Ressource R501

WiFi avancé

IUT de Béziers, dépt. R&T © 2004-2024
http://www.borelly.net/
Christophe.BORELLY@umontpellier.fr

Objectifs de la ressource

- Les étudiants seront capables de déployer et maintenir une infrastructure sans fil centralisée, ainsi que de mesurer la qualité de la couverture radio (puissance, canaux, débit, interférences, ...).

Contenus

- Normes (rappels)
- Couche physique (antennes, spectre, ...)
- Couverture radio
- Gestion centralisée (contrôleur)
- Sécurité (Authentification, Chiffrement, ...)

WLAN (Wireless LAN)

- Normes IEEE 802.11
- Points d'accès (**AP**) reliés au réseau fixe.
- Stations mobiles (**STA**).
- 4 usages principaux :
  - Les réseaux indépendants (**ad-hoc**)
  - Extension d'un réseau LAN (**infrastructure**)
  - L'interconnexion de réseaux LAN (ponts)
  - Création de réseaux maillés (**mesh**)

Produits

Les « lois » de la radio

- La puissance des ondes radio varie avec à la fréquence et la distance (Equation de FRIIS) :
  - $Pr_{dBm} \approx Pe_{dBm} + Ge_{dBi} + Gr_{dBi} - Pertes_{dB}$
  - $FreeSpaceLoss_{dB} = 32{,}4 + 20.Log10(f_{MHz}) + 20.Log10(d_{Km})$
- Puissance d'émission élevée :
  - Couverture plus grande, mais durée de vie des batteries plus faible...
- Fréquences radio élevées :
  - Couverture plus faible...

WECA / Wifi

- Interopérabilité entre constructeurs 802.11 certifiée par WECA (Wireless Ethernet Compagny Alliance 1999).
- Nouvelle appellation en octobre 2002
- Wifi Alliance (Wireless Fidelity)

Principales bandes de fréquences Wifi

- Bande des 2,4 GHz : Fn=2407+5.n MHz
  - 14 canaux de 22 MHz
  - 13 en Europe (max. 100 mW), 11 aux US
  - Utilisation jusqu'à 3 canaux (3 AP) sans chevauchement
- Bande des 5 GHz : Fn=5000+5.n MHz
  - Canaux de 20 MHz (19 en Europe)
    - 8 Canaux de 36 à 64 (intérieur max. 200 mW)
    - 11 Canaux de 100 à 140 (intérieur et extérieur max. 1 W)

802.11 (Wifi 0)

- Publiée en 1997
- Bande 2,4 GHz
- Étalement de spectre :
  - **FHSS** (Frequency Hopping Spread Spectrum)
  - **DSSS** (Direct Sequence Spread Spectrum)
- Débit maximum 2 Mbps.

802.11a (Wifi 2)

- Publiée en 1999
- Bande 5 GHz
- Étalement de spectre : **OFDM**
- Modulations : BPSK, QPSK, 16-QAM, 64-QAM
- Débits supportés :
  - 6, 12, 24, 36, 48 et 54 Mbps

802.11b (Wifi 1)

- Publiée en 1999
- Bande 2,4 GHz
- Étalement de spectre : **DSSS**
- Modulations :
  - **DBPSK**, **DQPSK** (11 chips)
  - **CCK** (Complementary Code Keying - 8 chips)
- Débits supportés : 1, 2, 5,5 et 11 Mbps
- Consommation plus faible que 802.11a

802.11g (Wifi 3)

- Publiée en 2003
- Bande 2,4 GHz (compatible 802.11b)
- Étalement de spectre : **DSSS** ou **OFDM**
- Débits supportés :
  - 1, 2, 5,5 et 11 Mbps
  - 6, 12, 24, 36, 48 et 54 Mbps

802.11n (Wifi 4)

- Publiée en 2009
- Bande 2,4 GHz et 5 GHz
- MIMO (Multiple Input Multiple Output) - Max. 4X4
- Intervalle de garde court : **SGI** = 400 ns
- Modulations : BPSK, QPSK, 16-QAM et 64-QAM
- **HT** (High Throuput) : 76 **MCS**
  - HT20 (20 MHz) : jusqu'à 72,2 Mbps (1 stream)
  - HT40 (40 MHz) : jusqu'à 150 Mbps (1 stream)
- En option, correction d'erreurs avec **LDPC** (Low-Density Parity Check)

Canaux de 40 MHz

- Channel bonding
- Canaux adjacents + ou – 20 MHz du canal primaire
- Notation (Numéro primaire, +/- 1)
  - Par exemple :
    - (36,+1) => canaux 36 et 40
    - (48,-1) => canaux 48 et 44
- Associations possibles, dans la bande des 2,4 GHz
  - HT40+ : 1-5, 2-6, 3-7, 4-8, 5-9, 6-10, 7-11, 8-12, 9-13
  - HT40- : 5-1, 6-2, 7-3, 8-4, 9-5, 10-6, 11-7, 12-8, 13-9

802.11ac (Wifi 5)

- Publiée en décembre 2013
- Bande des 5 GHz
- Bande des 2,4 GHz (d'après la norme 802.11n)
- Regroupement de canaux jusqu'à 160 MHz (**VHT**)
- MIMO - Max. 8X8
- MU-MIMO (Downlink multi-user MIMO)
  - 4 clients simultanés
- Débits de 433 Mbps à 6,77 Gbps
- Modulation supplémentaire : **256-QAM**

802.11ad

- Publiée en 2012
- Bande des 60 GHz (WiGig)
- 4 canaux de 2160 MHz en Europe
  - 58.32, 60.48, 62.64 et 64,8 GHz
- Débits jusqu'à 6,75 Gbps (sur moins de 10 m)
- Evolution 802.11ay (2019)
  - Channel bonding : 4 (8,64 GHz)
  - MU-MIMO : jusqu’à 4 flux de 44 Gbps (256-QAM)

802.11ax (Wifi 6/6E)

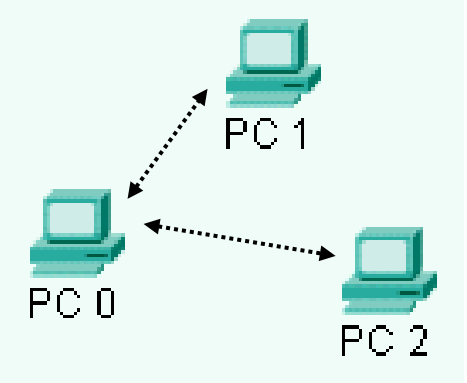
- Juillet 2019
- Bande 2,4 GHz et 5 GHz (WiFi 6)
- Bande 6 GHz (WiFi 6E)
- OFDMA (OFDM Access) : Version multi utilisateurs
  - Resource Unit (RU) : Groupe de sous porteuses
- Modulations jusqu'à 1024-QAM
- Débits MCS11 : 143.4 Mbps (20 MHz), 286.8 Mbps (40 MHz), 600.5 Mbps (80 MHz) et 1201 Mbps (160 MHz)
- Target Wake Time (TWT) : économie énergie
- Guard Interval : 0.8 µs, 1.6 µs ou 3.2 µs

Normes suivantes

- Wifi 7 (802.11be – 2024)
  - jusqu’à 23 Gbps (2.4, 5 et 6 GHz)
- Wifi 8 (802.11bn – d’ici 2028)
  - jusqu’à 100 Gbps ?
- ...

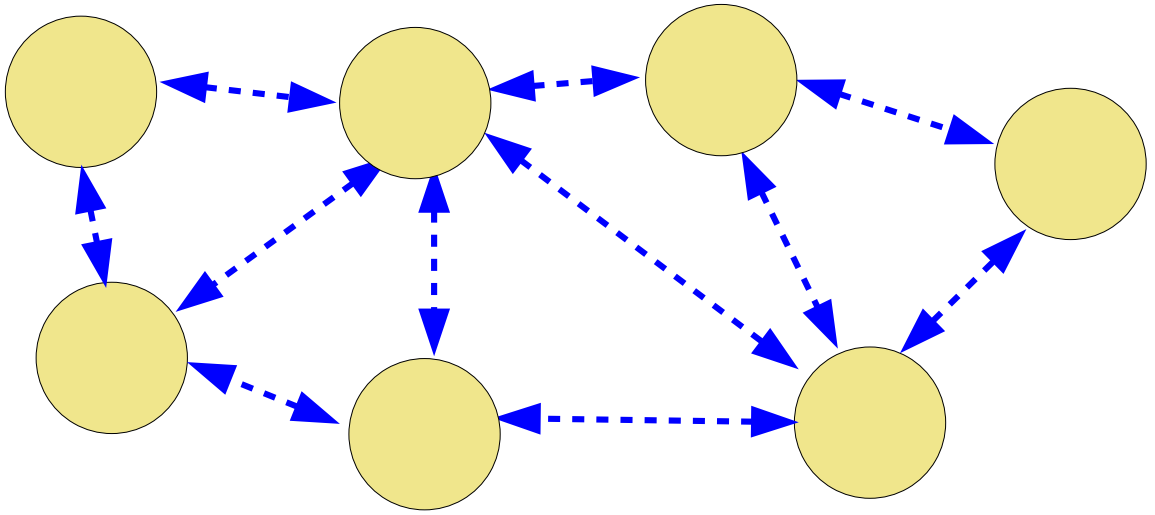
Mode ad-hoc

- En mode **ad-hoc** les machines sans fil se connectent les unes aux autres afin de constituer un réseau point à point (peer to peer en anglais), c'est-à-dire un réseau dans lequel chaque machine joue en même temps de rôle de client et le rôle de point d'accès.
- Dans chaque **IBSS** (Independant BSS), le BSSID est différent de l'adresse MAC de la machine maître.



Mode mesh

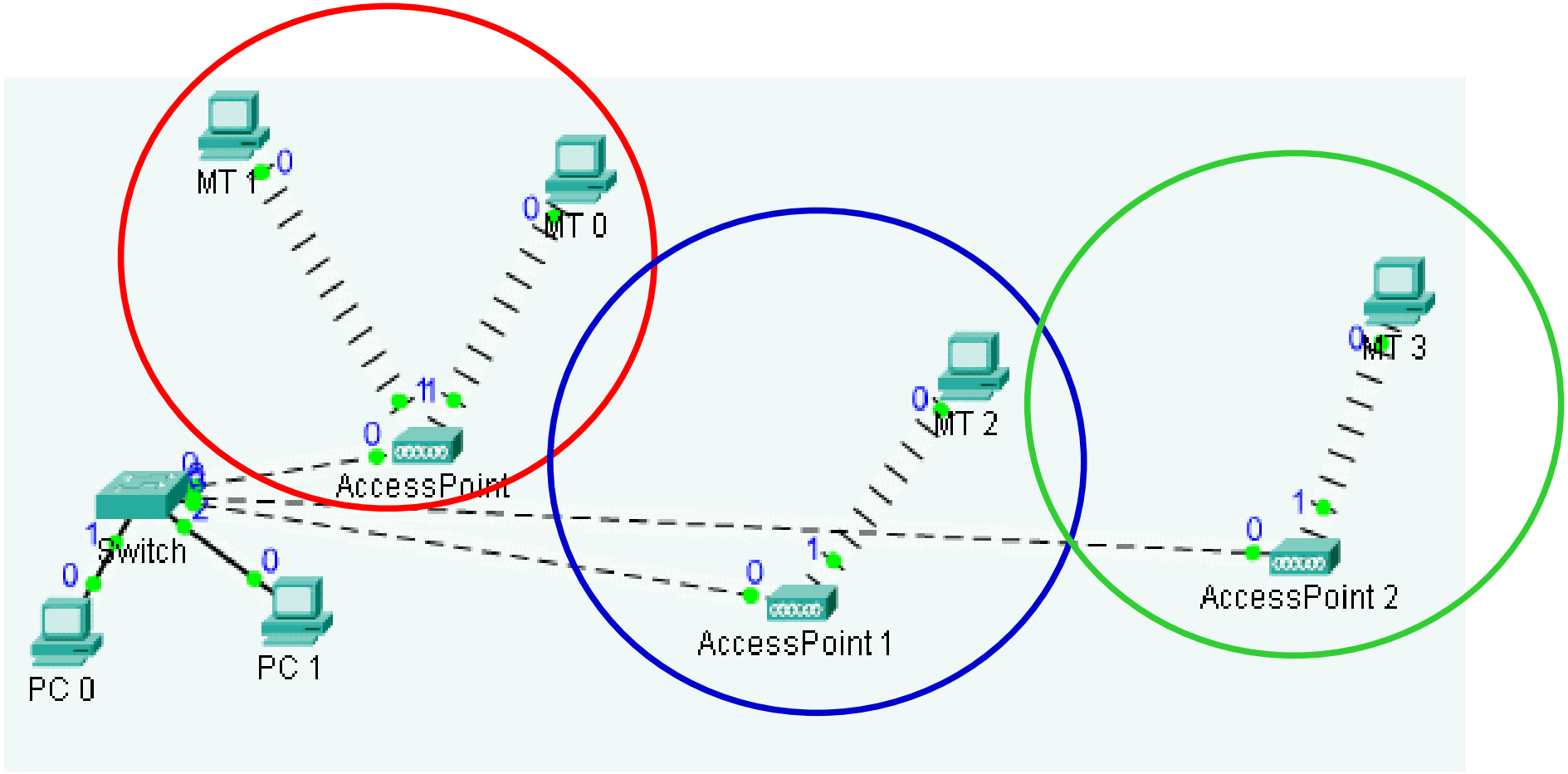
- En mode **mesh** (802.11s-2011), les machines sans fil se connectent avec leurs voisines afin de constituer un réseau maillé.
- Avec le système multi-sauts, les stations peuvent s'échanger des messages même si elles ne sont pas en « vision directe ».
- Le réseau est appelé **MBSS** (Mesh BSS).



