Sicurezza delle reti Wireless

WEP e WPA

Wired Equivalent Privacy

- Nelle reti senza fili, la riservatezza dei dati, e la sicurezza in generale, è un problema particolarmente importante, perché i frame trasportati dalle onde radio possono propagarsi anche all'esterno dell'edificio in cui si trovano le stazioni.
- I difetti delle misure di sicurezza presenti nello standard originale 802.11 sono risultati evidenti solo col tempo. Oggi esistono programmi di pubblico dominio, facilmente scaricabili, che possono essere usati per attaccare le reti senza fili, conformi allo standard originale 802.11, nelle quali i meccanismi di sicurezza sono così vulnerabili che le rendono uguali alle reti prive di protezione.
- Come suggerisce il nome, **Wired Equivalent Privacy** (WEP) è stato pensato per fornire un livello di sicurezza simile a quello delle reti cablate (wired).

Obiettivi del progetto WEP

- Usare la criptografia a chiave simmetrica per:
  - Garantire la Riservatezza dei dati
  - Garantire l'integrità dei dati
  - Autenticare i sistemi terminali

- Criptare separatamente ciascun pacchetto
  - Conoscendo la chiave, un pacchetto può essere decifrato;
  - Si può decifrare un pacchetto anche se il precedente è andato perso (a differenza del cifrario a blocchi concatenati: CBC)
- Efficienza
  - realizzabile in hardware o software

Autenticazione

Il protocollo WEP, incluso nelle specifiche dello standard IEEE 802.11 fu progettato nel 1999 per fornire i servizi di autenticazione e di criptografia dei dati tra un host e un access point (cioè, la stazione base di una rete senza fili), usando un algoritmo a chiave simmetrica condivisa.

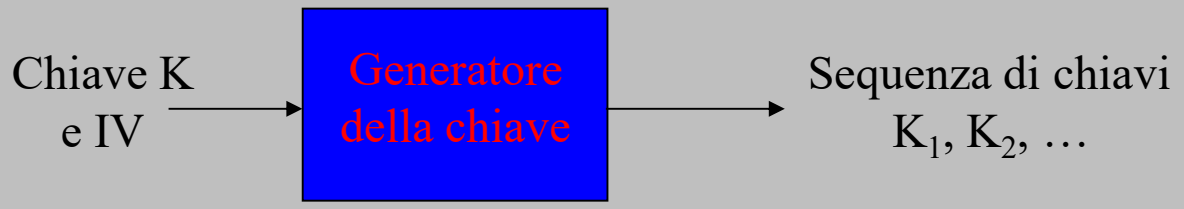
Il WEP non specifica un algoritmo di gestione delle chiavi, quindi si assume che l'host e l'access point abbiano preliminarmente concordato, in qualche modo, la chiave da usare.

L'autenticazione avviene come segue:

a) un host wireless richiede a un access point di autenticarsi.
b) l'access point risponde alla richiesta di autenticazione con un nonce di 128 byte.
c) l'host wireless cripta il nonce usando la chiave simmetrica, che condivide con l'access point.
d) l'access point decripta il nonce che l'host ha criptato.

Se il nonce decriptato corrisponde al nonce originariamente inviato all'host, allora l'host è autenticato dall'access point.

