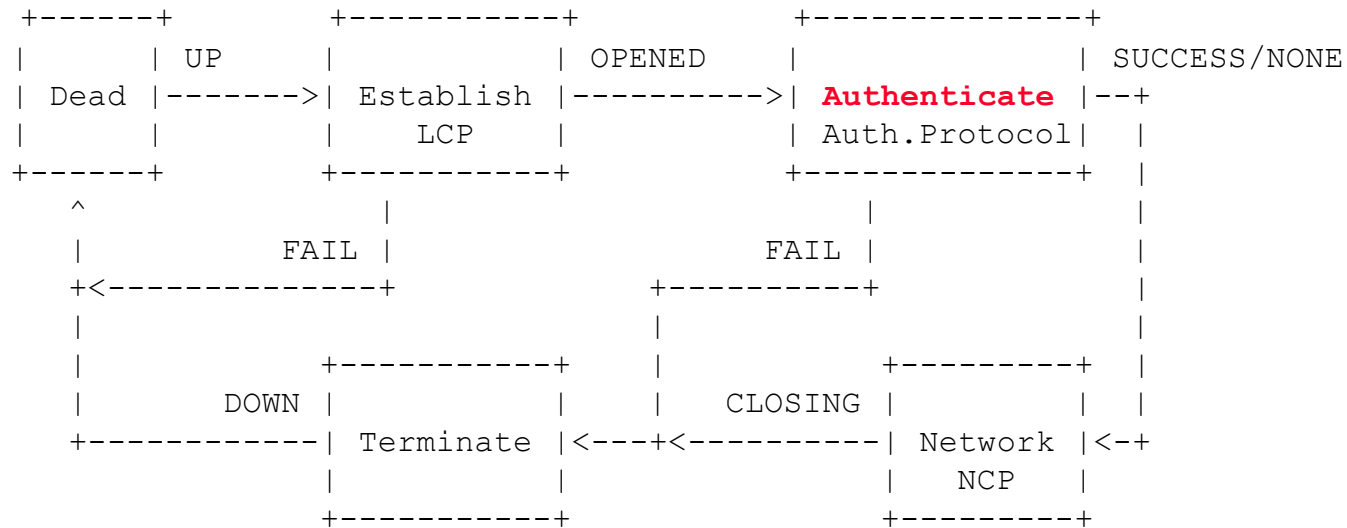

Sécurité du Wi-Fi



Au sujet du protocole PPP

- PPP (RFC 1661, 1994) largement déployer pour les interfaces MODEM et ADSL (PPPoE, PPP over Ethernet)
- L'authentification est réalisé AVANT l'allocation de l'adresse IP



Flag 0x7E	Address 0xFF	Control 03	Protocol 2 bytes	information 1500 octets max	CRC 2 bytes	Flag 0x7E
--------------	-----------------	---------------	---------------------	--------------------------------	----------------	--------------



Protocol Field Value

- 0x0021 : IP
- 0xC021 : Link Control Protocol (LCP)
- 0x8021 : Network Control Protocol (NCP)
- 0xC023 : Password Authentication Protocol (PAP)
- 0xC025 : Link Quality Report (LQR)
- 0xC223 : Challenge Handshake Authentication Protocol (CHAP)



A PPP Authentication example 1/2

LCP Coding

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
| Code | Identifier | Length | Data ...
LCP (code), 1-Request 2-Ack C-IDENTITY
```

LCP Option=3, Authentication Request

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
| Type=3 | Length=5 | Authentication-Protocol= c223 |
|Algorithm=5 MD5|
```

CHAP coding

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
| Code | Identifier | Length | Data ...
```

Code

1- Challenge, 2-Response

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
| Code | Identifier | Length | Value-Size | Value ...
| Name ...
```

3-Success, 4-Failure

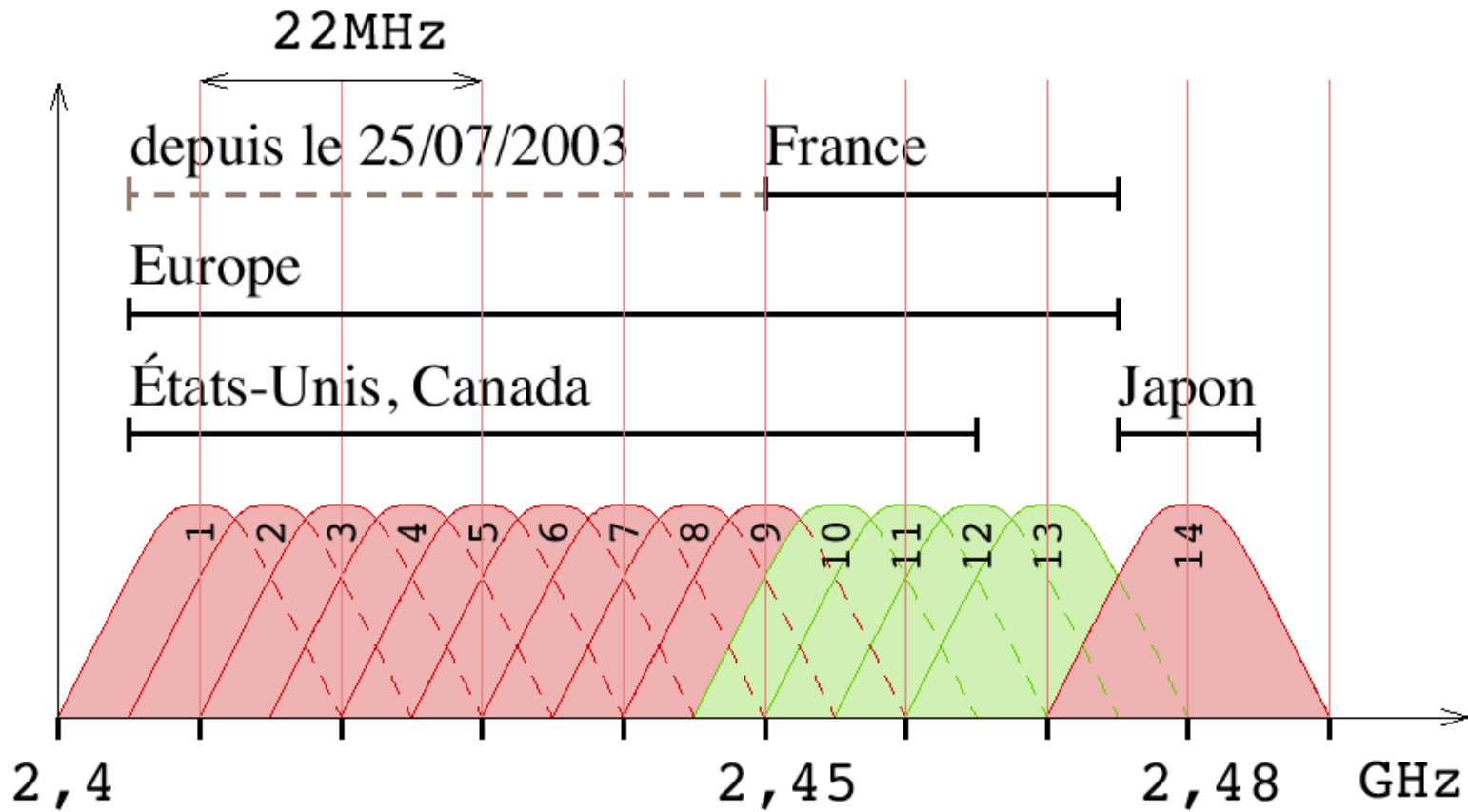
```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
| Code | Identifier | Length | Message ...
```



