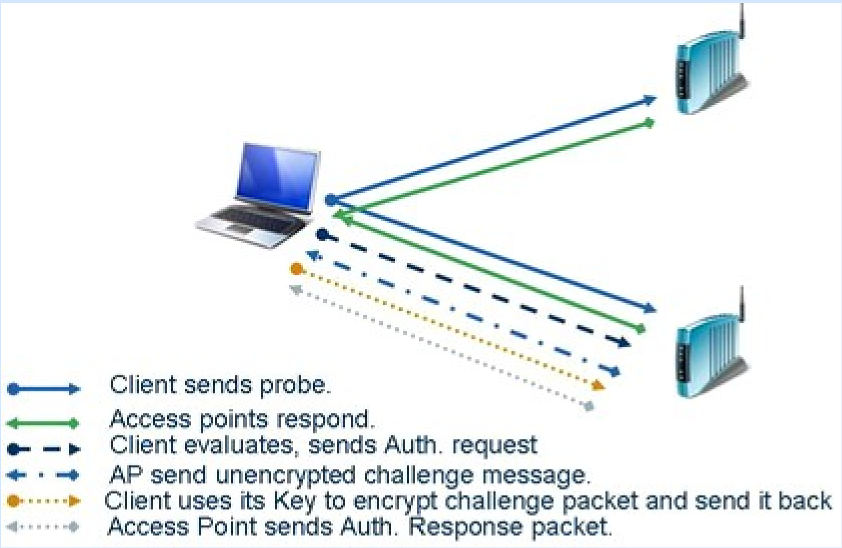
WLAN Security

WEP Overview 1/2

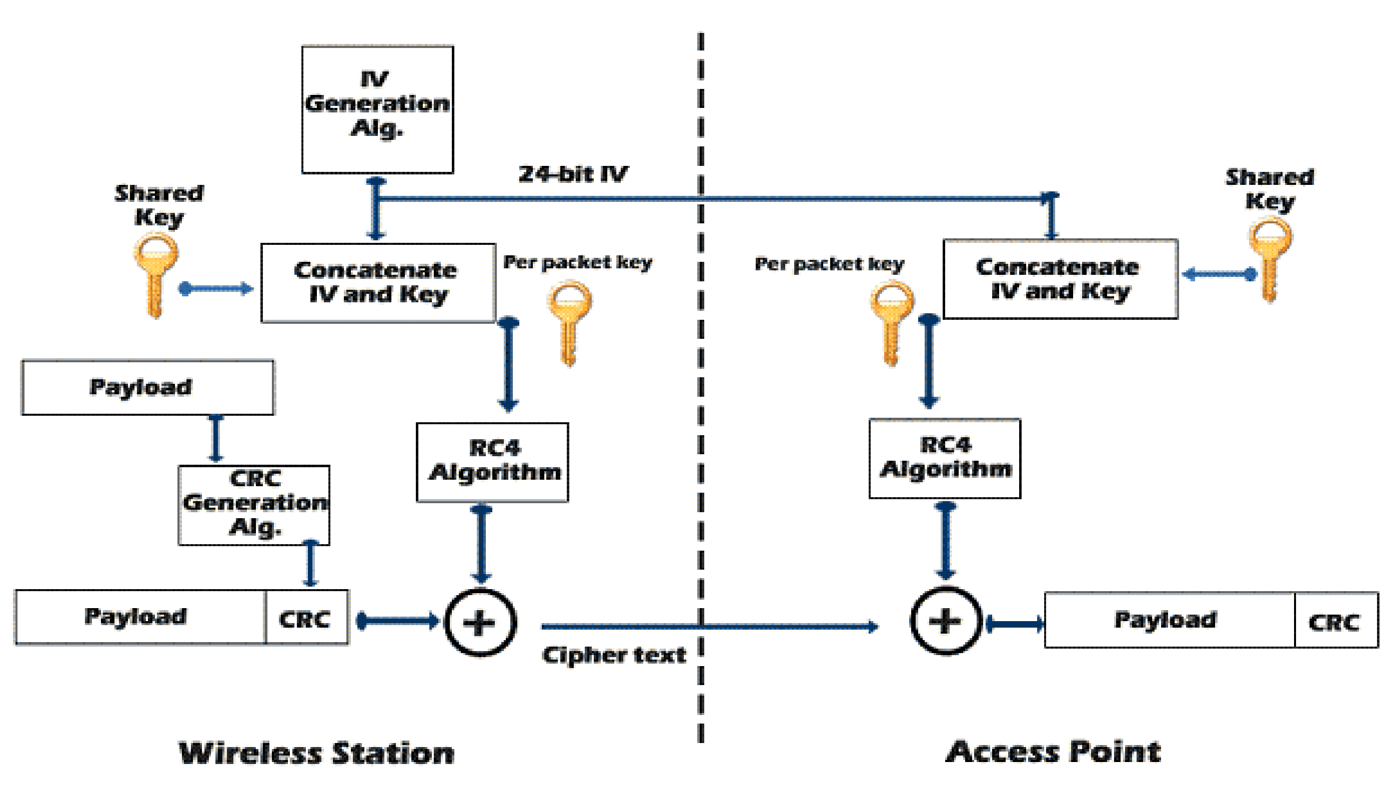
- WEP, Wired Equivalent Privacy
- Introduced in 1999 to provide confidentiality, authentication and integrity
- Includes weak authentication…
  - Shared key
  - Open key (the client will authenticate always)
- …and encryption mechanisms
- Now deprecated



