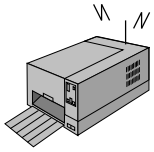
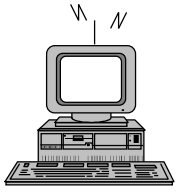
Redes locales inalámbricas
WLAN
IEEE 802.11

1

¿Qué es una red local inalámbrica?

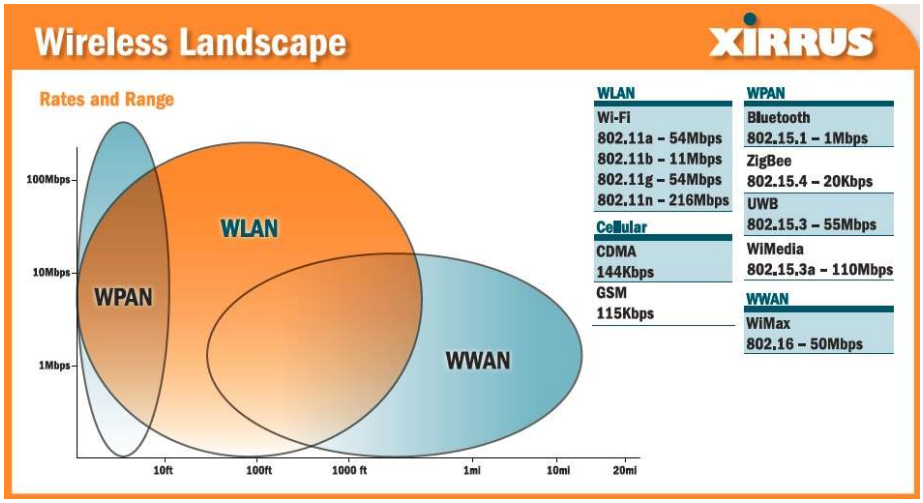
Un conjunto de nodos de cómputo en un área geográfica pequeña, que utilizan el espectro radioeléctrico para intercambiar información.





2

Clasificación de redes WLAN



3

Conectividad inalámbrica

	PAN	LAN	WAN
Velocidad	1-2 Mbps	> 11 Mbps	> 56 kbps
Rango	10 m	100 m	Global
Estándar	Bluetooth	IEEE 802.11	GPRS, etc
Escalabilidad	Baja, nivel dispositivo	Similar a ethernet	Alta, Regional
Arquitectura	FHSS	DSSS	Celular

4

¿Porqué son tan populares?

- Gran flexibilidad
  - Mejora la productividad en el trabajo
  - Conectividad continua a Internet/Intranet
  - Cambios en el ambiente de trabajo
- Conexión “inmediata” a la red
  - Instalación y modificación de cableado (aún estructurado) es difícil y costosa
- Estándares apoyados por la industria
  - IEEE 802.11 / WiFi
- Solución completa, interoperable, a altas velocidades y a precios accesibles

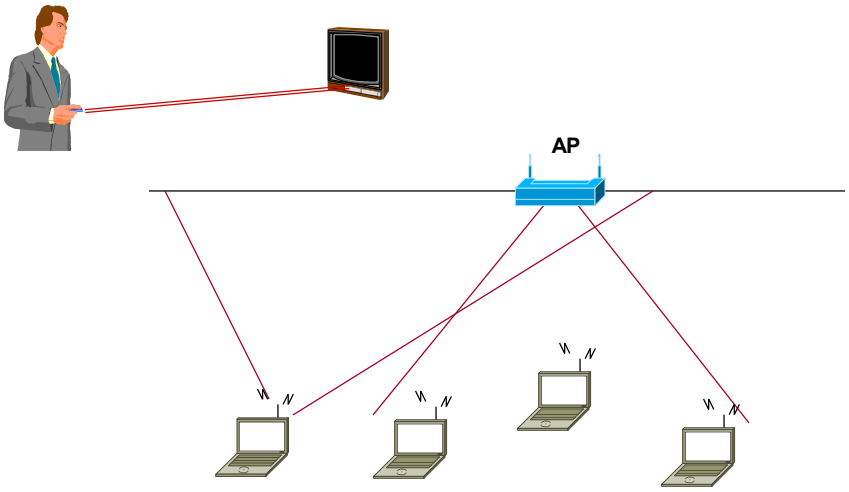
5

Medios de transmisión en WLANs

- Infrarrojo
  - En línea de vista (LOS)
  - Difuso ó Reflejado
- Radio frecuencia
  - Frecuencia dedicada
  - Espectro disperso (SS)
    - Por secuencia directa (DSSS)
    - Por salto de frecuencia (FHSS)
  - Multiplexaje en frecuencia ortogonal (OFDM)

6

Sistema infrarrojo



7

Características

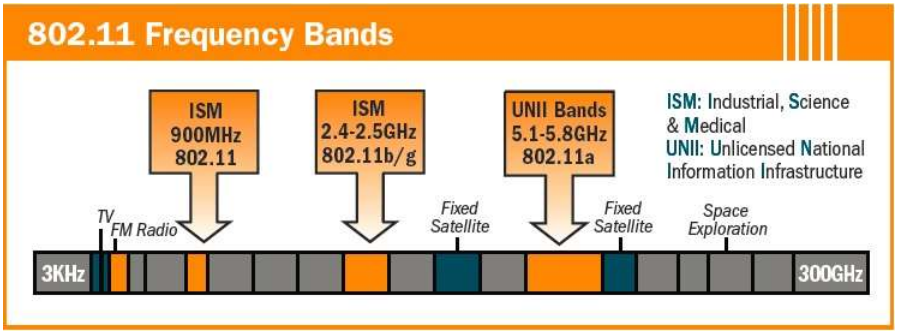
- ✓ Inherentemente seguro contra receptores no deseados
- ✓ Inmune a interferencias electromagnéticas
- ✓ Bajo costo
- ✓ Frecuencias no reglamentadas
- ◆ Cobertura muy limitada
- ✗ Muy sensible a objetos móviles
- ✗ Interferencia con luz brillante
- ✗ En sistemas por difusión, las trayectorias múltiples limitan la velocidad.

8

Tecnologías de Radiofrecuencia (Capa Física)

9

Bandas ISM y UNII para 802.11



10

Capa física original (802.11)

- Se definieron originalmente 3 capas físicas (2 de radio de espectro disperso) y una de infrarojo difuso.
- El radio opera en la banda de 2.4 Ghz, banda que no requiere licencia para operar.
- El 802.11 original definió una velocidad de 1 Mbps y 2 Mbps, usando tecnologías de radio frecuencia llamados FHSS (Frecuency Hopping Spread Sprectrum) y DSSS (Direct Sequence Spread Sprectrum). FHSS y DSSS no interoperan entre si.

11

Espectro disperso

- Transmite en un ancho de banda (mucho) mayor que el mínimo necesario.
- Excelentes características de seguridad.
  - Receptores no deseados
  - Interferencias accidentales ó intencionales
- Tecnología de facto en redes inalámbricas.