Mode infrastructure

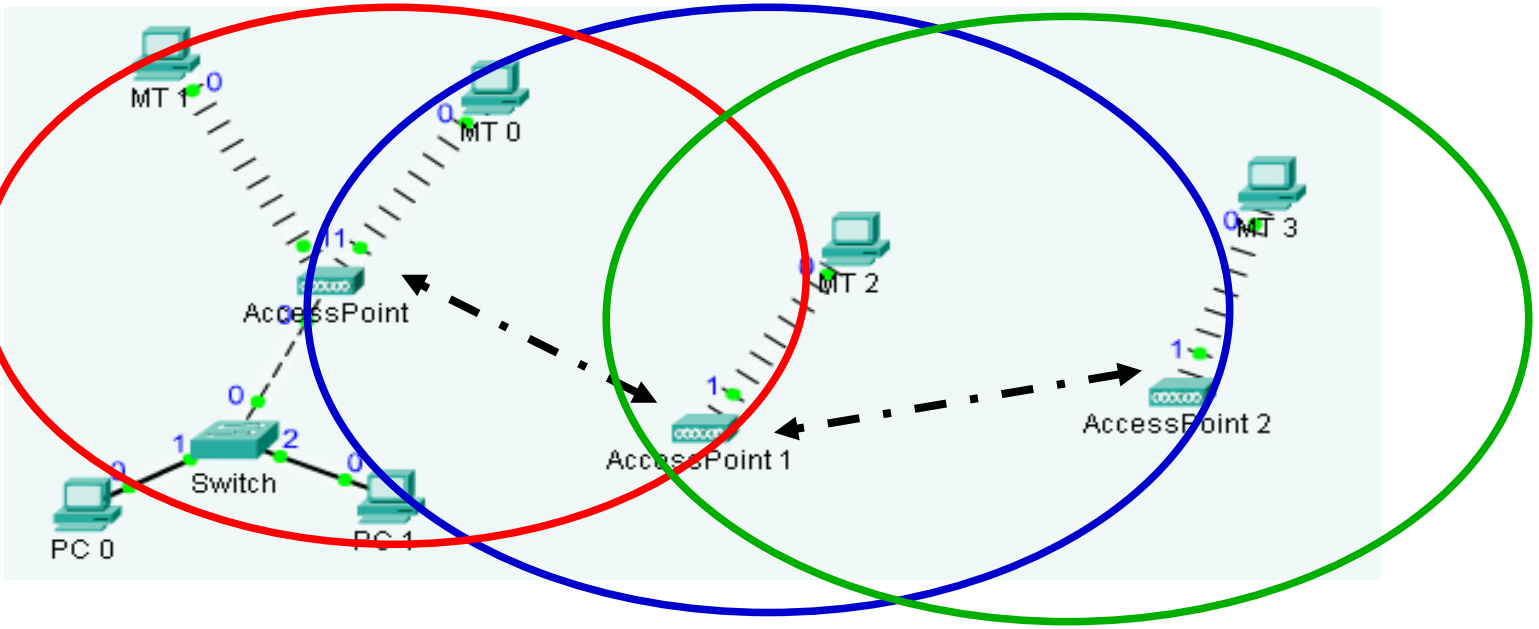
- Il faut au moins un point d'accès (**AP**).
- Un ESS (Extended Service Set) est repéré par un **ESSID** (ESS IDentifier), c'est-à-dire un identifiant de maximum 32 caractères de long (au format ASCII) servant de nom pour le réseau.
- L'ESSID, souvent abrégé en SSID.
- La connaissance du SSID est nécessaire pour qu'une station se connecte au réseau.

Extension d'un réseau LAN (1)



Extension d'un réseau LAN (2)

- **WDS** - Wireless Distribution System
- Configuration d'un point d'accès en répéteur
  - Permet d'étendre la zone de couverture
  - Partage de la bande passante totale sur toute la zone



Zone de couverture

- La zone de couverture est appelée ensemble de services de base (**BSS** : Basic Service Set).
- Chaque BSS est identifié par un **BSSID** (BSS IDentifier) de 6 octets (48 bits) qui correspond en général l'adresse MAC de l'équipement.
- Le système de distribution **DS** (Distribution System) permet d'interconnecter les BSS avec les autres réseaux.

Trames balise

- Chaque point d'accès diffuse toutes les 0.1 secondes environ, une trame balise (**beacon**) donnant des informations sur son BSSID, ses caractéristiques et éventuellement son SSID.
- Le SSID est automatiquement diffusé par défaut, mais on peut désactiver cette option.

La communication avec le point d'accès (1)

- Lors de l'entrée d'une station dans une cellule, celle-ci diffuse sur chaque canal une requête de sondage (PROBE REQUEST) contenant le SSID pour lequel elle est configurée ainsi que les débits que son adaptateur sans fil supporte.
- Si aucun SSID n'est configuré, la station écoute le réseau (Trames beacon) pour connaître les SSID existants.

La communication avec le point d'accès (2)

- L’AP vérifie le SSID de chaque PROBE REQUEST qu’il reçoit.
- Il répond (PROBE RESPONSE) avec des informations sur son paramétrage radio et sa sécurité.
- La station recevant la réponse peut ainsi constater la qualité du signal émis par le point d'accès afin de juger de la distance à laquelle il se situe.
- Si il y a plusieurs points d'accès accessibles, c'est la station qui choisit !
- L'identifiant d'association (AID) permet à l'AP de sauvegarder les trames pour un client qui s'est mis en mode d'économie d'énergie (Trames PS – Power Save).

Systèmes de sécurité

- **WEP** (Wireless Equivalent Privacy) (**RC4**) 1997
- **WPA** (Wifi Protected Access) - **TKIP** - 2003
  - WPA-PSK
  - WPA-Enterprise (802.1X)
- **WPA2** - **CCMP** (**AES**) 2004
  - WPA2-PSK
  - WPA2-Enterprise (802.1X)
- **WPA3** - **CCMP** - 2018
  - WPA3-SAE
  - WPA3-Enterprise (802.1X)

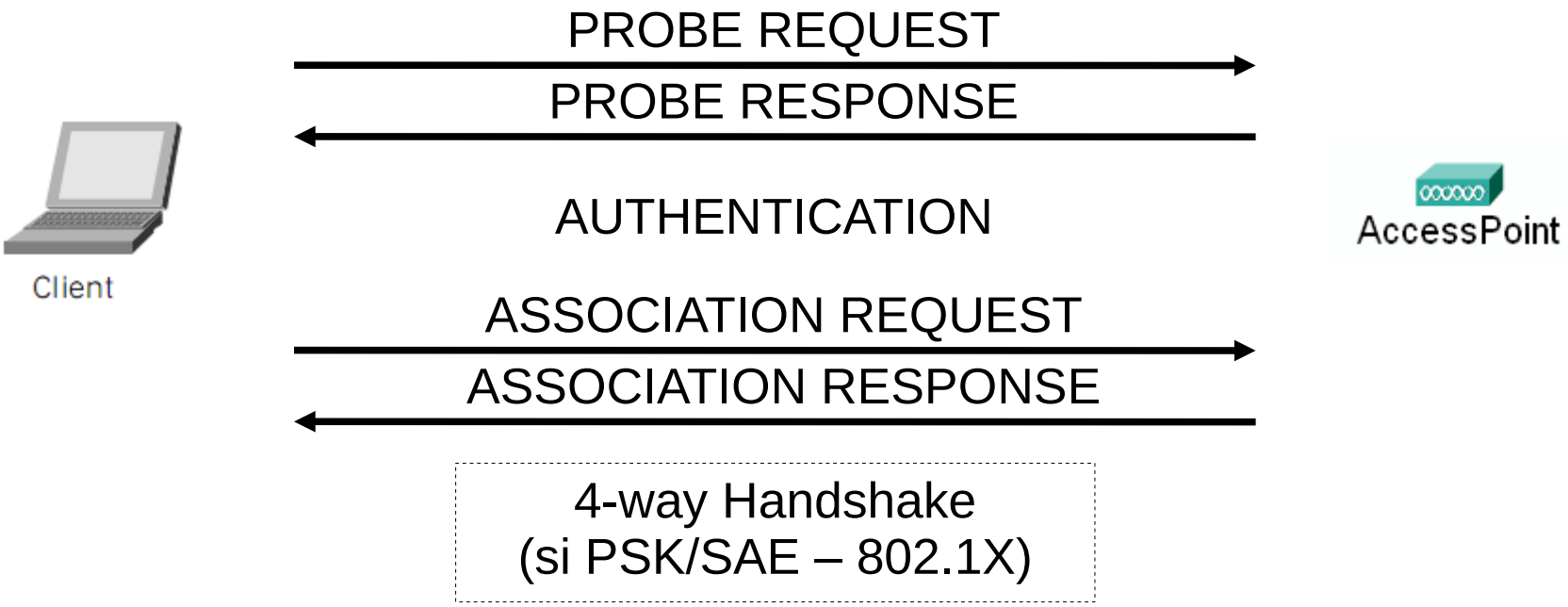
Algorithmes de chiffrement

- **RC4** (WEP et TKIP)
  - Rivest Cipher 4 – Ronald RIVEST 1987
  - Chiffrement symétrique par flot

- **AES** (CCMP)
  - Rijndael (Joan DAEMEN et Vincent RIJMEN)
  - Vainqueur du concours lancé en 1997 par le NIST
  - Chiffrement symétrique par blocs (16 octets)

Processus de connexion 802.11

- 3 étapes sont nécessaires (PROBE, AUTHENTICATION et ASSOCIATION) :



Authentifications

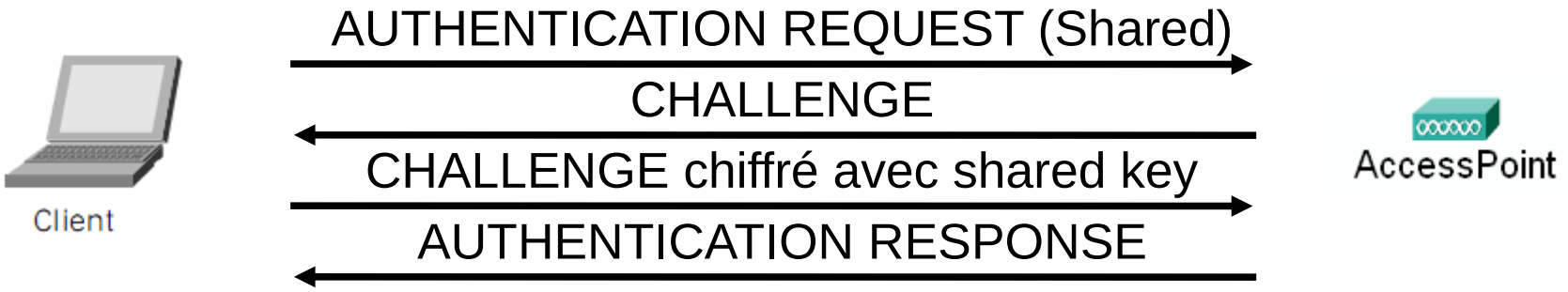
- La norme 802.11-2012 défini 4 systèmes d'authentification (page 73/2793) :
  - **Open system** (2 étapes, pas d'algorithme)
  - **Shared key** (4 étapes, mécanisme de challenge, nécessite une clé secrète **WEP**)
  - **SAE** : Simultaneous Authentication of Equals (4 trames)
  - **FT** (Fast BSS Transition) : 4 trames

Open System

- 2 trames (Status=0 => successful)
- Trame1 : 6 octets (Open Algo=0, SEQ=1, Status=0)
  - 00 00 01 00 00 00
- Trame 2 : 6 octets (Open Algo=0, SEQ=2, Status=0)
  - 00 00 02 00 00 00

Auth. Shared Key (WEP)

- 4 étapes sont nécessaires :
  - L'AP envoi un challenge qui sera chiffré par le client à l'aide de la clé secrète. En retour, si l'AP parvient à déchiffrer le message et retrouve le challenge, il en déduit que le client possède bien la même clé secrète que lui.



