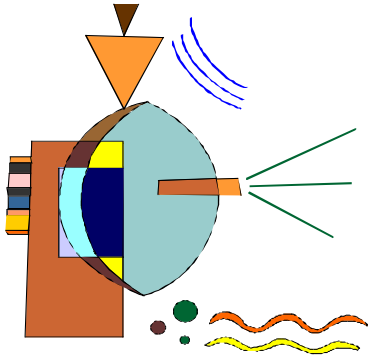


Redes de Datos

Tema XI:
Redes Inalámbricas
WLAN

¿Qué es una WLAN?

- Acrónimo de Wireless Local Area Network
  - ✓ Red de Área Local Inalámbrica
- Características más importantes
  - ✓ Red de alta velocidad, desde 11 Mbps hasta? 133 Mbps según el protocolo
  - ✓ Red sin cables
- Equivalente a una red local cableada estándar
  - ✓ Mismo tipo de aplicaciones
  - ✓ Mismo tipo de uso
- Ofreciendo ventajas inalámbricas
  - ✓ Movilidad, flexibilidad
  - ✓ Estética, rapidez de instalación, coste ...

Mbps: Mega bits por segundo

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

Nivel físico en 802.11

- **Infrarrojos**:
  - Solo válido en distancias muy cortas y en la misma habitación (802.11)
- **Radio**
  - Radio FHSS (Frequency Hoping Spread Spectrum):
    - Sistema de bajo rendimiento, poco utilizado actualmente.(802.11)
  - **Radio DSSS** (Direct Sequence Spread Spectrum):
    - Buen rendimiento y alcance. **El más utilizado hoy en día.** (802.11-/b/g)
  - Radio OFDM (Orthogonal Frequency Division Multiplexing):
    - Usado para altas velocidades (>11 Mb/s) en la banda de 5 GHz (802.11a/h). Emplea una técnica parecida a ADSL para aprovechar el espectro lo mejor posible
- Los equipos que utilizan diferentes sistemas no pueden interoperar entre sí (salvo que tengan varias etapas de radio).
- Dentro de un mismo sistema hay auto-negociación de la velocidad y funcionalidades

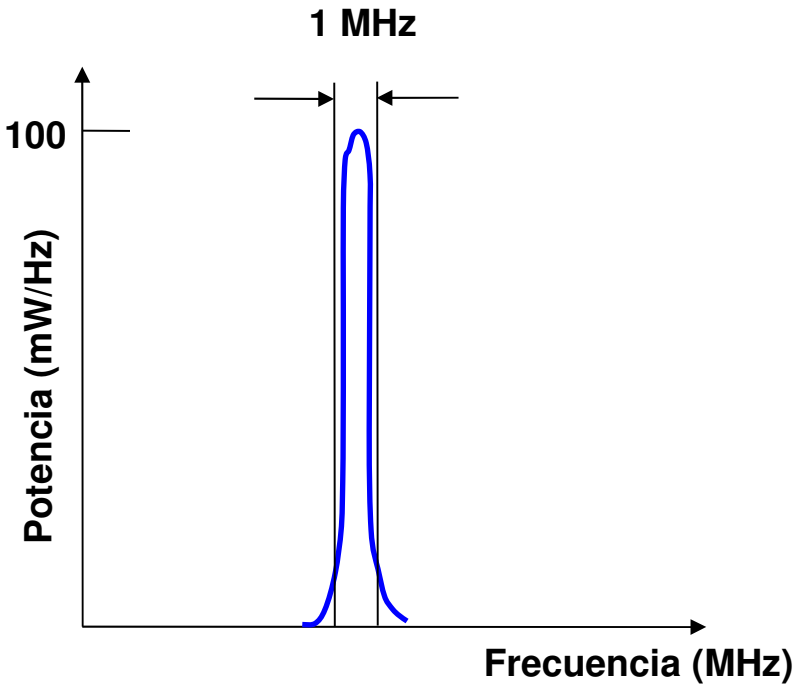
Nivel físico en 802.11

Medio físico	Infrarrojos	FHSS	DSSS	OFDM
Banda	850 – 950 nm	2,4 GHz	2,4 GHz	5 GHz
Velocidades* (Mb/s)	**1** y 2 (802.11)	**1** y 2 (802.11)	**1**, **2** (802.11) **5.5**, **11** (802.11b) **6**, 9, **12**, 18, 22, **24**, 33, 36, 48 y 54 (802.11g)	**6**, 9, **12**, **18**, 24, 36, 48 y 54 (802.11a/h)
Utilización	Muy rara	Poca. Sistema antiguo, a extinguir	Mucha	Poca
Características	No atraviesa paredes	Sensible a interferencias Bluetooth y hornos microondas	Buen rendimiento y alcance	Solo disponible en América, Japón, Singapur y Taiwan

Espectro Disperso

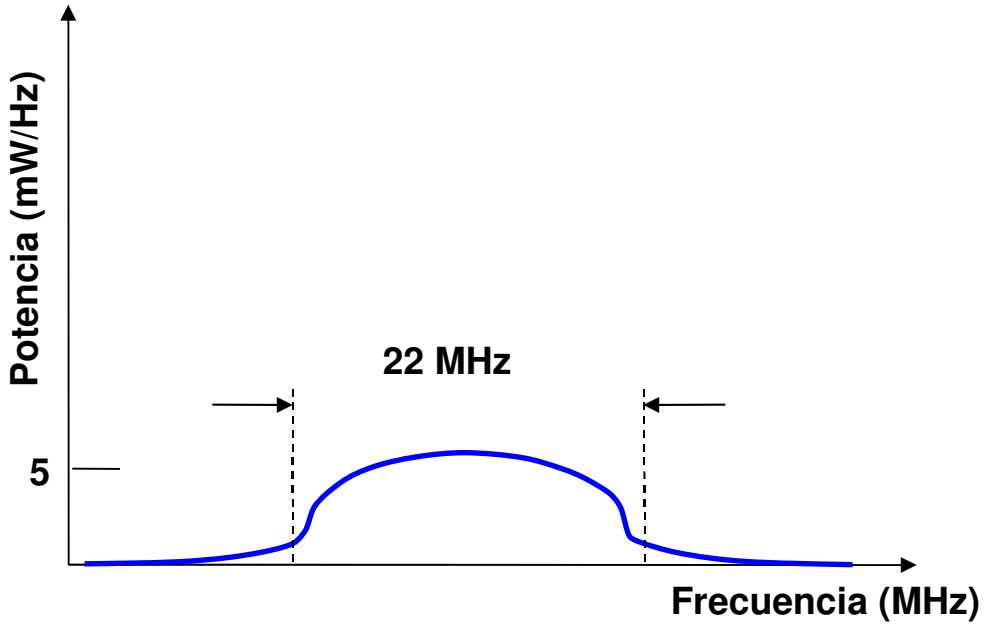
- El “espectro disperso” se utiliza para reducir la interferencia en la banda de 2,4 Ghz en las emisiones de más de 1 mW
- Hay dos formas de hacer una emisión de espectro disperso:
  - *Frecuency Hopping (salto de frecuencia)*.
    - El emisor va cambiando continuamente de canal.
    - El receptor ha de seguirlo.
  - *Direct Sequence (secuencia directa)*.
    - El emisor emplea un canal muy ancho.
    - La potencia de emisión es similar al caso anterior, pero al repartirse en una banda mucho mas ancha la señal es de baja intensidad (poca potencia por Hz).

Frequency Hopping *vs* Direct Sequence



Frequency Hopping

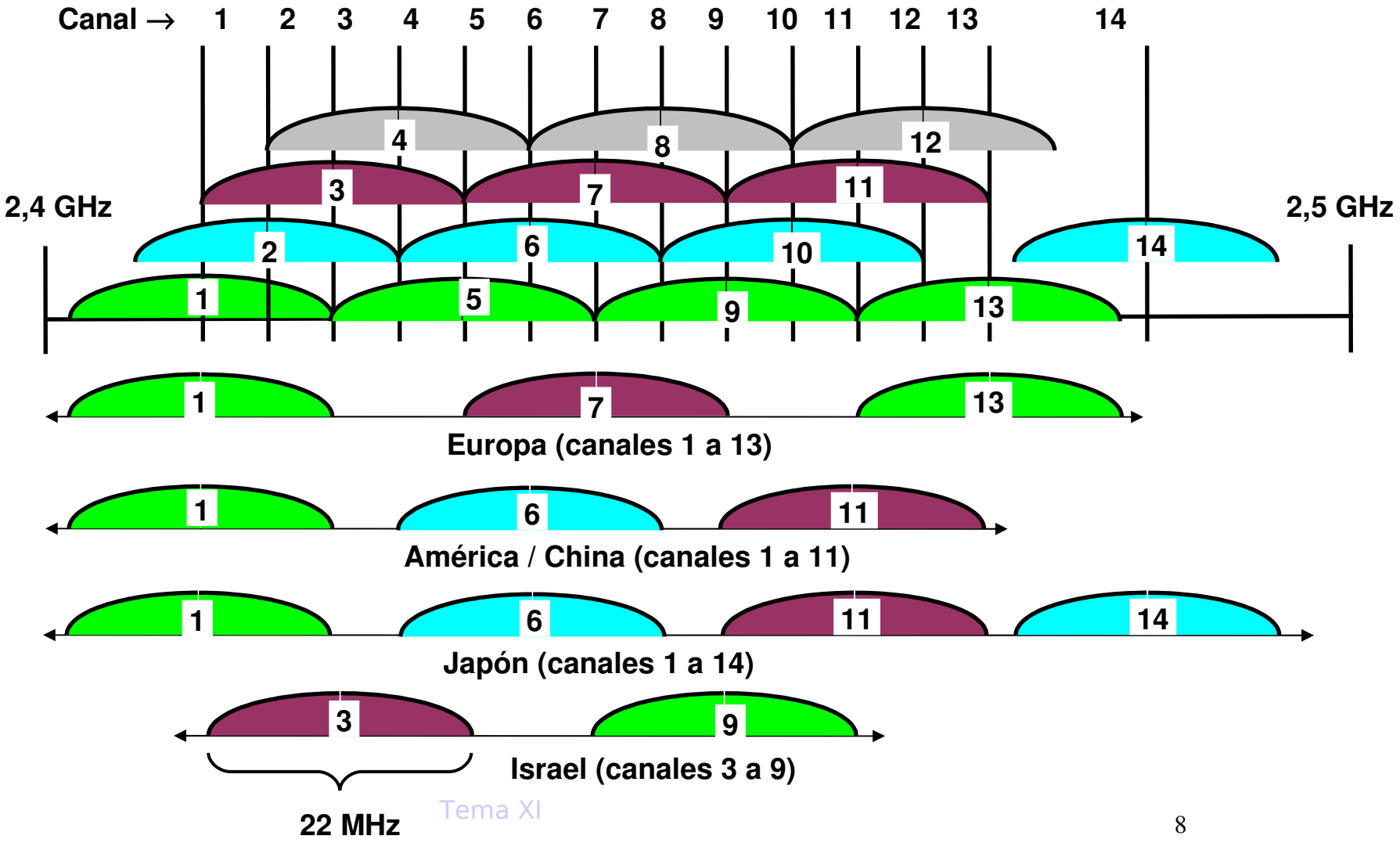
Señal concentrada, gran intensidad
Elevada relación S/R
Área bajo la curva: 100 mW



Direct Sequence

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

Reparto de canales DSSS a 2,4GHz 802.11b/g



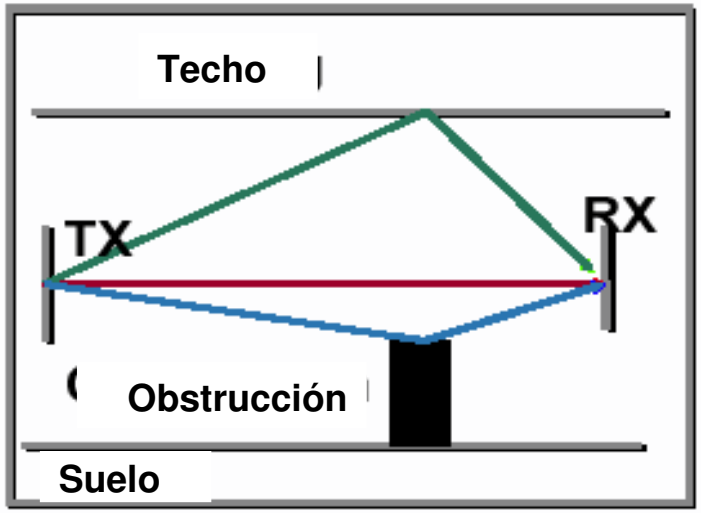
Canales DSSS simultáneos

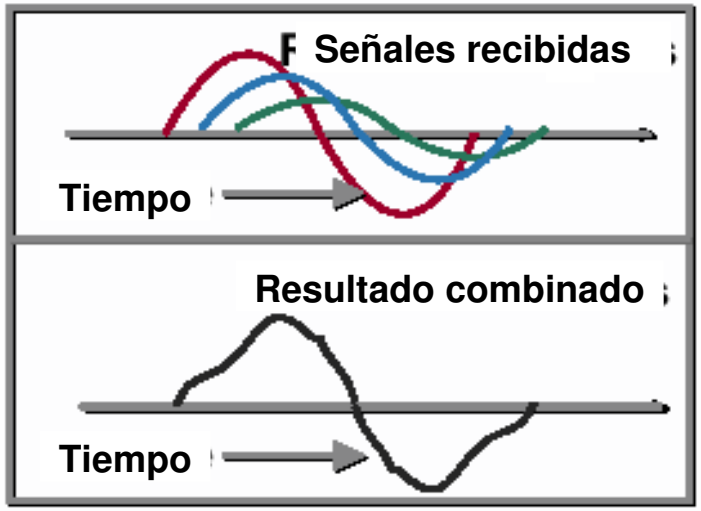
- Si se quiere utilizar más de un canal en una misma zona hay que elegir frecuencias que no se solapen.
  - El máximo es de tres canales:
    - América y China:
      - Canales 1, 6 y 11
    - Europa:
      - Canales 1, 7 y 13
- Con diferentes canales se pueden constituir LANs inalámbricas independientes en una misma zona

Posibles interferencias

- Externas:
  - Bluetooth transmite a 2,4 GHz por FHSS.
    - Interfiere menos con DSSS. Nada con 802.11a (5 GHz)
  - Los hornos de microondas (funcionan a 2,4 GHz) interfieren con FHSS.
    - A DSSS le afectan menos. Nada a 802.11a
  - Otros dispositivos que funciona en 2,4 GHz (teléfonos inalámbricos, mandos a distancia de puertas de garaje, etc.) tienen una potencia demasiado baja para interferir con las WLANs
  - En los sistemas por infrarrojos la luz solar puede afectar la transmisión
- Internas (de la propia señal):
  - Debidas a multitrayectoria (rebotes de la señal en paredes, techos, etc.)

Interferencia debida a la multitrayectoria





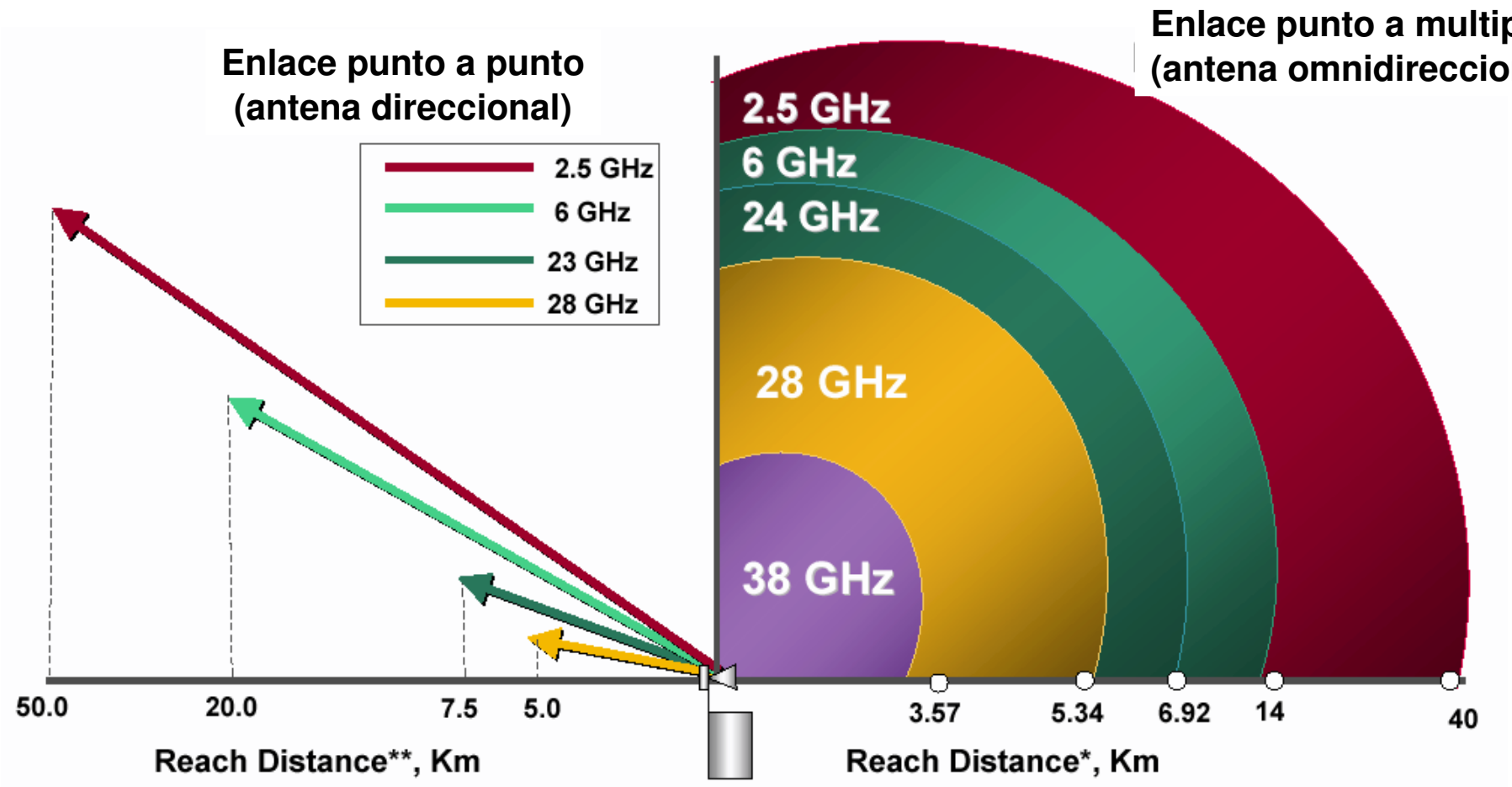
- Se produce interferencia debido a la diferencia de tiempo entre la señal que llega directamente y la que llega reflejada por diversos obstáculos.
- La señal puede llegar a anularse por completo si el retraso de la onda reflejada coincide con media longitud de onda.
  - En estos casos un leve movimiento de la antena resuelve el problema.
- FHSS es más resistente a la interferencia multitrayectoria que DSSS.
  - Este problema se resuelve con antenas diversidad

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 DSSS) 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
- Al resolver el problema de la interferencia multitrayectoria de DSSS el uso de FHSS ha caído en desuso

Alcance en función de la frecuencia

Las frecuencias altas se atenúan más.
Por tanto a mayor frecuencia menor alcance



Radiofrecuencias y Salud

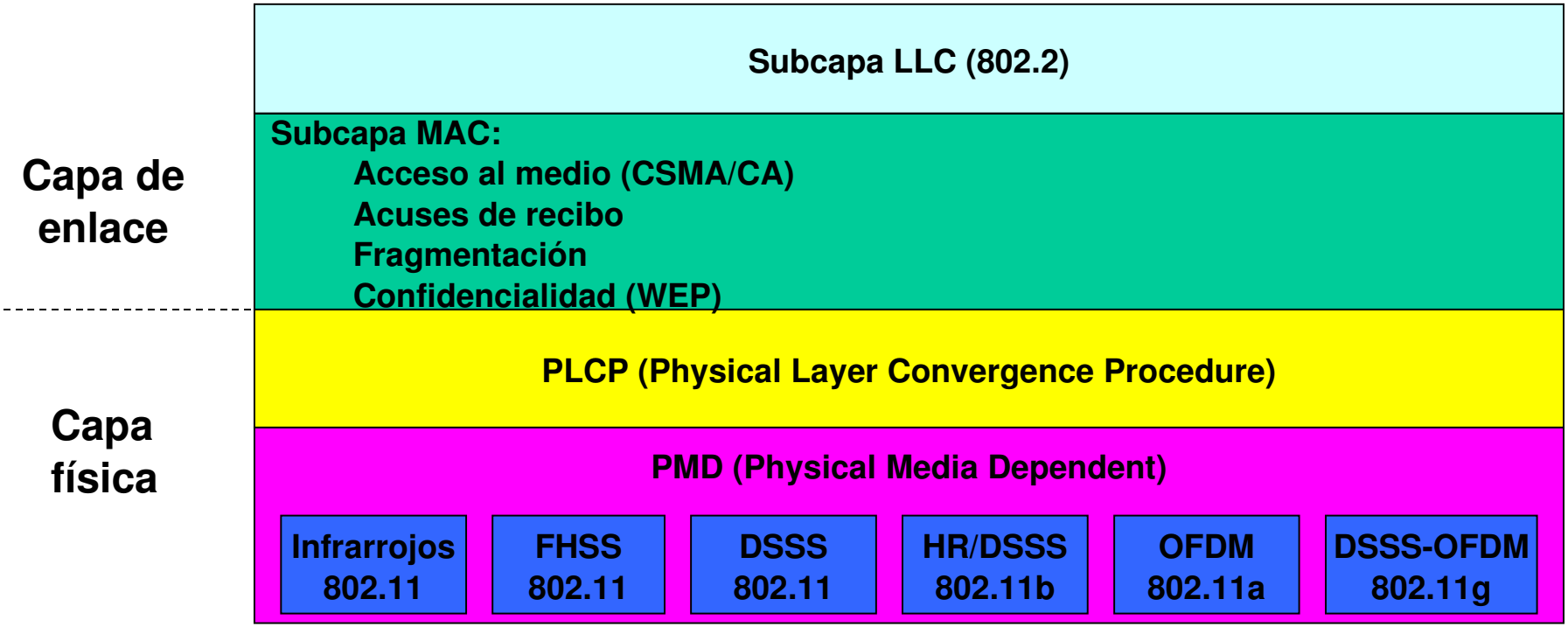
- La radiación electromagnética de 2,4 GHz es absorbida por el agua y la calienta (hornos de microondas).
  - Un emisor WLAN podría calentar el tejido humano, lo cual plantea posibles problemas de salud
    - La potencia radiada es tan baja (100 mW máximo) que el efecto es despreciable.
  - Es mayor la influencia de un horno de microondas en funcionamiento.
- Comparado con la telefonía móvil un terminal GSM transmite con más potencia (hasta 600 mW) y se tiene mucho más cerca del cuerpo normalmente (aunque GSM no emite en la banda de 2,4 GHz).
- Los equipos WLAN normalmente solo emiten cuando transmiten datos.
  - Un teléfono GSM emite siempre que está encendido.

Red Wi-FI

ESTANDAR 802.11

- Creada por los principales líderes de la industria inalámbrica a finales de los 90
- Objetivo:
  - ✓ Compatibilidad Ethernet Inalámbrica
- Misión:
  - ✓Certificar la ínter funcionalidad y compatibilidad de los productos de redes inalámbricas y
  - ✓Promover este estándar para la empresa y el hogar

Modelo de Referencia de 802.11



IEEE 802.11 Arquitectura (I)

Componentes de una WLAN

- ✓ Muy similares a una red cableada
  - Tarjetas de Red para los ordenadores
  - Puntos de Acceso, que actúan como concentradores y conectan si se desea a la red cableada
  - Repetidores, para amplificar la señal
  - Puentes (Bridges), para emitir la señal entre dos puntos

- Componentes de 802.11
  - ✓ Cliente (STA)
  - ✓ Punto de acceso (*Access Point* -AP)
  - ✓ Basic Service Set (BSS)
  - ✓ Extended Service Set (ESS)
  - ✓ Sistema de Distribución - Distribution System (DS)

Componentes de una WLAN (I)
Tarjeta WI-FI (TR)

- Tarjetas WIFI (TR)
  - ✓ Son equivalentes a una tarjeta de red normal, sólo que sin cables.
  - ✓ Su configuración a nivel de IP es EXACTAMENTE igual que una Ethernet.
  - ✓ Formato
    - PCMCIA, para portátiles,
    - USB
    - Otros formato PCI, en CompactFlash, Smart Card y similares
  - ✓ Las diferencias más importantes entre una WIFI y una Ethernet, son:
    - El cifrado de datos, el ESSID, el Canal,
    - y el ajuste de velocidad.

Componentes de una WLAN (II)
Puntos de Acceso

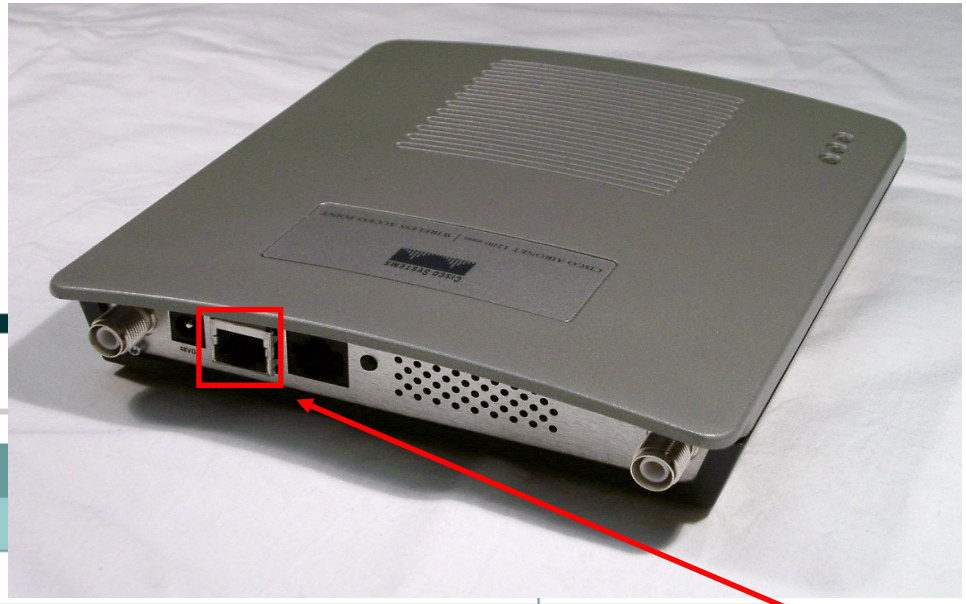
- Punto de acceso (*Access Point*) (PA)
  - ✓ Son el centro neurálgico de las redes inalámbricas
  - ✓ Coberturas omnidireccionales en torno a los 300 metros en exterior
  - ✓ Permiten conectar dispositivos entre sí, y con la red cableada


U.S.Robotics
U.S.Robotics
802.11g 54Mbps Router
100
10
1
2
3
4
100
10
802.11g
U.S.Robotics
54Mbps USB Adapter

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
- El BSSID (*BSS Identifier*).
  - ✓ Es la dirección MAC de la interfaz inalámbrica
  - ✓ Se utiliza como identificador del BSS que corresponde a ese AP
  - ✓ Este dato es fundamental para el funcionamiento de una red 802.11
- 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
- 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

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

Componentes de una WLAN (III)

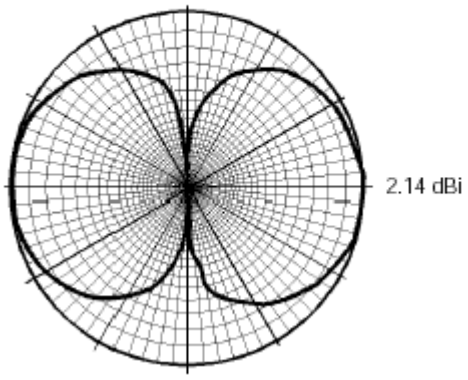
- Repetidores
  - ✓ Incrementan la cobertura

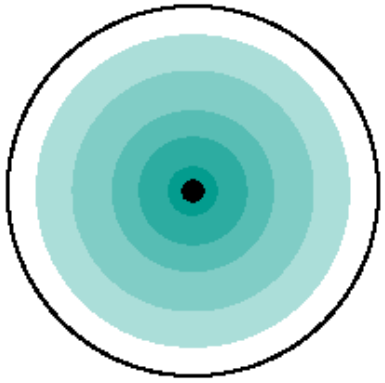
Dispositivos Wireless
Antenas

- Las antenas Direccionales :
  - ✓ Envían la información a una cierta zona de cobertura, a un ángulo determinado,
  - ✓ Su alcance es mayor
  - ✓ Tipos:
    - Las de Rejilla o Grid
    - Las Yagi
    - Las parabólicas
    - Las "Pringles" y
    - Las de Panel
- Las antenas Omnidireccionales
  - ✓ Envían la información teóricamente a los 360 grados pero sólo sobre el plano perpendicular de la antena.
  - ✓ El alcance de estas antenas es menor que el de las antenas direccionales.

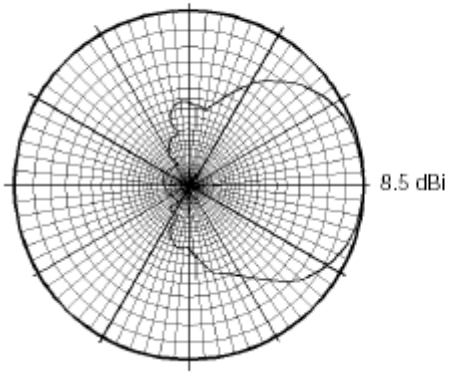
Antenas más habituales

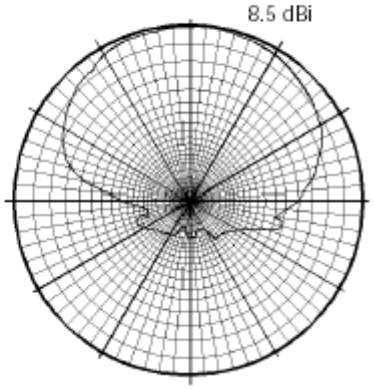
Antena dipolo omnidireccional de 2,14 dBi de ganancia





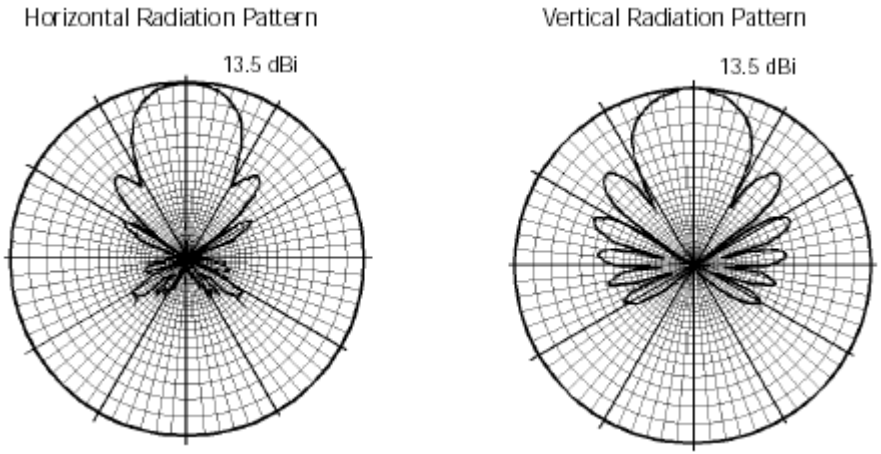
Antena de parche para montaje en pared interior o exterior (8,5 dBi) Alcance: 3 Km a 2 Mb/s, 1 Km a 11 Mb/s