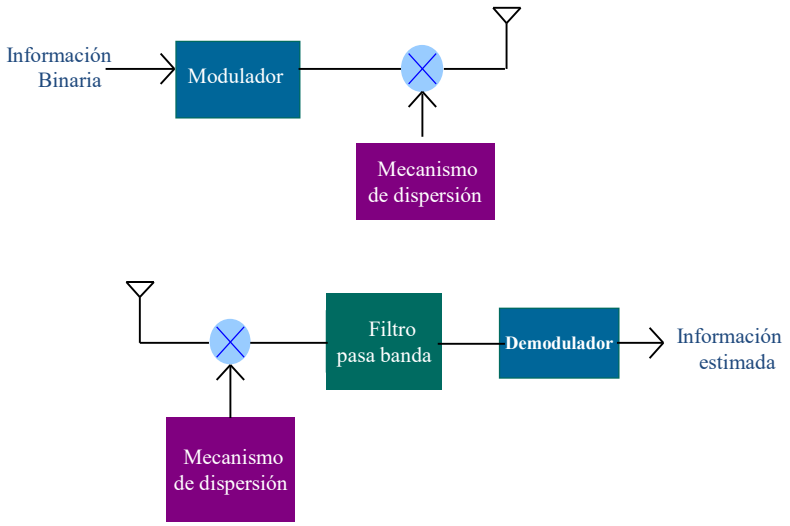
12

Espectro disperso

- Transmite en un ancho de banda (mucho) mayor que el mínimo necesario.
- Excelentes características de seguridad.
  - Receptores no deseados
  - Interferencias accidentales ó intencionales
- Tecnología de facto en redes inalámbricas.

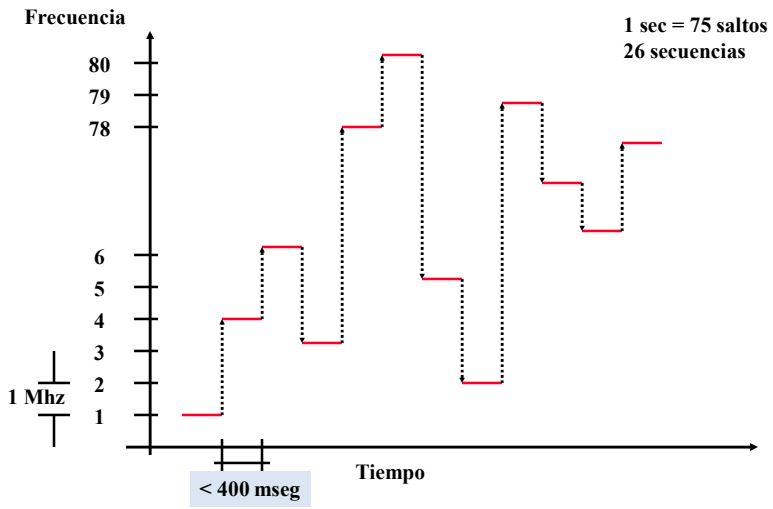
13

Espectro disperso



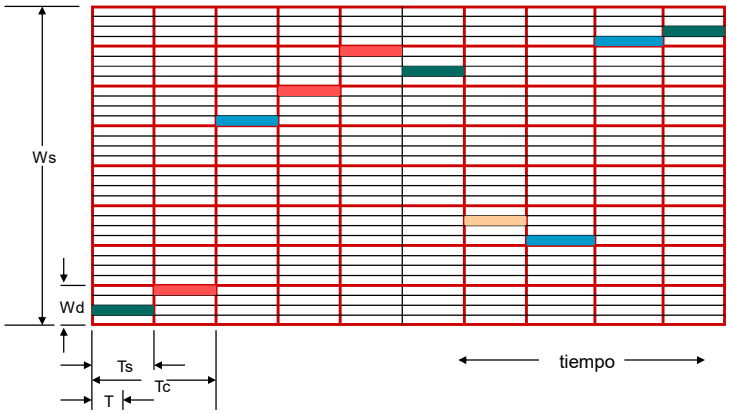
14

FH (Frecuency Hopping)



15

Espectro disperso por salto de frecuencia (FHSS)



Datos: 01 11 00 11 11 01 10 00 00 01

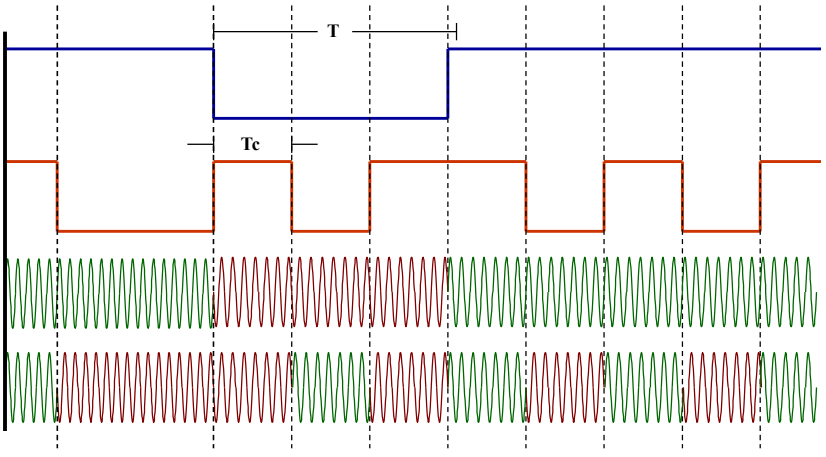
16

Sabias de donde viene FH?

- La idea original de FH viene de la actriz de cine Hedy Lamarr.
- Se inspiró en la tecnología de radio frecuencia utilizada para el control de los misiles empleados durante la segunda guerra mundial.
- Patentó su idea, pero cuando fue aplicada, la patente ya había expirado por lo que no recibió dinero alguno.

17

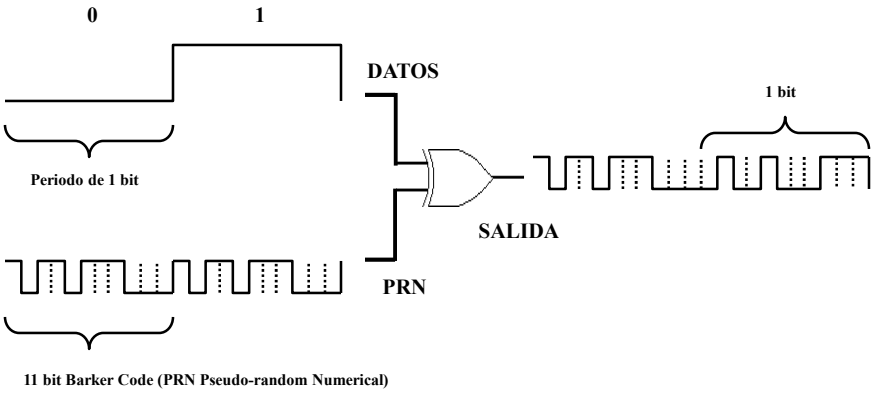
Espectro extendido por secuencia directa (DSSS)



Datos: 1 0 1

18

Direct Sequence



19

CDMA-Ejemplo DS

- Tres nodos envían información al mismo tiempo:
  - Nodo A ‘1’
  - Nodo B ‘0’
  - Nodo ‘C’ ‘1’
- Los códigos de dispersión son:
  - Nodo A 10111001 XOR → 0 1 0 0 0 1 1 0
  - Nodo B 01101110 XOR → 0 1 1 0 1 1 1 0
  - Nodo C 11001101 XOR → 0 0 1 1 0 0 1 0
- NRZI: Si el “chip” es ‘1’, se emite +V volts; de lo contrario, se emite –V volts

20

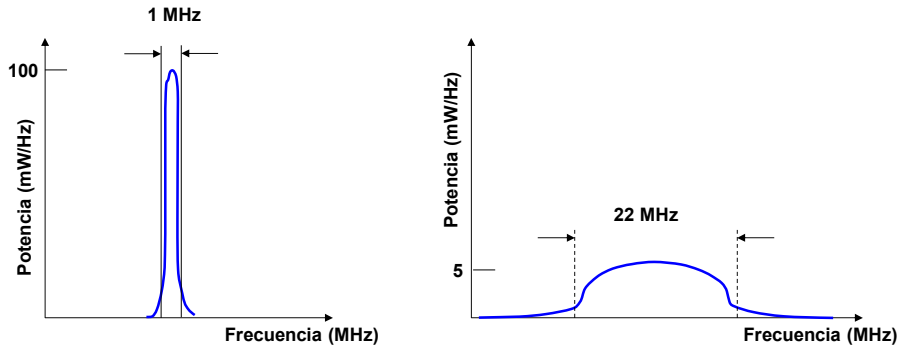
CDMA-Ejemplo DS

- Tras la dispersión, los nodos emiten:
  - Nodo A ‘1’ => + – + + + – – +
  - Nodo B ‘0’ => + – – + – – – +
  - Nodo ‘C’ ‘1’ => + + – – + + – +
- El receptor recibe la suma de estas señales:

  +3 –1 –1 +1 +1 –1 –3 +3
- Para “demultiplexar” el receptor multiplica esta señal por el código de dispersión que le corresponde.
  - Nodo A: (3)(-1)+(-1)(1)+(-1)(-1)+(1)(-1)+(1)(-1)+(–1)(1)+(–3)(1)+ (3)(-1)= -9
    Se interpreta como ‘1’
  - Nodo B: (3)(1)+(-1)(-1)+(-1)(-1)+(1)(1)+(1)(-1)+(–1)(-1)+(–3)(-1)+(3)(1)= 9
    Se interpreta como ‘0’
  - Nodo C: (3)(-1)+(-1)(-1)+(-1)(1)+(1)(1)+(1)(-1)+(–1)(-1)+(–3)(1)+(3)(-1)= -5
    Se interpreta como ‘1’

21

Frequency Hopping *vs* Direct Sequence



Frequency Hopping

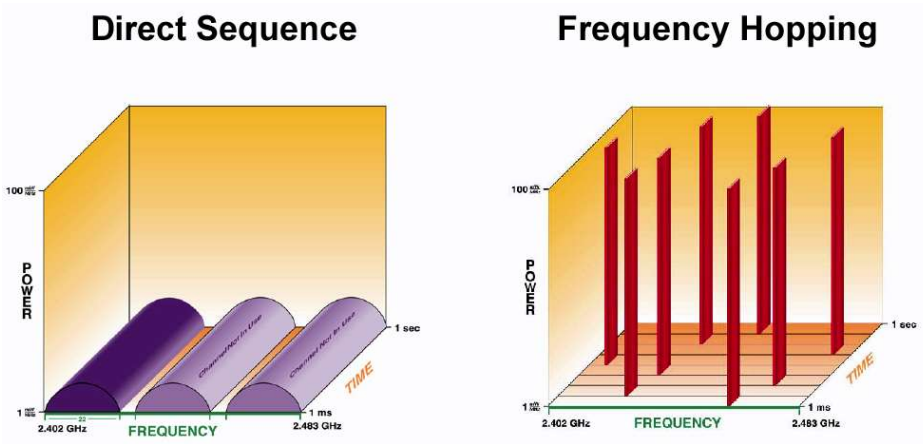
Señal concentrada, gran intensidad
Elevada relación S/R
Área bajo la curva: 100 mW

Direct Sequence

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

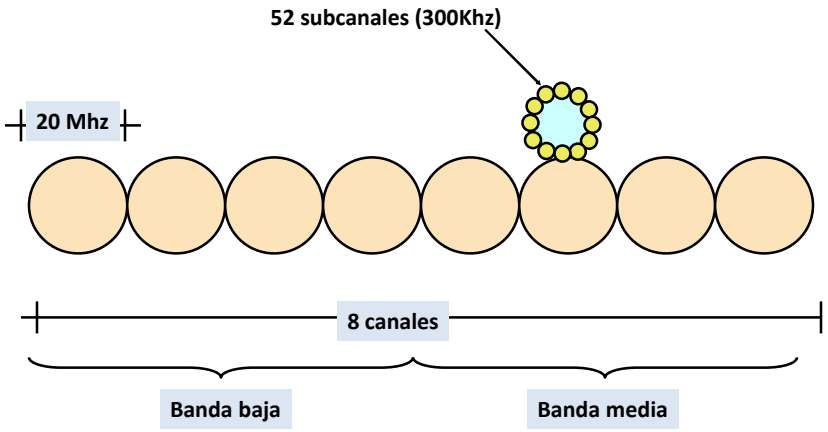
22

Salto de frecuencia vs secuencia directa



23

Esquema de modulación (OFDM-Ortogonal Frecuency Division Multiplexing)



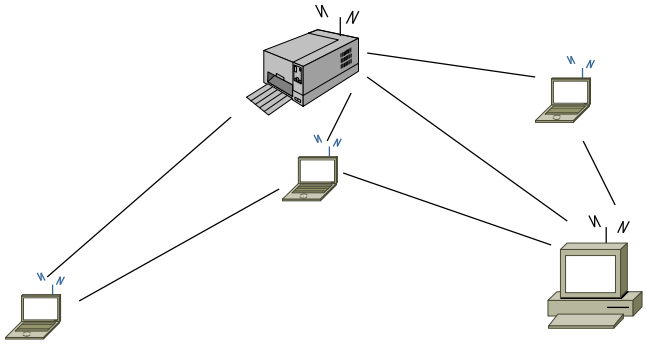
24

Modo de Operación (Arquitectura)

25

Arquitectura independiente - IBSS

- Comunicación entre pares (*ad hoc*)
  - Los nodos en la red pueden comunicarse directamente entre sí.
  - No necesariamente es conexión punto a punto.

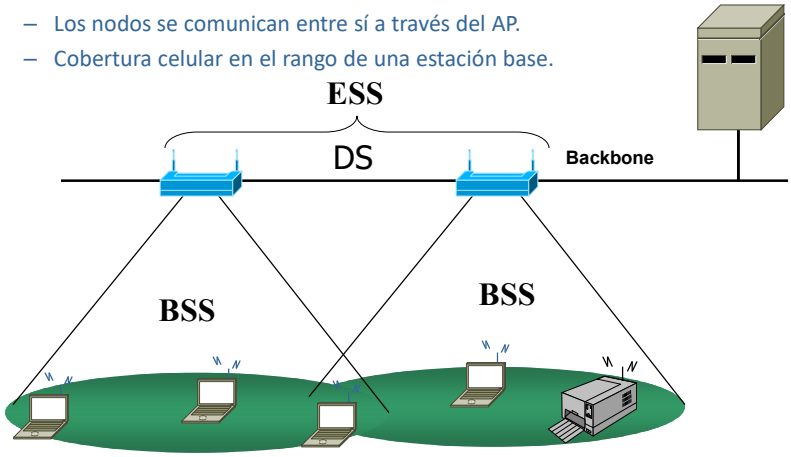


26

Basada en infraestructura

Comunicación base – móvil

- Puntos de acceso a backbone de alta velocidad
- Los nodos se comunican entre sí a través del AP.
- Cobertura celular en el rango de una estación base.

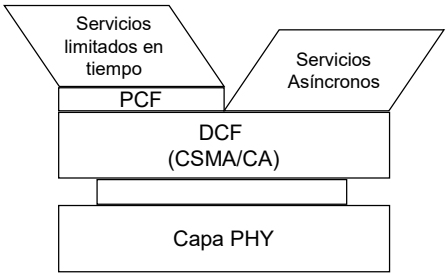


27

Mecanismo de Control de Acceso (Capa MAC)

28

Actividades IEEE 802.11
Protocolo DFWMAC



Para transmitir tráfico con restricciones de tiempo

- Utiliza una supertrama con campos para tráfico asíncrono e isocrono
- Emplea mecanismos de prioridad.

