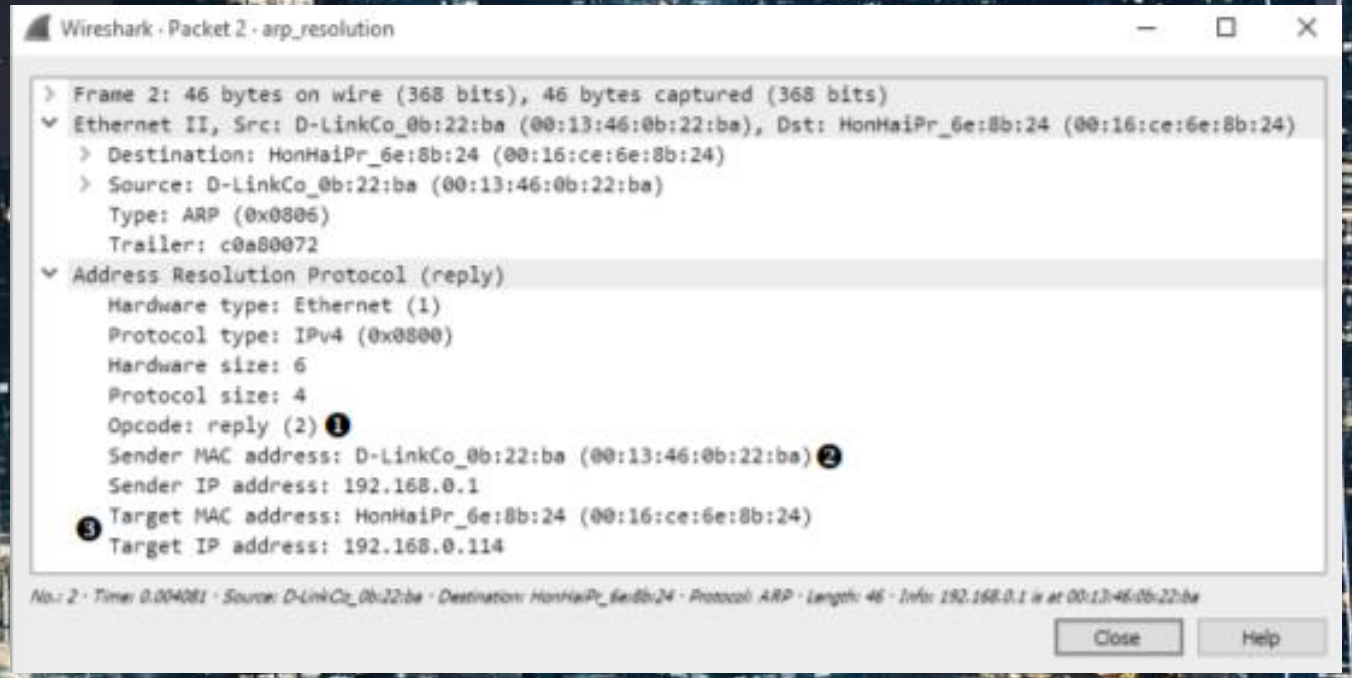


ESILV
ENGINEERING SCHOOL
DE VINCI PARIS

Julien Fink
A5 ESILV Student

Wi-Fi core mechanism (1/N)

ARP (Address Resolution Protocol) - ARP reply



ESILV
ENGINEERING SCHOOL
DE VINCI PARIS

Julien Fink
A5 ESILV Student

Summary

- Wi-Fi definition and presentation
- Core mechanism - protocols overview
- **Security issues**

ESILV
ENGINEERING SCHOOL
DE VINCI PARIS

Julien Fink
A5 ESILV Student

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

ESILV
ENGINEERING SCHOOL
DE VINCI PARIS

Julien Fink
A5 ESILV Student

Useful links

- https://repository.root-me.org/R%C3%A9seau/EN%20-%20Hacking%20wifi.pdf
- https://github.com/koutto/pi-pwnbox-rogueap/wiki/05.-WPA-WPA2-Personal-(PSK)-Authentication
- http://www.c-jump.com/bcc/common/Talk/WlFIconfig/index.html
- https://cylab.be/blog/32/how-does-wpawpa2-wifi-security-work-and-how-to-crack-it
- https://wifi.pressbooks.com/chapter/securite/

ESILV
ENGINEERING SCHOOL
DE VINCI PARIS

Julien Fink
A5 ESILV Student