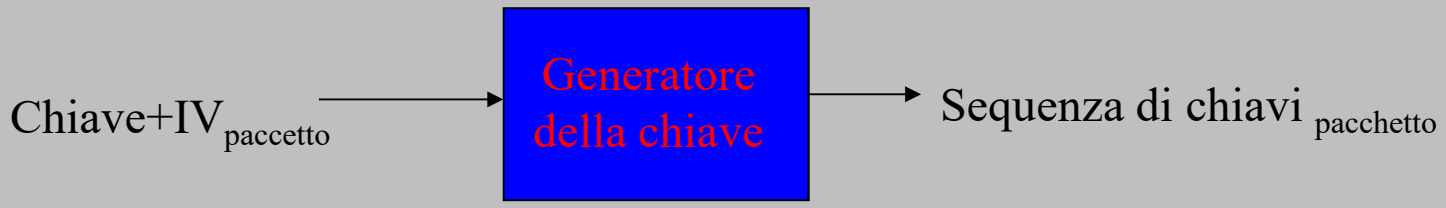
Cifrario a flusso con chiave simmetrica



- *combinare ogni byte della sequenza di chiavi con i byte del testo in chiaro per ottenere il testo cifrato:*
  - IV: Vettore di inizializzazione
  - m(i): i-ma unità del messaggio
  - ks(i): i-ma unità della sequenza di chiavi
  - c(i): i-ma unità del testo cifrato
  - c(i): ks(i) $\oplus$ m(i) ($\oplus$ = exclusive or)
  - m(i): ks(i) $\oplus$ c(i)
- WEP usa l'algoritmo RC4

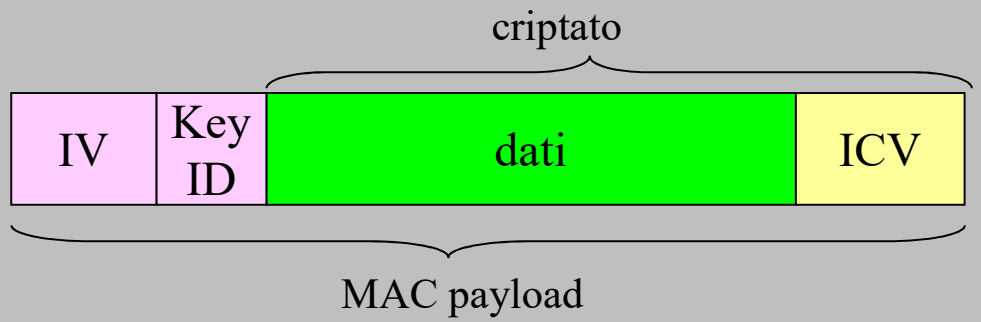
Indipendenza dei pacchetti nel cifrario a flusso

- Uno degli scopi del protocollo è di criptare separatamente ciascun pacchetto
- Se per il frame n + 1 si riprende la sequenza delle chiavi da dove era terminato il frame n, allora ogni frame non è crittografato separatamente dal precedente
  - Bisogna sapere il punto in cui è terminato il pacchetto n
- La soluzione WEP: inizializza il generatore della sequenza di chiavi con la chiave e il nuovo IV per ogni pacchetto:



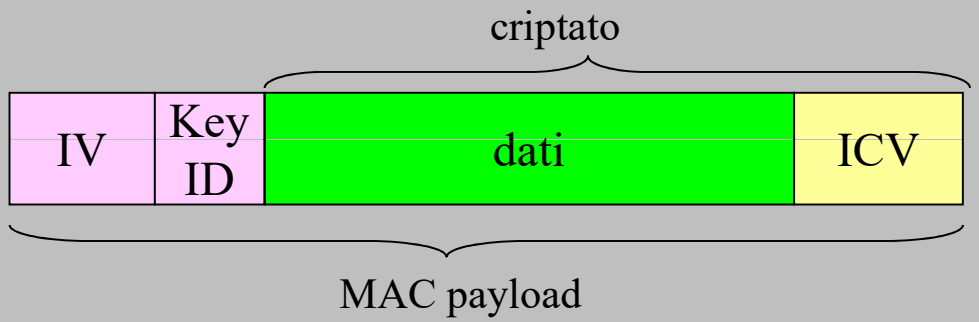
Criptografia WEP (1)

