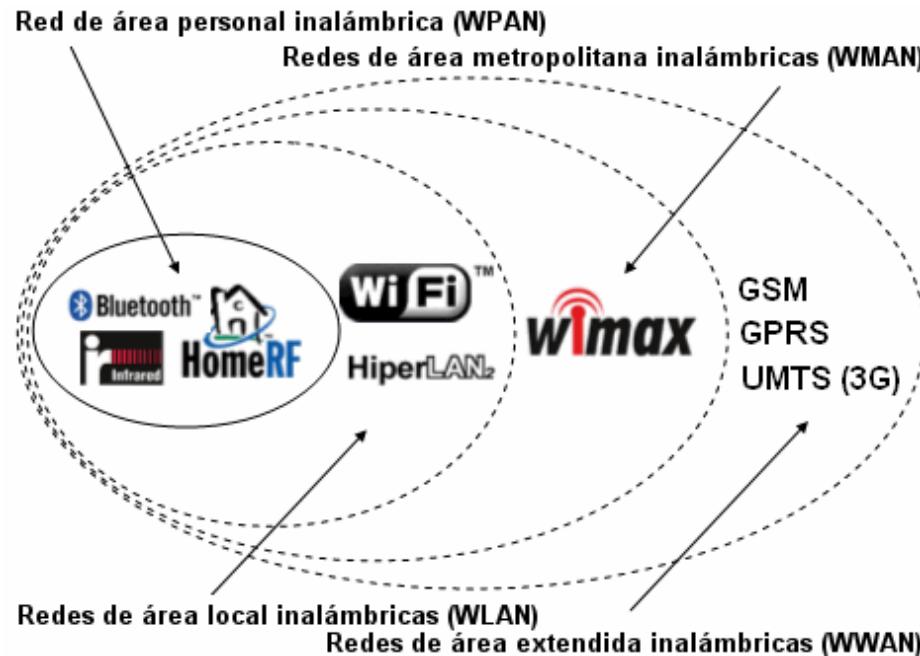


Redes LAN Inalámbricas

Tema 2

Contenido

Redes de Área Personal Inalámbricas (WPAN)
Redes de Área Local Inalámbricas (WLAN)



Redes LAN Inalámbricas (WLAN)

IEEE 802.11

- 0 IEEE: Institute of Electrical and Electronics Engineers
- 0 Organizado en comités y grupos de trabajos
 - 0 802 comité: Normas relacionadas con redes
 - 0 .11 grupo de trabajo: Wireless LAN
- 0 Cubre los niveles físicos y de enlace de datos
- 0 Principales problemas
 - 0 Interferencias
 - 0 Seguridad
 - 0 Cifrado de los datos
 - 0 Autenticación de los usuarios de la red

802.11

0 Un solo estándar: 802.11

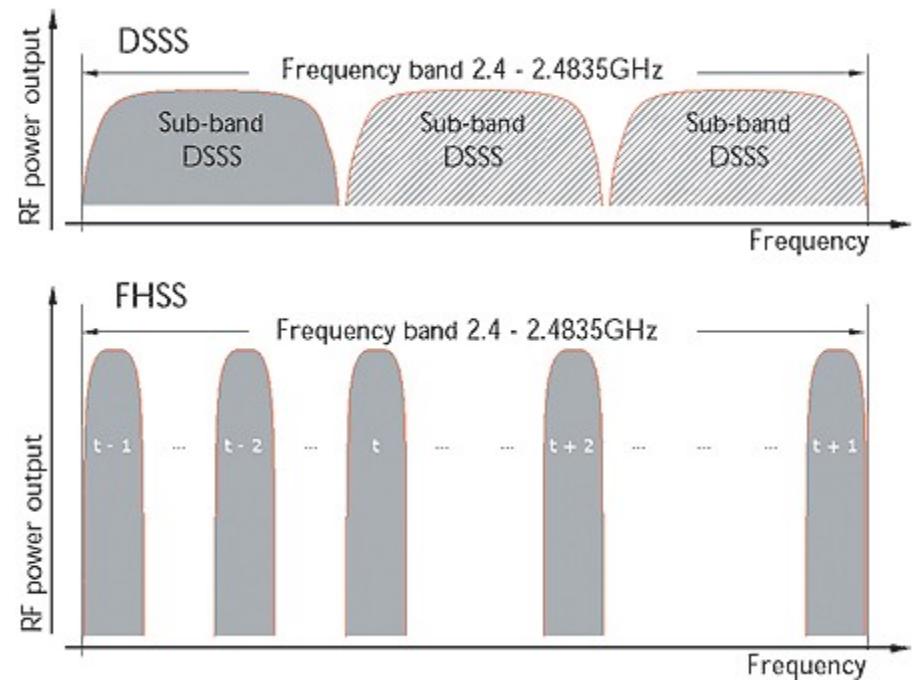
- 0 El resto son modalidades (“amendments”), la mayoría retrocompatibles
- 0 802.11F y 802.11T prácticas recomendadas
- 0 Las principales modalidades son
 - 0 802.11a/b/g/n/ac/ad/ah
 - 0 802.11e/i/w

802.11

- 0 Estándar publicado en 1997
- 0 Tasas: 1-2Mbits por segundo
- 0 Medio compartido de broadcast
- 0 Half-duplex, TDD (Time-Division Duplexing, TDD)
- 0 CSMA/CA como protocolo de control de acceso
(prevención de colisiones)

802.11 (estándar original)

- 0 Define tres clases de tecnologías para la capa física:
 - 0 Portadoras RF moduladas en espectro ensanchada por salto de frecuencia (FHSS)
 - 0 Portadoras RF moduladas en espectro ensanchando por secuencia directa (DSSS)
 - 0 Transmision por infrarrojos



802.11

- 0 Las dos primeras técnicas para la capa física operan en la banda de 2,4 GHz atribuida a servicios y aplicaciones ISM (Industrial, Scientific, Medical)
 - 0 902-928 MHz, 2'400-2'4835 GHz y 5'725-5'850 GHz
 - 0 Banda de uso común
 - 0 No requiere licencia



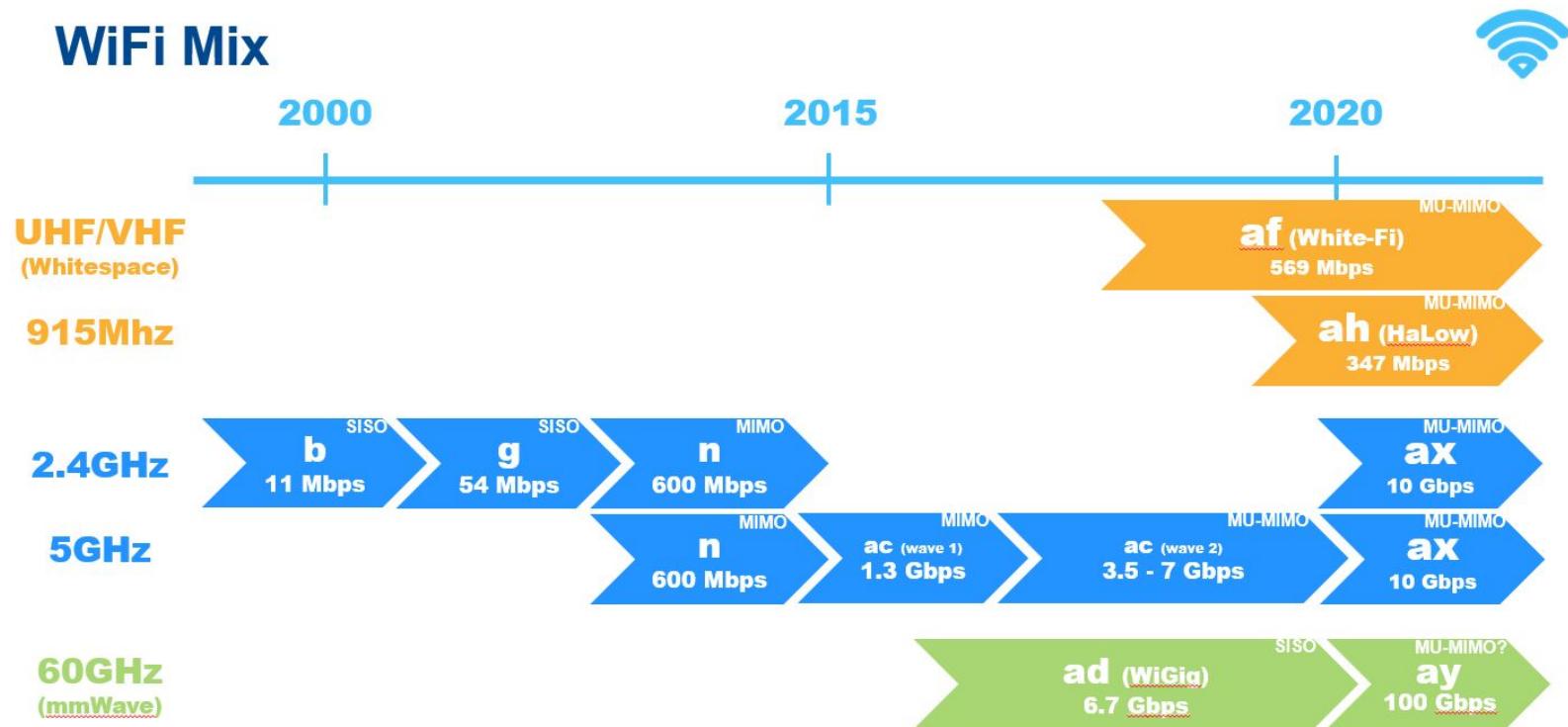
Wi-Fi

- ① Wi-Fi es una marca registrada por la Wi-Fi Alliance para productos certificados basados en el estándar IEEE 802.11
- ① Wi-Fi Alliance (anteriormente conocida como WECA – Wireless Ethernet Compatibility Alliance)
 - ① Asegurar la compatibilidad de equipos a través de la certificación bajo la marca Wi-Fi

Evolución



Evolución



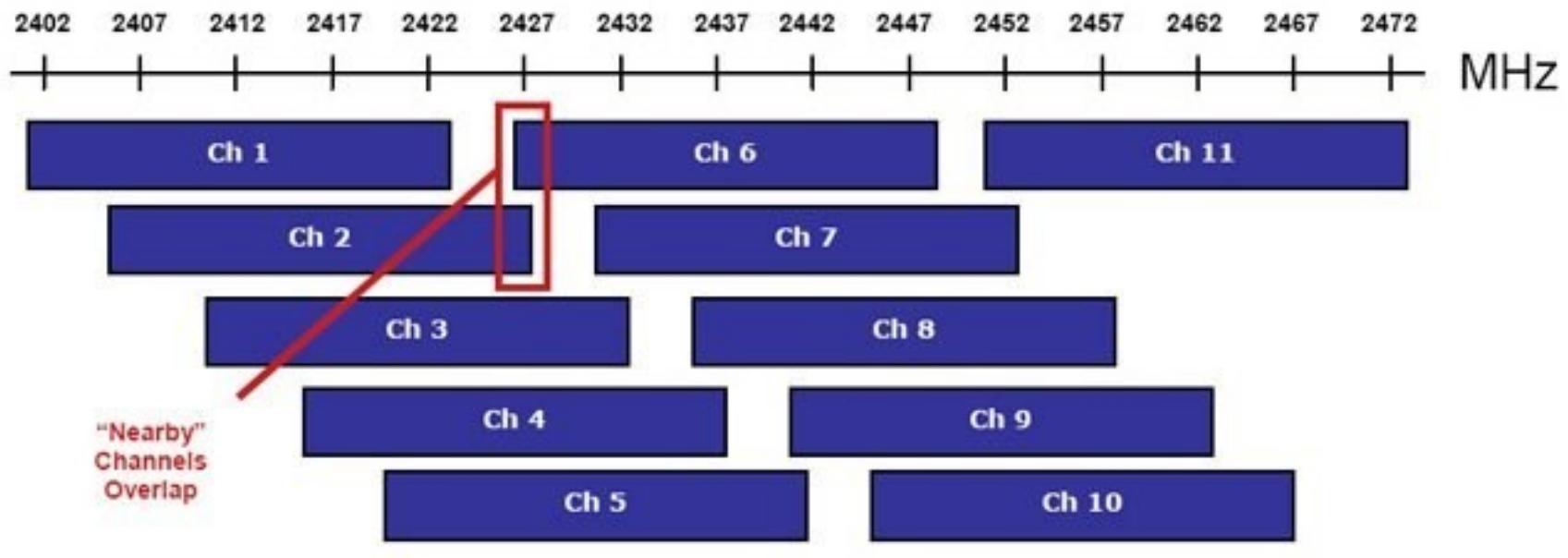
JAYCOR

802.11b

- 0 Publicada en 1999. Nueva tasa de hasta 11Mbps
- 0 DSSS (espectro ensanchando por secuencia directa)
- 0 El espectro se divide en 14 canales solapados
 - 0 Canales de 22MHz
 - 0 Separación de 5 MHz entre canales

Canal	Fracuencia	Canal	Fracuencia
1	2412 MHz	8	2447 MHz
2	2417 MHz	9	2452 MHz
3	2422 MHz	10	2457 MHz
4	2427 MHz	11	2462 MHz
5	2432 MHz	12	2467 MHz
6	2437 MHz	13	2472 MHz
7	2442 MHz	14	2484 MHz

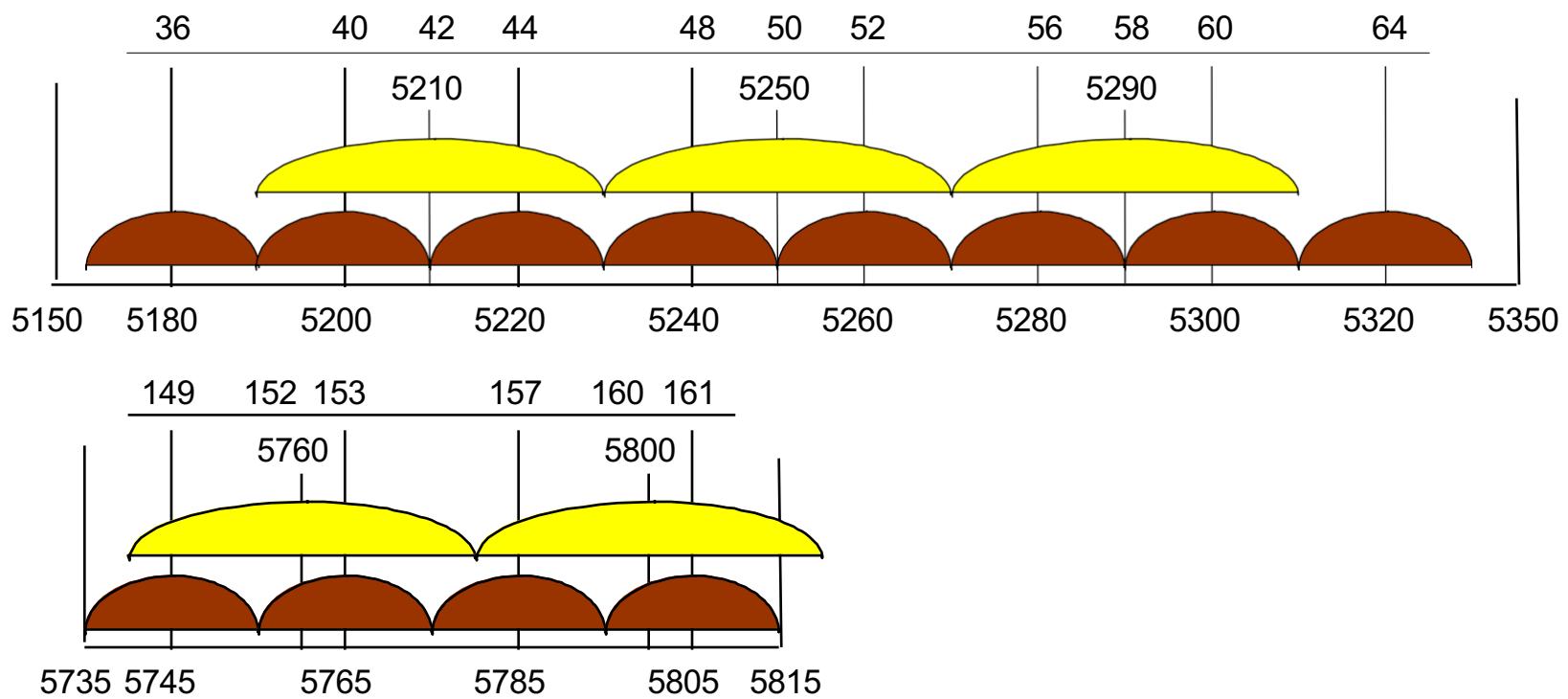
802.11b



802.11a

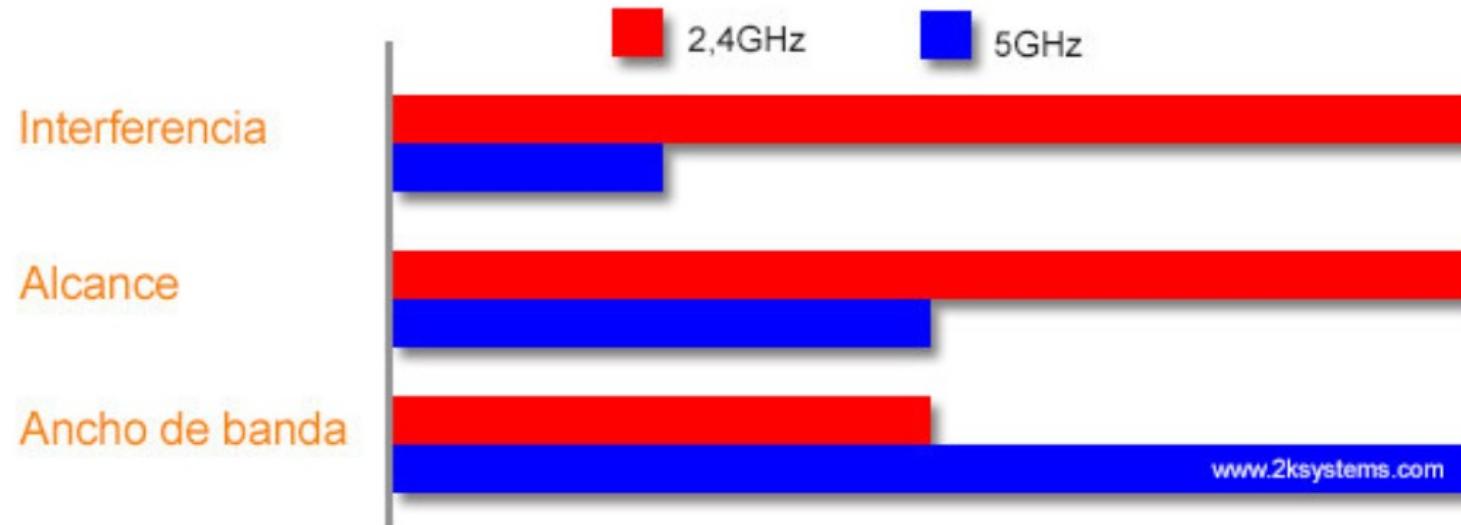
- 0 Publicada en 1999 después de 802.11b
- 0 Banda 5GHz
 - 0 5180-5320Mhz (36-64)
 - 0 5500-5700Mhz (100-140)
 - 0 5745-5825Mhz (149-165)
- 0 OFDM (Multiplexación por División de Frecuencias Ortogonales) -> Tasa máxima: 54Mbps
- 0 Podemos encontrar hasta un total de 23 de canales de 20MHz **libres de solapamiento**
- 0 Más cara (mayor consumo y requiere la instalación de infraestructuras diferentes) -> menos masificada

802.11a

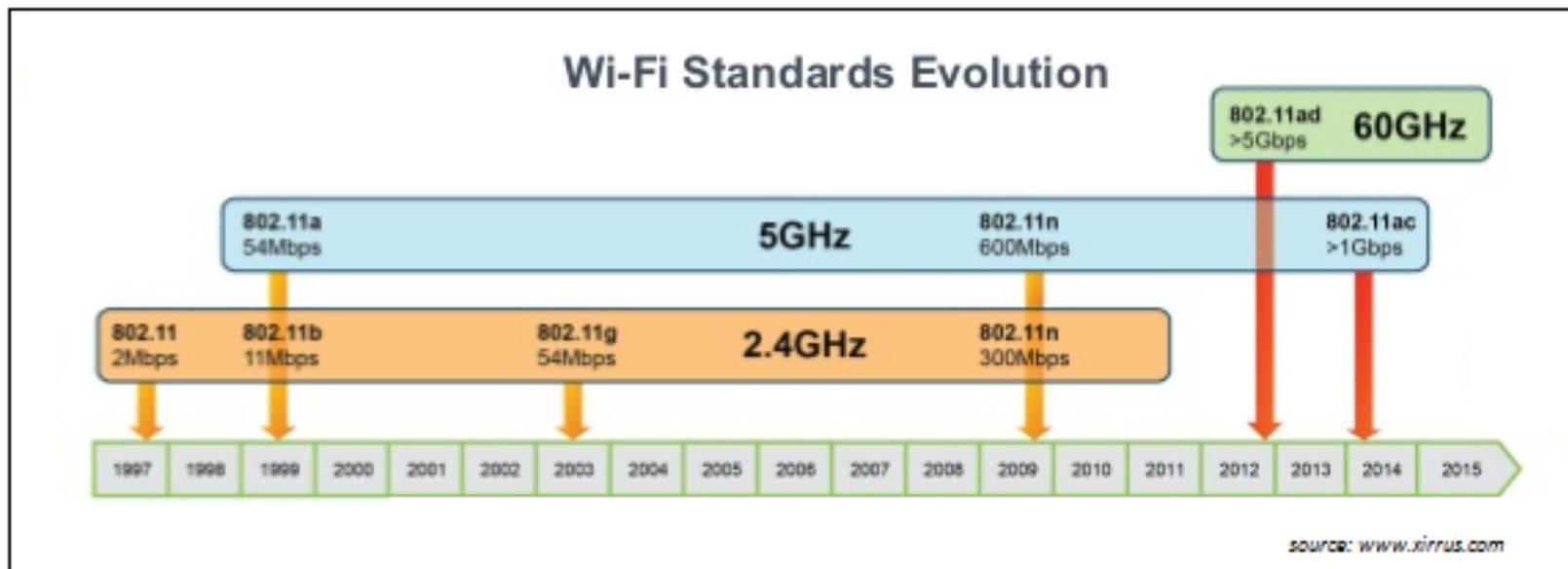


Comparativa bandas

Comparativa de 2,4Ghz y 5GHz



Comparativa bandas



802.11h

- 0 Introduce un mecanismo de control de potencia para resolver problemas de interferencia con otros sistemas en la banda de 5 GHz (publicado en 2003)
 - 0 DFS (Dynamic Frequency Selection) -> Cambia de canal en caso de interferencia con otros sistemas
- 0 Introduce un mecanismos que permite negociar la potencia transmitida
 - 0 TPC (Transmit Power Control)

802.11g

- 0 Estándar publicado en 2003
- 0 Muy similar 802.11a pero opera en la banda de 2.4GHz
- 0 Uso de la tecnología OFDM
- 0 Se le considera la evolución natural de 802.11b
- 0 Compatible con 802.11b (equipos y puntos de acceso)
- 0 Tasas de 54 Mbps

802.11n

- 0 Modalidad iniciada en 2004 y finalizada en 2009
- 0 Hasta 4 spatial streams
- 0 Tecnología MIMO
 - 0 Transmisión mejorada (Legacy beam forming)
 - 0 Recepción mejorada (Maximal Ratio Combining – MRC)
- 0 2.4GHz y 5GHz
- 0 Canales de 40MHz
- 0 Tasas de 300 Mbps (2.4GHz) y 600Mbps (5GHz)

802.11n

0 MIMO



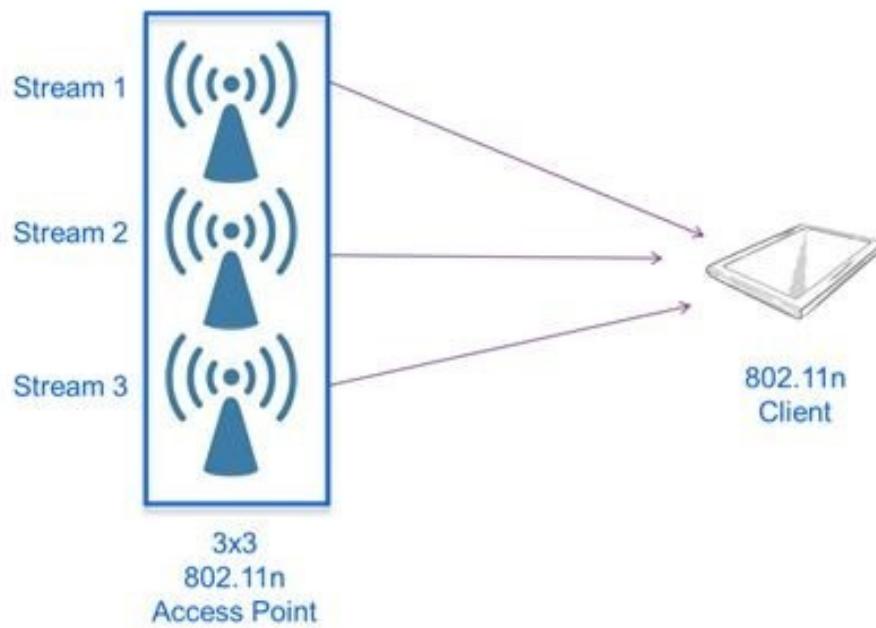
802.11ac – Very High Throughput

- 0 5GHz
- 0 Multi user MIMO
- 0 256-QAM (vs 64-QAM in 802.11n) - Modulación de amplitud en cuadratura
- 0 4 spatial streams
- 0 Canales de 80/160MHz
- 0 Hasta 2.34Gbit/s

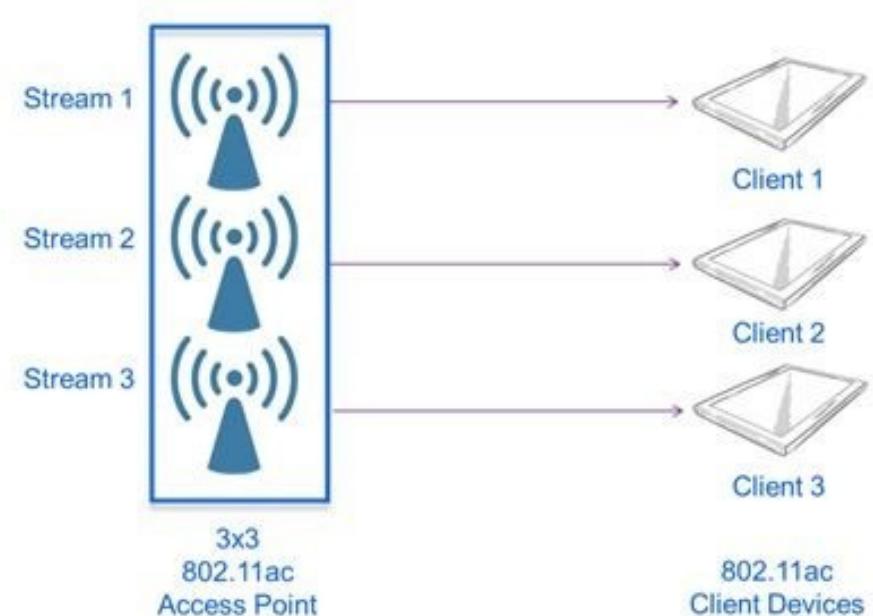
802.11ac



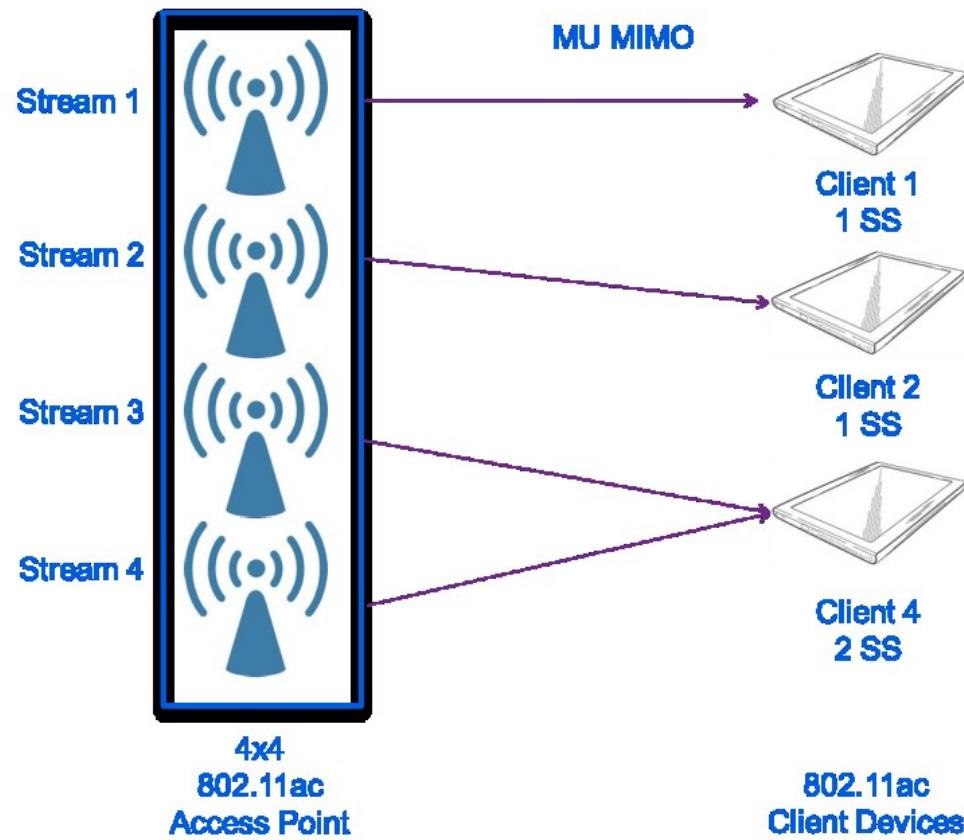
SU MIMO



MU MIMO



802.11ac



802.11ad



- 0 Publicado por WiGig (Wireless Gigabit Alliance)
 - 0 Aplicaciones y dispositivos de audio/vídeo
- 0 Bandas 2.4, 5 y 60GHz (Unlicensed)
 - 0 USA/Canada/Korea:57-64GHz
 - 0 Europe: 57-66GHz
 - 0 China: 59-64GHz and 45-50GHz
 - 0 Japan: 59-66GHz
- 0 Tasas
 - 0 Entre 385 y 6785 Mbits (equiparable a 802.11ac)
 - 0 OFDM, Single Carrier y Low Power SC

802.11ad channels

Channel	Center [GHz]	Low [GHz]	Up [GHz]
1	58.32	57.24	59.4
2	60.48	59.4	61.56
3	62.64	61.56	63.72
4	64.8	63.72	65.88

0 Cada canal dispone de un ancho de banda de 2.16GHz

Otras bandas de frecuencia

- 0 802.11ah: IoT, 900MHz
- 0 802.11y: licenciada, 3.6GHz (3655–3695 MHz)
- 0 802.11p: Vehículos (WAVE), 5.9GHz

Tipos de redes

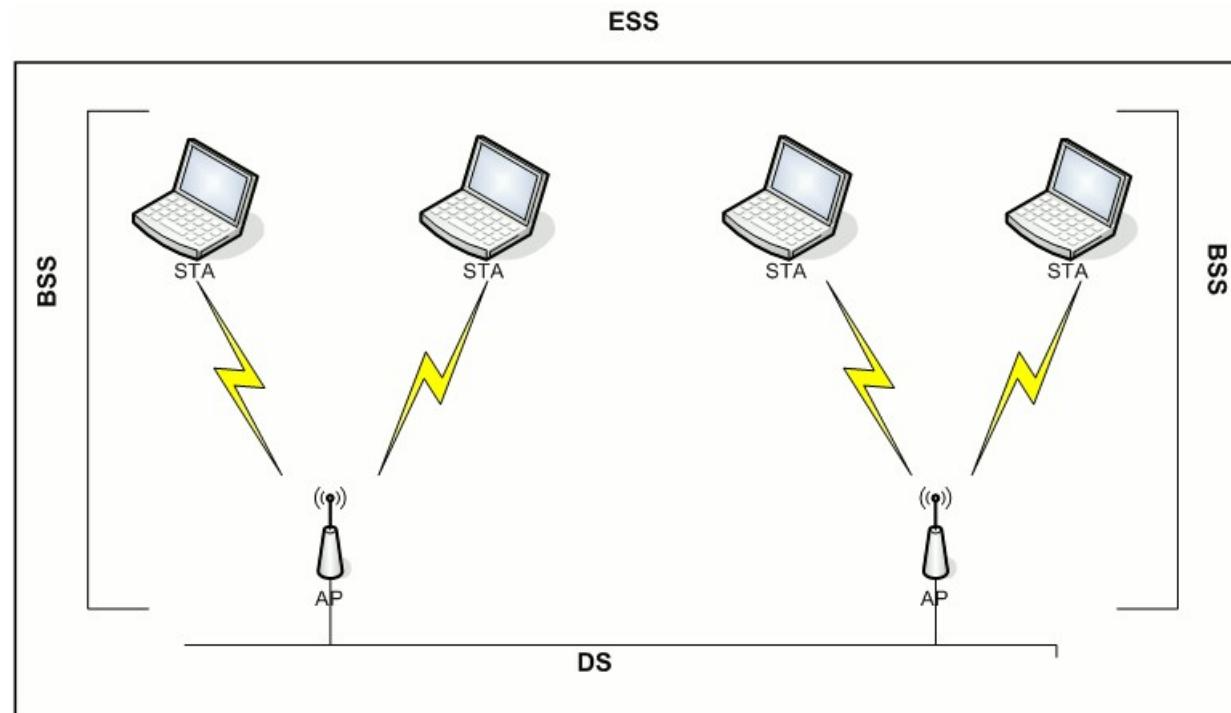
- 0 3 tipos de redes
 - 0 Infrastructure
 - 0 Ad-Hoc
 - 0 WDS (Wireless Distribution System)

Infrastructure

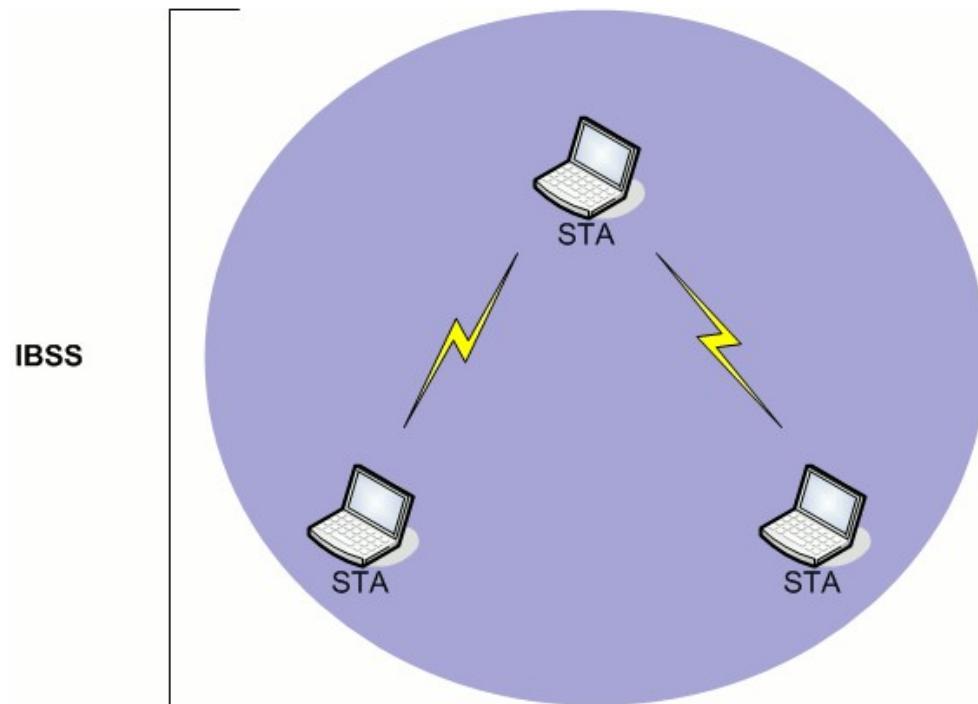
BSS: Basic Service Set

ESS: Extended Service Set

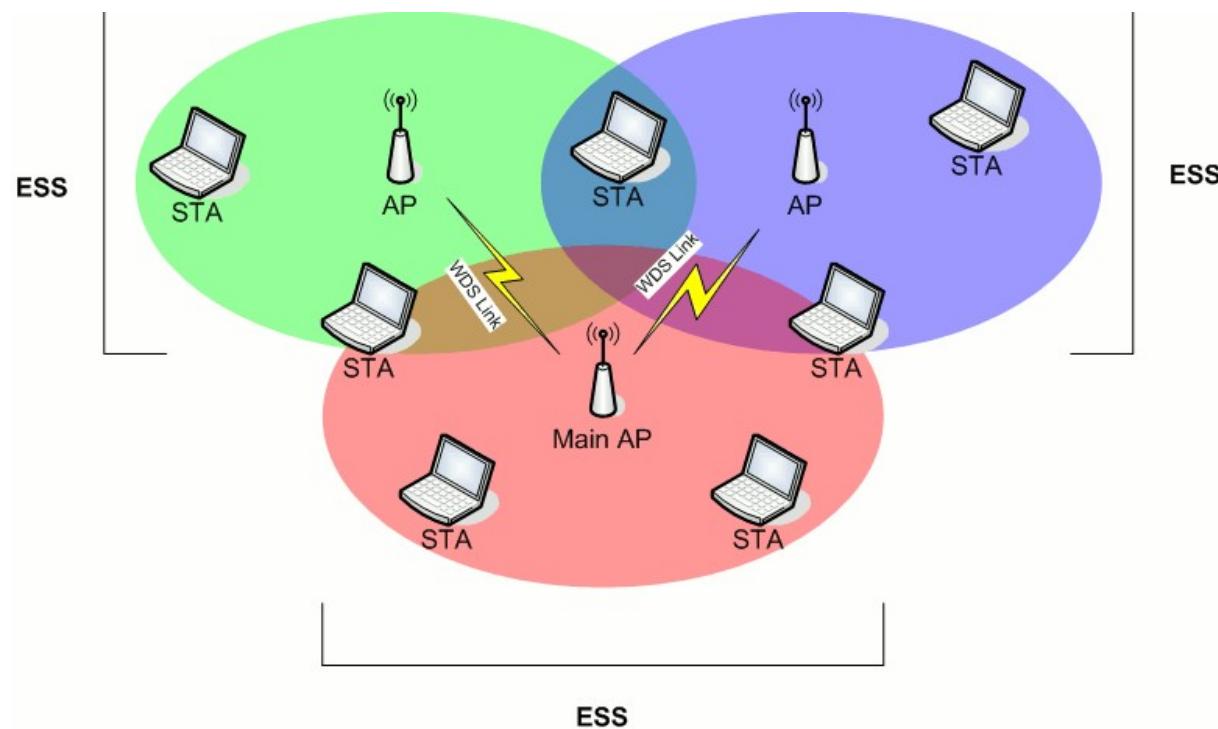
DS: Distribution system



Ad-Hoc (independent BSS)



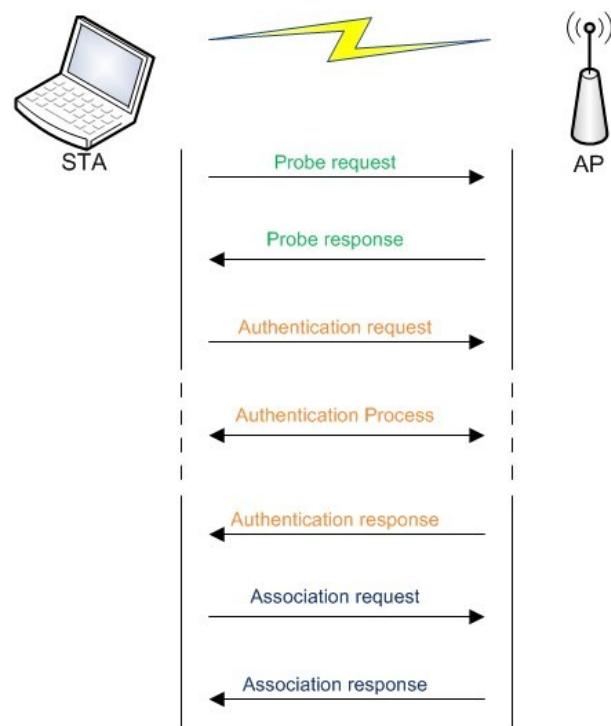
WDS (Wireless Distribution System)



SSID

- 0 El SSID (Service Set Identifier) es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red.
- 0 El código consiste en un máximo de 32 caracteres
 - 0 La mayoría de las veces son alfanuméricos
 - 0 Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.
- 0 SSID en redes ad-hoc → BSSID (Basic Service Set Identifier).
- 0 SSID en redes con infraestructura → ESSID (Extended Service Set Identifier)
- 0 A menudo al SSID se le conoce como “nombre de la red”.

Interacción con la red



WEP

- 0 Wired Equivalent Privacy
- 0 Parte del estándar 802.11
- 0 Las tramas están cifradas con el algoritmo RC4
 - 0 Algoritmos de cifrado de clave secreta
 - 0 Genera una serie pseudo-aleatoria a partir de la clave secreta.
 - 0 El mensaje se cifra con una clave de la misma longitud que el mensaje pero que depende de la clave original
- 0 Se le añade un CRC32 para proteger la integridad

WPA

- 0 IEEE creó el grupo de trabajo 802.11i cuando las vulnerabilidades de WEP fueron descubiertas
- 0 Autenticación basada en 802.1x
- 0 Se introducen dos nuevos protocolos de cifrado
 - 0 TKIP (Temporal Key Integrity Protocol) : basado en RC4
 - 0 CCMP (Counter with CBC-MAC Mode Protocol): completamente nuevo, basado en AES (Advanced Encryption Standard)
- 0 Dos versiones
 - 0 Personal: autenticación PSK
 - 0 Enterprise: autenticación con Radius server

WPA

0 WPA 1

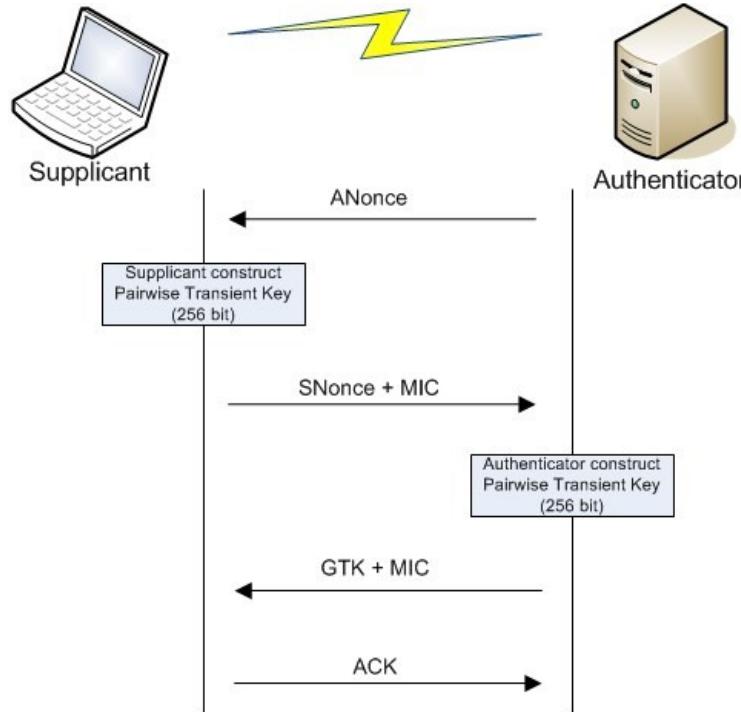
- 0 Basado en el 3er borrador de 802.11i
- 0 Usa TKIP
- 0 Compatibilidad hacia atrás

0 WPA 2

- 0 Basado en la version final de la 802.11i
- 0 Usa CCMP (AES)
- 0 Rompe la compatibilidad con hardware antiguo
- 0 Nuevas vulnerabilidades encontradas en 2017 -> WPA3 en marcha

Autenticación PSK

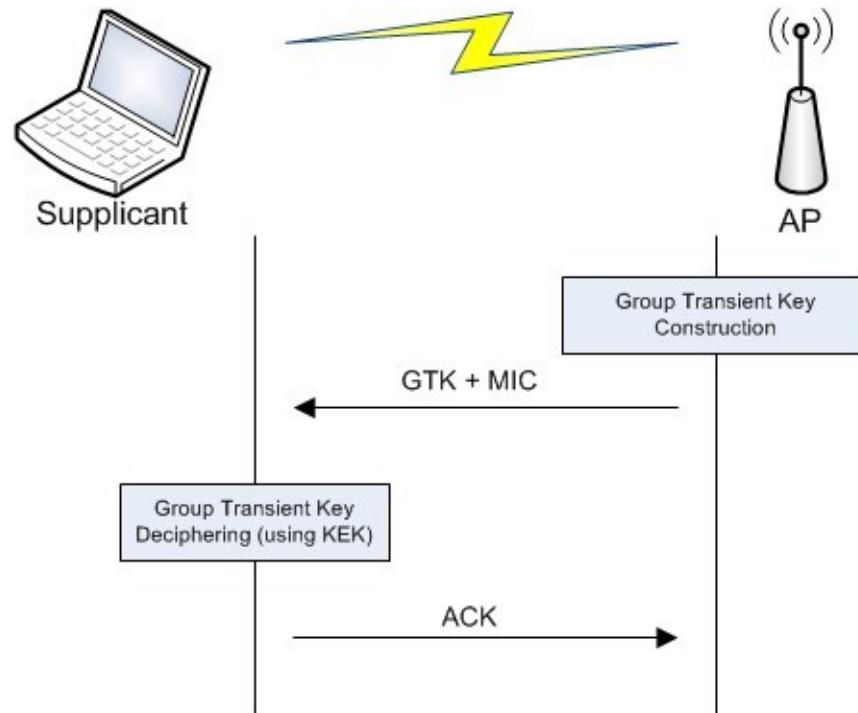
PSK: Pre-Shared Key



- 0 Clave compartida previamente
- 0 Se introduce la contraseña en la estación para acceder a la red
- 0 Clave para iniciar autenticación, no para el cifrado
- 0 Usuarios domésticos

WPA – GTK basado en 802.1x

GTK: Group Temporal Key



- 0 Uso empresarial
- 0 Requiere servidor RADIUS

WPS

0 WiFi Protected Setup

0 Permite el intercambio seguro y sencillo en WPA PSK
Introducido en 2007 por WiFi Alliance

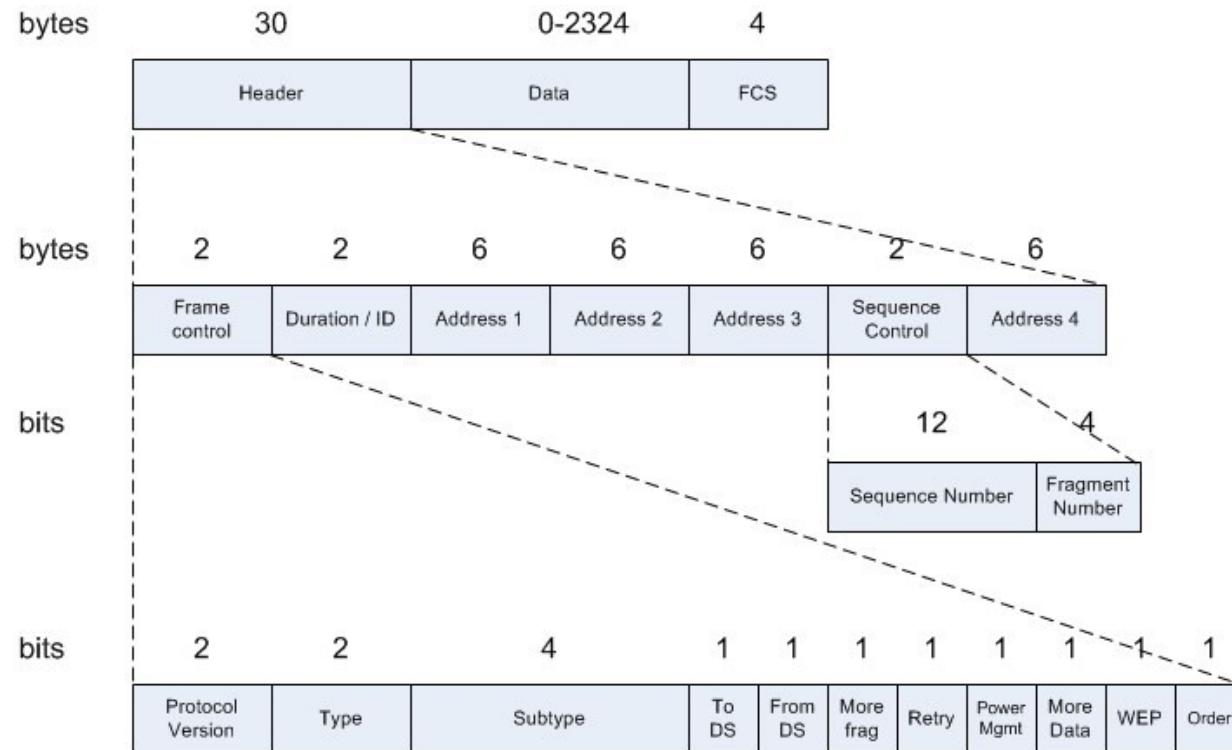
0 Unificación de diferentes vendedores

0 Métodos:

0 PIN

0 Push Button

Estructura de trama genérica 802.11



Campos ToDS/FromDS

DS: Distribution System

ToDS	FromDS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	
0	1	DA	BSSID	SA	
1	0	BSSID	SA	DA	
1	1	RA	TA	DA	SA

0 DA: Destination Address

0 RA: Recipient Address

0 SA: Source Address

0 TA: Transmitter Address

0 BSSID: Basic Service Set Identifier – MAC of the Access Point

Tipos de tramas 802.11

0 Tramas de gestión

0 Tramas de control

0 Tramas de datos

Tramas de gestión

Type	Subtype	Meaning
0	0	Association Request
0	1	Association Response
0	2	Reassociation Request
0	3	Reassocation Response
0	4	Probe Request
0	5	Probe Response
0	6	Measurement Pilot
0	7	Reserved

Tramas de gestión(2)

Type	Subtype	Meaning
0	8	Beacon
0	9	ATIM
0	10	Disassociation
0	11	Authentication
0	12	Deauthentication
0	13	Action
0	14	Action No ACK
0	15	Reserved

Tramas de gestión (3)

0 Tramas beacon

- 0 Los puntos de acceso mandan constantemente tramas en las que anuncian su presencia para que los clientes puedan detectarlos y conectarse
- 0 El punto de acceso manda normalmente el SSID de la red en las traman beacon

Tramas de control

Type	Subtype	Meaning
1	0-6	Reserved
1	7	Control Wrapper
1	8	Block ACK request
1	9	Block ACK
1	10	PS Poll
1	11	RTS
1	12	CTS
1	13	ACK
1	14	CF End
1	15	CF End + CF ACK

Tramas de datos

Type	Subtype	Meaning
2	0	Data
2	1	Data + CF ACK
2	2	Data + CF Poll
2	3	Data + CF ACK + CF Poll
2	4	Null Function (no data)
2	5	CF ACK (no data)
2	6	CF Poll (no data)
2	7	CF ACK + CF Poll (no data)

Tramas de datos (2)

Type	Subtype	Meaning
2	8	QoS data
2	9	QoS data + CF ACK
2	10	QoS data + CF Poll
2	11	QoS data + CF ACK + CF Poll
2	12	QoS Null (no data)
2	13	Reserved
2	14	QoS CF Poll (no data)
2	15	QoS CF ACK (no data)

Wireshark & WiFi

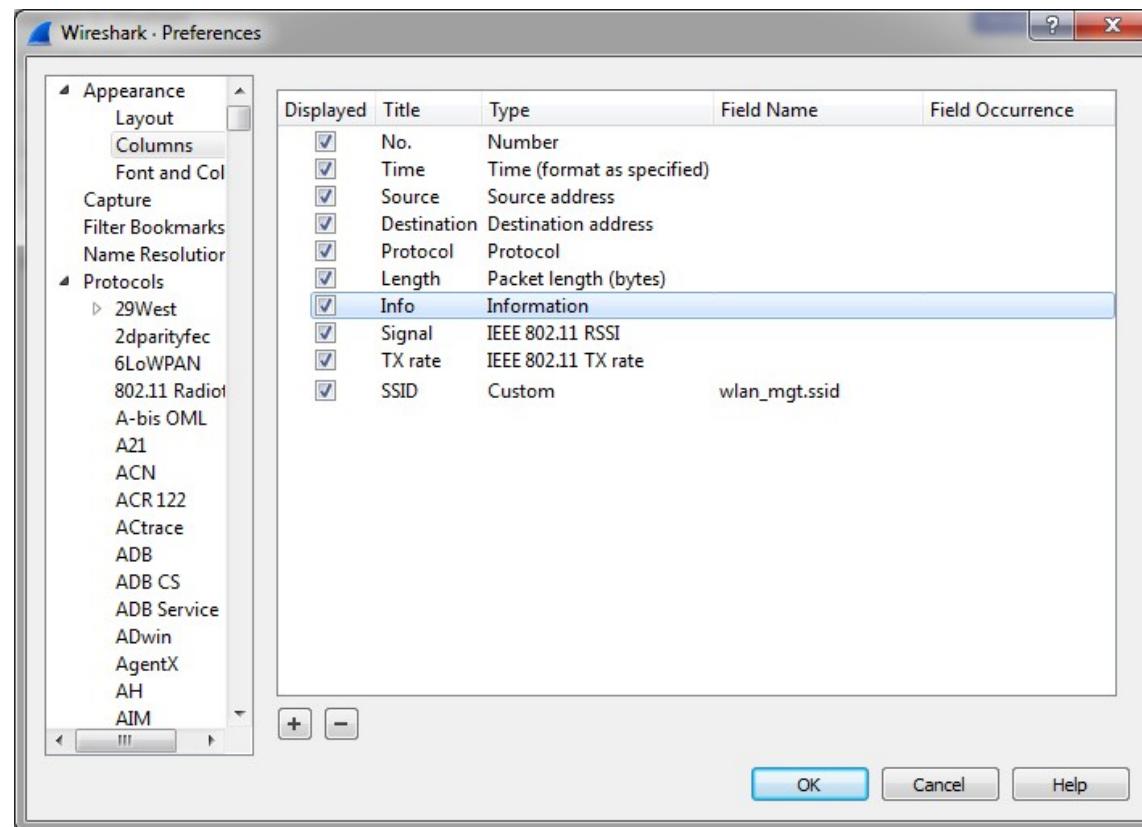
Wireshark & WiFi

- 0 Options
 - 0 Columns
 - 0 Protocols
 - 0 Decrypt traffic
 - 0 Wireless toolbar

- 0 Capture headers

- 0 Filter
 - 0 Display
 - 0 BPF (Berkeley Packet Filter)

Nuevas columnas



Nuevas columnas

AirPcap USB wireless capture adapter nr. 00 [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

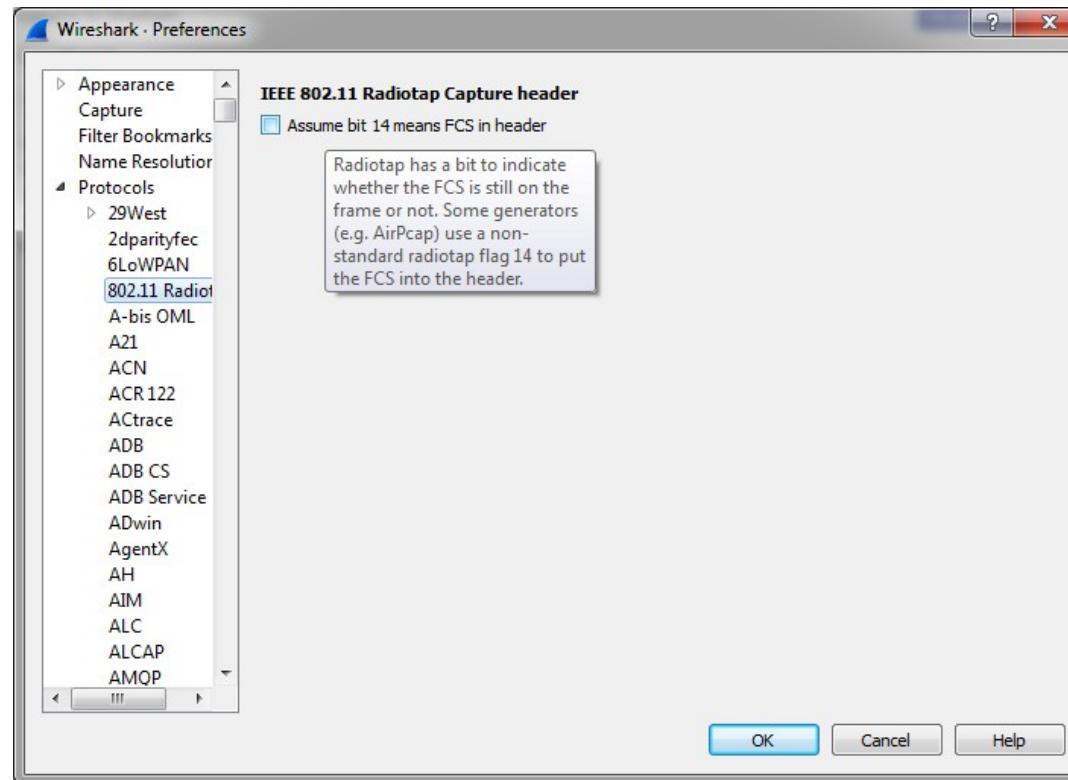
802.11 Channel: 2437 [BG 6] Channel Offset: 0 FCS Filter: Valid Frames Driver Wireless Settings... Decryption Keys...

No.	Time	Source	Destination	Protocol	Length	Info	Signal	TX rate	SSID
4	0.05%	LgElectr_8a:f4:59	LgElectr_8a:f4:59	(802.11)	40	Clear-to-send, Flags=.....C	10 dB	24.0	
5	0.114	LgElectr_8a:f4:59	Broadcast	(802.11)	228	Beacon frame, SN=1908, FN=0, Flags=.....C, BI=100, SSID=personal	8 dB	1.0	personal
6	0.134	Ruckuswi_13:6e:68	Broadcast	(802.11)	162	Beacon frame, SN=1702, FN=0, Flags=.....C, BI=100, SSID=Wild Palms Hotel	18 dB	2.0	Wild Palms Hotel
7	0.186	Ruckuswi_33:57:38	Broadcast	(802.11)	162	Beacon frame, SN=3935, FN=0, Flags=.....C, BI=100, SSID=Wild Palms Hotel	20 dB	2.0	Wild Palms Hotel
8	0.205	Ruckuswi_14:fd:68	Broadcast	(802.11)	162	Beacon frame, SN=2563, FN=0, Flags=.....C, BI=100, SSID=Wild Palms Hotel	29 dB	2.0	Wild Palms Hotel
9	0.288	Ruckuswi_33:57:38	Broadcast	(802.11)	162	Beacon frame, SN=3936, FN=0, Flags=.....C, BI=100, SSID=Wild Palms Hotel	33 dB	2.0	Wild Palms Hotel
10	0.307	Ruckuswi_14:fd:68	Broadcast	(802.11)	162	Beacon frame, SN=2564, FN=0, Flags=.....C, BI=100, SSID=Wild Palms Hotel	15 dB	2.0	Wild Palms Hotel
11	0.319	LgElectr_8a:f4:59	Broadcast	(802.11)	228	Beacon frame, SN=1910, FN=0, Flags=.....C, BI=100, SSID=personal	9 dB	1.0	personal
12	0.339	Ruckuswi_13:6e:68	Broadcast	(802.11)	162	Beacon frame, SN=1704, FN=0, Flags=.....C, BI=100, SSID=Wild Palms Hotel	12 dB	2.0	Wild Palms Hotel
13	0.375	SamsungE_38:fb:be	(802.11)	40	Acknowledgement, Flags=.....C	13 dB	1.0		
14	0.391	Ruckuswi_33:57:38	Broadcast	(802.11)	162	Beacon frame, SN=3937, FN=0, Flags=.....C, BI=100, SSID=Wild Palms Hotel	21 dB	2.0	Wild Palms Hotel
15	0.409	Ruckuswi_14:fd:68	Broadcast	(802.11)	162	Beacon frame, SN=2565, FN=0, Flags=.....C, BI=100, SSID=Wild Palms Hotel	30 dB	2.0	Wild Palms Hotel
16	0.414	LgElectr_8a:f4:59	(802.11)	40	Clear-to-send, Flags=.....C	11 dB	24.0		
17	0.414	Intelcor_98:18:77	LgElectr_8a:f4:59	(802.11)	58	802.11 Block Ack, Flags=.....C	10 dB	24.0	
18	0.421	LgElectr_8a:f4:59	Broadcast	(802.11)	228	Beacon frame, SN=1911, FN=0, Flags=.....C, BI=100, SSID=personal	7 dB	1.0	personal
19	0.422	LgElectr_8a:f4:59	(802.11)	40	Clear-to-send, Flags=.....C	10 dB	24.0		
20	0.422	Intelcor_98:18:77	LgElectr_8a:f4:59	(802.11)	58	802.11 Block Ack, Flags=.....C	9 dB	24.0	
21	0.423	Intelcor_98:18:77	LgElectr_8a:f4:59	(802.11)	58	802.11 Block Ack, Flags=.....C	10 dB	24.0	
22	0.441	Ruckuswi_13:6e:68	Broadcast	(802.11)	162	Beacon frame, SN=1705, FN=0, Flags=.....C, BI=100, SSID=Wild Palms Hotel	24 dB	2.0	Wild Palms Hotel
23	0.444	LgElectr_8a:f4:59	(802.11)	40	Clear-to-send, Flags=.....C	10 dB	24.0		
24	0.493	Ruckuswi_33:57:38	Broadcast	(802.11)	162	Beacon frame, SN=3938, FN=0, Flags=.....C, BI=100, SSID=Wild Palms Hotel	32 dB	2.0	Wild Palms Hotel
25	0.524	LgElectr_8a:f4:59	Broadcast	(802.11)	228	Beacon frame, SN=1912, FN=0, Flags=.....C, BI=100, SSID=personal	10 dB	1.0	personal
26	0.544	Ruckuswi_13:6e:68	Broadcast	(802.11)	162	Beacon frame, SN=1706, FN=0, Flags=.....C, BI=100, SSID=Wild Palms Hotel	14 dB	2.0	Wild Palms Hotel
27	0.595	LgElectr_8a:f4:59	(802.11)	40	Clear-to-send, Flags=.....C	9 dB	24.0		
28	0.614	Ruckuswi_14:fd:68	Broadcast	(802.11)	162	Beacon frame, SN=2567, FN=0, Flags=.....C, BI=100, SSID=Wild Palms Hotel	30 dB	2.0	Wild Palms Hotel
29	0.646	Ruckuswi_13:6e:68	Broadcast	(802.11)	162	Beacon frame, SN=1707, FN=0, Flags=.....C, BI=100, SSID=Wild Palms Hotel	23 dB	2.0	Wild Palms Hotel

File: "C:\Users\Thomas\AppData\Local\Temp..." Packets: 11319 · Displayed: 11319 (100.0%) · Dropped: 0 (0.0%) Profile: Default

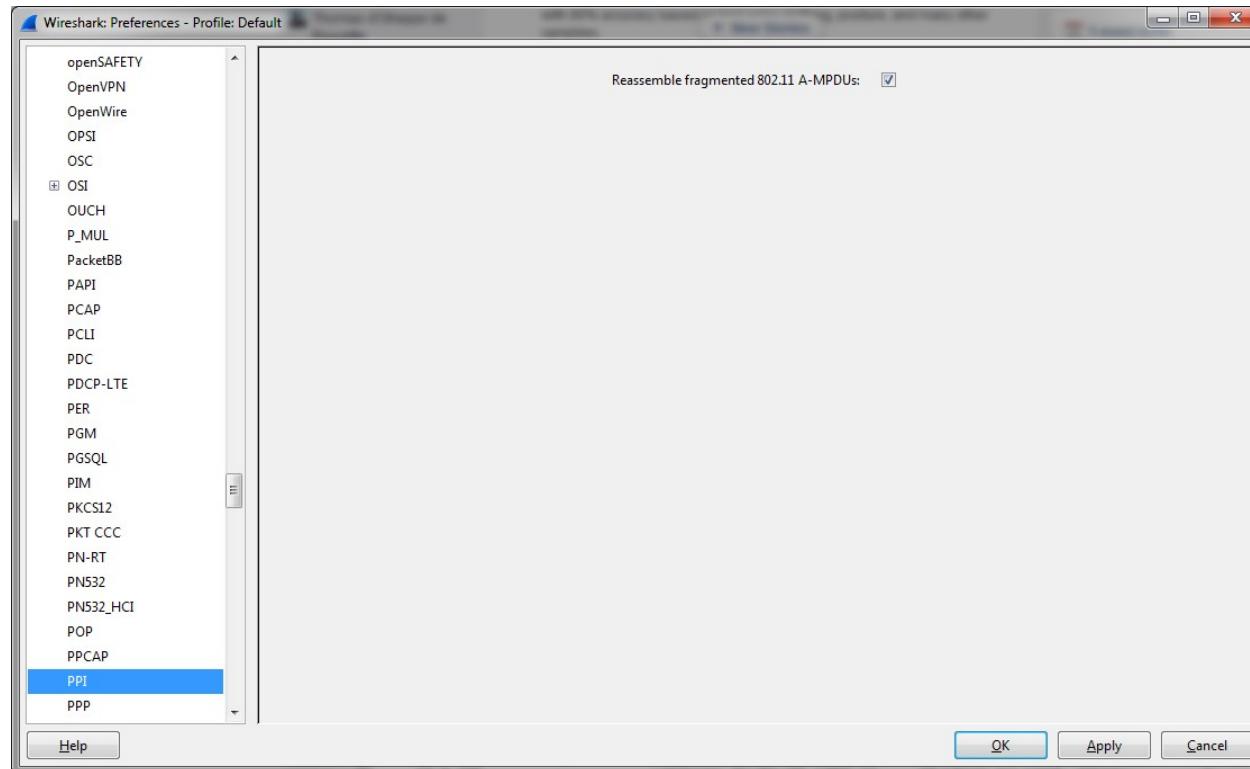
Cabeceras

Radiotap pseudo header (Airpcap)

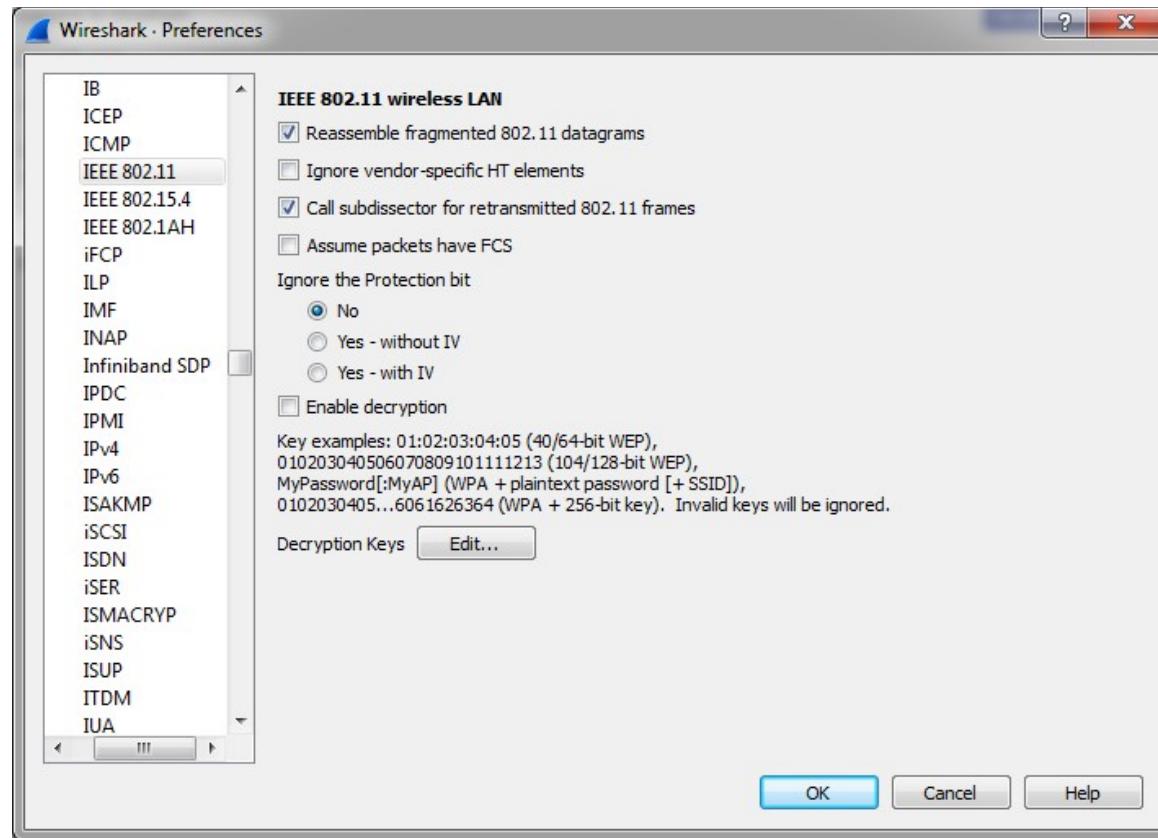


Cabeceras

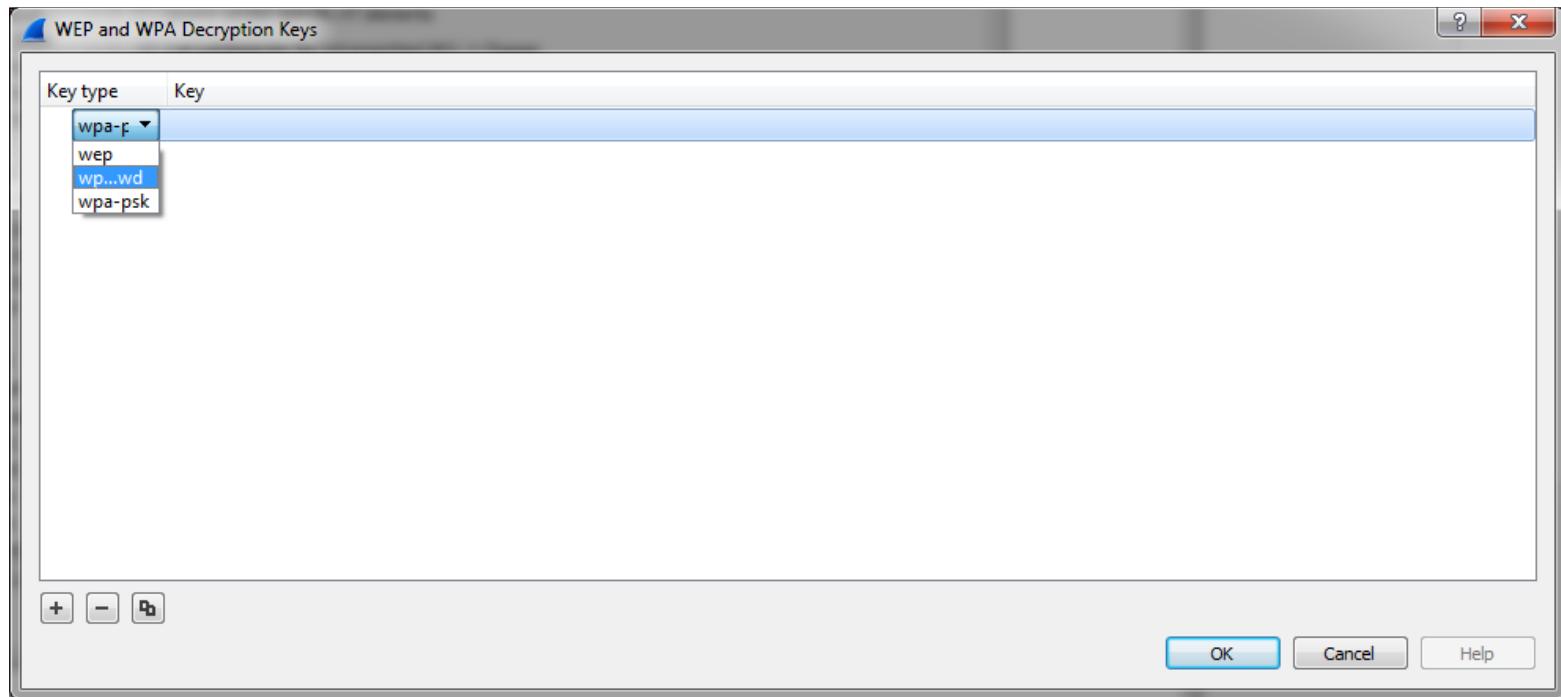
PPI (Per-Packet Information)



Cabeceras



Descifrando tráfico



Descifrando tráfico

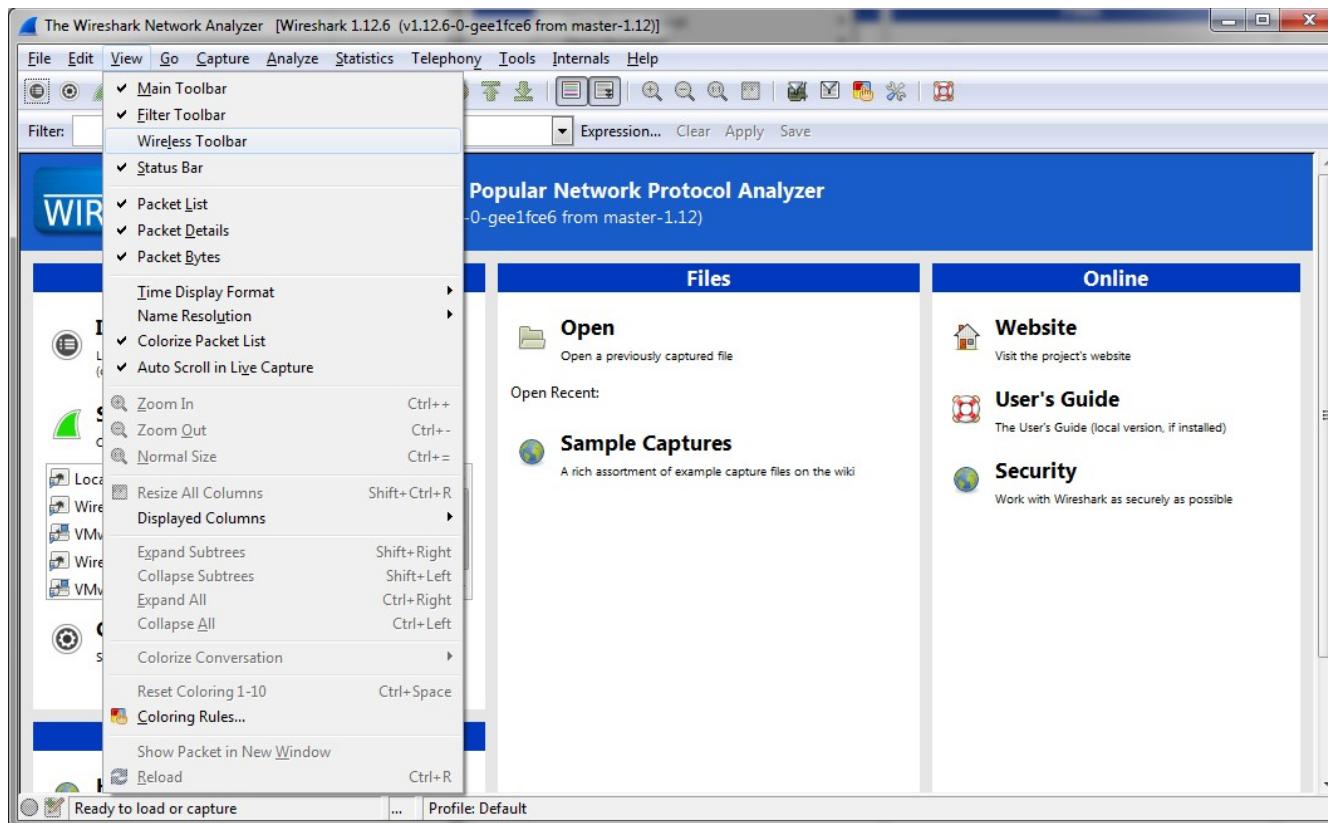
0 WEP

- 0 Introducir la clave con o sin separación entre bytes
 - 0 aa:aa:aa:aa:aa
 - 0 aaaaaaaaaa

0 WPA

- 0 PWD: password y SSID se combinan para crear una pre-shared key
 - 0 Clave:SSID
- 0 PSK: Raw pre-sharedkey (no enterprise)
 - 0 aaaaaaaaa

Wireless toolbar



Filtros de visualización

Relativos a las cabeceras

- 0 ppi: Cabecera PPI (Per-Packet Information)
- 0 ppi_antenna: PPI antenna decoder
- 0 prism: Prism capture header
- 0 radiotap: IEEE 802.11 Radiotap Capture header
- 0 wlancap: AVS WLAN Capture header

Display Filters (2)

- 0 eapol: 802.1X Authentication
- 0 wifi_display: Wi-Fi Display
- 0 wifi_p2p: Wi-Fi Peer-to-Peer
- 0 wlan: IEEE 802.11 wireless LAN
- 0 wlan_aggregate: IEEE 802.11 wireless LAN aggregate frame
- 0 wlan_mgt: IEEE 802.11 wireless LAN management frame
- 0 wlan_rsna_eapol: IEEE 802.11 RSNA EAPOL key
- 0 wlancertextn: Wlan Certificate Extension
- 0 wlccp: Cisco Wireless LAN Context Control Protocol
- 0 wps: Wifi Protected Setup

Filtros de captura

- 0 También conocido como BPF (Berkeley Packet Filter)
 - 0 wlan host XX:XX:XX:XX:XX:XX
 - 0 wlan[0] != 0x80 (para ocultar tramas beacon)

Referencias

- 0 Cómo capturar : <https://wiki.wireshark.org/CaptureSetup/WLAN>
- 0 Filtros: <https://www.wireshark.org/docs/dref/>

The screenshot shows the 'Display Filter Reference' page of the Wireshark documentation. At the top, there's a blue header bar with the Wireshark logo and navigation links for 'Get Acquainted', 'Get Help', and 'Develop'. Below the header, a message says 'We're having a conference! You're invited!'. The main content area has a light gray background and a dark blue header 'Display Filter Reference'. It contains text about display filters and a link to the 'User's Guide'. An 'Index' section lists categories from 1 to Z. Under category 1, there are links to '104apci', '104asdu', and '1722a'. Under category 2, there is a link to '2dparityfec'.

We're having a conference! You're invited!

Display Filter Reference

Wireshark's most powerful feature is its vast array of display filters (over 174000 fields in 1000 protocols as of version 1.12.6). They let you drill down to the exact traffic you want to see and are the basis of many Wireshark's other features, such as the coloring rules.

This is a reference. For general help using display filters, please see the [wireshark-filter](#) manual page or the [User's Guide](#).

Index

1 · 2 · 3 · 4 · 6 · 9 · _ · A · B · C · D · E · F · G · H · I · J · K · L · M · N ·
O · P · Q · R · S · T · U · V · W · X · Y · Z

1

104apci: IEC 60870-5-104-Apci (1.0.0 to 1.12.6, 6 fields)
104asdu: IEC 60870-5-104-Asdu (1.0.0 to 1.12.6, 77 fields)
1722a: IEEE 1722a Protocol (1.0.0 to 1.12.6, 26 fields)

2

2dparityfec: Pro-MPEG Code of Practice #3 release 2 FEC Protocol (1.0.0 to 1.12.6, 14 fields)

Quiz 1

0 Utilizar traza *wlan_desencriptar.pcapng*

0 Desencriptar contenido

0 Contraseña “Induction”

0 SSID “Coherer”

0 ¿A qué página web se está accediendo? ¿desde qué página se navega hasta llegar a ella?

Quiz 2

- 0 Utilizar traza *wlan_signal.pcapng*
- 0 Añade las columnas necesarias para contestar rápidamente a las siguientes preguntas
 - 0 ¿Cuál es el señal recibida más baja? (RSSI)
 - 0 Representa con una gráfica en Excel evolución temporal de la señal
 - 0 ¿Qué canal está usando? ¿Hay cambio de canal?

Quiz 3

- 0 Utilizar traza *wlan_problem.pcapng*
- 0 ¿Qué tipo de tráfico contiene la traza?
- 0 ¿Cuál es el problema?