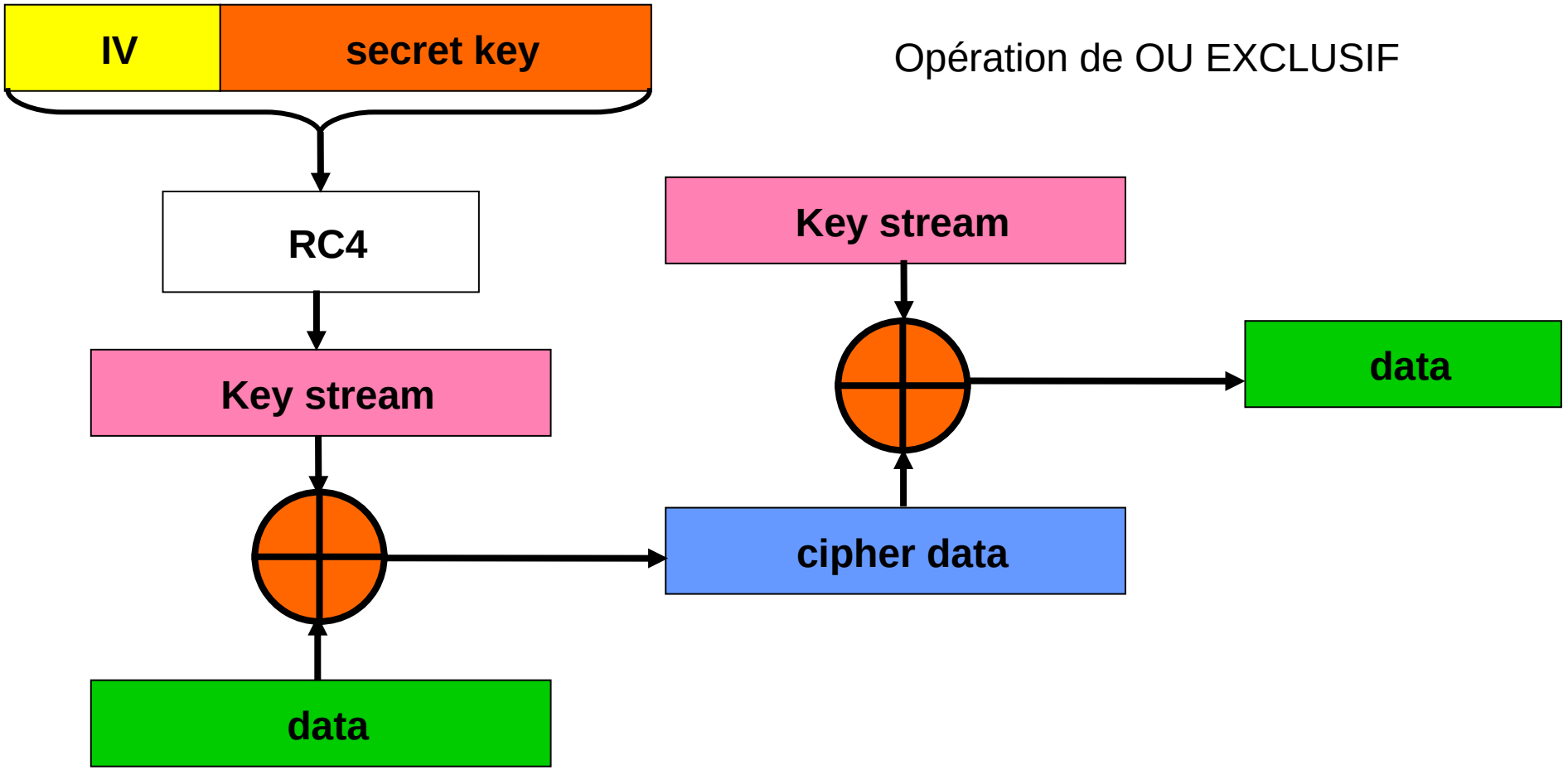
Protocoles de confidentialité et d'intégrité

- Depuis **RSN** (Robust Security Network – 802.11i-2004) :
  - **WEP** (Wireless Equivalent Privacy) est le système de chiffrement originel (Pre-RSNA).
  - **TKIP** (Temporal Key Integrity Protocol) est une évolution compatible avec WEP.
  - **CCMP** (Counter Mode/CBC-MAC Protocol) est le système de chiffrement le plus avancé.

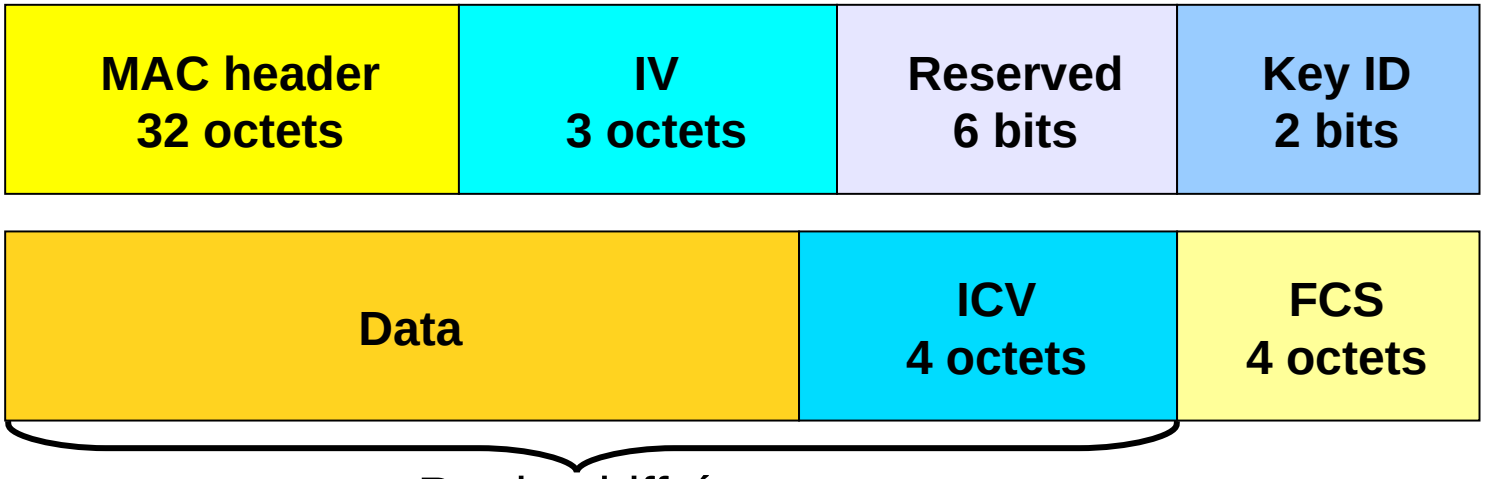
WEP

- Wireless Equivalent Privacy
- Algorithme RC4 (64, 128 jusqu’à 256 bits)
- Utilisation d'un vecteur d'initialisation IV (24 bits) pour éviter d'obtenir le même résultat chiffré à partir d'un même message en clair.
- En 64 bits, la clé utilisateur fait 40 bits (5 car. ou 10 digits hexadécimaux).
- En 128 bits (WEP2), la clé utilisateur fait 104 bits (13 car. ou 26 digits hexadécimaux).

Schéma WEP


IV
secret key
RC4
Key stream
Key stream
data
Opération de OU EXCLUSIF
Key stream
data
cipher data

Trame WEP (+8 octets)




```
▾ WEP parameters
    Initialization Vector: 0xaf0300
    Key Index: 0
    WEP ICV: 0x00640024 (not verified)
▾ Data (84 bytes)
  Data: 85dc0311e5ddb19dae17754d258b670
  [Length: 84]
```

Key ID est le numéro de clé à utiliser (0-3).
ICV (Integrity Check Vector) est un CRC-32 des données.
FCS (Frame Check Sequence) est un CRC-32 de la trame.

Déchiffrement WEP

- Pour déchiffrer, on utilise l'IV donné en clair dans la trame et le numéro de clé secrète (e.g. 0) pour calculer le keystream (la clé de chiffrement) en utilisant l'algorithme RC4.
- Ce keystream est ensuite « XORisé » aux données chiffrées.
- On peut ensuite vérifier la valeur de l'ICV des données pour voir s'il n'y a pas eu d'erreurs de transmission.

WPA
(Wifi Protected Access)

- **TSN** : Transition Security Network
- Compatible avec les versions précédentes.
- Utilisation de clés dynamiques pour chaque paquet et possède un système anti-re-jeu.
- Temporal Key Integrity Protocol (TKIP)
  - MIC - Message Integrity Check (Algo. Michael)
  - IV sur 48 bits : **TSC** (TKIP Sequence Counter)
  - Fonction de mélange (2 phases)

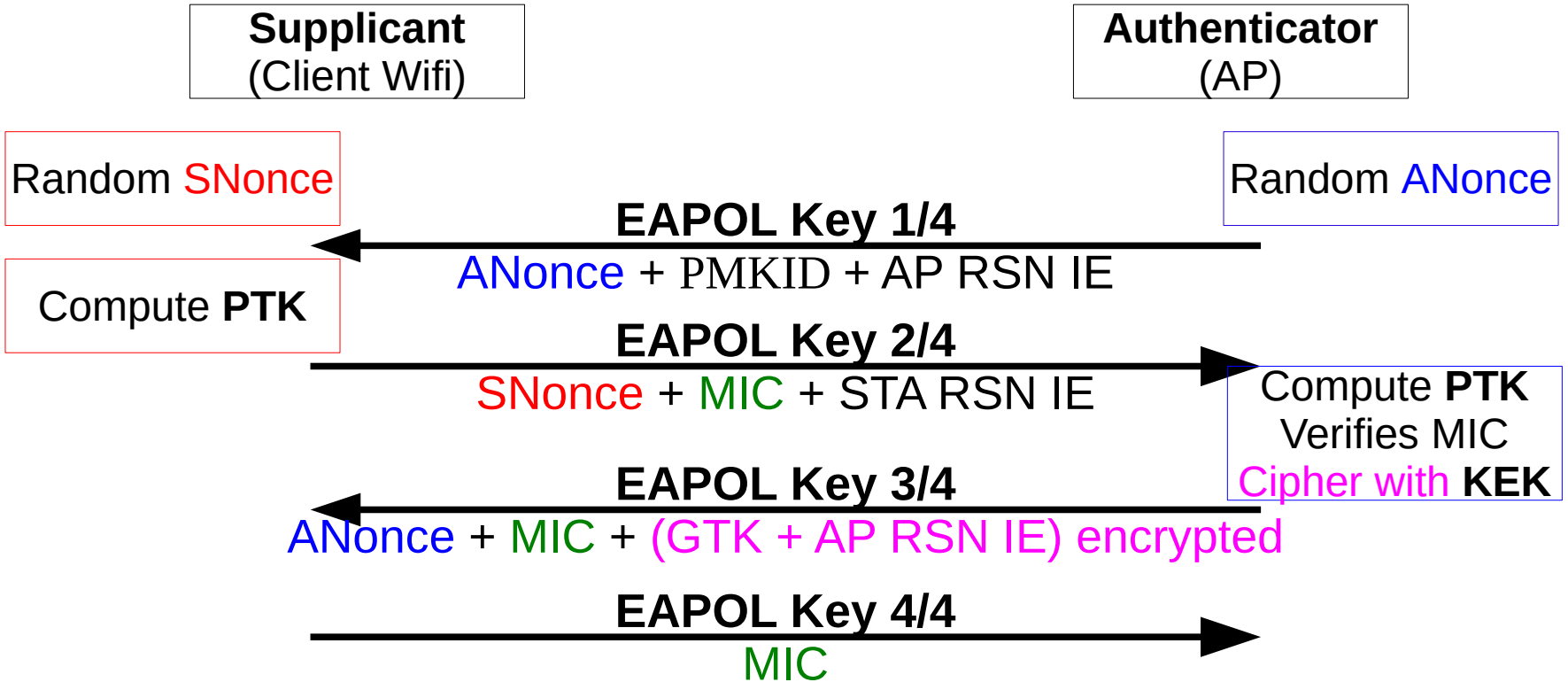
Modes de WPA

- 2 modes de fonctionnement existent :
  - **WPA-Personal** (ou **WPA-PSK**) : Pre-Shared Key
  - **WPA-Enterprise** qui ajoute une méthode d'authentification respectant la norme IEEE 802.1x/EAP et nécessitant l'utilisation d'un serveur RADIUS.

Échange de clés

- Le supplicant (le client wifi) et l'authenticator (le point d'accès) s'échangent des données (4-Way handshake) avec EAPOL (EAP Over LAN) pour obtenir la clé **PTK** (Pairwise Transient Key) utilisée pour le chiffrement des flots unicast.
- Cette clé est ensuite découpée :
  - **KCK** (Key Confirmation Key)
  - **KEK** (Key Encryption Key)
  - **TK** (Temporal Encryption Key)
  - **TMK1** et **TMK2** (Temporal MIC Key)

4-way handshake



WPA-PSK

- La pass phrase est transformée en PSK (Pre-Shared Key) sur 256 bits (32 octets)

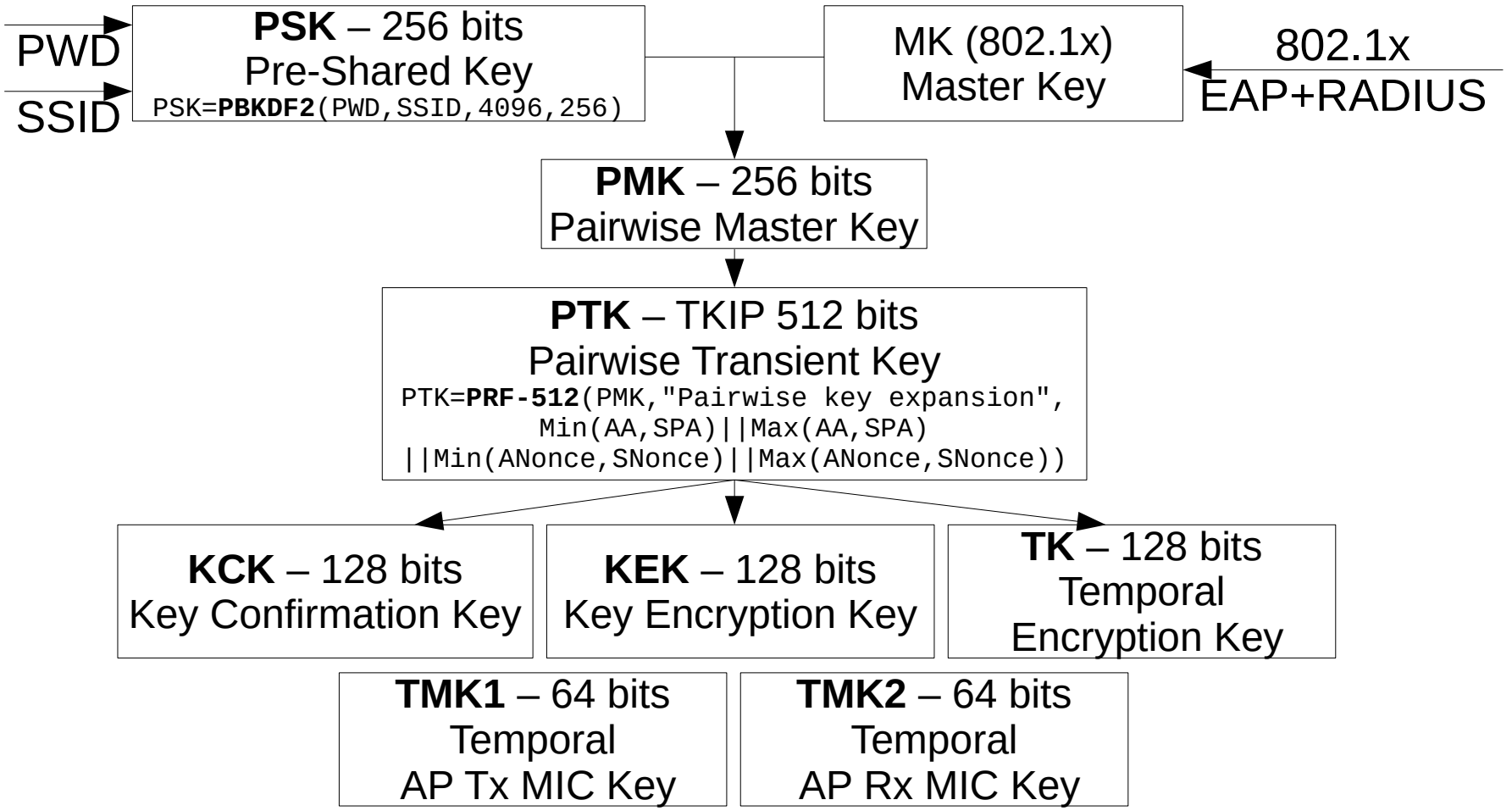
  `PSK=`**`PBKDF2`**`(PassPhrase,SSID,4096,256)`
- Fonction issue de PKCS #5 (RFC 2898)
- Vecteurs de tests RFC 6070
- On appele alors cette clé PMK (Pairwise Master Key)
- On dérrive ensuite la PTK (Pairwise Transient Key) à partir des adresses de l'authenticator (AA), du supplicant (SPA) ainsi que de 2 nombres ANonce et SNonce issus du 4-Way handshake EAPOL.

```
PTK=PRF-512(PMK,"Pairwise key expansion",
                Min(AA,SPA)||Max(AA,SPA)
    ||Min(ANonce,SNonce)||Max(ANonce,SNonce))
```

WPA-Entreprise

- Après la mise en place d'un tunnel TLS entre le serveur RADIUS et le supplicant (802.1X), on utilise la clé de session **MK** (Master Session Key) comme **PMK** (Pairwise Master Key).
- Cette clé est envoyée au point d'accès (Authenticator) dans l'attribut Vendor Specific **MS-MPPE-RECV-KEY** du paquet Radius Access-Accept.
- Le calcul de PTK est identique.

Hiérarchie des clés



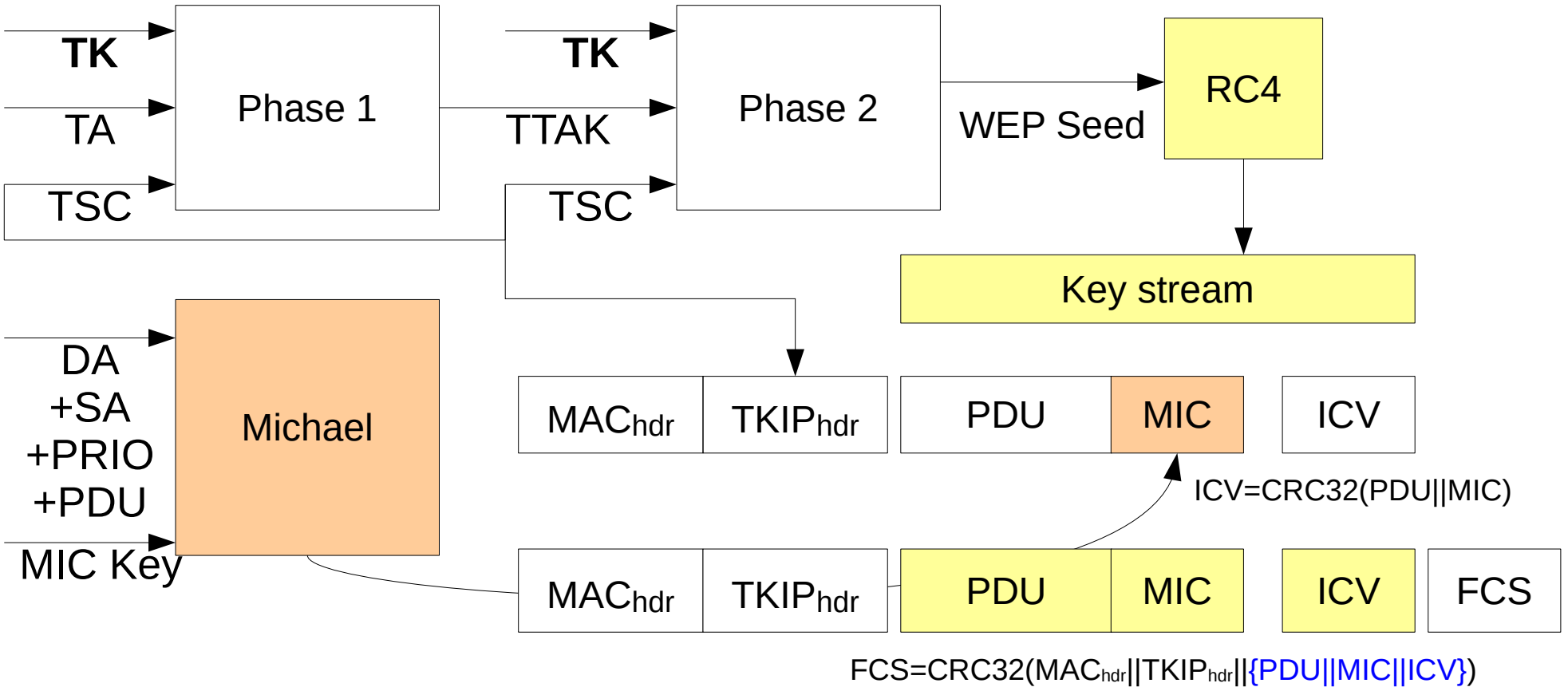
Fonctions de mélange TKIP

- L’équivalent de la clé WEP est générée en 2 phases à partir de l'adresse TA (Transmitter Address), la clé temporaire **TK** (Temporal encryption Key) et les 48 bits **TSC** (TKIP Sequence Counter).
- TTAK := Phase1 (TA, TK, TSC)
  - TKIP mixed Transmit Address and Key
- WEP seed := Phase2 (TTAK, TK, TSC)

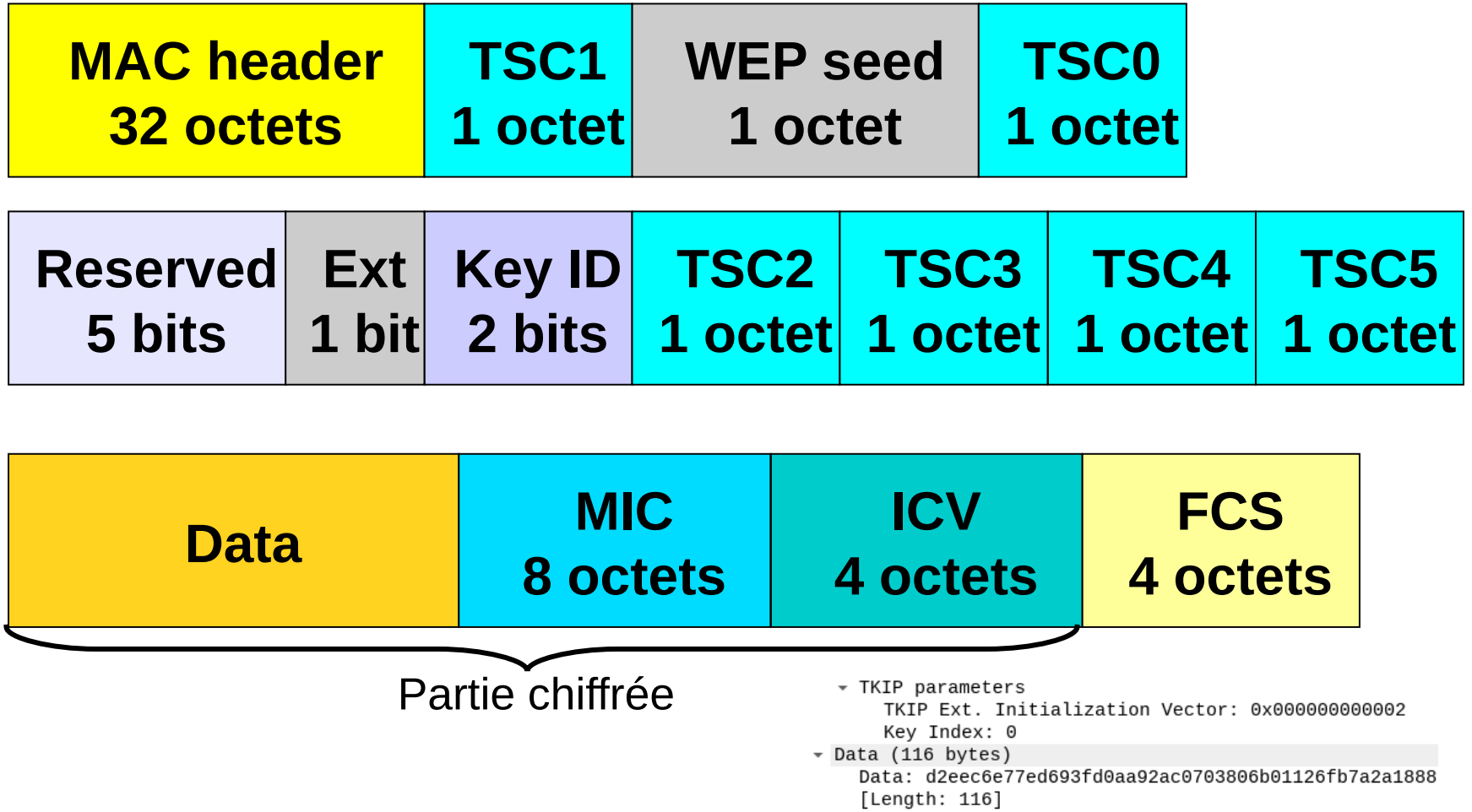
Algorithme Michael

- Le message d'intégrité est calculé à partir des éléments suivants du message (MSDU – Mac Service Data Unit) :
  - Adresse DA (Destination Address)
  - Adresse SA (Source Address)
  - Champ priorité (e.g. 4 octets : 00000000)
  - Données
- Le résultat fait 8 octets (cf. page 1196/2793 802.11-2012).

TKIP
(Temporal Key Integrity Protocol)



Trame TKIP (+20 octets)

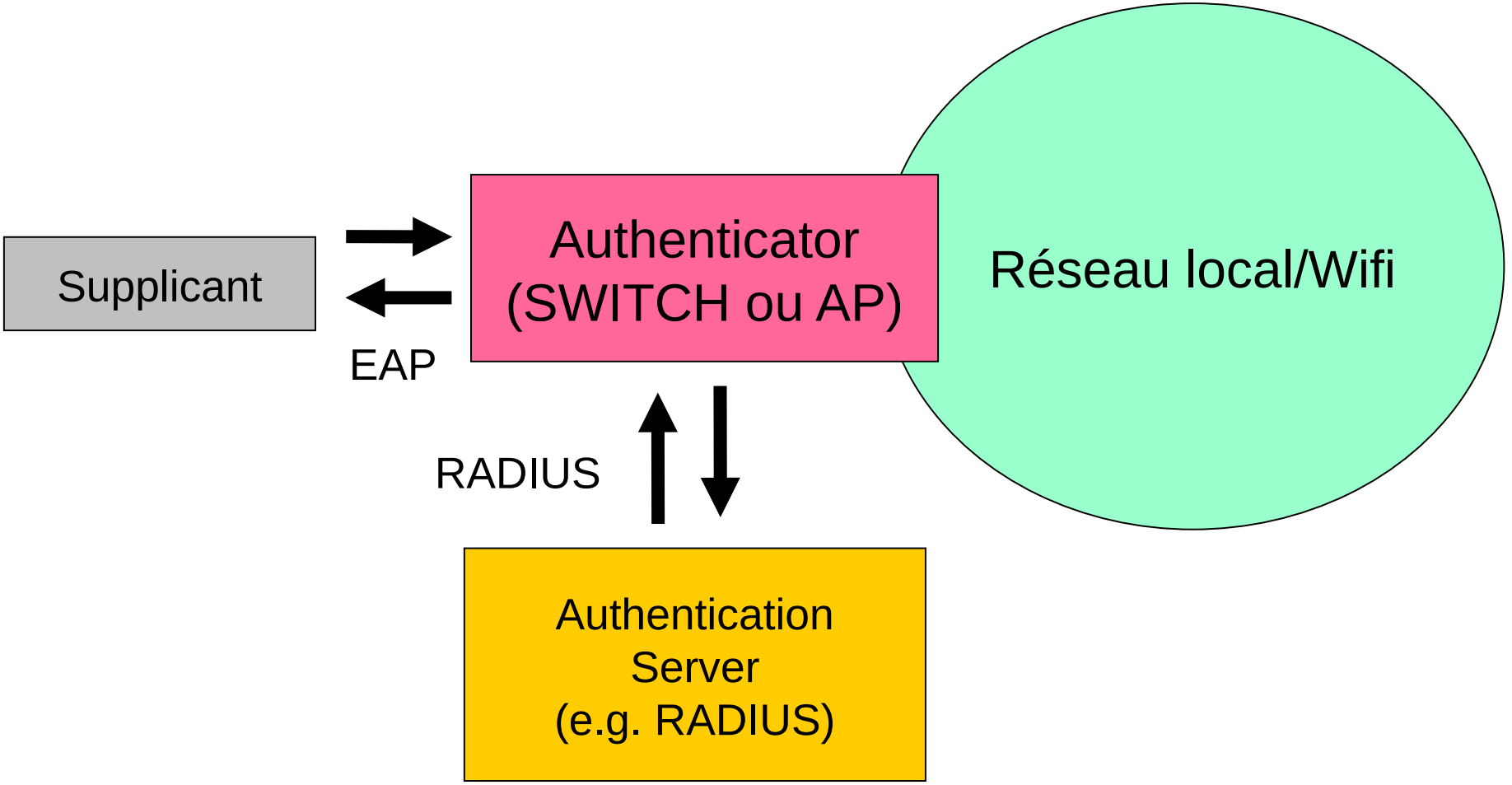



```
▾ TKIP parameters
    TKIP Ext. Initialization Vector: 0x000000000002
    Key Index: 0
▾ Data (116 bytes)
  Data: d2eec6e77ed693fd0aa92ac0703806b01126fb7a2a1888
  [Length: 116]
```

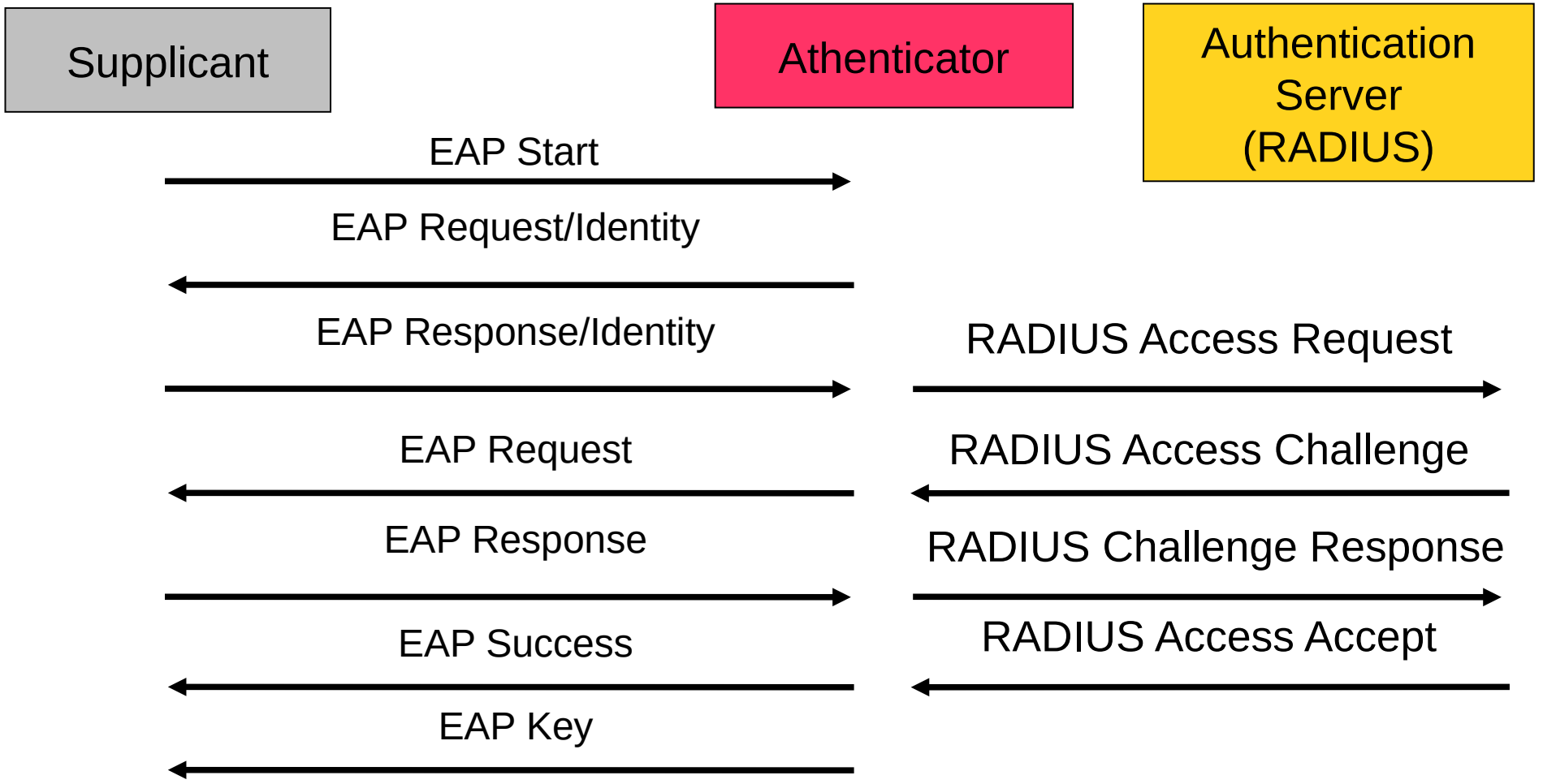
802.1X

- Le protocole entre le client (“Supplicant”) et l’équipement d'interconnexion (“Authenticator” - e.g. le commutateur ou la borne Wifi) est **EAP** (Extensible Authentication Protocol).
- La requête est ensuite mise au format RADIUS (Remote Authentication Dial-In User Service) et envoyée vers le serveur d’authentification (AS).
- Suivant la réponse du serveur, l’accès au réseau local est ouvert ou non par l’Authenticator.

802.1X
Port-Based Authentication



EAP (RFC 3748 – 4137)



EAP (1)

- **EAP-MD5** : Challenge MD5 équivalent au protocole CHAP de PPP CHAP [RFC 1994]. Non résistant aux attaques par dictionnaire, pas d'authentification mutuelle.
- **LEAP** (Lightweight EAP) : C'est un protocole propriétaire (CISCO) qui utilise une combinaison username/password pour l'authentification. Il est considéré comme non suffisamment sécurisé et il vaut mieux utiliser PEAP.
- **EAP-TLS** [RFC 2716] : Crée une session TLS entre le Supplicant et l'Authentication Server avant l'utilisation de EAP. Le serveur et le client ont besoin de certificats valides car l'authentification se fait dans les deux sens.

EAP (2)

- **PEAP** (Protected EAP): Mise en place d'un tunnel TLS avant d'envoyer les données d'authentification. Le serveur d'authentification fourni un certificat, le supplicant s'authentifie par user/mot de passe (**MS-CHAPv2**).
- **EAP-TTLS** : Idem PEAP avec un transport des données d'authentification encapsulées dans des paquets AVP (Attributes Value Pair). Développé par Funk Software et Certicom.
- EAP-SIM, EAP-AKA, EAP-FAST, EAP-PAX...