- Il mittente calcola un valore che consente al ricevitore di convalidare i dati ricevuti: Integrity Check Value (ICV)
  - Un codice di quattro byte (hash o CRC)
- Il mittente e il ricevitore condividono una chiave K di 104-bit
- Il mittente crea il vettore di inizializzazione di 24-bit (IV), aggiunge la chiave e ottiene una chiave di sessione di 128-bit che verrà usata per criptare un solo frame.
- Il mittente aggiunge anche un keyID (un campo di 8 bit)
- La chiave di 128 bit costituisce il valore iniziale del generatore di numeri pseudocasuali che genererà la sequenza di chiavi
- I dati nel frame + ICV sono criptati con l'algoritmo RC4:
  - B byte della sequenza di chiavi sono messi in XOR con i byte dei dati + ICV
  - IV + keyID sono aggiunti per criptare i dati che formano il payload
  - Il payload viene inserito in un frame 802.11



Criptografia WEP

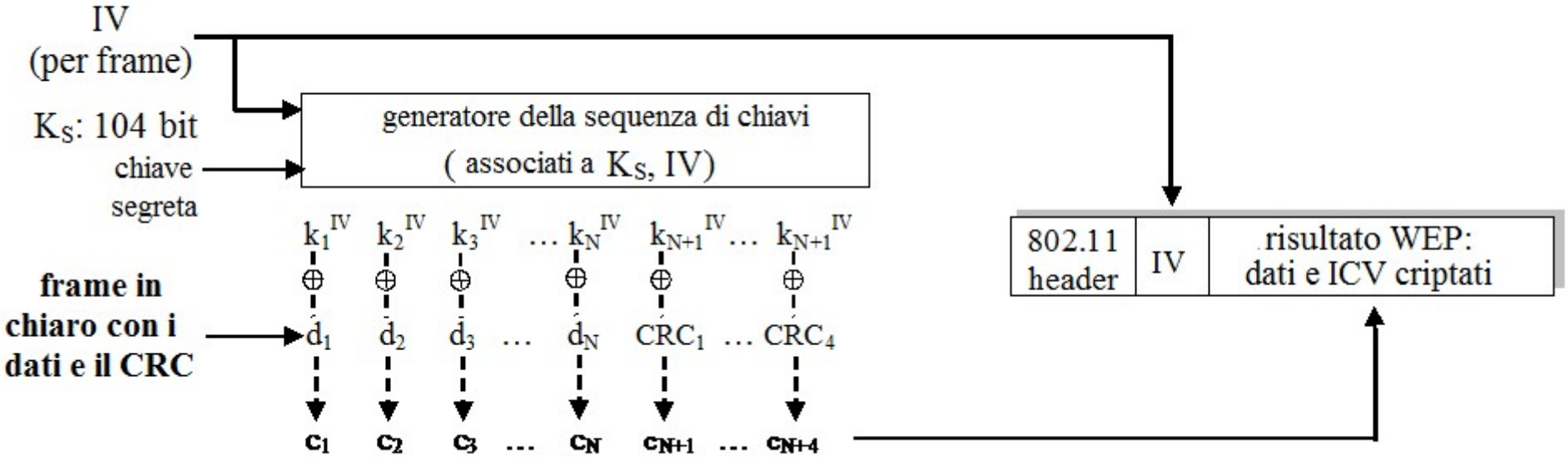
- Il valore di IV cambia ad ogni frame, quindi ciascun frame sarà criptato con una chiave di 128 bit diversa. La criptografia avviene come segue.
- Prima viene calcolato un CRC (ICV) di 4 Byte dai dati del payload.
- Poi, il payload e il CRC vengono criptati con il cifrario RC4.



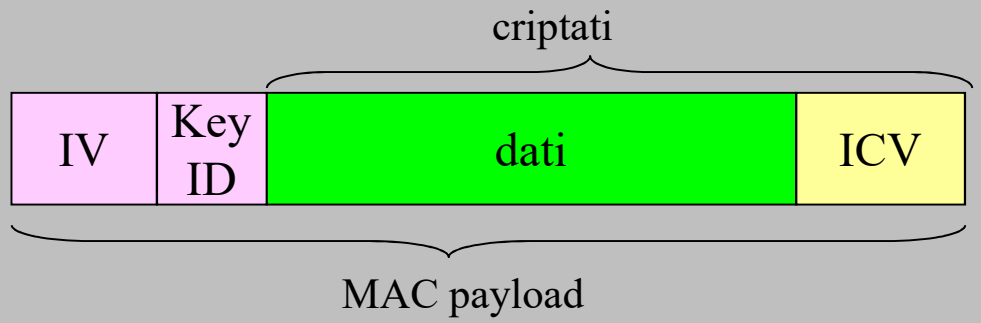
Criptografia WEP

- Non interessa sapere come funziona l'algoritmo RC4, basta sapere che fornendo all'algoritmo RC4 la chiave formata da K_S e IV, questo produce un insieme di chiavi, k_1^{IV}, k_2^{IV}, k_3^{IV}, …, che sono usate per criptare i dati e il CRC di un frame.
- Si può pensare che questa operazione avviene su un byte alla volta.
- La criptografia consiste nell'eseguire l'or esclusivo del byte i-mo dei dati con la chiave i-ma (k_i^{IV}) dell'insieme delle chiavi ottenute dalla chiave di 128 bit. Si ottiene in questo modo un blocco criptato c_i:

$$c_i = d_i \oplus k_i^{IV}$$



Decriptografia WEP



- Il ricevitore estrae IV. Il valore IV cambia da un frame al successivo, ed è trasmesso in chiaro nell'header di ogni frame 802.11 WEP criptato.
- Usa IV e la chiave condivisa come numero iniziale del generatore di numeri pseudo casuali, ottiene la sequenza di chiavi
- Calcola l'XOR della sequenza di chiavi con i dati criptati per decifrare i campi dati + ICV:

$$d_i = c_i \oplus k_i^{IV}$$

- Usa ICV per verificare l'integrità dei dati
  - nota: in questo caso, l'integrità è diversa dal MAC (message authentication code) e dalla firma digitale (che usa PKI).

Debolezza della criptografia WEP

Si supponga che la chiave sia lunga 64 bit:

- L'uso corretto dell'algoritmo RC4 richiede che la stessa chiave di 64 bit venga usata solo una volta. Non ci dovrebbero essere due frame criptati con la stessa chiave. La chiave WEP cambia frame dopo frame.
- Per una data chiave K_S (che non cambia mai, o al massimo viene cambiata raramente), significa che ci sono solo 2^{24} chiavi possibili.
- Se queste chiavi vengono scelte a caso, si può calcolare che la probabilità di scegliere lo stesso valore IV (e quindi la stessa chiave di bit) è maggiore del 99 per cento dopo appena 12000 frame.
- Assumendo che un frame sia lungo 1 Kbyte e la velocità di trasmissione sia 11 Mbps, dopo pochi secondi sono stati trasmessi 12000 frame. Inoltre, poiché il valore IV è trasmesso in chiaro nel frame, un intruso che intercetta i frame sarà in grado di vedere quando viene usato un valore duplicato di IV.

Violare la criptografia 802.11 WEP

- Per vedere uno dei possibili problemi che nasce quando si usa una chiave duplicata, si consideri il seguente attacco di scelta del testo in chiaro, che un intruso compie verso il sito di Alice.
- Si supponga che l'intruso (usando la tecnica dell'IP spoofing) invia una richiesta (ad esempio, HTTP o FTP) ad Alice per ricevere un file del quale conosce il contenuto: d_1, d_2, d_3, d_4, …. L'intruso osserva i dati criptati c_1, c_2, c_3, c_4, …. Poichè $d_i = c_i \oplus k_i^{IV}$, se si applica l'OR-esclusivo ad entrambi i membri di questa uguaglianza, si ha:

$$d_i \oplus c_i = k_i^{IV}$$

- In base a questa relazione, l'intruso può usare i valori noti d_i e c_i per calcolare k_i^{IV}. La volta successiva che l'intruso vede che vengono usati gli stessi valori di IV, sarà in grado di conoscere la sequenza delle chiavi k_1^{IV}, k_2^{IV}, k_3^{IV}, … e quindi riuscirà a decriptare tutti i messaggi criptati.
- Se manca il controllo di integrità, l'attaccante può modificare il contenuto del payload del frame, calcolare il nuovo CRC del frame e far accettare il frame.