Shared key authentication

WEP Overview 2/2

- **WEP algorithms (between client and AP):**
  - RC4 stream cipher for encryption purpouses
    - WEP-40: 40 bit key + 24 bit of IV (changed on every pkt and sended in clear)
    - WEP-128: uses a 128 bit key (Vendor's "de facto" standard)
  - CRC-32 as Integrity Check (IC) value



WEP Weakness

- Key management…
  - Not specified
  - Key long-lived and of poor quality (e.g. use of single key)
- …and size
  - In 1997 40-bit keys were considered reasonables, but now…
- Initialization Vector (IV) too small
  - IV reuse is a problematic issue: incremental or random
- Integrity Check Value (ICV) not appropriate
- Weak use of RC4 algorithm
  - Fluhrer attack, weak keys
- Authentication messages can be easily forged

IV based weakness

- WEP's IV size: 24 bits. About over 16 millions of keystreams per key, but …
- …the reuse of an IV make easy to found a keystream
  - Starting from 0 and increasing IV for each pkt
  - IV randomly choose: 50% chance of reuse after less 5000 pkts
- Having a keystream, you don't know the WEP key to decrypt pkts with the same IV:

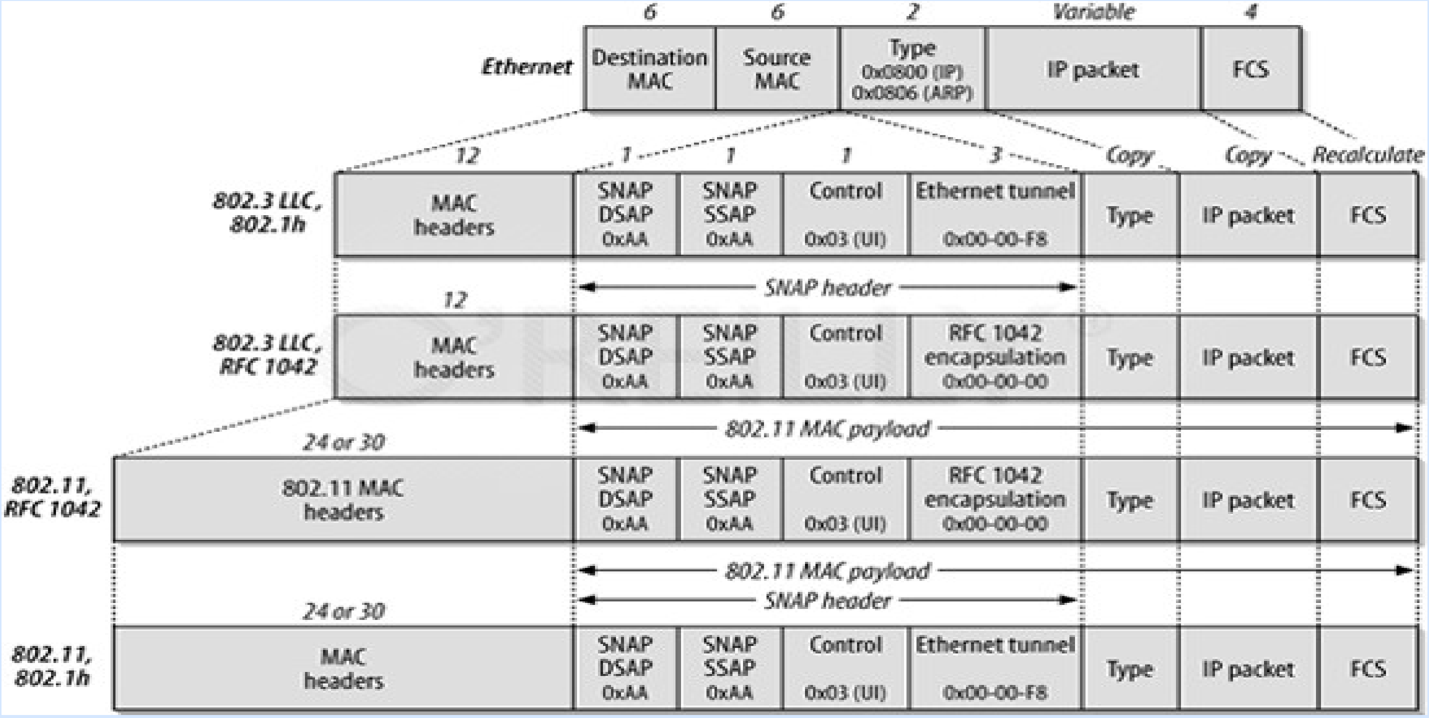
$$C_1 \text{ XOR } C_2 = P_1 \text{ XOR } P_2$$

- Having a keystream is trivial
  - E.g. by sending on wlan a known pkt

FMS attack 1/2

FMS: Fluhrer - Mantin - Shamir

- **Statistical passive attack that aims the reconstruction of the WEP secret key from a number of collected encrypted messages**
- **An attacker knowing the *m*th byte of the keystream can derive the (*m+1*)th byte due to a weakness in the PRNG used to generate the keystream**



FMS attack 2/2

FMS: Fluhrer - Mantin - Shamir

- **Fluhrer, Mantin and Shamir found a class of RC4 keys called "weak keys" (due to weak IV)**

$$\mathbf{IV_{weak}: (A+3,\ N-1,\ X)}$$

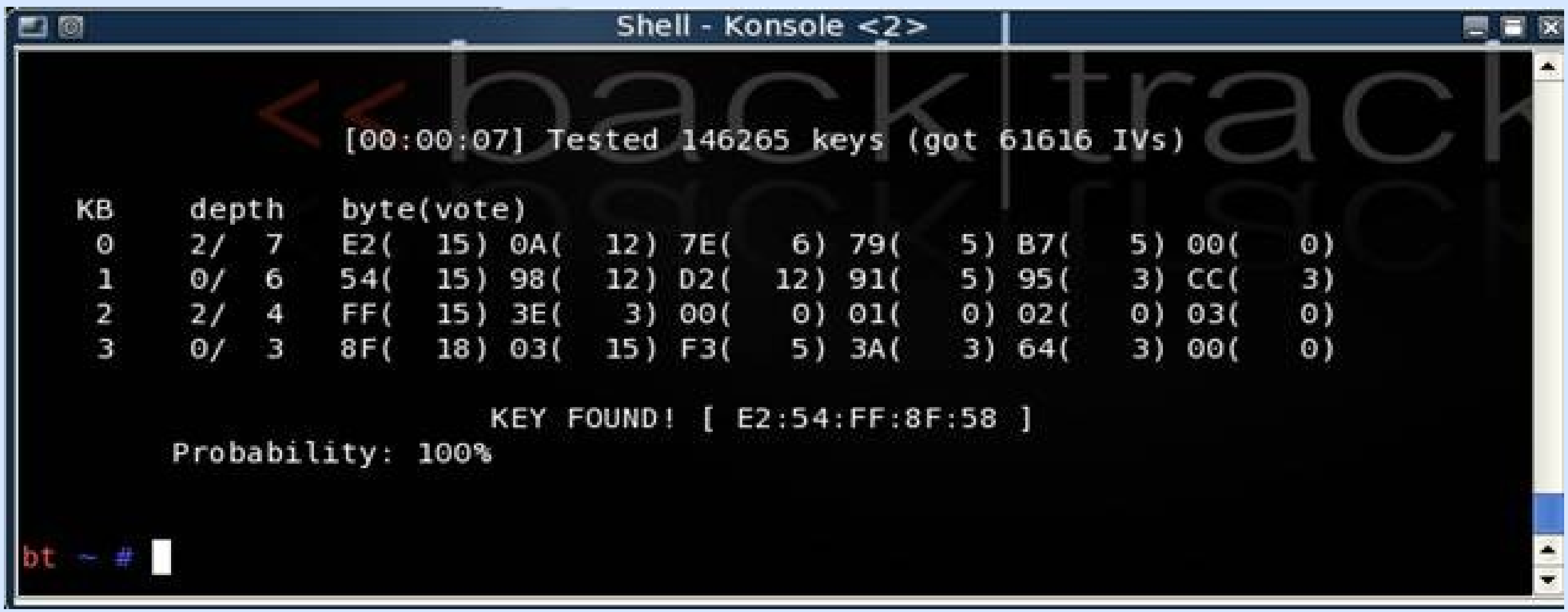
- **If the first 2 bytes of enough key stream are known -> The RC4 key is discovered with a chance of 5% analysing 1 IV…**
- **…observing 60 IV the probability to found the WEP key is 50%**
- **Most of WEP cracking tools implement this attack**
  - **Recovers key after 20,000 packets = 11 seconds**

REFERENCES: S.Fluhrer, I.Mantin, A.Shamir, ***"Weakness in the key scheduling algorithm of RC4"***

WEP cracking

AIRCRACK-NG[1]**: set of tools used to attack a WEP-protected WLAN**

- **Airmon-ng: activate monitor mode**
- **Airodump-ng: capture and save 802.11 frames**
- **Aircrack-ng: cracking a WEP key**
- **Aireplay-ng: packet injection**