29

Mecanismos de control de acceso

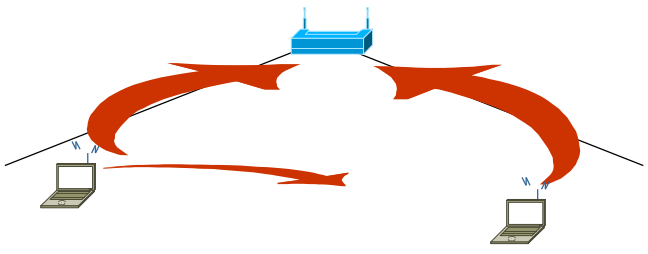
- Función de coordinación distribuida (DCF)
  - Mecanismo de acceso por contención
  - No permite garantías de retraso
- Función de coordinación centralizada (PCF)
  - Opcional
  - Utiliza mecanismo de poleo
  - Ineficiente para servicios VoIP y otros en redes con muchos dispositivos

30

IEEE 802.11e

- Mejoras para ofrecer QoS en redes inalámbricas
- Introduce función de distribución híbrida (HCF) que puede ser compatible con DCF y PCF
- Dos modos de operación
  - EDCA (*Enhanced distributed coordination access)*
    - Mismas funciones que DCF más cuatro categorías de acceso con cuatro prioridades
  - HCCA (*HCF Controlled Channel Access)*
    - Se otorgan oportunidades de transmisión durante un tiempo determinado por poleo o ganando solicitud durante un intervalo de contención

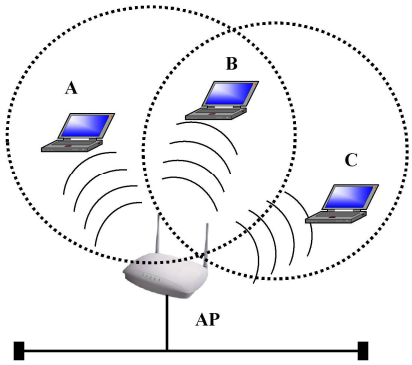
El problema de la terminal oculta

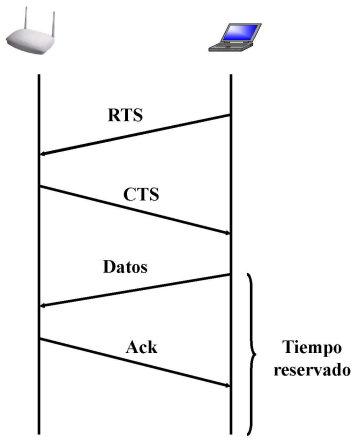


La estación “A” transmite con potencia suficiente para acceder al *AP* pero no para que sea escuchada por la estación “B”

Algoritmo de reservación CSMA/CA

PCF (Point Coordination Function)



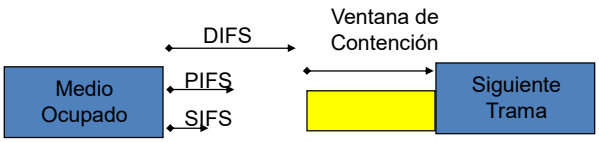


Problema de terminal oculta

33

Mecanismo de control de acceso

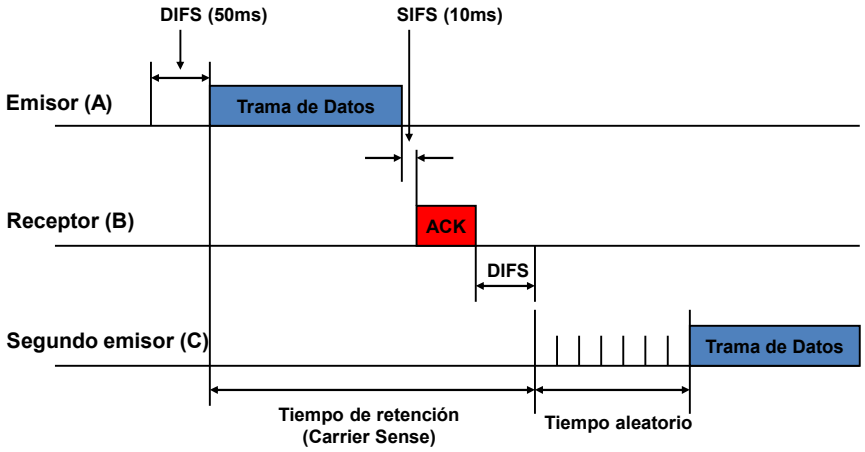
- IFS: interframe space: depende del tipo de trama a transmitir
  - SIFS: Short IFS
    - Trama de alta prioridad antes de contender por el canal
    - Tramas ACK, CTS MSDU fragmentadas, respuestas a poleo del AP, tramas desde el AP durante un CFP (Contention Free Period)
  - PIFS: PCF-IFS
    - Utilizado por PCF para ganar acceso prioritario al medio al inicio de un CFP
  - DIFS: DCF-IFS
    - Transmisión convencional de tramas



34

Algoritmo de contención CSMA/CA

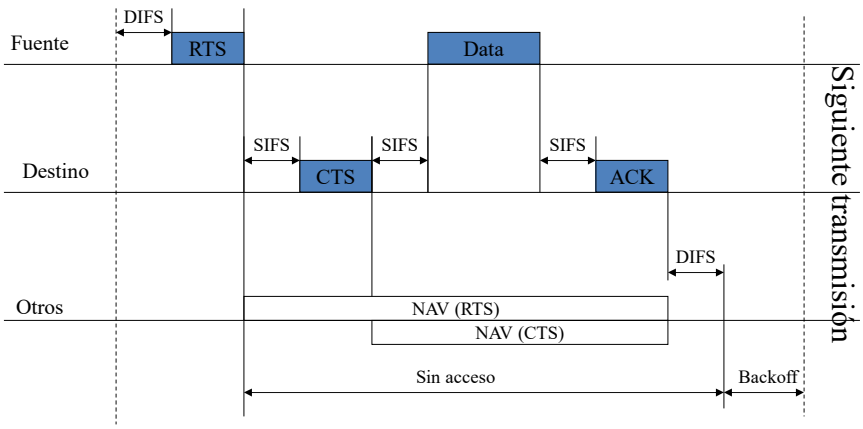
DCF (Distributed Coordination Function)



35

Algoritmo de reservación CSMA/CA

PCF (Point Coordination Function)



36

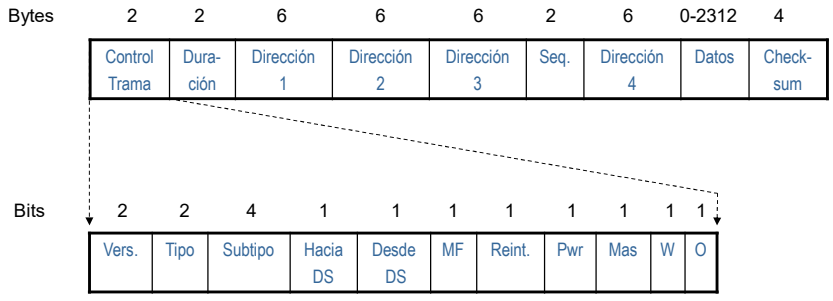
Duración IFS

- La duración de los intervalos de espera depende de varios factores; entre ellos, la banda de frecuencia y la técnica de modulación. La siguiente tabla muestra los valores típicos para SIFS, PIFS, DIFS

PHY	SIFS	PIFS	DIFS
DSSS/802.11b	10 µs	30 µs	50 µs
802.11g	10 µs	Long=30 µs Short=19 µs	Long=50 µs Short=28 µs
OFDM/802.11a	16 µs	25 µs	34 µs
802.11n	10 µs-2.4 GHz 16 µs-5 GHz	Long=20 µs-2.4GHz Short=19 µs-2.4 GHz 25 µs - 5 GHz	Long=50 µs-2.4GHz Short=28 µs-2.4 GHz 34 µs - 5 GHz

37

Formato de trama 802.11



MF: Indica que siguen más fragmentos
Reint.: Indica que esta trama es un reenvío
Pwr: Para 'dormir' o 'despertar' a una estación
Mas: Advierte que el emisor tiene más tramas para enviar
W: La trama está encriptada con WEP (Wireless Equivalent Privacy)
Duración: Dice cuanto tiempo va a estar ocupado el canal por esta trama
Dirección n: Dirección de origen y destino. Dirección de est. base origen y destino.