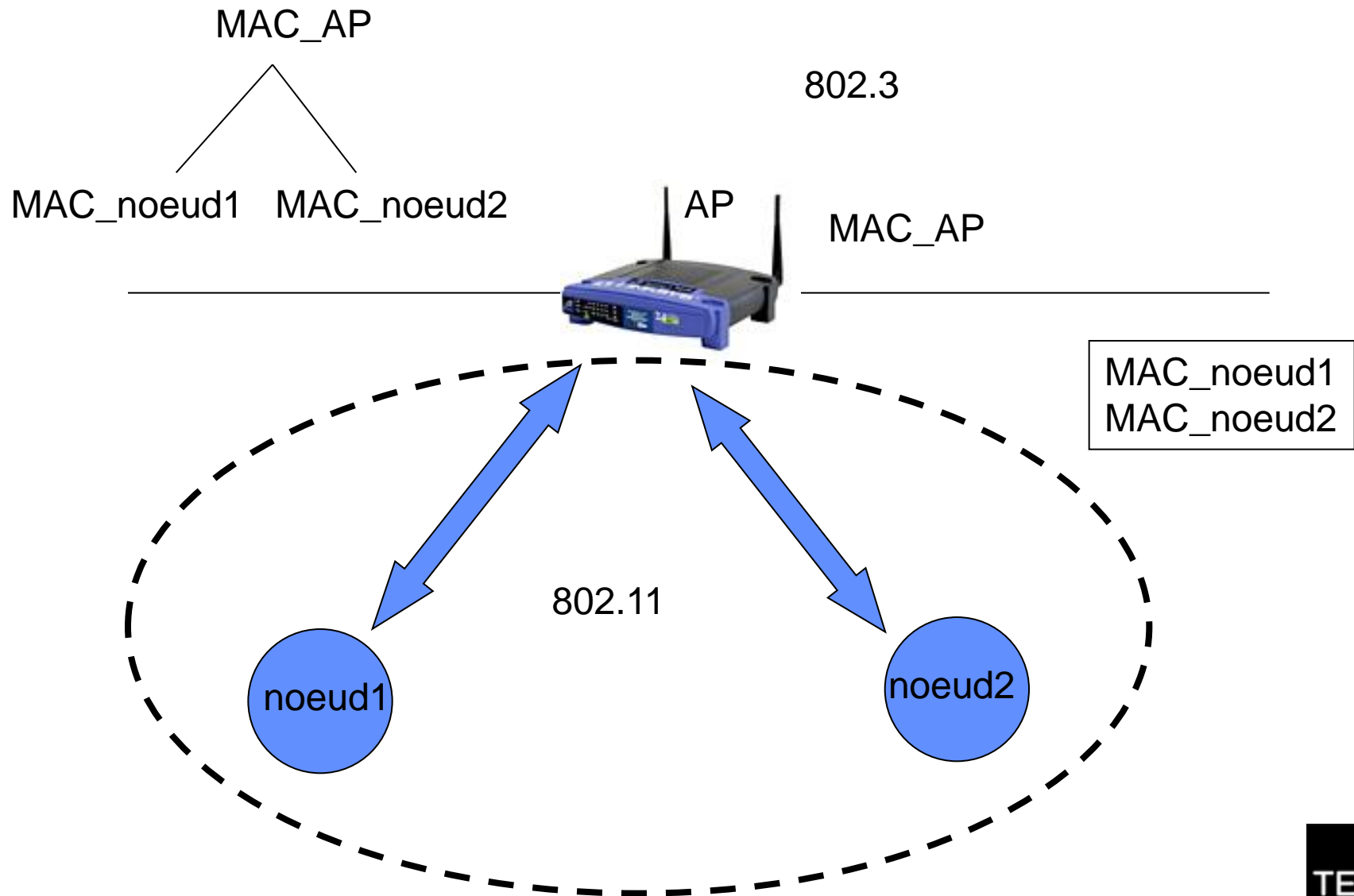
La sécurité du Wi-Fi

Pascal Urien

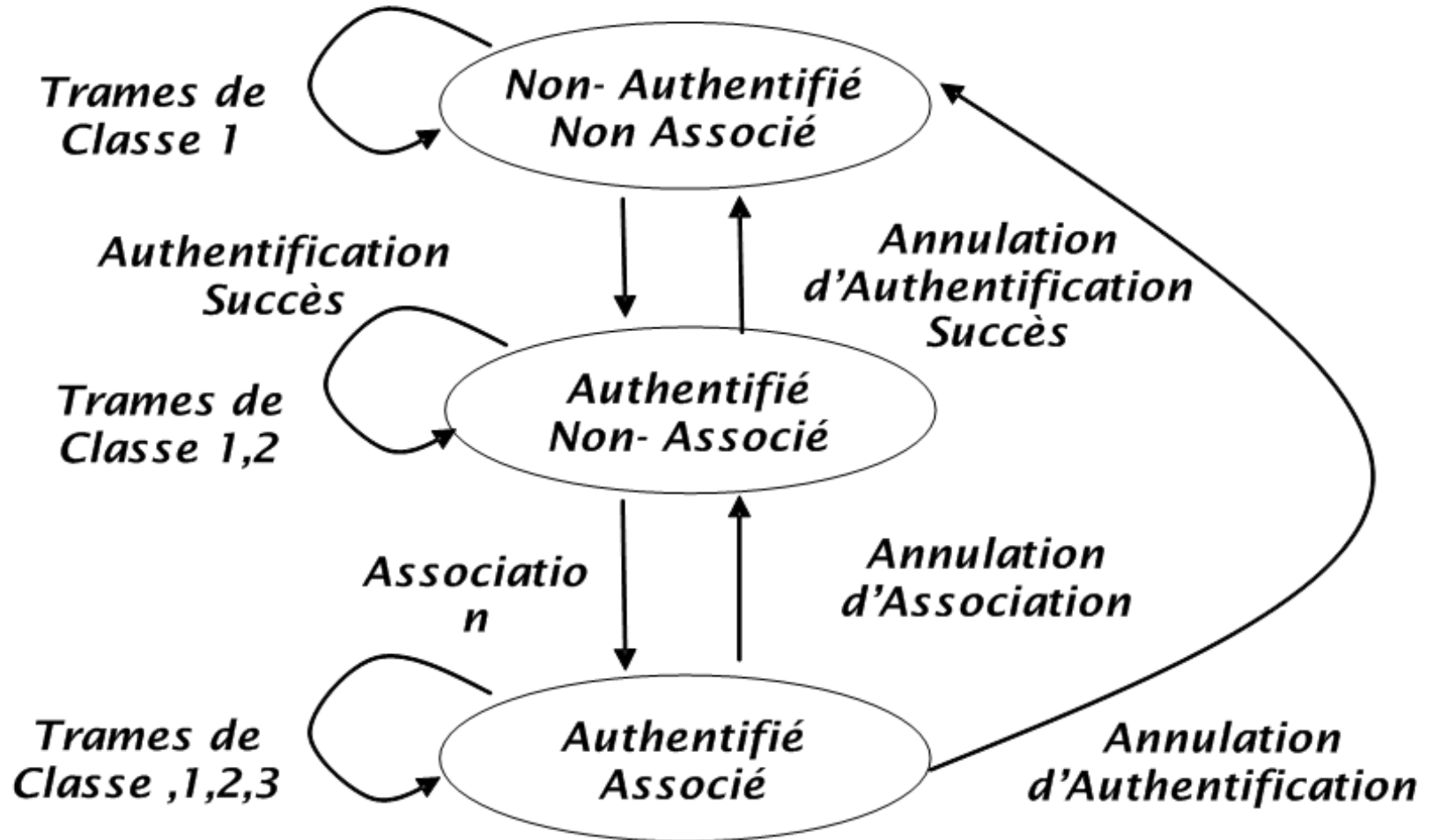
802.11b, 14 canaux de 22 Mhz



Association



Authentication



Wi-Fi, introduction à la Sécurité



Les enjeux du sans fil 1/4

- ✚ Le succès du réseau Internet, véritable moteur de la nouvelle économie de la dernière décennie, a imposé le protocole IP comme un standard de facto pour l'échange des données numériques. Surfant sur cette vague les entreprises ont adoptée cette technologie pour le stockage et la diffusion de leurs informations stratégiques ; intranet, courrier électronique, bases de données trois tiers, annuaires LDAP sont des services aujourd'hui indispensables à la compétitivité et la survie de toute activité économique.
- ✚ Si la prédominance des réseaux IP est actuellement incontestable, il convient également de remarquer que les technologies des réseaux locaux tendent également vers un standard de fait, le réseau Ethernet. Cette technologie, initialement basée sur le partage d'un guide d'onde (un câble en fait) a petit à petit migré vers une infrastructure basée sur des commutateurs de trames («*switchs*»).



Les enjeux du sans fil 2/4

✚ A la base les réseaux sans fil 802.11 ne sont que l'extension naturelle des réseaux Ethernet câblés. La croissance exponentielle de ce marché s'explique par un réel besoin des utilisateurs d'accéder au réseau de manière quasi transparente, sans l'obligation de connecter leur ordinateur personnel à une prise. Le réseau sans fil remplace le câble par un lien radio; cependant en raison des lois de propagation des ondes électromagnétiques cette prise virtuelle est utilisable dans un rayon de l'ordre de 100m, c'est-à-dire dans certain cas à l'extérieur des murs de l'entreprise. On introduit donc de nouveaux risques d'intrusion ou de fuite d'information, parfois qualifiés [Arbaugh *et al.*2001] d'attaque par le parking (*parking lot attack*).



Les enjeux du sans fil 3/4

- ✚ L'apparition de l'IP sans fil dans des architectures câblées préexistantes implique donc la mise en place de nouvelles mesures de sécurité. Jusqu'à présent les entreprises ont déployés leurs réseaux locaux sans protection particulière des points d'accès. Typiquement le réseau est organisé autour d'un arbre de commutateur de paquets (HUB), auquel sont reliées des stations de travail, à l'aide de prises marquant les points d'accès au réseau (souvent dénommées *port d'accès*).
- ✚ L'entrée de l'établissement étant contrôlé et réservé au personnel autorisé, les ports d'accès ne sont pas usuellement sécurisés, en particulier pour permettre une libre connexion des ordinateurs portables. La mobilité des usagers s'appuie sur le protocole DHCP allouant dynamiquement une adresse, compatible avec l'organisation logique et géographique de l'intranet. Celui ci ne conduisant pas en règle générale une procédure d'authentification avant l'allocation des paramètres de configuration, il est très facile d'accéder à l'intranet d'une entreprise depuis un port d'accès.
- ✚ RFC 2131, Chapter 7 - Security Considerations, «...Therefore *DHCP in its current form is quite insecure*».

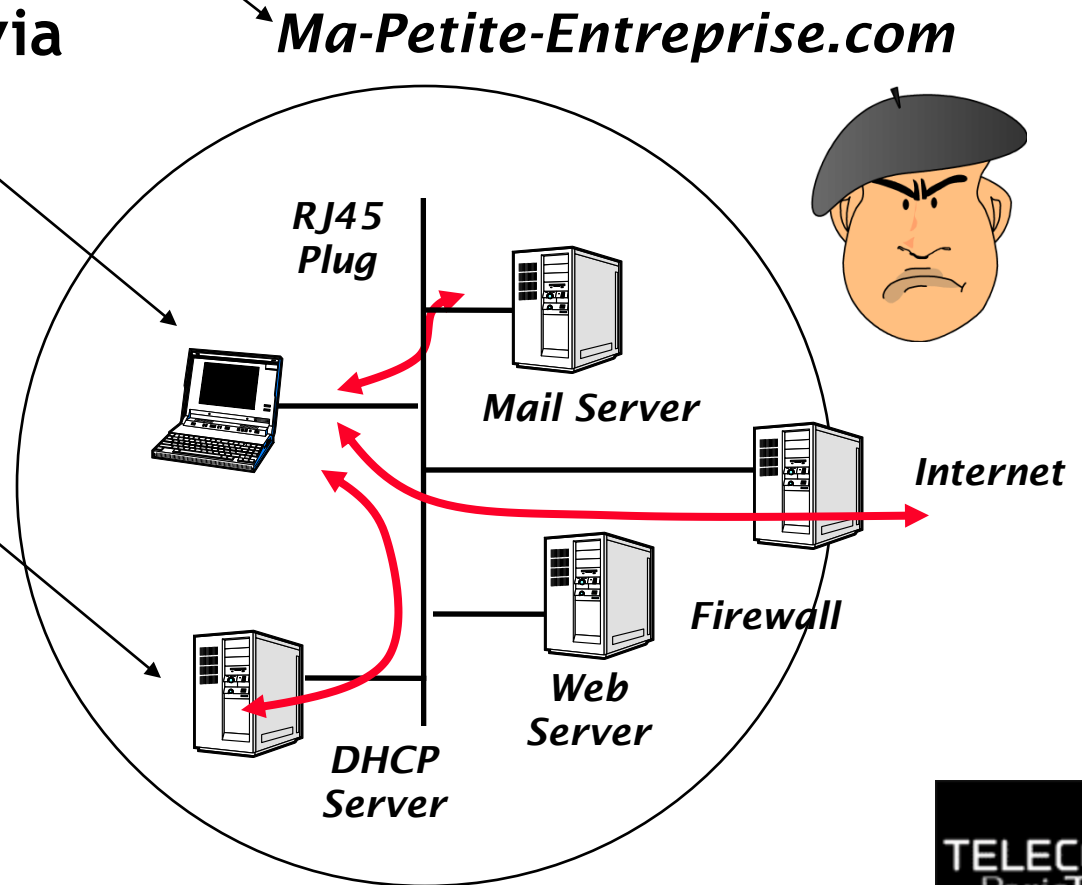


- ✚ En conséquence le contrôle des accès, quasi inexistant dans le cas des réseaux câblés, devient un pré requis pour le déploiement des réseaux 802.11. De même la signature des trames est également indispensable, en son absence, un pirate peut facilement usurper l'adresse MAC d'un utilisateur authentifié (*MAC spoofing*) et accéder aux ressources numériques disponibles. Le chiffrement des données transitant sur le lien radio est également souhaitable afin de garantir la confidentialité des échanges ; cependant de nombreuses méthodes (IPSEC, SSL, SSH ...) sont déjà en mesure d'assurer ce service.
- ✚ En résumé les services sécurisés indispensables aux extensions IP sans fil sont les suivants
 - - Identification et authentification des utilisateurs du réseau
 - - Signature des trames échangées (intégrité, authentification).
 - - Chiffrement des données (confidentialité)

