Seguridad en Redes Wireless

Daniel Calzada del Fresno

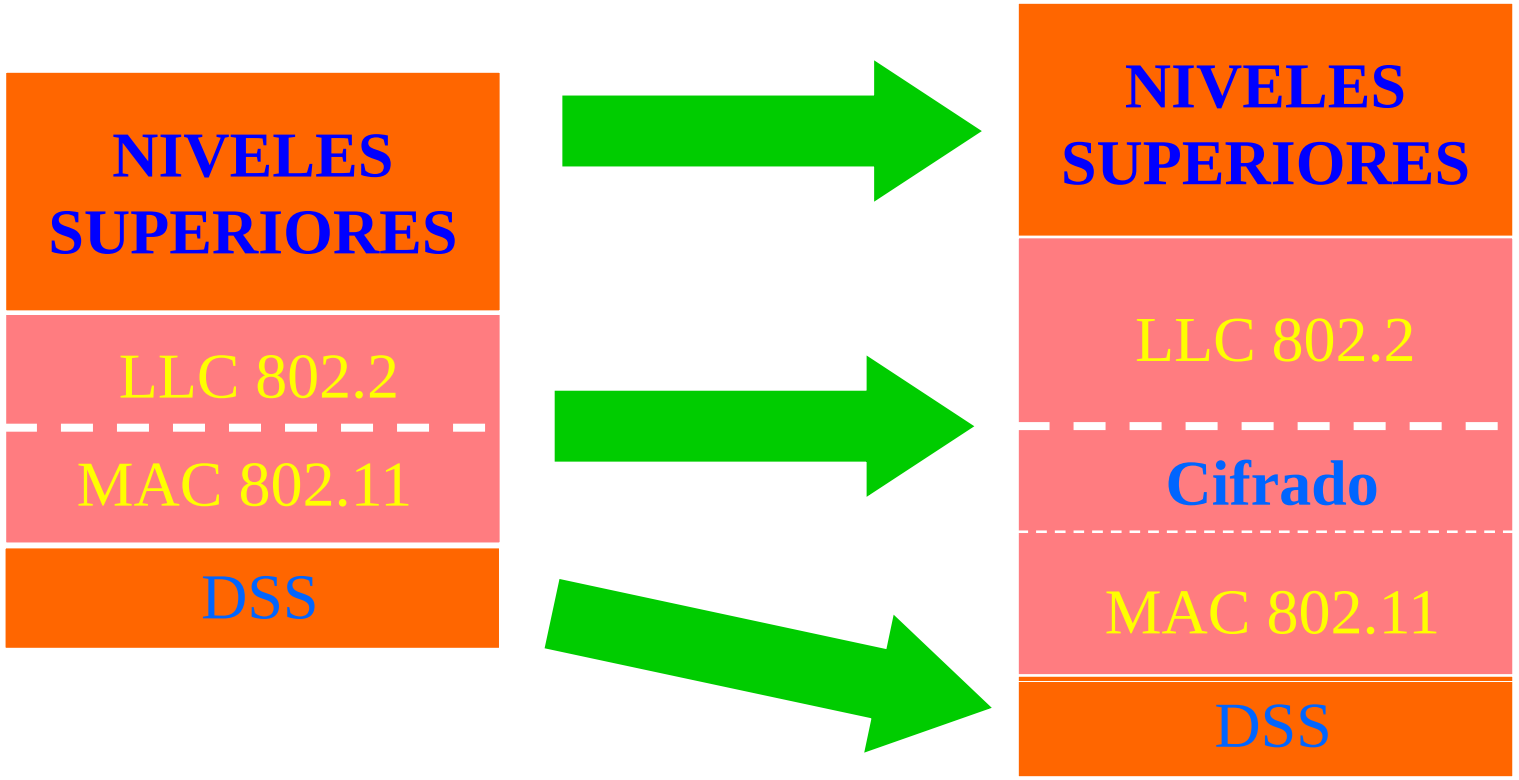
Desarrollo

- **WEP**
- **802.11i**
  - Fases operacionales de la 802.11i.
  - Fase 1: Acuerdo sobre política de seguridad.
  - Fase 2: Autentificación.
  - Fase 3: 4-way-handsake. Group key handsake.
  - Fase 4: Cifrado TKIP. Cifrado CCMP.
  - Definiciones :WPA, WPA-PSK, WPA2, WPA2-PSK.
  - Debilidades.

Posibles configuraciones

Red abierta: sin seguridad.
WEP (Wired Equivalent Privacity)
WPA (Wi-Fi Protected Access)
WPA-PSK (WPA con Preshared Key)
WPA2 (Wi-Fi Protected Access 2)
WPA2-PSK (WPA2 con Preshared Key)

Cifrado en WIFI



El cifrado puede ser considerado como una capa incorporada y por encima de la capa MAC. Es transparente para las capas superiores.

WEP

Wired Equivalent Privacy

Asociación. Con WEP.

WEP

WEP

Petición de Prueba

Respuesta a Prueba

Petición de autentificación de sistema abierto

Aceptación de autentificación de sistema abierto

Pre-asociación

Pre-asociación

Petición de Asociación

Nonce

(aleatorio para que lo cifre la estación)

Nonce cifrado con la clave WEP

Verificado

Aceptación de Asociación

Asociación

MAC-STA MAC-AP

ID de sesión

Asociación

MAC-STA MAC-AP

ID de sesión

Datos

Cifrado y Descifrado WEP

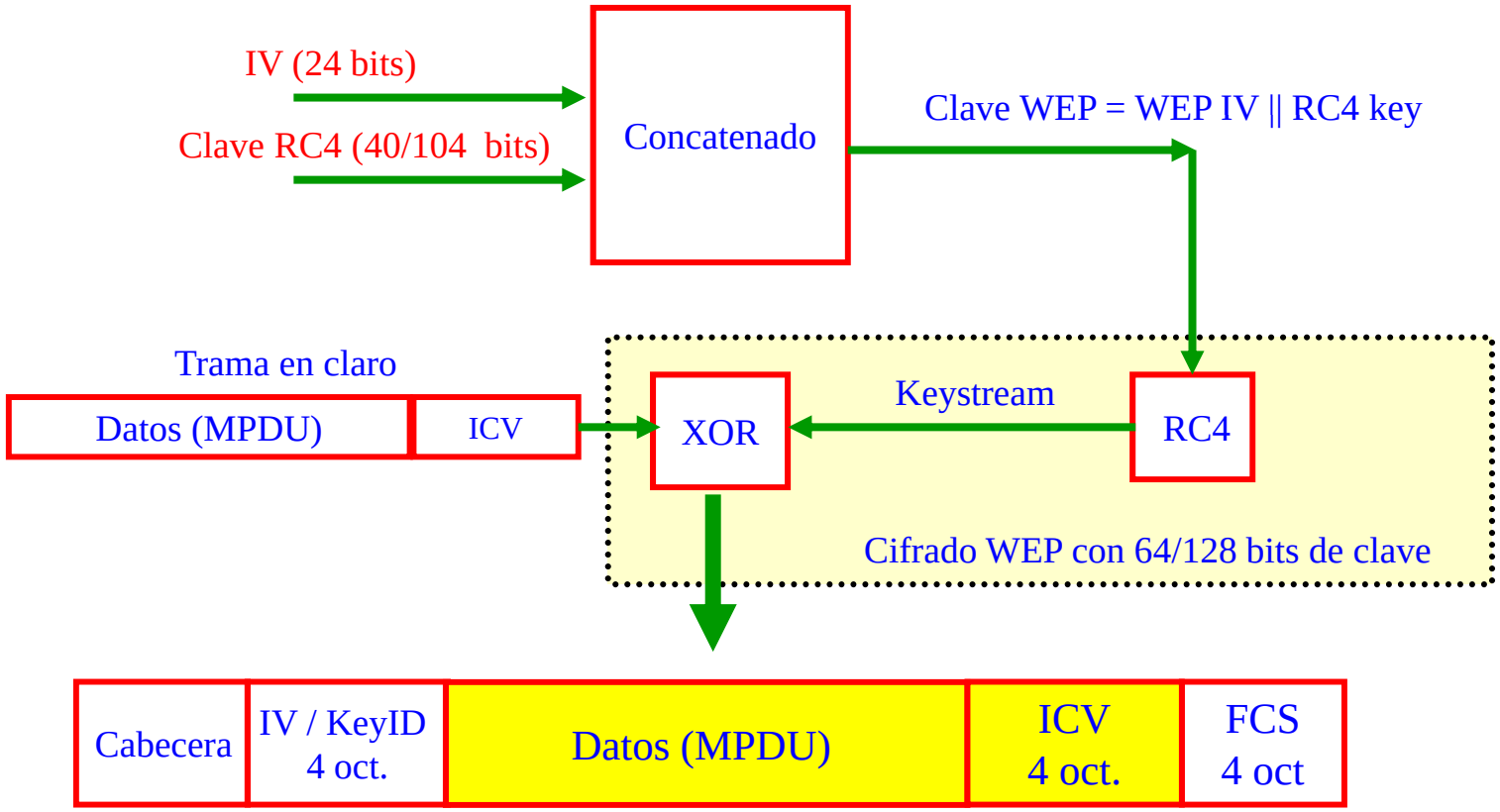
CIFRADO, T: ORX DE M (mensaje) y K (Keystream)

M	0	1	1	1	0	0	0	1	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0
K	1	0	1	0	1	0	0	0	1	1	1	0	1	0	1	0	1	0	0	1	0	0	1	1
T	1	1	0	1	1	0	0	1	0	0	1	0	0	0	0	1	1	0	1	0	0	1	0	1

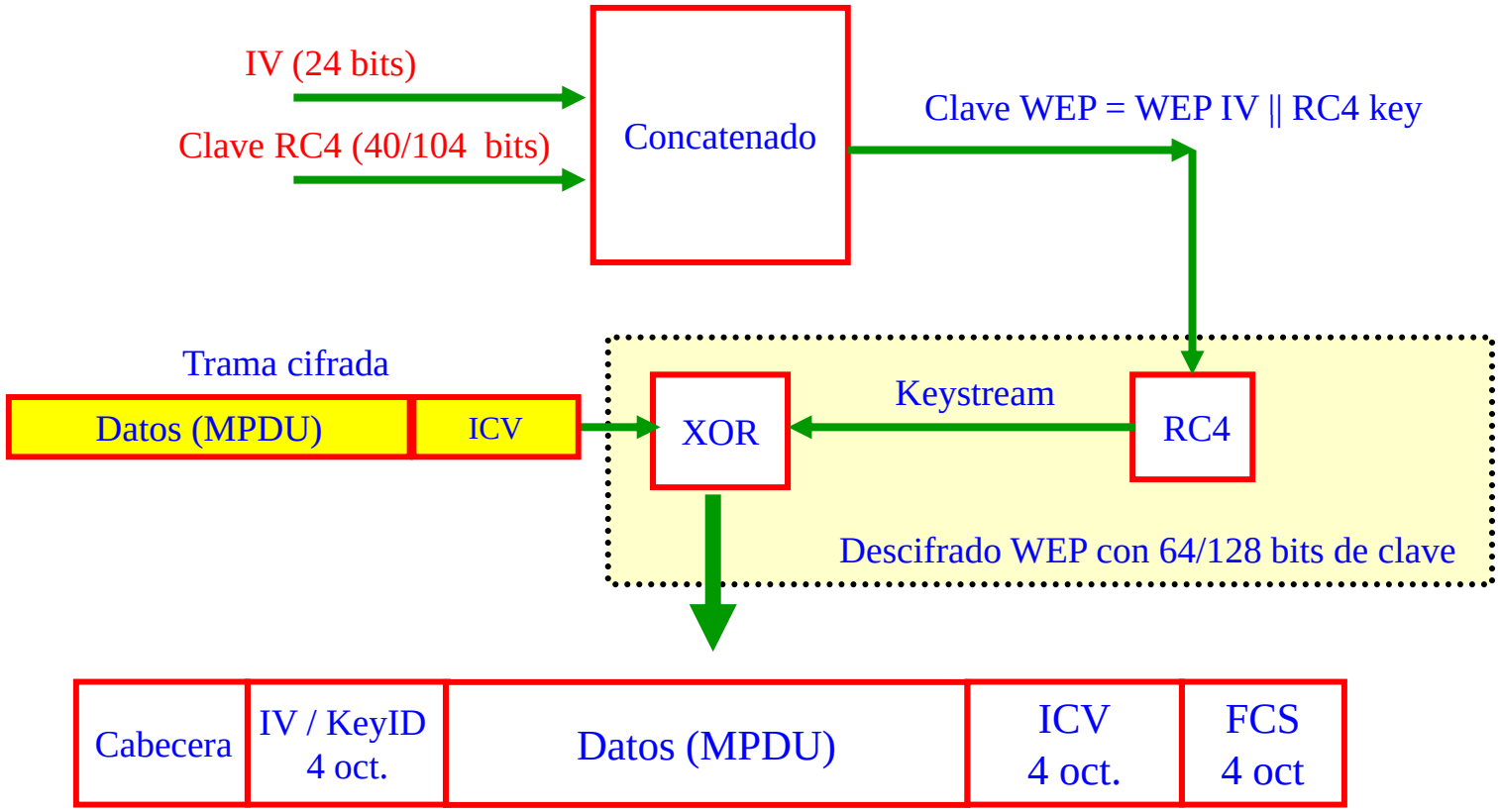
DESCIFRADO, M: ORX DE T (mensaje cifrado) y K (Keystream)

T	1	1	0	1	1	0	0	1	0	0	1	0	0	0	0	1	1	0	1	0	0	1	0	1
K	1	0	1	0	1	0	0	0	1	1	1	0	1	0	1	0	1	0	0	1	0	0	1	1
M	0	1	1	1	0	0	0	1	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0

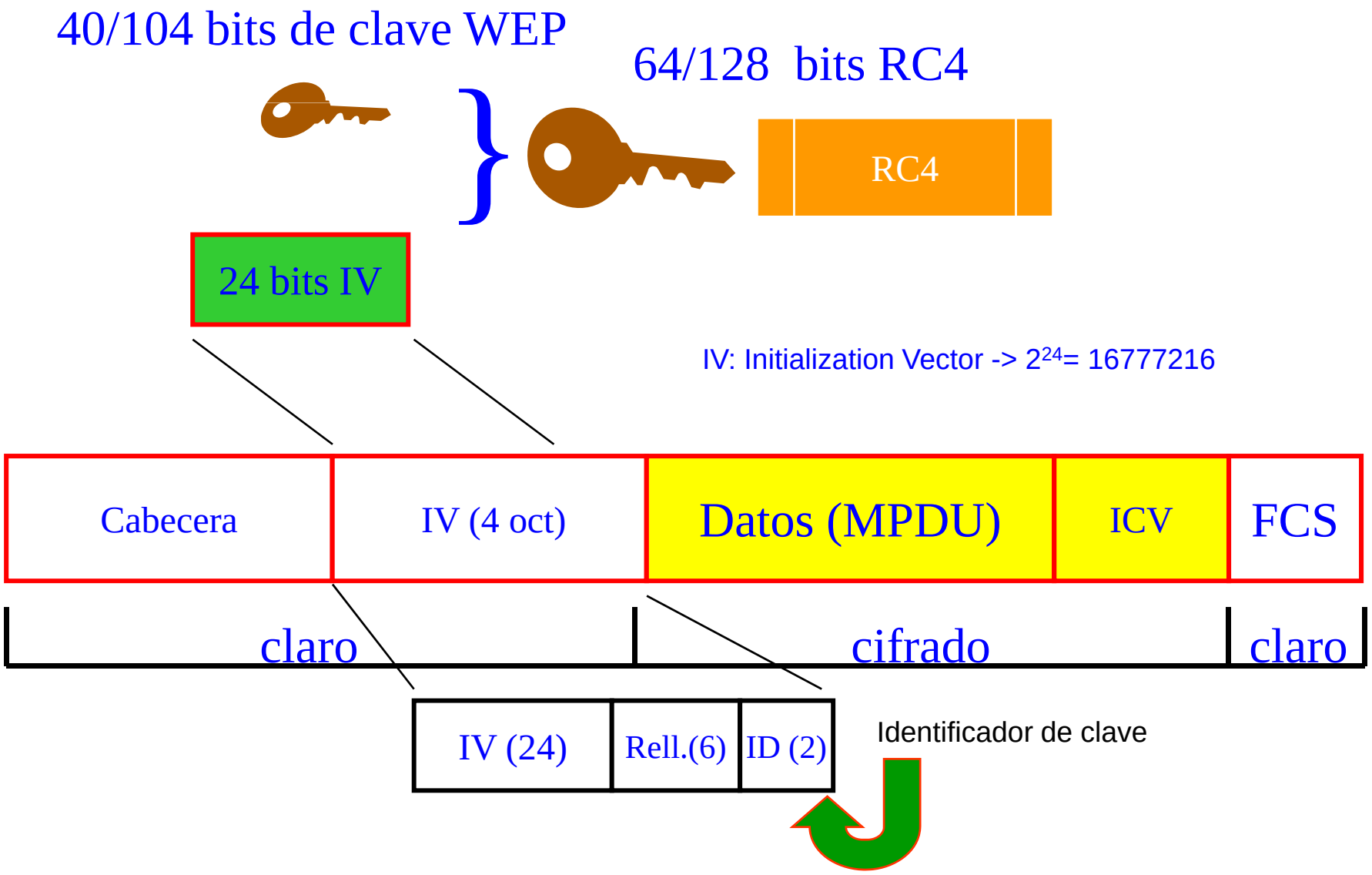
Cifrado WEP


IV (24 bits)
Clave RC4 (40/104 bits)
Concatenado
Clave WEP = WEP IV || RC4 key
Trama en claro
Datos (MPDU)
ICV
XOR
Keystream
RC4
Cifrado WEP con 64/128 bits de clave
Cabecera
IV / KeyID
4 oct.
Datos (MPDU)
ICV
4 oct.
FCS
4 oct

Descifrado WEP



WEP y los Initialization Vectors



Debilidades del WEP

- **Las debilidades del WEP son múltiples.**
- **Su rotura se produce en unos pocos minutos.**
- **NO SE DEBE CONFIGURAR NUNCA.**

802.11i

802.11i (1)

- Junio de 2004.
- Proporciona autentificación y confidencialidad.
- Separa autentificación de usuario del cifrado de mensajes.
- Proporciona una arquitectura robusta y escalable.
- Útil en redes domésticas y empresariales.
- RSN: Robust Security Network.
- TSN: Transitional Security Network. (Etapa transitoria).

802.11i (2)

- Utiliza autenticación 802.1x, distribución de claves y nuevos mecanismos de integridad y privacidad.
- TKIP (Temporal Key Integrity Protocol). WEP con una clave distinta por cada trama. Dispositivos antiguos que soportaban WEP, con actualización de firmware.
- CCMP (Counter-mode con Cipher block chaining Messsage authentication code Protocol). AES(128,128) con una clave por trama.
- Soporta redes AdHoc.

Redes Modo enterprise y SOHO

- Con autentificación.

  Redes empresariales (Enterprise)

  No se pueden poner todos los identificadores de usuario y claves en cada uno de los numerosos puntos de acceso.

  Es necesario un servidor de autentificación (RADIUS).

  Se ponen dos o más servidores, por redundancia.

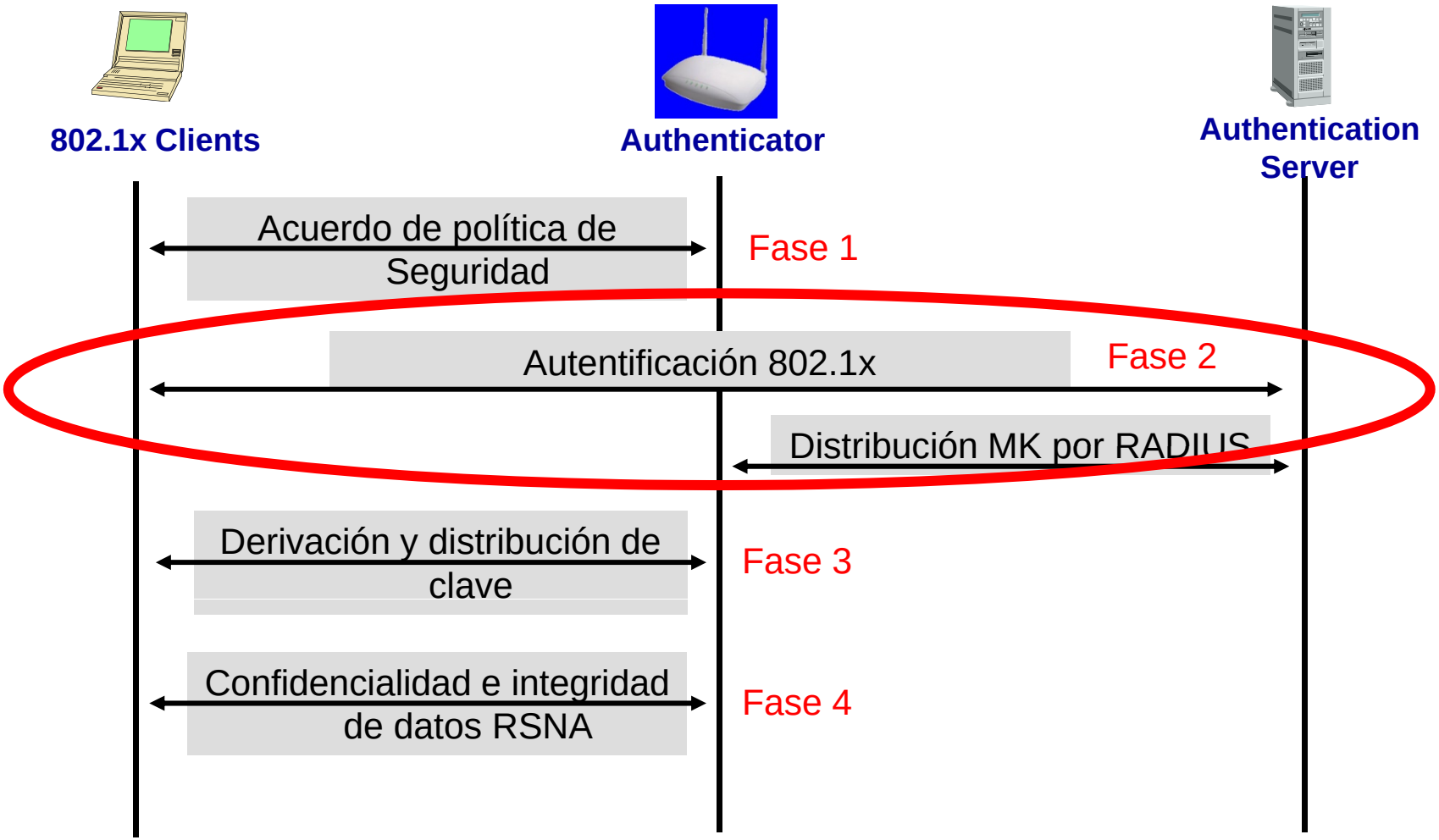
- Sin autentificación.

  SOHO (Small Office Home Office).

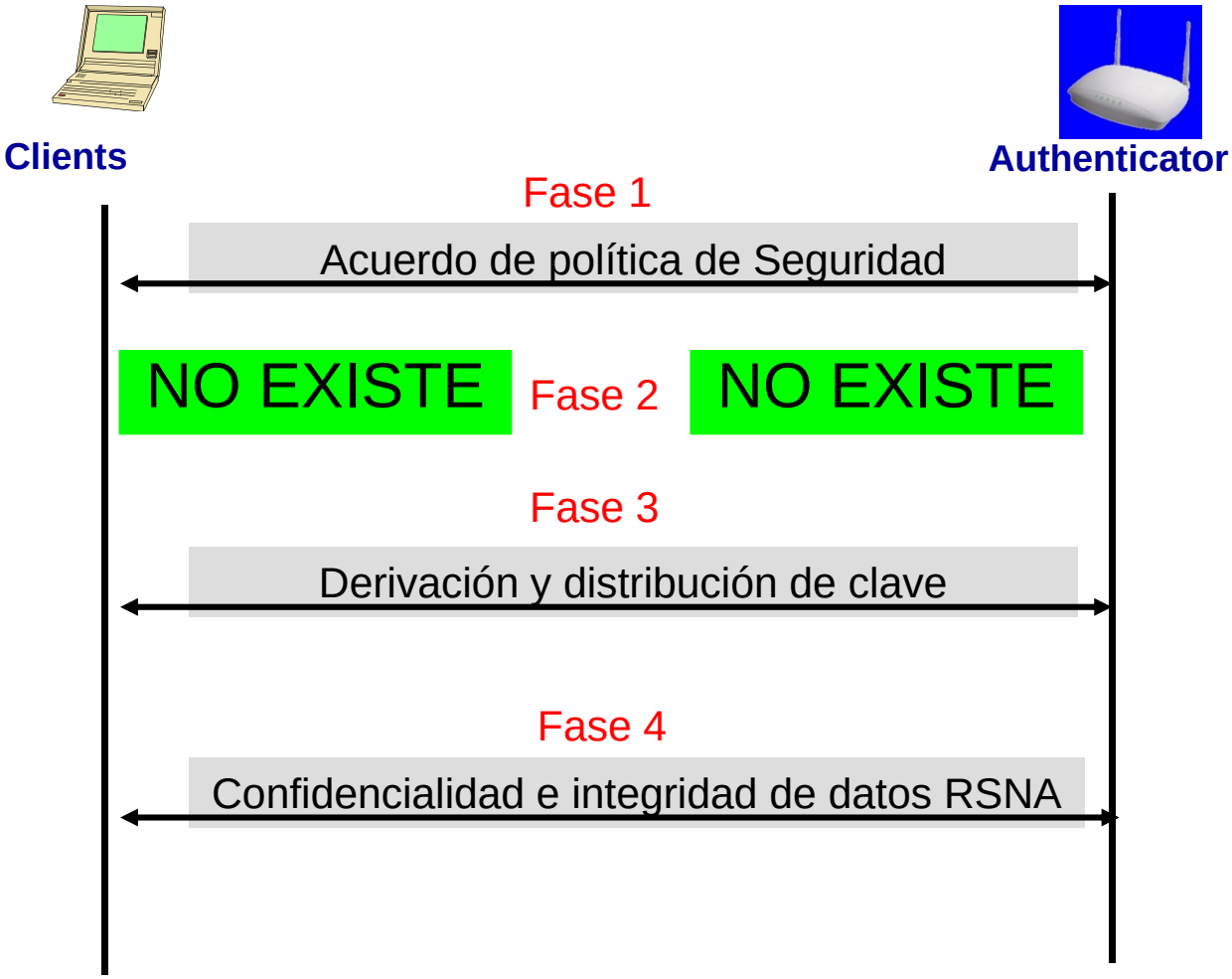
  Pequeñas oficinas e instalaciones domésticas.

  No es preciso servidor de autentificación. No se utiliza la autentificación (Pre Shared Key == PSK). Los pocos usuarios de la red, utilizan la misma PSK.