Violare la criptografia 802.11 WEP

Carenza del meccanismo di sicurezza:

- IV lungo 24-bit, un IV per frame, -> lo stesso IV potrebbe essere ripetuto
- IV viene trasmesso in chiaro -> si individua un IV ripetuto

attacco:

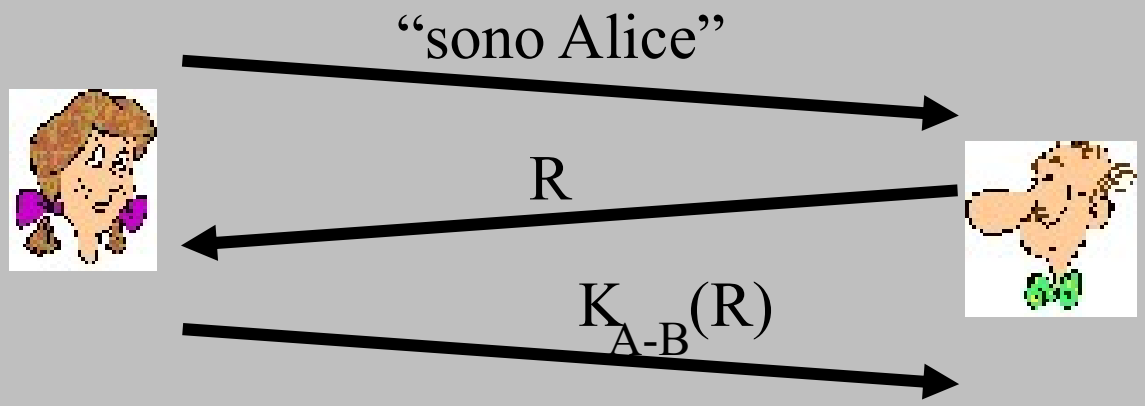
- Trudy costringe Alice a criptare un testo in chiaro di sua conoscenza: $d_1\ d_2\ d_3\ d_4\ \ldots$
- Trudy vede: $c_i = d_i$ XOR k_i^{IV}
- Trudy conosce c_i e d_i, quindi può calcolare k_i^{IV}
- Trudy entra in possesso della sequenza $k_1^{IV}\ k_2^{IV}\ k_3^{IV}\ \ldots$
- Quando verrà usato nuovamente IV, Trudy decripta!

Autenticazione delle parti con il nonce

Nonce: numero (R) usato solo una volta

Per provare che Alice è "presente", Bob invia un *nonce*, R, ad Alice.

Alice deve restituire R a Bob, criptato con la chiave segreta condivisa (K_{A-B})



Bob ha la certezza che non si tratta di un attacco di ripetizione.
Alice è presente, perché solo Alice conosce la chiave per criptare il nonce.

autenticazione WEP

Stazione

Richiesta di autenticazione

Access Point

nonce (128 byte)

Nonce criptato con la chiave condivisa

Richiesta accettata se il valore decriptato è uguale al nonce

Note:

- Non tutti gli AP la richiedono, anche se si usa il WEP
- L'AP indica la necessità di autenticazione nel pacchetto beacon
- Viene fatta prima dell'associazione

802.11i: sicurezza rafforzata

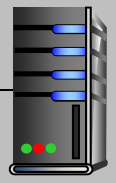
Il protocollo 802.11i

- Introduce numerose (e più robuste) forme di criptografia
- Prevede la distribuzione delle chiavi
- Usa un server di autenticazione separato dall'access point

802.11i: quattro fasi

STA:
Stazione client

AP: access point



AS:
Authentication
server

1 Riconoscimento del metodo di sicurezza

2 STA ed AS si autenticano a vicenda, entrambi
generano una Master Key (MK). *AP agisce da "intermediario"*

3 STA deriva
una Master
Key (PMK) abbinata

3 AS deriva
La stessa PMK,
La invia all'AP

4 STA, AP usano PMK per derivare
La Temporal Key (TK) usata per criptare i messaggi e assicurarne l'integrità

802.11

- Oltre alla stazione wireless e all'access point, lo standard 802.11i definisce un authentication server con cui l'AP può comunicare.
- La Separazione dell'authentication server dall'AP permette:
  - ad un authentication server di rispondere a molti AP,
  - di centralizzare in un solo server le decisioni relative all'autenticazione e all'autorizzazione ad accedere,
  - Si riducono i costi e la complessità dell'AP.

802.11: fase di scoperta

Lo standard 802.11i opera in quattro fasi:

1) **Scoperta**.

   Nella fase di scoperta, l'AP, nei pacchetti beacon, segnala la sua presenza e indica le forme di autenticazione e criptografia che fornisce ai client wireless.

   Il client, quindi, accetta quelle specifiche forme di autenticazione e criptografia. Sebbene il client e l'AP stiano già scambiando messaggi, il client non è stato ancora autenticato né possiede la chiave di criptografia, quindi sono necessari ancora altri passi prima che il client possa comunicare sul canale wireless con un qualsiasi host remoto.

802.11: fase di Autenticazione

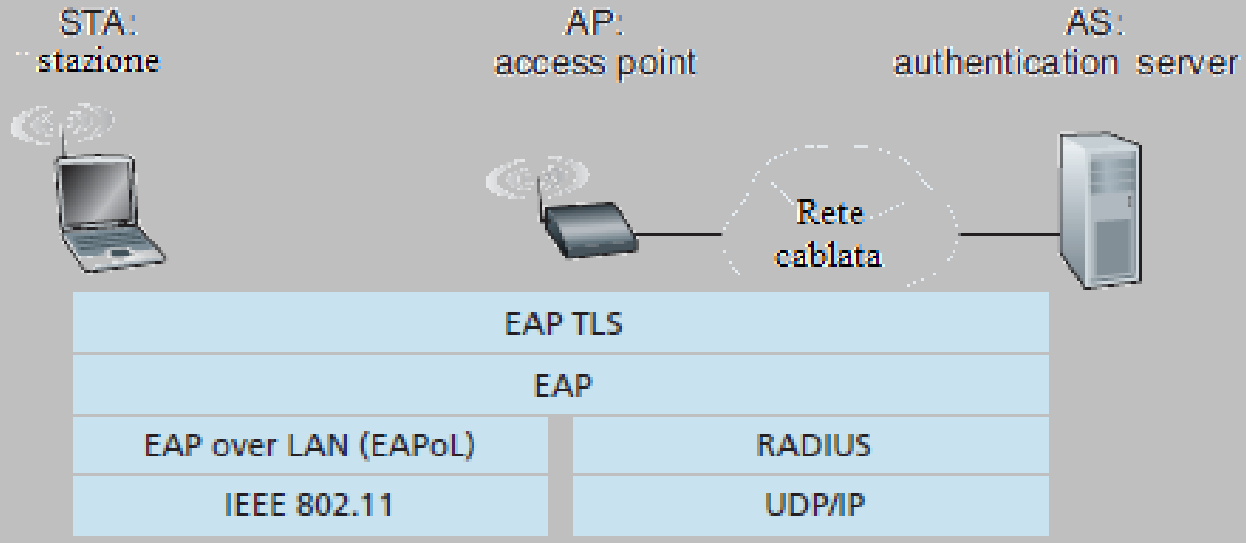
2) **Autenticazione reciproca e generazione della Master Key (MK)**.

   Il processo di autenticazione avviene tra il client wireless e il server di autenticazione. In questa fase, l'access point funziona come intermediario, si limita a consegnare al client i messaggi generati dall'authentication server e viceversa.

   L'Extensible Authentication Protocol (EAP) definisce i formati dei messaggi usati nel modo request/response durante l'interazione tra il client e l'authentication server.

802.11: generazione Master Key

2 La figura mostra che i messaggi EAP sono incapsulati usando EAPoL (EAP over LAN, [IEEE 802.1X]) ed inviati sul canale wireless 802.11. Questi messaggi EAP vengono estratti all'access point, e quindi nuovamente incapsulati usando il protocollo RADIUS per la trasmissione su UDP/IP all'authentication server. Il server RADIUS e il protocollo non sono imposti dal protocollo 802.11i, essi sono componenti standard *de facto* per 802.11i. Il protocollo DIAMETER, recentemente standardizzato, dovrebbe sostituire presto il RADIUS.



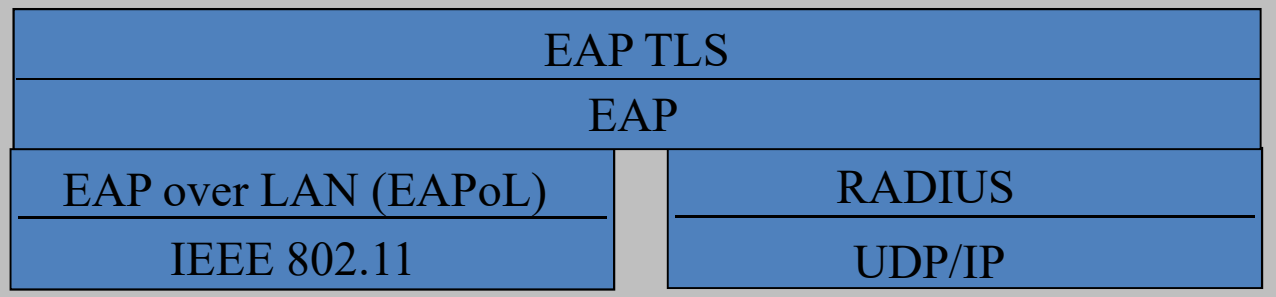
EAP è un protocollo tra sistemi terminali. I messaggi EAP sono incapsulati secondo il formato EAPoL e trasmessi sul canale wireless tra il client e l'access point, e usando RADIUS su UDP/IP tra l'access point e l'authentication server.

802.11: autenticazione e Master Key

2. Con EAP, l'authentication server può scegliere tra vari modi di autenticazione. Lo standard 802.11i non impone un particolare metodo di autenticazione, si usa, comunque, lo schema di autenticazione EAP-TLS.
   EAP-TLS usa la criptografia a chiave pubblica (incluso il nonce criptato e il message digest) per consentire al client e all'authentication server di autenticarsi reciprocamente, e derivare una Master Key (MK) che sarà nota a entrambe le parti.

EAP: extensible authentication protocol

- EAP: protocollo end-to-end tra client (mobile) ed authentication server
- EAP viene trasmesso su un “canale” separato
  - mobile-to-AP (EAP over LAN)
  - AP verso authentication server (RADIUS over UDP)



802.11 Generazione della Pairwise Master Key

3) Generazione della Pairwise Master Key

La MK è una chiave segreta condivisa nota solo al client e all'authentication server, che questi possono usare per generare una seconda chiave, la Pairwise Master Key (PMK). L'authentication server allora invia la PMK all'AP. Il client e l'AP adesso posseggono una chiave condivisa (nel WEP manca la tecnica per la distribuzione delle chiavi) e si sono autenticati l'uno con l'altro. Sono pronti per iniziare una comunicazione protetta.

802.11: Generazione della Temporal Key

4) **Generazione della Temporal Key**

   Con la PMK, il client wireless e l'AP, adesso, possono generare ulteriori chiavi che saranno usate per la comunicazione. Di particolare interesse è la Temporal Key (TK), che sarà usata per eseguire, a livello collegamento, la criptografia dei dati inviati sul canale wireless verso un qualsiasi host.

Il protocollo 802.11i fornisce varie forme di criptografia, ad esempio prevede uno schema basato su AES e una versione più robusta della criptografia WEP.