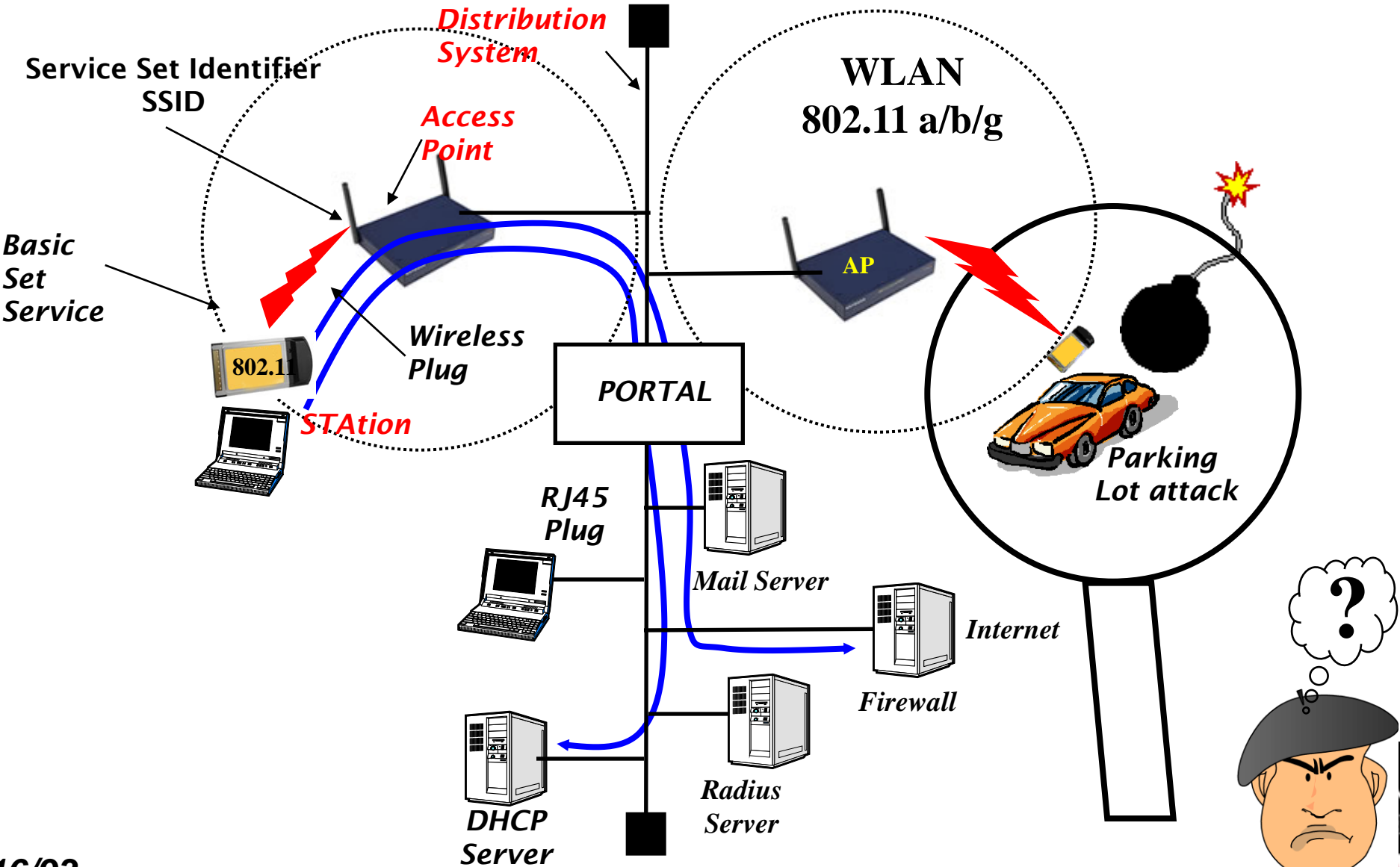


Intranet Câblé Classique

- ✚ Les accès aux locaux sont contrôlés.
- ✚ Connexion des PCs via une prise RJ45.
- ✚ Serveur DHCP non sécurisé.



L'Architecture 802.11.



La Nécessaire Sécurité des Accès Sans Fil.

+ Authentification des accès.

- *Simple*, identification du nomade (prévention du *spoofing*) et de ses droits (*credentials*).
- *Mutuelle*, protection contre des AP indésirables (*rogue access point*).
- Contrôle d'accès au réseau, **protection du réseau = qui utilise le réseau.**

+ Confidentialité (chiffrement) des trames.

- Protection du transport de l'information
- Prévention des écoutes des canaux radio, au niveau 2 (MAC)
- Mais d'autres méthodes sont disponibles IPSEC (3) SSL/TLS (application), SSH (application).

+ Intégrité des trames.

- Prévention des attaques par corruption de données (*bit flipping attack*)

+ Signature des trames.

- Non répudiation. Nécessaire à l'obtention de services.

+ Fourniture/Facturation des services.

- Roaming, Voice Over IP (VoIP), Qualité de services (QoS).

AAA *Authentication, Authorization, Accounting.*

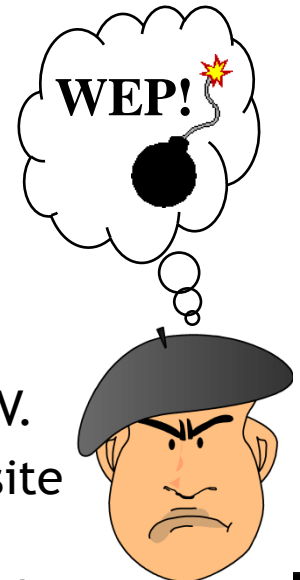
- Groupe de travail IETF RFC 2904



WEP



- ✚ **Open Authentication, c'est à dire pas d'authentification**
 - Utilise le SSID comme mot de passe, peu sûre.
- ✚ **Filtrage des adresses MAC**
 - Address Control List, peu sûre.
- ✚ **Clés RC4 fixes (64 ou 128 bits), partagées entre stations et points d'accès.**
 - Authentification re-jouable.
 - Intégrité des données non garantie.
 - Pas de signature
 - Confidentialité des données, *sous réserves*.
 - Attaque par enregistrement des 16 millions de vecteurs IV.
 - Attaque RC4 *Fluhrer, Mantin, Shamir* (août 2001), nécessite l'enregistrement d'environ de 1 million de trames.
 - Implique un rafraîchissement périodique des clés WEP (*rekeying* exemple changement de clés toutes les 10,000 trames (1 million le seuil critique de sécurité).

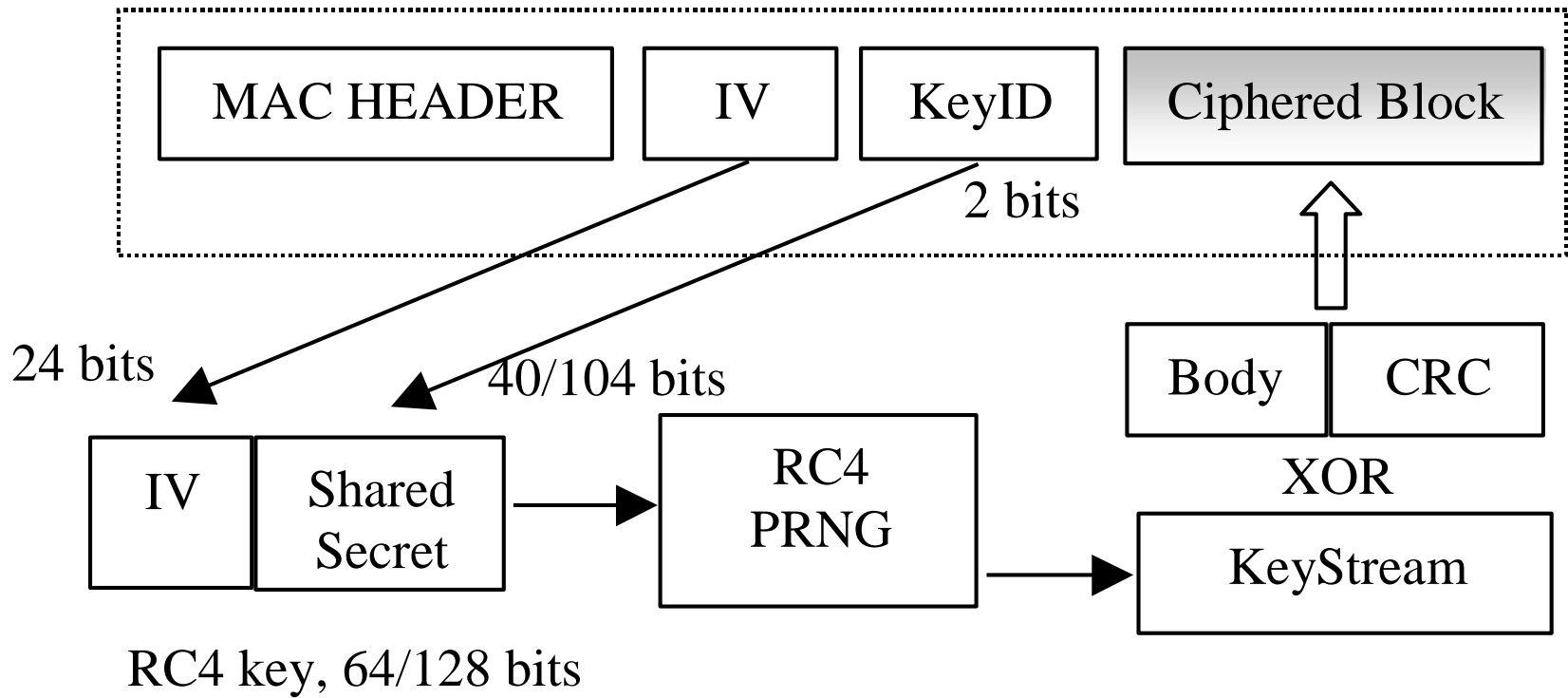


Wireless Equivalent Privacy. 1/5

- ✚ Station et AP partagent 4 secrets de 40 bits.
- ✚ Une trame WEP transporte des données chiffrées par une clé RC4 de 64 bits déduite d'un secret partagé (40 b) et d'une valeur IV (24b) fixée par l'émetteur de l'information.
 - Le chiffrement RC4 (C_i) est réalisé par le ou exclusif (*code de Vernam*) du message (M_i) en clair avec suite d'octets pseudo aléatoire X_{si} déduit de la clé.
 - On peut déduire la valeur de la clé X_{si} connaissant la valeur en clair C_i .
 - $C_i = M_i \oplus X_{si}$, $C_i \oplus M_i = X_{si}$
 - Une clé RC4 ne doit pas être réutilisée ($2^{24} = 16$ millions de trames chiffrées par clé)



La trame WEP 2/5.



Association

- Le BSS est identifié par le paramètre SSID présent dans les trames fanion (Beacon) émises périodiquement.
- Une station s'associe volontairement à un AP.

Authentification

- AP émet un challenge en clair. La station chiffre cet aléa avec un IV (24 b) et une clé RC4 (1 parmi 4).
 - 🌐 On en déduit la suite aléatoire de chiffrement Xsi.
- La procédure d'authentification peut être rejouée.



✚ Confidentialité.

- Seulement 2^{24} valeurs IV.
- 50 % de chances de réutiliser une valeur IV au bout de 4823 trames.
- Les suites de chiffrement Xsi se déduisent des valeurs en clair.
- 2^{40} essais (1million/s x 12 jours) permettent de trouver les secrets partagés de 40 bits.

✚ WEP est cassable en quelques heures.

- Des logiciels sont disponibles sur le WEB
- Attaque de Fluhrer par des valeurs dites *résolvantes*, $IV=(B+3,255,x)$ $x \in [0,255]$. Environ 60 valeurs sont nécessaires pour obtenir l'octet de la clé de rang B.

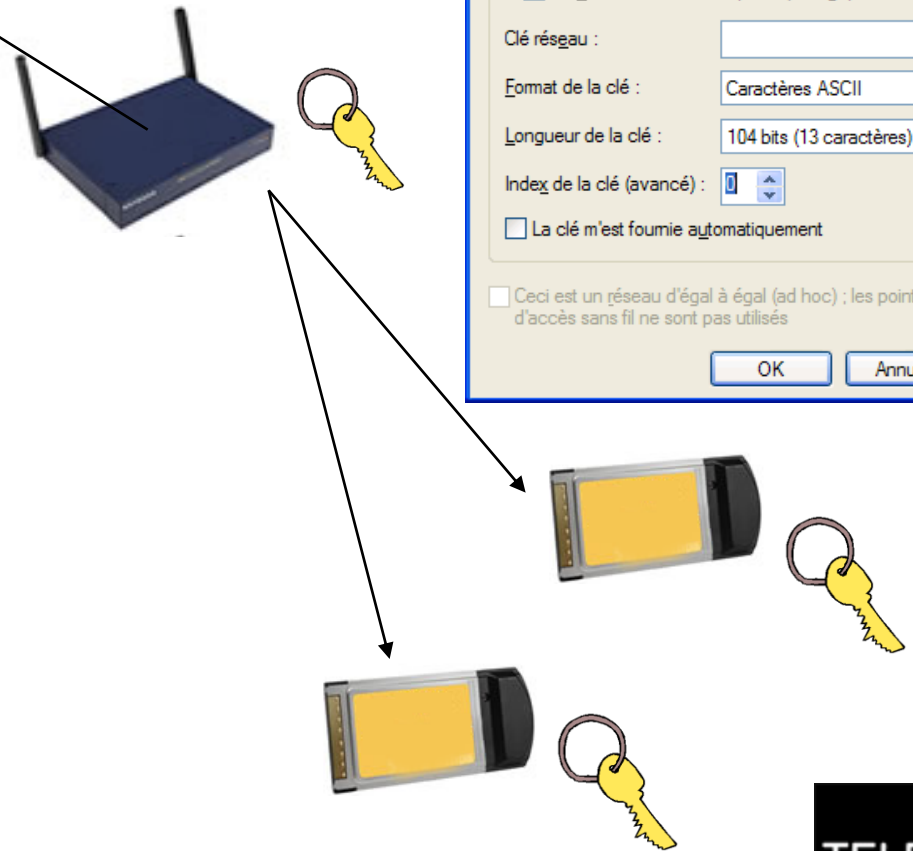
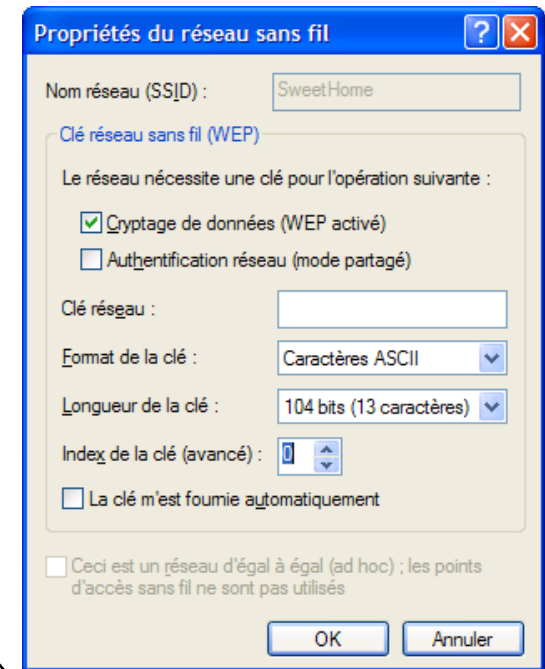
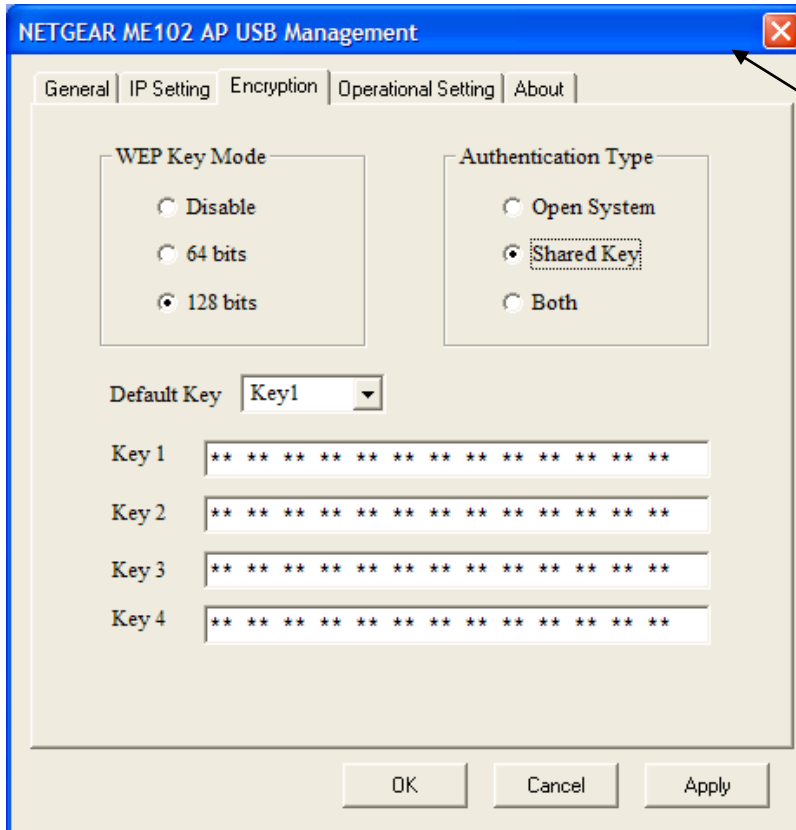


✚ Intégrité des données.

- Dans une trame WEP le CRC est chiffré.
- Le CRC est une fonction linéaire du ou exclusif, le CRC du ou exclusif (octet à octets) de deux trames de même longueurs est le ou exclusif de leur CRC respectif.
- Le ou exclusif (octets à octets) d'une trame WEP (chiffrée) et d'une trame en clair fournit un CRC correcte.
- WEP n'assure pas l'intégrité des données.



WEP + Windows

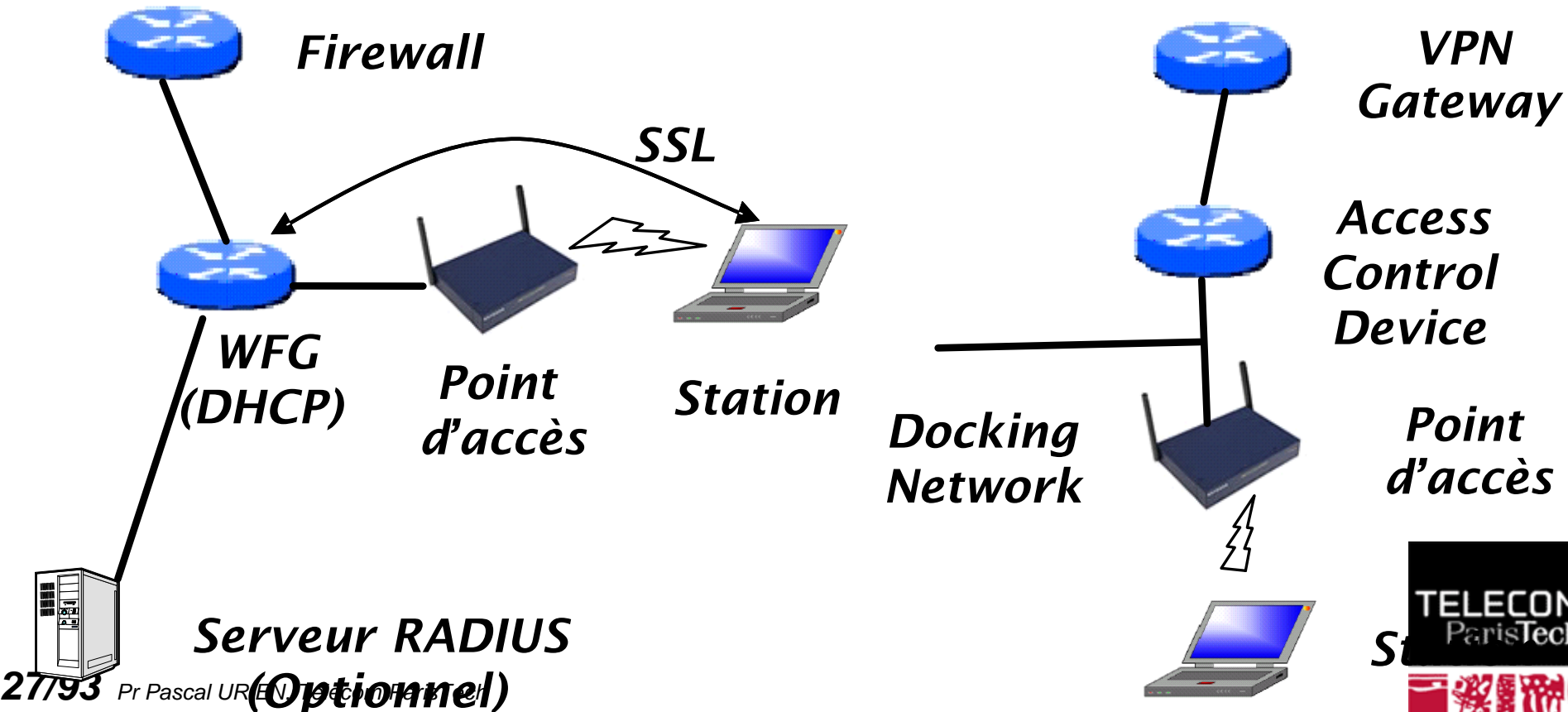


Architectures Alternatives

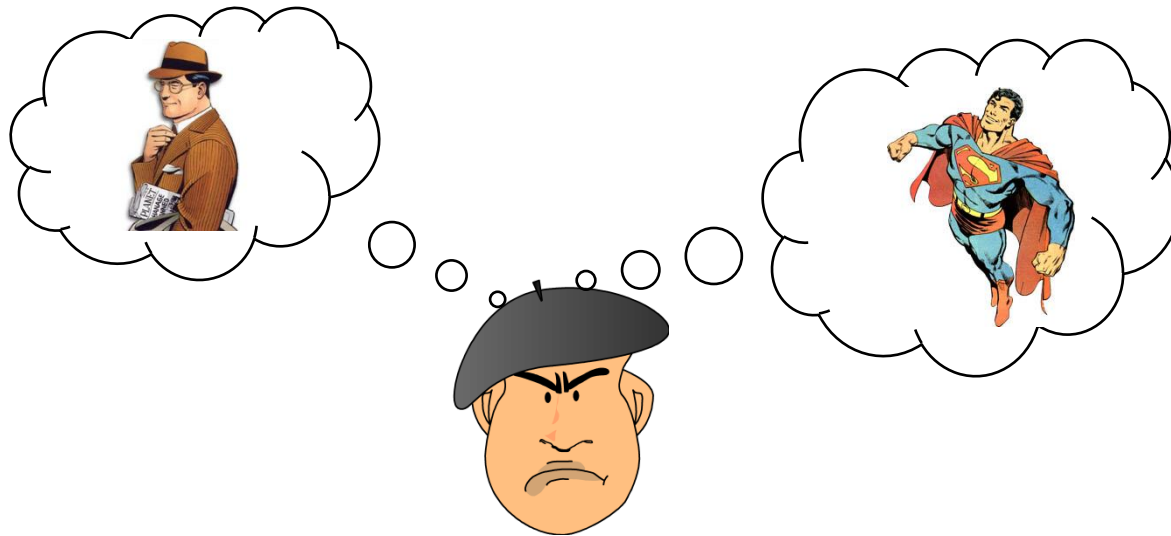


Architectures Alternatives

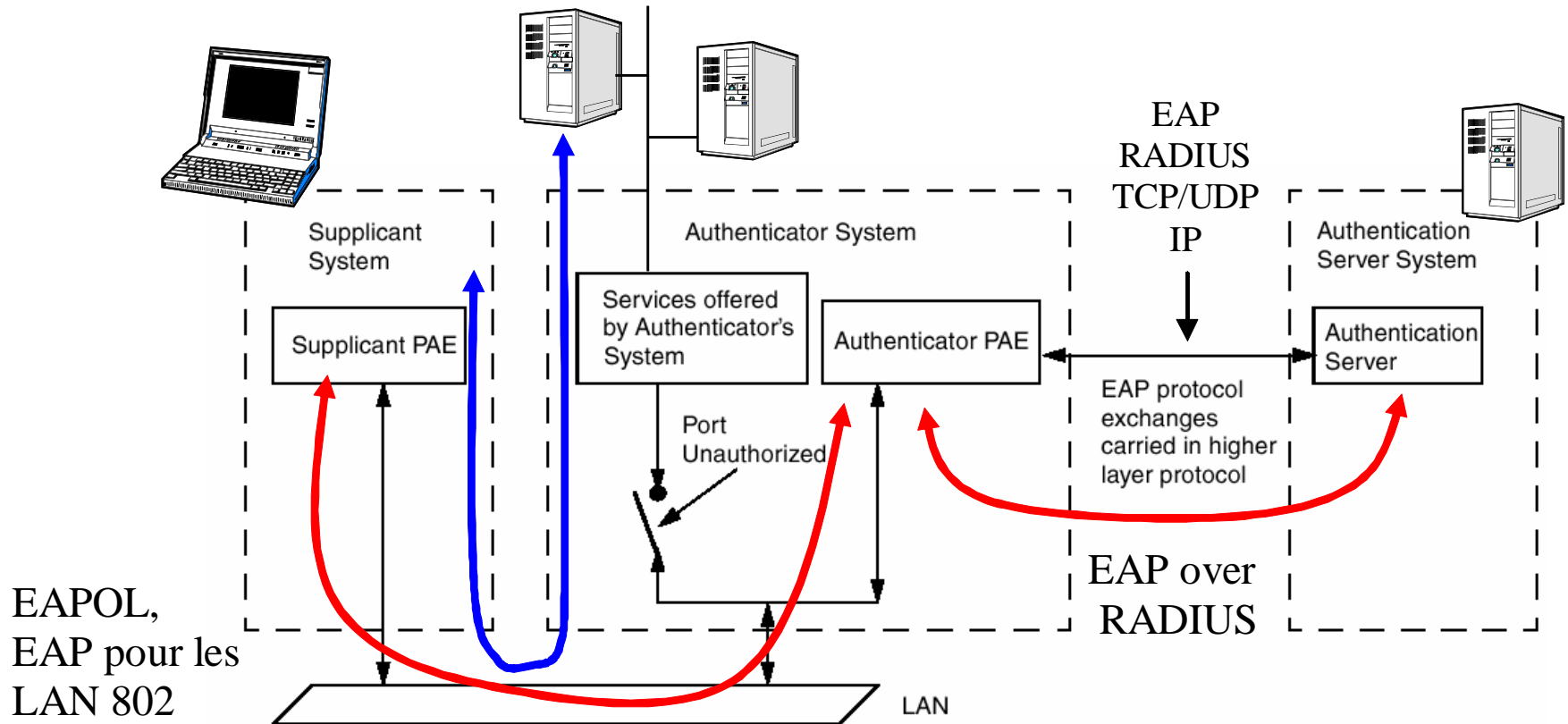
- + Tunnels VPN
 - IPSEC
- + Les portails captifs
 - WFG - *Wireless Firewall Gateway*
- + Access Control List
 - Switch Mobile (2004)



Le modèle 802.1x



Architecture d'authentification 802.1x. 2/2



EAPOL,
EAP pour les
LAN 802

EAP over
RADIUS



Network Port Authentication - 802.1x. 1/2

- ✚ Les trames émises par une station non authentifiée sont **filtrées** par le système d'authentification.
- ✚ Les éléments de la procédure d'authentification sont échangés via par le protocole EAP (*Extended Authentication Protocol*) .
- ✚ EAP est transporté par des **trames 802** (EAP encapsulation over LAN) entre station et système d'authentification.
- ✚ Le processus d'authentification est conduit avec un serveur distant (et non par un AP).
 - Architecture centralisée.
- ✚ EAP est transporté par le protocole RADIUS (*Remote Access Dialing User Service*) entre système d'authentification et serveur d'authentification distant.

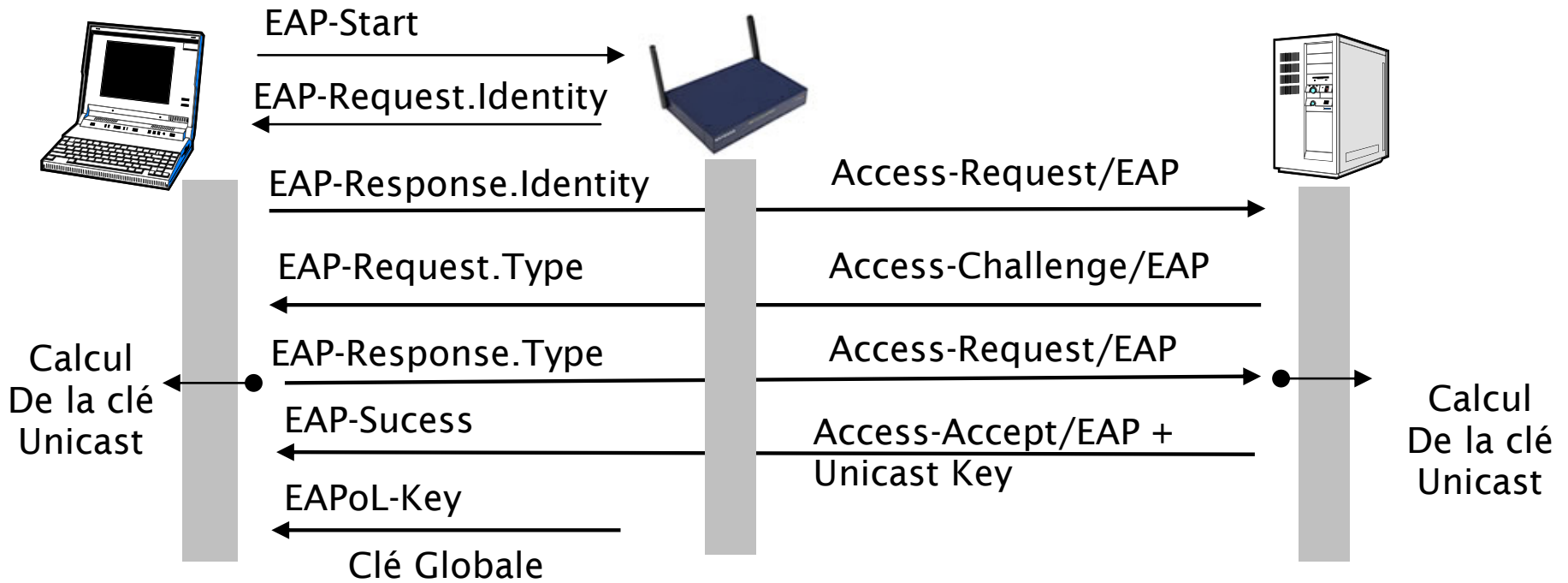


1. L'identité du client (EAP_ID) détermine un serveur d'authentification (RADIUS). Elle est transmise au serveur RADIUS (RS), via le point d'accès (AP).
2. Le processus d'authentification se déroule entre le client (*supplicant*) et le serveur radius (RS). Le point d'accès (*Authenticator*) se comporte comme un relais entre ces deux entités.
3. A la fin du processus d'authentification une clé unicast (ou clé maître MSK) est calculée par le client et le RS.
4. La clé MSK est transmise (chiffrée) par RS vers AP, à l'aide du protocole RADIUS.
5. AP calcule alors une clé globale (WEP), il chiffre cette valeur par la clé SK, et la transmet au client (via trame EAPOL-Key).



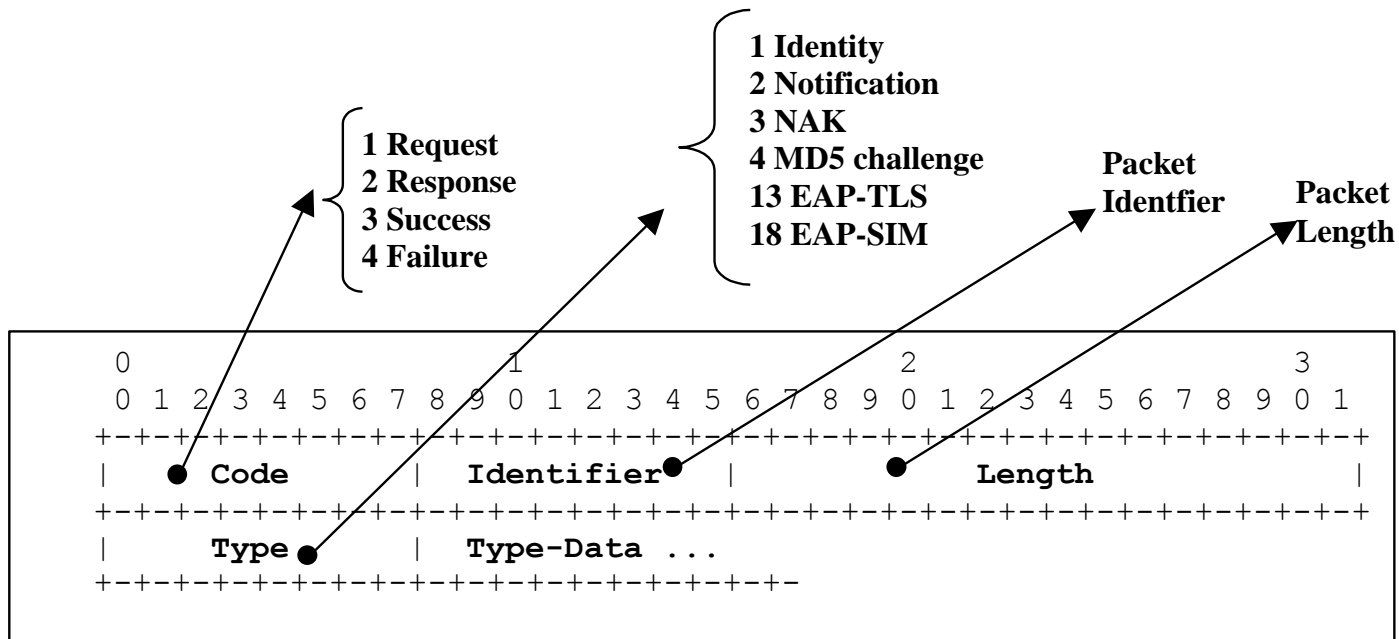
EAPoL key Descriptor

Descriptor Type - 1 octet	
Key Information - 2 octets	Key Length - 2 octets
Key Replay Counter - 8 octets	
Key Nonce - 32 octets	
EAPoL-Key IV - 16 octets	
Key RSC - 8 octets	
STA MAC Address - 6 octets	
GTK Length - 2 octets	
Key MIC - 16 octets	
Key Data Length - 2 octets	Key Data - n octets



Le protocole EAP.

- EAP est conçu pour transporter des scénarios d'authentification.
- Quatre types de messages, requêtes, réponses, succès, échec

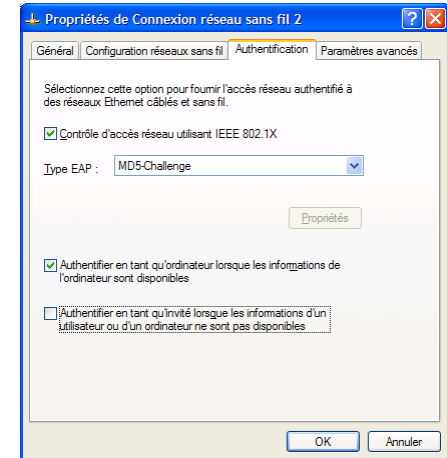


EAP, what else ?

- ✚ The Extensible Authentication Protocol (EAP) was introduced in 1999, in order to define a **flexible authentication framework**.
 - EAP, RFC 3748, "Extensible Authentication Protocol, (EAP)", June 2004.
 - **EAP-TLS**, RFC 2716, "PPP EAP TLS Authentication Protocol", 1999.
 - **EAP-SIM**, RFC 4186, " Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM) ", 2006
 - **EAP-AKA**, RFC 4187, " Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) ", 2006
- ✚ **EAP Applications.**
 - Wireless LAN
 - Wi-Fi, IEEE 802.1x, 2001
 - WiMAX mobile, IEEE 802.16e , PKM-EAP, 2006
 - Wired LANs
 - ETHERNET, IEEE 802.3
 - PPP, RFC 1661, "The Point-to-Point Protocol (PPP)", 1994
 - VPN (Virtual Private Network) technologies
 - PPTP, Point-to-Point Tunneling Protocol (PPTP), RFC 2637
 - L2TP, Layer Two Tunneling Protocol (L2TP), RFC 2661
 - IKEv2, RFC 4306, "Internet Key Exchange (IKEv2) Protocol", 2005
 - Authentication Server
 - RADIUS, RFC 3559, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", 2003
 - DIAMETER, RFC 4072, "Diameter Extensible Authentication Protocol Application", 2005
 - Voice Over IP
 - UMA, Unlicensed Mobile Access, <http://www.umatechnology.org>



Réseau local ou Internet à haute vitesse



PSWD: 5678



Exemple 2/2

EAP-Start

00 30 ab 14 68 ef 00 30 ab 1a 07 8f 88 8e **01 01 00 00**

Identity-Request

00 30 ab 1a 07 8f 00 30 ab 14 68 ef 88 8e **01 00 00 05 01 a7 00 05 01**

Identity-Response

00 30 ab 14 68 ef 00 30 ab 1a 07 8f 88 8e **01 00 00 0e 02 a7 00 0e 01 41 42 43 44
5c 31 32 33 34**

MD5-Request

00 30 ab 1a 07 8f 00 30 ab 14 68 ef 88 8e **01 00 00 06 01 a8 00 06 04 00**

MD5-Response

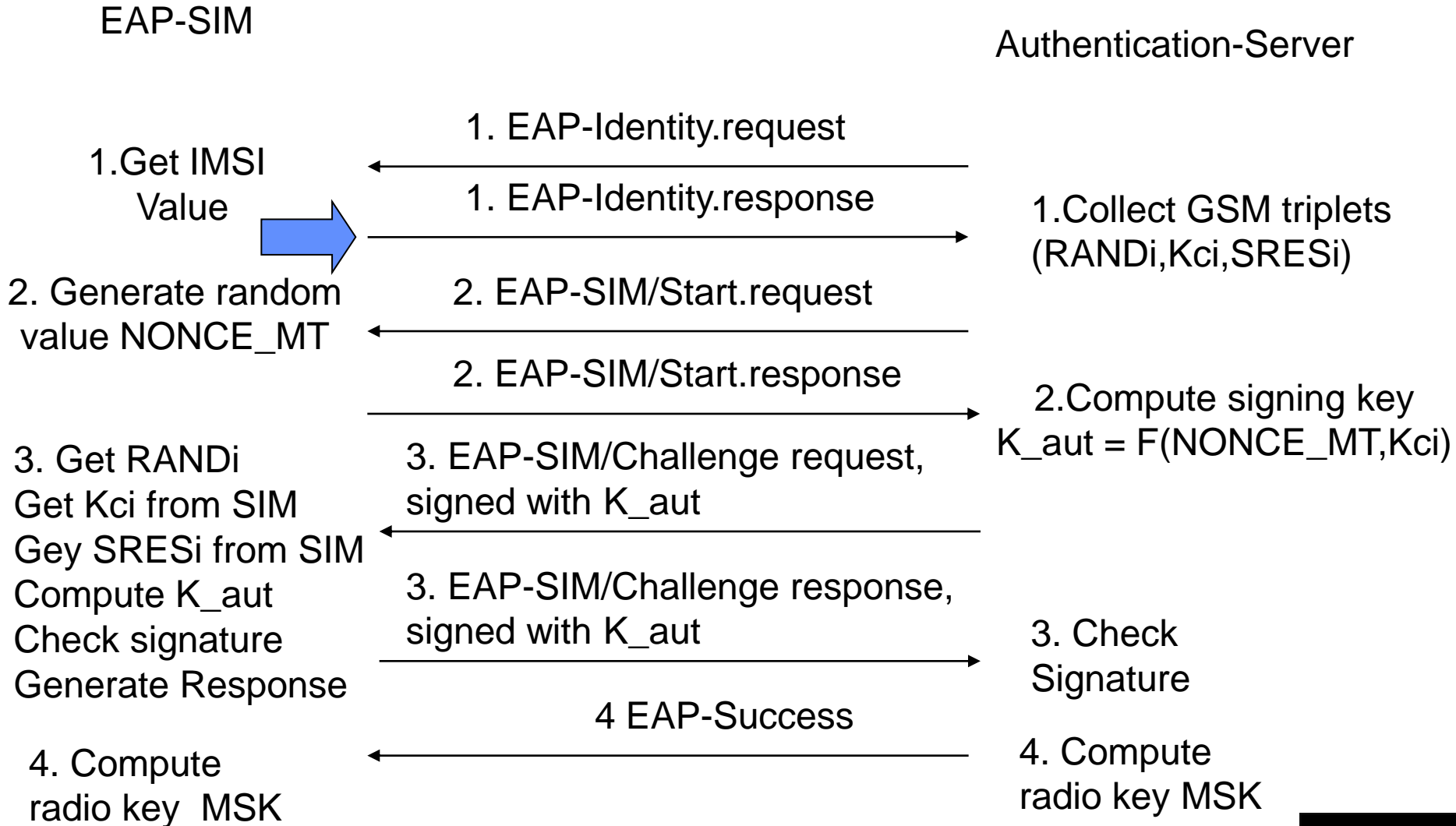
00 30 ab 14 68 ef 00 30 ab 1a 07 8f 88 8e **01 00 00 1f 02 a8 00 1f 04 10 3d 92 48 f4
2b be 0f 81 05 4e d4 39 87 77 a3 82 41 42 43 44 5c 31 32 33 34**

EAP-Success

00 30 ab 1a 07 8f 00 30 ab 14 68 ef 88 8e **01 00 00 05 03 a9 00 05 02**




Exemples EAP



EAP-Identity.request/response 2/8

```
01 ; Code: Request
00 ; Identifier: 0
00 05 ; Length: 5 octets
01 ; Type: Identity
```

```
02 ; Code: Response
00 ; Identifier: 0
00 20 ; Length: 32 octets
01 ; Type: Identity
    31 32 34 34 ; "1244070100000001@eapsim.foo"
    30 37 30 31
    30 30 30 30
    30 30 30 31
    40 65 61 70
    73 69 6d 2e
    66 6f 6f
```


IMSI

EAP-ID may be null or only includes a NAI realm portion



EAP-SIM/Start 3/8

```
01          ; Code: Request
01          ; Identifier: 1
00 10      ; Length: 16 octets
12         ; Type: EAP-SIM
0a         ; EAP-SIM subtype: Start
00 00      ; (reserved)
0f         ; Attribute type: AT_VERSION_LIST
           ; Attribute length: 8 octets (2*4)
           ; Actual version list length: 2 octets
           ; Version: 1
           ; (attribute padding)
```

```
02          ; Code: Response
01          ; Identifier: 1
00 20      ; Length: 32 octets
12         ; Type: EAP-SIM
0a         ; EAP-SIM subtype: Start
00 00      ; (reserved)
07         ; Attribute type: AT_NONCE_MT
           ; Attribute length: 20 octets (5*4)
           ; (reserved)
```

01	23	45	67
89	ab	cd	ef
fe	dc	ba	98
76	54	32	10

; NONCE_MT 16 bytes value



Random value 16 bytes
generated by the client

```
10         ; Attribute type: AT_SELECTED_VERSION
           ; Attribute length: 4 octets (1*4)
           ; Version: 1
```



Key Hierarchy & Derivation 4/8

```
(RAND1, SRES1, Kc1) = (10111213 14151617 18191a1b 1c1d1e1f, d1d2d3d4, a0a1a2a3, a4a5a6a7)
(RAND2, SRES2, Kc2) = (20212223 24252627 28292a2b 2c2d2e2f, e1e2e3e4, b0b1b2b3 b4b5b6b7)
(RAND3, SRES3, Kc3) = (30313233 34353637 38393a3b 3c3d3e3f, f1f2f3f4, c0c1c2c3 c4c5c6c7)
```

XKEY = SHA1(Identity | Kc1 | Kc2 | Kc3 | NONCE_MT | Version List | Selected Version)

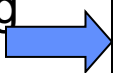
XKEY = e576d5ca 332e9930 018bf1ba ee2763c7 95b3c712

And the other keys are derived using the **FIPS-186-2** PRF (Pseudo Random Function)

$x_j = \text{PRF}_{\text{FIPS-186-2}}(\text{XKEY})$

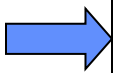
K_encr = 536e5ebc 4465582a a6a8ec99 86ebb620

Signing
Key



K_aut = 25af1942 efcbf4bc 72b39434 21f2a974

Radio
Key



MSK = 39d45aea f4e30601 983e972b 6cfd46d1
c3637733 65690d09 cd44976b 525f47d3
a60a985e 955c53b0 90b2e4b7 3719196a
40254296 8fd14a88 8f46b9a7 886e4488

EMSK = 5949eab0 fff69d52 315c6c63 4fd14a7f
0d52023d 56f79698 fa6596ab eed4f93f
bb48eb53 4d985414 ceed0d9a 8ed33c38
7c9dfdab 92ffbfd2 40fcec6f 5a2c93b9



EAP-SIM/Challenge request 5/8

```

01      ; Code: Request
02      ; Identifier: 2
01 18   ; Length: 280 octets
12      ; Type: EAP-SIM
0b      ; EAP-SIM subtype: Challenge
00 00   ; (reserved)
01      ; Attribute type: AT_RAND
0d      ; Attribute length: 52 octets (13*4)
00 00   ; (reserved)
10 11 12 13
14 15 16 17
18 19 1a 1b
1c 1d 1e 1f
20 21 22 23
24 25 26 27
28 29 2a 2b
2c 2d 2e 2f
30 31 32 33
34 35 36 37
38 39 3a 3b
3c 3d 3e 3f
; first RAND
; second RAND
; third RAND

81      ; Attribute type: AT_IV
05      ; Attribute length: 20 octets (5*4)
00 00   ; (reserved)
9e 18 b0 c2
9a 65 22 63
c0 6e fb 54
dd 00 a8 95
; IV value

82      ; Attribute type: AT_ENCR_DATA (AES(K_encr) 128 bits)
2d      ; Attribute length: 180 octets (45*4)
00 00   ; (reserved)
55 f2 93 9b bd b1 b1 9e a1 b4 7f c0 b3 e0 be 4c
ab 2c f7 37 2d 98 e3 02 3c 6b b9 24 15 72 3d 58
ba d6 6c e0 84 e1 01 b6 0f 53 58 35 4b d4 21 82
78 ae a7 bf 2c ba ce 33 10 6a ed dc 62 5b 0c 1d
5a a6 7a 41 73 9a e5 b5 79 50 97 3f c7 ff 83 01
07 3c 6f 95 31 50 fc 30 3e a1 52 d1 e1 0a 2d 1f
4f 52 26 da a1 ee 90 05 47 22 52 bd b3 b7 1d 6f
0c 3a 34 90 31 6c 46 92 98 71 bd 45 cd fd bc a6
11 2f 07 f8 be 71 79 90 d2 5f 6d d7 f2 b7 b3 20
bf 4d 5a 99 2e 88 03 31 d7 29 94 5a ec 75 ae 5d
43 c8 ed a5 fe 62 33 fc ac 49 4e e6 7a 0d 50 4d

0b      ; Attribute type: AT_MAC
05      ; Attribute length: 20 octets (5*4)
00 00   ; (reserved)
fe f3 24 ac
39 62 b5 9f
3b d7 82 53
ae 4d cb 6a
; MAC value

```



Signing Value

The MAC is calculated over the EAP packet above (with MAC value set to zero), followed by the NONCE_MT value (a total of 296 bytes).

$$\text{MAC_Value} = \text{HMAC_SHA1}(k_{\text{aut}}, \text{message})$$



Decrypted Content of AT_ENCR 6/8

```
84          ; Attribute type: AT_NEXT_PSEUDONYM
13          ; Attribute length: 76 octets (19*4)
00 46      ; Actual pseudonym length: 70 octets
77 38 77 34 39 50 65 78 43 61 7a 57 4a 26 78 43
49 41 52 6d 78 75 4d 4b 68 74 35 53 31 73 78 52
44 71 58 53 45 46 42 45 67 33 44 63 5a 50 39 63
49 78 54 65 35 4a 34 4f 79 49 77 4e 47 56 7a 78
65 4a 4f 55 31 47
00 00      ; (attribute padding)
85          ; Attribute type: AT_NEXT_REAUTH_ID
16          ; Attribute length: 88 octets (22*4)
00 51      ; Actual re-auth identity length
              ; 81 octets
59 32 34 66 4e 53 72 7a 38 42 50 32 37 34 6a 4f
4a 61 46 31 37 57 66 78 49 38 59 4f 37 51 58 30
30 70 4d 58 6b 39 58 4d 4d 56 4f 77 37 62 72 6f
61 4e 68 54 63 7a 75 46 71 35 33 61 45 70 4f 6b
6b 33 4c 30 64 6d 40 65 61 70 73 69 6d 2e 66 6f
6f
00 00 00   ; (attribute padding)
06          ; Attribute type: AT_PADDING
03          ; Attribute length: 12 octets (3*4)
00 00 00 00
00 00 00 00
00 00
```

AT_NEXT_PSEUDONYM

"w8w49PexCazWJ&xCIARmxuMKht5S1sxR DqXSEFBEG3DcZP9clxTe5J4OylwNGVzxeJOU1G"

AT_NEXT_REAUTH_ID

"Y24fNSrZ8BP274jOJaF17Wfxl8YO7QX00pMXk9XMMVOW7broaNHtCzuFq53aEpOkk3L0dm@ea



EAP-SIM/Challenge Response 7/8

```
02          ; Code: Response
02          ; Identifier: 2
00 1c      ; Length: 28 octets
12         ; Type: EAP-SIM
0b         ; EAP-SIM subtype: Challenge
00 00      ; (reserved)
0b         ; Attribute type: AT_MAC
05         ; Attribute length: 20 octets (5*4)
00 00      ; (reserved)
```

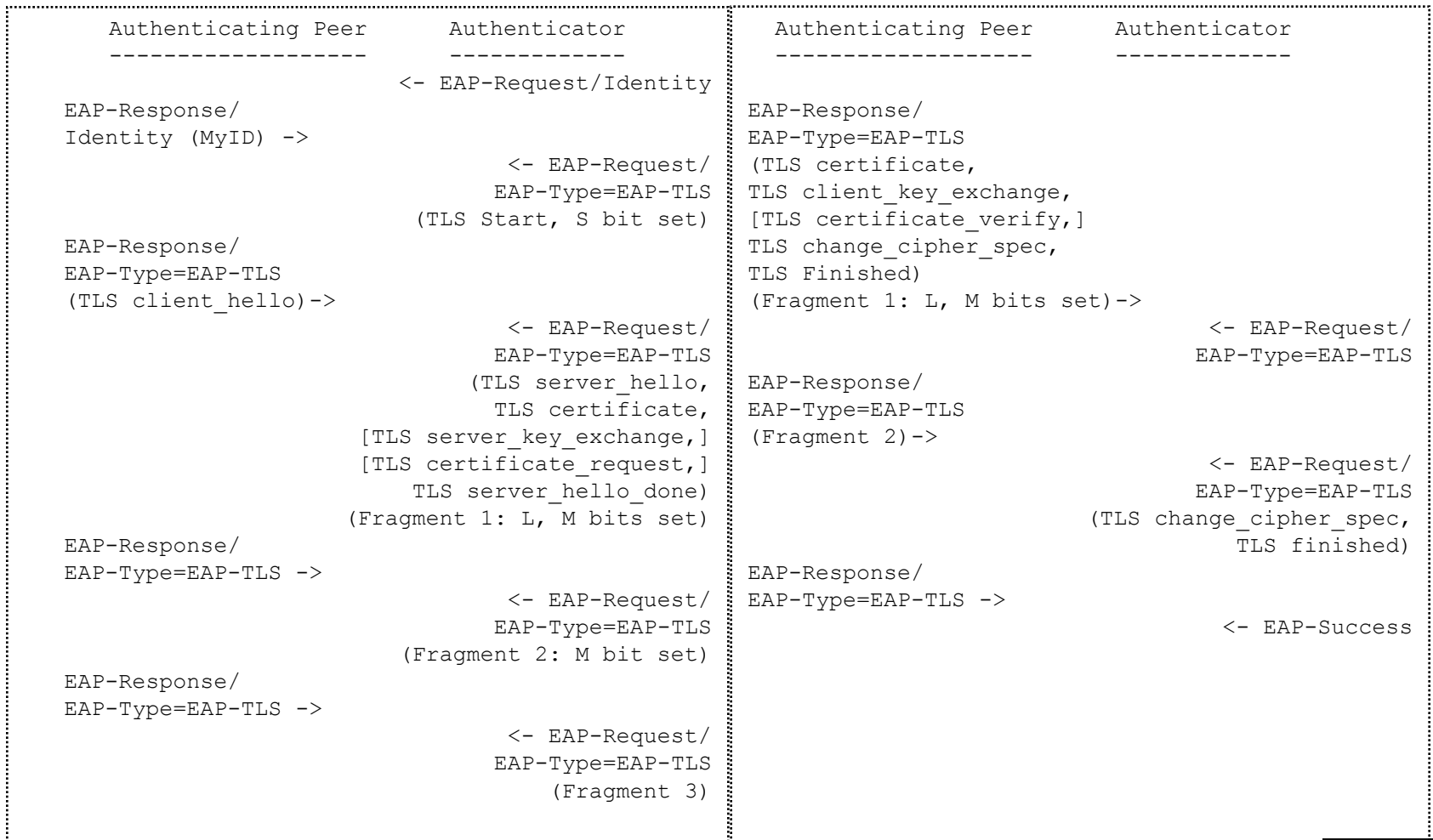
<pre>f5 6d 64 33 ; MAC value e6 8e d2 97 6a c1 19 37 fc 3d 11 54</pre>
--

The MAC is calculated over the EAP packet above (with MAC value set to zero), followed by the SRESi (SRES1| SRES2| SRES3) values (a total of 40 bytes).



```
03           ; Code: Success
03           ; Identifier: 3
00 04       ; Length: 4 octets
```





```

        EAP-Request/Identity
    <-----
EAP-Response/Identity
----->
        EAP-Request/TTLS-Start
    <-----
EAP-Response/TTLS:
ClientHello
----->
        EAP-Request/TTLS:
            ServerHello
            Certificate
            ServerKeyExchange
            ServerHelloDone
    <-----
EAP-Response/TTLS:
ClientKeyExchange
ChangeCipherSpec
Finished
----->
        EAP-Request/TTLS:
            ChangeCipherSpec
            Finished
    <-----
EAP-Response/TTLS:
    {EAP-Response/Identity}
----->
        EAP-Request/TTLS:
    {EAP-Request/MD5-Challenge}
    <-----
EAP-Response/TTLS:
    {EAP-Response/MD5-Challenge}
----->
        EAP-Success
    <-----
    
```

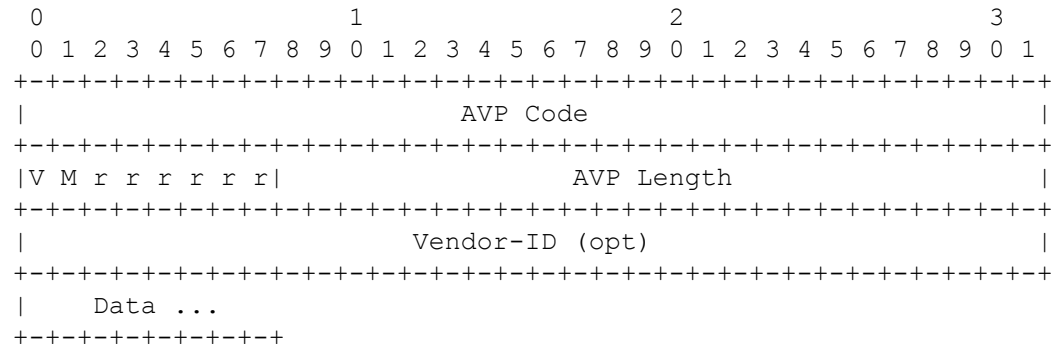
Phase 1

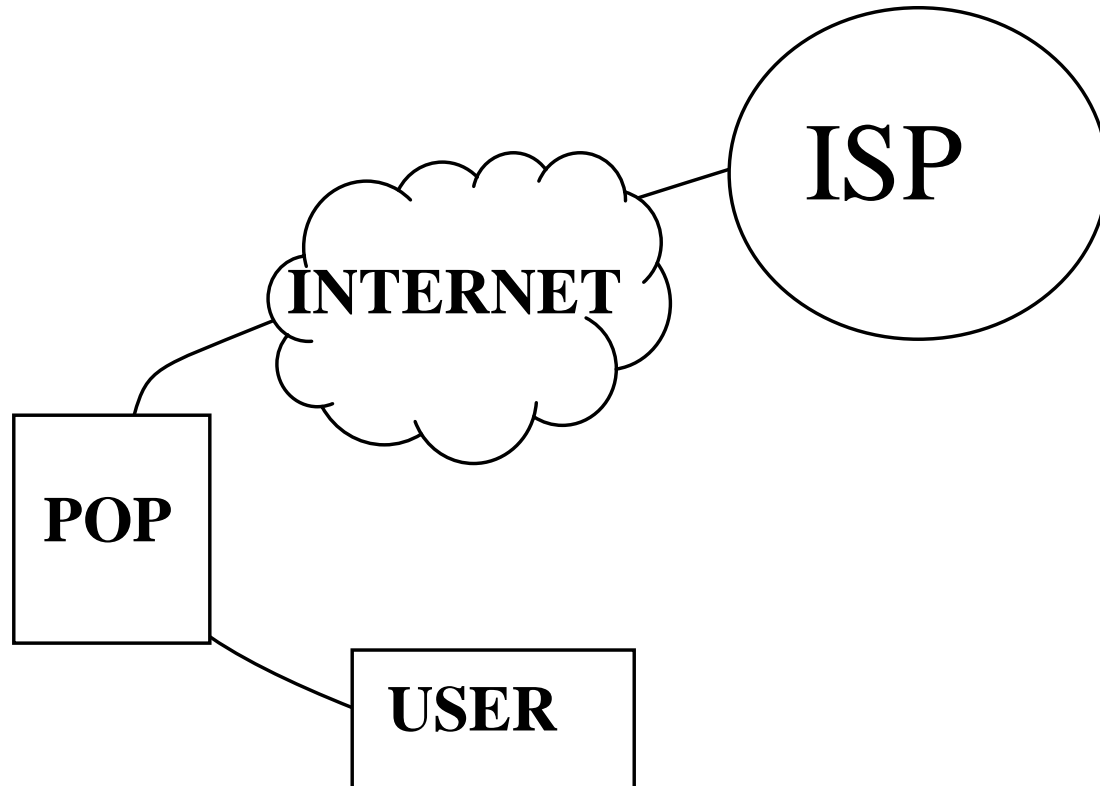
Phase 2



TTLS works in two phases

- Phase 1.
 - A EAP-TTLS session open a secure TLS tunnel
 - EAP-TTLS phase 1 is very similar to EAP-TLS
- Phase 2.
 - Multiple protocols (EAP and other) are transported and protected by the previously opened TLS tunnel.
 - Protocols are transported in AVP





RADIUS



- ✚ Le protocole *Remote Authentication Dial In User Service* est spécifié par la RFC 2865. La RFC 2866 (*RADIUS accounting*) définit les attributs utiles à la facturation. Les messages sont transportés par des paquets UDP, utilisant les ports 1812 (*radius*) et 1813 (*radacct*).
- ✚ Un fournisseur de service Internet (ISP) réalise/vend un lien entre un terminal (PC) et son réseau IP. De manière logique le client est connecté via une liaison point à point (PPP, ADSL...) à un intranet (domaine) géré par l'ISP, qui loge les serveurs abritant les services (messagerie, site WEB, ...) et offre généralement des éléments de sécurité (pare-feu, protection contre les virus ...).