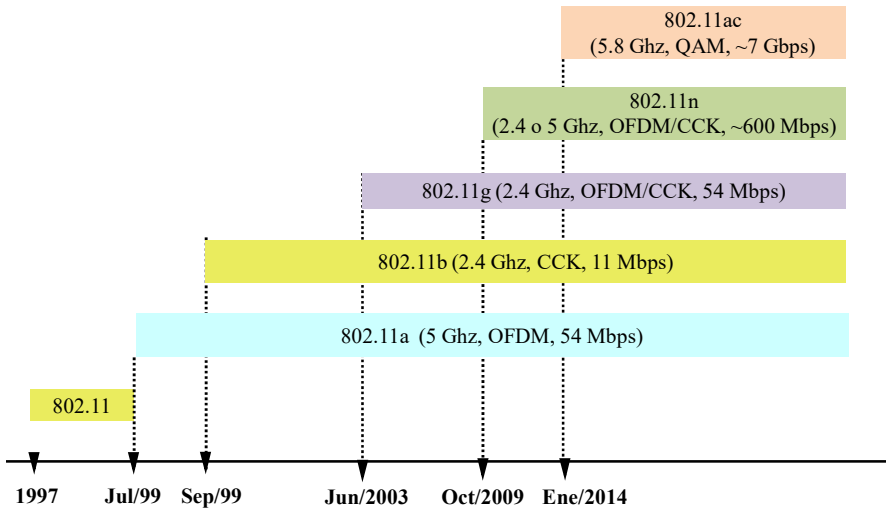
38

Evolución de la norma 802.11

- 802.11 1 y 2 Mbps DS/FHSS 2.4 GHz
- 802.11b 11 Mbps DSSS 2.4 GHz
- 802.11a 54 Mbps OFDM 5 GHz
- 802.11g 22 y 54 Mbps DSSS 2.4 GHz
- 802.11e 22 Mbps con Calidad de servicio
- 802.11i Mejoras a mecanismo de seguridad
- 802.11n 540 Mbps (100-200 Mbps efectivo) 5/2.4 GHz
- 802.11f Protocolo entre APs (IAPP)

39

Estándares 802.11



40

Implementación de una red inalámbrica

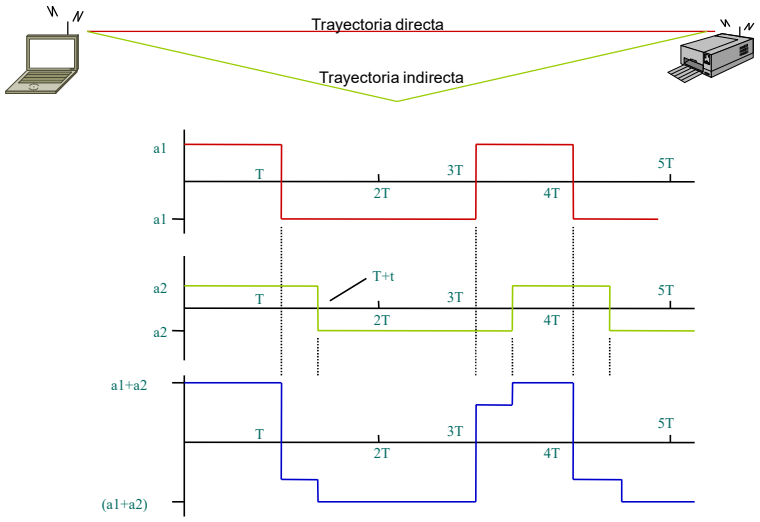
41

Implementación de red inalámbrica

- Requisitos
  - Seguridad
  - Disponibilidad
  - Desempeño
  - Escalabilidad
  - Facilidad de administración
- Puntos a considerar
  - Uso
  - Tipo y potencia de nodo de acceso
  - Tipo de antenas
  - Energía sobre cableado
  - Herramientas de evaluación del sitio

42

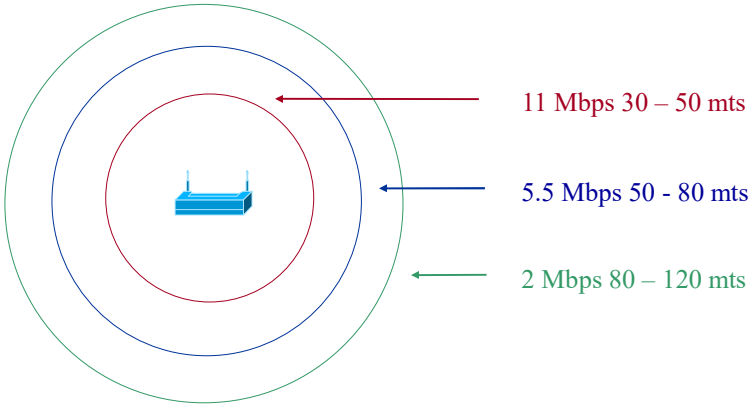
Efecto de trayectorias múltiples



43

Nodo de acceso - características

- Tipo de antena
- Mecanismos de seguridad
- Energía por cableado UTP
- Velocidad, potencia y alcance
- Interoperabilidad



44

Tipo de antena

- Dipolo
  - Omnidireccional
  - Cobertura circular
  - Usuario típico en oficina
- *Patch*
  - Direccional con un cono de apertura amplio
  - Energía concentrada hacia delante
- *Yagi*
  - Altamente direccional con cono de apertura angosto
  - Enlaces punto a punto

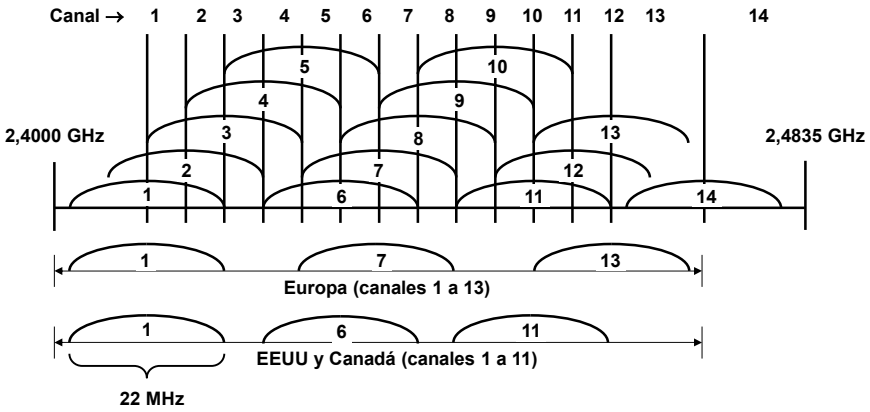
Canales 802.11b DSSS a 2,4 GHz

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

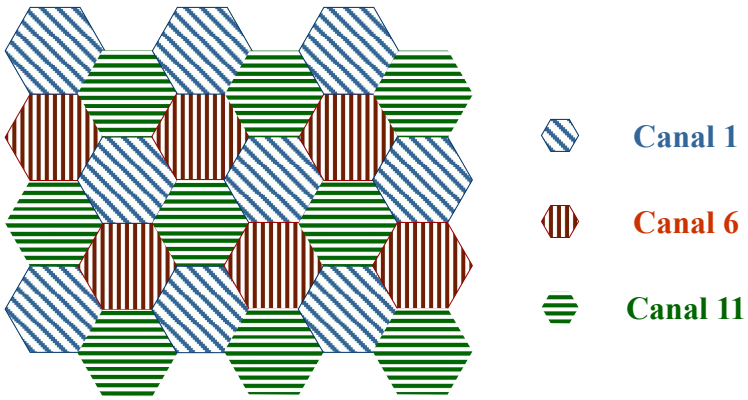
Reparto de canales DSSS a 2,4GHz



47

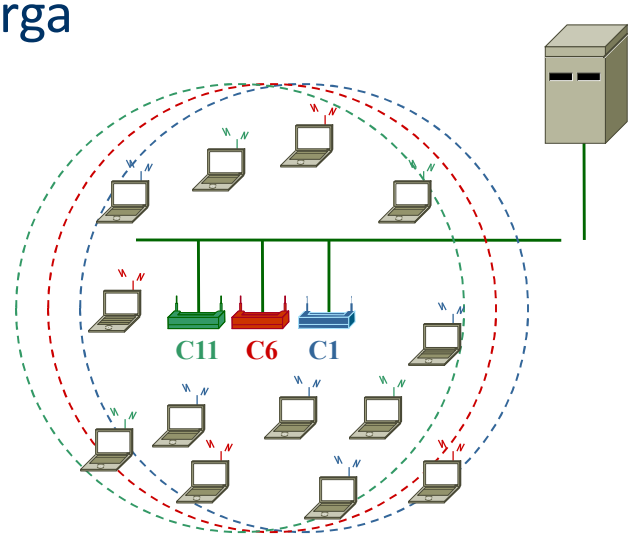
Reutilización de frecuencias

- En 802.11b hay 14 canales traslapados de 22 MHz cada uno. De ellos, 3 no se traslapan



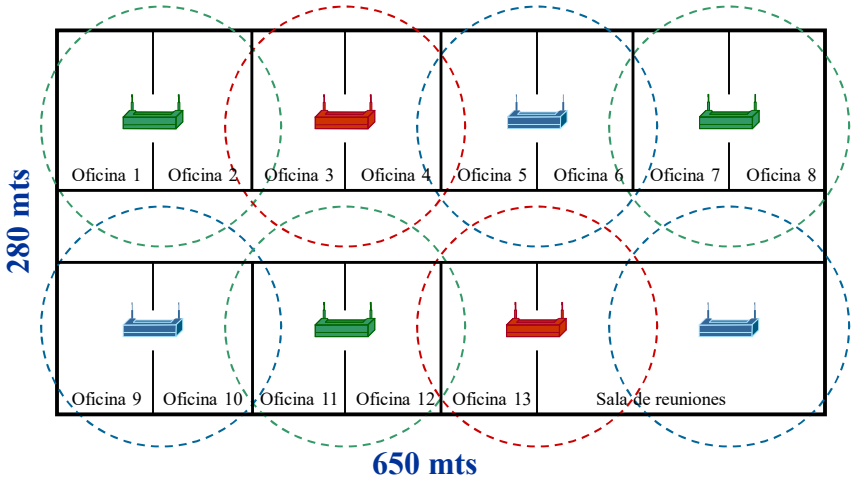
48

Topología redundante – balanceo de carga



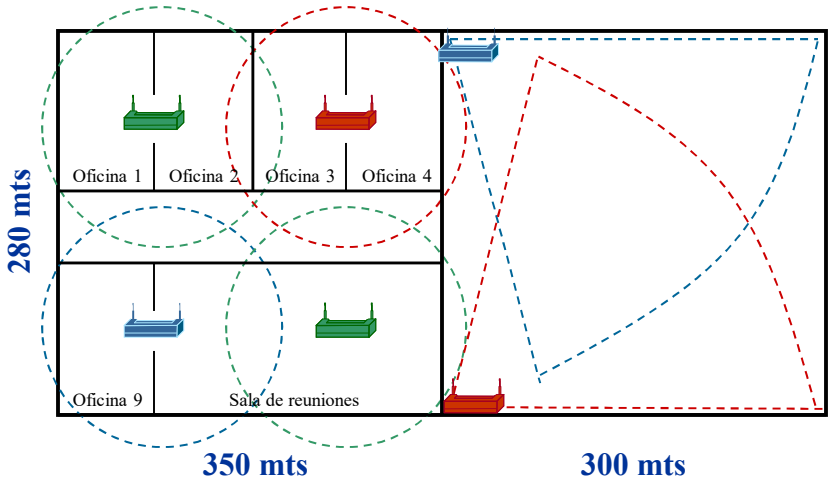
49

Oficina inalámbrica



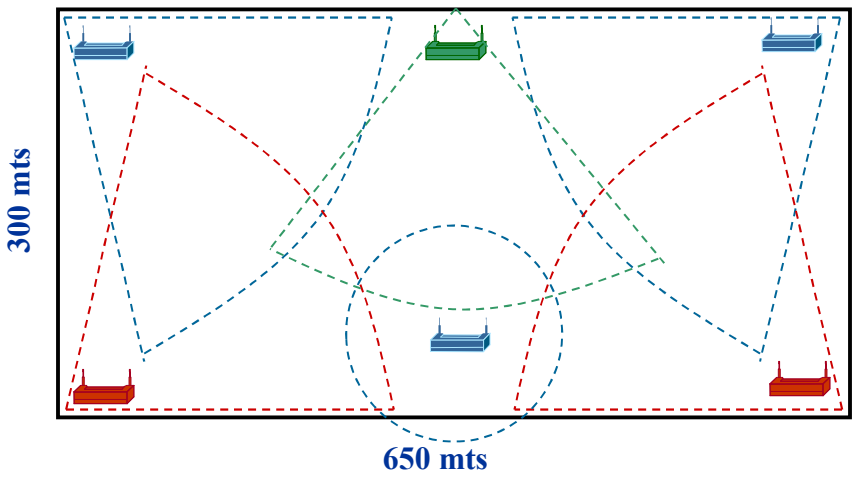
50

Cobertura adentro y afuera



51

Cobertura en bodega



52

Proceso de asociación

- Cuando un cliente entra en el rango de uno o más APs, este selecciona un AP para asociarse "BSS joining". La asociación se realiza en base a la potencia de la señal y a la razón de error de paquetes.
- Una vez aceptado por el AP, el cliente sintoniza el canal del radio al AP.
- Periódicamente el cliente supervisa por otros AP que pudieran proveer mejores características de desempeño, si este es el caso, se reasocia con un nuevo access point resintonizando su canal de radio.

53

Itinerancia ('Handover')

- Los AP envían regularmente (10 veces por segundo) mensajes de guía (beacon) para anunciar su presencia a las estaciones que se encuentran en su zona
- Si una estación se mueve y cambia de celda detectará otro AP más potente y cambiará su registro. Esto permite la itinerancia ('handover') sin que las conexiones se corten.
- Los estándares 802.11 no detallan cómo debe realizarse la itinerancia, por lo que la interoperablidad en este aspecto no siempre es posible
- Para corregirlo varios fabricantes han desarrollado el IAPP (Inter-Access Point Protocol) que ha dado lugar al estandar 802.11f

54

IEEE 802.11n

55

Incentivos

- En la oficina
  - Acceso inalámbrico con movilidad a cualquier sistema empresarial con alta calidad
  - Acceso a bases de datos a alta velocidad
  - Gráficos con alta definición
  - Aplicaciones de video
- En el hogar
  - Evita puntos ciegos
  - Navegación a alta velocidad
  - Aplicaciones de audio y video con alta fidelidad
  - Confiabilidad