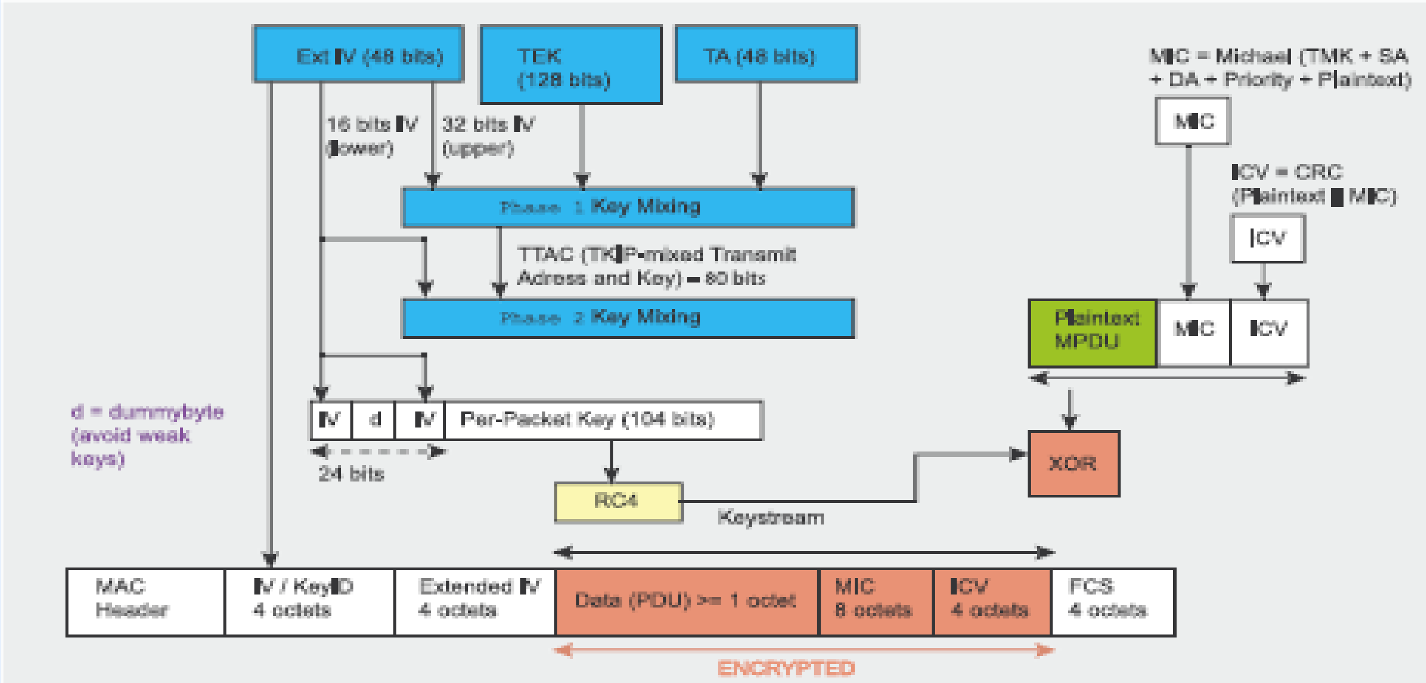
[1] ***http://aircrack-ng.org/***

WPA: Wireless Protected Access

- Subset of standard IEEE 802.11i (also known as WPA2)
- Solution created to substitute WEP and intended as intermediate security platform
  - Between WEP and 802.11i formalization
  - Hardware backward compatibility
- Designed to be used with 802.1X authentication server (WPA Enterprise)
  - Distributes different keys to each user
- Can be used in less secure pre-shared key (PSK) mode (WPA Personal)
  - Weakness of WPA
- Data encrypted with RC4 with 128 bit key
  - 48 bit IV

WPA improvements

- Temporal Key Integrity Protocol (TKIP)
  - Major improvement over WEP (Modification of WEP protocol, but not substitution)
  - Dynamically changes key as system is used (Per-packet Key)
  - Combined with larger IV, this defeats well known attacks
- Improved payload integrity vs. WEP
  - Uses more secure message integrity check (MIC) known as Michael, designed as a compromise between security and backward compatibility with WEP HW



WPA weakness and cracking

- **Fundamentally much harder to crack than WEP**
- **Weakness still lies in the key: WPA-PSK**
  - **Possible to passively intercept initial authentication messages then use an offline dictionary attack to find password**
- **Could allow DoS attacks (De-authentication)**
- **Counter-measure: use of strong password (e.g. Alice APs)**

Use of Aicrack-NG tools

- intercept handshake
- cracking PSK
- de-authenticate clients

IEEE 802.11i Features

Introduces fundamental changes as separating user authentication from enforcing message integrity and privacy, thus providing a robust and scalable security architecture