RADIUS (RFC 2865)

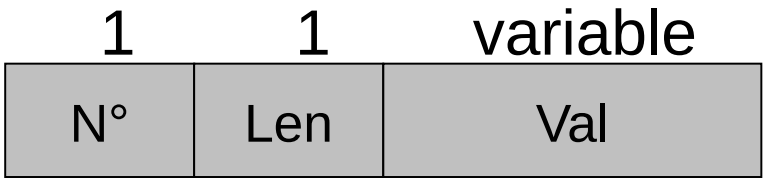
- Système **AAA**
  - Authentification
  - Autorisation
  - Accounting
- Port UDP
  - 1812 (Authentification, Autorisation)
  - 1813 (Accounting – comptabilité)
- Echanges Requêtes/Réponses avec les clients Radius (NAS – Network Access Server)

Paquets RADIUS

- 255 types de paquets (cf. RFC 3575)
  - Access-Request (1)
  - Access-Challenge (11)
  - Access-Accept (2)
  - Access-Reject (3)
  - Accounting-Request (4)
  - Accounting-Response (5)

Attributs RADIUS

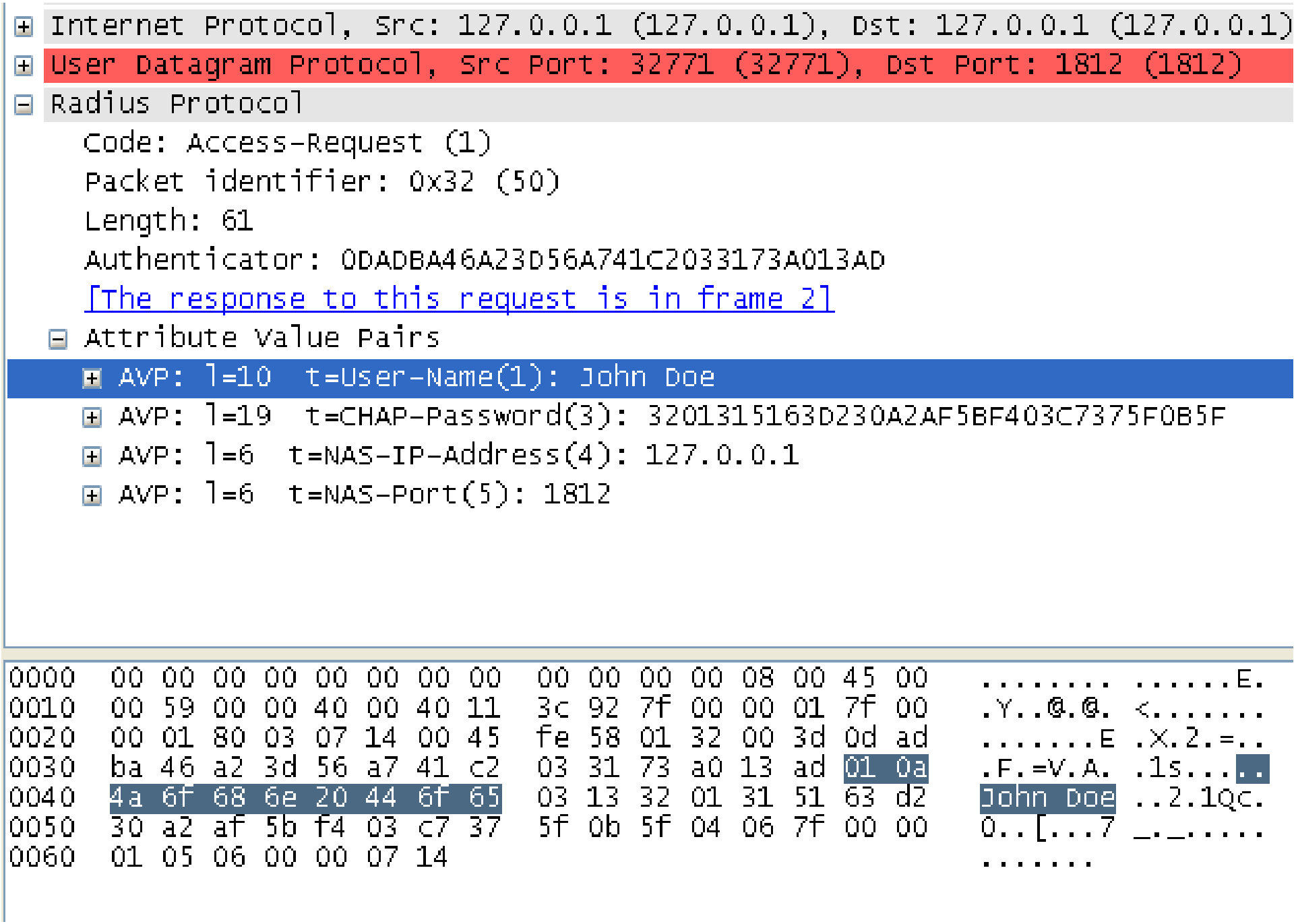
- AVP : Attributes Value Pair



- User-Name (1)
- User-Password (2)
- CHAP-Password (3)
- NAS-IP-Address (4)
- NAS-Port (5)
- Vendor Specific (26)
- Called-Station-Id (30)
- Calling-Station-Id (31)
- Nas-Identifier (32)
- ...

Extensions RADIUS (RFC 2868 - 2869)

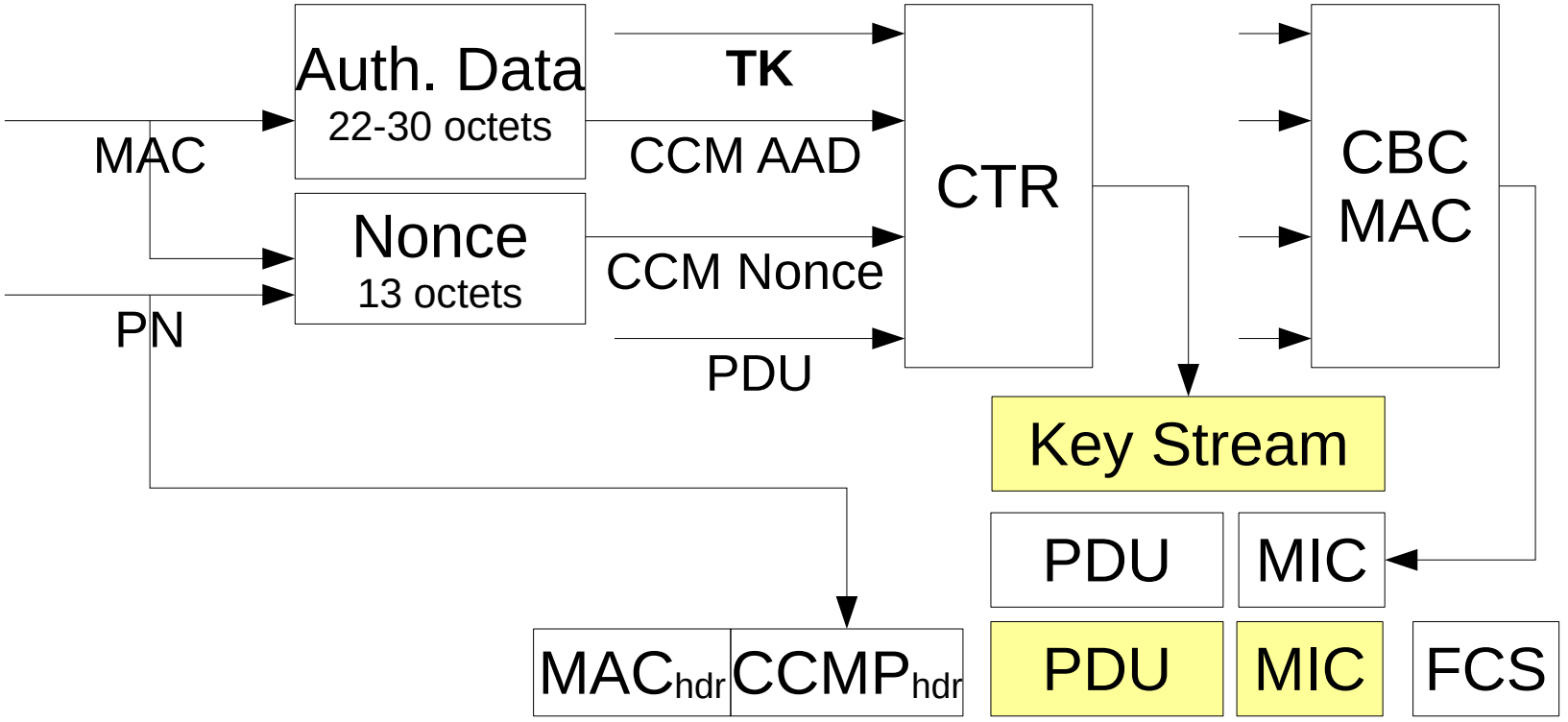
- Support VLAN :
  - Tunnel-Type (64) : 13
  - Tunnel-Medium-Type (65) : 802
  - Tunnel-Private-Group-Id (81) : Numéro de VLAN
- EAP-Message (79)
- Message-Authenticator (80)


Internet Protocol, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
User Datagram Protocol, Src Port: 32771 (32771), Dst Port: 1812 (1812)
Radius Protocol
Code: Access-Request (1)
Packet identifier: 0x32 (50)
Length: 61
Authenticator: 0DADBA46A23D56A741C2033173A013AD
[The response to this request is in frame 2]
Attribute Value Pairs
AVP: l=10 t=User-Name(1): John Doe
AVP: l=19 t=CHAP-Password(3): 3201315163D230A2AF5BF403C7375F0B5F
AVP: l=6 t=NAS-IP-Address(4): 127.0.0.1
AVP: l=6 t=NAS-Port(5): 1812
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 ....E.
0010 00 59 00 00 40 00 40 11 3c 92 7f 00 00 01 7f 00 .Y..@.@. <.....
0020 00 01 80 03 07 14 00 45 fe 58 01 32 00 3d 0d ad .....E .X.2.=..
0030 ba 46 a2 3d 56 a7 41 c2 03 31 73 a0 13 ad 01 0a .F.=V.A. .1s.....
0040 4a 6f 68 6e 20 44 6f 65 03 13 32 01 31 51 63 d2 John Doe ..2.1Qc.
0050 30 a2 af 5b f4 03 c7 37 5f 0b 5f 04 06 7f 00 00 0..[...7 _._.....
0060 01 05 06 00 00 07 14 .....