56

Requerimientos de nuevos flujos

		Características de los flujos		
Aplicación	Ejemplo	Tipo	Tasa	Duración/Vol
Audio/Video 1	HDTV y DV para uso comercial y doméstico	Constante (jitter bajo)	27 Mbps	Horas
Audio/Video 2	SDTV para uso comercial y doméstico	Constante (jitter bajo)	6 Mbps	Horas
Audio/Video 3	Video conferencia con VoIP	Constante (jitter bajo)	2 Mbps	< 1 hr
Interactiva 1	Juegos interactivos, navegación en internet, correo electrónico	Variable	2 Mbps	1 hr
Interactiva 2	VoIP, juegos interactivos	Constante con intervalos	0.2 MB/s	1 min - 1 hr
Grandes transferencias	Actualizaciones flash, transferencia archivos, transferencia MM	Variable	30 Mbps	10 MB - 10 GB

57

Principales características

- Velocidad: 540 Mbps pico en capa física, 100 a 200 Mbps efectivos en MAC
- Pretende ser la red de acceso dominante en el hogar y la oficina
- Distintos modos para ofrecer compatibilidad con estándares anteriores.
  - Sistemas instalados. AP 802.11 y STA a/b/g
  - Operación mixta. AP 802.11n y STA a/n
  - "*Green field*" AP y STA 802.11n

58

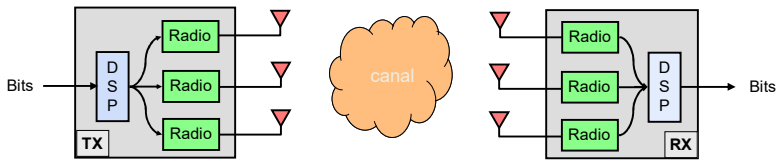
Características técnicas

- Capa física
  - Operación en la banda de 2.4GHz y de 5GHz
  - MIMO – OFDM
    - Multiplexaje espacial
    - *Beamforming*
  - Ancho de banda extendido 40 MHz mediante dos canales adyacentes de 20MHz
  - Técnicas avanzadas de codificación
- Capa MAC
  - Técnicas avanzadas para reducir tiempos entre transmisiones
    - Agregación de tramas pequeñas en una sola MPDU (similar a *packet bursting)*
    - Acuses de recibo por bloques.
  - Mecanismos para facilitar el ahorro de energía en los dispositivos móviles

59

MIMO (Multiple Input Multiple Output

- Transmite y recibe con varios radios simultáneamente en el mismo canal

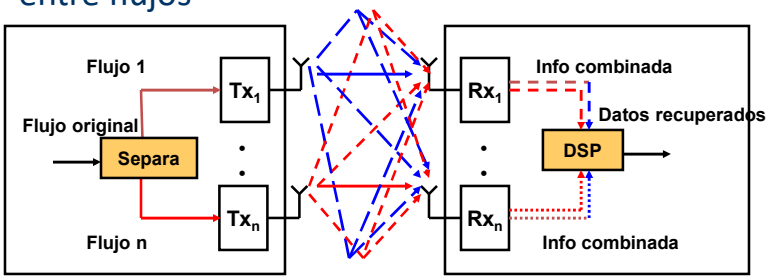


- A diferencia de SISO que ocupa un solo radio

60

Características generales

- Cada Tx envía un flujo independiente (multiplexaje espacial) o no (beamforming) en el mismo canal al mismo tiempo
- Se aprovechan las trayectorias múltiples para recuperar la señal (mayor energía, mayor SNR)
- Sofisticadas técnicas DSP para anular la interferencia entre flujos



61

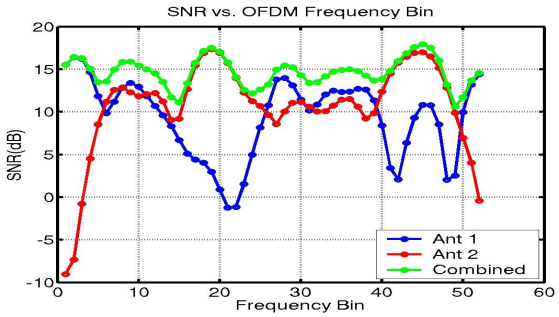
Ventajas

- Aprovecha efecto multi-trayectoria reduciendo la posibilidad de encontrar espacios muertos
  - *Beamforming*
- La potencia total de transmisión puede aumentar pues cada radio cuenta con su propio amplificador
- Tasas de transmisión mayores
  - Multiplexaje espacial
- Interferencia entre transmisión y recepción puede reducirse

62

Beamforming

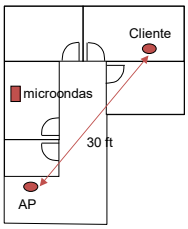
- Mismo flujo en cada antena, aumenta la potencia total recibida (y con ella la SNR)
- Aumenta el rango y reduce la posibilidad de zonas muertas
- Reduce interferencia de otros sistemas

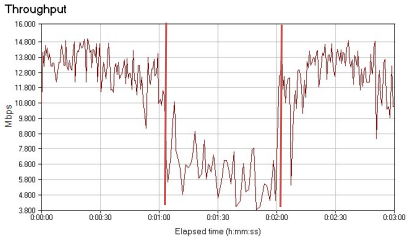


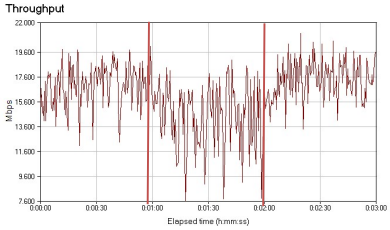
63

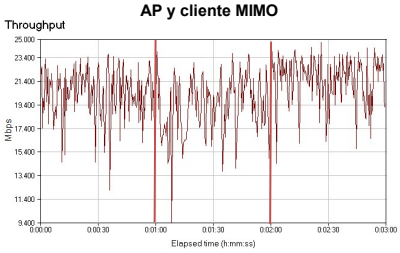
Ejemplo de efecto anulando interferencia

- Pruebas durante 3 min
- Entre los minutos 1 y 2 se enciende el horno de micro-ondas









64

Consideraciones

- Contexto
  - Canales de 40 MHz en la banda de 2.4 GHz limitan seriamente el desplegado de células sin interferencia entre canales.
  - En la banda de 5 GHz, hay sub-bandas (en EUA y México) que pueden estar asignadas a otros servicios. Se pide el uso de radios con salto de frecuencia dinámica (DFS). Esto también afecta el desplegado de células.
  - Tecnología MIMO es óptima cuando hay múltiples trayectorias
    - Reubicación de APs
    - Site survey o técnicas sofisticadas de simulación para colocación óptima de AP
  - Ambientes de alta densidad (micro células) han presentado problemas de interferencia

65

Consideraciones

- Cobertura
  - Señales en la banda de 5 GHz se atenúan más rápidamente. Estaciones muy remotas pueden no ser vistas a pesar de la ganancia de beamforming
  - En redes híbridas, se recomienda dejar la banda de 5 GHz para nodos 11n y la de 2.4 GHz para nodos 11b y g
- Migración
  - Un esquema de simple sustitución de APs puede no dar los resultados esperados

66

Seguridad en redes inalámbricas

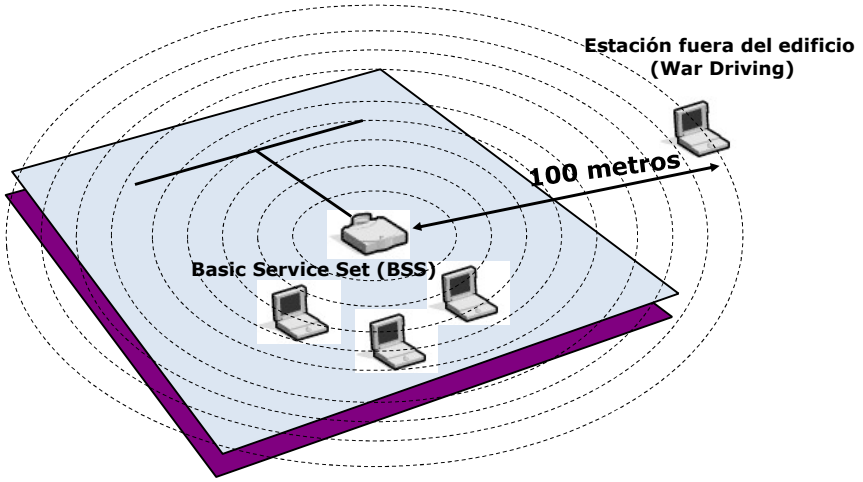
67

Amenazas típicas

- Acceso no autorizado
  - De usuarios y de nodos de acceso
- Monitoreo de tráfico
  - Análisis de paquetes, de volúmenes
- Interferencias
  - Negación de servicio con dispositivos en banda ICM
- Ataques cliente a cliente
  - Usurpación de direcciones, de identidad
- Ataques contra mecanismos de autenticación y encripción

68

Monitoreo no autorizado



69

Resultados del *War Driving*

>http://www.wigle.net/
- 568,000 GPS redes inalámbricas localizadas

- WorldWide WarDrive Otoño 2002
  - Chris Hurley, DefCon11

CATEGORY	TOTAL	PERCENT
TOTAL APs FOUND	**9374**	**100**
WEP Enabled	**2825**	**30.13**
No WEP Enabled	**6549**	**69.86**
Default SSID	**2768**	**29.53**
Default SSID and No WEP	**2497**	**26.64**
Unique SSIDs	**3672**	**39.17**
Most Common SSID	**1778**	**18.97**
Second Most Common SSID	**623**	**6.65**

70

Mecanismos de seguridad

- Básicos
  - Configurar SSID (*Service Set Identifier*)
  - Filtrado a partir de direcciones MAC
  - Control de potencia de emisión
- Avanzados
  - WEP – *Wired Equivalent Privacy*
  - IEEE 802.11i / WPA – *WiFi Protected Access Security*
  - VPN
  - Mecanismos de capas superiores

71

Mecanismos avanzados de seguridad

Nivel de Seguridad	Encripción	Autentificación
Bajo (original)	WEP	MAC
Medio (interino WPA)	TKIP	802.1x (EAP)
Alto (802.11i)	AES	802.1x (EAP)

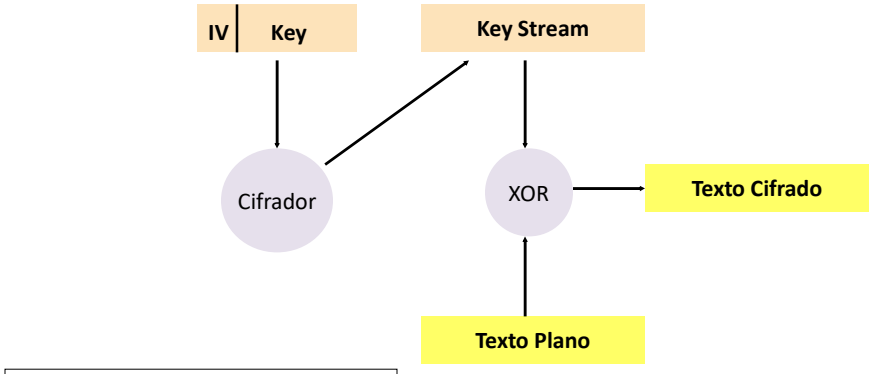
72

Wired Equivalent Privacy

- Autenticación
  - Cliente solicita autenticación
  - AP envía desafío en texto plano
  - Cliente responde enviando desafío encriptado con llave compartida
  - AP verifica y permite o restringe acceso
- Encripción
  - Utiliza algoritmo RC4 (algoritmo simétrico) con llave de 64 bits
    - 40 bits llave de encripción + 24 bits vector inicial (IV)
  - Llave es semilla a PRNG para generar una secuencia que se combina con texto para producir el mensaje cifrado
- Integridad
  - Campo ICV (CRC-32) agregado para verificar integridad

73

Encripción WEP (Wired Equivalent Privacy)

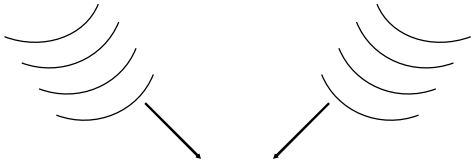


IV : Vector de Inicialización
- Entero de 24 bits
- Se suma a las llaves de 40 ó 104 bits

74

Vulnerabilidad de WEP (reuso de llave)

Texto Cifrado



Derivación de llave:
- Estadística
- Inductiva

75

Limitaciones WEP

- Autenticación es opcional. Por omisión, ésta no se lleva a cabo (*hot* spots)
- No se especifica cómo se establece la llave secreta. Lo común es que ésta sea compartida por todos los clientes y el AP
- RC4 es un protocolo de encripción débil
- El vector de inicialización se repite en un intervalo relativamente corto
- Varios investigadores han demostrado estas limitaciones y de hecho se encuentra disponible el código para romper la seguridad de WEP

76

Evolución de la seguridad en WLANs

- El grupo IEEE 802.11i realizó mejoras a WEP para ofrecer un sistema realmente seguro
  - Esquema de encripción robusto: AES
  - Esquema de autentificación 802.1x
  - Administración jerárquica de llaves
  - Negociación de protocolos de encripción y autenticación
  - TKIP (*temporal key integrity protocol*)
- WECA (Wireless Ethernet Alliance) exige desde agosto de 2003 que los productos cuenten con un subconjunto de estos esquemas (WPA: WiFi protected access) para que reciban la certificación WiFi

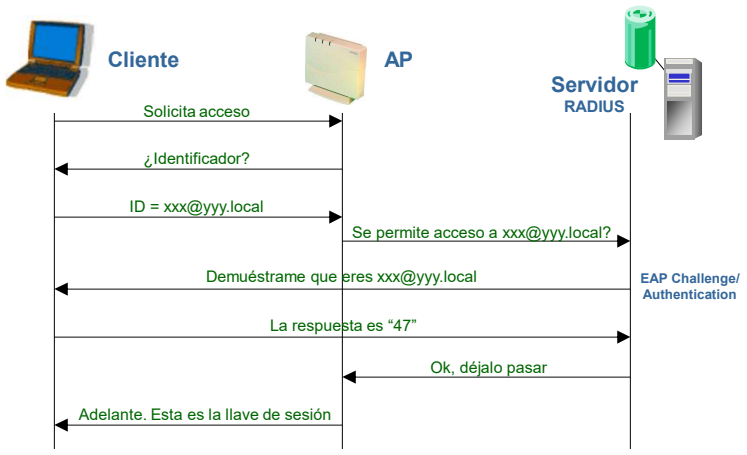
77

Control de acceso 802.1x

- Protocolo de capa 2 para redes basadas en puertos (conmutadores)
  - Independiente de la capa física: redes alambradas e inalámbricas
- Protocolo de autentificación EAP (RFC 2284)
  - Método a seleccionar por los participantes (contraseña, certificados, *smart cards*, …)
- Utiliza llaves de sesión
  - Las llaves de sesión son válidas durante un intervalo de tiempo
  - Llave de usuario para poder cambiar llave de sesión
- Aumenta seguridad de acceso remoto vía módem
  - Llaves de sesión dinámicas
  - Re-autentificación

78

802.1X. Ejemplo



79

Tipos de autentificación EAP

- EAP-Cisco (LEAP)
  - Basado en contraseña
- EAP-TLS (Transport Layer Security)
  - Basado en certificados (PKI)
- EAP-PEAP (Protected EAP)
  - Híbrido: Certificados/contraseña
- EAP-TTLS (Tunel TLS)
  - Híbrido: Certificado/contraseña

80