Universidad de Oviedo

Departamento de Informática

Campus de Gijón

Seguridad Wi-Fi

Presentación

Daniel F. García

Introducción a las redes locales inalámbricas

La mayoría de las redes locales inalámbricas actuales se basan en el estándar IEEE 802.11

IEEE 802.11-1977 → Estándar inicial

… Nuevas versiones en 1999, 2007 …

IEEE 802.11-2020 → Estándar actual

https://standards.ieee.org/standard/802_11-2020.html

Cada versión del estándar es actualizado progresivamente mediante enmiendas (***amendments***)

Para generar una nueva versión del estándar se integran las enmiendas en la versión previa

Nomenclatura:

Las versiones del estándar se definen poniéndoles como sufijo el año de creación

Las enmiendas se definen usando como sufijo una o dos letras

Ejemplo: IEEE 802.11i → Enhanced Security (2004)

Wi-Fi Alliance https://www.wi-fi.org/

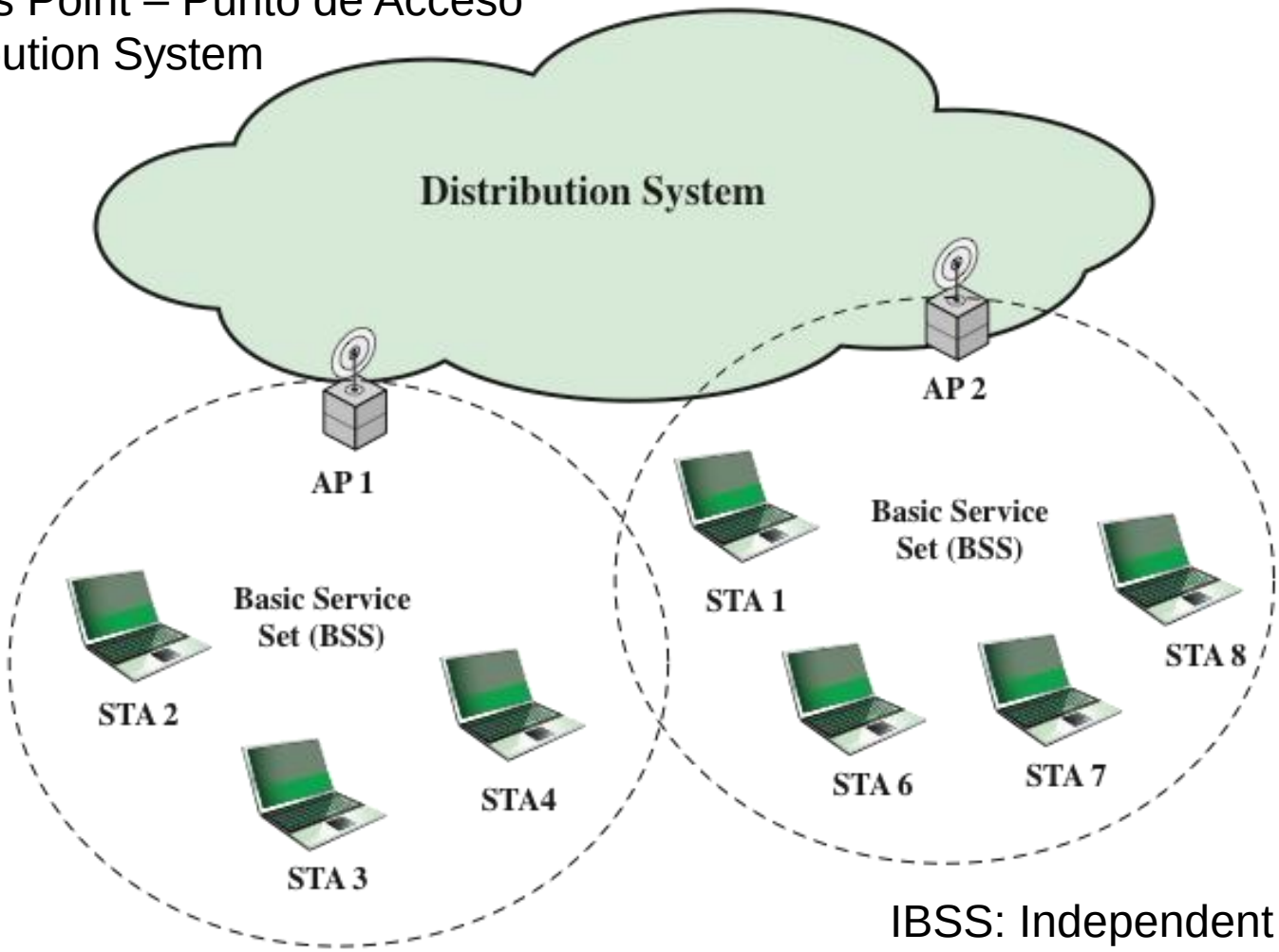
En 1999 se creó WECA (*Wireless Ethernet Compatibility Alliance*)

Renombrada a Wi-Fi (*Wireless Fidelity Alliance*)

Para certificar la interoperabilidad de productos de diversos fabricantes basados en 802.11

Componentes de una WLAN IEEE 802.11

STA: Station – Estación
AP: Access Point – Punto de Acceso
DS: Distribution System



Stallings – Cryptography & Network Security

IBSS: Independent BSS

ESS: Extended Service Set

Componentes de una WLAN IEEE 802.11

BSS: Conjunto de Servicio Básico

(Basic Service Set)

Conjunto de estaciones inalámbricas, ejecutando el mismo protocolo MAC y compitiendo por el acceso al mismo medio inalámbrico compartido

Un BSS puede estar aislado o conectado a un sistema de distribución mediante un AP

Cada estación del BSS siempre envía/recibe datos a través del AP

IBSS: Conjunto de Servicio Básico Independiente

(Independent Basic Service Set)

Es un BSS sin punto de acceso

Las estaciones se comunican directamente entre ellas y forman una red ad-hoc

ESS: Conjunto de Servicio Extendido

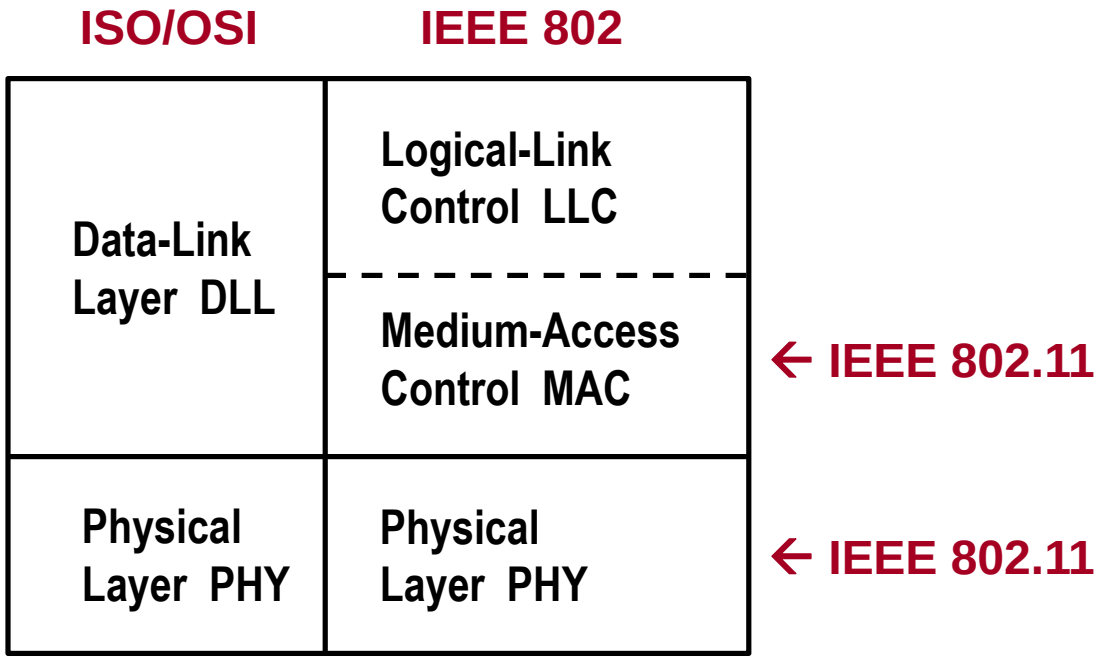
(Extended Service Set)

Consiste de dos o más BSS interconectados por un sistema de distribución

Un ESS se comporta como una única LAN al nivel LLC

Capas en el protocolo 802.11

IEEE 802.11 solo especifica las 2 capas inferiores del ISO/OSI para redes inalámbricas



Capa LLC Control del enlace lógico

Controla las tramas que se han recibido correctamente y las que faltan

Se encarga de la retransmisión de las tramas que faltan (debido a fallos)

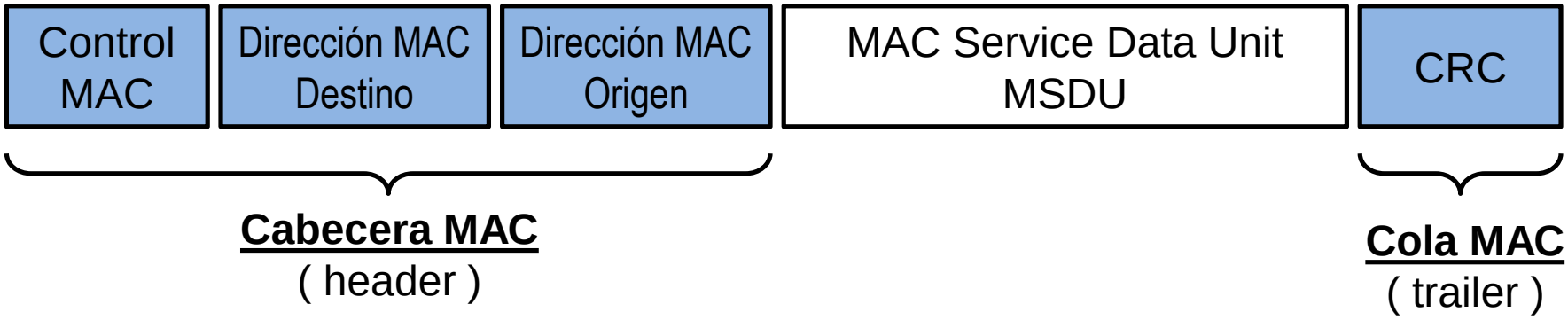
Pero la detección de errores se hace en la capa MAC

Capa MAC - Control de Acceso al Medio

La capa MAC recibe de / envía a / la capa superior un bloque de datos denominado **MSDU** (*MAC Service Data Unit*) con el que hace estas funciones:

- En Transmisión: ensambla los datos en tramas, denominadas **MPDU** (*MAC Protocol Data Unit*)
- En Recepción: desensambla tramas, reconoce direcciones y detecta errores
- Siempre controla el acceso al medio de transmisión

MPDU → Elementos que intercambian 2 capas MAC usando sus capas PHY



Usa direcciones MAC de 48 bits (Representadas en 6 grupos de 2 dígitos hexadecimales)
También usadas en Ethernet, Bluetooth, IEEE 802.5 Token-Ring, etc.

Capa PHY – Medio físico de transmisión (1)

La capa PHY especifica la codificación de los bits a nivel físico, frecuencias de trabajo, técnicas de modulación en el aire de tipo half-duplex, etc.

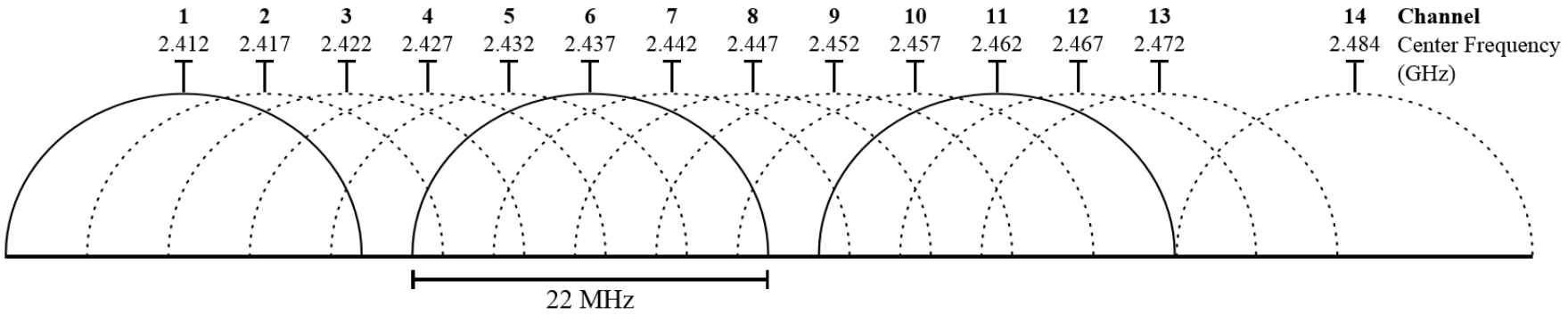
Frecuencias de trabajo más comunes

Banda de 2.4 GHz (2.400 – 2.500)

Se definen 14 canales, cada uno con un ancho de banda de 20 ó 22 MHz

Banda de 5 GHz (4.915 – 5.825)

Se definen 13 canales, cada uno con un ancho de banda de 20 MHz



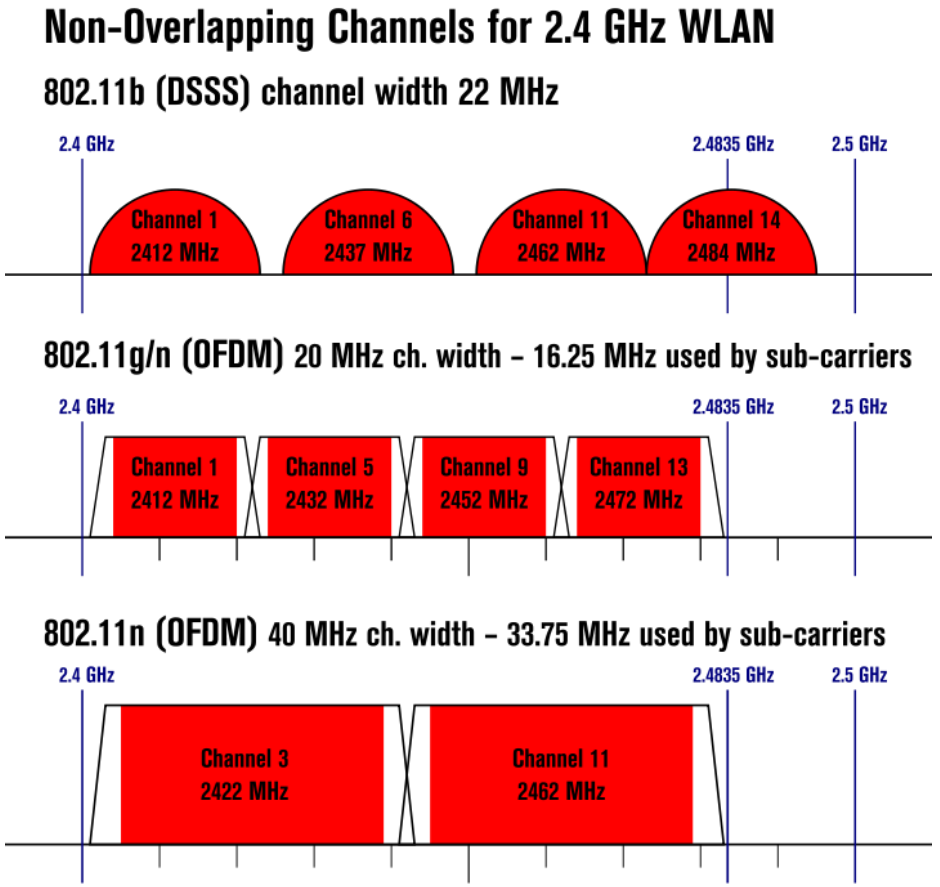
Al crear una WLAN conviene usar un canal que no se solape con otros ya utilizados

Capa PHY – Medio físico de transmisión (2)

Combinación de canales

El estándar 802.11**n** permite combinar 2 canales de 20 MHz para obtener uno de 40 MHz

El estándar 802.11**ac** permite combinar 2, 4 u 8 canales de 20 MHz para obtener un nuevo canal de 40, 80 ó 160 MHz



Un canal con más ancho de banda permite una señalización de mayor frecuencia y una velocidad de transmisión mayor

Capa PHY – Medio físico de transmisión (3)

Velocidades de transmisión

Cada versión del estándar 802.11 permite unas determinadas velocidades de transmisión entre un valor mínimo y un valor máximo

En los canales combinados, al duplicar el ancho de banda del canal, aproximadamente se duplica su velocidad de transmisión de datos en el canal

MIMO Streams

Los estándares IEEE 802.11**a/b/g** solo permiten una antena y un flujo de datos (*data stream*)

El estándar IEEE 802.11**n** introduce la tecnología MIMO (*Multiple-Input and Multiple-Output*) que permite el uso de hasta 4 antenas, y por tanto, 4 flujos de datos

El estándar IEEE 802.11**ac** introduce la tecnología Multiuser-MIMO que permite el uso de hasta 8 antenas, y por tanto, 8 flujos de datos simultáneos de usuarios distintos

Modulación

Casi siempre se utiliza OFDM (*Orthogonal frequency-division multiplexing*) para codificar una secuencia de bits en múltiples frecuencias portadoras

Evolución del estándar IEEE 802.11

V·T·E **IEEE 802.11 network PHY standards** [hide]