- Robust Security Network (RSN): use of 802.1X auth, robust key distribution, new integrity and privacy mechanisms
- Backward compatibility: Transitional Security Network, both RSN and WEP systems can participate (…remember WPA)

Communication Context

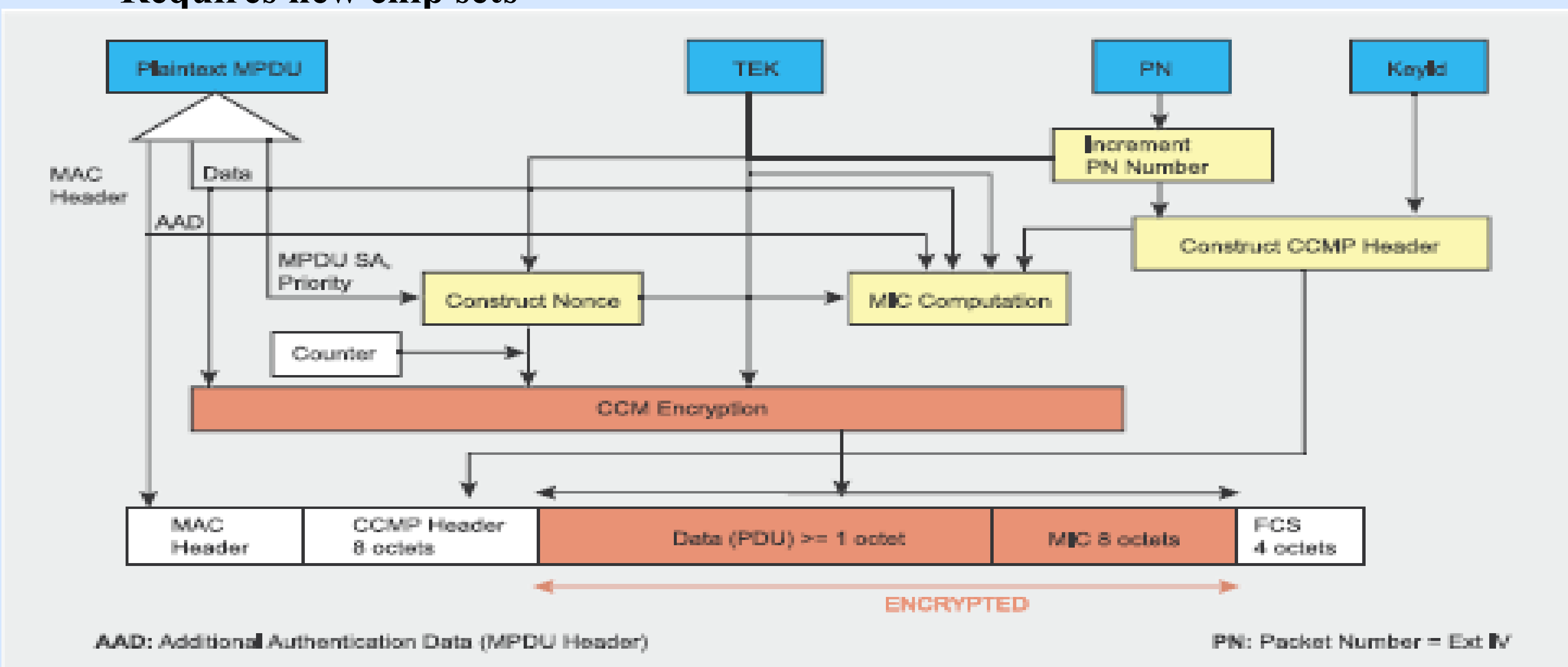
- Agreeing on the security policy: PSK/802.1X, TKIP/CCMP
- 802.1X Authentication
- Key hiearchy and distribuition
- Data confidentiality and integrity

UNIVERSITA' degli STUDI di ROMA TOR VERGATA

WPA2 Algorithms

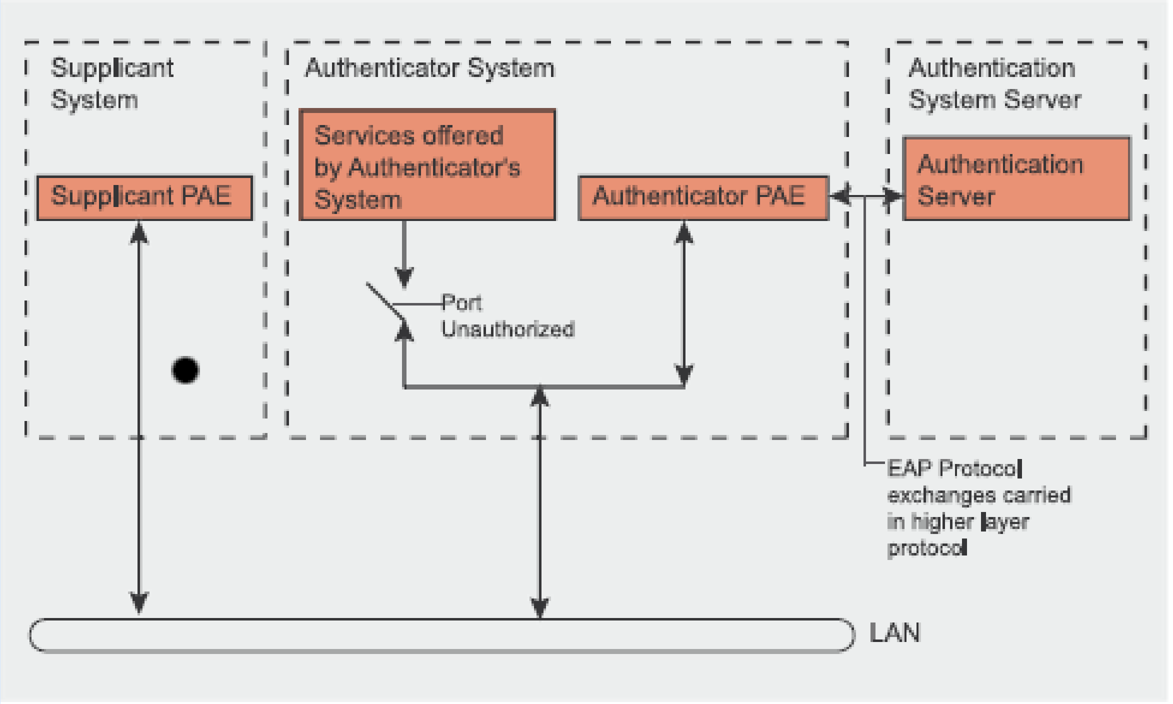
University of Rome "Tor Vergata"
Department of Electronics Engineering
NETWORKING GROUP

- CCMP: Counter-Mode / Cipher Block Message
- Uses Advanced Encryption Standard algorithm (AES)
  - Variable key sizes of 128, 192 and 256 bits
  - Much harder to decrypt than WPA or WEP
- Not compatible with legacy devices
  - Requires new chip sets



802.1X Authentication

The IEEE 802.1X authentication protocol (also known as *Port-Based Network Access Control*) is a framework originally developed for wired networks, providing Authentication, authorisation, key distribution and access control.

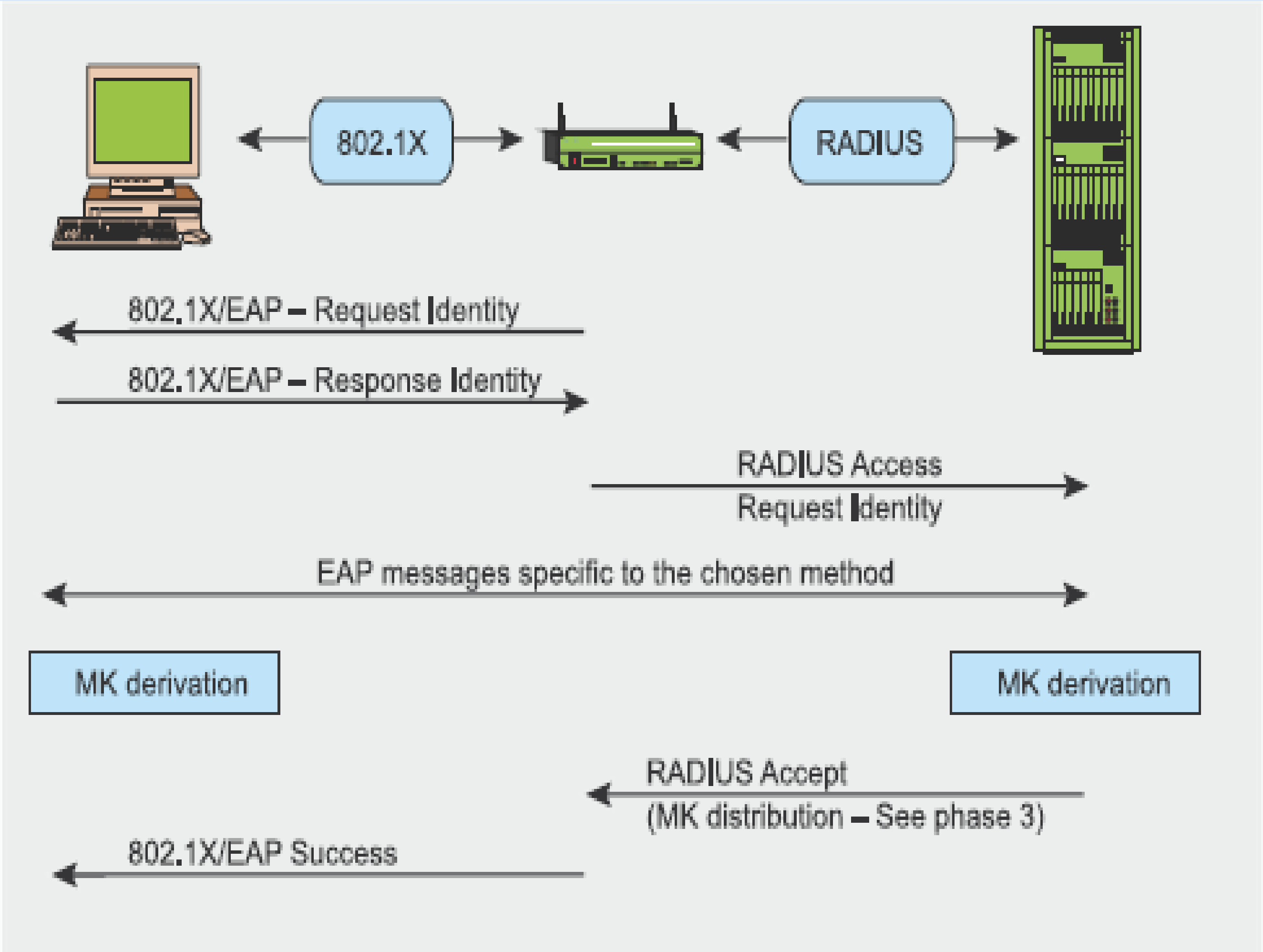


Entities:

- **supplicant joining the network**
- **Authenticator providing access control**
- **Authenticator server making authorization decisions**

Physical port divided into two logical ports making ud the PAE (Port Access Entity)

802.1X and WLAN



- Physical port -> logical association
- Supplicant and authenticator (AP) communicate using an EAP-based protocol
- At the end both entities (i.e. supplicant and auth server) have a secret master key