Le protocole RADIUS

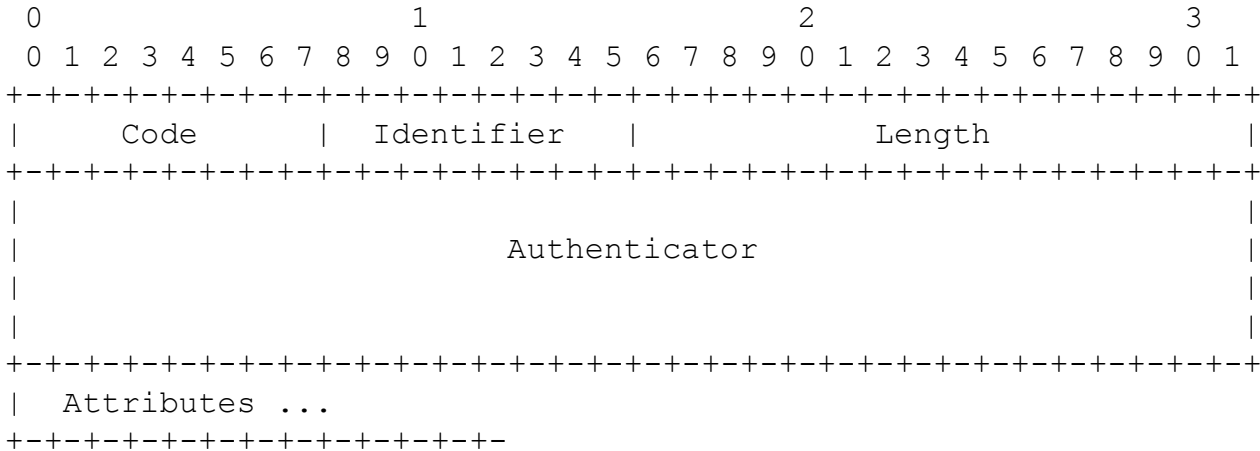
- ✚ Permet d'échanger des services entre fournisseurs de service.
- ✚ Network Access Server (NAS), est un serveur réalisant l'authentification d'un utilisateur désirant accéder au réseau (connexion PPP, accès sans fils...).
- ✚ NAS se comporte comme le client d'un serveur d'authentification RADIUS qui stocke les paramètres d'authentification de l'utilisateur et ses droits.
- ✚ Les messages entre NAS et serveur RADIUS sont signés à l'aide d'un secret partagé et d'une empreinte MD5.
- ✚ Le protocole RADIUS est également utilisé pour la facturation.



- ✚ Le NAS génère des requêtes *Access-Request*, associées à un nombre aléatoire de 16 octets (le champ *Authenticator*). La réponse du serveur d'authentification est l'un des trois messages suivants
 - *Access-Challenge*
 - *Access-Reject*
 - *Access-Success*.
- ✚ Elle est signée par un nombre *Response Authenticator* (16 octets), une empreinte MD5 calculée à partir des données de la réponse, du champ *Authenticator* importé de la requête, et d'un *secret partagé* .
- ✚ De surcroît un paquet RADIUS comporte un attribut de signature (le *Message-Authenticator #80*), qui conformément à la RFC 2104, est déduit du secret partagé et du contenu du message.



Format des paquets RADIUS



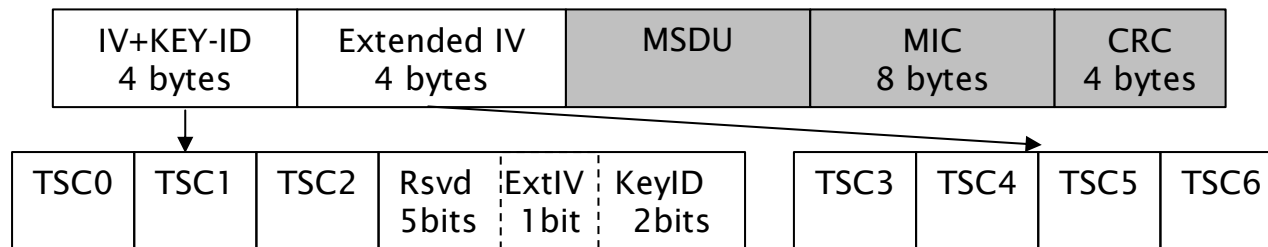
- ✚ **Code**
 - 1 Access-Request
 - 2 Access-Accept
 - 3 Access-Reject
 - 4 Accounting-Request
 - 5 Accounting-Response
 - 11 Access-Challenge
- ✚ **Identifiant**
 - Identifiant d'une requête et de la réponse associée.
- ✚ **Length**
 - Longueur totale du paquet en tête incluse (à partir du champ code).
- ✚ **Authenticator**
 - Un champ de 16 octets. C'est un nombre aléatoire dans le cas d'un message access-request.
 - Pour les paquets access-accept, access-reject, access-challenge, accounting-response c'est l'empreinte MD5 du message (en tête incluse, à partir de code) concaténé aux valeurs RequestAuthenticator et secret partagé.
 - ResponseAuth = MD5(Code || ID || Length || RequestAuth || Attributes || Secret)
- ✚ **Attributes**
 - Type, un octet, l'identifiant d'un attribut (0..255)
 - Length, un octet, la longueur, champ type inclus (2,...255)
 - Value, la valeur de l'attribut



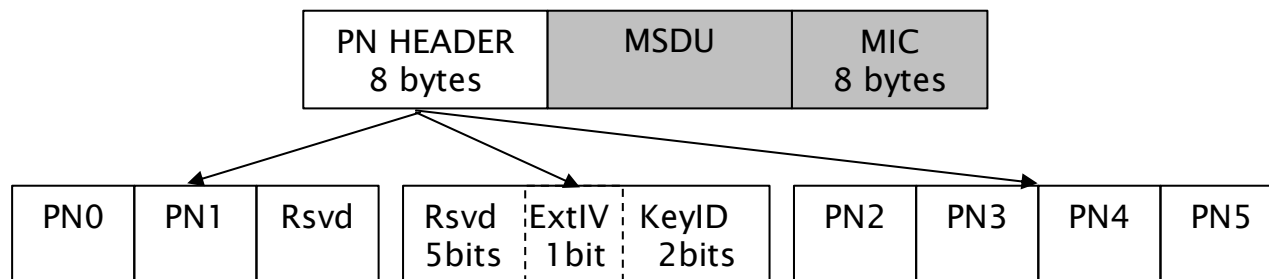
IEEE 802.11i



- + Définition des *Information Elements IE*.
- + Distribution des clés globales à l'aide d'un protocole à quatre passe.
- + Gestion de plusieurs protocoles radio
 - TKIP (RC4)
 - CCMP (AES)



Trame TKIP



Trame CCMP



✚ Éléments d'information IE

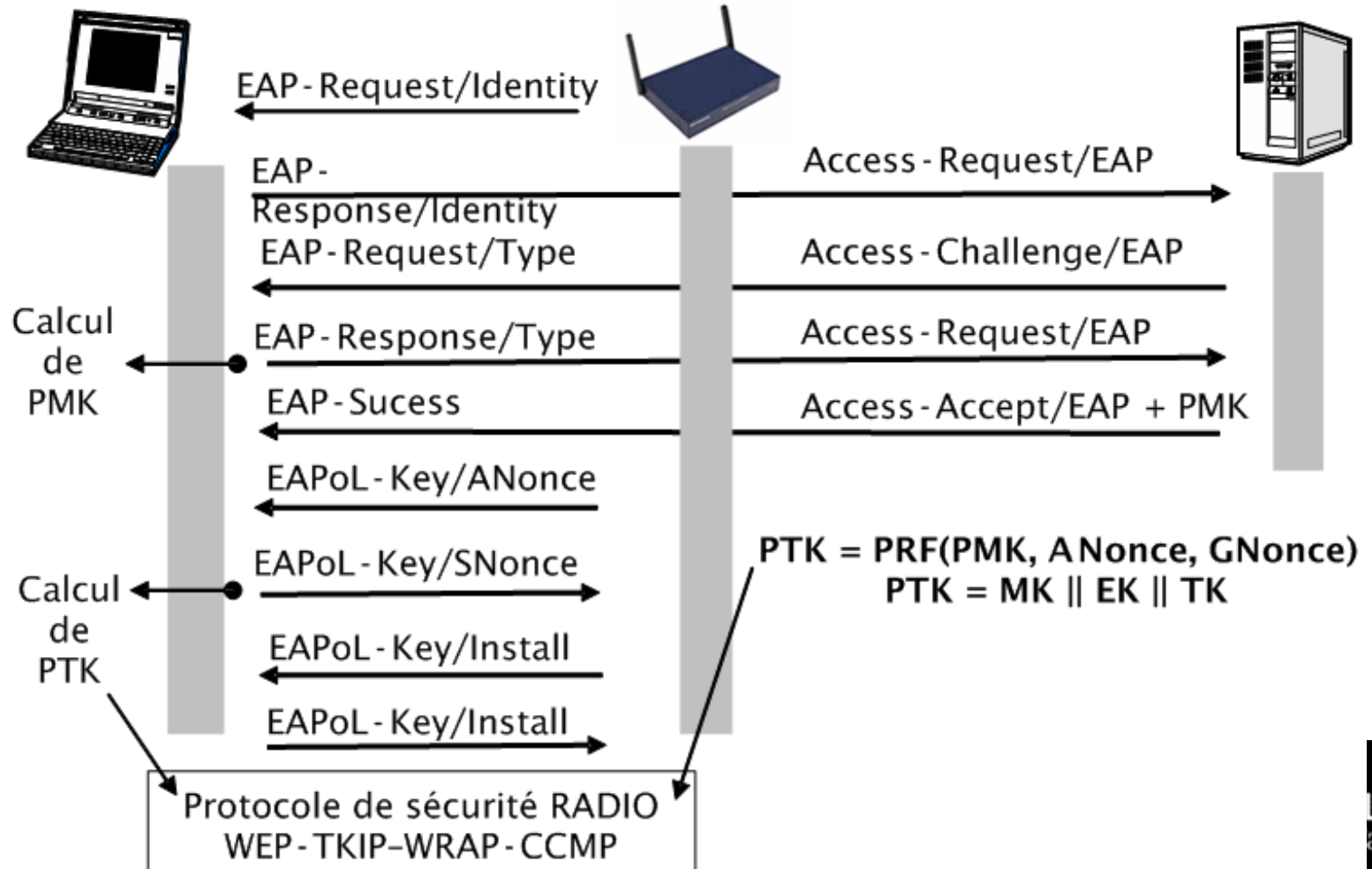
- Un point d'accès diffuse dans ses trames *Beacon* ou *Probe* des éléments d'information afin de notifier aux nœuds sans fil les informations suivantes,
 - La liste des infrastructures d'authentification supportées (typiquement 802.1X)
 - La liste des protocoles de sécurité disponibles (TKIP, CCMP,...)
 - La méthode de chiffrement pour la distribution d'une clé de groupe (GTK).
- Une station 802.11 notifie son choix par un élément d'information transmis lors de sa demande d'association.

✚ Distribution de clés avec mutuelle authentification entre AP et Supplicant.



Distribution des clés

- ✚ Four ways handshake (PTK).
- ✚ Two ways handshake (GTK).



802.11 i: Hiérarchie des clés

- ✚ PMK est déduite de l'authentification EAP.
- ✚ PSK est une alternative à PMK.
- ✚ GMK est une clé maître de groupe.