IEEE 802.11i ou WPA2

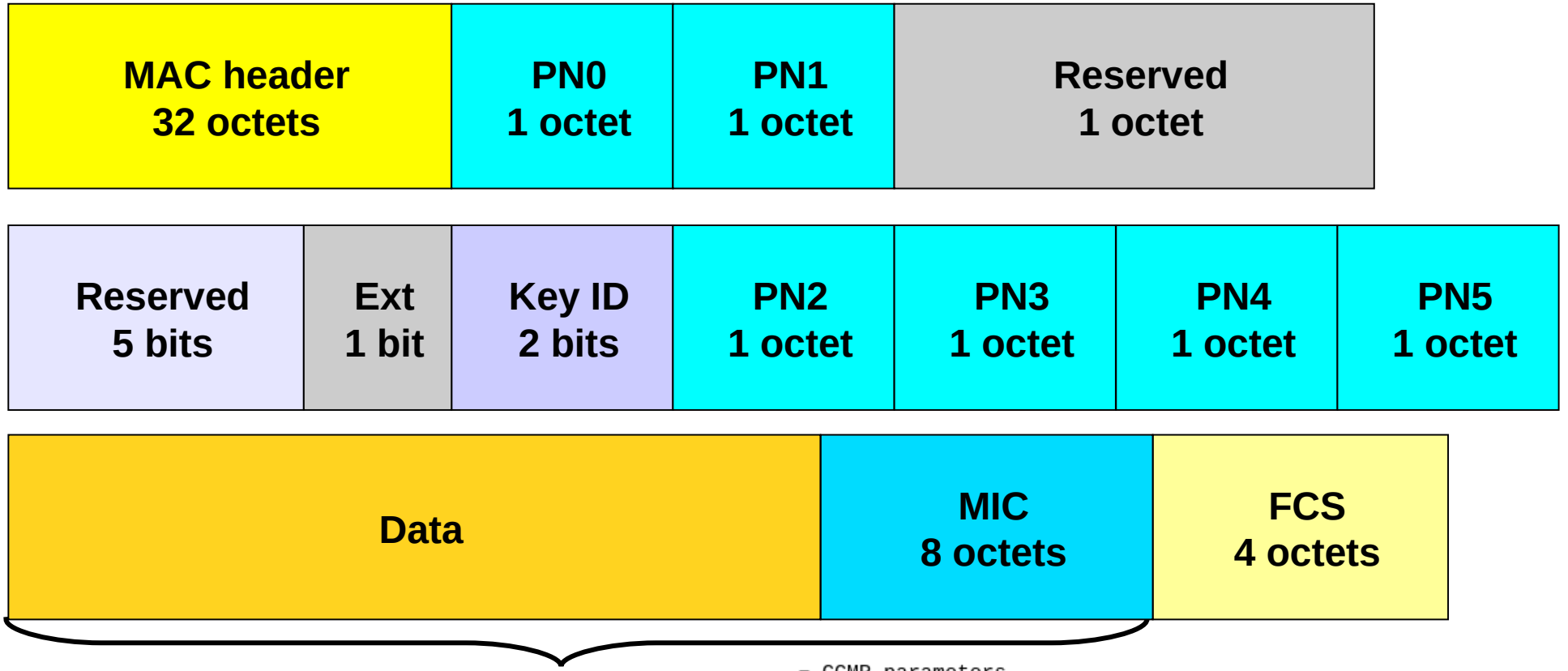
- **RSN** - Robust Security Network
- CCMP (Counter Mode/CBC-MAC Protocol)
  - Counter Mode : confidentialité
  - CBC-MAC : intégrité
- RFC 3610
- Algorithme AES
- Finalisation en juin 2004

CCMP (CTR CBC-MAC Protocol)



FCS=CRC32(MAC$_{hdr}$||CCMP$_{hdr}$||{PDU||MIC})

Trame CCMP (+16 octets)




```
▾ CCMP parameters
    CCMP Ext. Initialization Vector: 0x000000000001
    Key Index: 0
▾ Data (112 bytes)
  Data: bb443aba2efa2dfc58fb5500dbfd1c29c2b86a092a8813
  [Length: 112]
```

WPA3

- Avril 2018
- Forward secrecy
- Nécessite **MFP** (802.11w-2009 PMF)
  - Management Frames Protection
- Plus de PSK => Utilisation de SAE
- WPA3-Enterprise : 192 bits
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Auth. SAE

- **S**imultaneous **A**uthentication of Equals
- Depuis 802.11s-2011 (mesh)
- Authentification par mot de passe sécurisé
- Variante de Dragonfly Key Exchange (RFC 7664)
- Basé sur un échange de clé Diffie-Hellman utilisant des groupes cycliques finis (modulo p) :
  - **ECC** (Elliptic Curve Cryptography)
  - **FFC** (Finite Field Cryptography)

Détermination de PWE

- **P**ass**W**ord **E**lement

```
counter,z = 1,len(p)
pwd-seed = H(MAX(A-MAC,B-MAC)||MIN(A-MAC,B-MAC),password||counter)
pwd-value = KDF-z(pwd-seed,"SAE Hunting and Pecking", p)
```

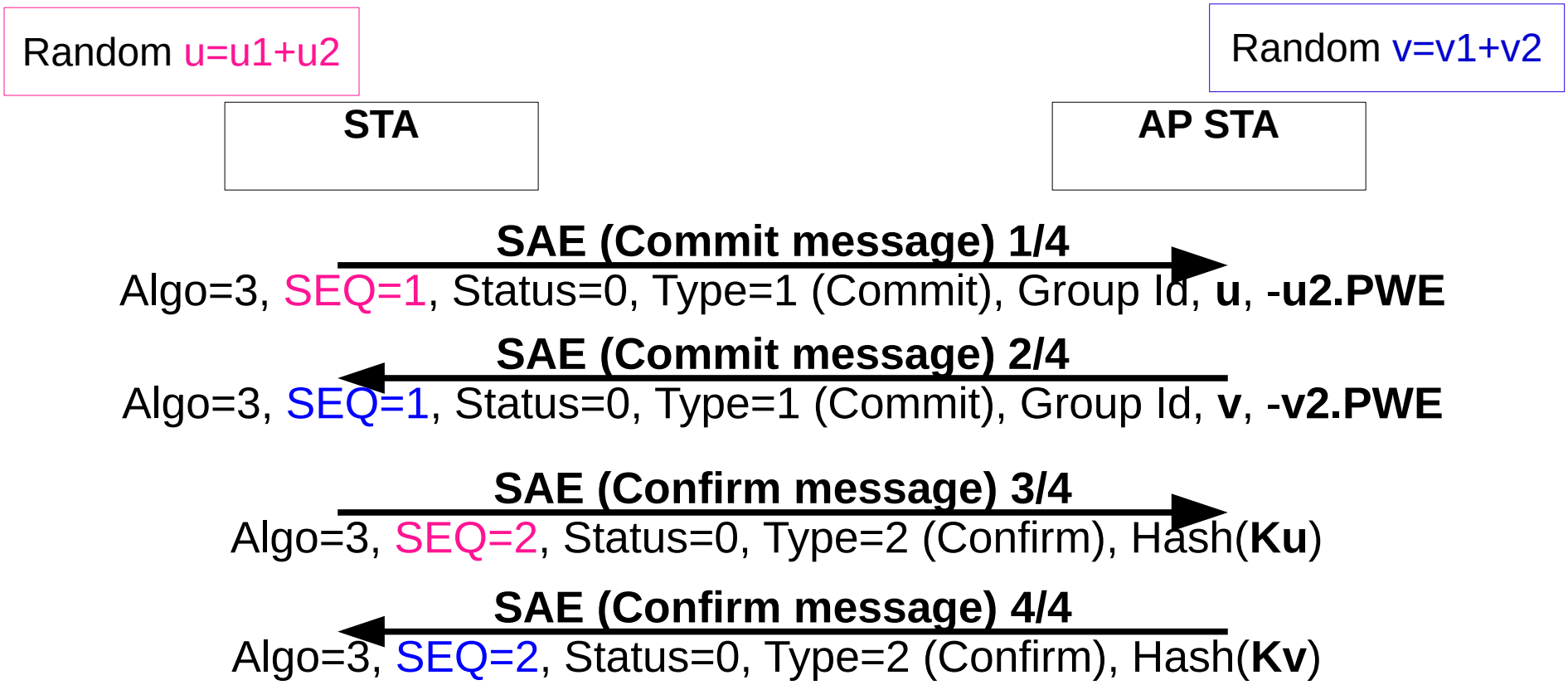
- ECC : Point sur une courbe elliptique

```
x = pwd-value
Si il existe y tel que y² = x³ + ax + b modulo p
Si LSB(pwd-seed)=LSB(y) alors PWE=(x,y) sinon PWE=(x,p–y)
```

- FCC : Valeur modulo p (r est l'ordre du groupe)

```
PWE = pwd-value^((p-1)/r) modulo p
```

Trames SAE (ECC)



PWE=function(Group Id,pwd,MACu,MACv) p1177-1179 IEEE802.11-2012
Ku=u1.(v.PWE-v2.PWE)=u1.v1.PWE
Kv=v1.(u.PWE-u2.PWE)=v1.u1.PWE

Fast BSS Transition (1)

- Norme 802.11r-2008 (Support indiqué dans les beacons)
- Itinérance (Roaming)
- Lorsqu'un utilisateur nomade passe d'un AP à un autre lors de son déplacement au sein de l'ESS, l'adaptateur réseau sans fil est capable de changer de point d'accès selon la qualité de réception des signaux provenant des différents points d'accès.
- FT permet d’accélérer le processus d’association sans avoir a refaire le 4 way-handshake (e.g. se ré-authentifier sur le serveur RADIUS - 802.1X)

Fast BSS Transition (2)

- FTO (FT Originator)
  - Over-the-Air ou Over-the-DS
- Première association : 8 trames
  - 2 auth. + 2 assoc. + 4 way-handshake
- FT re-association : 4 trames
  - 2 FT authentication
  - 2 FT re-association

FT initial association

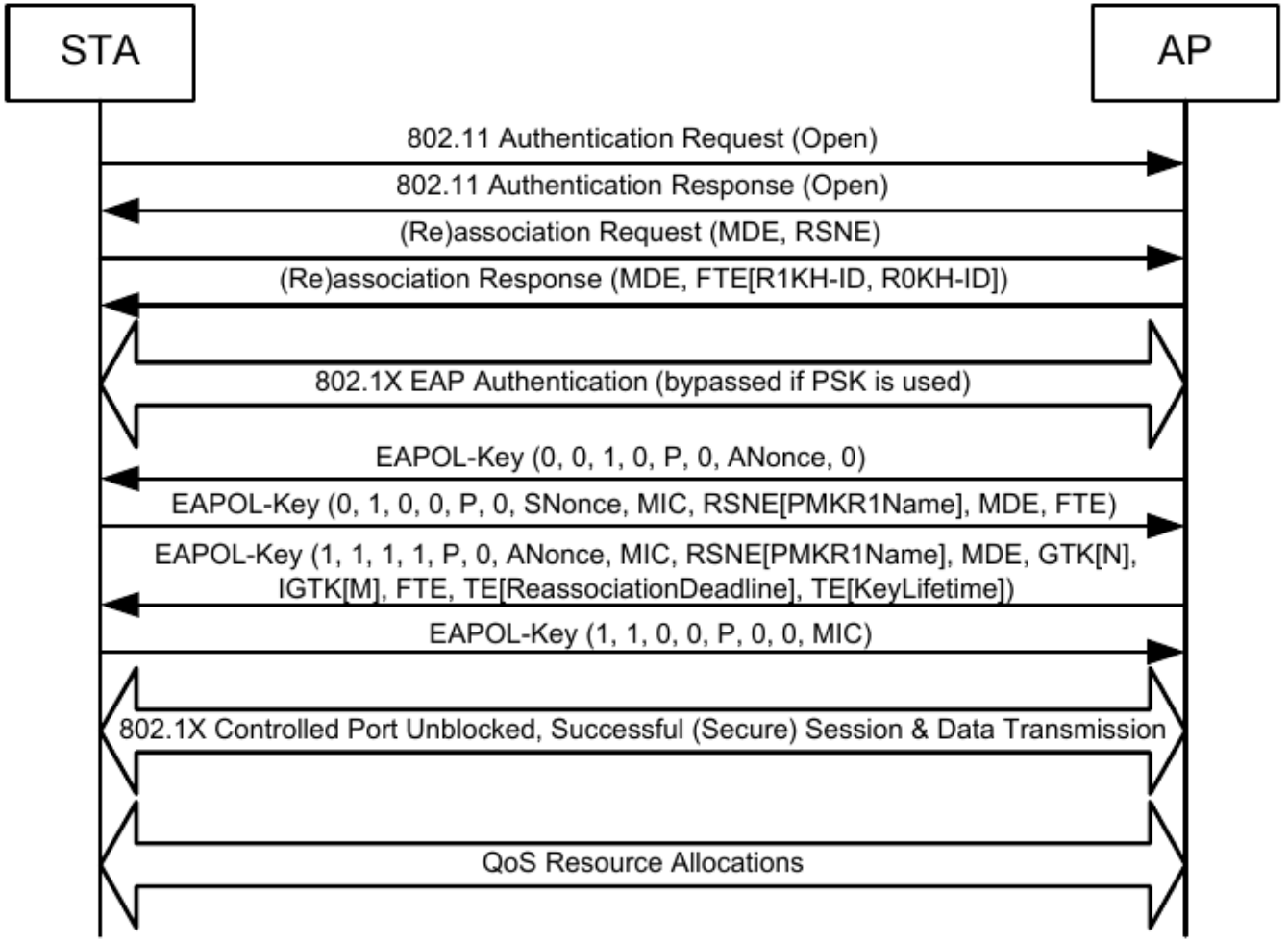


Figure 12-2—FT initial mobility domain association in an RSN

FT re-association (1)

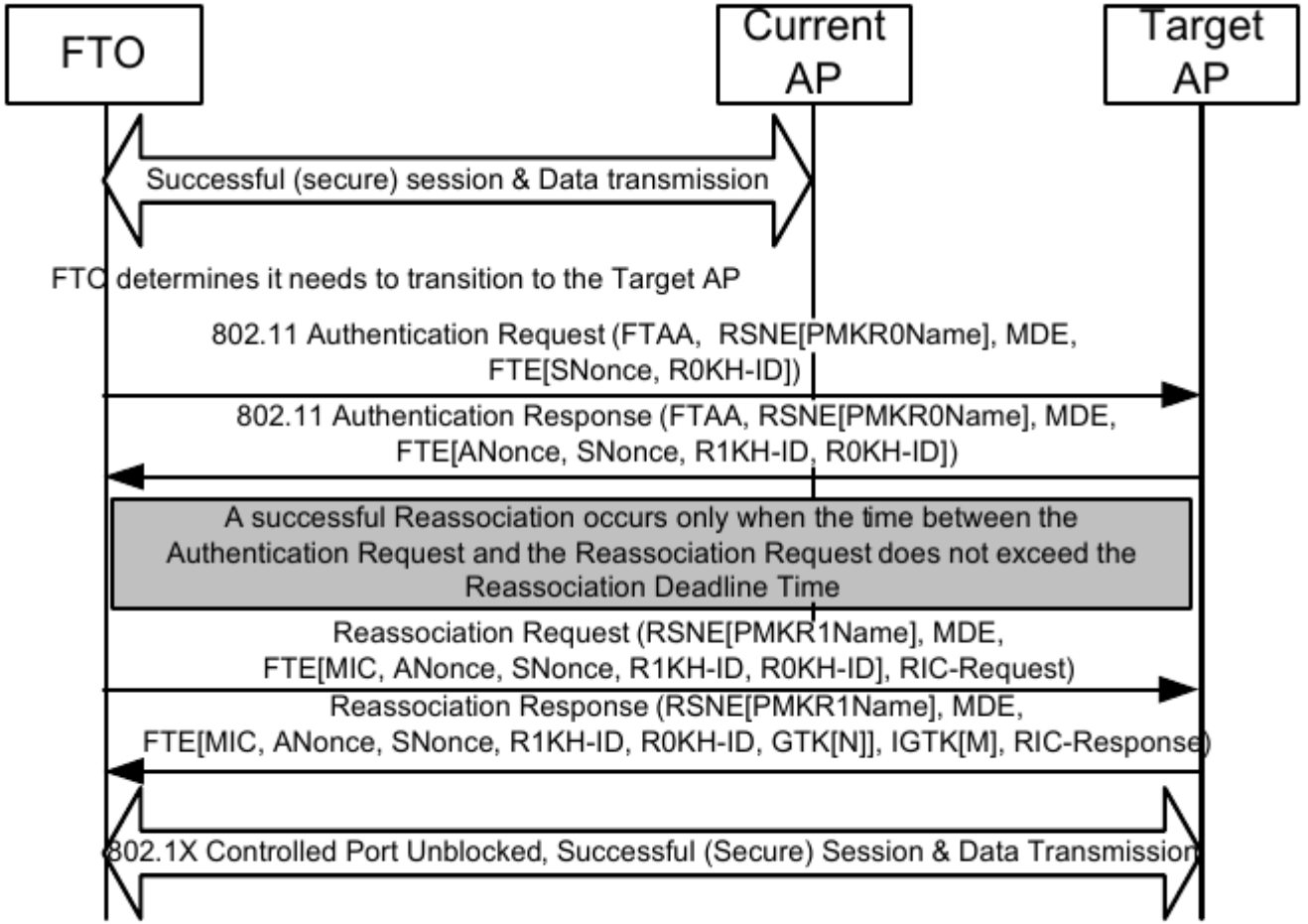


Figure 12-4—Over-the-air FT Protocol in an RSN

FT re-association (2)

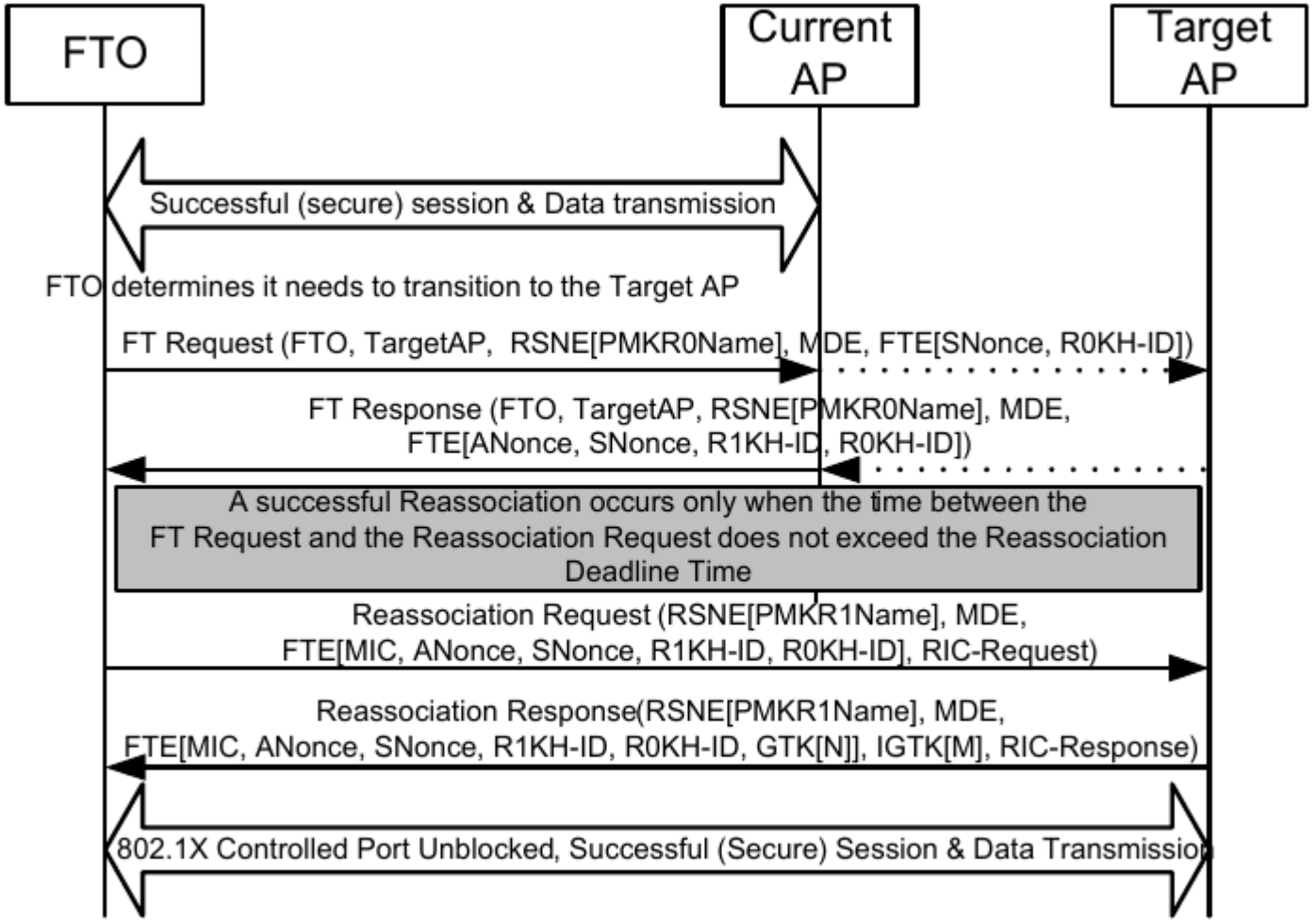


Figure 12-5—Over-the-DS FT Protocol in an RSN

Vulnérabilité SharedKey (WEP)

- Ce système n'est pas sécurisé si une station se place en écoute pendant l'authentification, car le chiffrement se fait avec un OU EXCLUSIF (cf. WEP).
- Un attaquant en écoute passive peut récupérer le challenge (Trame 2) et la réponse (Trame 3), et ainsi obtenir le keystram (la clé de chiffrement) pour l'IV donné et la longueur du paquet :

  `T3 = T2′ XOR KEY_STREAM`

  `KEY_STREAM = T2′ XOR T3`
- On peut ensuite faire une attaque « Brute-force » ou dictionnaire pour trouver la clé WEP partagée car le début des données est connu (01 00 03 00 00 00) !

Vulnérabilités WEP (1)

- Voir MISC magazine n° 54 janvier 2011
- « Cryptanalyse du protocole WEP » - Martin VUAGNOUX
- Attaque **FMS** en **2001** (FLUHRER, MANTIN et SHAMIR) utilisant les « clés faibles » de RC4 (voir en 1995 : Andrew ROOS, « A Class of Weak Keys in RC4 Stream Cipher » et David Wagner, « Weak Keys in RC4 ») – 4 millions de trames Wifi suffisent à découvrir une clé WEP secrète de 13 octets.
- 17 attaques de « **KOREK** » en **2004** : la complexité de recouvrement diminue : 800 mille trames suffisent...
  - Médiatisée par « aircrack » de Christophe DEVINE
    - Génération/rejeu de traffic ARP= quelques minutes pour cracker une clé WEP !

Vulnérabilités WEP (2)

- Attaques de **KLEIN** en **2006** : utilisable sur tous les paquets chiffrés (pas en fonction de l'IV et du keystream). En théorie, seulement 25 mille trames suffisent, mais compter plutôt 100 mille.
- Attaques **PTW** en **2007** (PYSHKIN, TEWS et WEINNMANN) : détermination de différentes somme des valeurs de la clé au lieu de retrouver la clé octet par octet. Il faut 40 mille trames.
- Attaques de **VAUDENAY** et **VUAGNOUX** en **2007** : Attaques sur les mêmes principes découvertes indépendamment mais avec quelques variantes. Il faut dans ce cas, 32 mille trames.
- En **2009**, **BECK** et **TEWS** (Chercheurs Allemands) améliorent les coefficients de pondération, ce qui permet d'arriver à 24,2 mille trames.

Vulnérabilités WEP (3)

- Attaques **SVV** en **2010** (SEPHERDAD, VAUDENAY et VUAGNOUX) : Analyse exhaustive des biais de RC4 (Transformée de FOURIER) => 48 biais additionnels sont trouvés dans le PRGA de RC4. Au final 10 mille trames suffisent pour une clé WEP de 13 octets.

Vulnérabilités TKIP (1)

- Novembre 2008, **BECK** et **TEWS** : détermination de la clé MIC (algorithme Michael réversible) et transmission de quelques paquets en utilisant une variante de la technique WEP « chop-chop » (détermination octet par octet des données en fonction des réponses de l'AP). Nécessite un délai de renouvellement de clé long.
- Aout 2009, Masakatu **MORII** et Toshihiro **OHIGASHI** : Falsification en moins d'une minute de paquets ARP ou DNS en améliorant l'attaque précédente et en utilisant un « Man-in-the Middle ».
- Juillet 2010, **Hole 196** (en référence à la page 196 du standard WPA2), Sohail AHMAD, démontre que connaissant la clé partagée, un attaquant peut injecter du trafic à destination de plusieurs machines connectées sans être détectable. La méthode utilise la clé GTK pour le trafic multicast.

Vulnérabilités TKIP (2)

- En 2013, Mathy **VANHOEF** et Frank **PIESSENS**, améliorent encore l'attaque sur MIC (par l'utilisation de la fragmentation i.e. max. 112 octets) et augmentent le nombre de paquets qu'un attaquant peut forger. Ils montrent aussi comment déchiffrer un paquet arbitraire.
- En 2015, l'attaque **NOMORE** (Numerous Occurrence MOnitoring & Recovery Exploit) permet en 1 heure décrypter et d'injecter des paquets.

Vulnérabilités WPA/WPA2

- Le mode **PSK** est sensible aux attaques par dictionnaire ou par « force brute » dans la cas de clés partagées « simples ».
- Octobre 2017, **KRACK** (Key Reinstallation Attacks) - Mathy VANHOEF - permet une attaque de type Man in the Middle en interférant sur le système 4-Way Handshake...
  - https://www.krackattacks.com/

Références

- http://www.wi-fi.org
- http://standards.ieee.org/
- https://www.bluetooth.org/
- http://www.palowireless.com/