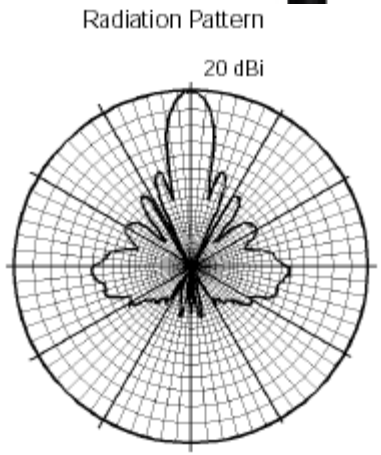


Antenas de alta ganancia

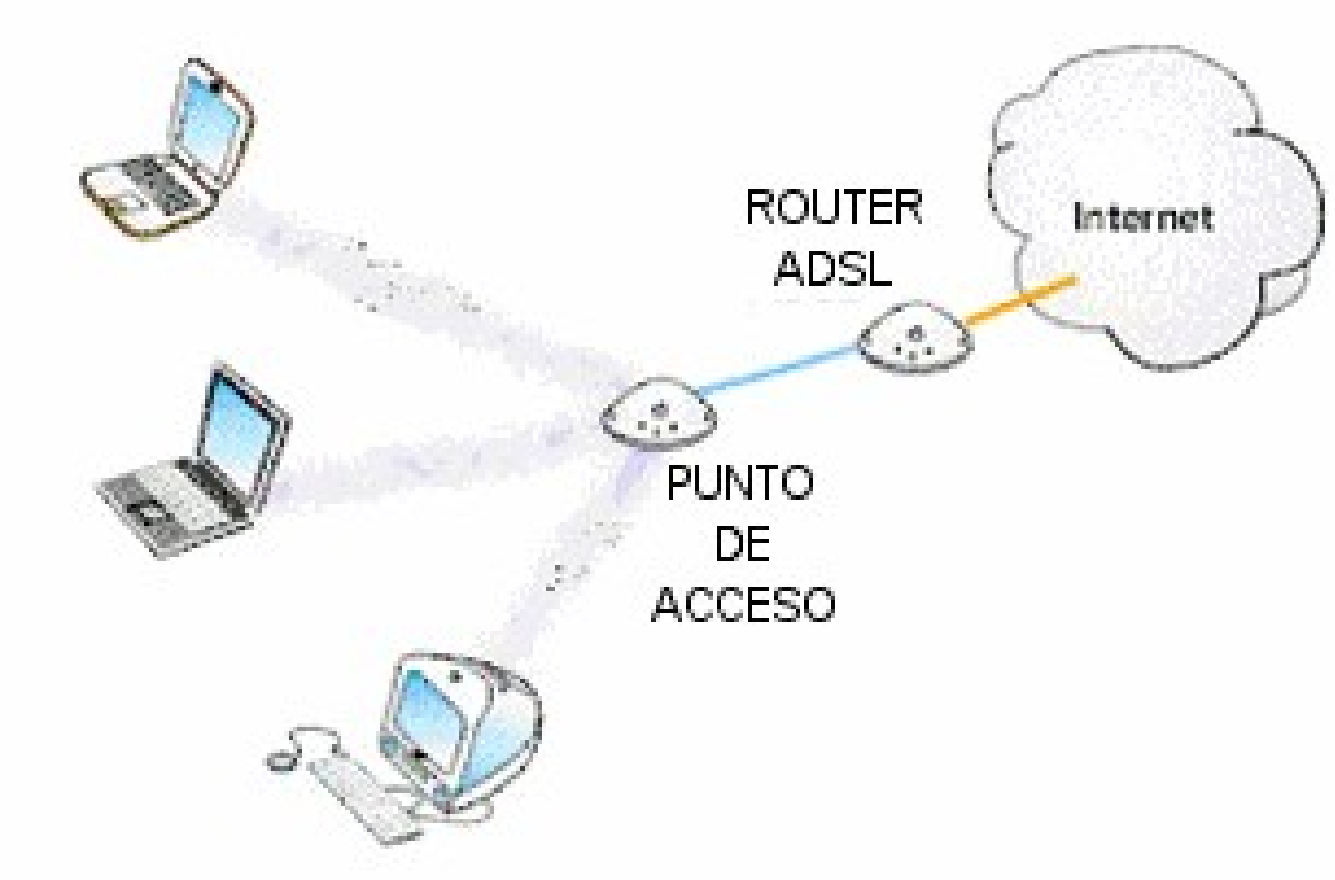
Antena Yagi exterior (13,5 dBi)
Alcance: 6 Km a 2 Mb/s, 2 Km a 11 Mb/s



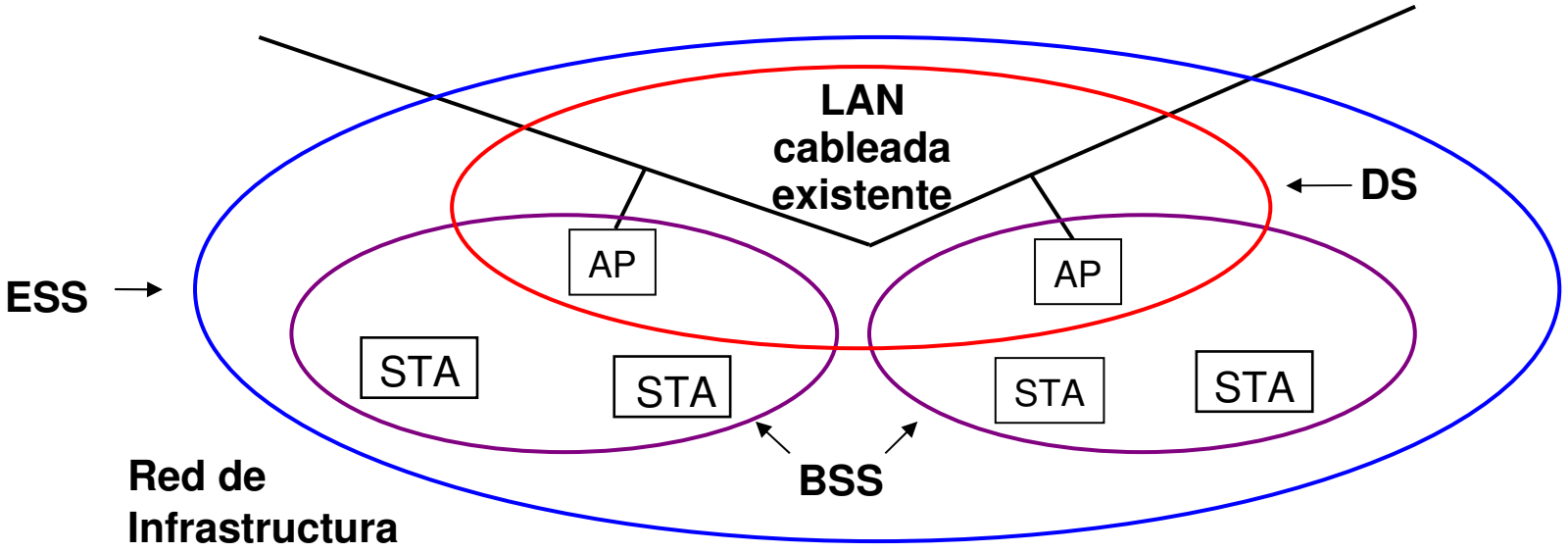
Antena Parabólica exterior (20 dBi)
Alcance: 10 Km a 2 Mb/s, 5 Km a 11 Mb/s

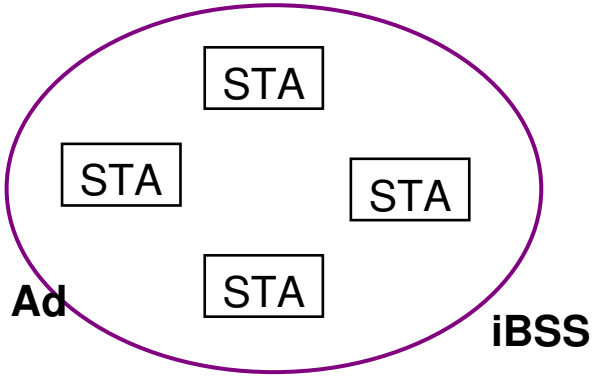


Elementos necesarios



Arquitectura de 802.11 (II)





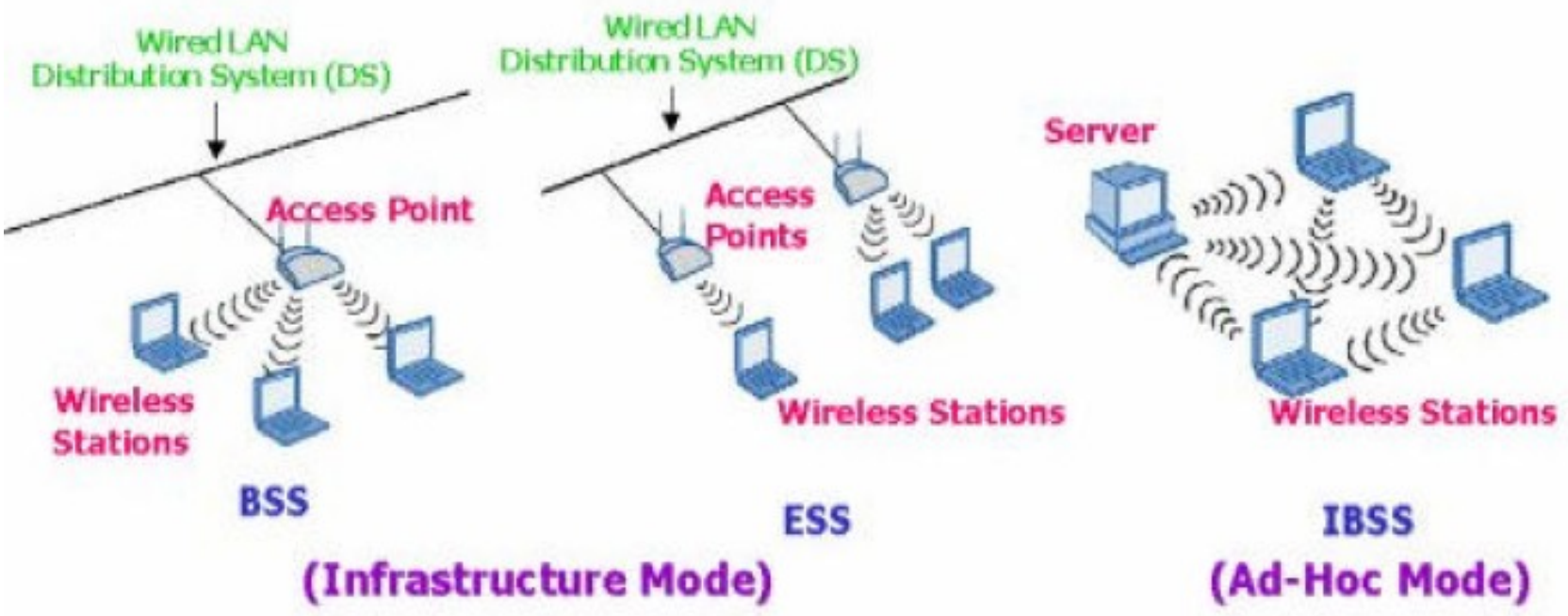
STA: Station
AP: Access Point
DS: Distribution System
BSS: Basic Service Set
ESS: Extended Service Set

Modos de Operación (Funcionamiento)

- Ad-hoc
  - ✓ Los ordenadores de la red trabajan "par a par"
    - Todos reciben los paquetes de todos y envían sus propios paquetes a todos los ordenadores de la red.
- Modo Managed
  - ✓ Existe un servidor independiente.
    - Es el modo en el que el TR se conecta al AP para que éste último le sirva de concentrador.
    - El TR sólo se comunica con el AP.
- Modo Master
  - ✓ Este modo es el modo en el que trabaja el PA, pero en el que también pueden entrar los TRs si se dispone del firmware apropiado o de un ordenador que sea capaz de realizar la funcionalidad requerida.
  - ✓ Soportan roaming
    - Los clientes pueden estar en movimiento a ir cambiando de punto de acceso de acuerdo a la potencia de la señal
  - ✓ Suelen ofrecer servicios de enrutado IP, servidor DHCP y *bridging* sobre una Ethernet.

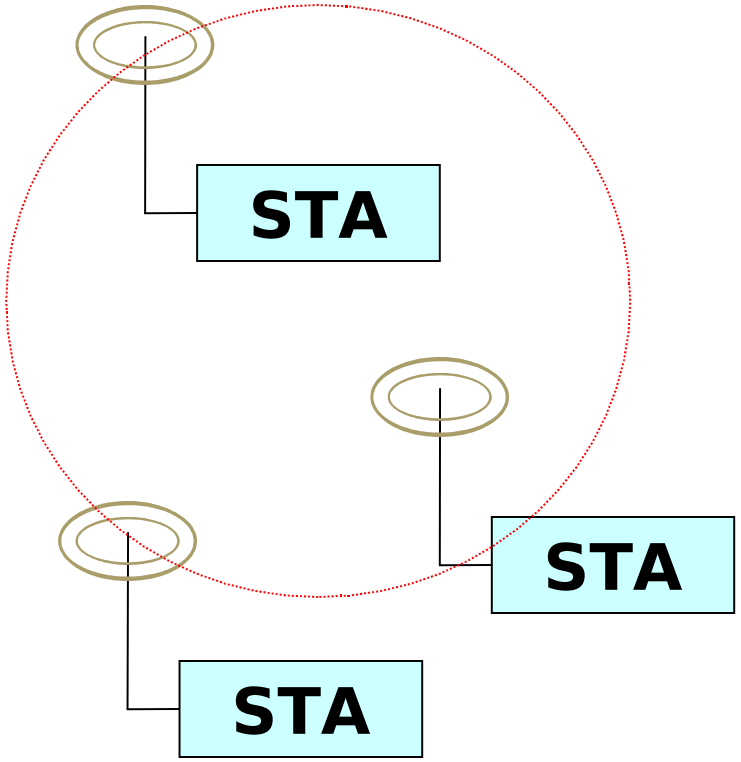
Tipos de redes 802.11 (topologías)

- **Redes ad hoc**
  - Sin puntos de acceso (Aps).
  - IBSS (*Independent BSS)*
    - Los ordenadores se comunican directamente
- **Redes de infraestructura**
  - Con al menos un AP
    - Es bastante más eficaz que AD-HOC
  - 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)*

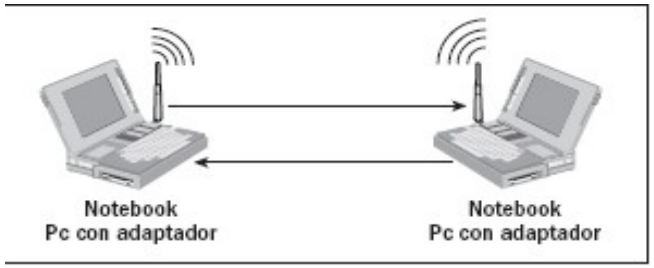

Wired LAN
Distribution System (DS)
Access Point
Wireless
Stations
BSS
Wired LAN
Distribution System (DS)
Access
Points
Wireless Stations
ESS
(Infrastructure Mode)
Server
Wireless Stations
IBSS
(Ad-Hoc Mode)

IBSS (*Independent Basic Service Set*)
red ad-hoc

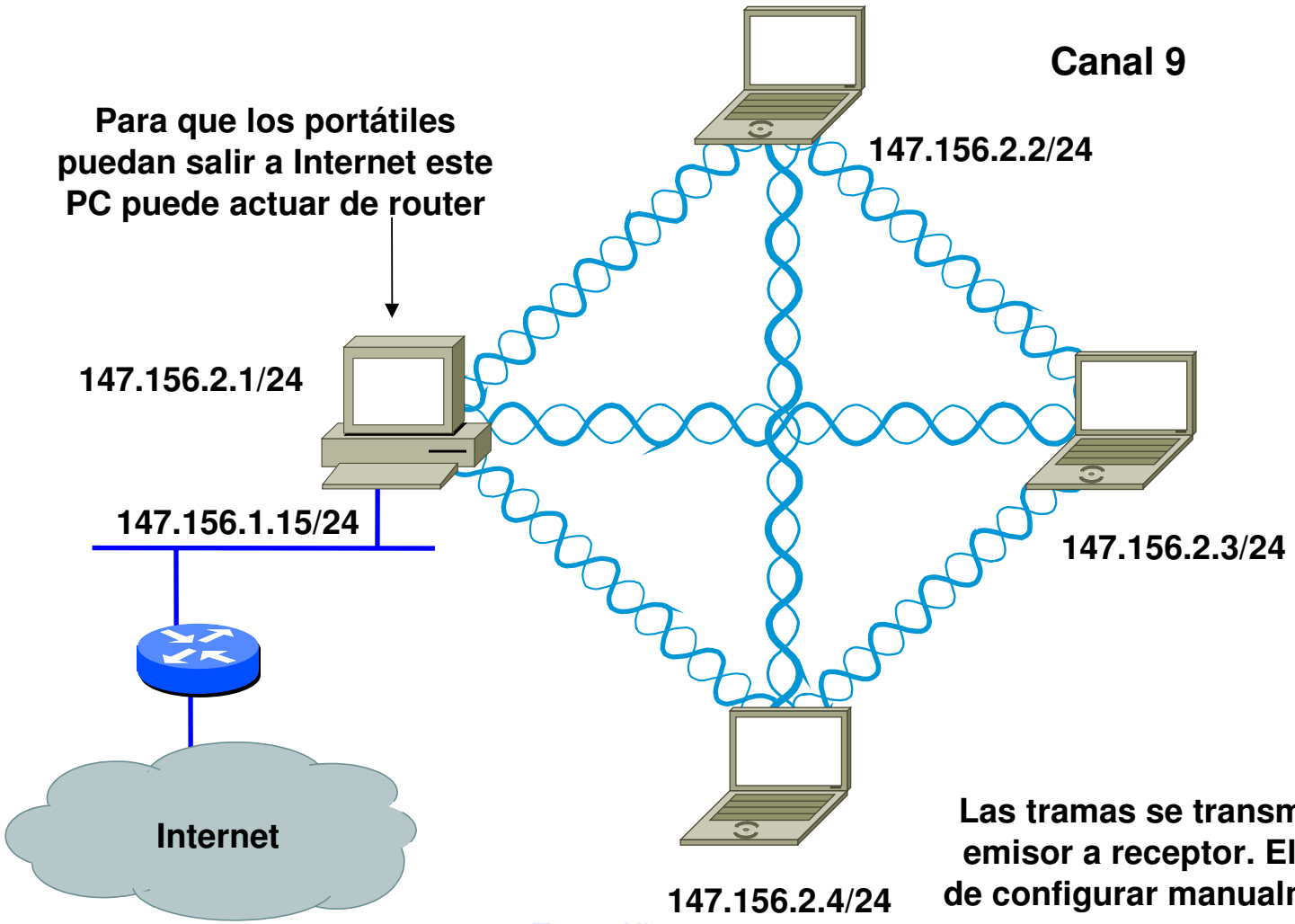
- Una IBSS es un conjunto de estaciones que
  - ✓ No tiene una infraestructura de conexión y
  - ✓ Que esta compuesto por más de dos estaciones inalámbricas
- Es una BSS sin puntos de acceso
- Sin conexiones a otras redes
- Las redes *ad-hoc* satisfacen las necesidades de usuarios que ocupan un área de cobertura pequeña como un aula de clases, un piso de un hospital, etc.



Ejemplos de IBSS (Ad-Hoc)



Otro ejemplo de Red ‘ad hoc’ (sin APs)



Tarjeta PCI

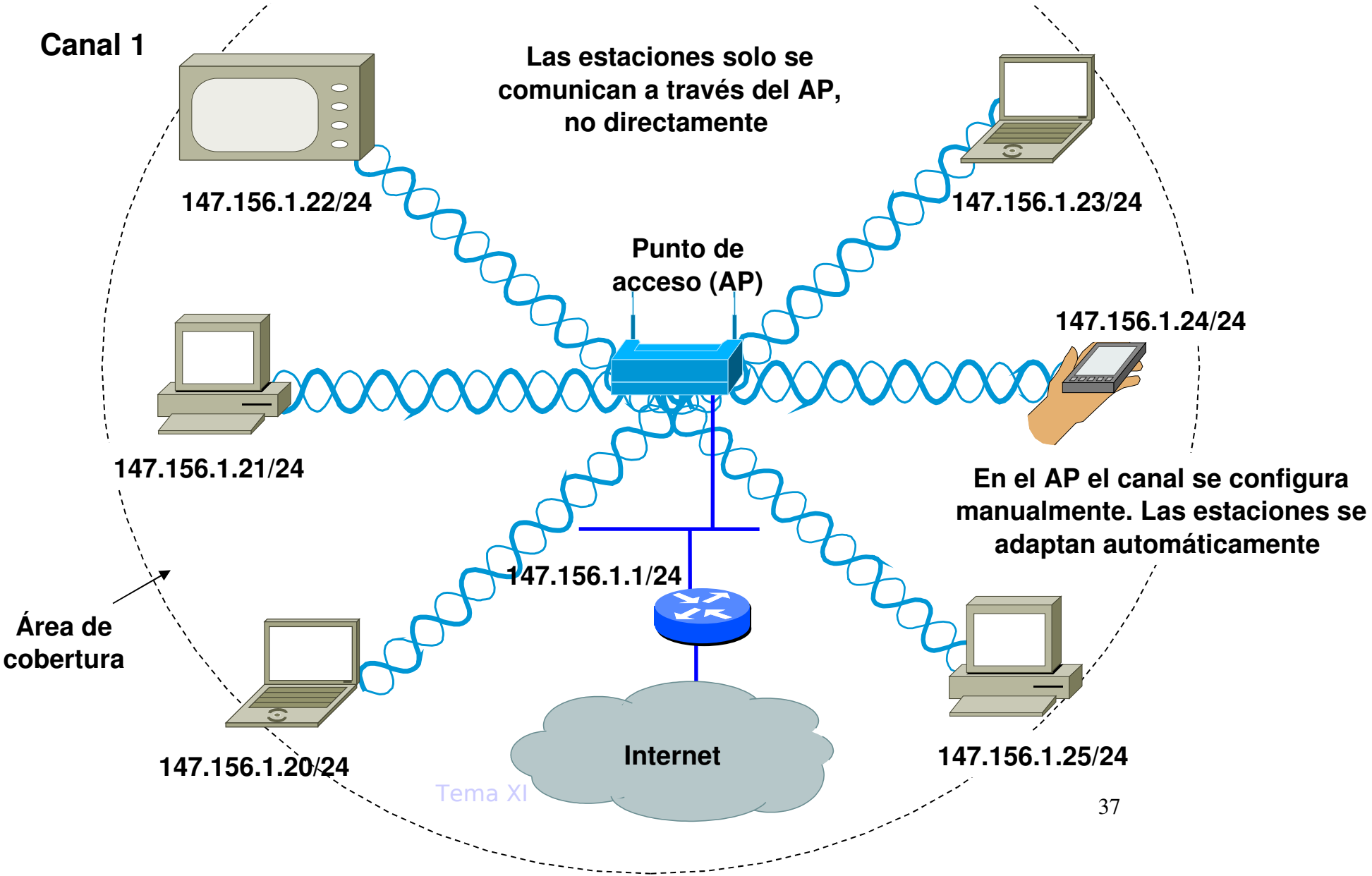
Tarjeta PCMCIA

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

BSS
Modo infraestructure

- Es una BSS con un Punto de Acceso (*access point* – AP)
  - ✓ Se identifica por su SSID
- Elementos
  - ✓ El Punto de Acceso (AP)
    - Funciona como un concentrador inalámbrico de la red WLAN
      - – Todo el tráfico pasa a su través
    - Extienden una red LAN
    - Hace de Puente entre la LAN y las estaciones inalámbricas
    - Puede servir como repetidor en la conectividad de las dos redes WLAN
    - Roaming:
      - – Posibilidad de que una estación se asocie a otros AP
    - Interfaz web para su configuración
    - Desplegando varios se puede cubrir un gran área
  - ✓ Estaciones:
    - PCs, portátiles, PDAs, etc.

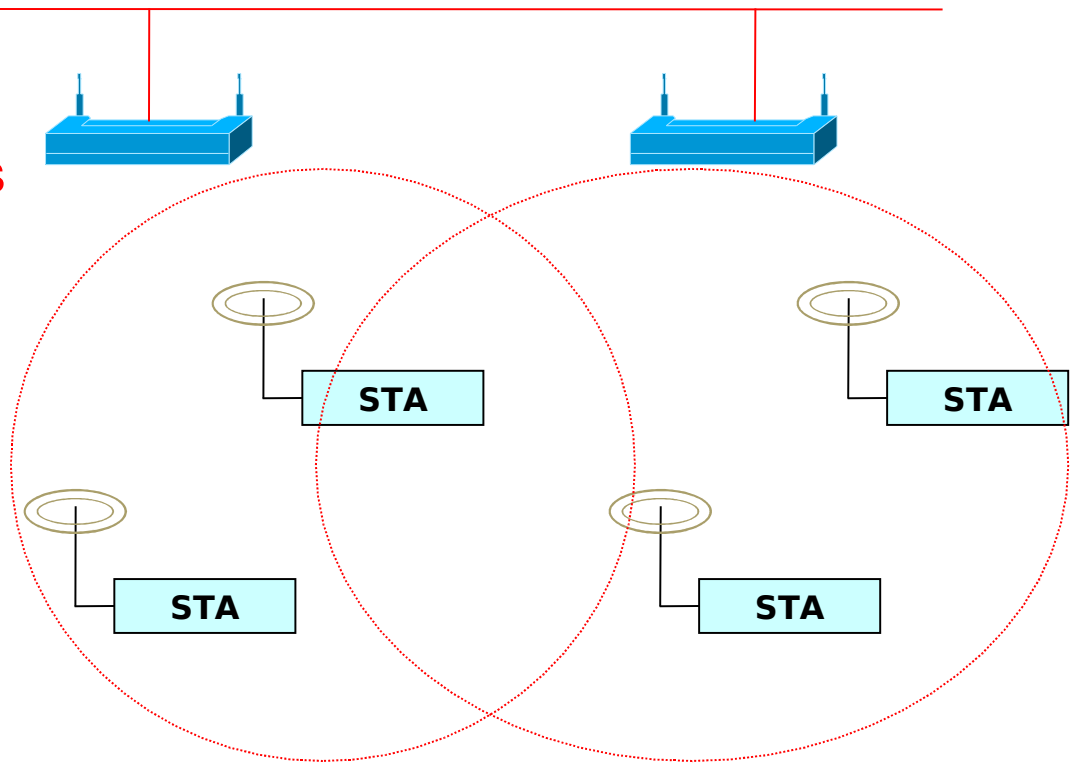
Ejemplos de BSS (*Basic Service Set*)



Ejemplo de BSS (Infraestructura)

Extended Service Set (ESS)

- Es un conjunto de dos o más BSS, es decir dos o más APs, interconectados de alguna manera a nivel 2.
    - Dos o más BSS conectadas por un backbone
  - ✓ La red que interconecta los APs se denomina el DS (*Distribution System*)
  - ✓ Se vé como una misma red a nivel LLC (802.2)
- Los APs se envían información a través de la red cableada o la red inalámbrica para permitir movilidad de las estaciones o STAs

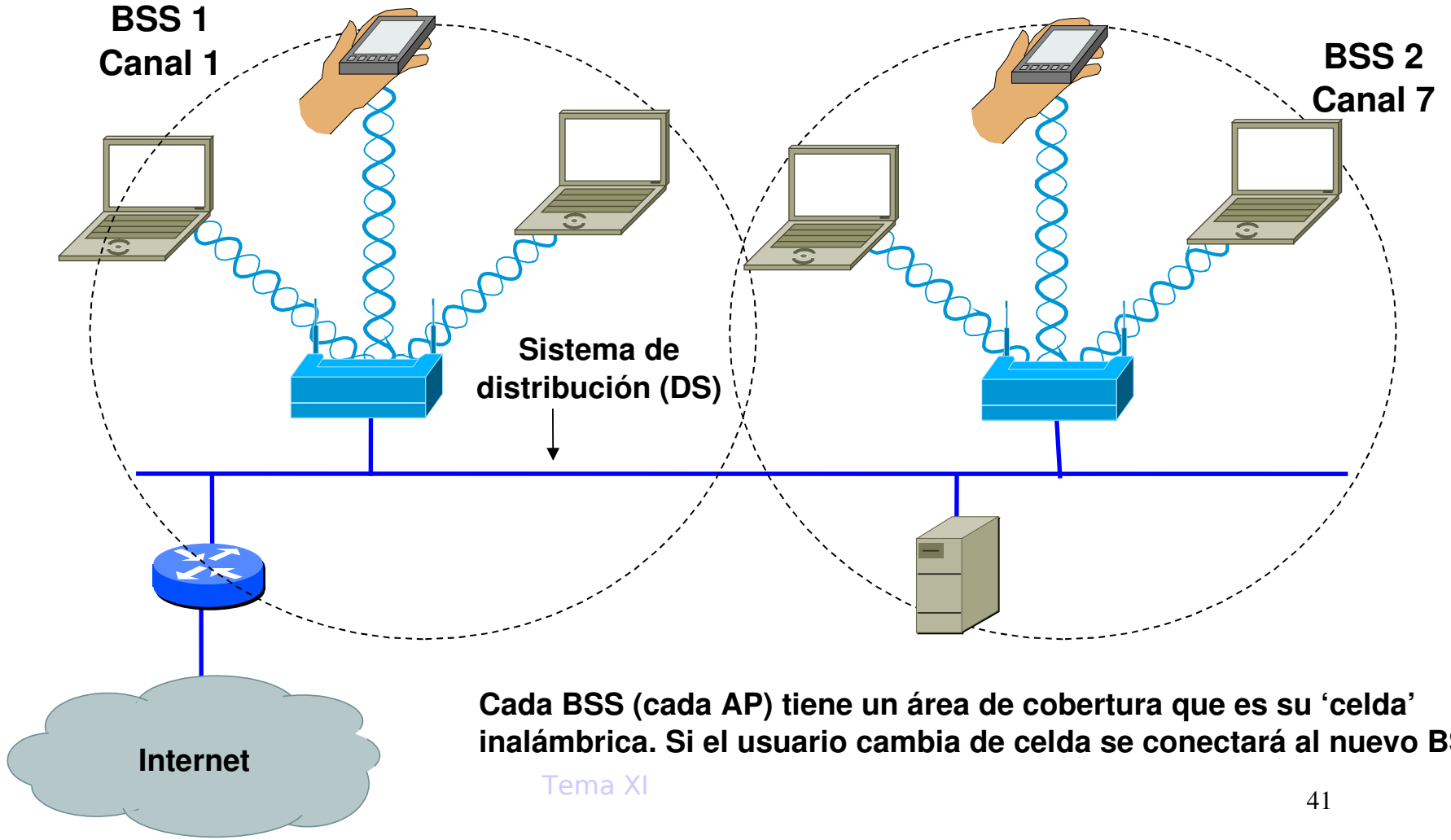


Sistema de Distribución
Distribution System (DS)

- El mecanismo que permite a los puntos de acceso comunicarse entre si y con una infraestructura cableada (si existe)
  - ✓ El DS es sencillamente la forma en que se interconectan varios puntos de acceso (o AP) para permitir la interconexión de las estaciones inalámbricas registradas en los distintos APs
- Es el Backbone de la WLAN
- Debe contener redes cableadas e inalámbricas
- El AP determina en función del destinatario a donde transmitir:
  - ✓ A otra estación del mismo BSS
  - ✓ Al DS de otro AP (ej.,para comunicar con otro BSS)
  - ✓ A la infraestructura cableada para un destinatario que no pertenece al ESS

Ejemplo de 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

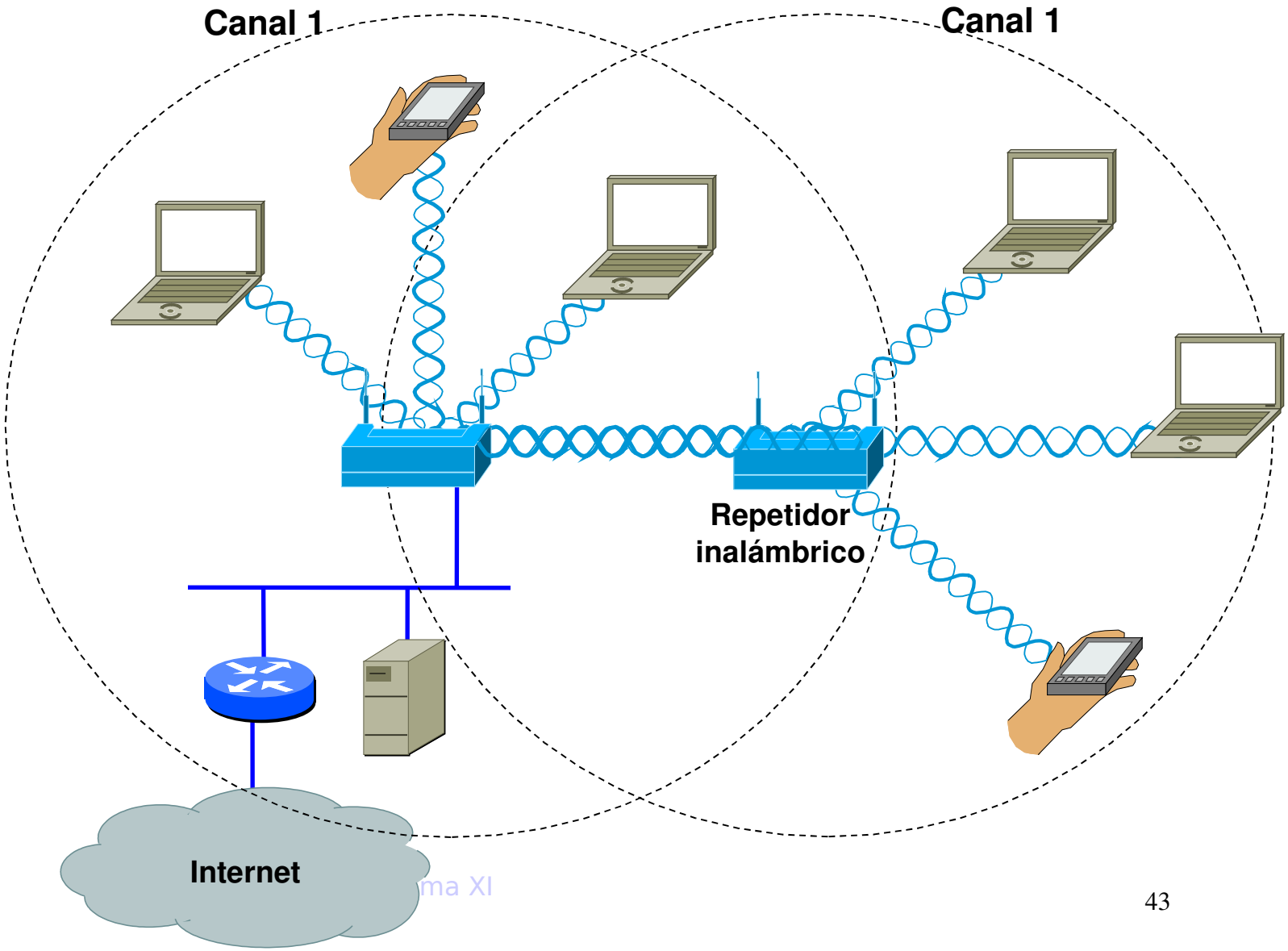


Cada BSS (cada AP) tiene un área de cobertura que es su 'celda' inalámbrica. Si el usuario cambia de celda se conectará al nuevo BSS.

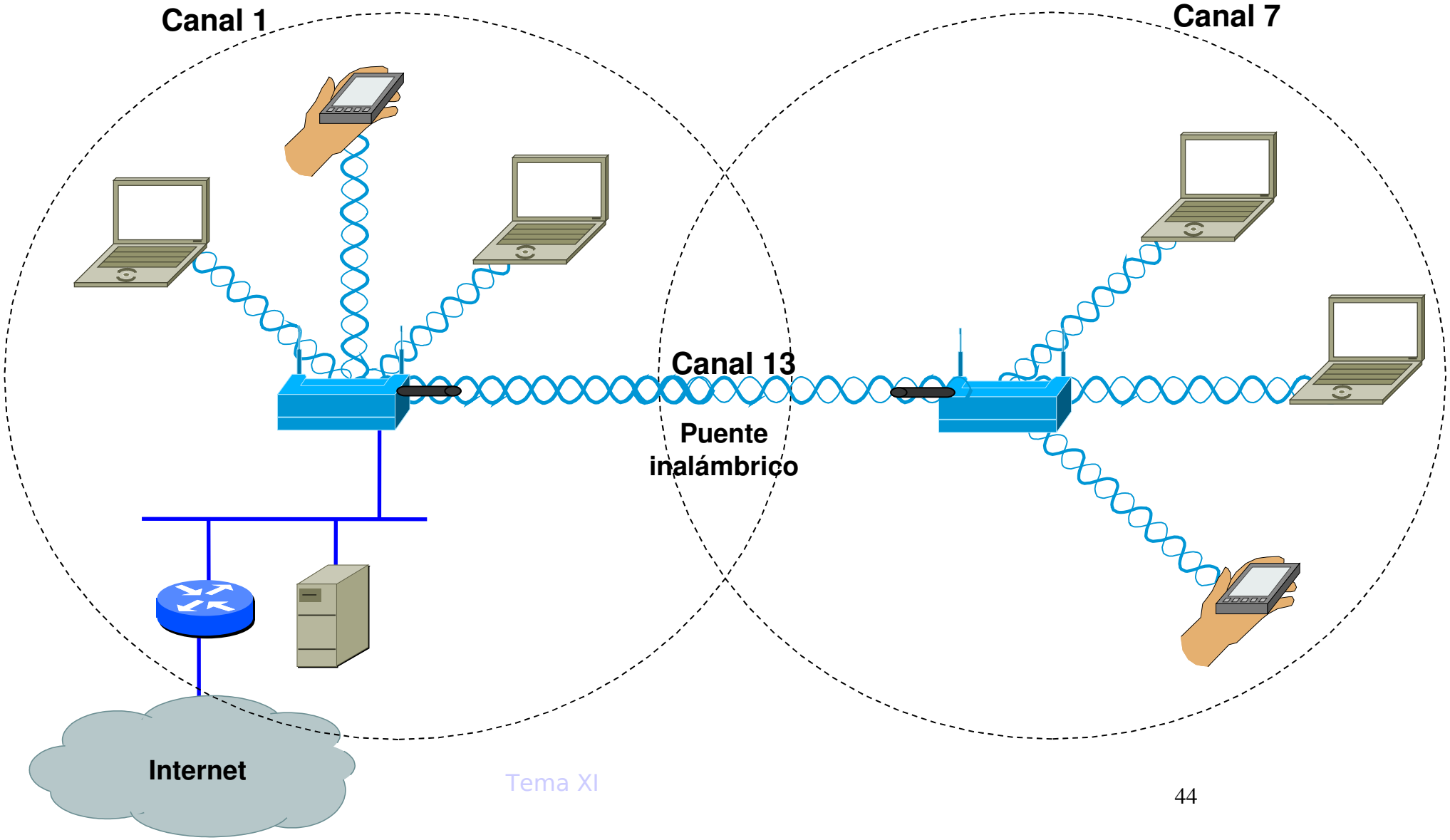
Sistema de distribución inalámbrico DSI o WDS (Wireless Distribution System)

- Es posible interconectar APs mediante un sistema de distribución inalámbrico (WDS) mediante "canales punto a punto" y
- Hacer "*bridging*" a Nivel 2 entre todas las estaciones registradas en los puntos de accesos interconectados mediante WDS.

Ejemplo de en ESS con DS sin cables (WDS)con un único canal



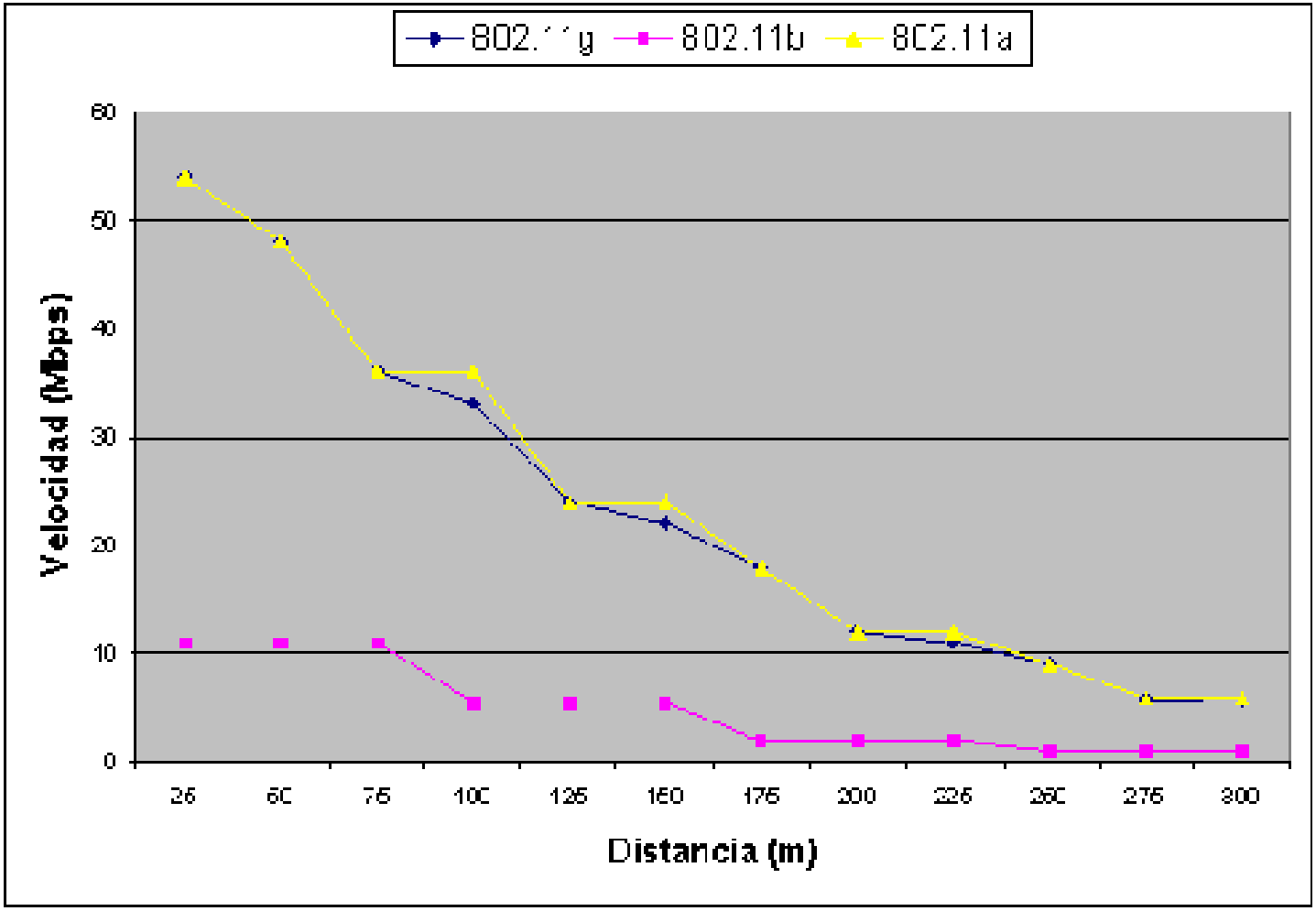
Ejemplo de DS sin cables (WDS) con un canal dedicado



Alcance de la red

- Cuando un TR se conecta a un PA se ve afectado principalmente por los siguientes parámetros:
  - ✓ Velocidad máxima del PA
    - Normalmente en 802.11g será de 54Mbps
  - ✓ Distancia al PA
    - A mayor distancia menor velocidad
  - ✓ Elementos intermedios entre el TR y el PA
    - Las paredes, campos magnéticos o eléctricos u otros elementos interpuestos entre el PA y el TR modifican la velocidad de transmisión a la baja
  - ✓ Saturación del espectro e interferencias
    - Cuantos más usuarios inalámbricos haya en las cercanías más colisiones habrá en las transmisiones por lo que la velocidad se reducirá
    - Esto también es aplicable para las interferencias.

Relación velocidad/distancia



Conectividad en redes 802.11
EL SSID

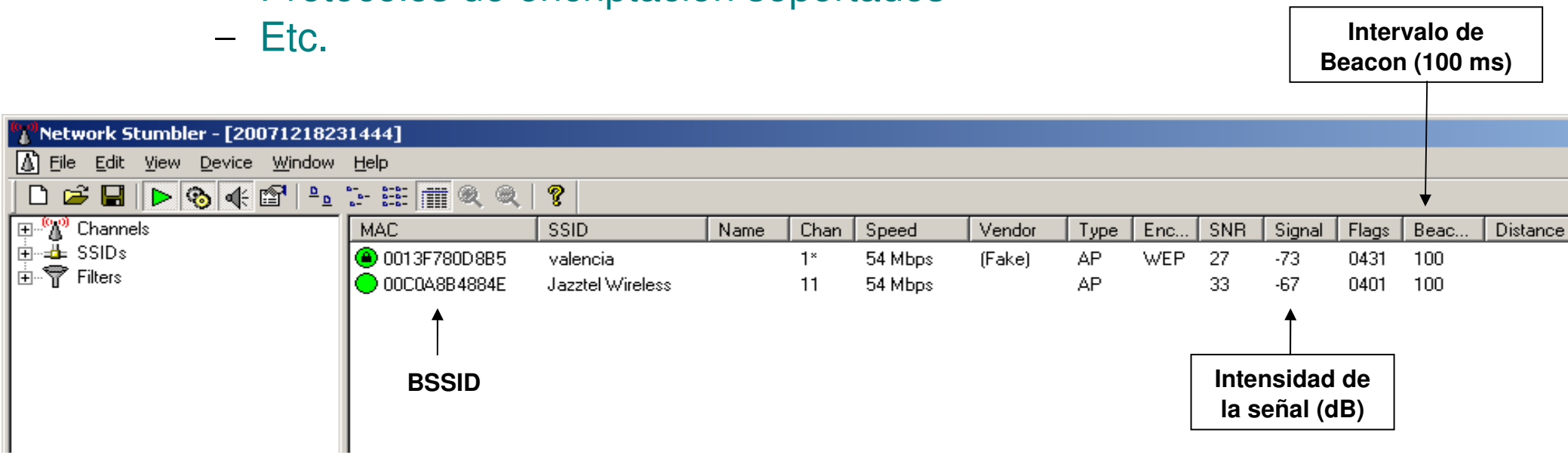
- El SSID (*Service Set Identifier*)
  - Es el identificador de la red
    - Cada red inalámbrica (ad hoc, BSS o ESS) se identifica por un SSID
    - Cuando el SSID corresponde a un ESS a veces se denomina ESSID (*Extended Service Set Identifier)*
  - ✓ Es una cadena de 32 caracteres máximo que identifica a cada red inalámbrica.
    - 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
  - ✓ CNAC (Closed Network Access Control).
    - Impide que los dispositivos que quieran unirse a la red lo hagan si no conocen previamente el SSID de la misma.
    - Los TRs deben conocer el nombre de la red para poder unirse a ella.

Difusión del SSID

- Los APs difunden periódicamente unos mensajes difusión (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
- Las estaciones, además de esperar a recibir "*beacons*", 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)
- Cualquier estación que pretenda participar en una red debe configurarse con el SSID correcto

Escaneo activo: programa NetStumbler

- NetStumbler envía un “ t” con el SSID broadcast por cada canal de radio. A continuación analiza los “probe response” recibidos
- De esta forma ‘descubre’ todos los APs, excepto aquellos que han sido configurados para ocultar su SSID
- Tanto los “beacon” como los “probe response” contienen información del AP:
  - Su BSSID y su SSID
  - Velocidades soportadas
  - Protocolos de encriptación soportados
  - Etc.



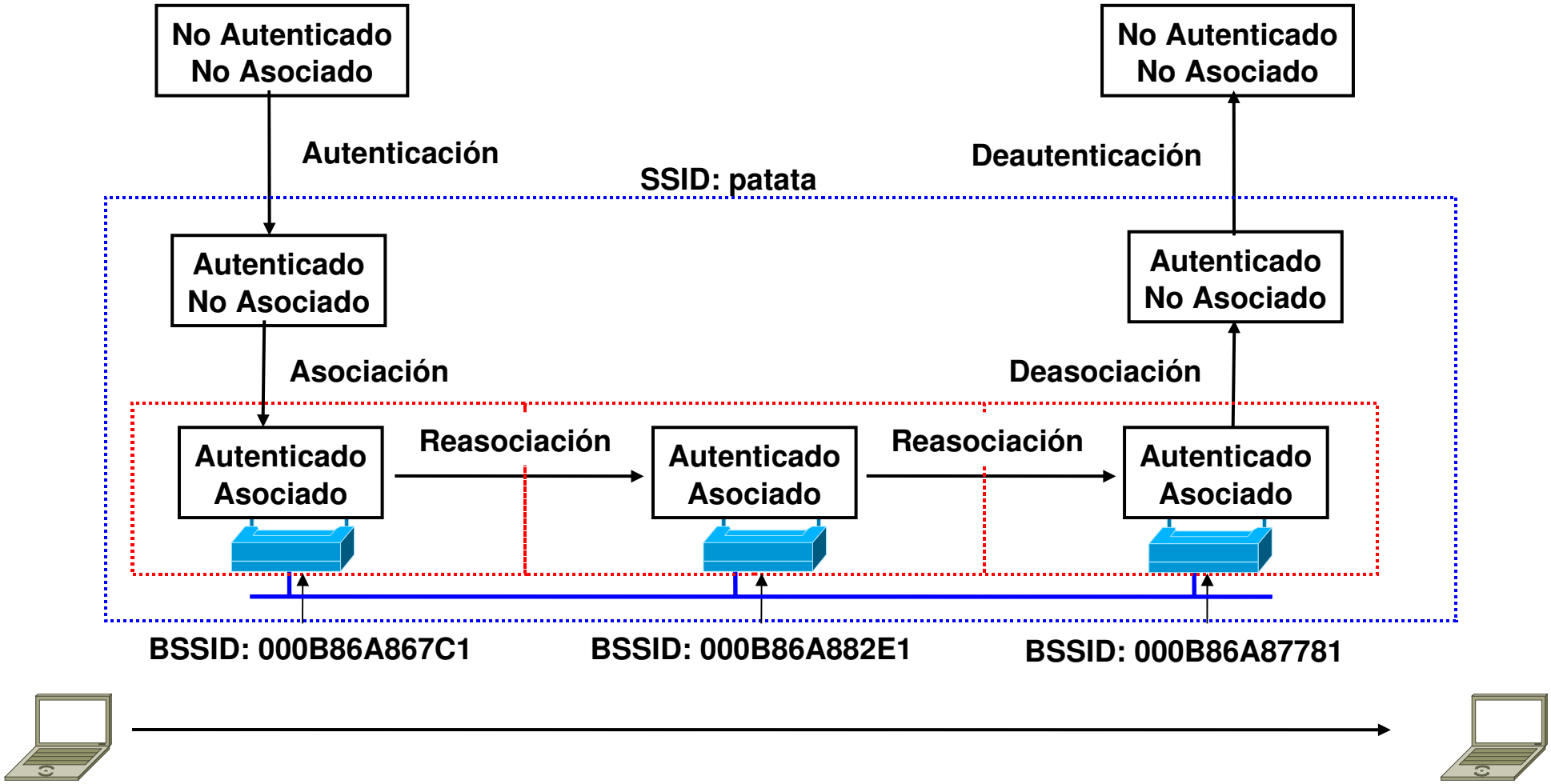
Seguridad Wireless

- Las redes inalámbricas están mucho más expuestas que las LANs normales a problemas de seguridad
  - ✓ Todo el tráfico es accesible a un atacante
- Sniffing
  - ✓ El tráfico de redes inalámbricas puede espiarse con mucha más facilidad que en una LAN
  - ✓ Basta con disponer de un portátil con una tarjeta inalámbrica
  - ✓ El tráfico que no haya sido cifrado, será accesible para el atacante
- Análisis de tráfico
  - ✓ El atacante obtiene información por el mero hecho de examinar el tráfico y sus patrones:
    - A qué hora se encienden ciertos equipos, cuánto tráfico envían, durante cuánto tiempo, etc.

Servicios de seguridad necesarios

- Autenticación:
  - ✓ Identificación con un grado aceptable de confianza de los usuarios autorizados
- Confidencialidad:
  - ✓ La información debe ser accesible únicamente a las personas autorizadas
- Integridad:
  - ✓ La información debe mantenerse completa y libre de manipulaciones fortuitas o deliberadas, de manera que siempre se pueda confiar en ella.
- Las estaciones para integrarse en una red inalámbrica deben de:
  - ✓ 1º.- Autenticarse
    - La autenticación se hace con un determinado SSID
  - ✓ 2º.- Asociarse a un Punto de Acceso
    - La asociación se hace con un determinado BSSID

Proceso de conexión de una estación en 802.11



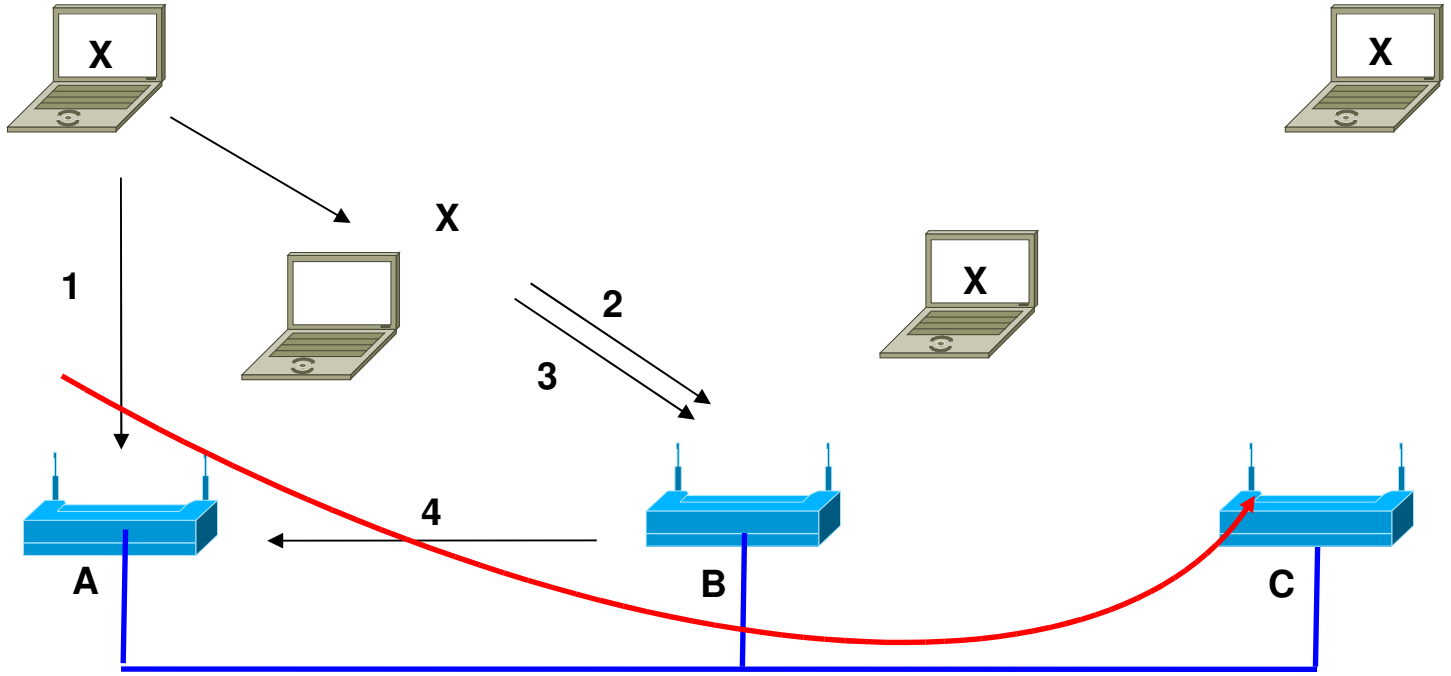
La asociación a un punto de acceso

- La asociación a un AP equivale a conectarse por cable a un *switch* en una red ethernet
  - En la asociación, el TS (la estación) determina con qué BSSID de qué AP va a trabajar
- 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 PA de la red inalámbrica mantiene en todo momento una relación de las estaciones que tiene asociadas
  - Identificadas por sus direcciones MAC
- Cuando un PA 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

La itinerancia (Handoff o roaming)

- Una estación no puede estar asociada a más de un AP a la vez
  - Necesitaría dos radios y podría provocar bucles
- 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

Proceso de itinerancia (*Handover*)



1: La estación se enciende. Se autentifica y asocia con el AP A (el más próximo)

2: La estación se mueve y se pre-autentifica con el AP B

3: La estación decide reasociarse con B

4: B notifica a A la nueva ubicación de X con lo que X se desasocia de A. A envía a B cualquier trama para X en curso

5: X sigue moviéndose por lo que más tarde repite el proceso con C

Autenticación

- 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 autenticarse antes de asociarlas
  - La autenticación 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 **autenticación** se hace con un determinado SSID
  - La **asociación** con un determinado BSSID de un determinado punto de acceso

Autenticación de las estaciones WEP

- Autenticación de sistema abierto (OSA *Open System Authentication*)
  - ✓ Cualquier interlocutor es válido para establecer una comunicación con el AP.
  - ✓ Método totalmente inseguro,
    - No puede ser dejado de lado, para permitir conectarse desde sitios públicos anónimamente (Terminales, hoteles, aeropuertos, etc.).
- Autenticación de clave compartida(SKA *Shared Key Authentication*)
  - ✓ Es el método mediante el cual ambos dispositivos disponen de la misma clave de encriptación, entonces, el dispositivo TR pide al AP autenticarse.
    - Se trata de un envío de interrogatorio (desafío) por parte del AP al cliente.
    - El AP le envía una trama al TR, que si éste a su vez devuelve correctamente codificada, le permite establecer comunicación.

Características de WEP
(*Wired Equivalet Privacy*)

- Originalmente 802.11 contempló para seguridad el protocolo WEP (*Wired Equivalent Privacy)*
- Características
  - ✓ Cifrado:
    - Clave simétrica,
    - Algoritmo RC4
    - Puede ser WEP64 (40 bits reales)
    - WEP128 (104 bits reales)
    - Este protocolo no es 100% seguro
  - ✓ Integridad:
    - CRC-32
  - ✓ Debilidades:
    - Clave secreta pequeña
    - Integridad pensada para el cable
    - Misma clave de cifrado y autenticación

La in-Seguridad WEP y el nuevo WPA

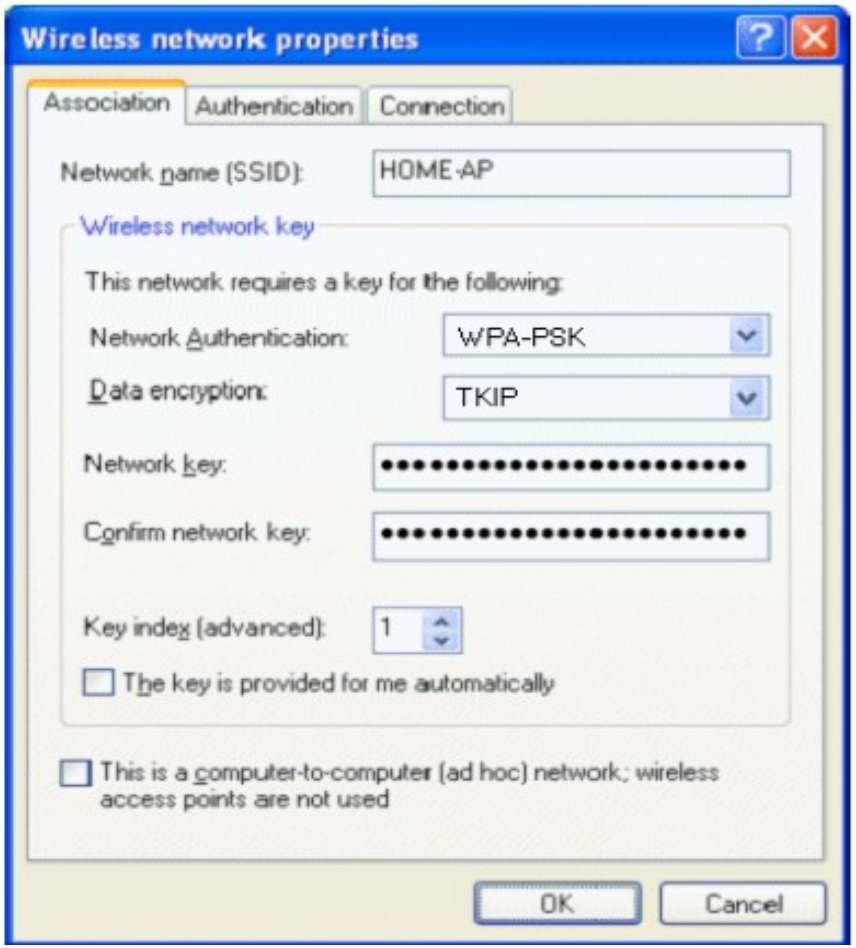
- WEP es vulnerable e inseguro.
  - El comité 802.11 ha sido muy criticado por ello, ver p. ej:
    - http://www.cs.umd.edu/~waa/wireless.html
    - http://www.drizzle.com/%7Eaboba/IEEE/rc4_ksaproc.pdf
- Para resolver esas deficiencias se ha desarrollado el estándar 802.11i, aprobado en julio de 2004.
- Para cubrir el hueco de forma provisional la WiFi Alliance había desarrollado dos 'anticipos' de 802.11i que son:
  - El WPA (Wi-Fi Protected Access) y
  - El WPA2
- 802.11i, WPA y WPA2 se apoyan en el estándar 802.1x (port based control) aprobado en el 2001.

Seguridad WPA (*Wi-Fi Protected Access*)

- Define múltiples claves:
  - ✓ PSK (compartida),
  - ✓ PMK (maestra),
  - ✓ PTK (temporales)…

- Para controlar el acceso a una red inalámbrica se pueden usar dos mecanismos:
  - WPA- PSK- (Personal Share Key- Clave secreta compartida)
    - La clave secreta es más sencilla de implementar, pero menos flexible.
    - No es práctica en grandes organizaciones
  - WPA- Empresarial (RADIUS,802.1x/EAP).
    - Validación por usuario/password frente a un servidor RADIUS (Remote Authentication Dial In User Server)
- ¿Es WPA vulnerable?: cowpatty.

WPA-PSK (autentificación)



Protocolo TKIP (*Temporal Key Integrity Protocol*).

- Propone mejoras importantes:
  - ✓ Combinación de clave por paquete:
    - Combina con la dirección MAC y el número secuencial del paquete.
    - Se basa en el concepto de PSK (*Pre-shared Key*).
    - Esta metodología, genera dinámicamente una clave entre 280 trillones por cada paquete.

TPKI (II)

- VI (Vector de inicialización) de 48 bits:
  - ✓ Este tema era una de las mayores debilidades de WEP al emplear sólo 24 bits.
    - 24 bits son 16 millones de combinaciones,
    - 48 bits son 280 billones.
  - ✓ Se divide 280 billones sobre 16 millones, el resultado es:
    - 17.500.000
    - Si un VI de 24 bits se repite en el orden de 5 horas en una red wireless de una mediana empresa, entonces un VI de 48 bits = 5 x 17.500.00 horas = 87.500.000 horas = 3.645.833 días = 9.988 años
- MIC (*Message Integrity Check - Integridad*)
  - Se plantea para evitar el conocido ataque inductivo o de hombre del medio.
  - Propone descartar todo mensaje que no sea validado.

802.1X
Conceptos

- Es un mecanismo estándar para autenticar centralmente estaciones y usuarios.
- Posee mecanismos de autentificación, autorización y distribución de claves.
  - ✓ Incorpora control de acceso para los usuarios que se unan a la red
- Es un estándar abierto
  - ✓ Soporta diferentes algoritmos de encriptación.
- Se apoya en el protocolo de autenticación EAP (*Extensible Authentication Protocol*)
  - ✓ EAP es soportado por muchos Puntos de Acceso y por HostAP.
- Antes de la autenticación sólo se permite tráfico 802.1X (petición de autenticación).

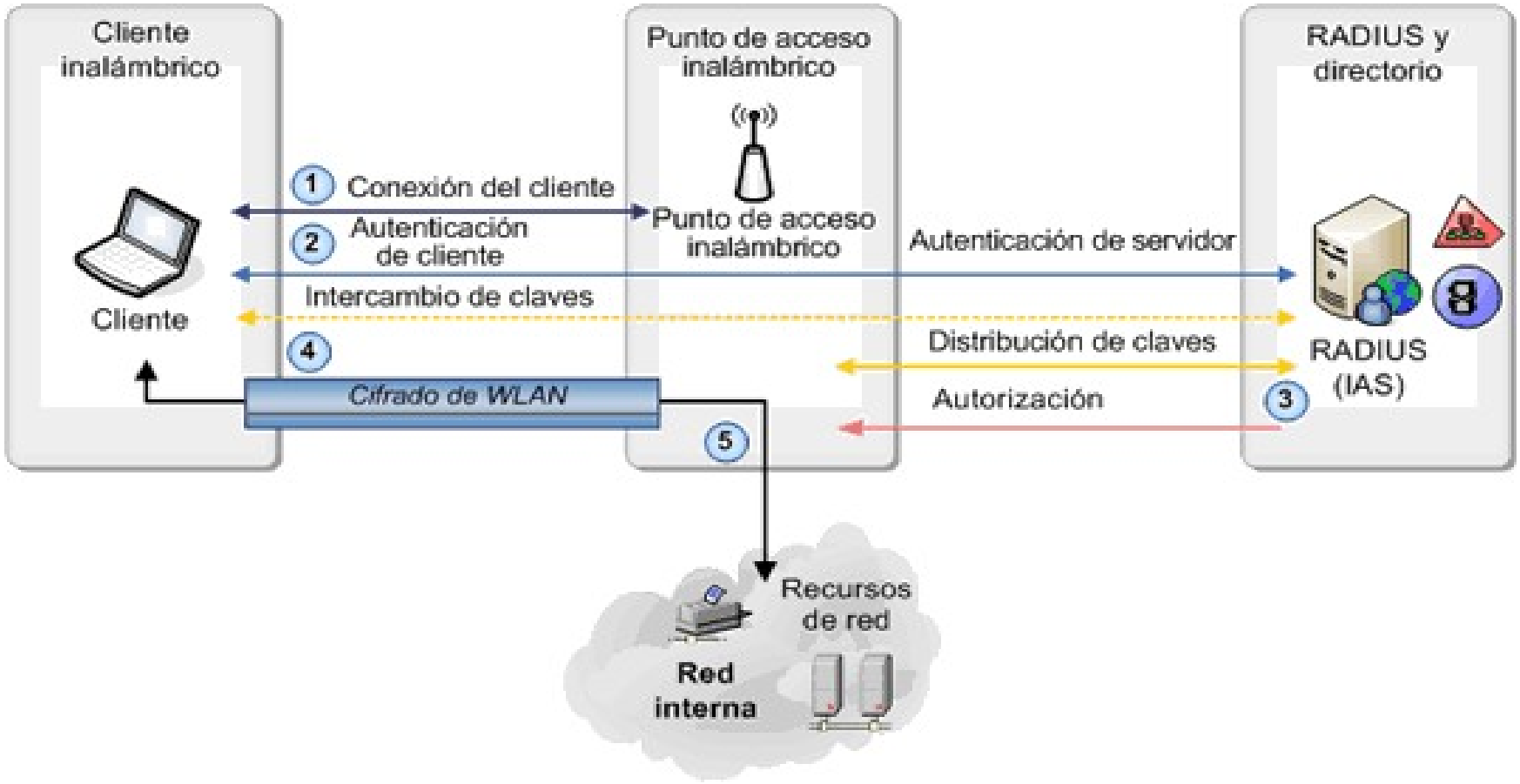
La arquitectura 802.1x autenticación

- Está compuesta por tres entidades funcionales:
  - ✓ El Solicitante (El suplicante: cliente)
    - Generalmente se trata del cliente WiFi
  - ✓ El Autenticador (que hace el control de acceso)
    - Suele ser el AP (Punto de acceso), que actúa como mero traspaso de datos y como bloqueo hasta que se autoriza su acceso (importante esto último).
  - ✓ El Servidor de autenticación (que toma la decisión de autorización)
    - Suele ser un Servidor RADIUS (*Remote Authentication Dial In User Service*) o Kerberos, que intercambiará el nombre y credencial de cada usuario.
    - El almacenamiento de las mismas puede ser local o remoto en otro servidor de LDAP, de base de datos o directorio activo.

Funciones del Servidor RADIUS

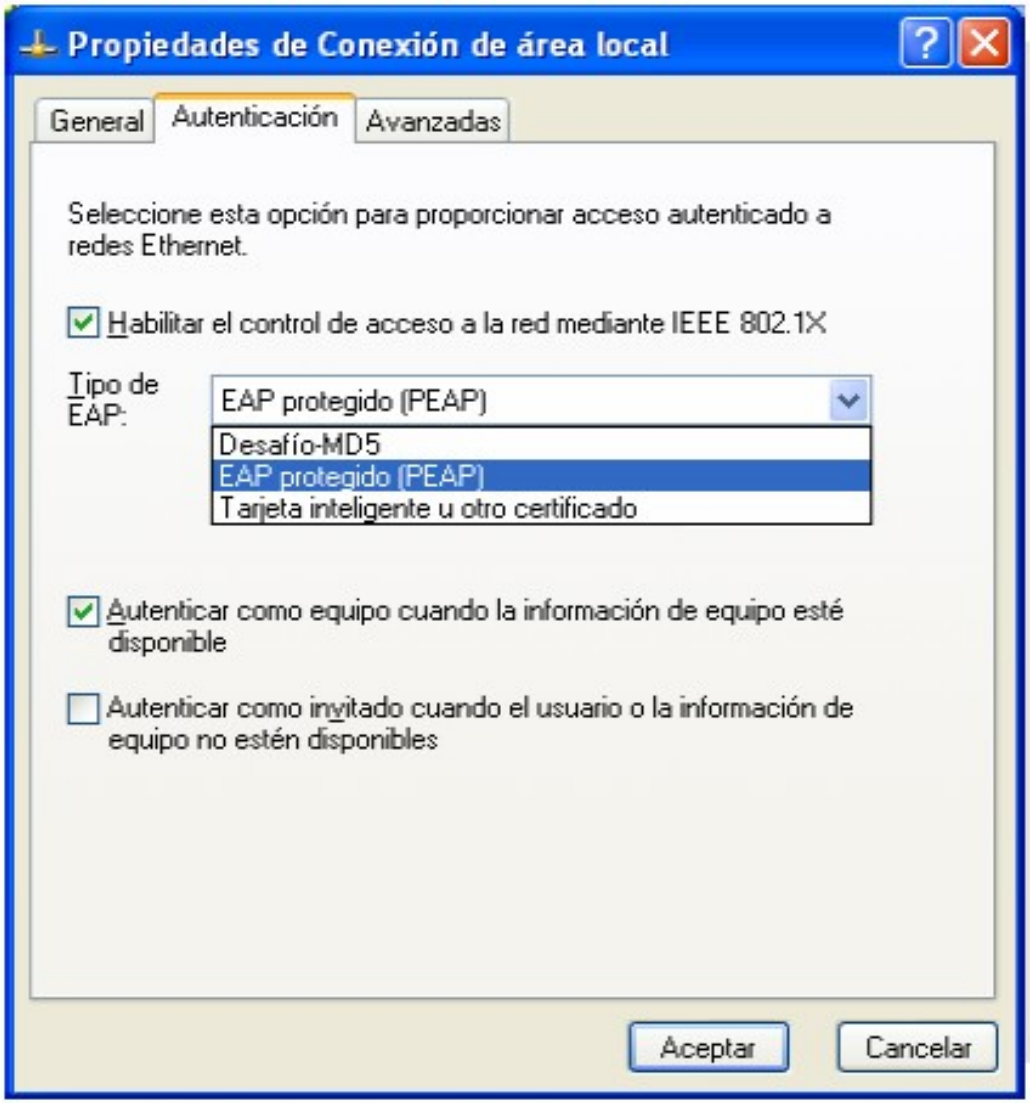
- Autenticación
  - ✓ Verificar que una entidad es quien dice ser.
  - ✓ Suele incluir unas credenciales (usuario/contraseña, certificados, tokens, etc.).
- Autorización
  - ✓ Decidir si la entidad, una vez autenticada, tiene permiso para acceder al recurso.
- Control de Acceso
  - ✓ Conceder el permiso definitivo. ACL. Registro, monitorización, contabilidad e informes.

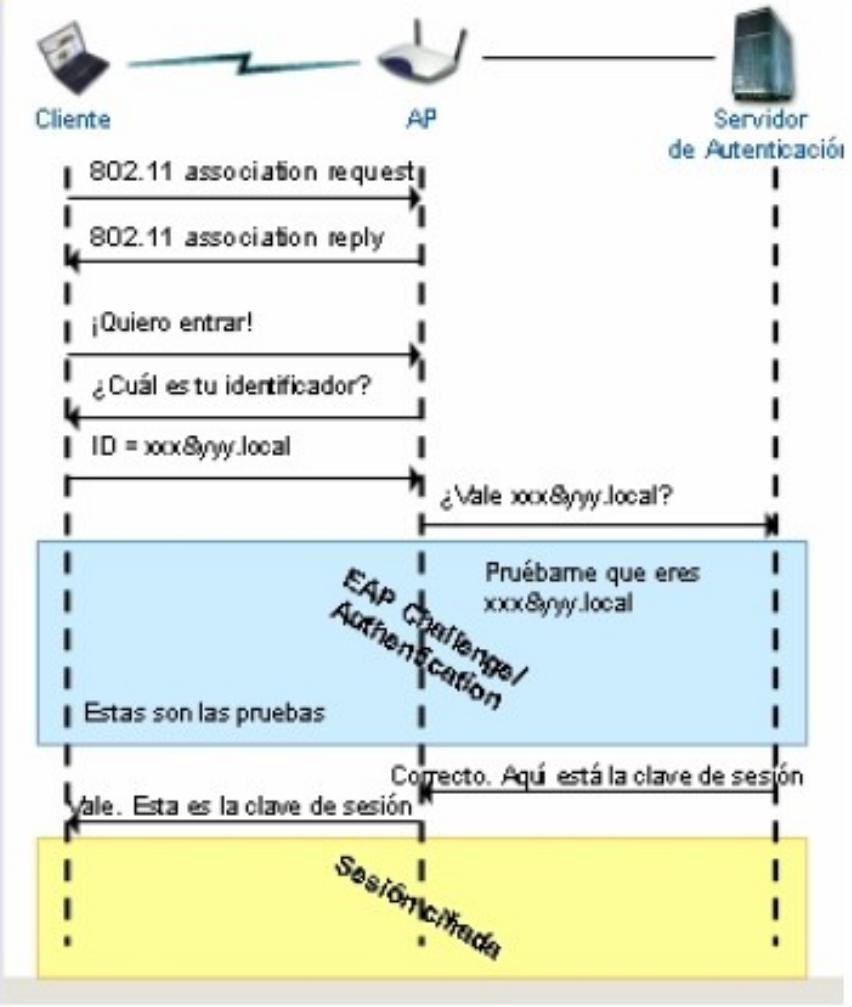
Funcionamiento de 802.1X con PEAP y contraseñas



Fuente: Microsoft

Autenticación por cliente con EAP (802.1X)





EAP RFC 2284 (Extensible Authentication Protocol)

- LEAP (*Lightweigth EAP*)
  - ✓ Implementacion de Cisco, autenticación mutua, permite el uso dinámico de WEP
- EAP-TLS (*Extensible Authentication Protocol with Transport Layer Security* - RFC: 2716).
  - ✓ Se basa en certificados en lugar de contraseñas como credenciales de autenticación.
  - ✓ Autenticación mutua, cifrada y depende de certificados de una CA. Soportado por hostapd. Propuesta por Microsoft (W XP)
- EAP-MD5
  - ✓ El servidor envía un mensaje desafío al cliente y este contesta con otro mensaje MD5 o no autentica.
  - ✓ Fácil de implementar pero menos fiable

EAP RFC 2284 (Extensible Authentication Protocol)

- EAP-TTLS (*EAP with Tunneling Transport Layer Security*)
  - ✓ Realiza un túnel de nivel 2 entre el cliente y el AP, una vez establecido el túnel, EAP/TTLS opera sobre él, lo cual facilita el empleo de varios tipos de credenciales de autenticación que incluyen contraseñas y certificados,
  - ✓ No deja de ser una variante de EAP/TLS.
  - ✓ No necesita ambos certificados, solo el de el servidor para crear un tunel.
- PEAP (*Protected Extensible Authentication Protocol*)
  - ✓ El una amplia variedad de credenciales de autenticación.
  - ✓ Desarrollado por M$, Cisco y RSA, similar a EAP-TTLS
  - ✓ Se considera que PEAP es el método más seguro del momento.

802.1X EN ACCIÓN

1. Cuando el cliente precisa realizar una transacción, envía antes un mensaje de "inicio" a un punto de acceso, el cual solicita su identidad e incapacita al puerto para cursar tráfico, salvo el relacionado con 802.x.
2. El cliente contesta con un paquete de respuesta que contiene la identidad, y el punto de acceso lo envía a un servidor de autenticación.
3. El servidor de autenticación envía un paquete de "aceptación" al punto de acceso.
4. El punto de acceso devuelve de nuevo el puerto del cliente a un estado autorizado y comienza la transmisión.

Autentificación RADIUS con WPA y 802.1x (eduroam)

1: A solicita asociarse al AP por WPA/802.1x y envía un usuario

2: El AP envía a D el usuario

3: D devuelve al AP el 'reto'

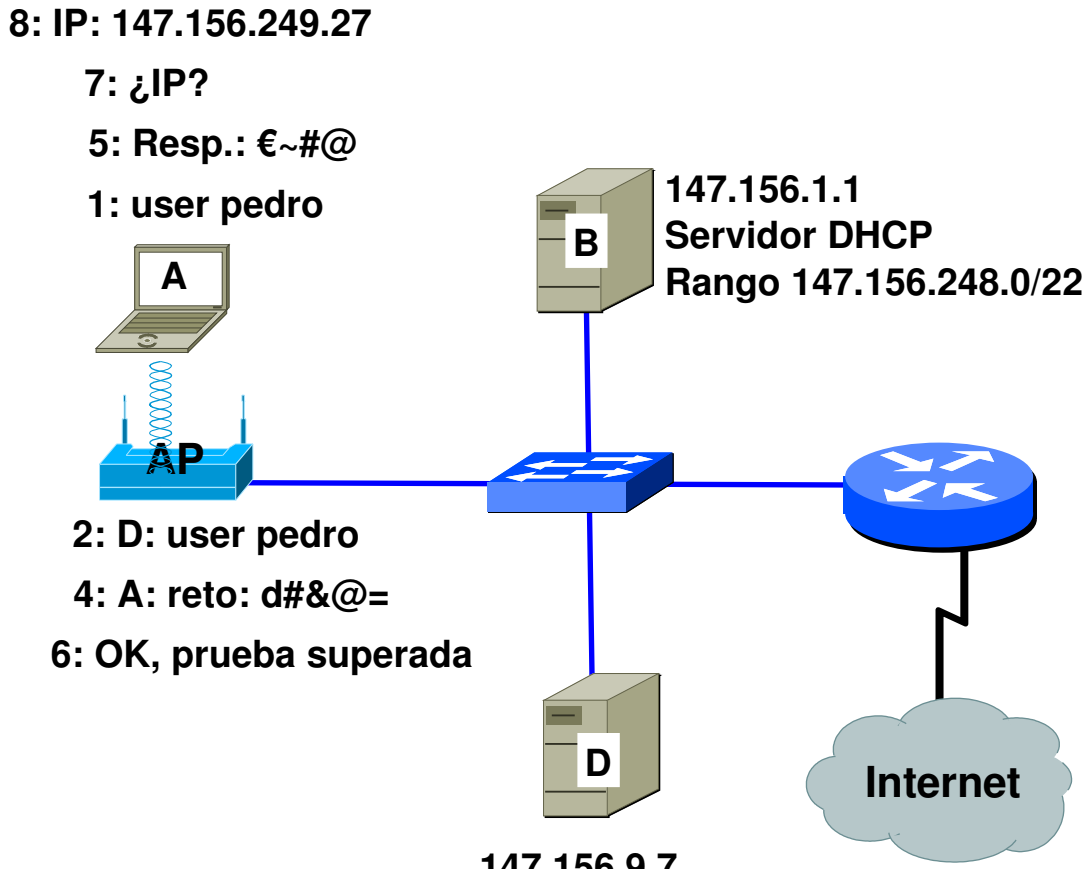
4: El AP envía a A el 'reto' y espera la respuesta

5: A devuelve al AP la respuesta, que la reenvía a D

6: Al comprobar D que es correcta le dice al AP que admita la asociación

7: Una vez conectado a la red A solicita por BOOTP una dirección

8: B le asigna una dirección pública



Autentificación RADIUS con túneles VPN (eduroam-vpn)

1: A se asocia al AP por WEP usando una clave secreta compartida

2: A solicita por BOOTP una dirección

3: B asigna a A una dirección privada

4: A solicita a C crear un túnel y le manda un usuario

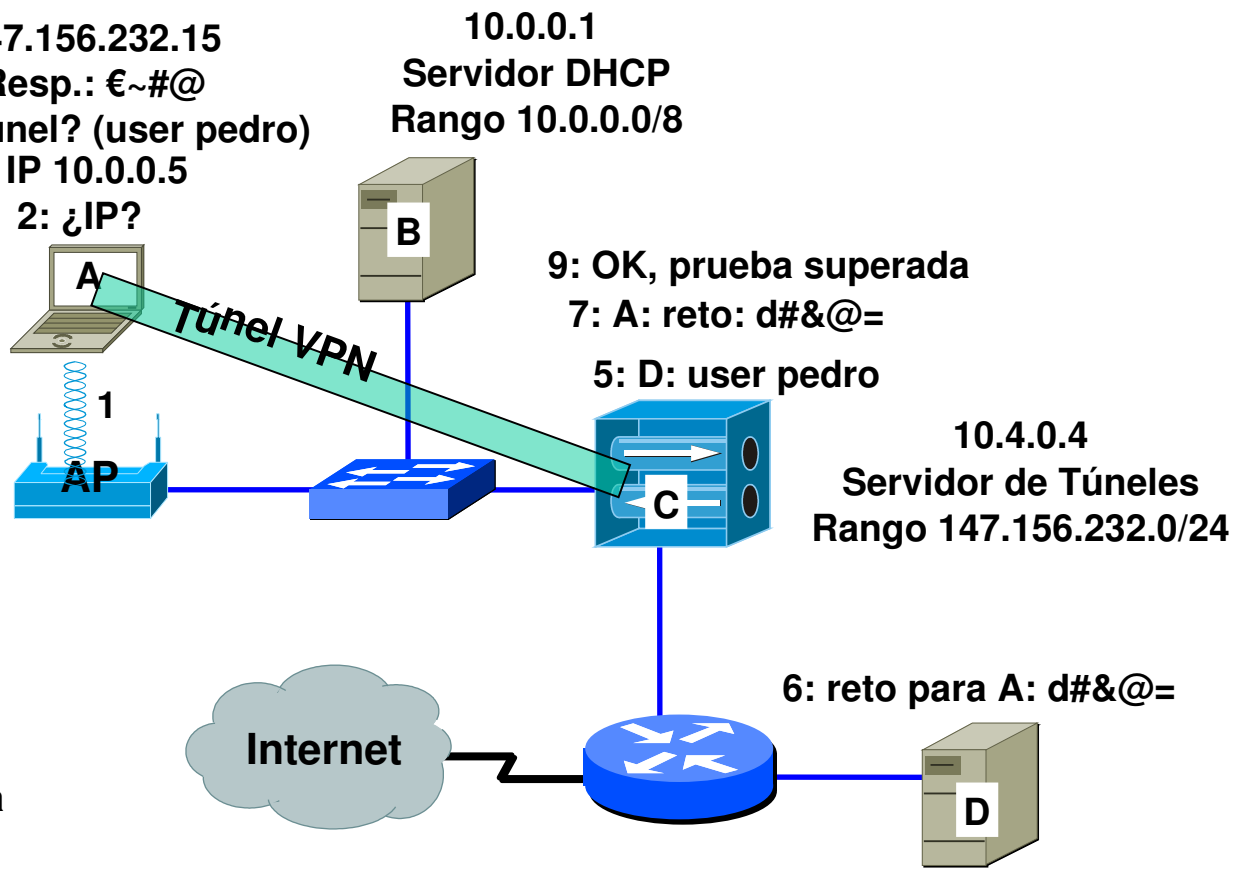
5: C envía a D el usuario

6: D devuelve a C el 'reto'

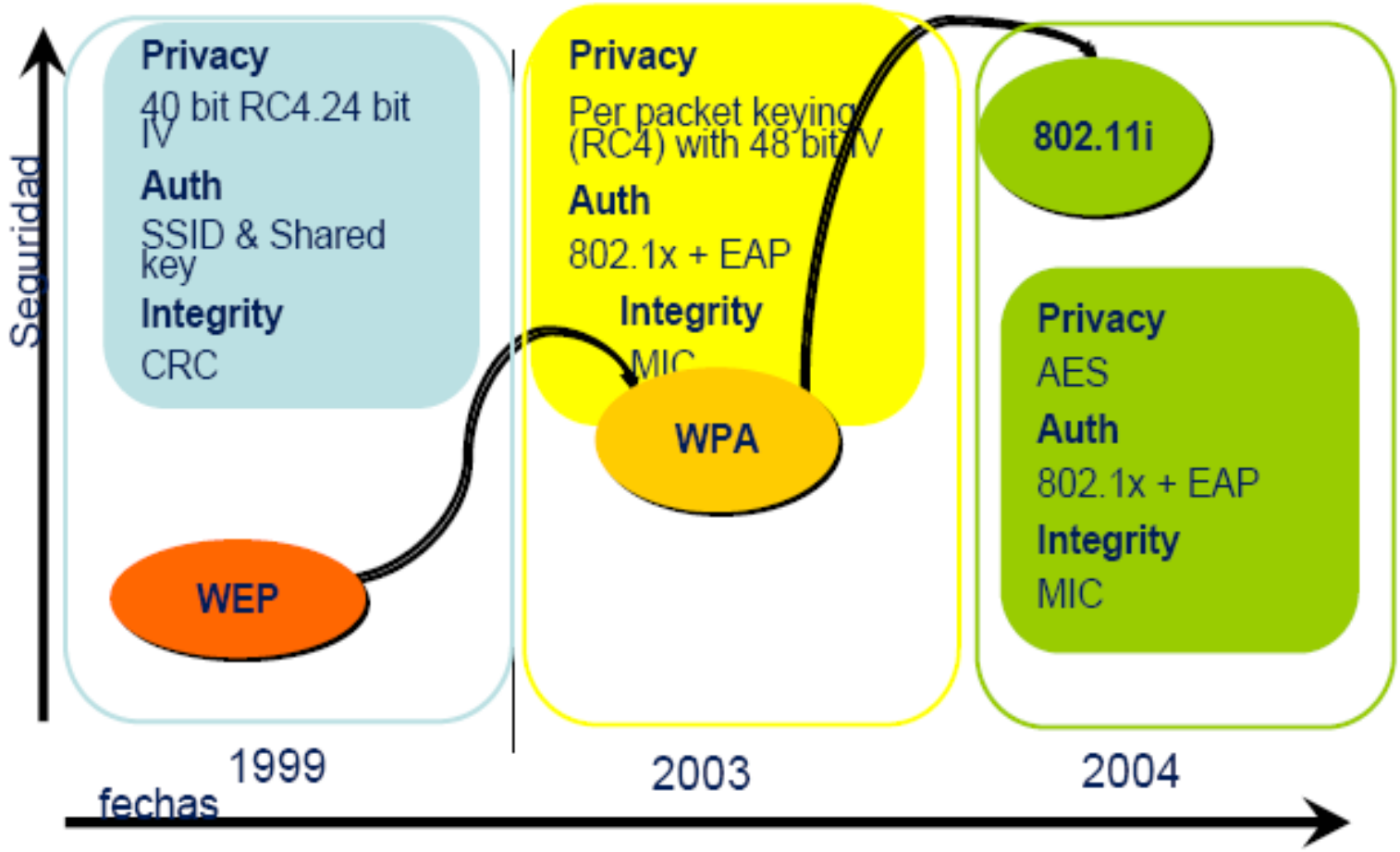
7: C envía a A el 'reto' y espera la respuesta

8: A devuelve a C la respuesta, que la reenvía a D

9: Al comprobar D que es correcta informa a C que entonces le asigna a A una dirección y establece el túnel



Seguridad


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

Problemas de Seguridad WI-FI

- No existencia clara de un perímetro
  - ✓ Facilidad para rastreo
  - ✓ Accesibilidad sin acceso físico (por proximidad)
- Valores por defecto
  - ✓ Cambiar valores
- Posibilidad de cambiar MAC
  - ✓ Detección
- Autenticación por máquina
  - ✓ 802.1X (usuario)
- Debilidad de WEP
  - ✓ WPA o WPA2

Algunos mecanismos que ayudan a mejorar la seguridad son

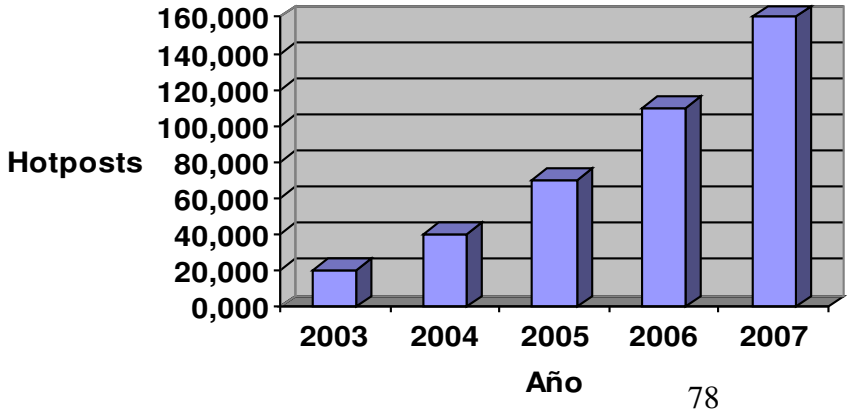
- Eliminar todos los valores predeterminados
  - ✓ SSID
  - ✓ Contraseña de la aplicación de administración (fuerte)
  - ✓ Acceso al router desde Internet
  - ✓ Deshabilitar DHCP
- Activar el cifrado de datos (mínimo 128 bits)
- Cerrar la red a dispositivos ajenos
  - ✓ Desactivar la difusión del SSID(en modo broadcast)
    - En este caso los usuarios deben conocer el SSID para conectarse a la red.
    - No es un mecanismo seguro pues el SSID se transmite no encriptado en los mensajes de conexión.
  - ✓ ACL (Access Control List) Filtrar por dirección MAC.
    - Sólo se permite unirse a la red a aquellas direcciones MAC que estén dadas de alta en una lista de direcciones permitidas.
    - Tampoco es seguro porque otras estaciones pueden cambiar su MAC y poner una autorizada cuando el verdadero propietario no está conectado

Propuesta de La WiFi Alliance

- Modelo Empresas:
  - ✓ WPA:
    - Autenticación: IEEE 802.1x/EAP.
    - Cifrado: TKIP/MIC.
  - ✓ WPA2:
    - Autenticación: IEEE 802.1x/EAP.
    - Cifrado: AES-CCMP.
- Modelo personal (SOHO/personal):
  - ✓ WPA:
    - Autenticación: PSK.
    - Cifrado: TKIP/MIC.
  - ✓ WPA2:
    - Autenticación: PSK.
    - Cifrado: AES-CCMP.

Hotspots

- Los hotspots son sitios de gran concentración de personas que ofrecen acceso a Internet a través de WLAN, como aeropuertos, hoteles, restaurantes, cafés, etc.
- Hoy día existen más de 30.000 hotspots en todo el mundo, una tercera parte de ellos localizados en los Estados Unidos
- Se ha llamado WISP a los operadores que ofrecen hotspots por Wireless ISP
- Un WISP ofrece a los sitios la capacidad de convertirse en hotspot ofreciéndole un kit de conexión compuesto por puntos de acceso, antenas, etc.
  - ✓ Aunque existen varios modelos económicos, el dueño del sitio cobra en tarifas por minuto, semanales o por mes de acuerdo a los precios del WISP.



Wireless Standard	802.11b		802.11a		802.11g	
Popularity		Widely adopted. Readily available everywhere.		New technology. Limited adoption.		New technology. Limited adoption, but rapid growth expected.
Speed	11 Mbps	Up to 11Mbps	54 Mbps	Up to 54Mbps (5X greater than 802.11b)	54 Mbps	Up to 54Mbps (5X greater than 802.11b)
Cost		Inexpensive		Expensive		Moderate
Frequency	2.4 GHz	Crowded 2.4GHz band. May conflict with other 2.4GHz devices like cordless phones, microwave ovens, etc.	5 GHz	Uncrowded 5GHz band.	2.4 GHz	Crowded 2.4GHz band. May conflict with other 2.4GHz devices like cordless phones, microwave ovens, etc.
Range	100-150	Good Range. Typically up to 100-150 feet indoors, depending on construction, building materials, room layout.	25-75	Limited range. Typically no more than 25 to 75 feet indoors.	100-150	Good Range. Typically up to 100-150 feet indoors, depending on construction, building materials, room layout.
Public Access		The number of public "Hot Spots" is growing rapidly, allowing wireless connectivity in many airports, hotels, college campuses, public areas, and restaurants.	X	None at this time.		Compatible with current 802.11b "Hot Spots" (at 11Mbps)
Compatibility	OK 802.11b	Widest adoption Wi Fi	OK 802.11a	Incompatible with 802.11b or 802.11g	OK 802.11b 802.11g	Interoperates with 802.11b networks (at 11Mbps) Incompatible with 802.11a

802.11n

Año 2006/2007

- 540 Mbps

Resumen

- IEEE 802.11: Especificaciones para 1-2 Mbps en la banda de los 2.4GHz. usando salto de frecuencias (FHSS) o secuencia directa (DSSS).
- IEEE 802.11b: Extension de 802.11 para proporcionar 11 Mbps usando DSSS.
- Wi-Fi (Wireless Fidelity): Termino registrado promulgado por la WECA para certificar productos IEEE 802.11b capaces de interoperar con los de otros fabricantes.
- IEEE 802.11a: Extension de 802.11 para proporcionar 54 Mbps usando OFDM.
- IEEE 802.11g: Extension de 802.11 para proporcionar 20-54 Mbps usando DSSS y OFDM. Es compatible hacia atras con 802.11b. Tiene mayor alcance y menor consumo de po-tencia que 802.11a

- IEEE 802.11 - The original 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and IR standard (1999)
- IEEE 802.11a - 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
- IEEE 802.11c - Bridge operation procedures; included in the IEEE 802.1D standard (2001)
- IEEE 802.11d - International (country-to-country) roaming extensions (2001)
- IEEE 802.11e - Enhancements: QoS, including packet bursting (2005)
- IEEE 802.11F - Inter-Access Point Protocol (2003)
- IEEE 802.11g - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h - Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- IEEE 802.11i - Enhanced security (2004)
- IEEE 802.11j - Extensions for Japan (2004)
- IEEE 802.11k - Radio resource measurement enhancements
- IEEE 802.11l - (reserved, typologically unsound)
- IEEE 802.11m - Maintenance of the standard; odds and ends.
- IEEE 802.11n - Higher throughput improvements
- IEEE 802.11o - (reserved, typologically unsound)
- IEEE 802.11p - WAVE - Wireless Access for the Vehicular Environment (such as ambulances and passenger cars)
- IEEE 802.11q - (reserved, typologically unsound, can be confused with 802.1q VLAN trunking)
- IEEE 802.11r - Fast roaming
- IEEE 802.11s - ESS Mesh Networking
- IEEE 802.11T - Wireless Performance Prediction (WPP) - test methods and metrics
- IEEE 802.11u - Interworking with non-802 networks (e.g., cellular)
- IEEE 802.11v - Wireless network management
- IEEE 802.11w - Protected Management Frames

Software libre para análisis/ataque de redes 802.11

- Análisis:
  - Netstumbler (www.netstumbler.org)
    - Detecta APs y muestra información sobre ellos
  - Wellenreiter (www.remote-exploit.org)
    - Similar a Netstumbler
  - Kismet (www.kismetwireless.net)
    - Sniffer inalámbrico
- Ataque:
  - Airsnort (airsnort.shmoo.com)
    - Para espiar redes inalámbricas que usan WEP
  - Wepcrack (http://sourceforge.net/projects/wepcrack)
    - Parecido a airsnort
- AirPcap (http://www.cacetech.com/products/airpcap.htm)

Enlaces

- Información sobre todos los estándares en:
- http://standards.ieee.org/getieee802/portfolio.html
- Wlana Wireless LAN Association
- http://www.wlana.org/
- http://www.wi-fi.org /

Glossary of 802.11 Wireless Terms

- Station (STA):
  - ✓ A computer or device with a wireless network interface.
- Access Point (AP):
  - ✓ Device used to bridge the wireless-wired boundary, or to increase distance as a wireless packet repeater.
- Ad Hoc Network:
  - ✓ A temporary one made up of stations in mutual range.
- Infrastructure Network:
  - ✓ One with one or more Access Points.
- Channel:
  - ✓ A radio frequency band, or Infrared, used for shared communication.
- Basic Service Set (BSS):
  - ✓ A set of stations communicating wirelessly on the same channel in the same area, Ad Hoc or Infrastructure.
- Extended Service Set (ESS):
  - ✓ A set BSSs and wired LANs with Access Points that appear as a single logical BSS.

Glossary of 802.11 Wireless Terms, cont.

- BSSID & ESSID:
  - ✓ Data fields identifying a stations BSS & ESS.
- Clear Channel Assessment (CCA):
  - ✓ A station function used to determine when it is OK to transmit.
- Association:
  - ✓ A function that maps a station to an Access Point.
- MAC Service Data Unit (MSDU):
  - ✓ Data Frame passed between user & MAC.
- MAC Protocol Data Unit (MPDU):
  - ✓ Data Frame passed between MAC & PHY.
- PLCP Packet (PLCP_PDU):
  - ✓ Data Packet passed from PHY to PHY over the Wireless Medium.