Seguridad contra ataques en medios inalámbricos

Dr. Luis Gerardo de la Fraga

Departamento de Computación
Cinvestav
Correo-e: fraga@cs.cinvestav.mx

Junio 7, 2014

Contenido parte 1

1. Seguridad en redes
2. Señales de radio
3. IEEE 802.11
4. Redes inalámbricas
5. Interacción de paquetes y redes
6. Instalando una primera red

Los retos de la seguridad en computadoras

La seguridad en computadores y redes es tanto fascinante como compleja. Algunas de las razones son:

1. La seguridad no es tan simple como podría parecer a algún novato. Los requerimientos parecen directos; la mayoría de los requerimientos para servicios de seguridad pueden darse de forma autoexplicatoria, con etiquetas en una sola palabra:
   - confidencialidad,
   - autenticación,
   - no repudio, o
   - integridad

   pero los mecanismos que se usan para alcanzar estos requerimientos son complejos y entenderlos envuelve más que un razonamiento sútil

2. Al desarrollar un mecanismo de seguridad en particular, uno debe de considerar ataques potenciales sobre esas características de seguridad. En muchos casos, ataques exitosos se diseñan mirando el problema desde un punto de vista completamente diferente, explotando una debilidad inesperada en el mecanismo.
3. Debido al punto 2, frecuentemente los procedimientos usandos para proveer servicios particulares no son intuitivos. Típicamente, un mecanismo de seguridad es complejo y no es obvio desde el enunciado de un requerimiento particular que tales medidas elaboradas sean necesarias. Solamente cuando se consideran los distintos aspectos de la tarea es que los mecanismos elaborados tienen sentido

4. La seguridad en las computadores y redes es esencialmente una batalla de ingenio entre el perpetrador que intenta encontrar agujeros de seguridad y el diseñador o administrador quien trata de cerrarlos. La gran ventaja del atacador es que necesita encontrar una sola debilidad, mientras que el administrador debe encontrar y eliminar todas las debilidades para alcanzar una seguridad perfecta.
5. Hay una tendencia natural de parte de los usuarios y los administradores de sistemas a percibir un beneficio pequeño a partir de una inversión en seguridad, hasta que un fallo de seguridad ocurre.

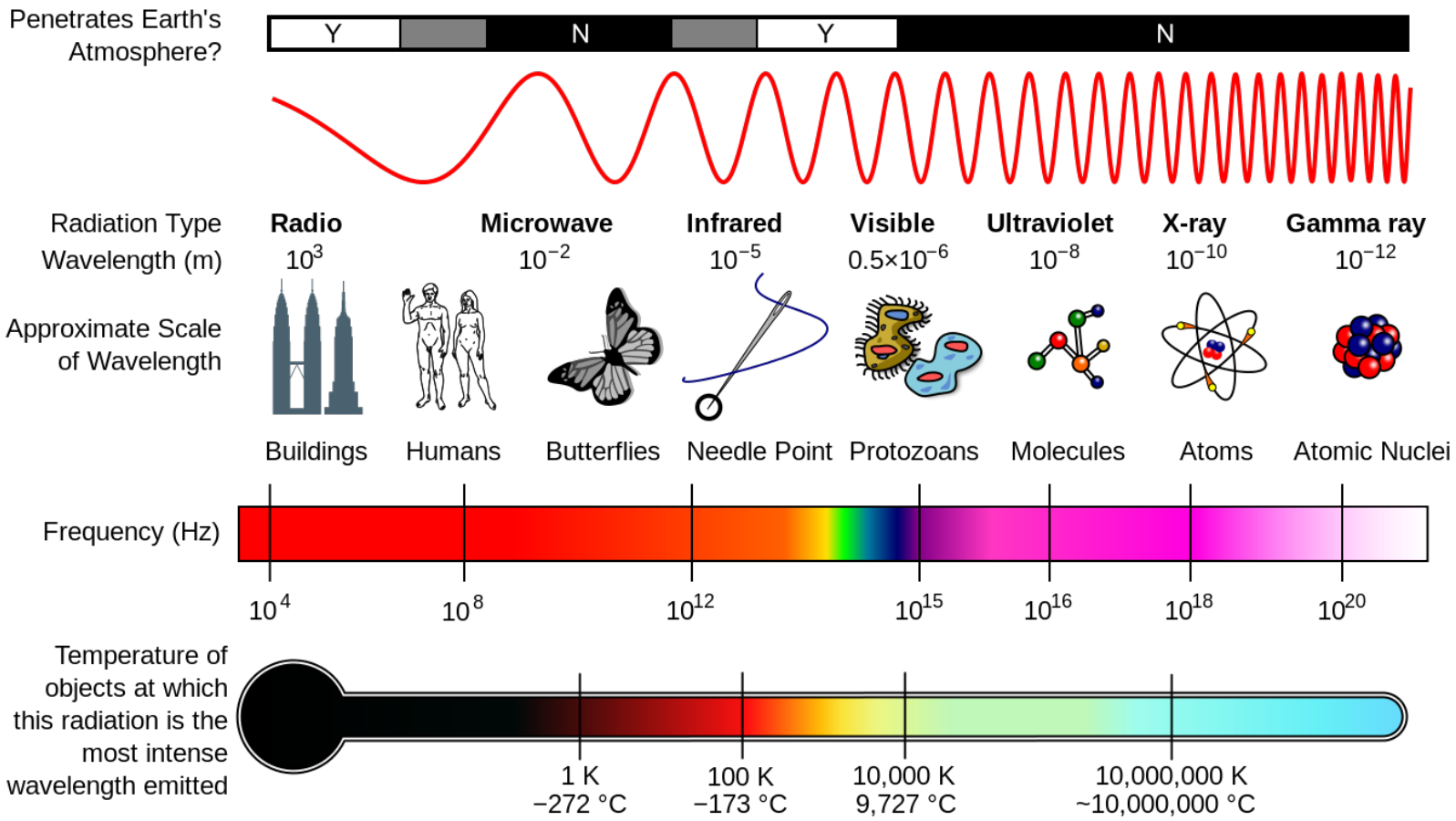
6. La seguridad requiere un monitoreo regular, siempre constante, y esto es difícil hoy en día en nuestros ambientes a corto plazo y sobrecargados
7. La seguridad aún hoy en día se incorpora a los sistemas después de que se completa el diseño, en vez de ser una parte integral del proceso de diseño.
8. Muchos usuarios, y aún administradores de seguridad, ven la seguridad fuerte como un impedimento a la operación eficiente y amigable de un sistema de información.

Señales de radio. El espectro electromagnético

Es la amplitud de todas las posibles frecuencias de la radiación electromagnética

Radiación electromagnética

Es el fenómeno fundamental del electromagnetismo, comportándose como ondas que viajan a través del espacio y también como partículas (fotones) viajando a través del espacio, llevando energía radiante.


Penetrates Earth's Atmosphere?
Y
N
Y
N
Radiation Type
Wavelength (m)
Approximate Scale of Wavelength
Radio
10^{3}
Microwave
10^{-2}
Infrared
10^{-5}
Visible
0.5×10^{-6}
Ultraviolet
10^{-8}
X-ray
10^{-10}
Gamma ray
10^{-12}
Buildings
Humans
Butterflies
Needle Point
Protozoans
Molecules
Atoms
Atomic Nuclei
Frequency (Hz)
10^{4}
10^{8}
10^{12}
10^{15}
10^{16}
10^{18}
10^{20}
Temperature of objects at which this radiation is the most intense wavelength emitted
1 K
−272 °C
100 K
−173 °C
10,000 K
9,727 °C
10,000,000 K
~10,000,000 °C

Las distintas tecnologías inalámbricas

- Radio AM (500 - 1700 KHz [ondas medias de 535 a 1705 KHz])
- Radio FM (88 - 108 MHz)
- Telefonía celular
- 802.11 (2.4 GHz)
- Bluetooth (infrarrojos)

Frecuencias

- Las comunicaciones inalámbricas abarcan el espectro desde 9 KHz a 300 GHz.
- $$\lambda = \frac{c}{f},$$

  donde λ es la longitud de onda, c la velocidad de la luz (3×10^8 m/s) y f representa la frecuencia usada del espectro electromagnético.

- Wifi trabaja a 2.4 GHz
- 2.4×10^9 s^{-1}
- $\frac{1}{2.4} \times 10^{-9} = 0.4167 \times 10^{-9}$ s
- $\lambda = (3 \times 10^8$ m/s$)(0.4167 \times 10^{-9}$ s $=$
- $= 1.2501x10^{-1}$ metros $= 12.5$ centímetros

Frecuencia	Longitud de onda
10 KHz	30 Km
100 KHz	3 Km
300 KHz	1 Km
600 KHz	500 m
1 MHz	300 m
10 MHz	30 m
100 MHz	3 m
1 GHz	30 cm
10 GHz	3 cm
100 GHz	3 mm
300 GHz	1 mm

Bluetooth

La radiación infrarroja que usa bluetooth es de tamaño:

$$10^{-5}\ \text{m} = 0.00001\ \text{m} = 0.001\ \text{cm} = 10 \times 10^{-6}\ \text{m} =$$
$$= 10\ \text{micrómetros}$$

IEEE 802.11

IEEE 802.11 (1/2)

- IEEE 802.11 es un estándar para construir redes locales inalámbricas.
- Fue realizado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE en inglés)
- La primera especificación fue terminada en 1997
- Las realizaciones que pueden interoperar entre ellas y están de acuerdo con el estándar se les conoce como Wi-Fi.

IEEE 802.11 (2/2)

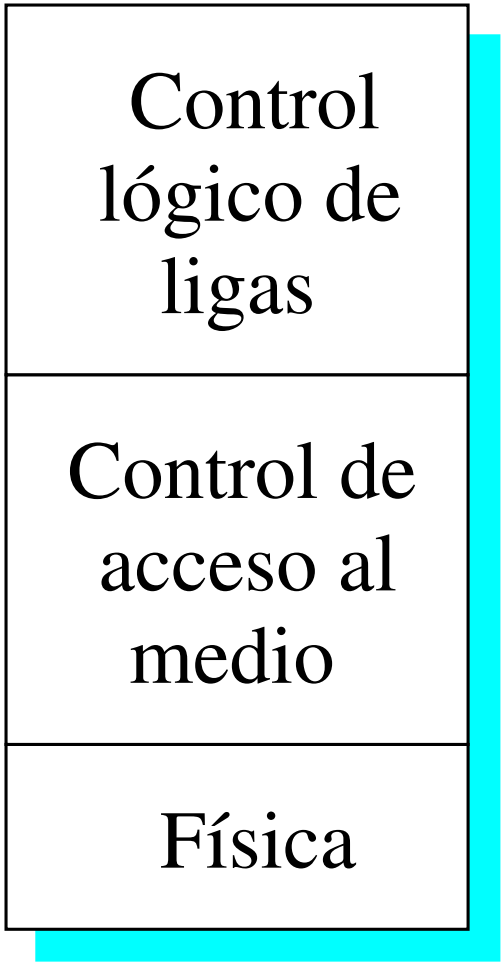
- El primer estándar que logró una aceptación amplia en la industria fue el 802.11b
- Las especificaciones usan las bandas de frecuencia de 2.4, 3.6, 5 y 60 GHz.
- 802.11b usa la banda de 2.4 GHz
- Otra especificación usada apliamente es la 802.11g (usa tambien la banda de 2.4 GHz)
- Otras son la 802.11a y la 802.11n
- Las especificaciones c–f, h y j son enmiendas (correcciones y extensiones) a las especificaciones previas

- IEEE 802.11-1997: El estándar original para realizar WLAN a 1 Mbit/s y 2 Mbit/s, a 2.4 GHz e infrarrojos
- IEEE 802.11a: 54 Mbit/s, 5 GHz (1999, venta de productos en 2001)
- IEEE 802.11b: Mejoras al 802.11 para lograr 5.5 y 11 Mbit/s (1999)
- IEEE 802.11c: Operaciones para operar puertes
- IEEE 802.11d: Extensiones para roaming internacional (2001)
- IEEE 802.11e: Mejora: Calidad de Servicio (Quality of Service) (2005)
- IEEE 802.11f: Protocolo para inter puntos de acceso (2003) Retirado en febrero de 2006
- IEEE 802.11g: 54 Mbit/s, 2.4 GHz (compatibilidad con b) (2003)
- IEEE 802.11h: Manejo del espectro 802.11a (5 GHz) para compatibilidad europea (2004)

- IEEE 802.11i: Mejoras en la seguridad (2004)
- IEEE 802.11j: Extensiones para Japón (2004)
- IEEE 802.11-2007: Nueva versión del estándar que incluye las enmiendas a, b, d, e, g, h, i y j (julio 2007)
- IEEE 802.11k: Mejoras para la medición de recursos de radio (2008)
- IEEE 802.11n: Rendimiento más alto usando MIMO (antenas multiple input, multiple output) (septiembre 2009)
- IEEE 802.11-2012: Nueva versión del estándar que incluye las enmiendas k, n, p, r, s, u, v, w, y and z (marzo 2012)

Fuente: `http://en.wikipedia.org/wiki/IEEE_802.11`

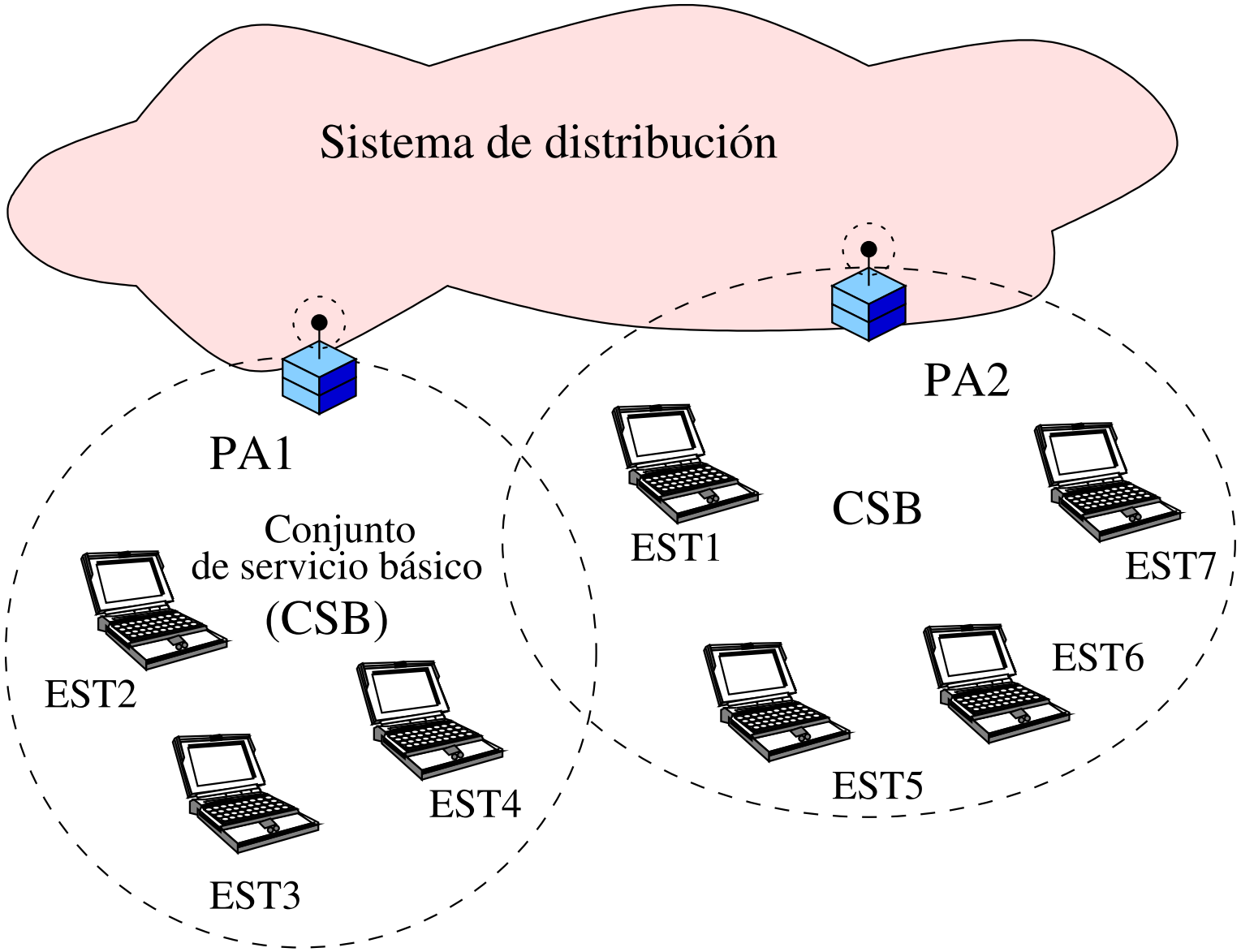
La pila del protocolo IEEE 802.11



Arquitectura del protocolo IEEE 802.11

Capa	Funciones generales IEEE 802	Funciones específicas del 802.11
Control lógico de ligas	Control de flujo Control de errores	
Control de acceso al medio	Ensamblar datos en una trama Direccionamiento Deteccion de errores Acceso al medio	 Entrega segura de datos Protocolos de control de acceso inalámbrico
Capa física	Señales para codificar/decodificar Recepción/transmisión de bits Medio de transmisión	Definición de la banda de frecuencia Codificación de la señal inalámbrica

Redes inalámbricas (1/4)



Conjunto de servicio extendido del IEEE 802.11

Redes inalámbricas (2/4)

- El bloque de construcción básico es un **conjunto de servicio básico** (BSS en inglés)
- Un CSB consiste de estaciones inalámbricas ejecutando el mismo protocolo MAC y compitiendo por el acceso al mismo medio inalámbrico compartido.
- Puede haber una o varios CSB conectados a una espina dorsal (un *sistema de distribución* [SD]) a través de un **punto de acceso** (PA)
- El PA funciona como un puente o como un punto de retransmisión

Redes inalámbricas (3/4)

- Una estación cliente dentro de un CSB no se comunica directamente a otra estación
- La estación se comunica al PA y el PA al otro cliente
- La CSB corresponde a una *celda*
- El SD puede ser un switch, otra red inalámbrica o una red alámbrica

Redes inalámbricas (4/4)

- Cuando las estaciones se comunican directamente sin usa un PA, el CSB se le llama **CSB independiente** (IBSS en inglés)
- Un CSBI es una red ad hoc donde todas las estaciones se comunican directamente
- Un **conjunto de servicio extendido** (ESS en inglés) consiste de dos o más CSBs interconectados por un sistema de distribución.
- Todo un CSB aparece como una sola red local

Modos de operación de una tarjeta inalámbrica

Existen seis modos en los que puede operar una tarjeta inalámbrica:

1. Modo **maestro** (master), actuando como un punto de acceso
2. **Gestionado** (managed), funcionando como un cliente, conocido también como una *estación*
3. Modo **ad hoc**
4. **En malla**
5. Modo **repetidor**, y
6. Modo en monitoreo (monitor)

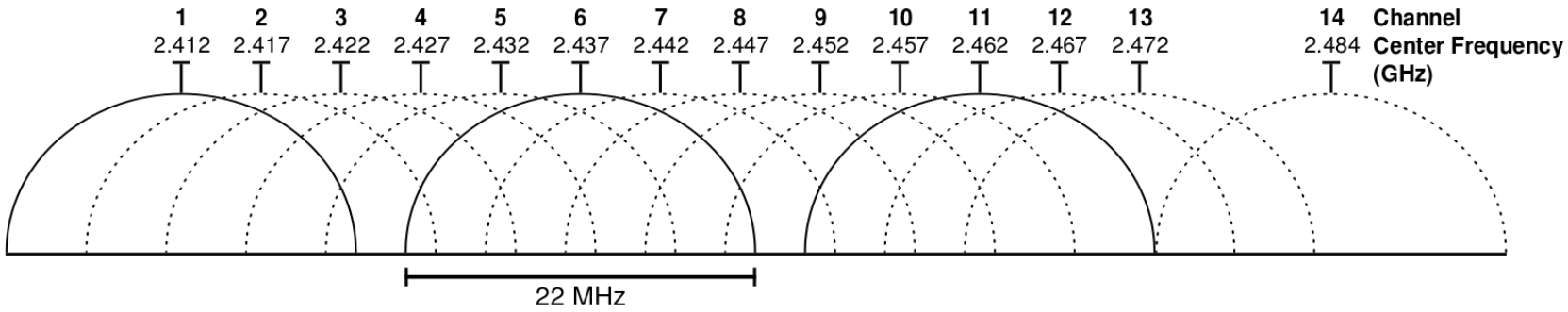
Para una tarjeta de red inalámbrica se puede checar sus capacidades:

- Primero checar el módulo que está usando (lsmod, dmesg, etc.)
- Luego checar las capacidades de ese driver en Linux en: `http://en.wikipedia.org/wiki/Comparison_of_open-source_wireless_drivers#Driver_capabilities`

Modo monitor

- Permite a un controlador de la interfaz de una red inalámbrica (WNIC en inglés) monitorear todo el tráfico que recibe de la red inalámbrica
- Este modo permite capturar los marcos sin estar asociado a un punto de acceso o a una red ad hoc
- Se usa para análisis geográfico de marcos observando como se esparse el tráfico
- Es también útil durante la fase de diseño de redes Wi-Fi para descubrir cuantos dispositivos Wi-Fi ya están usando el espectro dentro de un área y que tan ocupados están los canales Wi-Fi en esa misma área.

Canales en la banda de 2.4 GHz (802.11b) (1/5)



- El ancho de los canales es de 22 MHz
- Existen tres canales sin sobrelapamiento (1, 6, 11)

[a]http://en.wikipedia.org/wiki/802.11

[a] \unskip\penalty\@M\vrulewidth\z@height\z@depth\dpff

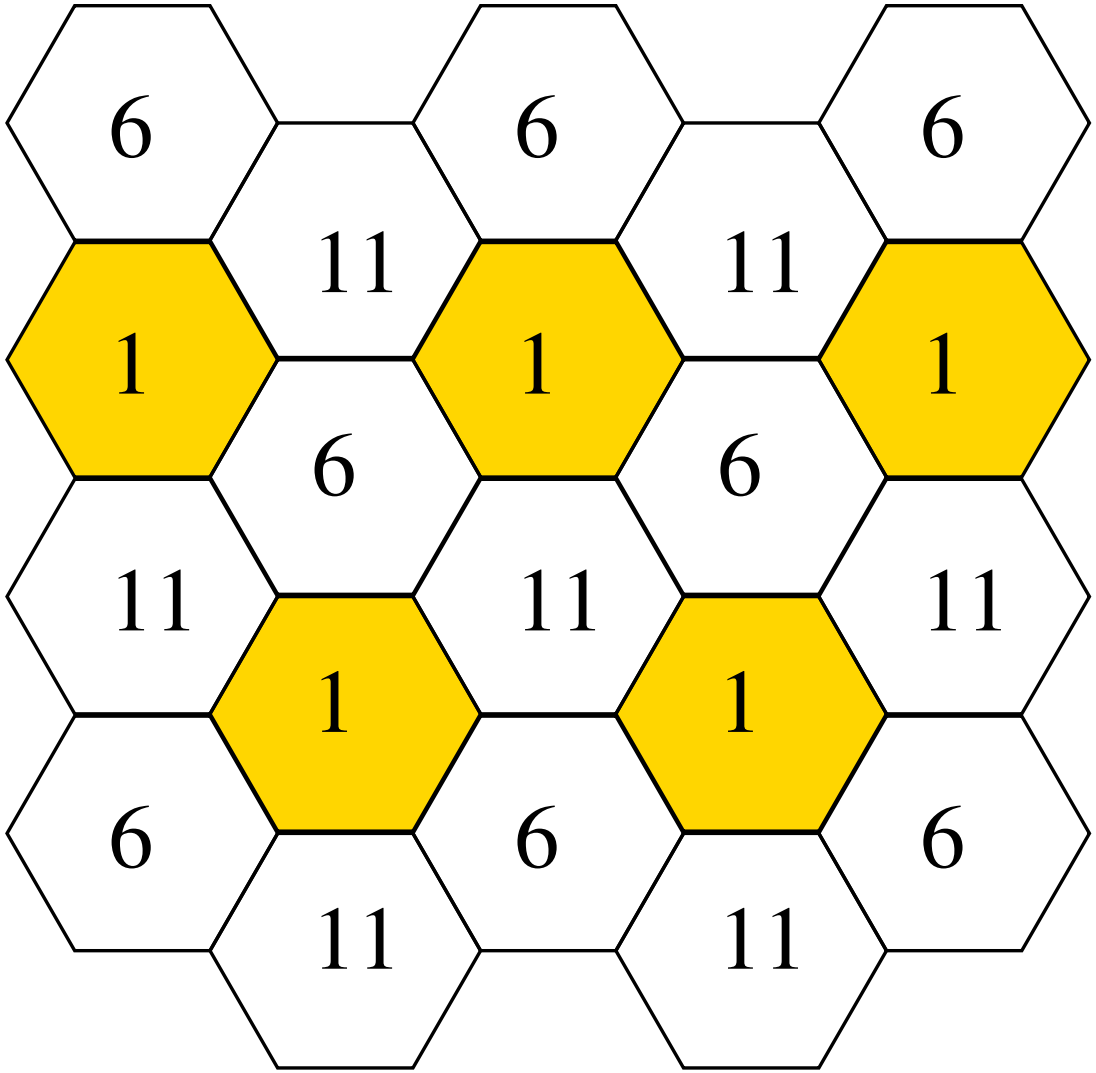
Pero casi no existe degradación de la señal si se usan los canales 1, 5, 9, 13

E.G. Villegas, E. Lopez Aguilera, R. Vidal and J. Paradells, Effect of adjacent-channel interference in IEEE 802.11 WLANs, 2nd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2007. CrownCom 2007. 1-3 Aug 2007, pp 118- 125.

Canales en la banda de 2.4 GHz (802.11b) (2/5)

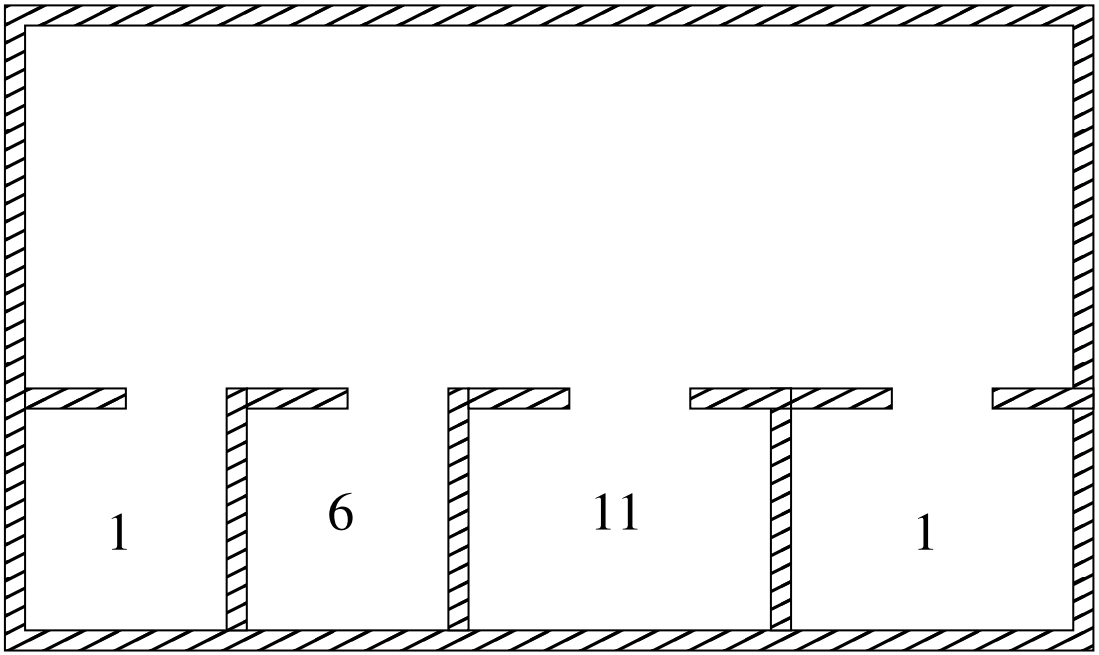
Identificador	Frecuencia	Dominios de regulación				
		America	EMEA	Israel	China	Japón
1	2412 GHz	X	X	–	X	X
2	2417 GHz	X	X	–	X	X
3	2422 GHz	X	X	X	X	X
4	2427 GHz	X	X	X	X	X
5	2432 GHz	X	X	X	X	X
6	2437 GHz	X	X	X	X	X
7	2442 GHz	X	X	X	X	X
8	2447 GHz	X	X	X	X	X
9	2452 GHz	X	X	X	X	X
10	2457 GHz	X	X	–	X	X
11	2462 GHz	X	X	–	X	X
12	2467 GHz	–	X	–	–	X
13	2472 GHz	–	X	–	–	X
14	2484 GHz	–	–	–	–	X

Canales en la banda de 2.4 GHz (802.11b) (3/5)



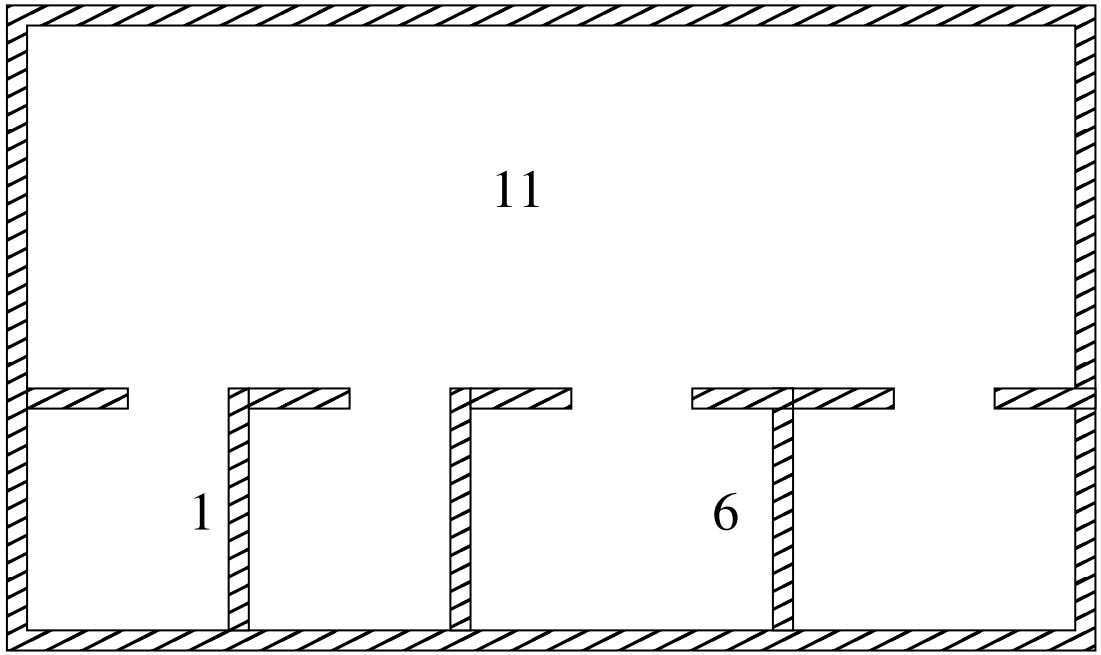
Distribución de los canales

Canales en la banda de 2.4 GHz (802.11b) (4/5)



Distribución de los canales

Canales en la banda de 2.4 GHz (802.11b) (5/5)



Distribución de los canales

Canales en la banda de 5 GHz (802.11a)

- Diferentes países aplican sus propias regulationes sobre los canales que pueden usarse, los usuarios que pueden usarlos y los niveles de potencia máximos en esas bandas de frecuencia.
- En 2007 el FCC (en los Estados Unidos de América) comenzó a requerir que los dispositivos que operan en 5.250–5.350 GHz y 5.470–5.725 GHz deben emplear selección dinámica de la frecuencia y control de la potencia de transmisión. Esto debe realizarse para evitar interferencias con radares del clima y aplicaciones militares.

Prácticas

Funciones capa MAC

- Controlar el canal de acceso
- Mantener la calidad de servicio
- Proveer seguridad

Paquetes inalámbricos, los marcos MAC del 802.11

- La capa MAC recibe datos de una capa superior
- Los datos vienen como una unidad de datos de servicio (MSDU, MAC Service Data Unit)
- En la transmisión, la capa MAC ensambla los datos en un **marco** conocido como unidad de datos del protocolo MAC (MPDU, MAC Protocol Data Unit)
- En la recepción, desensambla el marco y realiza el reconocimiento de la dirección y la detección de errores
- También gobierna el acceso al medio de transmisión de la red

Forma de un UDPM

La forma exacta defiere según el protocolo MAC, pero en general tiene la forma:

Control	Dirección destino	Dirección fuente	Unidad de datos de servicio UDS	CRC

- Control: Este campo contiene cualquier información de control para el protocolo, necesaria para el funcionamiento del protocolo MAC. Por ejemplo, los niveles de prioridad se podrían especcificar aquí.
- Dirección de destino: especifica la dirección física de destino sobre la red local para este UDPM
- Dirección fuente: especifica la dirección física fuente sobre la red local para este UDPM
- Unidad de Datos de Servicio: los datos de la capa superior siguiente
- CRC: el chequeo redundante cíclico. Este es un código para detección de errores. Se calcula con los bits de todo el UDPM. El que envía calcula el CRC y lo adiciona al marco. El que recibe realiza los mismos cálculos sobre el UDPM que recibe, si los dos valores no son iguales, entonces uno a más bits fueron alterados en el tránsito.

Los nueve servicios del 802.11

Servicio	Proveedor	Usado para
Asociación	Sistema de distribución	Entrega de UDSM
Atenticación	Estación	Acceso y seguridad en la red local
Desautenticación	Estación	Acceso y seguridad en la red local
Desasociación	Sistema de distribución	Entrega de UDSM
Distribución	Sistema de distribución	Entrega de UDSM
Integración	Sistema de distribución	Entrega de UDSM
Entrega de UDSM	Estación	Entrega de UDSM
Privacidad	Estación	Acceso y seguridad en la red local
Reasociación	Sistema de distribución	Entrega de UDSM

- Los dos servicios involucrados con la distribución de mensajes dentro de un SD son **distribución** e **integración**
- **Distribución** es el servicio primario usado por las estaciones para intercambiar UDPM cuando las UDPM deben atravesar el SD para alcanzar una estación en un CSB a otra estación en otro CSB.

- Antes de que el servicio de distribución pueda entregar o aceptar datos desde una estación, la estación debe estar **asociada**
- El estándar define tres tipos de transición basados en la mobilidad:
  - Sin transición: una estación de este ripo o está estacionaria o se mueve solo dentro de la amplitud de comunicación directa de las estaciones en un solo CSB
  - Transición en un CSB: esto define a una estación moviéndose de un CSB a otro CSB dentro del mismo CSE. Se requiere que la capacidad de dereccionamiento puede reconocer la localidad nueva de la estación
  - Transición en un CSE. Este caso se apoya solo en el sentido de que la estación puede moverse. El 802.11 no soporta el mantenimiento de estas conexiones, de hecho se espera que pueda ocurrir una interrupción del servicio.

- El SD necesita conocer la identidad del PA al cual entregará un mensaje
- Para esto, una estación debe mantener una asociación con el PA con su CSE actual.
- Tres servicios están relacionados a este requerimiento:
  - **Asociación**: Establece una asociación inicial entre una estación y un PA. Antes de que una estación pueda transmitir o recibir marcos en una red inalámbrica, su identidad y dirección debe conocerse. Para este propósito una estación debe establecer una asociación con un PA dentro de un CSB particular. El PA puede entonces comunicar esta información a otro PA dentro del CSE para facilitar el ruteo o entregar marcos direccionados.
  - **Reasociación**: Habilita una asociación establecida para ser transmitida desde un PA a otro, permitiendo a una estación móvil moverse de un CSE a otro.
  - **Disasociación**: Una notificación desde una estación o un PA de que se termina una asociación existente. Un estación debería dar esta notificación antes de dejar un CSE o cuando de apaga. Sin embargo, el manejo de MAC facilita protección a sí mismo contra estaciones que desaparecen sin notificarlo.

Marcos guía

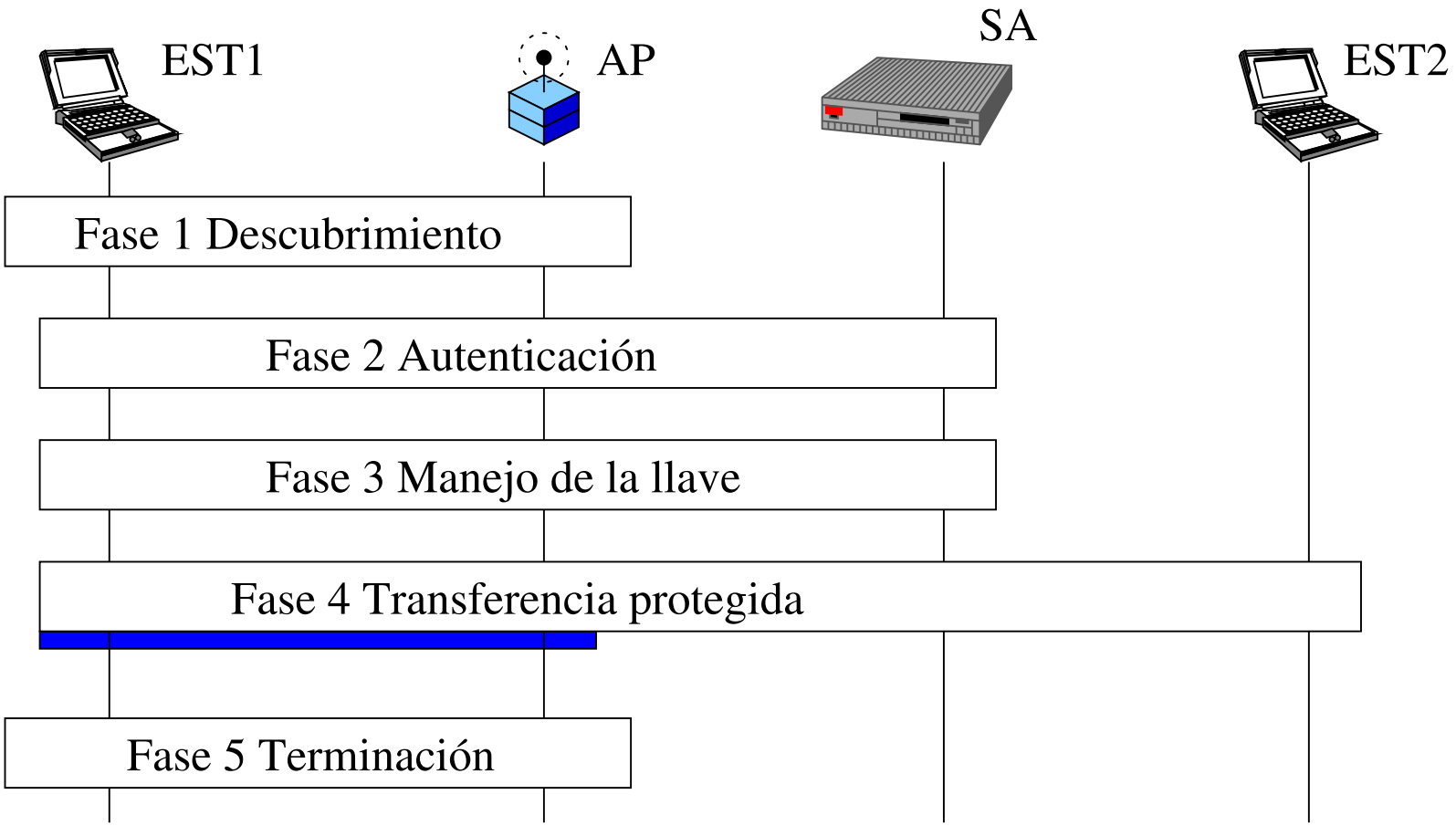
- Cada PA envía cerca de 10 marcos cada segundo de los que se le llama **marcos guía** (beacon frames)
- Estos marcos contienen la siguiente información:
  - Nombre de la red (ESSID)
  - Si se una encriptación (y cual encriptación se usa; puede ser que el dato no sea cierto solo porque lo envia el PA)
  - Cuál es la velocidad de transmisión en MBits
  - Cuál canal de la red se está usando

Estados del IEEE 802.11

- No autenticado, no asociado
- Autenticado, no asociado
- Autenticado y asociado

- Para conectarse a una red inalámbrica existen varias posibilidades.
- En la mayoría de los casos, se usa la Autenticación de Sistema Abierto:
  - Se pregunta al PA para autenticarse
  - El PA contesta: OK, estás autenticado
  - Se pregunta al PA para asociarse
  - El PA contesta: OK, estás ahora conectado.

Fases de operación del 802.11i



Privacidad

- Para privacidad, el 802.11 define el algoritmo de Privacidad Equivalente a la de Alambres (WEP, del inglés Wired Equivalent Privacy)
- La porción de privacidad del estándar 802.11 contiene debilidades mayores
- El grupo de desarrollo del 802.11i desarrolló un conjunto de capacidades para solventar los problemas de seguridad en las redes inalámbricas.
- Para acelerar la introducción de seguridad fuerte en las redes inalámbricas, la Alianza Wi-Fi promulgó el estándar de Acceso Protegido Wi-Fi (WPA, del inglés Wi-Fi Protected Access)