Frequency range, or type	PHY	Protocol	Release date[16]	Frequency (GHz)	Bandwidth (MHz)	Stream data rate[17] (Mbit/s)	Allowable MIMO streams	Modulation	Approximate range [citation needed] Indoor	Approximate range [citation needed] Outdoor
1–6 GHz	DSSS/FHSS[18]	802.11-1997	Jun 1997	2.4	22	1, 2	—	DSSS, FHSS	20 m (66 ft)	100 m (330 ft)
	HR-DSSS[18]	802.11b	Sep 1999	2.4	22	1, 2, 5.5, 11	—	DSSS	35 m (115 ft)	140 m (460 ft)
	OFDM	802.11a	Sep 1999	5	5/10/20	6, 9, 12, 18, 24, 36, 48, 54 (for 20 MHz bandwidth, divide by 2 and 4 for 10 and 5 MHz)	—	OFDM	35 m (115 ft)	120 m (390 ft)
		802.11j	Nov 2004	4.9/5.0[D][19] [failed verification]					?	?
		802.11p	Jul 2010	5.9					?	1,000 m (3,300 ft)[20]
		802.11y	Nov 2008	3.7[A]					?	5,000 m (16,000 ft)[A]
	ERP-OFDM	802.11g	Jun 2003	2.4					38 m (125 ft)	140 m (460 ft)
	HT-OFDM[21]	802.11n (Wi-Fi 4)	Oct 2009	2.4/5	20	Up to 288.8[B]	4	MIMO-OFDM	70 m (230 ft)	250 m (820 ft)[22] [failed verification]
					40	Up to 600[B]				
	VHT-OFDM[21]	802.11ac (Wi-Fi 5)	Dec 2013	5	20	Up to 346.8[B]	8	MIMO-OFDM	35 m (115 ft)[23]	?
					40	Up to 800[B]				
					80	Up to 1733.2[B]				
					160	Up to 3466.8[B]				
	HE-OFDMA	802.11ax (Wi-Fi 6)	Feb 2021	2.4/5/6	20	Up to 1147[F]	8	MIMO-OFDM	30 m (98 ft)	120 m (390 ft) [G]
					40	Up to 2294[F]				
					80	Up to 4804[F]				
					80+80	Up to 9608[F]				
mmWave	DMG[24]	802.11ad	Dec 2012	60	2,160	Up to 6,757[25] (6.7 Gbit/s)	—	OFDM, single carrier, low-power single carrier	3.3 m (11 ft)[26]	?
		802.11aj	Apr 2018	45/60[C]	540/1,080[27]	Up to 15,000[28] (15 Gbit/s)	4[29]	OFDM, single carrier[29]	?	?
	EDMG[30]	802.11ay	Est. March 2021	60	8000	Up to 20,000 (20 Gbit/s)[31]	4	OFDM, single carrier	10 m (33 ft)	100 m (328 ft)
Sub-1 GHz IoT	TVHT[32]	802.11af	Feb 2014	0.054–0.79	6–8	Up to 568.9[33]	4	MIMO-OFDM	?	?
	S1G[32]	802.11ah	Dec 2016	0.7/0.8/0.9	1–16	Up to 8.67 (@2 MHz)[34]	4		?	?
2.4 GHz, 5 GHz	WUR	802.11ba[E]	Oct 2021	2.4/5	4.06	0.0625, 0.25 (62.5 kbit/s, 250 kbit/s)	—	OOK (Multi-carrier OOK)	?	?
Light (Li-Fi)	IR	802.11-1997	Jun 1997	?	?	1, 2	—	PPM	?	?
	?	802.11bb	Est. Jul 2022	60000-790000	?	?	—	?	?	?
802.11 Standard rollups										
Org: Wikipedia		802.11-2007	Mar 2007	2.4, 5		Up to 54		DSSS, OFDM		
		802.11-2012	Mar 2012	2.4, 5		Up to 150[B]		DSSS, OFDM		
		802.11-2016	Dec 2016	2.4, 5, 60		Up to 866.7 or 6,757[B]		DSSS, OFDM		
		802.11-2020	Dec 2020	2.4, 5, 60		Up to 866.7 or 6,757[B]		DSSS, OFDM		

Servicios IEEE 802.11 (1)

El estándar IEEE 802.11 especifica 9 servicios → { 6 de transferencia de datos; 3 de seguridad }

Servicios de transferencia de datos

Distribution Service

Utilizado por una estación de un BSS para enviar datos a una estación de otro BSS usando el Sistema de Distribución (DS) en un mismo ESS

Integration Service

Utilizado para transferir datos entre una estación de una LAN 802.11 y otra estación integrada en otra LAN 802.xx

MSU Delivery

Servicio básico para enviar datos

Servicios IEEE 802.11 (2)

Servicios relacionados con asociaciones

Antes de que el servicio de distribución pueda enviar / recibir datos a / de una estación la estación debe estar asociada

El concepto de asociación está relacionado con
Las transiciones que se producen al moverse las estaciones

- SIN Transición

  La estación no se mueve o se mueve dentro del rango de cobertura de un único BSS

- Transición BSS

  Se produce cuando una estación se mueve de un BSS a otro BSS, ambos en el mismo ESS

- Transición ESS

  Se produce cuando una estación se mueve de un BSS en un ESS a otro BSS de otro ESS

  Generalmente no se pueden mantener las conexiones de alto nivel

Servicios IEEE 802.11 (3)

Servicio de Asociación

Establece la asociación inicial entre una STA y un AP

Este servicio lo proporciona el sistema de distribución (DS) y lo solicita cada STA

El estándar 802.11 no define como debe el DS almacenar las asociaciones

> En un determinado instante …
> Una STA solo puede estar asociada con un determinado AP
> Un AP puede estar asociado con muchas STAs

La asociación es necesaria, pero no suficiente, para soportar Transiciones BSS

La asociación es suficiente, para soportar un funcionamiento SIN Transiciones

Servicio de Reasociación

Una STA usa la reasociación al moverse de un BSS a otro BSS dentro de un ESS

El servicio de reasociación lo proporciona el DS

La reasociación es suficiente para soportar Transiciones BSS

Servicios IEEE 802.11 (4)

Servicio de Desasociación

Una STA o un AP notifica al DS que una asociación existente es eliminada
Ya no se podrán enviar mensajes con esa asociación

- Una STA debe desasociarse cuando abandona la red
- Un AP debe desasociarse cuando ya no proporciona el servicio (ej. se apaga)

El servicio de desasociación lo proporciona el DS

La desasociación es una notificación, no una solicitud

La desasociación no puede ser rechazada por ningún elemento
que forme parte de la asociación

La seguridad en redes inalámbricas: estándares

1999 Sep — **WEP = Wired Equivalent Privacy**

- Incluido en el estándar IEEE 802.11
- Presentaba diversas vulnerabilidades

2003 — **WPA = Wi-Fi Protected Access**

- La Wi-Fi Alliance propuso este estándar de seguridad para WLANs basándose en los trabajos ya realizados en el estándar IEEE 802.11i
  - WPA se adelantó al estándar final completo y por ello …
  - WPA se denomina Draft IEEE 802.11i standard

2004 Jun — **WPA2 = IEEE 802.11i standard**

- Estándar final del comité IEEE 802.11 y actualmente en uso

2018 Abr — **WPA3**

- Mejora de la tecnología propuesta por la Wi-Fi Alliance

Estándar IEEE 802.11i – Introducción

El estándar 802.11i está integrado en el IEEE 802.11 – 2020 (Sec.12: Security)

Servicios básicos de seguridad → { Control de acceso mediante autenticación; Confidencialidad e integridad de los mensajes }

- WPA, WPA2 y WPA3 se diseñaron para usar un ***Servidor de Autenticación*** que distribuye claves diferentes a cada usuario (estación)