Fases de 802.11i (Enterprise)



Fases de 802.11i (SOHO)



SOHO

(Small Office Home Office)

Redes sin autentificación

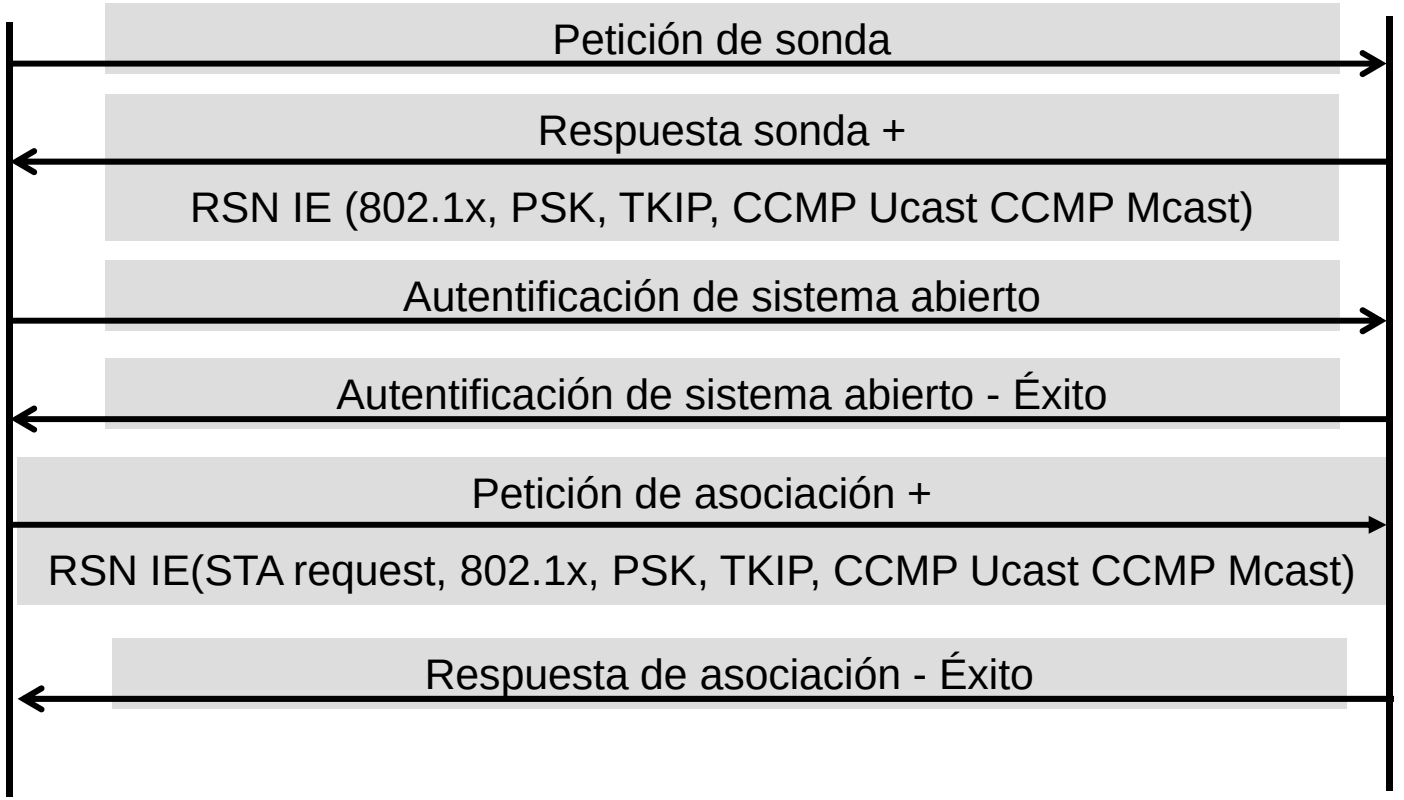
Fases: Terminología

- **Fase 1:** Acuerdo sobre la política de seguridad. Tanto el suplicante (Estación) como el autenticador (Punto de Acceso) se preasocian estableciendo una negociación de la política de seguridad que posteriormente les va a llevar a una asociación completa.
- **Fase 2:** En redes tipo SOHO, ésta fase no existe.
- **Fase 3:** 4-Way Handsake. Tanto el suplicante como el autentificador calculan y derivan unas claves para la confidencialidad. Estas claves sólo son válidas para esta sesión. Si es rota la asociación, por cualquier causa, al volver a establecerla se realiza un nuevo cálculo de claves.
- **Fase 4:** Se establece la RSNA (RSN Association). Se produce el intercambio cifrado de información.

802.11i: Fase 1 (Acuerdo sobre política de Seguridad)

802.1x Clients

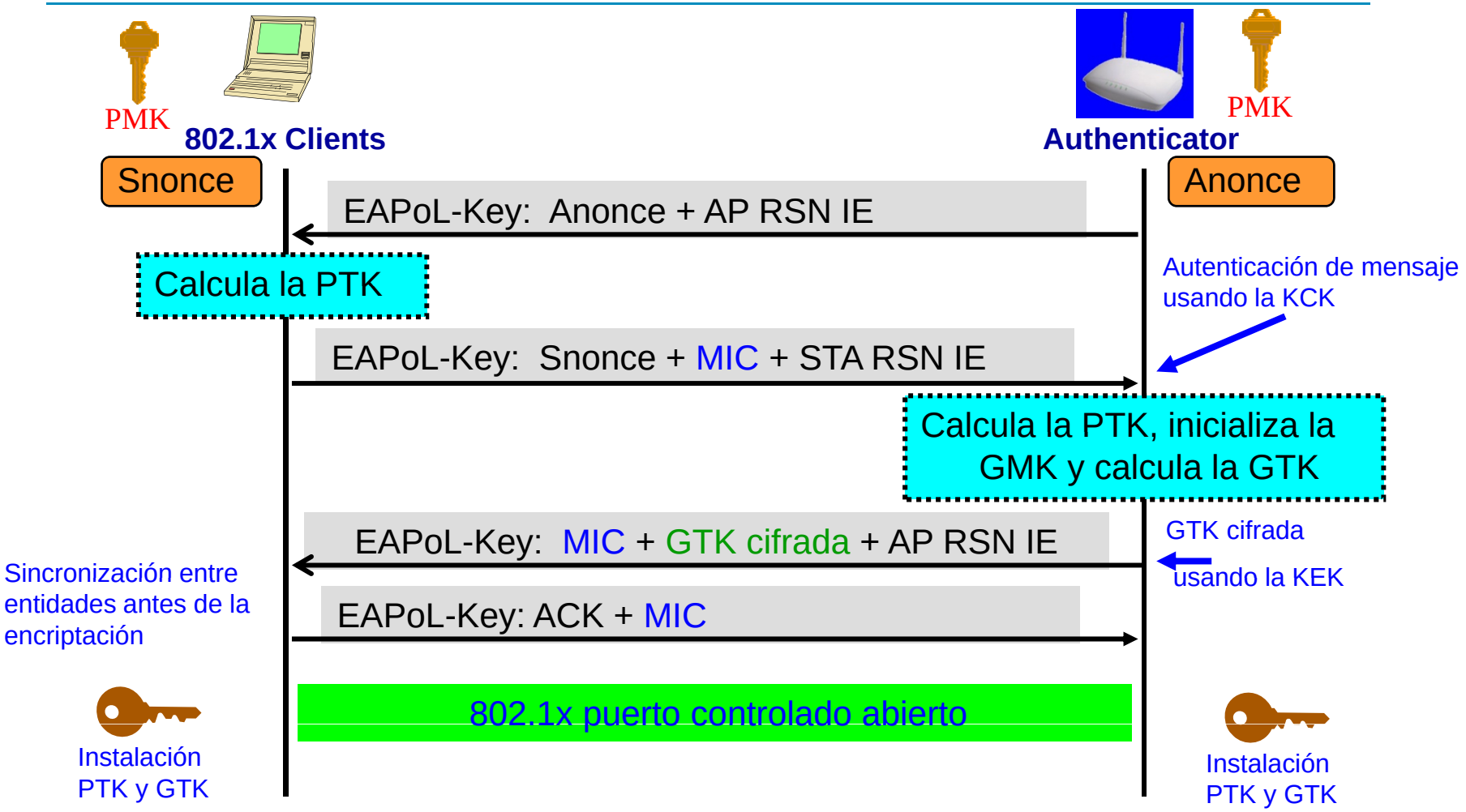
Authenticator



Fase 1: Terminología

- RSN IE (Robust Security Network Information Element).
  - El PA declara en esta trama los parámetros de seguridad para los que está configurado. Por ejemplo soporta TKIP o CCMP. Utiliza 802.1x o PSK.
- La autentificación de sistema abierto es una asociación en las tablas de la estación de su dirección MAC con la del PA. En el PA es idéntico. Es una preasociación.
- La petición de asociación de la estación incluye en su IE los parámetros con los que se asocia, aceptando los que le indicó el PA.
- La respuesta del PA acepta la asociación de la estación.

802.11i: Fase 3 (4-Way Handshake)



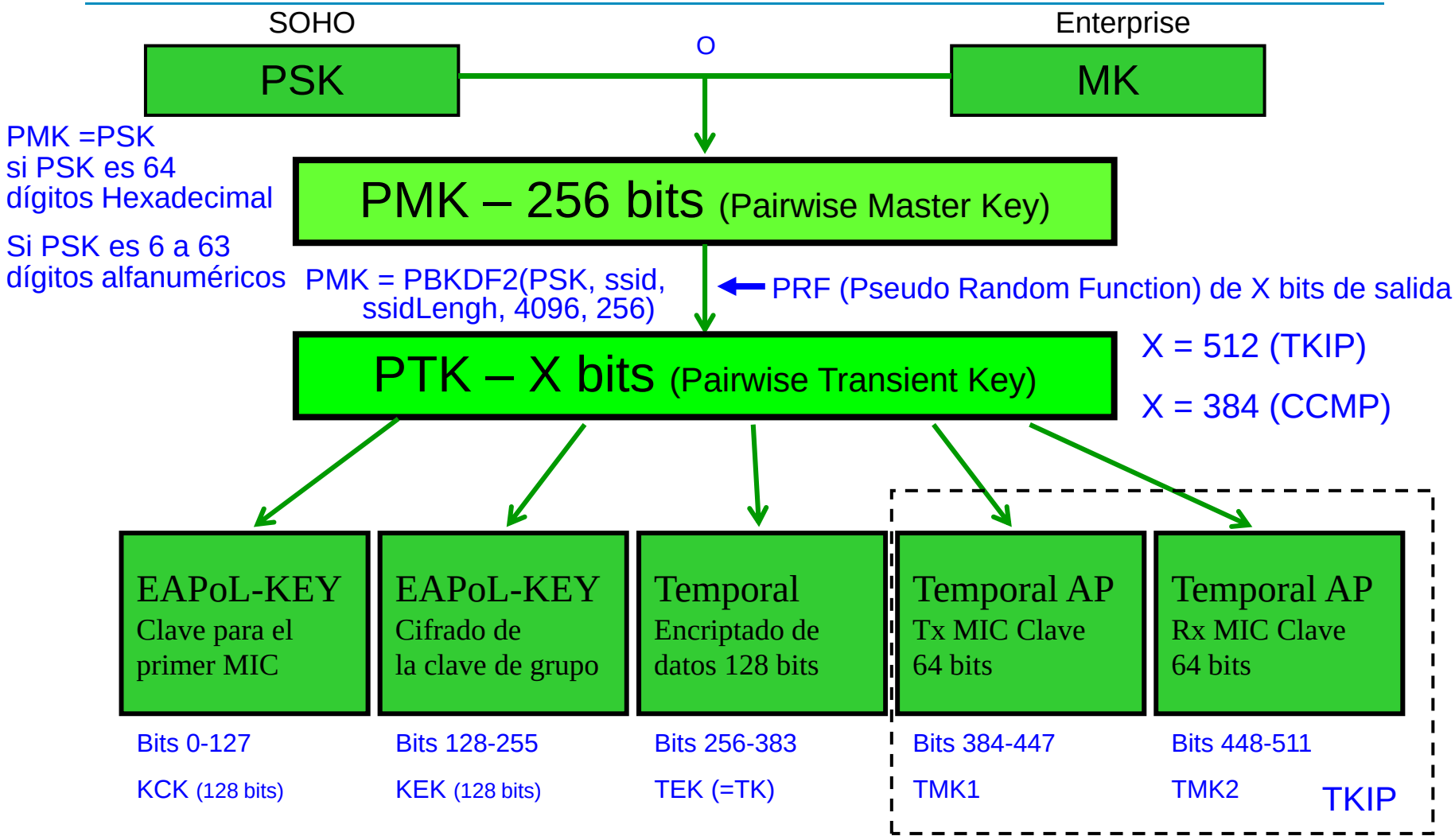
PTK = PRF-X (PMK, <<expansión de clave por pares>>, Min(AP_Mac, STA_Mac) || Max(AP_Mac, STA_Mac) || Min (ANonce, SNonce) || Max (Anonce, Snonce))

PRF-X es una Pseudo Random Function que genera X bits de salida

Fase 3: Descripción

- El suplicante y el autenticador tienen ambos la PMK (256 bits) (derivada de la MK de la fase anterior o de la PSK). En la primera trama el PA envía un Anonce (aleatorio), más una repetición del RSN IE (información del acuerdo de política de seguridad).
- La estación calcula la PTK (Pairwise Transient Key), por medio de una función pseudoaleatoria.
  - Esta PTK tiene una longitud de 512 bits en el caso de que hayan acordado usar TKIP ó 348 bits en el caso de que el acuerdo sea CCMP.
  - Si es TKIP los 512 bits se cortan en 5 trozos o claves.
  - Si es CCMP los 348 bits se cortan en tres trozos o claves.
- La estación envía una trama con un Snonce (aleatorio) más su RSN IE y le añade un MIC (Message Integrity Code, código de integridad de mensaje). El MIC es calculado usando los primeros 128 bits de la PTK.
- El PA, con el Snonce recibido deriva también la PTK, verifica la validez del MIC de la trama anterior. Calcula y cifra la clave de grupo con los bits 128 a 255 de la PTK y se la envía a la estación.
- La estación verifica el MIC, extrae la clave de grupo y le asiente al PA la trama anterior. A partir de aquí el autenticador abre el puerto 802.1x.

802.11i: Fase 3 (Jerarquía de claves por parejas)



PTK = PRF-X (PMK, <<expansión de clave por pares>>, Min(AP_Mac, STA_Mac) || Max(AP_Mac, STA_Mac) || Min (ANonce, SNonce) || Max (Anonce, Snonce))

Fase 3: Jerarquía de claves: descripción 1

- El suplicante y el autenticador tienen ambos la PMK (256 bits) (derivada de la MK de la fase anterior o de la PSK).
  - En el caso de utilizar PSK, si se introducen exactamente 64 dígitos en hexadecimal la PSK da lugar a la PMK. Si se introducen entre 6 y 63 caracteres alfanuméricos, por medio de un hash recursivo se obtiene la PMK de 256 bits.
  - Si se utiliza servidor de autentificación éste produce directamente la MK de 256 bits, que pasa a ser la PMK.
- Posteriormente, una PRF-X expande la PMK a la PTK.
- La PTK se trocea y cada trozo es una clave con una funcionalidad distinta.

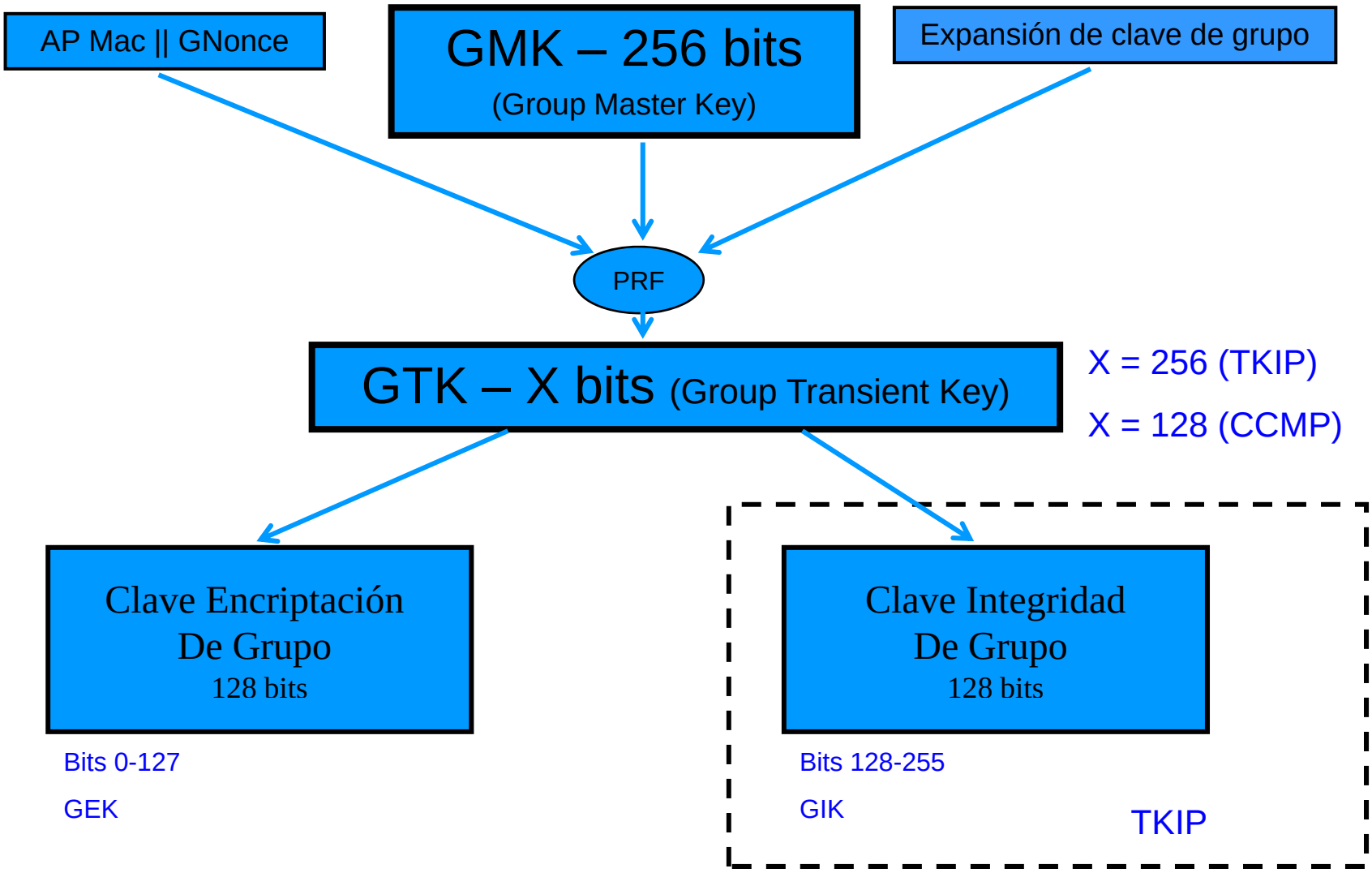
Fase 3: Jerarquía de claves: descripción 2

- KCK (128 bits). Para generar el primer MIC del 4-way -Handsake.
- KEK (128 bits). Cifra la clave de grupo para distribuirla a las estaciones.
- TEK (128 bits). Cifra los datos.
- TMK1 (64 bits). Genera los MIC de las tramas de datos, cuando los transmite.
- TMK2 (64 bits). Calcula la validez de los MIC de las tramas de datos en los MIC recibidos.
- En el caso de utilizar CCMP, estas dos últimas no se generan porque el cifrador AES genera su propio MIC.

Fase 3: Es preciso una clave de grupo

- Cada estación mantiene, en su asociación con el AP, un conjunto de claves para cada sesión.
- Obviamente las claves son distintas para cada asociación. Cada estación tiene claves de cifrado (confidencialidad) distintas.
- En el caso de tráfico de difusión:
  - La estaciones no hacen difusiones por sí solas, nunca.
  - Envían la trama al AP y éste difunde.
- En las difusiones desde el AP, es preciso usar una clave de grupo, distinta de la clave de sesión de las estaciones. La clave para el MIC, en las tramas de difusión, en TKIP ha de ser también “clave de grupo”.
- El AP genera una clave de grupo y la distribuye a las estaciones cuando se asocian. La distribuye cifrada para que no sea capturable. Cada vez que una estación se desasocia se regenera la clave de grupo, por el AP y la distribuye a las estaciones.

802.11i: Fase 3 (Jerarquía de claves de grupo)

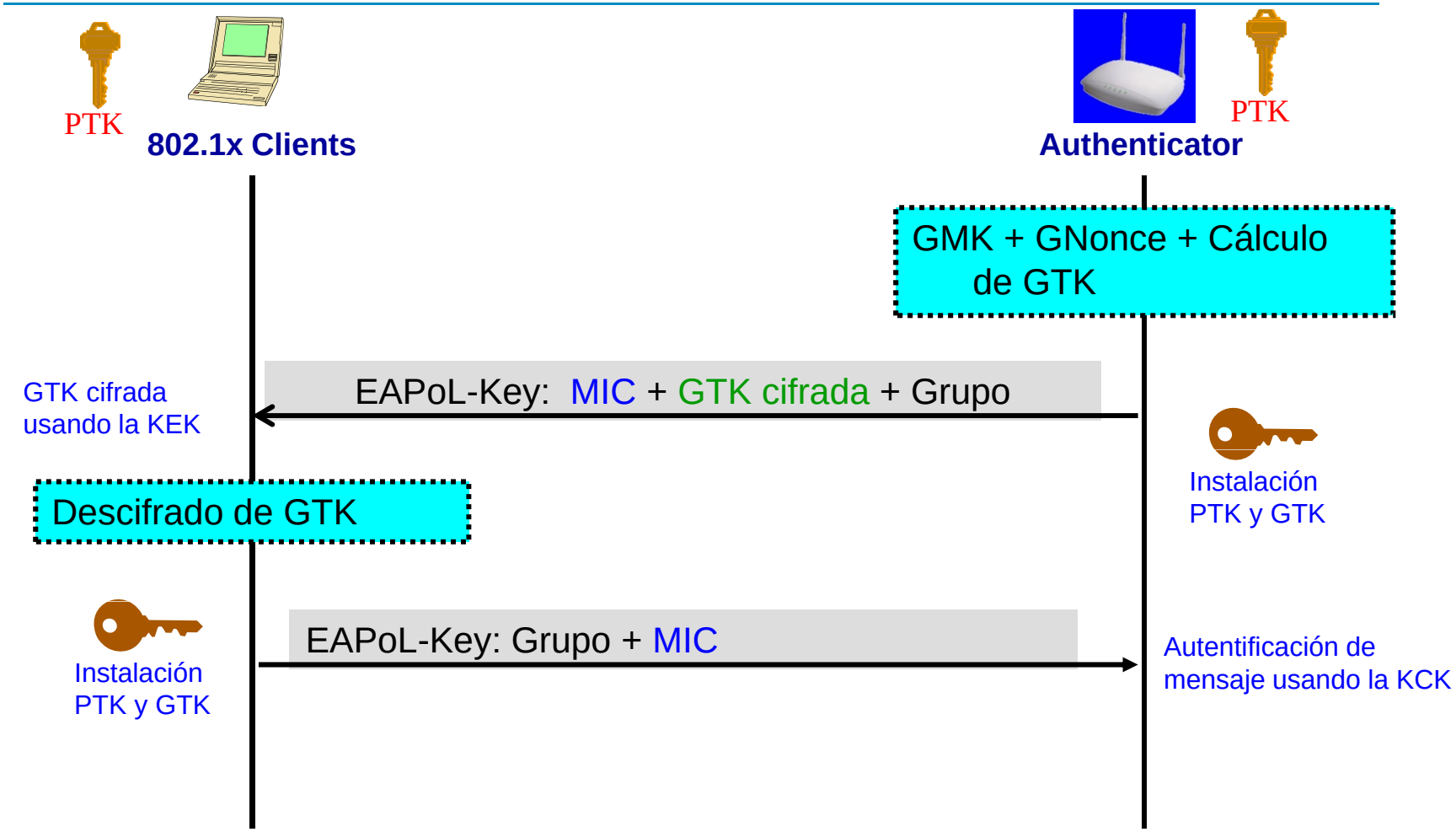


GTK = PRF-X (GMK, <<Group key expansión>>, (AP_Mac || GNonce))

Fase 3: Claves de grupo

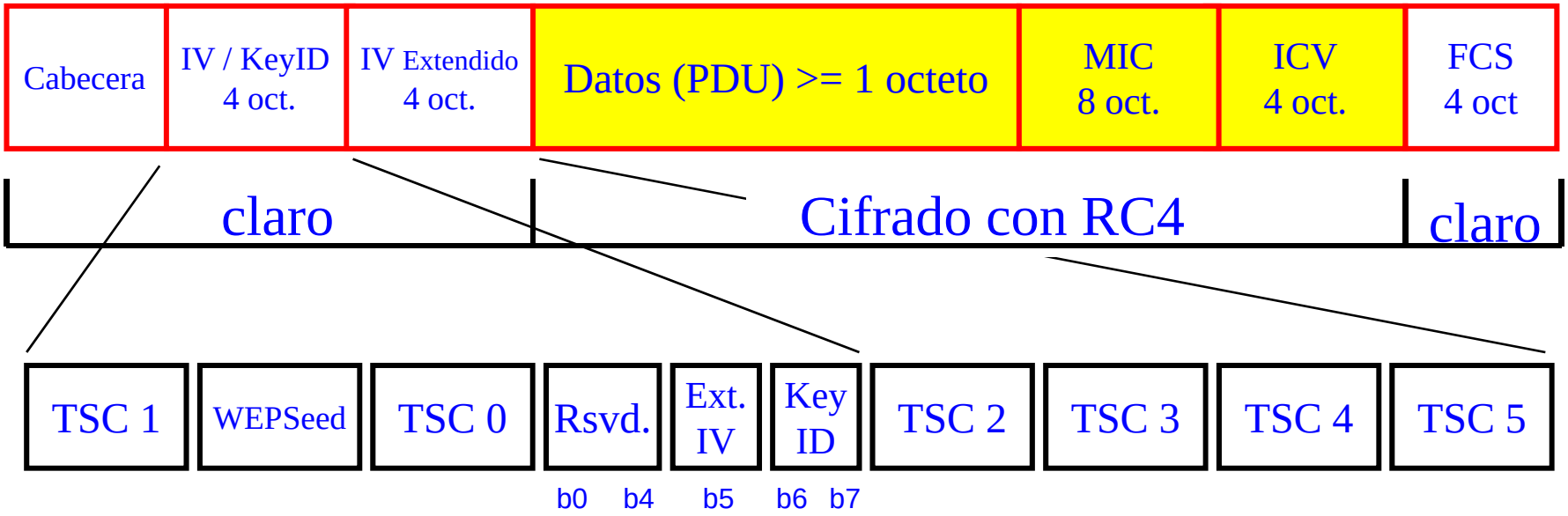
- GMK (256 bits) Group Master Key. Clave maestra de grupo. Se reinicializa periódicamente en el AP, para disminuir la posibilidad de que se comprometa la GTK.
- GTK (256 bits) Group Transient Key. Clave de grupo transitoria.
- GEK (128 bits) Group Encryption Key. Clave de cifrado de grupo. Cifra los datos de las tramas de difusión.
- GIK (128 bits) Group Integrity Key. Clave de integridad de grupo. Se utiliza para el cálculo del MIC en las tramas de difusión, con TKIP. Con CCMP no hace falta porque el MIC lo calcula el cifrador AES.

802.11i: Fase 3 (Group Key Handshake)



GTK = PRF-X (GMK, <<Group key expansión>>, (AP_Mac || GNonce))

Fase 4 (1).Trama con TKIP



TSC: TKIP Secuence Counter (48 bits): crece monotonamente

WEPSeed: No se usa para construir TSC (8 bits).

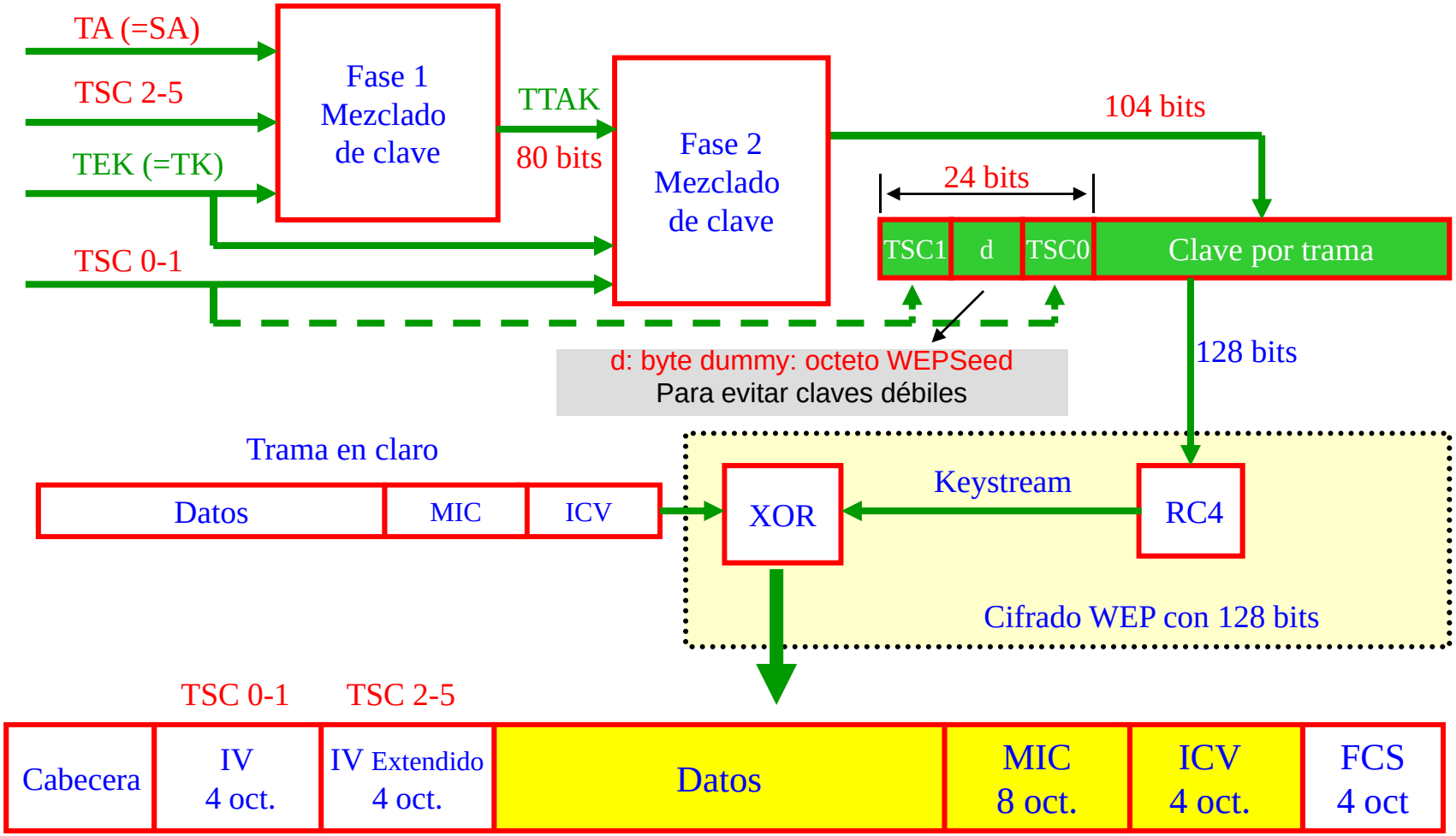
Ext. IV: Extensor de IV (1 bit). Cuando es 1 va IV extendido. Cuando es 0 no (WEP clásico)

Key ID: Identificador de la clave (2 bits) (de las cuatro posibles que se pueden poner)

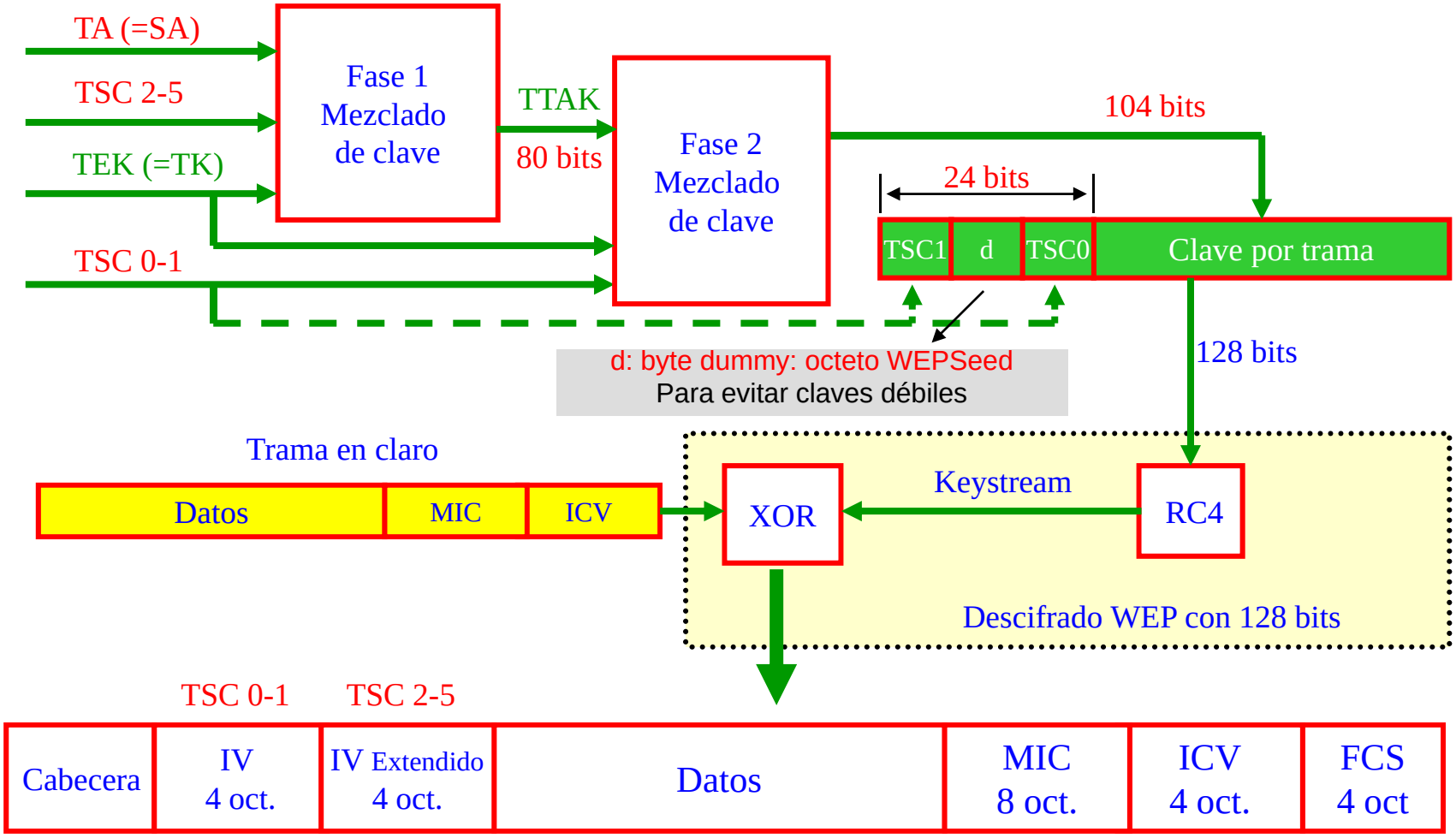
MIC: Message Integrity Code (64 bits).

ICV: Integrity Check Value (32 bits).

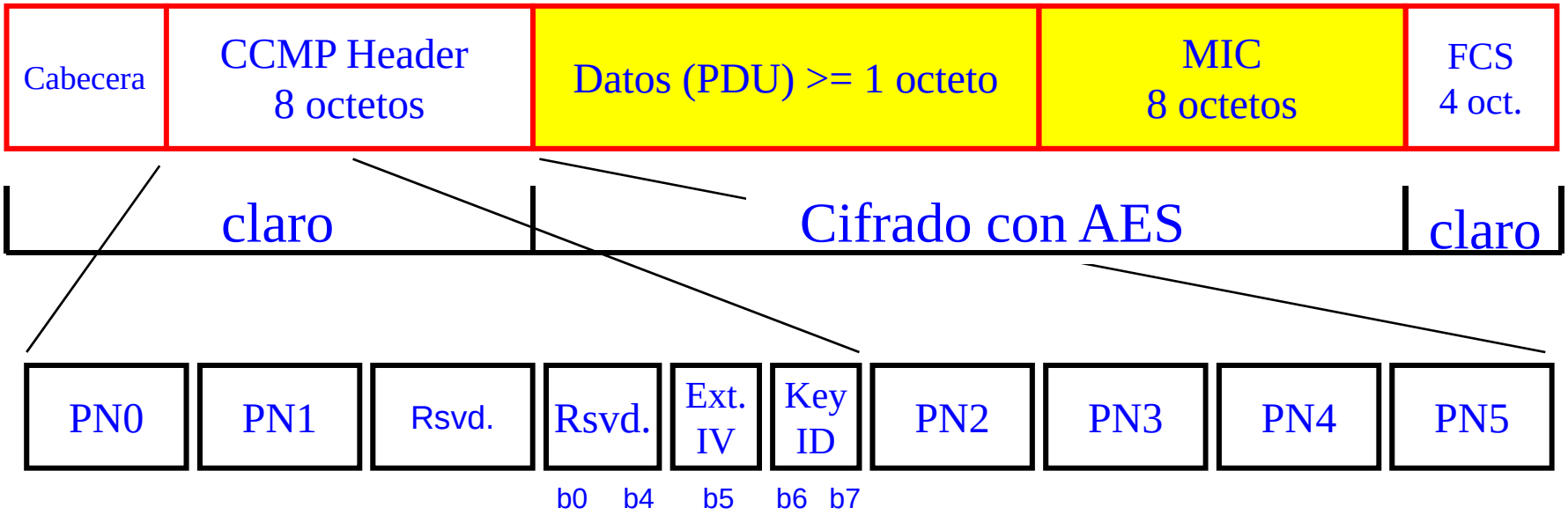
Fase 4 (2). Cifrado TKIP, una clave por trama.



Fase 4 (3). Descifrado TKIP



Fase 4 (4). Trama con CCMP



CCMP: Counter-mode con Cipher block chaining Messsage authentication code Protocol

Cifrado con AES: 128 bits de clave y 128 bits de tamaño de bloque.

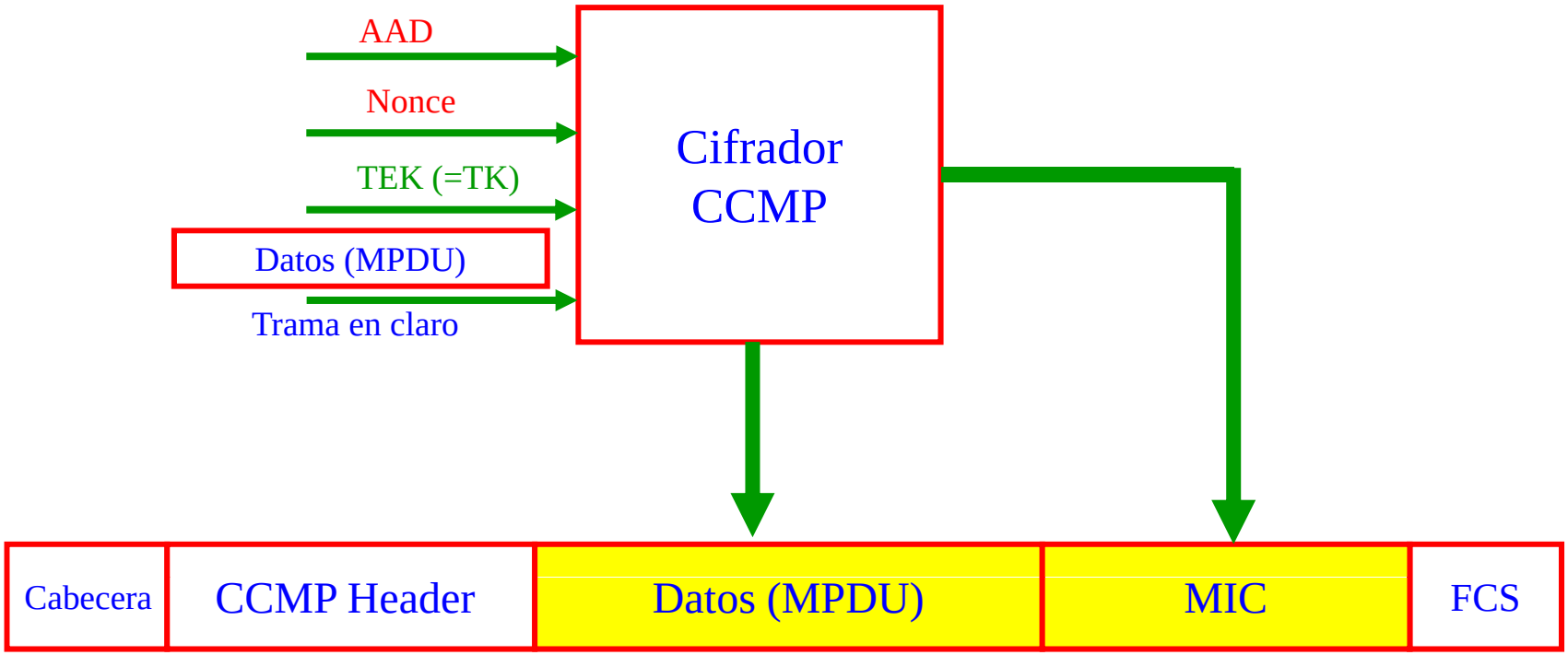
PN: Packet Number (numerador de tramas). Se incrementa en uno para cada trama.

Ext. IV: Extensor de IV (1 bit siempre puesto a 1).

Key ID: Identificador de la clave (2 bits) (de las cuatro posibles que se pueden poner)

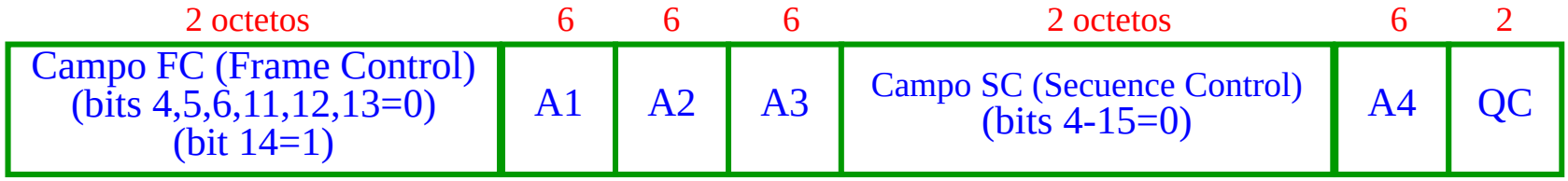
MIC: Message Integrity Code (64 bits).

Fase 4 (5). Cifrado CCMP

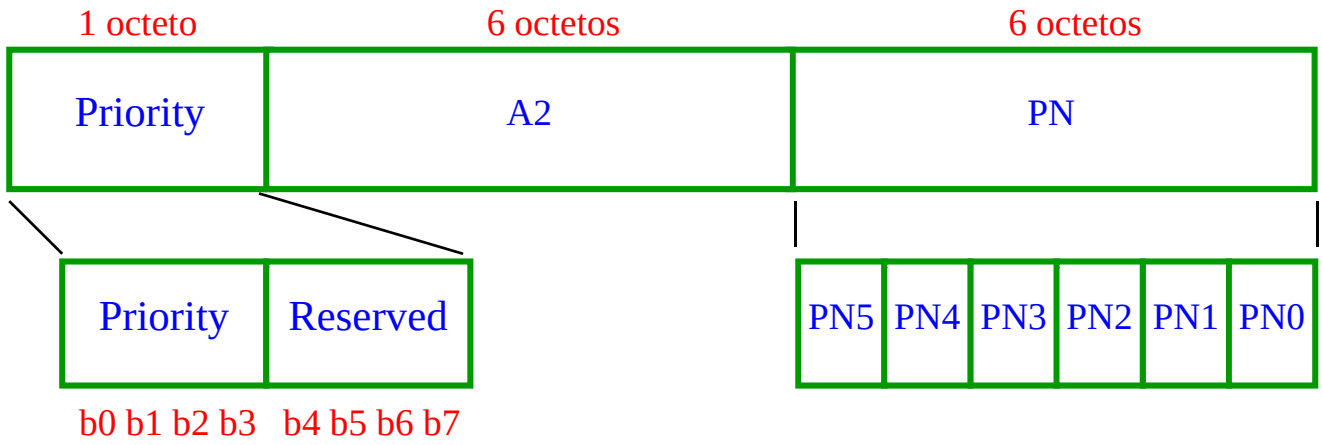


Fase 4 (6). Construcción de AAD y Nonce

AAD



Nonce

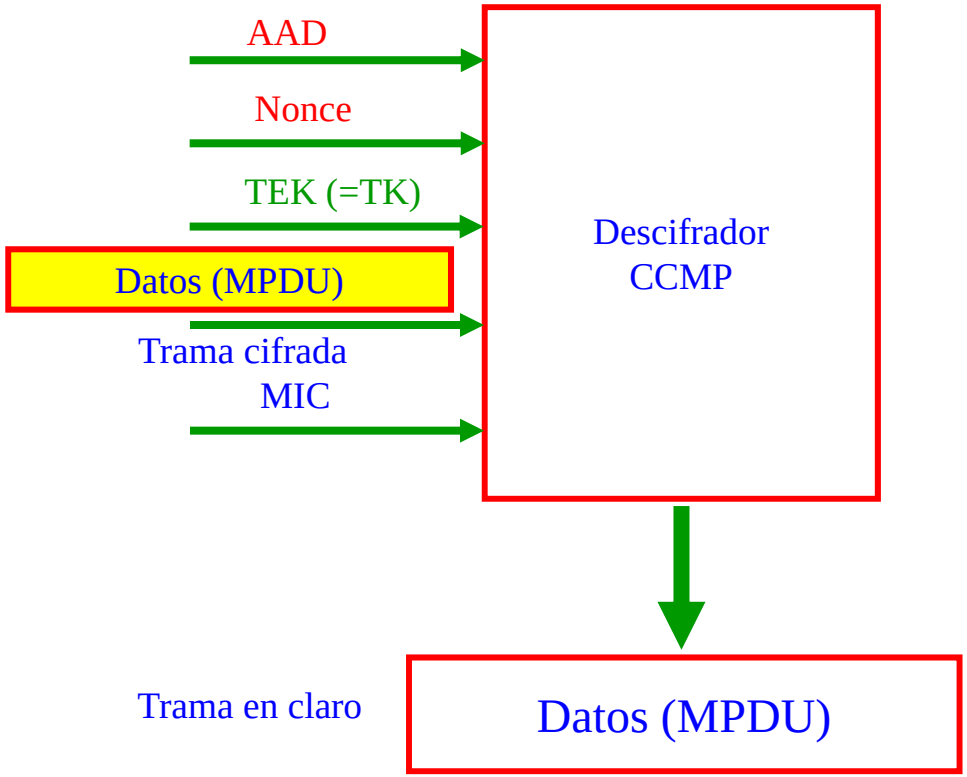


A1, A2, A3, A4 = Direcciones de la trama.

QC = Quality of Service Control Field = Reservado para el futuro, todo a ceros.

Priority= Reservado, todo a ceros.

Fase 4 (7). Descifrado CCMP



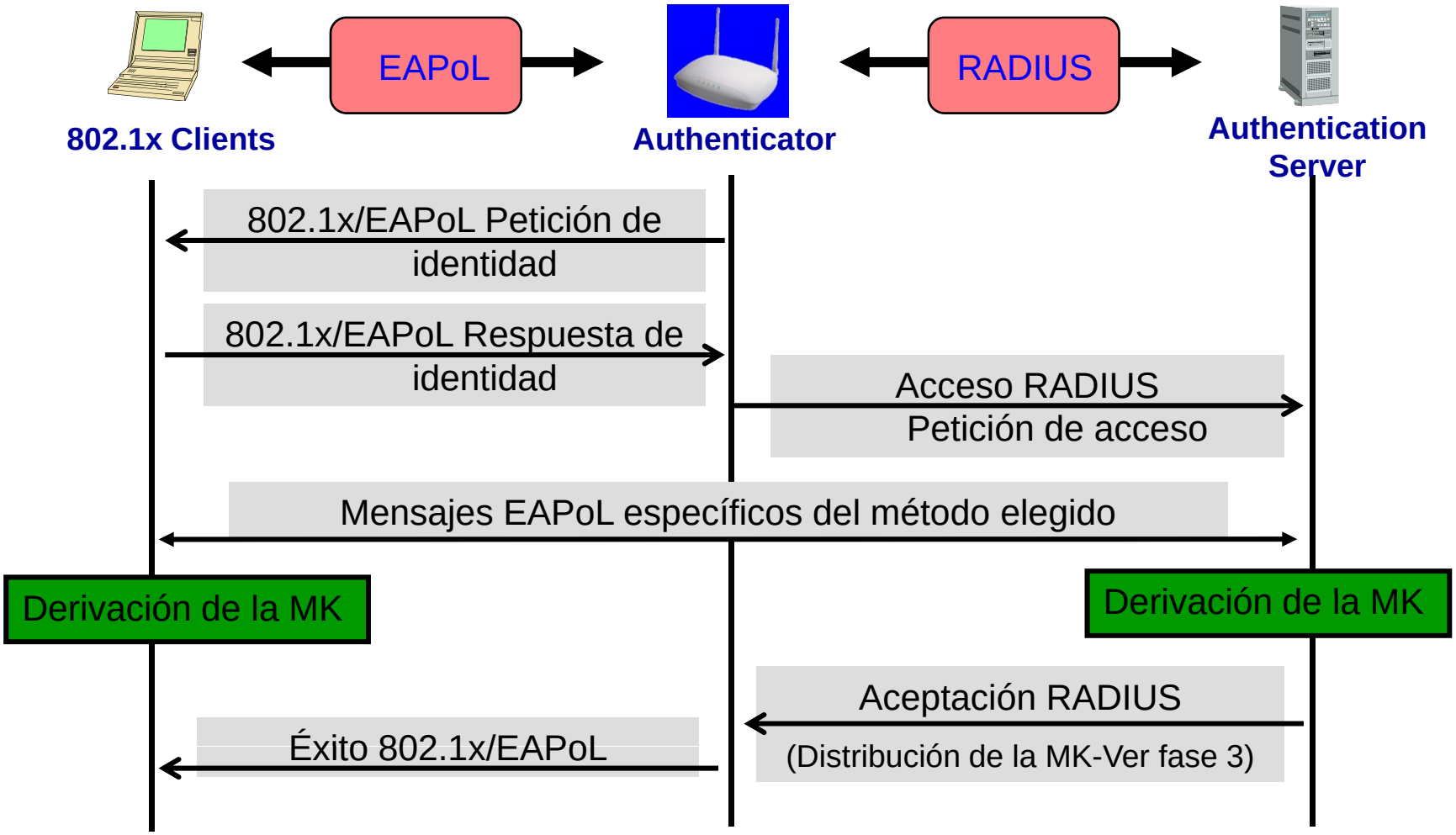
ENTERPRISE

Redes con autentificación

Fases: Terminología

- **Fase 1:** Acuerdo sobre la política de seguridad. Tanto el suplicante (Estación) como el autenticador (Punto de Acceso) se preasocian estableciendo una negociación de la política de seguridad que posteriormente les va a llevar a una asociación completa.
- **Fase 2:** Autentificación. En las redes tipo “enterprise”, donde se utiliza servidor de autentificación se realizará autentificación frente al servidor de autentificación. La forma de realizar la autentificación no está normalizada en la 802.11i.
- **Fase 3:** 4-Way Handsake. Tanto el suplicante como el autentificador calculan y derivan unas claves para la confidencialidad. Estas claves sólo son válidas para esta sesión. Si es rota la asociación, por cualquier causa, al volver a establecerla se realiza un nuevo cálculo de claves.
- **Fase 4:** Se establece la RSNA (RSN Association). Se produce el intercambio cifrado de información.

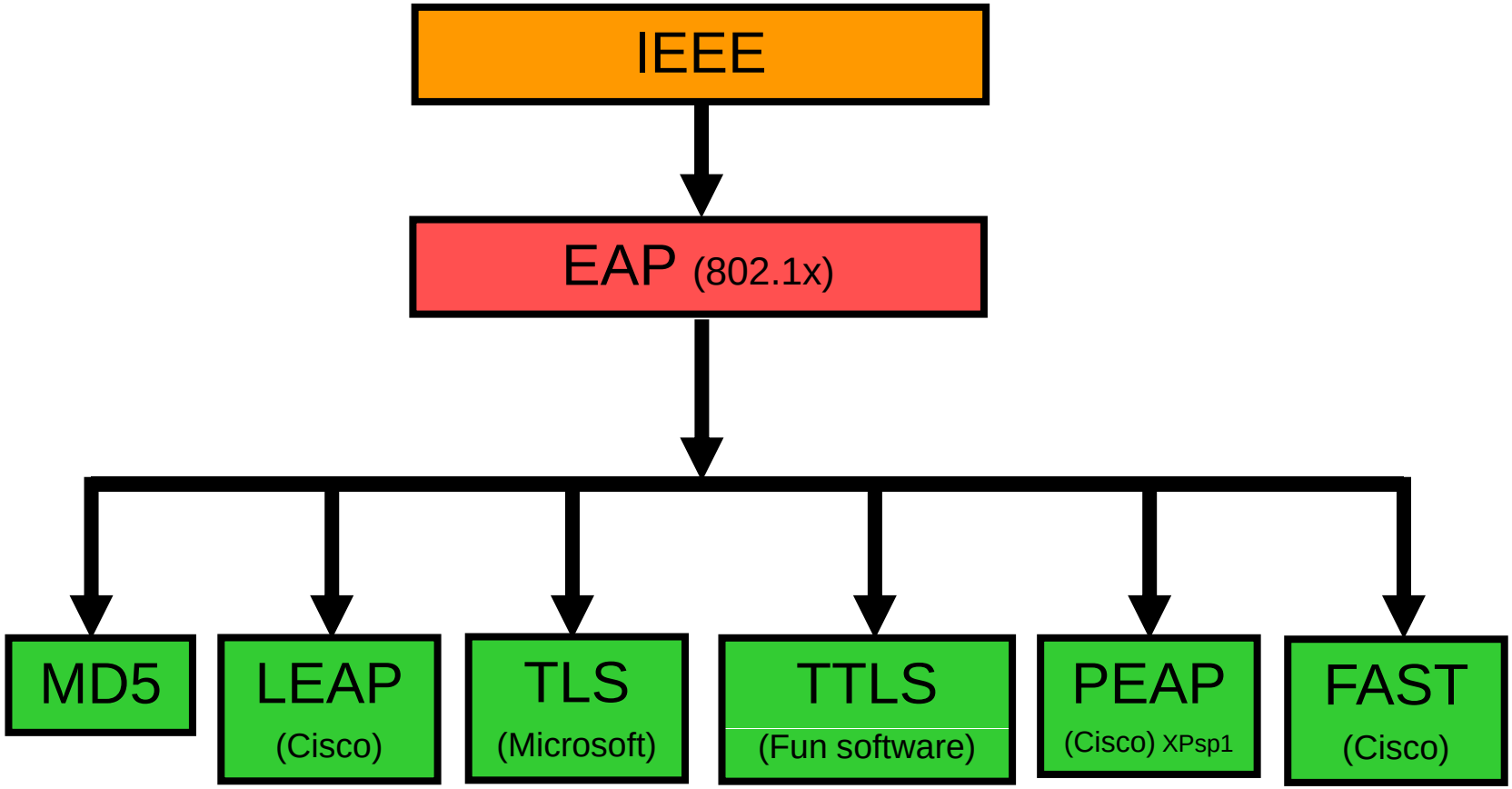
802.11i: Fase 2 (Autenticación 802.1x)



Fase 2: Descripción

- Cuando el tipo de red es empresarial, en esta fase se produce la autentificación del suplicante frente al servidor de autentificación. El puerto del autentificador (PA) no se abre hasta que no termina la Fase 3.
  - En este caso el servidor de autentificación envía un material (la MK: Master Key o clave maestra al autenticador, que la utilizará en la fase tres)
- En redes SOHO, esta fase no existe.
  - En redes pequeñas o domésticas la Master Key se deriva de una clave introducida a mano en el autenticador (PA) y en las estaciones. Esta clave se denomina PSK (Pre Shared Key).

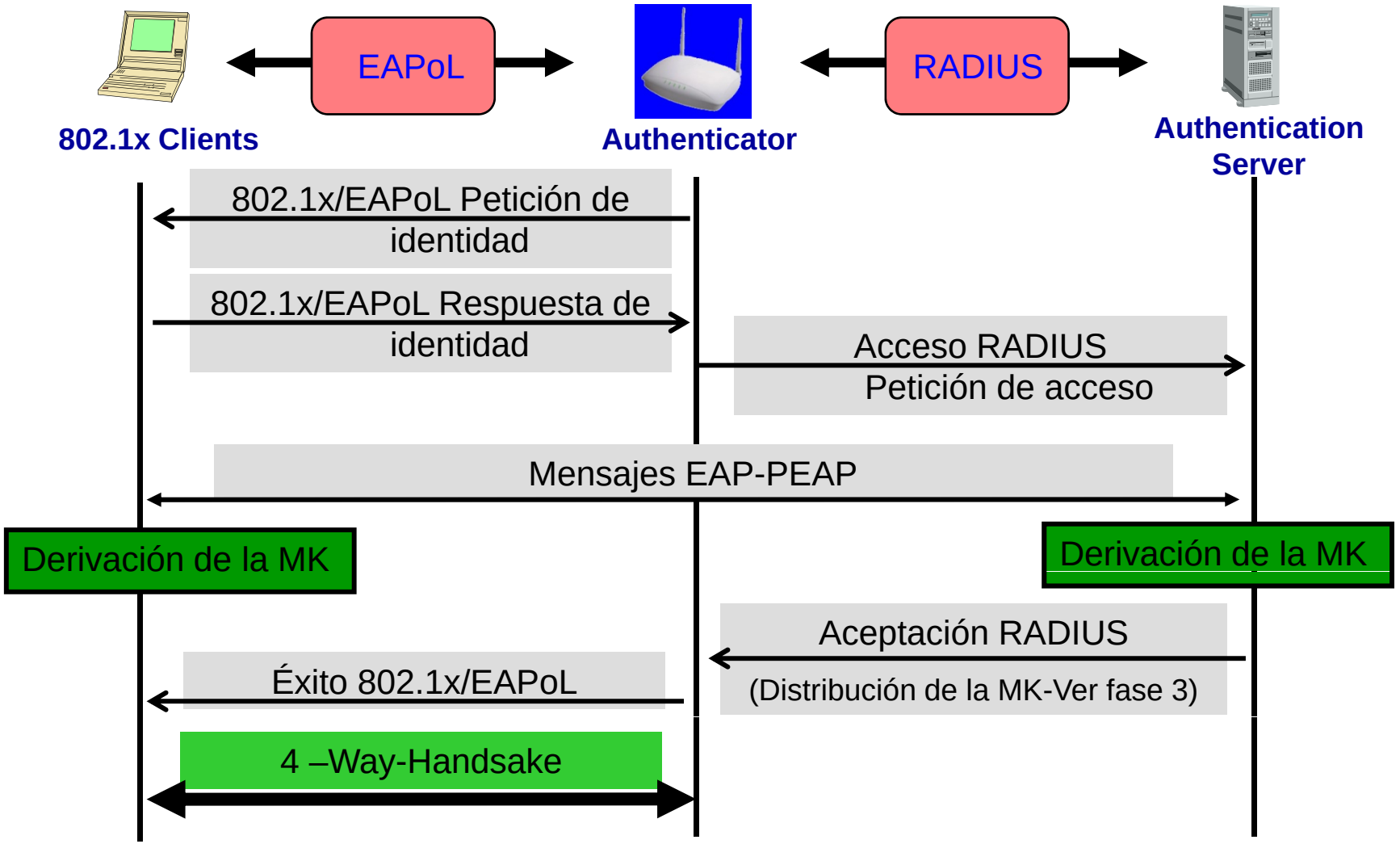
Fase 2: Protocolos de autentificación



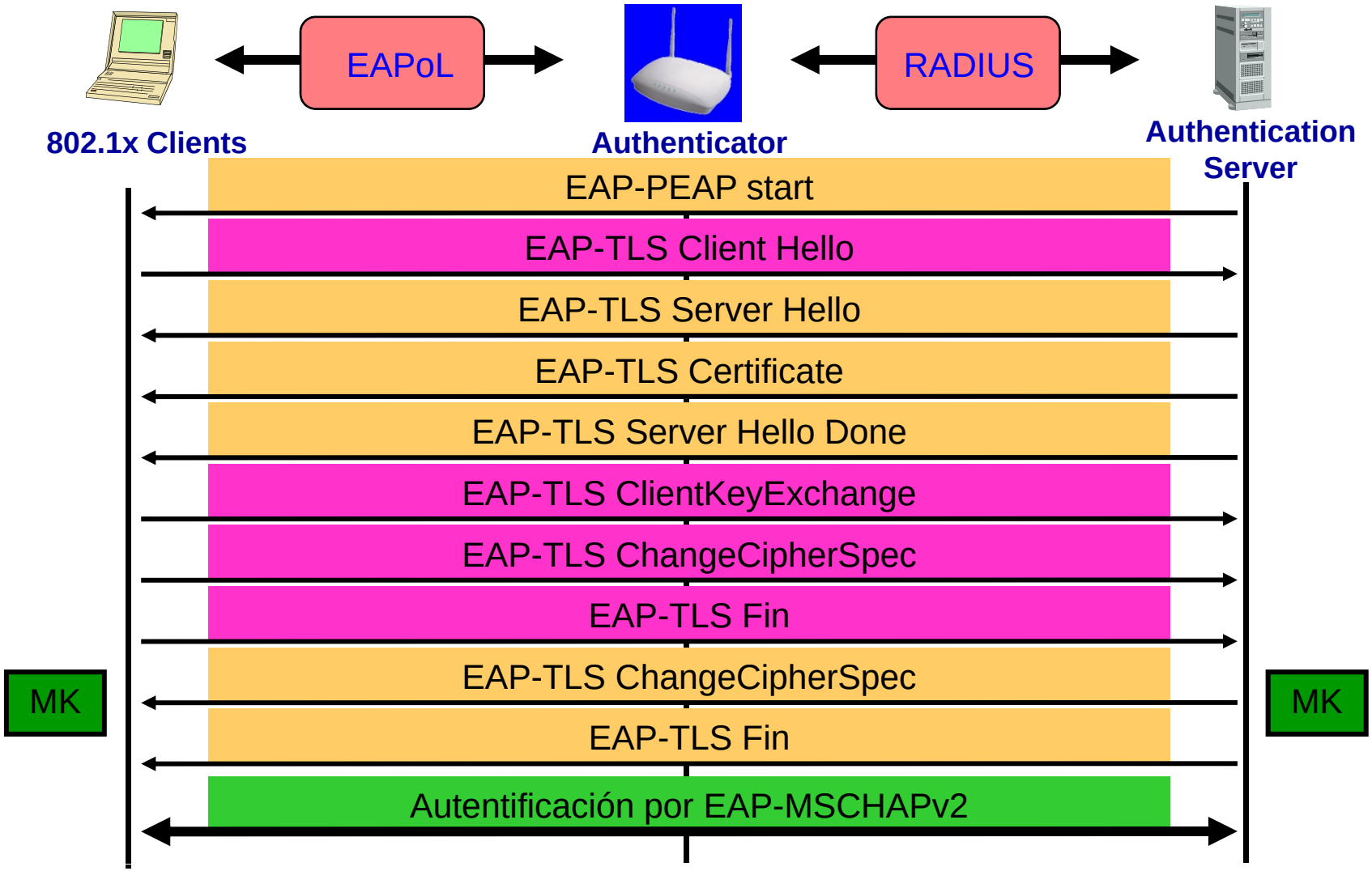
Fase 2: PEAPv0/EAP-MSCHAPv2

- Protected EAP.
- Propuesto por CISCO, Microsoft y RSA.
- Solo requiere certificado en el lado del servidor.
- Se realiza la creación de un túnel TLS.
- Una vez creado el túnel se autentifica con EAP-MSCHAPv2. (usuario y password).
- Se autentifican ambos: el cliente se autentifica ante el servidor y el servidor ante el cliente.
- Simplifica la configuración de los clientes y evita que estos tengan que tener un certificado propio.

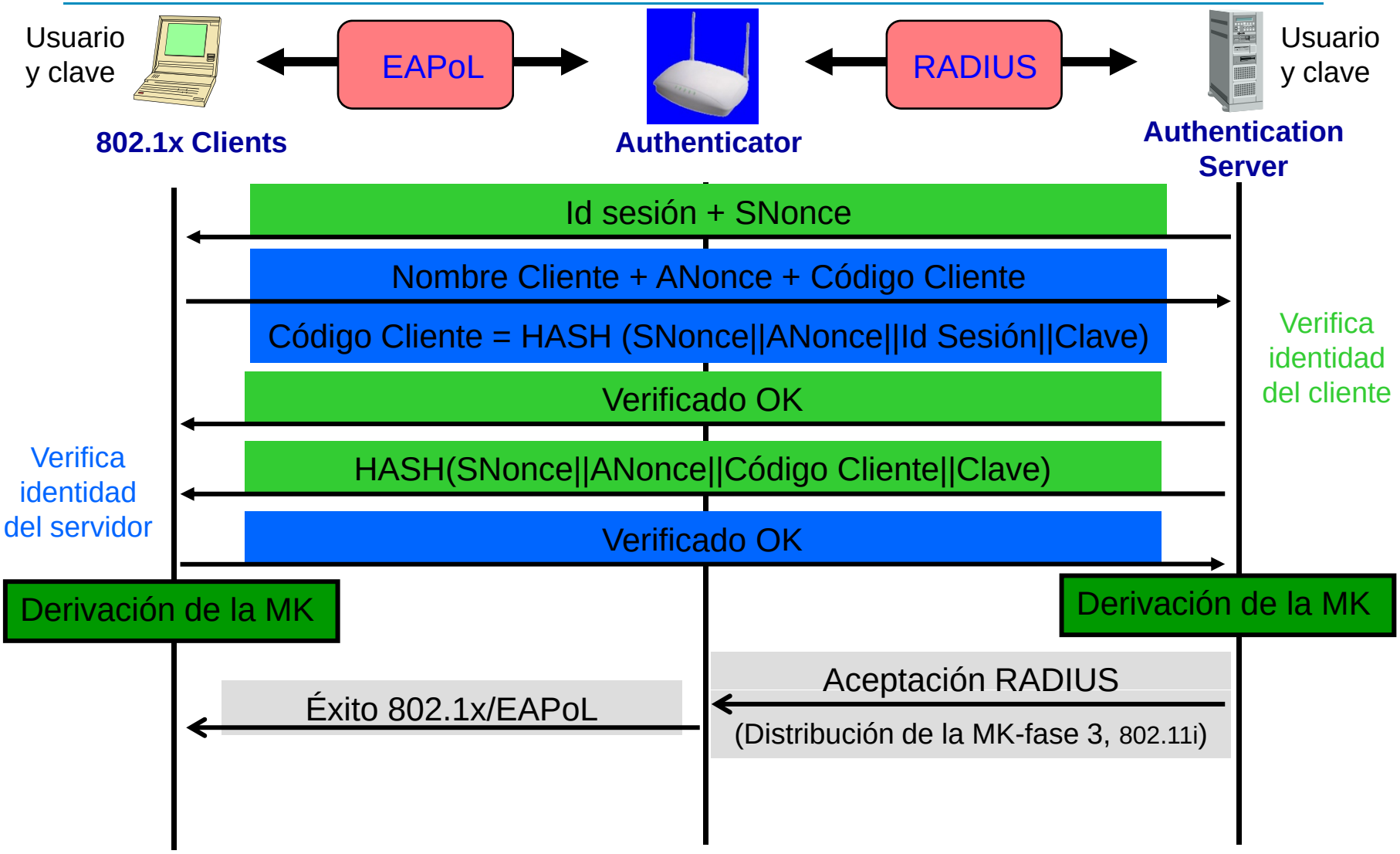
Fase 2: PEAPv0/EAP-MSCHAPv2



Fase 2: PEAPv0/EAP-MSCHAPv2 (fase TLS)



Fase 2: PEAPv0/EAP-MSCHAPv2 (fase MSCHAP)



Fases siguientes

- A continuación vendrían las Fases 3 y 4. Son idénticas al caso ya visto de las redes SOHO.
- La diferencia fundamental radica en que en la fase 3 se utiliza la MK (derivada del túnel TLS) en lugar de la PSK.

WPA / WPA-PSK

WPA (Para redes con autentificación):

-Con Servidor de Autentificación.

-Cifrado RC4 mejorado con una clave para cada paquete: TKIP (Temporal Key Integrity Protocol)

-Compatible en hardware con dispositivos anteriores actualizándoles el firmware.

WPA-PSK (Redes sin autentificación):

-Sin Servidor de Autentificación.

-Cifrado RC4 mejorado con una clave para cada paquete: TKIP (Temporal Key Integrity Protocol)

-Compatible en hardware con dispositivos anteriores actualizándoles el firmware.

WPA2 / WPA2-PSK

WPA2 (Para redes con autentificación):

-Con Servidor de Autentificación.
-Cifrado CCMP: AES con una clave de 128 bits.
-No es compatible en hardware con dispositivos anteriores.

WPA2-PSK (Redes sin autentificación):

-Sin Servidor de Autentificación.
-Cifrado CCMP: AES con una clave de 128 bits.
-No es compatible en hardware con dispositivos anteriores.

Debilidades WPA / WPA2

-Cuando se utiliza PSK, y no la autentificación 802.1x.

-PSK=PMK, si se conoce PMK se sabe PSK.

-Capturando los 4 mensajes de 4-Way-handsake.

-En el primero va el ANonce y en el segundo el SNonce y un MIC calculado con la KCK.

-Con un ataque por diccionario se puede ir probando PSK's, obtener, por cálculo la KCK y regenerar el MIC del segundo mensaje hasta que, por comparación, le coincida con el que ha capturado. Cuando sea así se obtendrá la clave PSK.

-Si se utiliza 802.1x La MK es distinta para cada sesión, si se averigua una **no sirve para las demás sesiones**.

-Si la fase de autenticación ya ha sido realizada se desasocia al cliente con aireplay (o con void11), para que al volver a asociarse se puedan capturar los mensajes del 4-way-handsake.

DEBILIDADES AJENAS A LA 802.11i

Modos de funcionamiento de la tarjeta

Distintos modos de funcionamiento:

MODO AP (MASTER), funcionalidad de Punto de Acceso

MODO MANAGED (CLIENTE), en infraestructura

MODO AD-HOC, redes a medida

MODO MONITOR (RFMON), Escucha de tramas en todos los canales, si se hace un barrido secuencial o en uno en particular.

Desasociación falsa

Petición de desasociación suplantando la dirección MAC del AP.

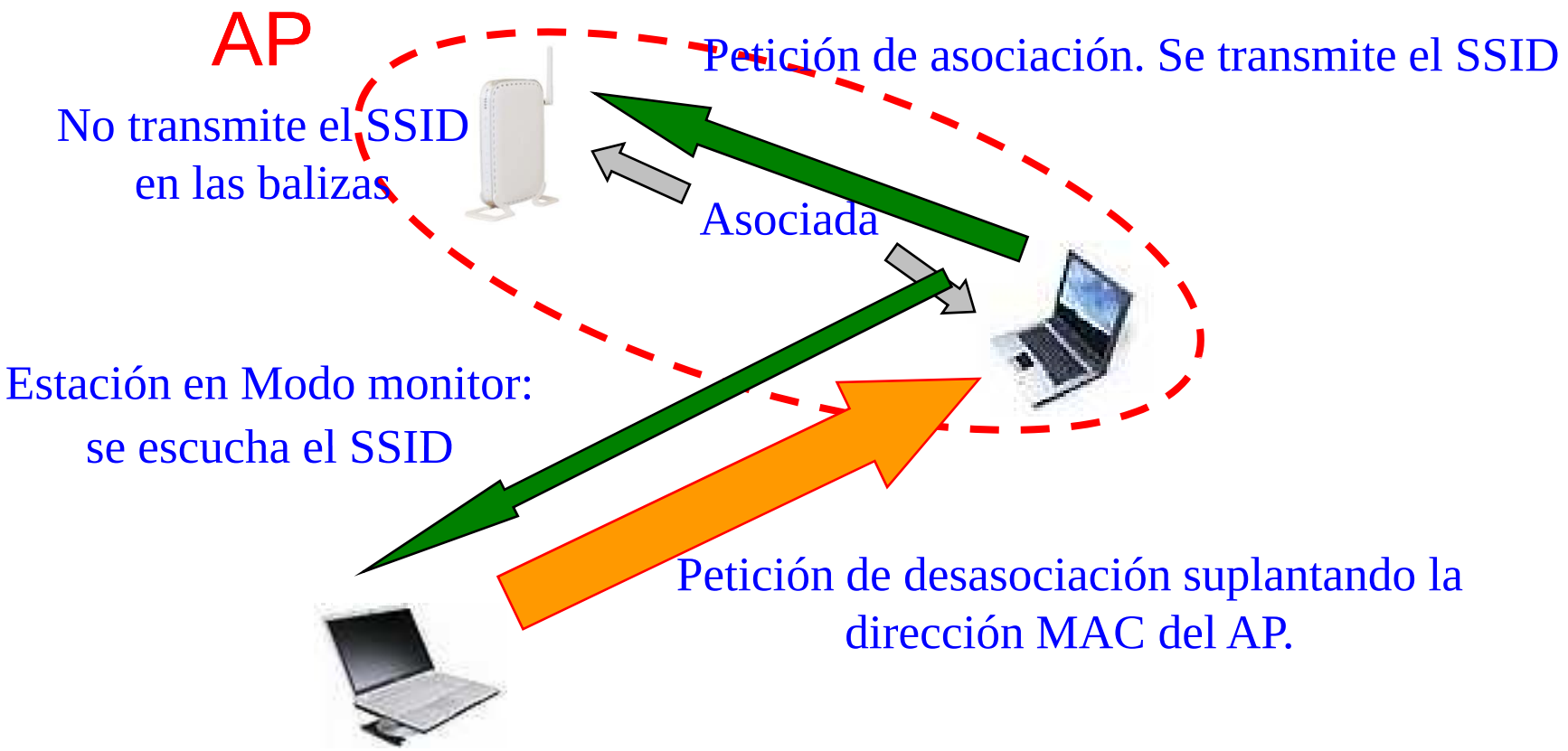
Se repite n veces por segundo.

Estación en modo AP (Master)

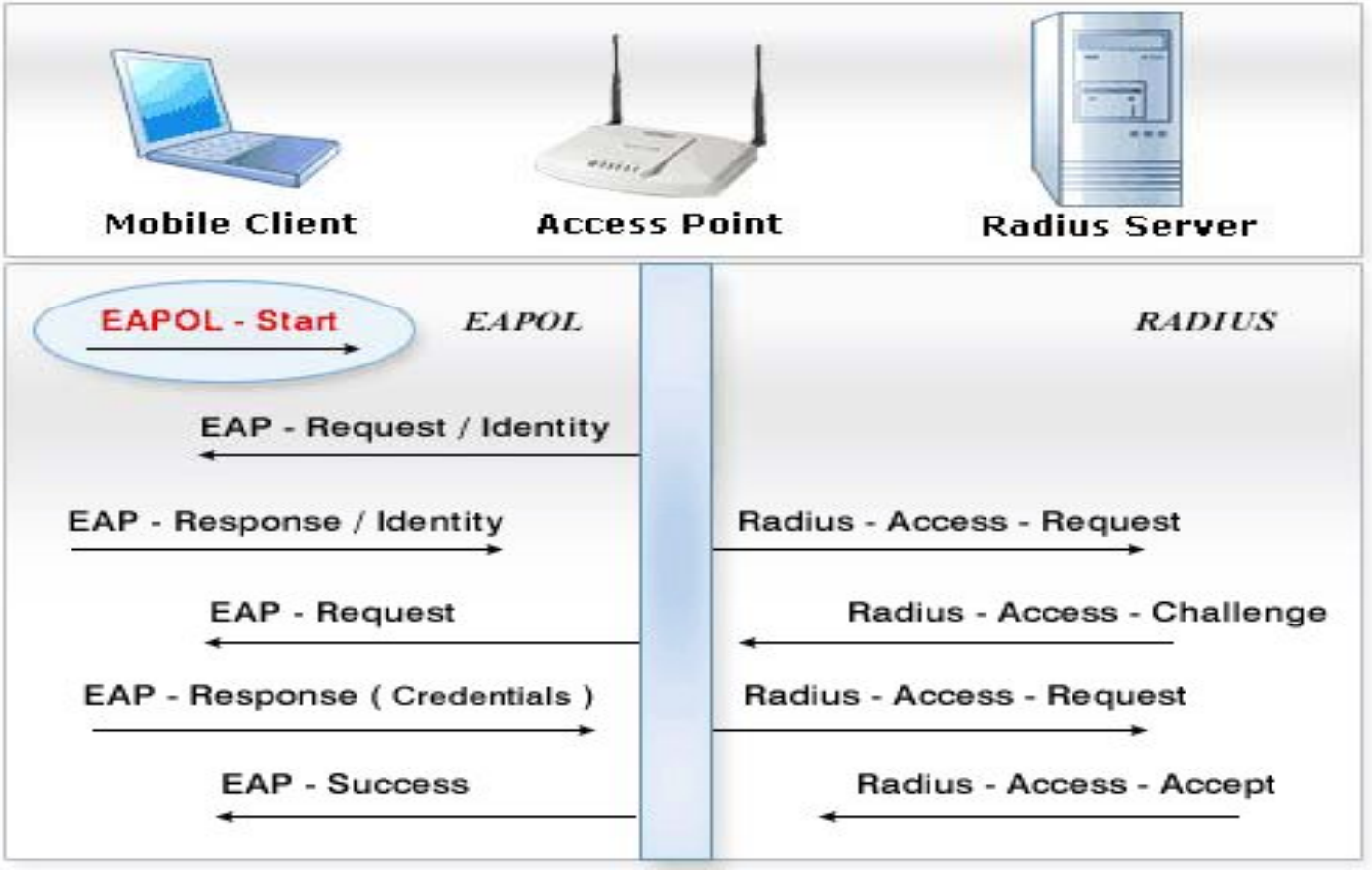
¡Inevitable!

Si se dirige a la dirección de difusión se deniega de servicio toda la red.

Obtención de ESSID en caso de red cerrada

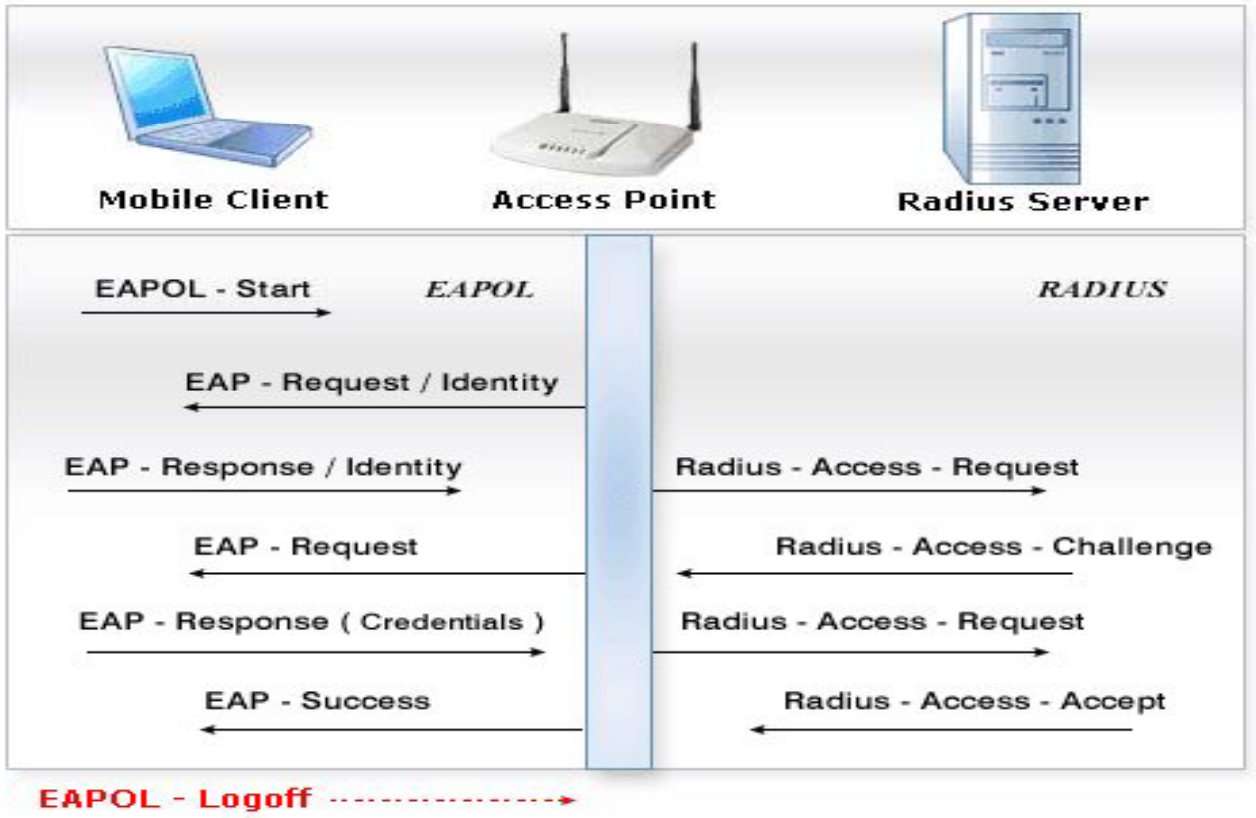


Ataque EAPoL- Start



Un atacante puede bloquear un AP enviando una inundación de tramas EAPOL-Start hasta consumir los recursos del AP.

Ataque EAPoL-Logoff



La trama EAPoL – Logoff no es autenticada. Un atacante envía esta trama simulando ser la estación asociada. Se produce un DoS.

FIN