IEEE 802.11

Ibéria Medeiros

Departamento de Informática

Faculdade de Ciências da Universidade de Lisboa

IEEE 802.11 at a Glance

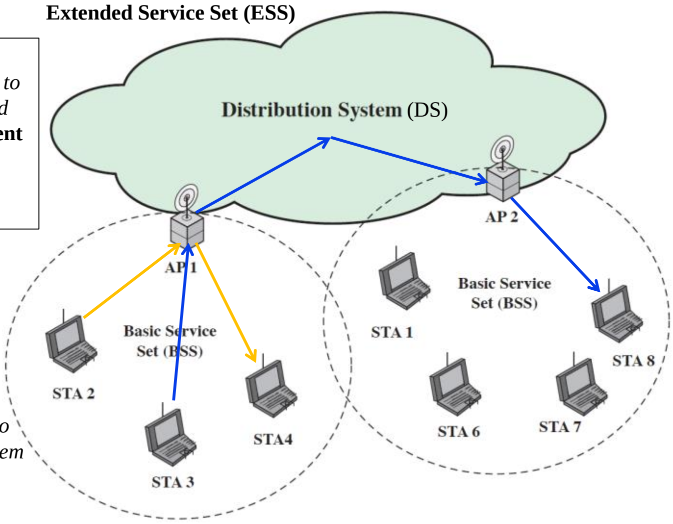
- IEEE 802.11 started to be defined in the mid-1990 for local area wireless communication
- It is compatible to Ethernet above the data link layer, meaning that an IP packet could be sent through wireless LAN the same way as Ethernet
- The standard had several versions through time

802.11	Date	Data Rate (Mbps)	Freq. (GHz)	Mod.
–	1997	1 - 2	2.4	FHSS
a	1999	6 -54	5	OFDM
b	1999	5.5 - 11	2.4	DSSS
g	2003	6 - 54	2.4	OFDM
n	2009	15 - 150	2.4, 5	OFDM
ac	2013	Up to 867	5	OFDM
ad	2012	Up to 6,912	60	OFDM
ay	*2019*	*Up to 20,000 (20GBits/s)*	*60*	*OFDM*

Architecture: IBSS, BSS, ESS

• *If there is* ***no AP****, and the stations communicate directly to each other, then we have an Ad hoc Network or an* **Independent Basic Service Set (IBSS)**

• *There is no routing or forwarding support*



The stations use the AP to communicate between them

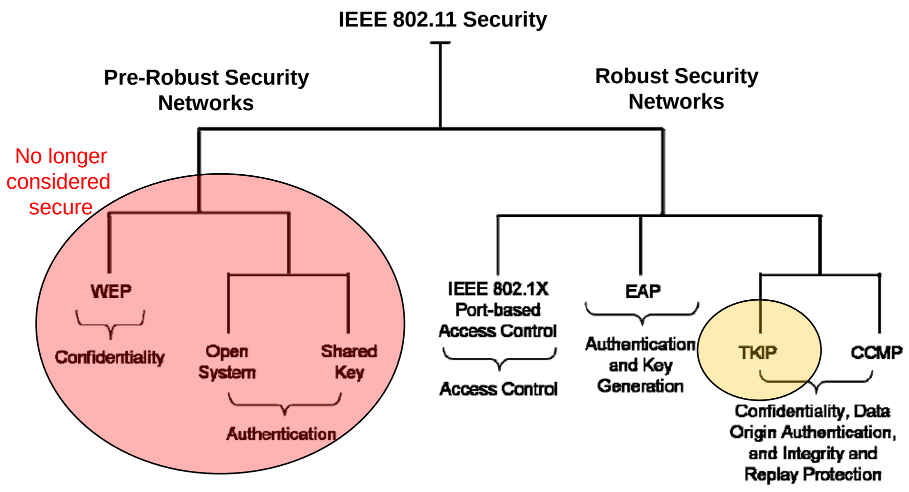
Security in 802.11 : Objectives

- Security objectives
  - **Confidentiality**: ensure that communication cannot be read by unauthorized parties
  - **Integrity**: detect any intentional or unintentional changes to data that occur in transit
  - **Availability**: ensure that devices and individuals can access a network and its resources whenever needed
  - **Access Control**: restrict the rights of devices or individuals to access a network or resources within a network.

Security in 802.11 : Threats

- Main threats
  - simpler access to the media, as the adversary only needs to be in range of the STA and AP to be able to **listen** and **inject** packets
    - » moreover, with highly sensitive directional antennas it is possible to extend the range of the wireless LAN beyond the standardized range
  - weak configurations in many deployments to favor convenience
- Example threats
  - DoS
  - eavesdropping (e.g., passively listens to the traffic)
  - man-in-the middle (e.g., with a rogue AP)
  - masquerading (e.g., impersonates an authorized user)
  - message modification (e.g., deletion, changes, reordering, adding)
  - message replay
  - traffic analysis (e.g., identify communication patterns and participants)

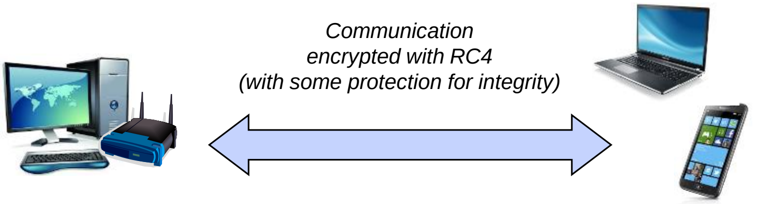
Security in 802.11: Overview of Security Mechanisms



PRE-ROBUST SECURITY NETWORKS

Background: Wired Equivalent Privacy (WEP)

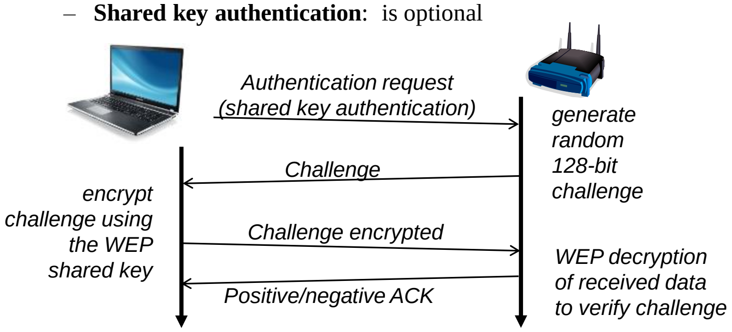
- WEP was the *first* IEEE 802.11 security solution, with the objective of providing at a lower-layer a similar level of trust that is put in wired communication



- In the beginning, typically the **same key** was used to protect the communication between the AP and all (mobile) hosts
- Later on, multicast communication is protected with the **same key**, and point-to-point communication with a **private AP to node key**

WEP Access Control and Authentication

- An external key management system is responsible for setting up the shared key
- The standard defines two modes of authentication
  - **Open system authentication**: basically **no** authentication, as the STA only needs to provide the SSID (Service Set Identifier) of the AP and its MAC address; the AP decides if it accepts the request based on some access control rule on the MAC address (called *MAC address filtering*)
  - **Shared key authentication**: is optional



(Some) Authentication Issues

- **MAC-based access control**: the AP keeps a list of acceptable MAC, which is rather limited since MAC can be easily listen and then forged
- **Unilateral authentication**: only the stations authenticates (**not the AP**)
- **Recovery of key sequence during authentication**: attacker listens to the challenge request and response, XORs the two and obtains the key sequence; then, she attempts to authenticate as the user, and generates the response by XOR the key sequence with the received challenge (*see next slide*)

- Others
  - **Brute force or dictionary attacks**: clear and encrypted challenge allows for this attack
  - **Same or small number of WEP keys**: typically, very few (or just one) key is used, which complicates accountability and facilitates malicious attacks

WEP Encryption

- Packet generation algorithm

Key { K – secret key (40 or 104 bits)
IV – initialization vector, typically different for each packet (24 bits)
IV.K – effective key to encrypt the packet (64 or 128 bits) }

cksum() – checksum algorithm (non-cryptographic CRC with 32 bits)
RC4(X) – RC4 stream cipher encryption algorithm with key X
M – message to be transmitted in the packet

Encrypted packet: $C = (M \,.\, cksum(M)) \oplus RC4(IV.K)$

Packet sent to the network: IV.C

Decryption and integrity verification: *simply apply the same steps in reverse*

(Some) Encryption Issues

- **Fluhrer, Mantin, and Shamir attack**: allows the recovery of the key by looking at the exchanged messages (namely the IV value)
- **Retrieve plaintext**: if a packet is captured and the adversary know the plaintext (e.g., well known values in the headers), then she can retrieve the plaintext of a second message later on when the IV is re-used (and sometimes the IV is static or reset to 0 for each new connection)
- **Replay attacks**: there is no replay protection on encrypted data, and therefore packets can simply be re-send
- **Integrity protection**: the checksum is calculated using a normal reliability integrity algorithm (not a cryptographic one); this algorithm is vulnerable to bit-flips attacks, even if it is encrypted (recall that encryption with RC4 does an XOR)
- **Network traffic analysis**: gain information just by looking at the size of packets and the interval of time between them

(Some) Other Security Issues

- **Factory set AP passwords**: AP management functionalities are protected using default passwords
- **Key refresh**: since keys are manually setup, there is no refresh in most cases
- **DoS attacks**:
  - air medium is vulnerable to interference
  - management frames are not integrity protected, implying that the attacker can send dissociation frames

ROBUST SECURITY NETWORKS

Wi-Fi Protected Access (WPA, WPA2 and 802.11i)

- **IEEE 802.11i** is a standard that specifies security mechanisms for wireless networks, amending the previous version of the IEEE 802.11 standard
  - it introduces something called a **Robust Security Network (RSN)**, which allows for the creation of **RSN Associations (RSNA)** in a wireless network

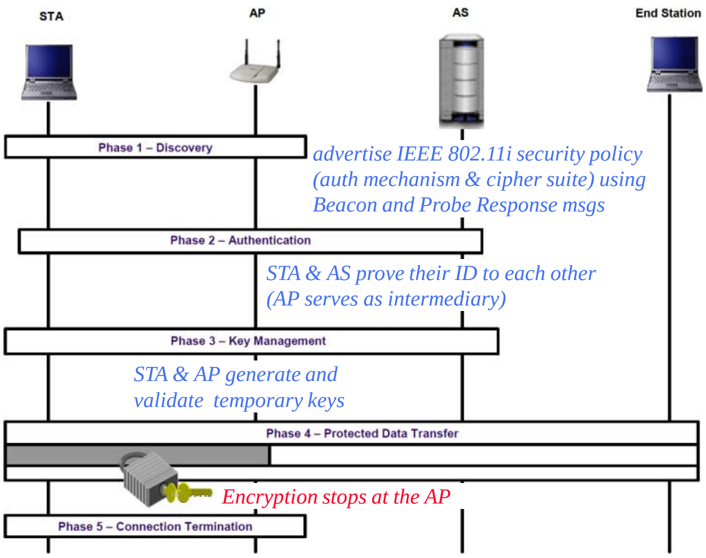
- Wi-Fi Protected Access (**WPA**) was created by the Wi-Fi Alliance to secure wireless computer networks when the WEP problems became impossible to ignore
- WPA implements the majority of the IEEE 802.11i (based on draft version 3), and was intended as an intermediate step to replace WEP while the standard was prepared
- The protocol was designed to work also with most pre-WPA wireless network interface cards through firmware upgrades

- **WPA2** came after 802.11i was introduced, ensuring that equipment is interoperable and implements the mandatory elements of 802.11i

IEEE 802.11i

- IEEE 802.11i defines protocols for
  - **authentication and access control**: uses a *pre-shared key* **or** *IEEE 802.1X specification* (and consequently EAP methods and an AAA server)
  - **key management**: uses a *four-way handshake* and a *group key handshake* mechanism to provide new keys
  - **confidentiality, integrity and data origin authentication**
    - » *Temporal key Integrity protocol (TKIP)*
      - a temporary solution for use with legacy hardware, whose core is based in RC4 and an integrity checksum called Michael
      - it does not provide perfect security, but is better than WEP (e.g., Michael can still be compromised)
    - » *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)*
      - full solution based on the Advanced Encryption Standard (AES)

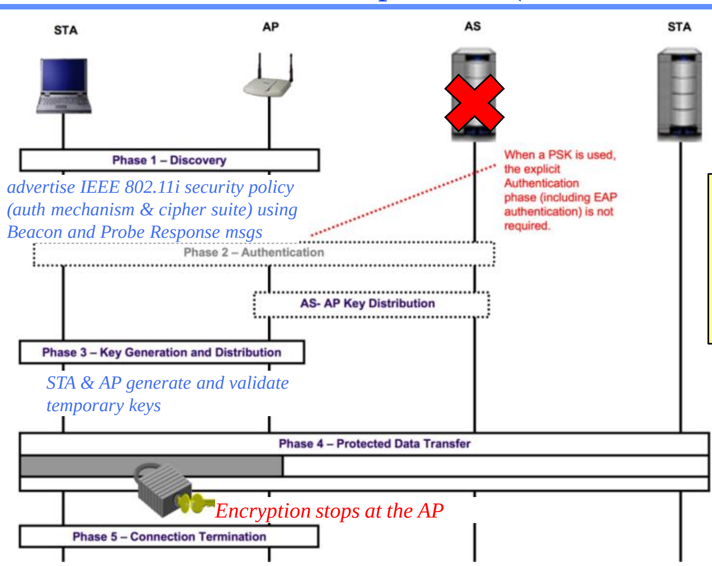
IEEE 802.11i Phases of Operation (with EAP)



AS – Authentication server

NOTES:
- IEEE 802.11i is **only** concerned with security between the STA and the AP
- If the communication between the two stations requires transmission through the DS then higher level protocols have to be employed to guarantee security

IEEE 802.11i Phases of Operation (with Pre-Shared Key)

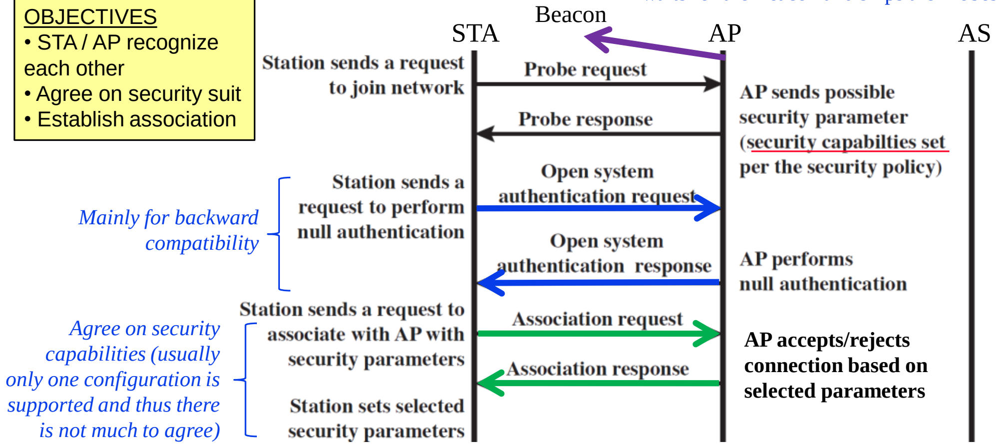


NOTES:
- often, all STA have the same pre-shared key
- therefore, a valid auth means that STA belongs to an authorized group

Discovery

NOTE: either 1) Probe request/response is actively performed, or 2) the STA simply waits for the Beacon and skips the Probes

OBJECTIVES
- STA / AP recognize each other
- Agree on security suit
- Establish association



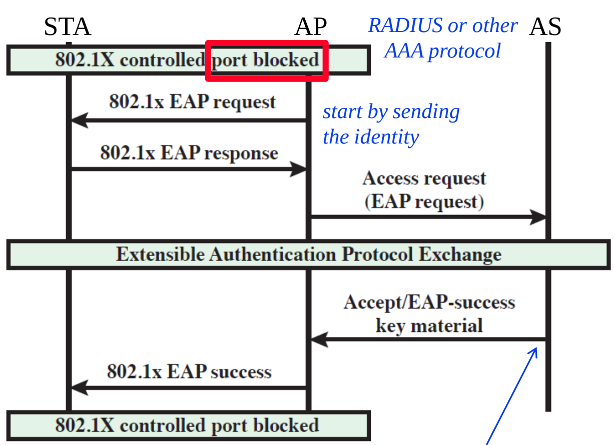
Authentication & key management: IEEE 802.1X; Pre-shared key; *vendor specific*

Confident & integrity: WEP with 40 or 104-bit keys; TKIP; CCMP; *vendor specific*

Authentication

- Ensures **mutual authentication**
- Based on the Extensible Authentication Protocol (EAP) of the **IEEE 802.1X**
- The AS typically resides in another host, but it could also be collocated at the AP
- The **"control port"** is used for access control, preventing the STA from contacting other hosts but the AS; it is unlocked when temporal keys are installed

- With a **pre-shared key** there is *no need* to perform this step because the authentication is obtained implicitly

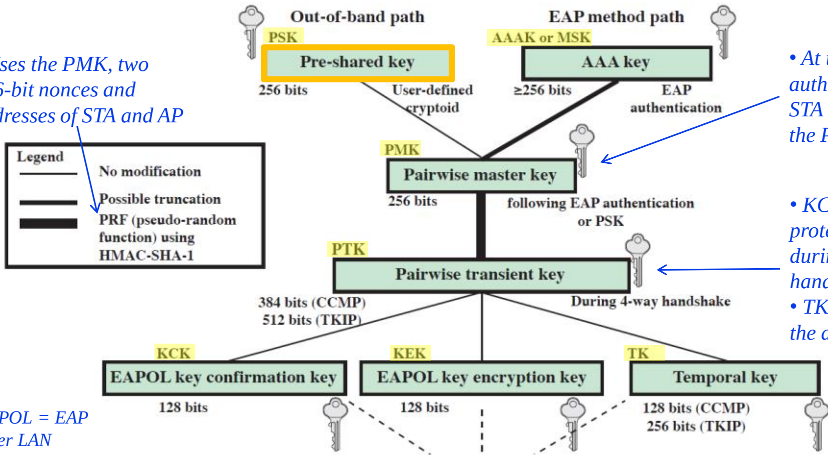


*Generates the **Master Session Key (MSK)**, also known as the **Authentication, Authorization, and Accounting (AAA) Key**, which is then securely transmitted to the AP and STA*

Key Management

- During this phase, several keys are produced and distributed through the STA
  - **pairwise keys**: for communication between the STA & AP

• *Uses the PMK, two 256-bit nonces and addresses of STA and AP*



• *At the end of the auth phase both STA & AP have the PMK*

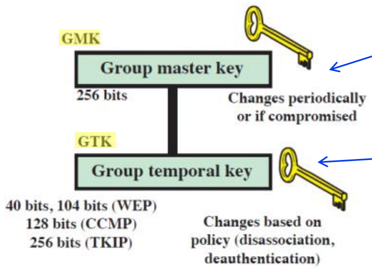
• *KCK & KEK to protect comms during 4-way handshake*

• *TK to secure the actual traffic*

EAPOL = EAP Over LAN

Key Management (cont)

- **group keys**: only needed for multicast / broadcast communication

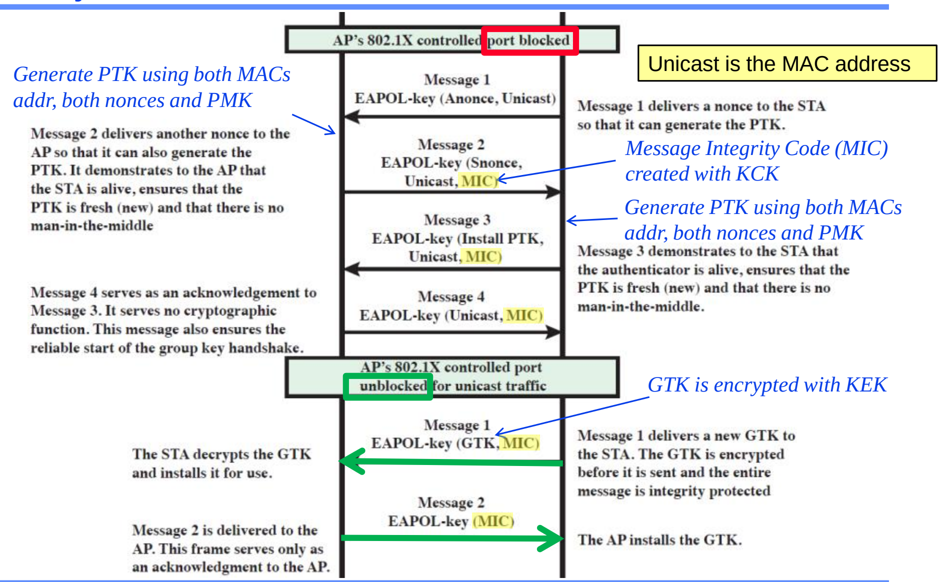


Generated and kept by the AP

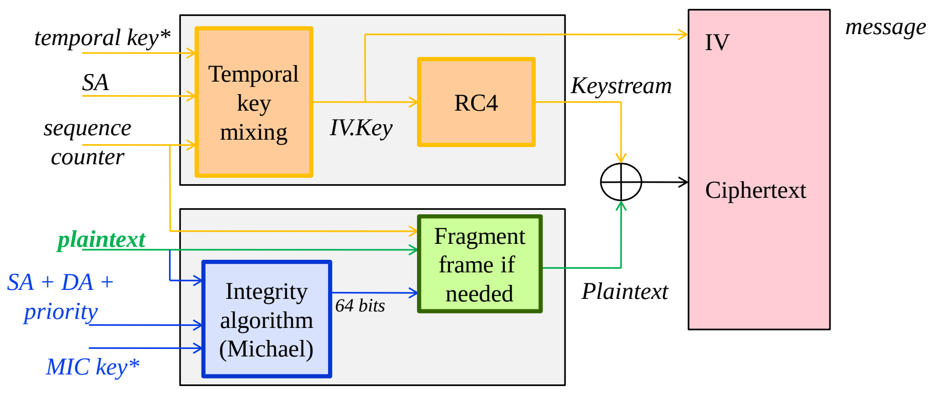
Generated by the AP using GMK and other inputs, which transmits to the STAs using the pairwise keys for protection

- The ***4-way handshake protocol*** is used by the STA & AP to
  - confirm the existence of the PMK
  - verify the selection of the cipher suite
  - derive a fresh PTK

4-Way Handshake



Temporal Key Integrity Protocol (TKIP)

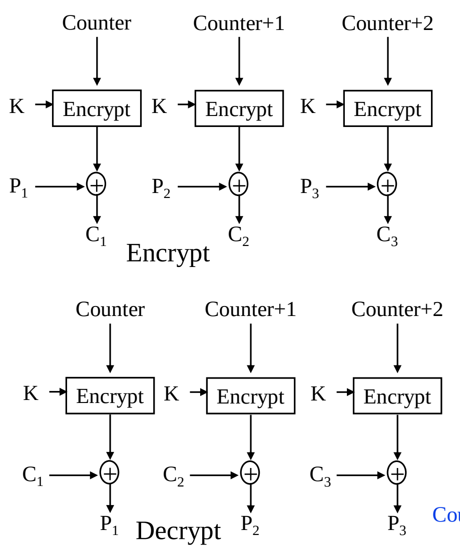


- *temporal key* & MIC key*: the 256-bits of the temporal key is divided to generate these keys*
- *sequence counter : 48-bit counter incremented for each packet (starting with 1)*
- *SA / DA : source and destination MAC address*
- *priority bits : some bits in the IEEE 802.11 header (is reserved for future user)*

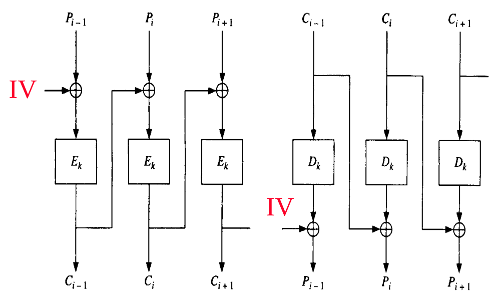
Temporal Key Integrity Protocol (TKIP)

- TKIP provides the following security features for IEEE 802.11 WLANs
  - **Confidentiality protection** using the RC4 algorithm
  - **Integrity protection** against several types of attacks using the Michael message digest algorithm (which is weak but better than WEP checksum)
  - **Replay prevention** through a frame sequencing technique
  - Use of a **new encryption key for each frame** to prevent attacks such as the Fluhrer-Mantin-Shamir (FMS) attack
  - Implementation of **countermeasures** whenever the STA or AP encounters a frame with a MIC error, which is a strong indication of an active attack
    - » logging security events so that they can later on be analyzed
    - » limiting MIC failures: two failures within a 60-second period cause the reception to be disabled for 60 seconds
    - » changing the PTK and GTK
    - » blocking the IEEE 802.1X ports

Review: Counter and Cipher-Block Chaining Modes



Counter Mode



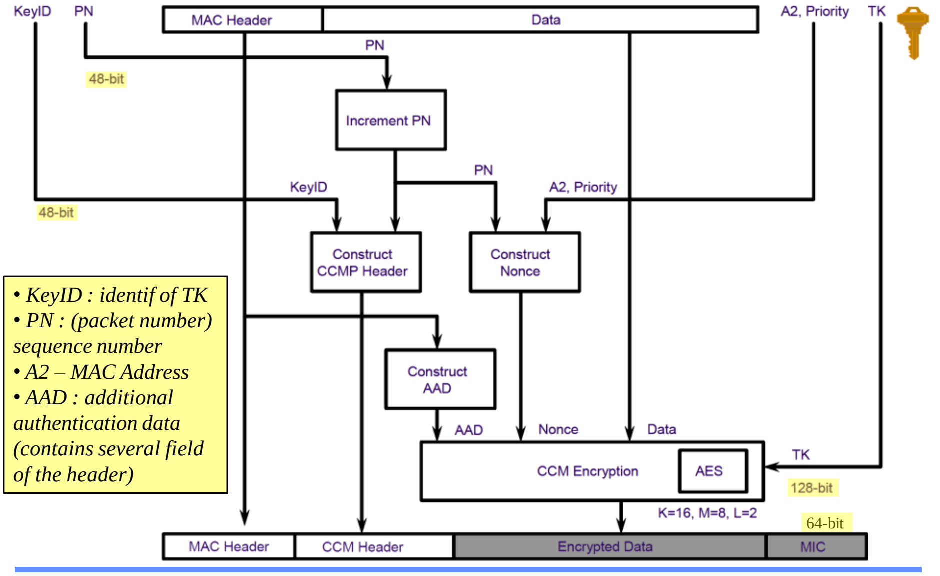
(a) CBC Encryption (b) CBC Decryption

Cipher-Block Chaining Mode

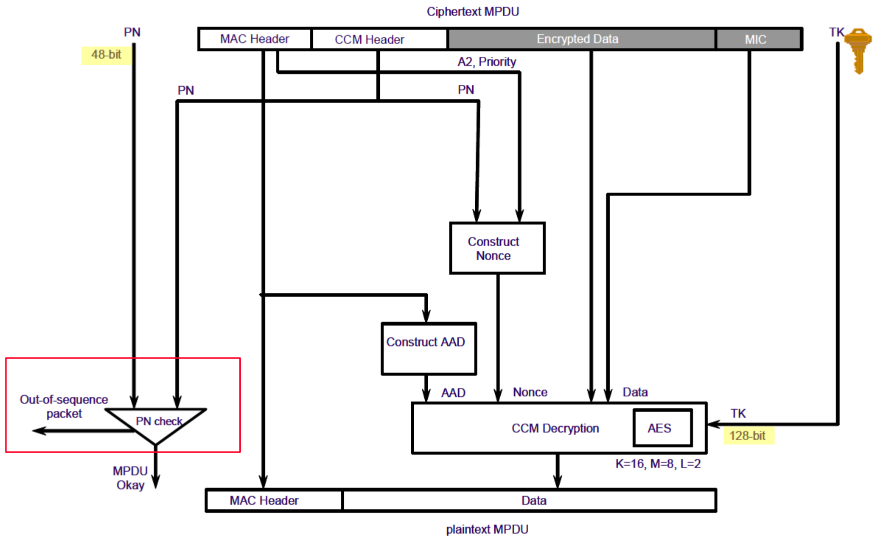
Counter Mode with Cipher Block Chaining MAC Protocol (CCMP)

- CCMP is based in a generic authentication encryption block cipher mode of AES called *Counter with CBC-MAC (CCM)* that uses
  - CTR mode for confidentiality and
  - Cipher Block Chaining MAC (CBC-MAC) for authentication and integrity
- Main characteristics
  - a single 128-bit cryptographic key is used both for confidentiality and integrity to minimize complexity and maximize performance
  - integrity protection of the packet header and packet payload, in addition to providing confidentiality of the payload
  - computation of some cryptographic parameters prior to the receipt of packets to enable fast comparisons when they arrive, which reduces latency
  - small footprint (hardware or software implementation size) to minimize costs
  - small security-related packet overhead (e.g., minimal data expansion due to cryptographic padding and integrity field)

CCMP in Action (Sender Side)



CCMP in Action (Receiver Side)



Bibliography

- W. Stallings, *Cryptography and Network Security: Principles and Practice, Six Edition*, Pearson, 2014 (chap:18 and 16.2 - 16.3)
- *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11*, NIST Special Publication 800-97, February 2007
- S. Aissi et al, *Security for Mobile Networks and Platforms*, Artech House, 2006
- M. Gast, *802.11 Wireless Security, The Definitive Guide (2 edition)*, O´Reilly, 2005 (chap: 5, 6, 7)
- Others:
  - S. Fluhrer, I. Mantin, e A. Shamir, *Weaknesses in the Key Scheduling Algorithm of RC4*, In the 8th Annual Workshop on Selected Areas in Cryptography, Aug. 2001
  - A. Stubblefield, J. Ioannidis, e A. Rubin, *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*, AT&T Labs Technical Report TD-4ZCPZZ, Revision 2, Aug. 2001.