  Usando el protocolo IEEE 802.1X

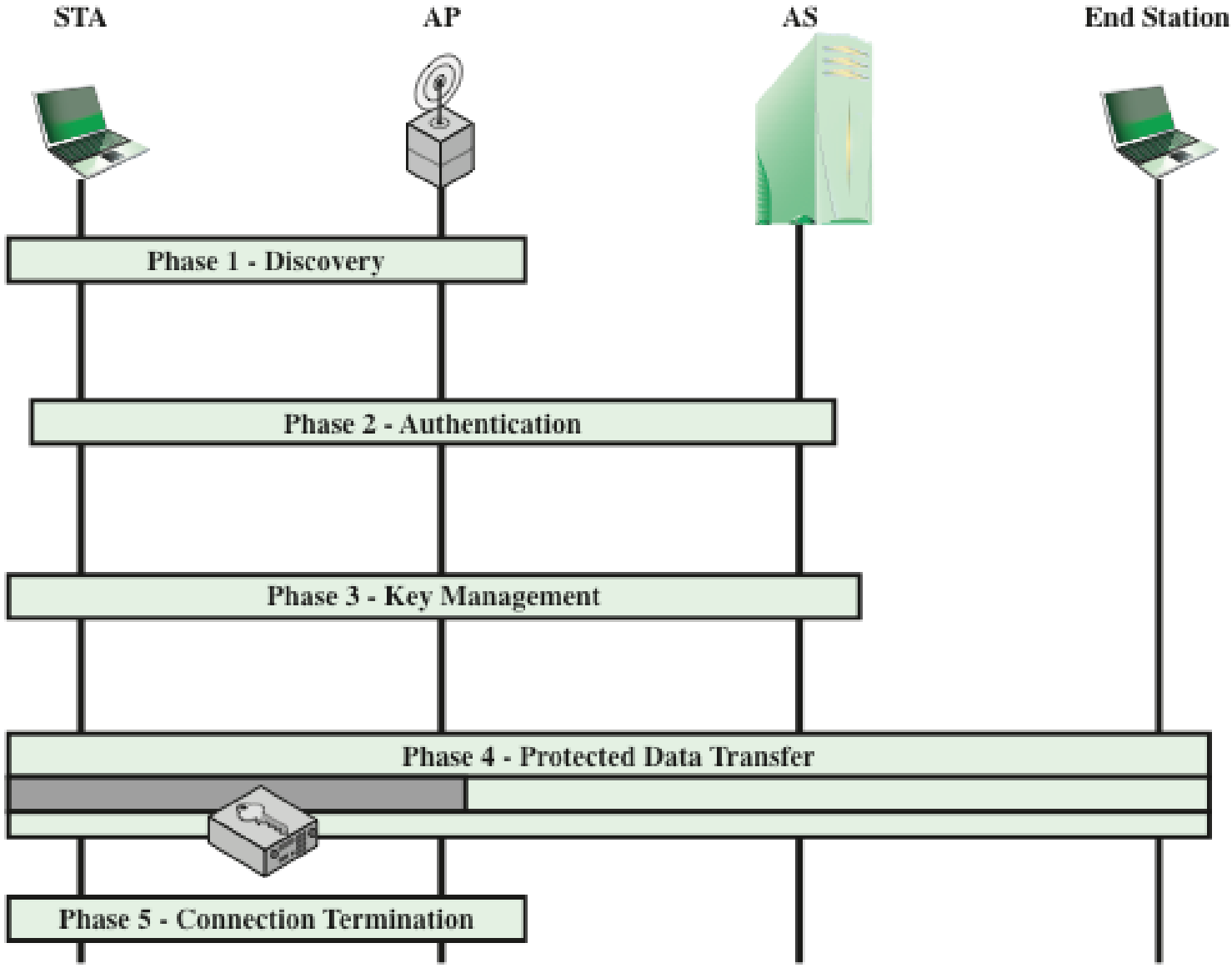
  La Wi-Fi Alliance los denomina → { WPA-Enterprise; WPA2-Enterprise; WPA3-Enterprise }

- WPA y WPA2 también se pueden usar de un modo menos seguro usando ***claves pre-compartidas*** por los usuarios
  Pero WPA3 utiliza SAE (***Simultaneous Authentication of Equals***)

  Esto se suele usar en el hogar y en pequeñas oficinas

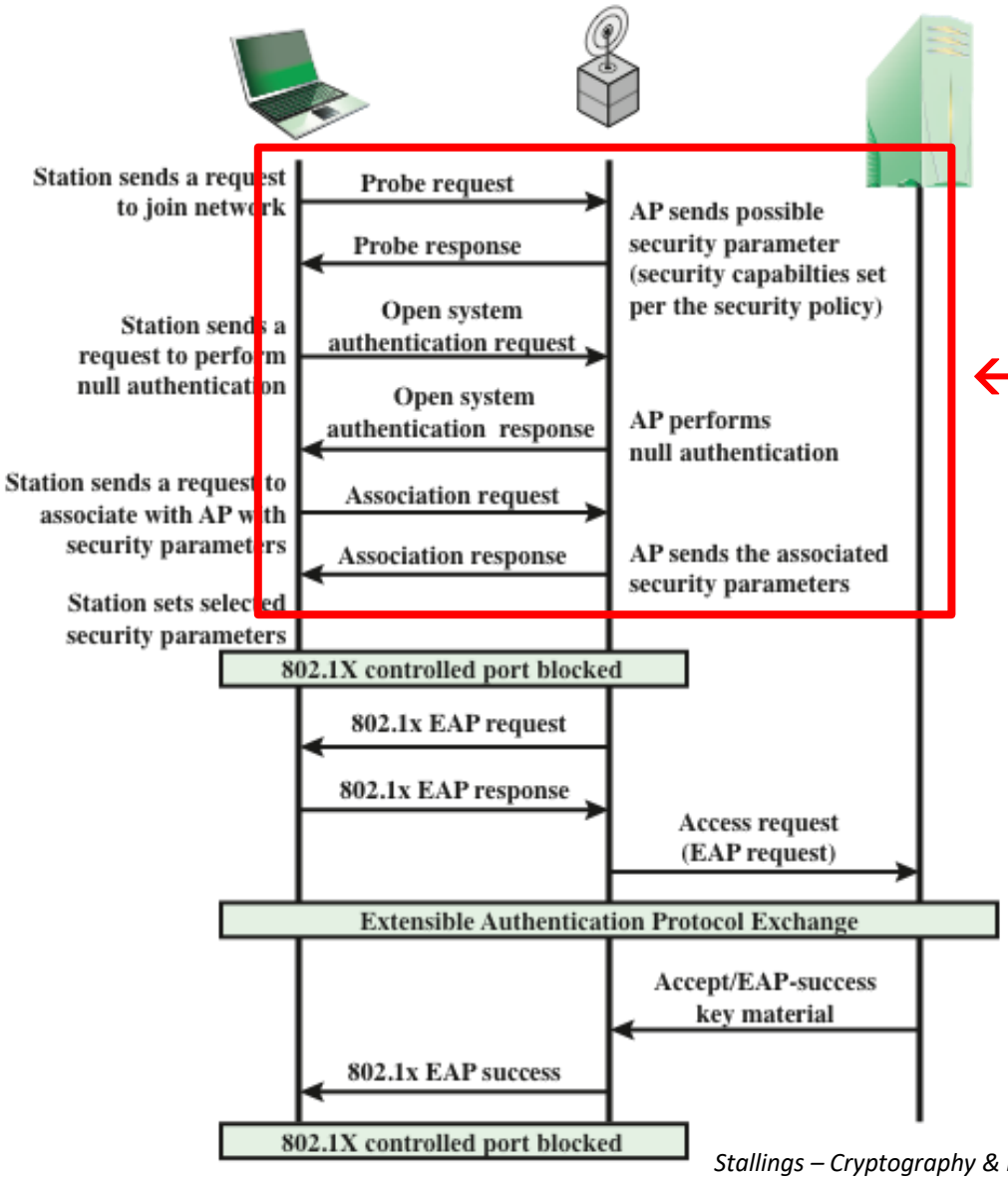
  La Wi-Fi Alliance los denomina → { WPA-Personal; WPA2-Personal; WPA3-Personal }

Fases de operación de una RSN



Stallings – Cryptography & Network Security

Fase 1: Descubrimiento



Stallings – Cryptography & Network Security

Propósito: que una STA y un AP se **reconozcan** mutuamente acuerden las **capacidades** de seguridad y establezcan una **asociación**

← **Consiste en 3 intercambios de mensajes**

Capacidades de seguridad

1) Autenticación y gestión de claves
(AKM = Authentication and Key Management)
- IEEE 802.1X
- Clave pre-compartida

2) Confidencialidad e integridad de tramas
- WEP
- TKIP
- CCMP

Fase 1: Descubrimiento

Interacción 1

Una STA descubre un AP de una WLAN y envía una petición para unirse a la red

- Pasivamente: monitorizando tramas Beacon que envía periódicamente el AP
- Activamente: probando cada canal posible para una WLAN

El AP responde con un RSN-IE (Robust Security Network – Information Element)

El RSN-IE contiene las capacidades de seguridad que soporta el AP

Interacción 2

Usada para mantener la compatibilidad con versiones previas de la máquina de estados 802.11 implementada en el hardware existente

La STA y el AP intercambian identificadores

Interacción 3

La STA envía una solicitud de asociación al AP con un método de autenticación y una suite de gestión de claves de entre las publicadas por el AP

Si no hay ninguna coincidencia en las capacidades, el AP rechaza la asociación

Durante esta fase los puertos controlados IEEE 802.1X están bloqueados

Fase 2: Autenticación - Introducción

Propósito: Permitir el uso de la red solo a STAs autorizadas y garantizar a las STAs que se comunican con una red legítima

Hay 2 formas de autenticación en función del modo de trabajo de la red Wi-Fi:

	Personal Mode	**Enterprise** Mode
WPA	Autenticación: **PSK** Cifrado: TKIP/MIC	Autenticación: **IEEE 802.1X/EAP** Cifrado: TKIP/MIC
WPA2	Autenticación: **PSK** Cifrado: AES-CCMP	Autenticación: **IEEE 802.1X/EAP** Cifrado: AES-CCMP
WPA3	Autenticación: **SAE** Cifrado: AES-GCMP	Autenticación: **IEEE 802.1X/EAP** Cifrado: AES-GCMP

PSK = Pre-Shared Key (claves compartidas previamente)
SAE = Simultaneous Authentication of Equals

Autenticación en el modo Enterprise

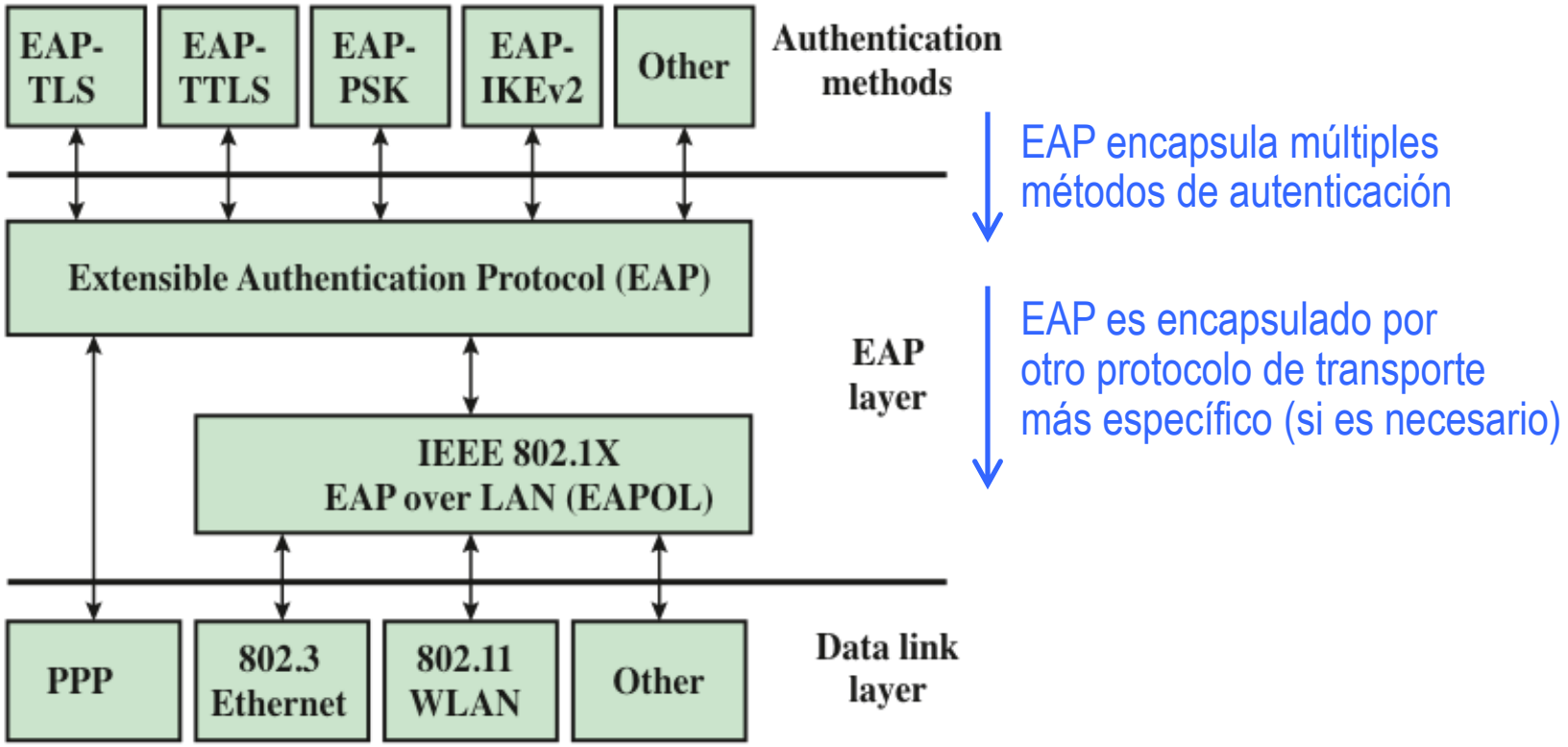
Utiliza el protocolo de autenticación extensible *Extensible Authentication Protocol (EAP)*

Definido en RFC 3748 (Junio 2004)
https://datatracker.ietf.org/doc/pdf/rfc3748

Protocolo EAP (1) Introducción

El protocolo EAP proporciona un servicio de transporte genérico para intercambiar información de autenticación entre un cliente y un servidor de autenticación

Extensible ←→ Soporta múltiples métodos (protocolos) de autenticación que deben estar instalados tanto en el cliente como en el servidor



Stallings – Cryptography & Network Security

Protocolo EAP (2) Métodos de autenticación

EAP-TLS (EAP Transport Layer Security) RFC 5216 (Marzo 2008)

Define la encapsulación del protocolo TLS en EAP
El cliente y el servidor se autentican mutuamente usando certificados

El cliente genera un número aleatorio que cifra con la clave pública del servidor y se lo envía

El cliente y el servidor usan el aleatorio para generar la misma clave secreta para una sesión

EAP-TTLS (EAP Tunneled Transport Layer Security) RFC 5281 (Agosto 2008)

Es igual que el EAP-TLS, excepto que solo el servidor tiene un certificado

EAP-GPSK (EAP Generalized Pre-Shared Key) RFC 5433 (Febrero 2009)

Define la autenticación mutua y la derivación de una clave de sesión
a partir de claves pre-compartidas

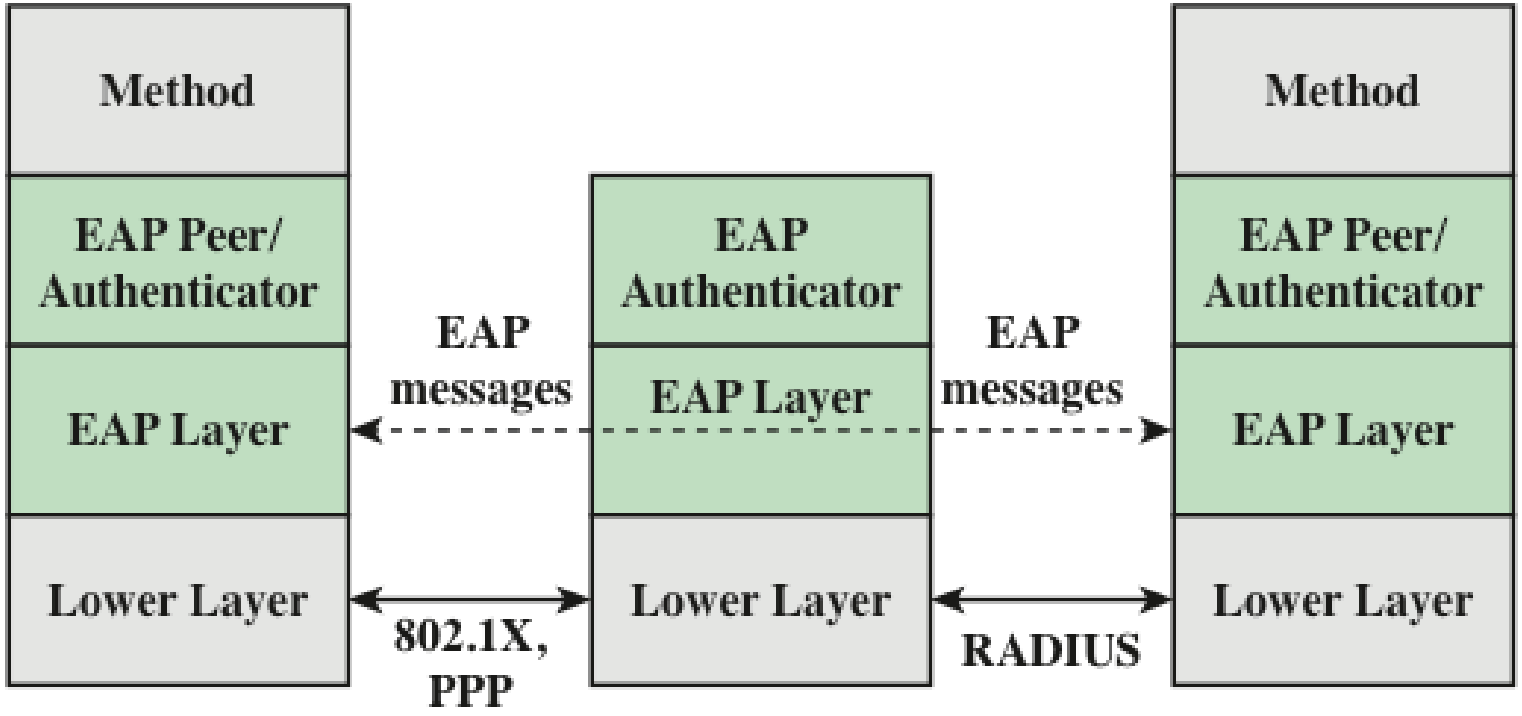
EAP-IKEv2 (EAP Internet Key Exchange v2) RFC 5106 (Febrero 2008)

Define la autenticación mutua y el establecimiento de claves de sesión
usando el protocolo IKE

Protocolo EAP (3) Entorno típico de utilización

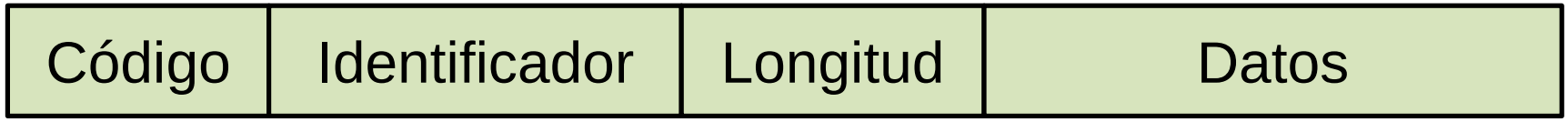
Nomenclatura de Entidades = F (protocolo)

EAP →	Peer	Authenticator	Authentication server
802.1X →	Supplicant	Authenticator	Authentication server
802.11 →	Station (STA)	Access Point (AP)	Authentication server (AS)



PPP=Point-to-Point Protocol (RFC 1661) RADIUS=Remote Authentication Dial-In User Service (RFC 2865)

Protocolo EAP (4) Formato de los mensajes



Código Identifica el tipo de mensaje EAP

(1) Solicitud o petición (*Request*)
(2) Respuesta (*Response*)
(3) Éxito (*Success*)
(4) Fallo (*Failure*)

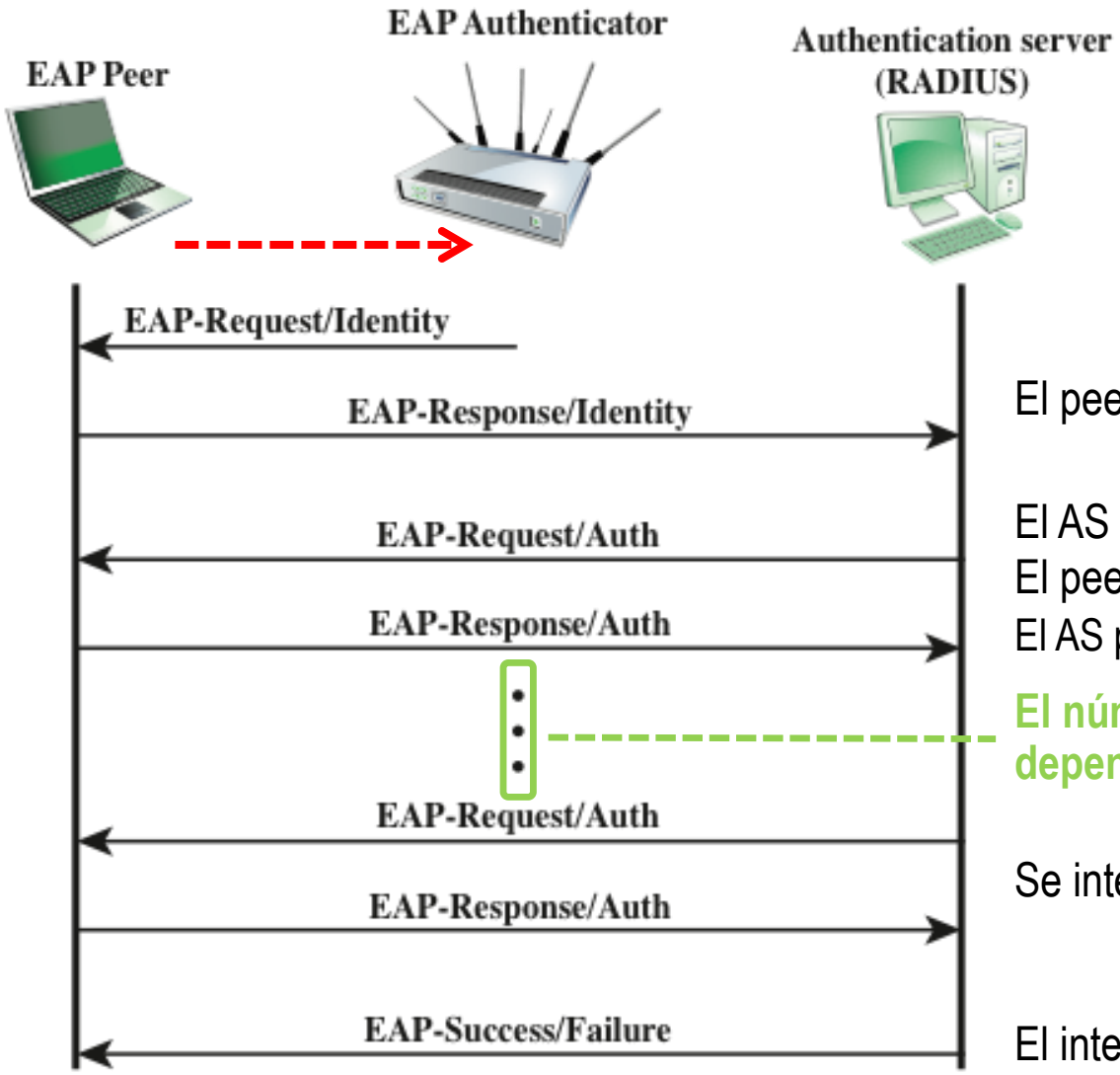
Identificador Se usa para asociar respuestas con peticiones

Longitud Indica la longitud, en bytes, del mensaje completo incluyendo los 4 campos del mensaje

Datos Contiene la información relacionada con la autenticación
Típicamente incluye un identificador del tipo de datos y luego los datos

Los mensajes de Éxito y Fallo no tienen el campo de datos

Protocolo EAP (5) Intercambio de mensajes



Stallings – Cryptography & Network Security

El peer envía un mensaje inicial usando un protocolo de bajo nivel

PPP ó IEEE 802.1X (**NO** EAP)

El peer envía su identidad al AS

El AS solicita usar un método EAP al peer
El peer responde aceptando o rechazando
El AS puede proponer otros métodos o abortar

El número de pares Petición/Respuesta depende del método usado

Se intercambia info de autenticación y claves

El intercambio termina con Éxito ó Fallo

Protocolo IEEE 802.1X (1) Introducción

IEEE 802.1X se diseñó para proporcionar funciones de control de acceso para LANs basadas en puertos (*port-based network access control*)

Entidades involucradas

Puerto == Canal lógico de comunicación que se mapea a una conexión física

Tipos de puertos

Puerto **NO** Controlado

Permite el intercambio de PDUs entre el Suplicante y el Autenticador independientemente del estado de autenticación del suplicante

Puerto Controlado

Permite el intercambio de PDUs entre el Suplicante y el Autenticador solo si el suplicante ha sido convenientemente autenticado

Protocolo IEEE 802.1X (2) Bloqueo de puertos

Las entidades (dispositivos) que usan el protocolo 802.1X disponen de **2 canales** de comunicación:

Canal de control ←→ Puerto NO controlado
Canal de datos ←→ Puerto controlado

▷ **ANTES** de que un suplicante este autenticado

El autenticador (AP) solo pasa mensajes de autenticación y control entre el suplicante y el AS por el canal de control (*puerto NO controlado*)

El canal (puerto) de datos está bloqueado

▷ **DESPUES** de que un suplicante este autenticado y las claves instaladas

El autenticador (AP) puede pasar mensajes de datos entre el suplicante y equipos de la red por el canal de datos (*puerto controlado*)

El canal (puerto) de datos está desbloqueado

Protocolo IEEE 802.1X (3) EAPOL Paquetes

Parte esencial de 802.1X es **EAPOL** == **EAP over LAN**

Define la encapsulación de EAP sobre una LAN (Ethernet, Wi-Fi, …)
Y algunas funciones y paquetes adicionales

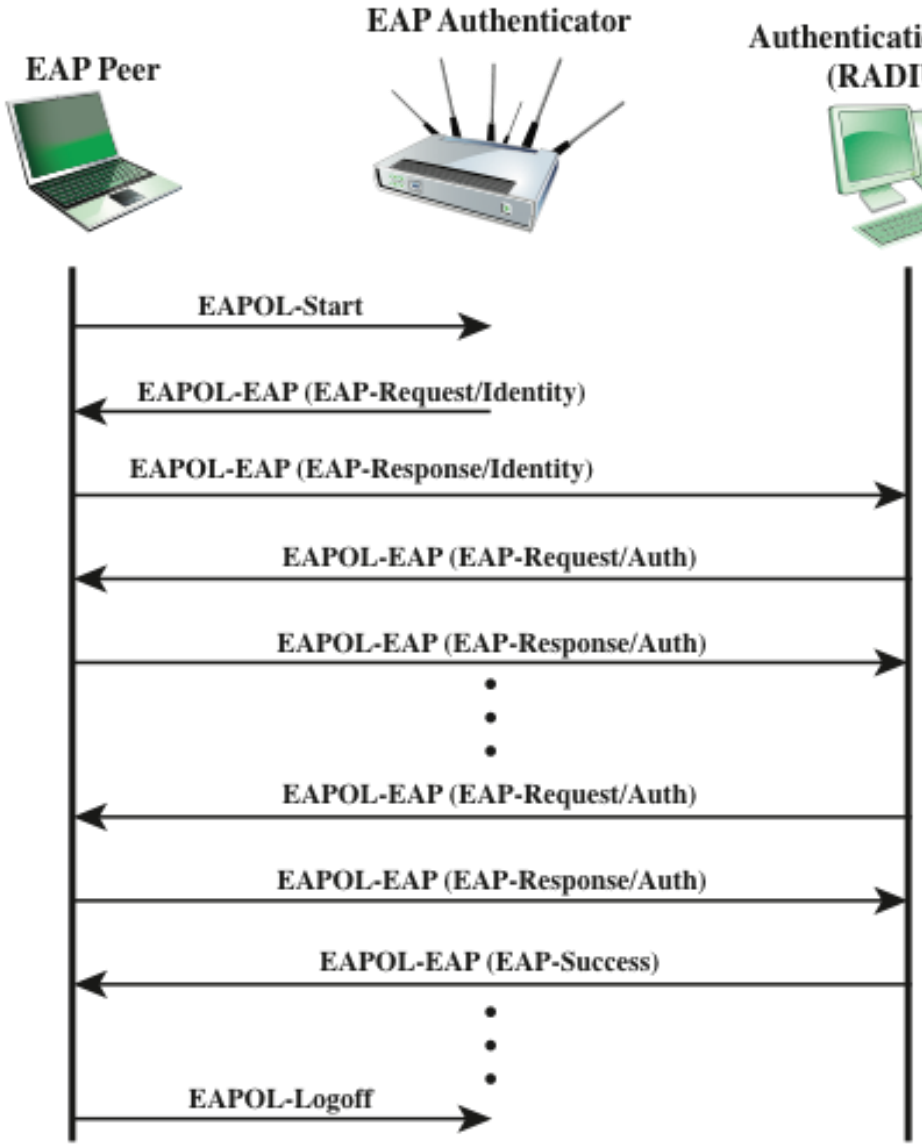
Paquetes EAPOL más comunes

EAPOL-EAP	Contiene un paquete EAP encapsulado
EAPOL-Start	Un suplicante puede enviar este paquete en vez de esperar por un desafío (*challenge*) de un autenticador
EAPOL-Logoff	Usado para devolver el estado del puerto a no autorizado cuando el suplicante termina de usar la red
EAPOL-Key	Usado para intercambiar claves criptográficas

Formato del paquete EAPOL

Versión del protocolo	Tipo de paquete	Longitud del cuerpo del paquete	Cuerpo del paquete

Protocolo IEEE 802.1X (4) EAPOL Intercambio Msgs



Stallings – Cryptography & Network Security

Al conectarse un suplicante a una LAN
NO conoce la MAC del autenticador
NO sabe si existe un autenticador

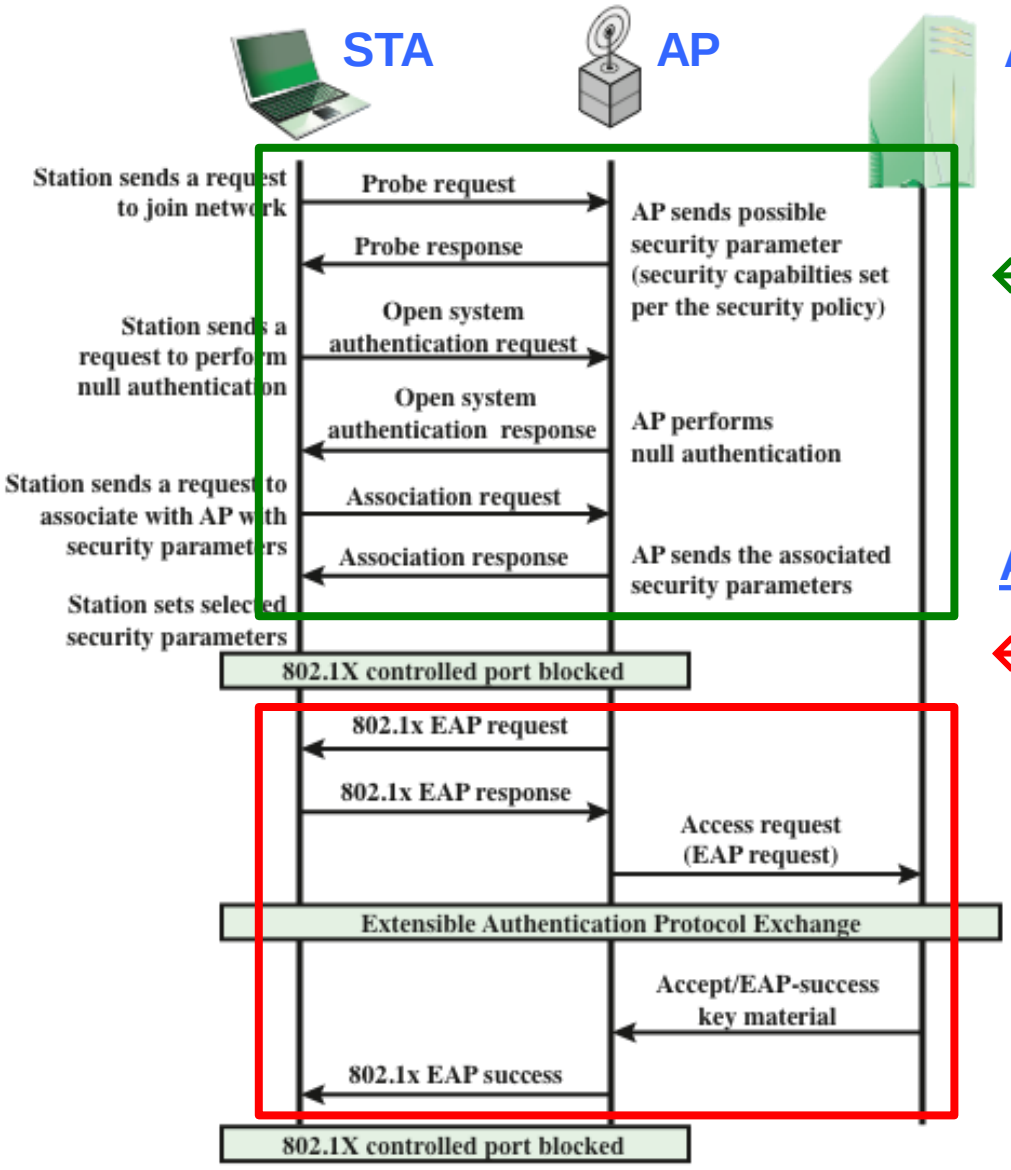
Envía EAPOL-Start a dir de Grupo Multicast reservada para autenticadores

El autenticador responde EAPOL Request/Identity
(Hay casos de envío inmediato)

El intercambio de Mensajes EAPOL
Es IGUAL que
El intercambio de Mensajes EAP

Para terminar, el suplicante envía EAPOL-Logoff que bloquea el puerto de datos del autenticador

Fase 2: Autenticación - Resumen



Stallings – Cryptography & Network Security

←Fase de descubrimiento ya realizada

Autenticación en modo Enterprise

←Arranca la fase de autenticación

STA → AP un EAPOL-Start (NO mostrado)

AP solicita identificación a STA

STA responde solicitando acceso al AS

EAP Exchange: Visto en diapositivas previas

Si la autenticación es satisfactoria …
AS envía la clave de sesión maestra a STA

MSK, Master Session Key
AAA, Authentication, Authorization & Accounting

Fase 3: Gestión de claves

En esta fase se generan claves y se distribuyen

Esta fase comienza si la fase previa de autenticación terminó satisfactoriamente

La STA, el AP y el AS disponen de la misma **PMK** (*Pairwise Master Key*)

Al comenzar esta fase el puerto controlado del AP está bloqueado para el tráfico general
Permanecerá bloqueado hasta que las claves temporales se instalen en la STA y el AP
Lo que sucede al terminar el "**4-Way Handshake**"

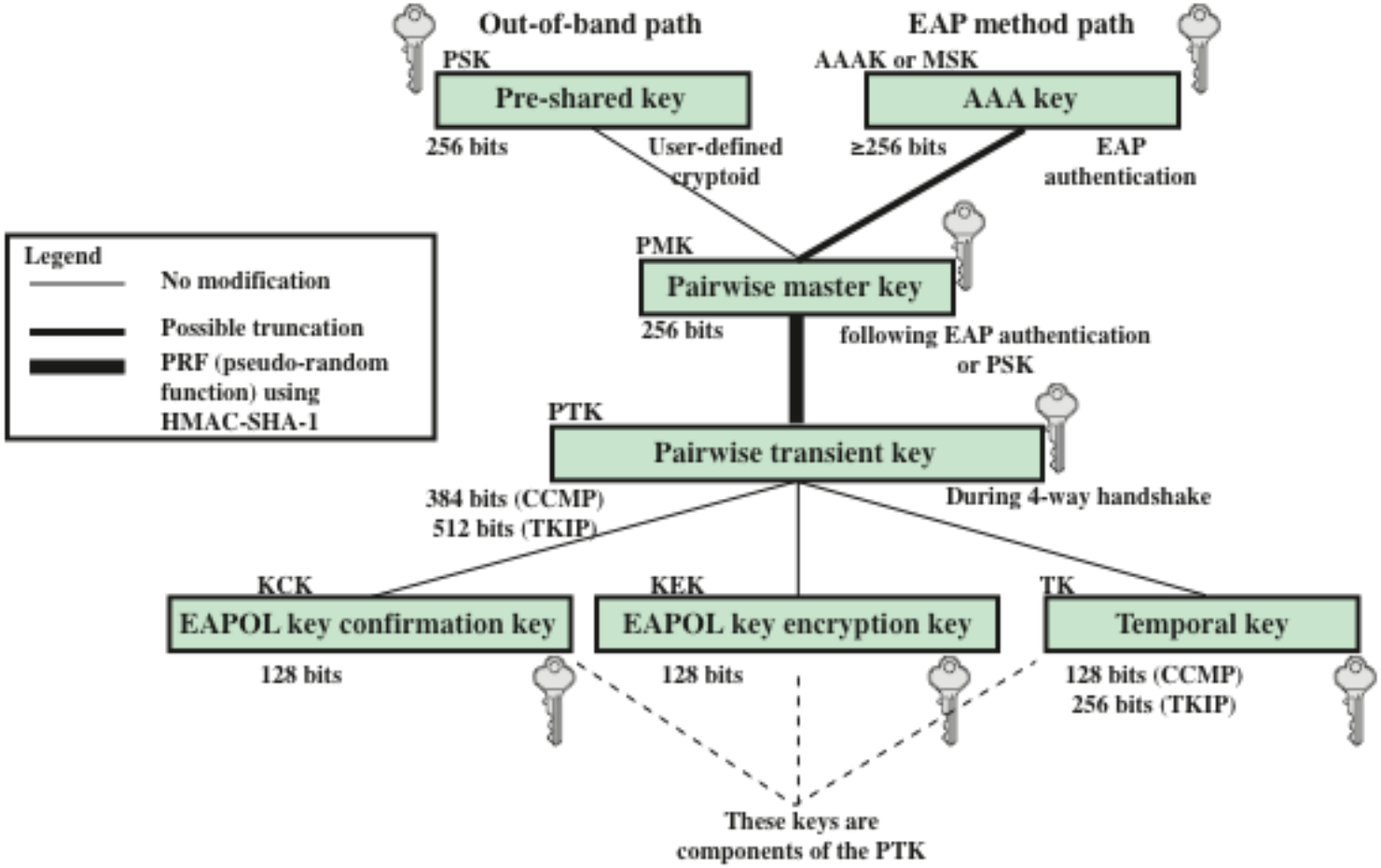
Hay 2 tipos de claves

Claves de parejas Usadas para la comunicación entre una STA y un AP
(*pairwise keys***)**

Claves de grupos Usadas para la comunicación multicast
(*group keys***)**

Fase 3: Claves de parejas

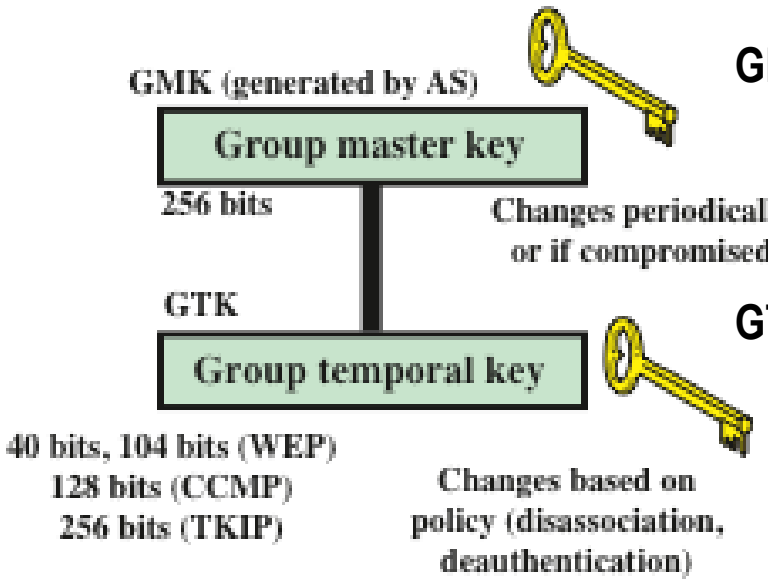
Las claves de parejas se utilizan en las comunicaciones entre una pareja de dispositivos, típicamente, una STA y un AP



Stallings – Cryptography & Network Security

Fase 3: Claves de grupos

Las claves de grupos se utilizan para las comunicaciones multicast: una STA envía MPDUs a múltiples STAs.



Stallings – Cryptography & Network Security

GMK se usa para generar la clave temporal del grupo

GTK se usa para proteger el tráfico multicast y broadcast

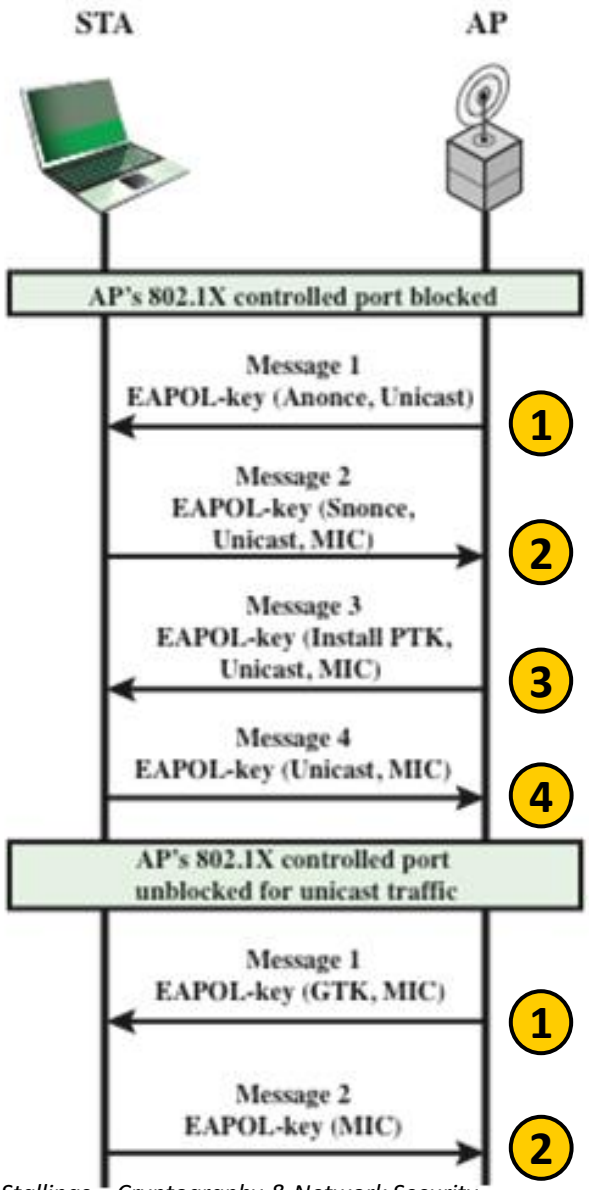
La genera sólo el AP y la transmite a las STAs asociadas

El estándar IEEE 802.11i requiere que la GTK generada sea **indistinguible** de un valor generado aleatoriamente

La GTK se **distribuye** a las STAs de forma segura usando las claves de parejas ya establecidas

La GTK se **cambia** cada vez que un dispositivo deja la red

Fase 3: Distribución de claves



Stallings – Cryptography & Network Security

En la distribución se usan nonces ≈ **n**umber **once**

nonce = arbitrary **n**umber that may only be used **once**

Distribución de claves de parejas (4-Way Handshake)

1. Msg con MAC-AP y Anonce
2. La STA genera la PTK = F(PMK, MAC-STA, MAC-AP, Snonce, Anonce)
   Envía Msg con MAC-STA y Snonce para que el AP genere la PTK
3. El AP genera la PTK
   Envía Msg con la misma información que el 1º incluyendo un MIC
4. Msg de acuse de recibo (*acknowledgement*) que incluye un MIC

Distribución de claves de grupos

1. El AP genera la GTK
   Envía la GTK cifrada con RC4 ó AES usando la clave KEK y un MIC
2. La STA notifica la recepción de la clave e incluye un MIC

Fase 4: Transferencia de datos protegida (1)

IEEE 802.11 especifica 2 técnicas para proteger los datos transmitidos:

- **TKIP** = **T**emporal **K**ey **I**ntegrity **P**rotocol
- **CCMP** = **C**ounter Mode-**C**BC **M**AC **P**rotocol

TKIP

Diseñado para mejorar la seguridad de dispositivos antiguos que usan WEP
Solo requiere cambios (mejoras) en WEP que se aplican usando software exclusivamente

Integridad: Se añade un MIC a los datos de cada MPDU calculado con alg. Michael

Confidencialidad: Se cifra la MPDU y el MIC usando RC4

CCMP

Diseñado para dispositivos nuevos cuyo hardware soporta directamente CCMP

Integridad: Utiliza el alg. CBC-MAC: **C**ipher **B**lock **C**haining – **M**essage **A**uthentication **C**ode

Calcula un MAC aplicando AES a cada bloque de información
Encadenando los cifradores con el modo CBC

Confidencialidad: Utiliza el alg. AES para cifrar la información
Encadenando los cifradores con el modo CTR

Fase 4: Transferencia de datos protegida (2)

La tecnología CCM ha sido estandarizada …

NIST SP 800-38C Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality July 2007

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf

IETF RFC 3610 Counter with CBC-MAC (CCM) Sept 2003

https://datatracker.ietf.org/doc/pdf/rfc3610

GCMP **G**alois/**C**ounter **M**ode – Utilización en WAP3

Diseñado para ser paralelizable lo que permite un elevado flujo con baja latencia

Integridad: Utiliza el alg. GHASH

Confidencialidad: Utiliza el alg. GCTR

La tecnología GCM ha sido estandarizada …

NIST SP 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC Nov 2007

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf