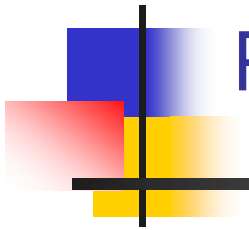
Dpto. Ingeniería de Sistemas Industriales
Div. Ingeniería de Sistemas y Automática



Redes de Computadores

Tema 5. Redes inalámbricas

Objetivos

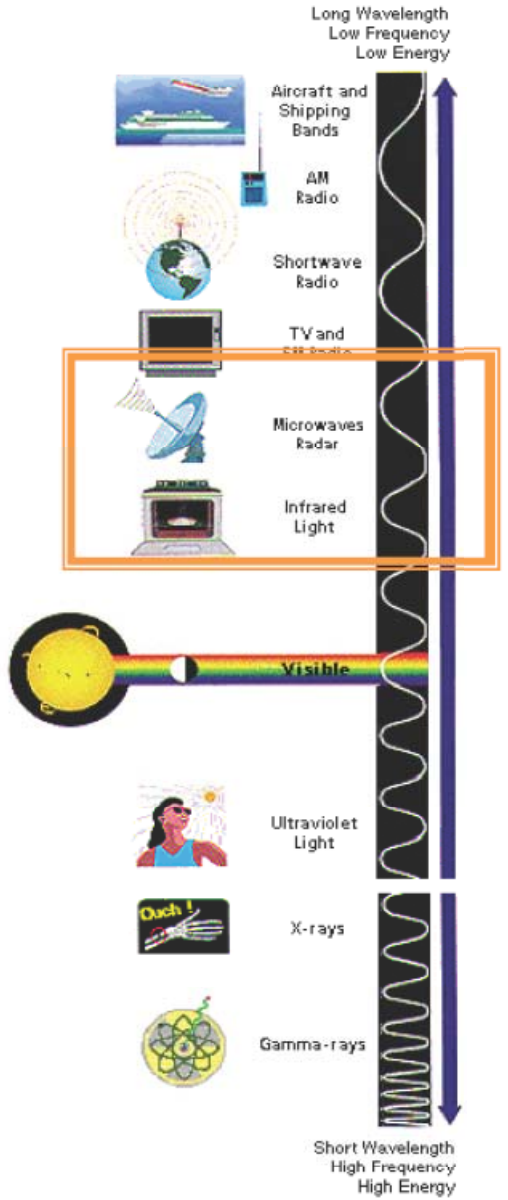
- Describir los estándares de redes de área local inalámbricas (WLAN)
- ¿Qué vamos a estudiar?
  - WLAN
  - Estándares IEEE 802.11x
  - Mecanismo de acceso al medio
  - Topologías
  - Seguridad

WLAN (1)

- WLAN (Wireless Local Area Network):
  - Conjunto de dispositivos que se comunican entre sí dentro de un área geográfica limitada utilizando como medio de transmisión el aire, sin necesidad de utilizar cables.
- Ventajas:
  - Movilidad
  - Facilidad y rapidez de instalación
  - Flexibilidad
  - Reducción del coste de mantenimiento
  - Escalabilidad
- Inconvenientes:
  - Velocidad
  - Rango de conectividad
  - Seguridad

WLAN (2)

- Zona de trabajo de las WLAN:
  - Microondas e infrarrojos.
  - Bandas de frecuencia que no requieren licencia gubernamental banda **ISM** (Industrial, Scientific and Medical).
  - Problemas:
    - No aseguran conseguir una transmisión adecuada sin interferencias ni seguridad.
    - Tienen limitada su potencia de transmisión para que la interferencia con otros usuarios quede más limitada.
  - La banda de 2.4 GHz-2.4835 GHz no requiere licencia en ningún lugar del mundo.



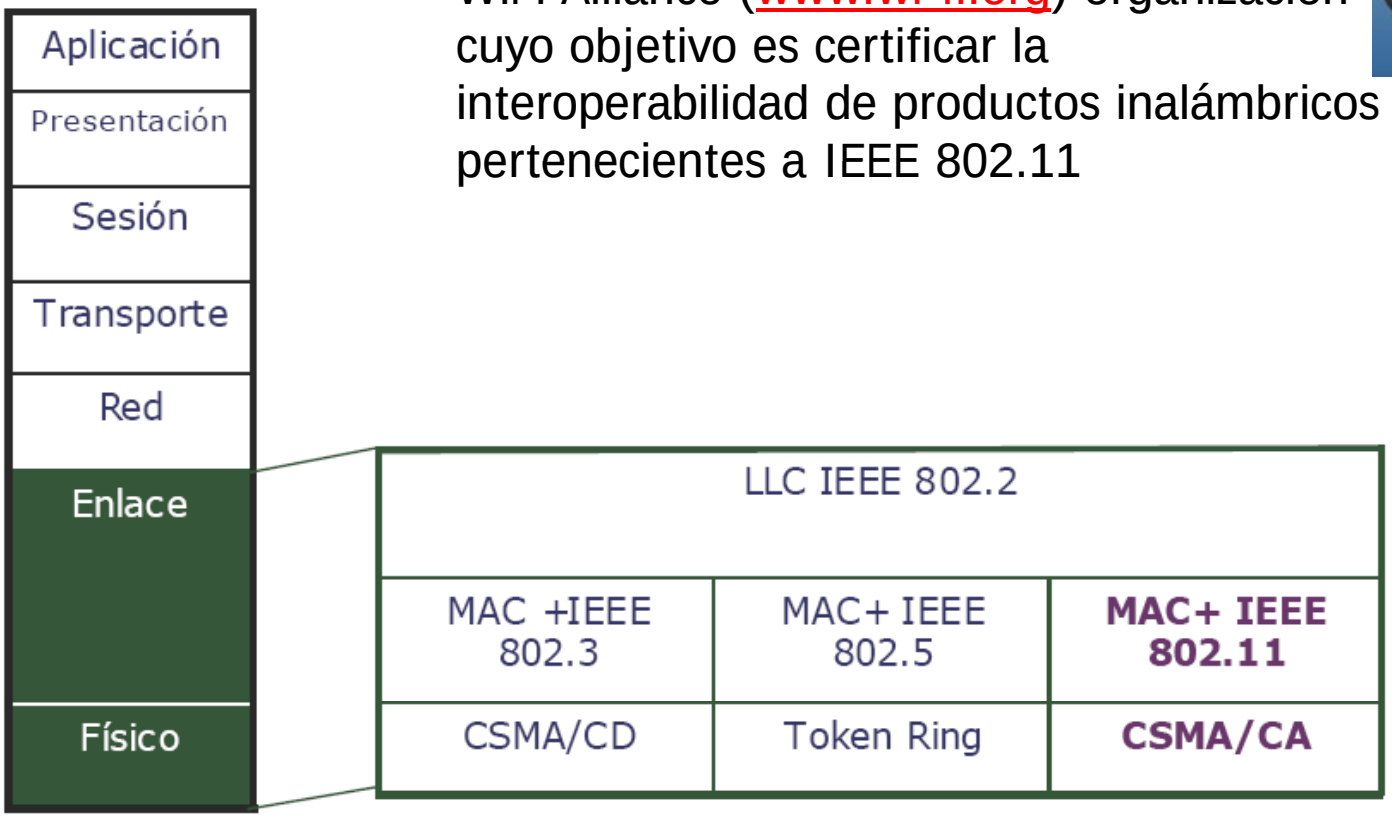
WLAN (3)

- Dispositivos:
  - Access Points, Routers Wireless

  - Tarjetas inalámbricas (PCI, PCMCIA, USB...)

Estándares IEEE 802.11x (1)

WiFi Alliance (www.wi-fi.org) organización cuyo objetivo es certificar la interoperabilidad de productos inalámbricos pertenecientes a IEEE 802.11



Estándares IEEE 802.11x (2)

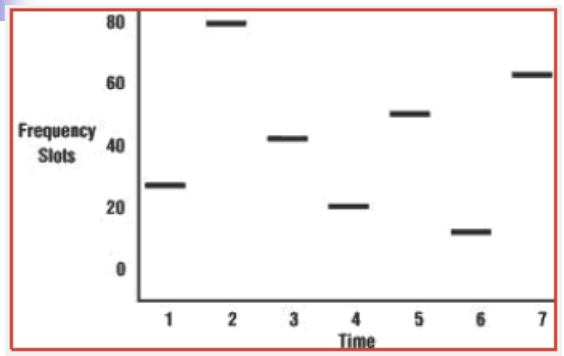
Norma	Banda de frecuencia	Modulación	Alcance	Velocidad máxima	Nº máx. canales sin solap.
802.11 b	2.4 GHz	DSSS	100 m	11 Mbps	3
802.11 a	5 GHz	OFDM	50 m	54 Mbps	12
802.11 g	2.4 GHz	OFDM	100 m	54 Mbps	3

Norma	Ampliación
802.11 d	Aspectos reglamentarios en países sin normativa vigente sobre 802.11
802.11 e	Define niveles de QoS
802.11 f	IAPP (Inter Access Point Protocol)
802.11 h	Mejora de 11 a en potencia y selección de canal de radio
802.11 i	Mecanismos de seguridad – AES (Advanced Encryption Standard)
802.11 j	Resuelve la adición del canal 4.9 GHz al de 5 GHz para 11 a en Japón

IEEE 802.11 (1)

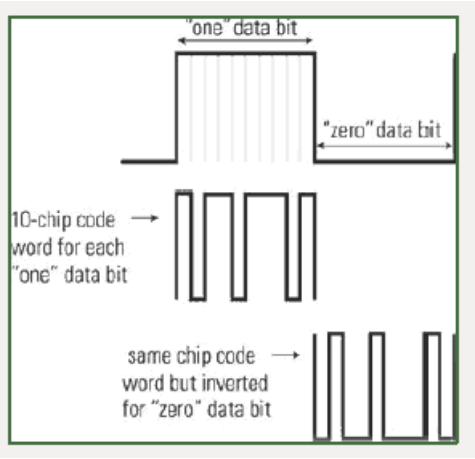
- Primer estándar para redes inalámbricas (1997).
- Se propusieron dos tecnologías:
  - Basado en infrarrojos. Descartado por limitaciones:
    - 2 Mbps
    - Transmisión en condiciones de línea vista
    - Factores externos afectan a la recepción de la señal
  - Basado en radiofrecuencia.
    - Se basa en las técnicas de *Spread Spectrum*
      - Alta inmunidad a interferencias
      - Sistemas de modulación para transmitir mucha información en un pequeño rango de frecuencias
    - Dos sistemas de modulación:
      - FHSS (Frequence Hopping Spread Spectrum): Espectro ensanchado por salto de frecuencia
      - DSSS (Direct Sequence Spread Spectrum): espectro ensanchado por secuencia directa

IEEE 802.11 (2)



FHSS (Frequency Hoping Spread Spectrum)

- La señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia síncronamente con el transmisor.
- Los receptores no autorizados escucharán una señal ininteligible.



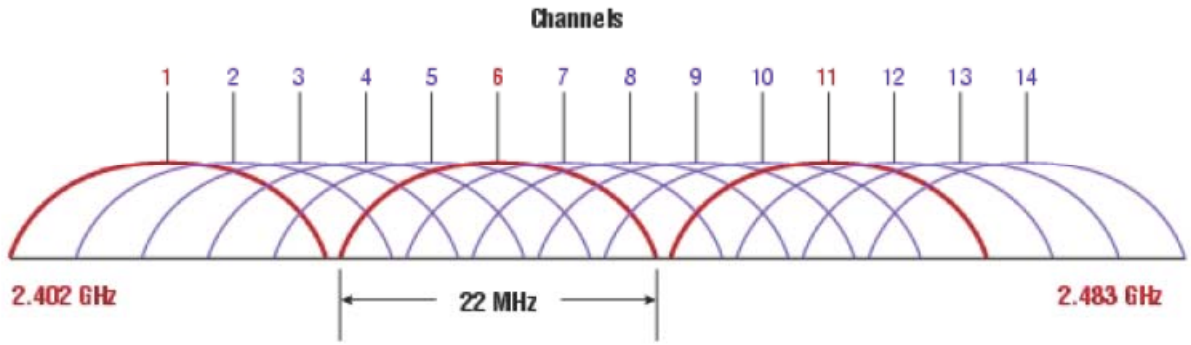
DSSS (Direct Sequence Spread Spectrum)

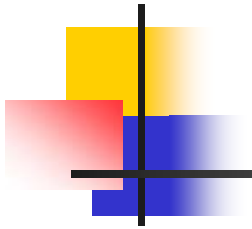
- Técnica de modulación que utiliza un código de pseudorruido para modular una portadora, de forma que aumente el ancho de banda.
- La señal resultante tiene un espectro muy parecido al del ruido, de tal forma que a todos los radiorreceptores les parecerá ruido menos al que va dirigida la señal.

- Características generales:
  - Utiliza la banda de 2,4 GHz
  - Velocidades de transmisión entre 1 y 2 Mpbs.
  - Evolución: 802.11a y 802.11b

IEEE 802.11 (3)

- IEEE 802.11 divide el espectro en canales de 22 MHz. Los canales están superpuestos.
  - Canal: Porción del espectro de radiofrecuencias que usan los dispositivos para comunicarse. El uso de diferentes canales ayuda a reducir interferencias.
- En Europa se distinguen 14 canales posibles en la banda de 2.4 GHz





IEEE 802.11a

- Utiliza la banda de 5 GHz
- Introdujo la técnica de modulación OFDM (Ortogonal Frequency Division Multiplexing)
  - Permite dividir una portadora de datos de alta velocidad en 52 subportadoras de baja velocidad que se transmiten en paralelo.
- Velocidades de hasta 54 Mbps
- Ratificado en 1999

IEEE 802.11b

- Utiliza la banda de 2.4 GHz
- Introdujo el sistema de codificación CCK (Complementary Code Keying) manteniendo el sistema DSSS
  - Velocidades de hasta 11 Mbps
- Técnica DRS (Dynamic Rate Shifting): permite variar las velocidades entre 1, 2, 5.5 y 11 Mbps.
  - Los adaptadores pueden reducir las velocidades para compensar problemas de recepción (por atravesar diversos materiales o por recorrer diferentes distancias)
- Consumo inferior a 802.11a
  - Idóneo para portátiles y PDAs
- Más implantado que el 802.11a. En 2004 el 95% de los equipos son 802.11b.
- Ratificado en 1999.

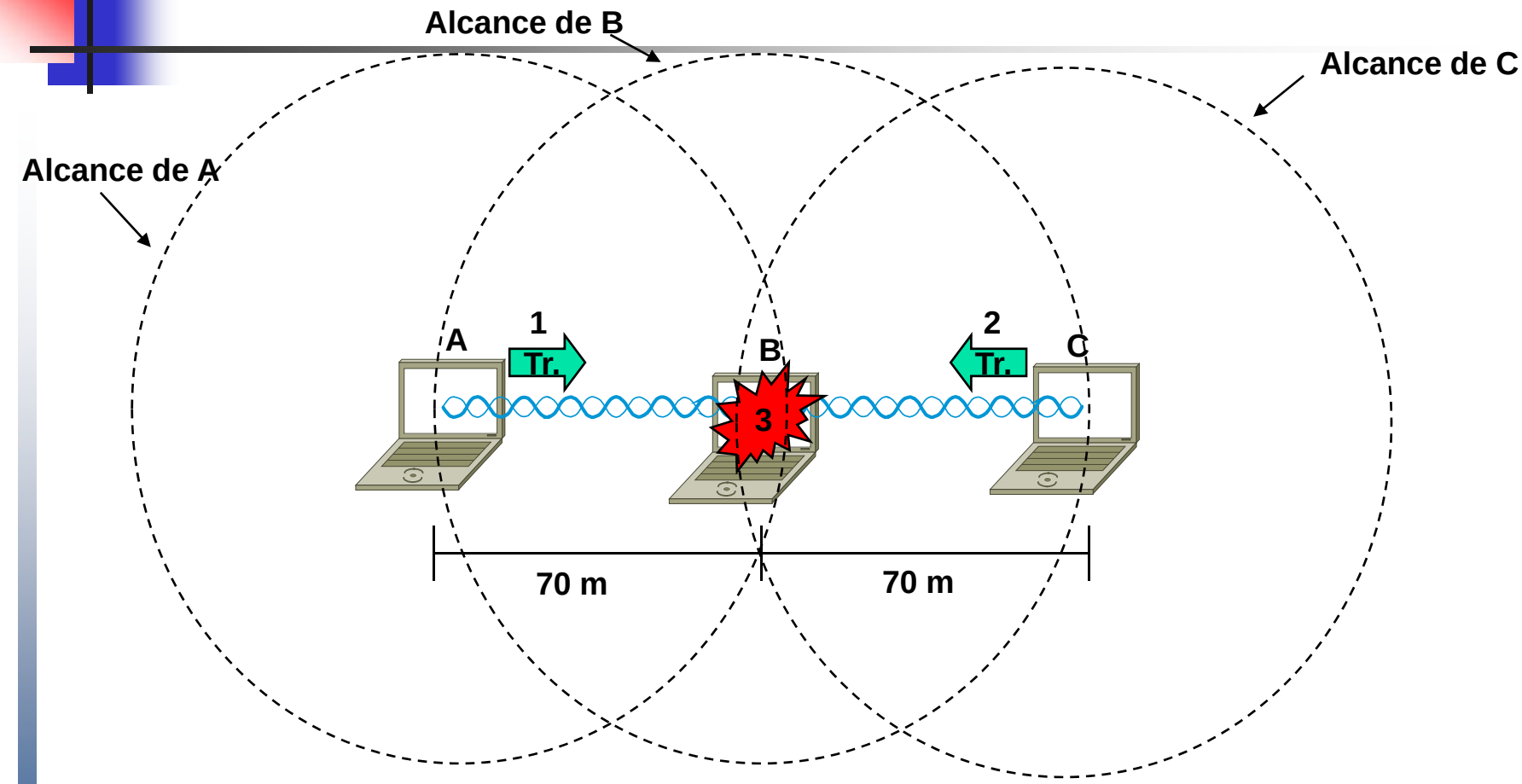
IEEE 802.11g

- Ratificado en 2003.
- Modulación OFDM
- Compatible con 802.11b
- Utiliza la banda de 2.4 GHz y consigue velocidades de 54 Mbps
- Dos implementaciones:
  - Estándar: 24 Mbps
  - 54g: 54 Mbps

Mecanismo de acceso al medio (1)

- Ethernet:
  - CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
- Wi-Fi:
  - No es posible detectar colisiones
  - Problema del nodo oculto
  - CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)
    - Se utiliza un protocolo de 4 fases

El problema de la estación oculta

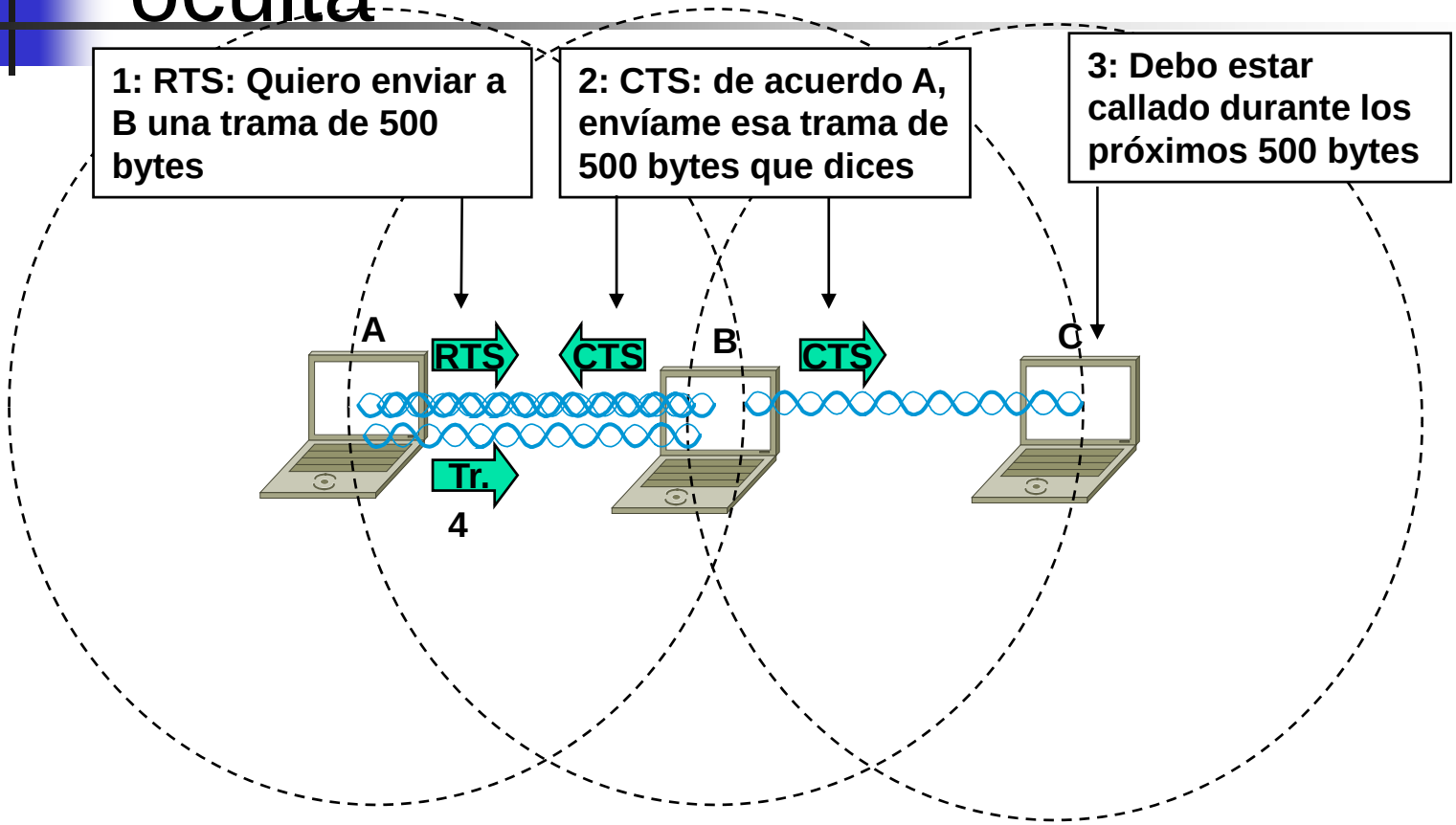


1: A quiere transmitir una trama a B. Detecta el medio libre y transmite

3. Se produce una colisión en la intersección por lo que B no recibe ninguna de las dos tramas

2: Mientras A está transmitiendo C quiere enviar una trama a B. Detecta el medio libre (pues no capta la emisión de A) y transmite

Solución al problema de la estación oculta



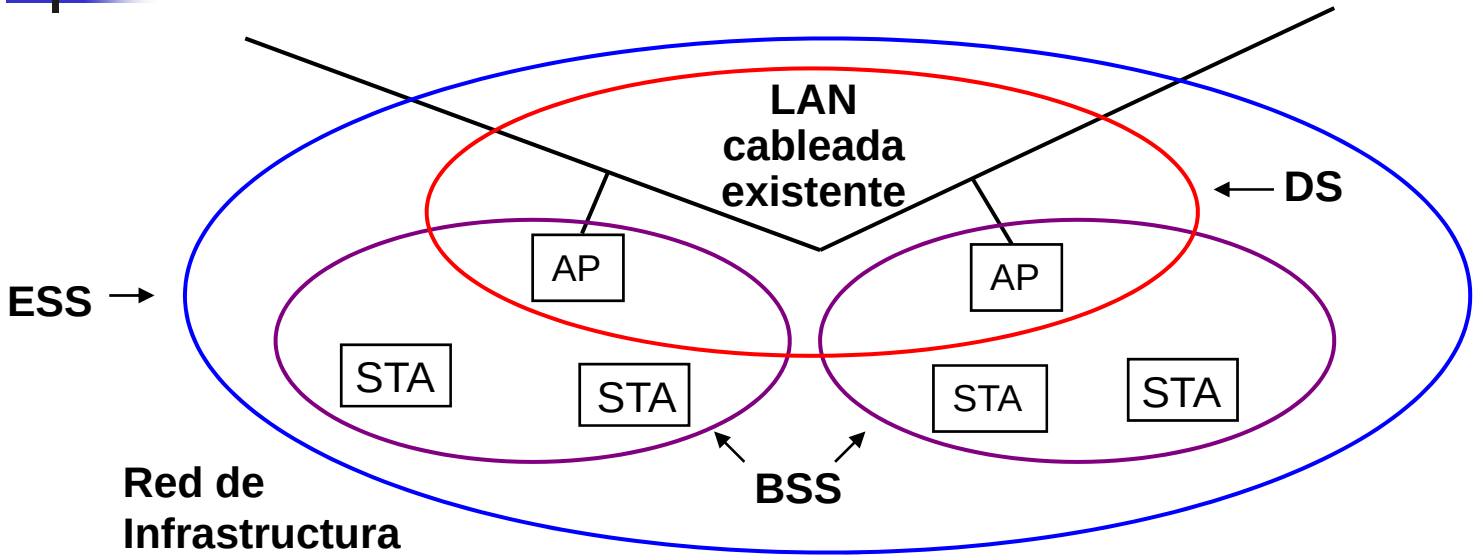
1: Antes de transmitir la trama A envía un mensaje RTS (Request To Send)

2: B responde al RTS con un CTS (Clear To Send)

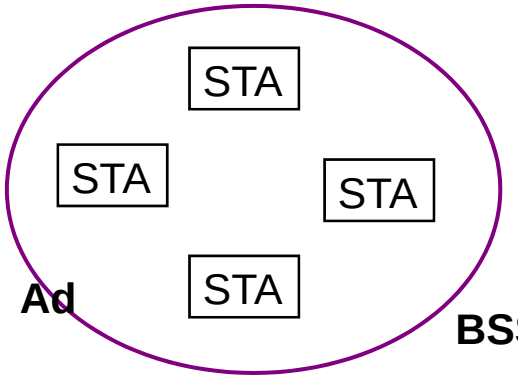
3. C no capta el RTS, pero sí el CTS. Sabe que no debe transmitir durante el tiempo equivalente a 500 bytes

4. A envía su trama seguro de no colisionar con otras estaciones

Topologías



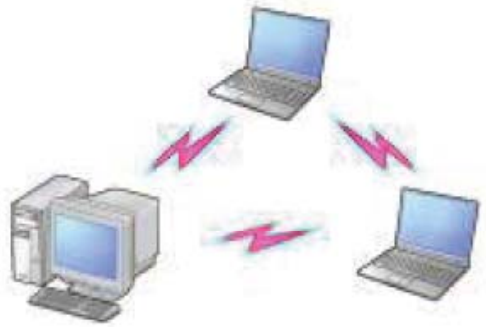
STA: Station
AP: Access Point
DS: Distribution System
BSS: Basic Service Set
ESS: Extended Service Set



Topologías (1)

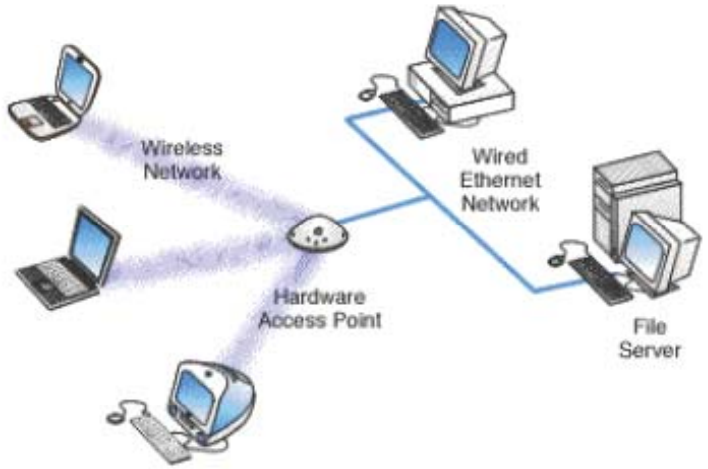
- BSS (Basic Service Set):
  - Conjunto de dispositivos que se comunican entre sí sin utilizar cables (celda).
  - BSSID: identificador de la red. Elemento que debe conocer cada equipo para unirse a la red.

- Topología Ad-hoc:
  - IBSS (Independent Basic Service Set)
  - Conjunto de dos estaciones como mínimo que se reconocen mutuamente según una configuración peer-to-peer.
  - No requieren un punto de acceso.
  - El número de equipos que formen parte de ella dependerá del rendimiento que se quiera obtener.
  - No tienen acceso a redes externas.
  - BSSID: nº aleatorio generado por el primer elemento de la red.



Topologías (2)

- Topología en Infraestructura:
  - Requieren de un Access Point (AP).
  - Sí tienen acceso a redes externas, gracias al AP.
  - Redes con cierta infraestructura y complejidad.
  - Pueden unirse a redes cableadas o conectarse a otras infraestructuras inalámbricas.

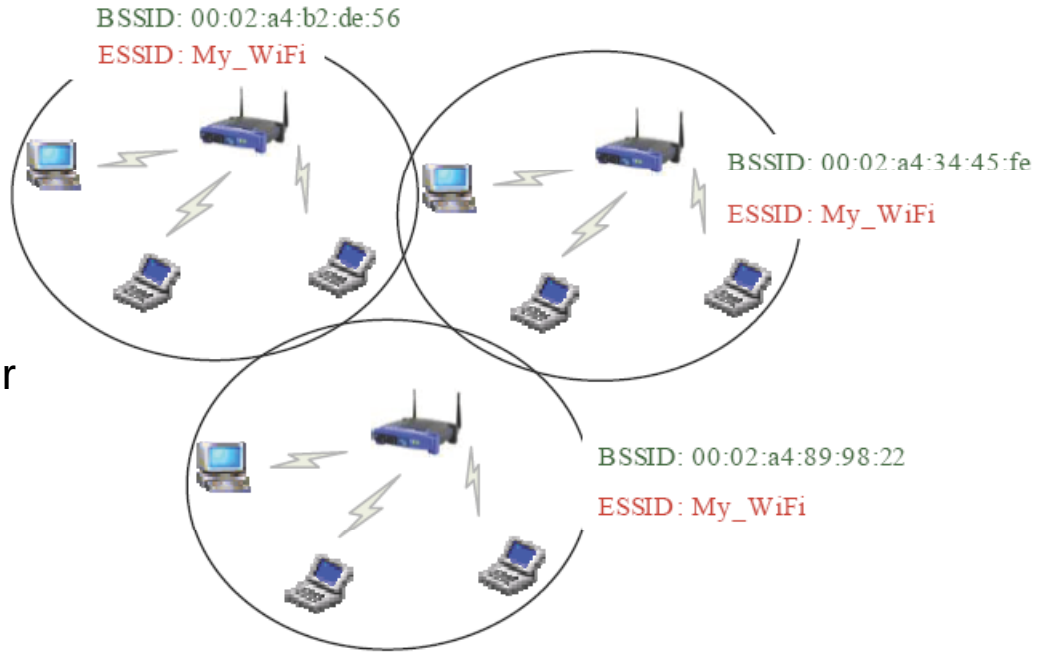


Topologías (3)

- Red en Infraestructura:
  - ESS (Extended Service Set):
    - Conjunto de varias celdas BSS unidas a través de enlaces cableados o inalámbricos.
    - Se consigue una arquitectura de red compleja.
    - Las BSSs pueden pertenecer a la misma o a distintas subredes.

BSSID: dirección MAC del APs

ESSID: Identificador asignado por el administrador para identificar a la red completa.



Seguridad (1)

- Red inalámbrica:
  - Los datos viajan por el espectro radioeléctrico, no se encuentran confinados en ningún medio físico.
  - Los datos llegarán a todos los puntos donde alcance la cobertura de la señal.
    - En el caso de una red WiFi típica, un radio de entre 10-100 metros.
- El equipamiento WiFi es diseñado con el objetivo de facilitar el despliegue de una red WiFi:
  - Los APs pensados para su uso en casas y pequeñas oficinas pueden utilizarse directamente con la configuración de fábrica.
  - SSID (Identificador de red) por defecto del fabricante.
  - Sin encriptación WEP.
  - Antena omnidireccional (emite en todas las direcciones con igual potencia).

Seguridad (2)

- Problemas de seguridad:
  - El funcionamiento de las tarjetas inalámbricas WiFi favorece:
    - la sencillez del despliegue.
    - los problemas de seguridad provenientes de:
      - configuraciones por defecto.
      - desconocimiento de las características del equipamiento.
      - desconocimiento de los mecanismos de seguridad.
  - El propio driver de las tarjetas muestra al usuario un resumen con todas las redes alcanzables:
    - BSSID (dirección MAC) de los APs alcanzables.
    - SSID (identificador) de la red a la que pertenece cada AP.
    - Canal en el que está emitiendo el AP.
  - Esta información mostrada, en el modo de funcionamiento más básico de una red WiFi, es todo lo que necesitamos para poder conectarnos a ella.

Fases de una comunicación inalámbrica

1. El equipo móvil inalámbrico escanea el espectro en busca de actividad:
   - Rastrea todos los canales en busca de puntos de acceso disponibles.
   - Envía peticiones y espera la recepción de anuncios por parte de los APs.
2. En el equipo móvil se muestra al usuario un resumen con las redes alcanzables por razones de cobertura.
   - En cada red aparece, normalmente, sólo el AP del que se recibe una mayor intensidad de señal.
3. El equipo móvil realiza una petición de autentificación contra el punto de acceso.
   - Si esta fase termina adecuadamente el equipo está autentificado.
4. El equipo realiza la asociación con el punto de acceso.
   - En este momento el equipo está asociado con el punto de acceso.
   - A partir de ahora el equipo inalámbrico móvil puede comenzar la transferencia de datos.
     - Con otros equipos inalámbricos incluidos en el rango de cobertura del punto de acceso.
     - Con otros equipos incluidos en la parte cableada de la red.

WEP (Wireless Equivalent Protocol)

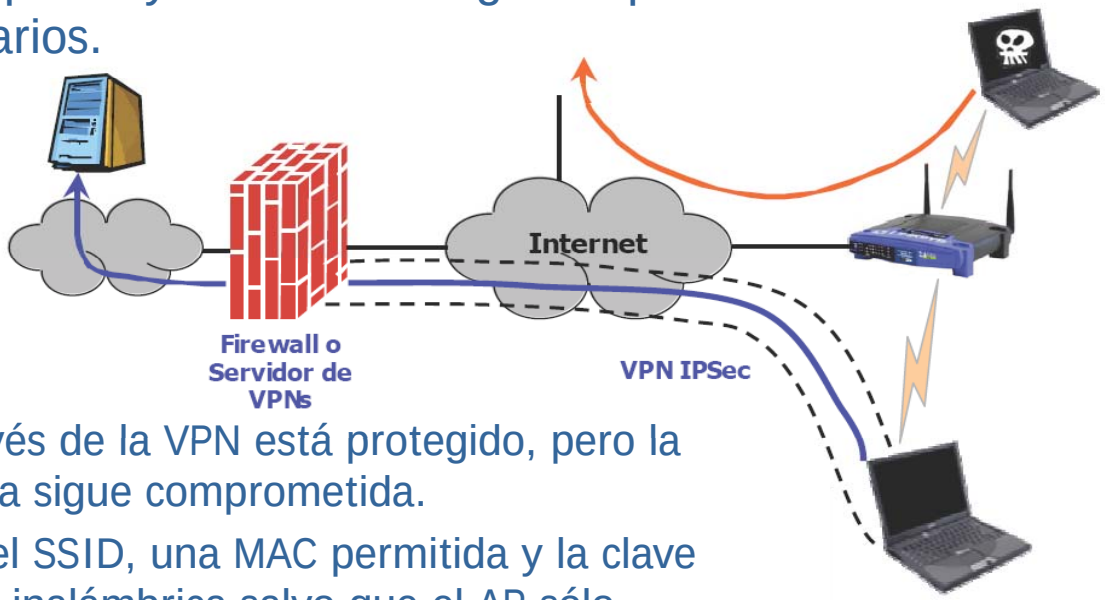
- Cifrado de la información
- Se basa en el algoritmo RC4 desarrollado por RSA Systems
  - El cliente y el punto de acceso comparten una clave que:
    - Permite o deniega la comunicación
    - Encripta/desencripta la comunicación.
  - Versiones con claves de 64 y 128 bits.

Radius

- Autentificación:
  - Proceso para controlar el acceso de los usuarios a la red.
  - IEEE 802.1x: grupo para obtener un estándar de autentificación para redes (cableadas o no).
- Radius: Remote Authenticated Dial-In User Service
  - Infraestructura recomendada por la WiFi Alliance como sistema de gestión centralizada de autentificación para entornos con un elevado número de usuarios.

VPN inalámbricas

- VPN (Virtual Private Network)
  - Solución de seguridad de redes convencionales
  - Se establecen túneles IPSec (Internet Protocol Security)
  - Utiliza algoritmos para la encriptación de datos, otros para la autentificación de paquetes y certificados digitales para la validación de los usuarios.



- Problema:
  - El tráfico que pasa a través de la VPN está protegido, pero la infraestuctura inalámbrica sigue comprometida.
  - Un usuario que consiga el SSID, una MAC permitida y la clave WEP podrá utilizar la red inalámbrica salvo que el AP sólo permita el paso de tráfico de VPN autenticado.

WPA (WiFi Protected Access)

- Nuevo mecanismo de seguridad propuesto por la Wi-Fi Alliance
- Sustituto de WEP
- Mejora la codificación de datos utilizando TKIP (Temporal Key Integrity Protocol)
- Proporciona autentificación de usuarios (IEEE 802.1x y EAP: Extensible Authentication Protocol).
- Escenario: