PAR - Unidad 6

Conexión de LANs: protocolos de la capa de enlace de datos:

IEEE 802.11 - WLAN y 802.15- WPAN

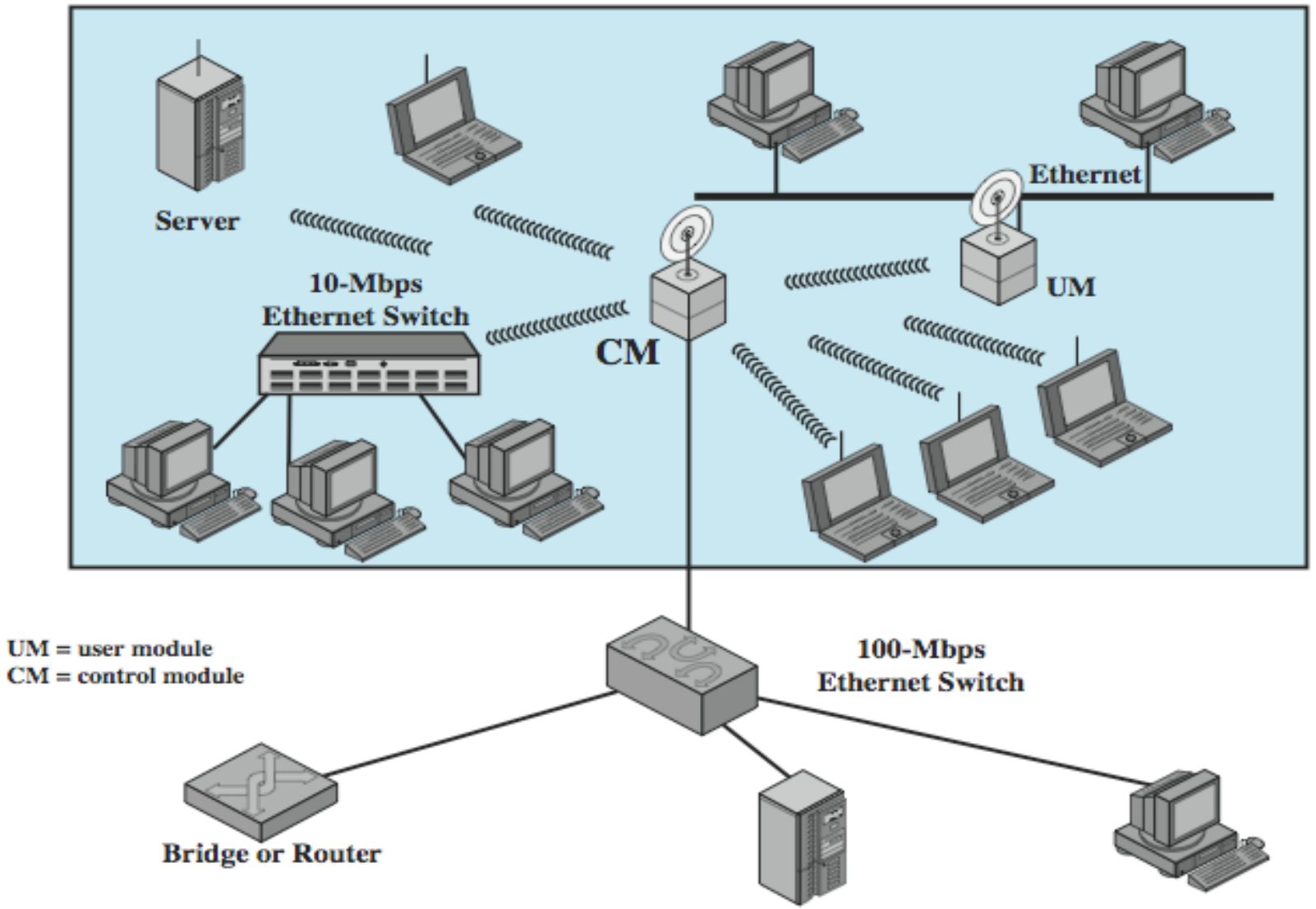
Visión General

- Uso de transmisión de radio:
  - para sustituir a redes cableadas preexistentes
  - para facilitar la movilidad de los usuarios
- Aplicaciones según el área de cobertura:
  - redes personales inalámbricas (*Bluetooth*):~10m
  - redes locales inalámbricas (Wifi): ~100m
  - redes inalámbricas metropolitanas (WiMAX) y de telefonía móvil (GSM/UMTS): hasta decenas kms.
  - futura integración de estos y otros sistemas inalámbricos
- Estándares: comparativa

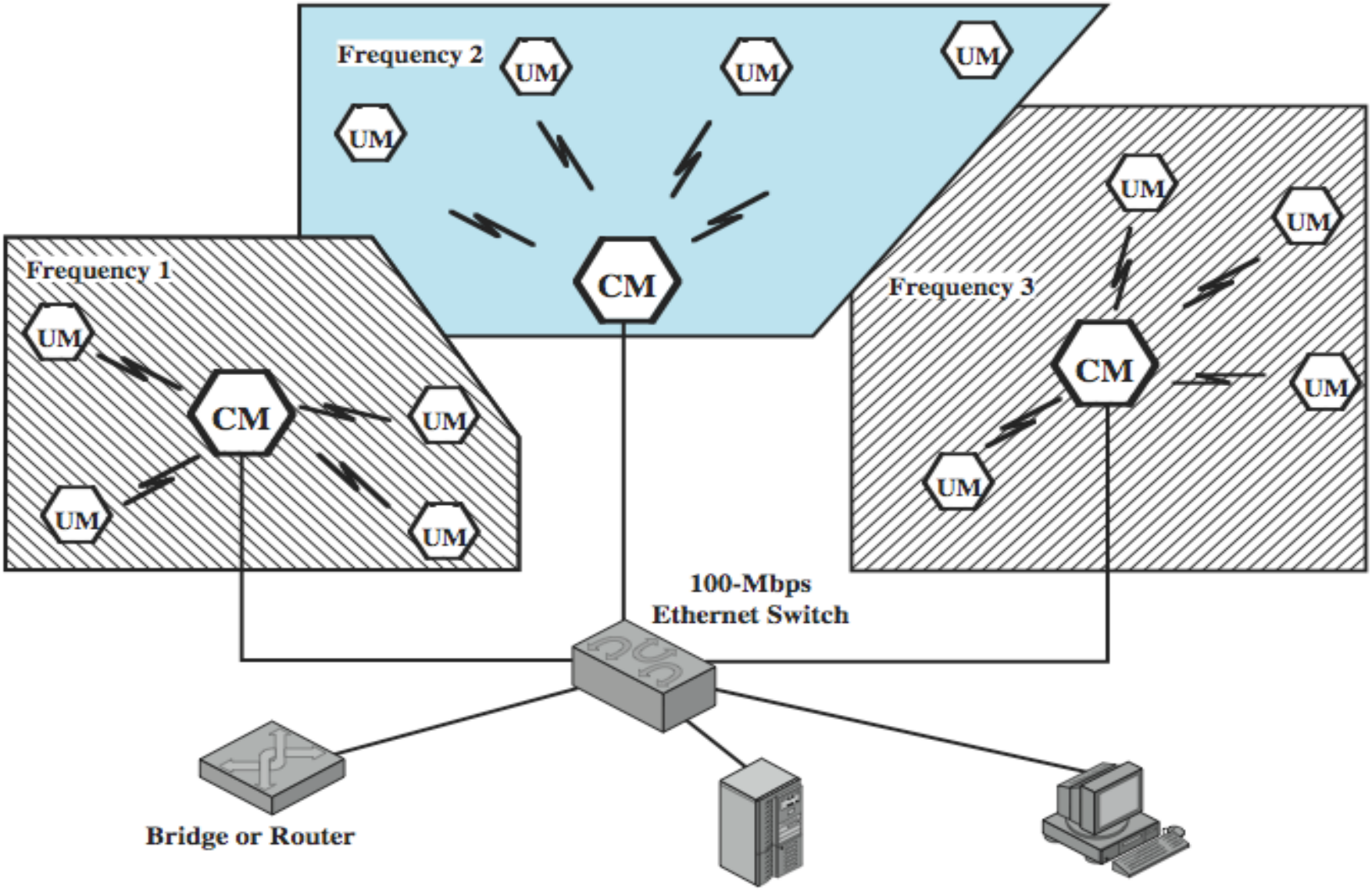
WLANs - Aplicaciones

- Ampliación de redes LAN (modo infraestructura)
  - rebaja costes
  - redes mixtas
- Interconexión de edificios próximos
  - conexión punto a punto de Puntos de accesos (A.P., o *bridge* inalámbrico)
- Acceso nómada (*Road warriors*)
- Creación de redes P2P temporales (modo *adhoc)*

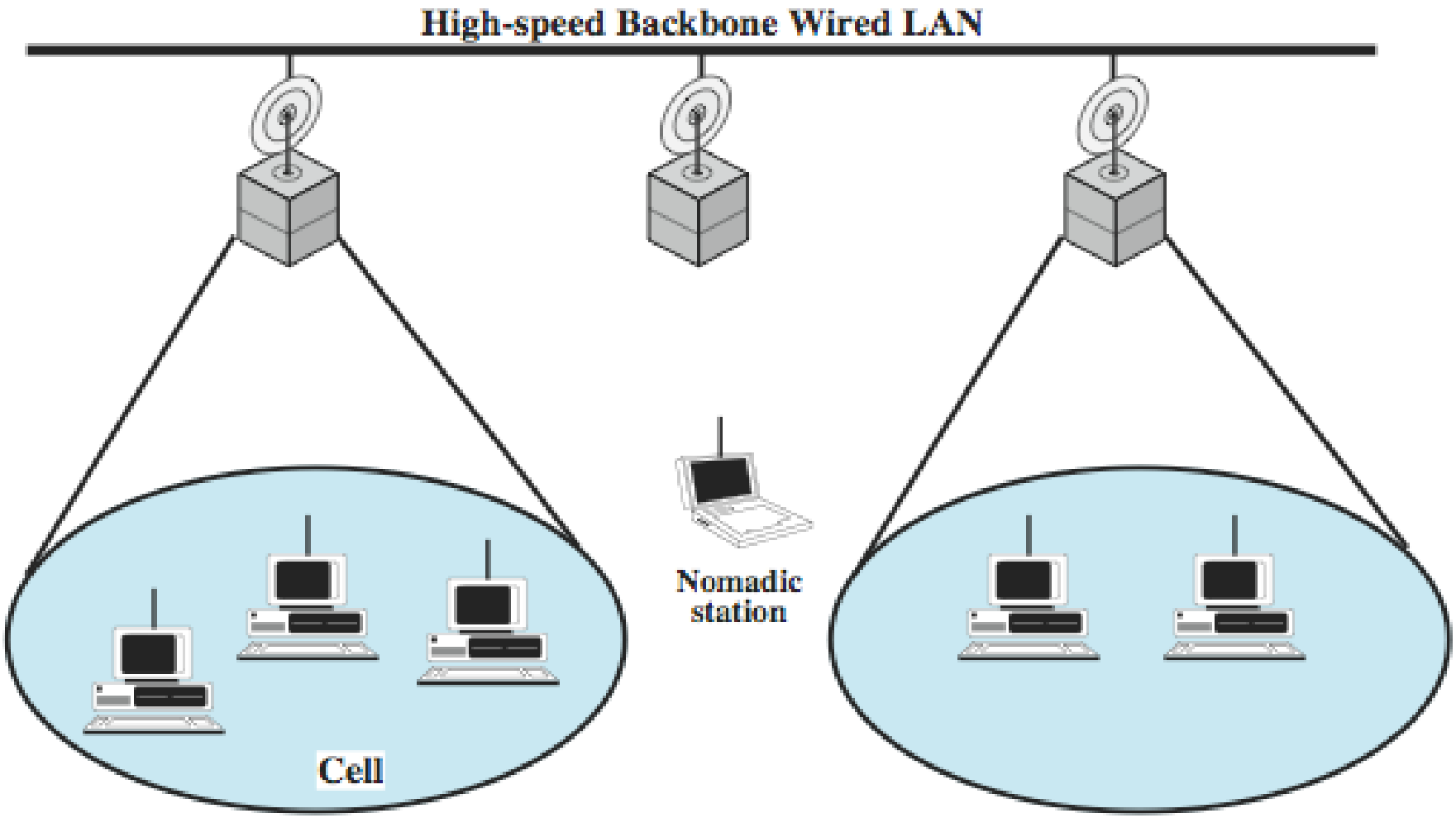
Extensión LAN - celda única



Extensión LAN- celdas múltiples

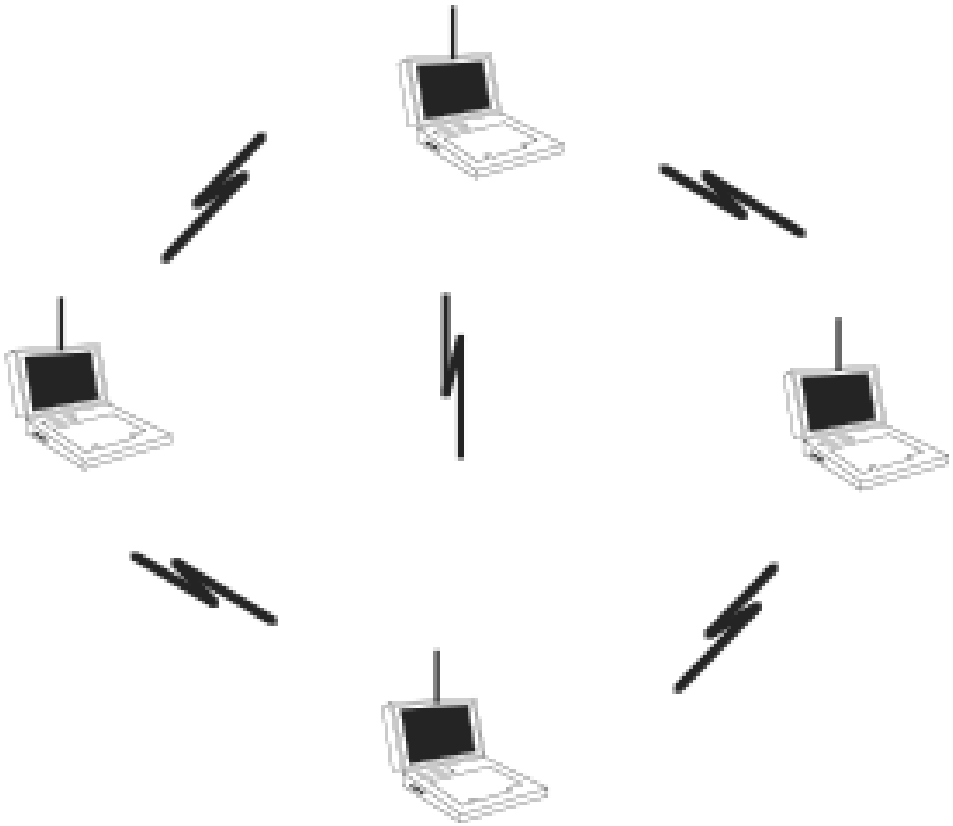


WLAN - Modo Infraestructura



(a) Infrastructure Wireless LAN

WLAN - Modo Adhoc



(b) Ad hoc LAN

WLAN - Requerimientos

- Rendimiento – uso eficiente del medio inalámbrico
- Nº de nodos - cientos de nodos en varias celdas
- Conexión a la LAN troncal
- Área de servicio - de 100 a 300 m
- Consumo de baja potencia
- Robustez y seguridad en la transmisión
- Funcionamiento junto a redes adyacentes
- Funcionamiento sin licencia de transmisión
- Traspasos (*handoff*)/itinerancia (*roaming*)
- Configuración dinámica - inserción, eliminación y reubicación de sistemas finales sin afectar a otros usuarios

IEEE 802.11

- **WLANs infrarrojas** (IR)
  - celda individual de LAN IR limitada por paredes
  - IR no atraviesan las paredes
- **WLANs de radiofrecuencia** (R.F.) **y espectro expandido** (E.E.)
  - opera en la banda ISM (*industrial, scientific, and medical*)
  - no se requiere licencia de uso

WLANs RF

- Se suelen organizar en múltiples celdas
- Las celdas adyacentes utilizan diferentes frecuencias para evitar interferencias
- Configuraciones:
  - con nodo central (*access point*) o infraestructura
    - conectado a una LAN alámbrica
    - conecta las estaciones a la LAN alámbrica y a otras celdas
    - puede hacer traspaso automático entre celdas
    - puede optarse por un MAC sin contienda o con contienda
  - p2p (*peer-to-peer*) o *ad hoc*
    - no necesita nodo central
    - MAC con contienda: algoritmo CSMA para resolver las colisiones

WLANs RF - Transmisión

- La regulación del espectro difiere entre países
- Bandas ISM (industrial científico médica):
  - emisiones de baja potencia.
  - algunas bandas ISM
    - 902 - 928 MHz (banda 915-MHz)
    - 2.4 - 2.4835 GHz (banda 2.4-GHz)
    - 5.420 - 5.725 GHz (banda 5.8-GHz)
- Interferencia
  - bastantes dispositivos en la banda de 900 MHz: teléfonos y micrófonos sin cables, móviles GSM, ...
  - muchos dispositivos en la banda de 2.4 GHz
  - menos competencia, por ahora, en la banda de 5.8 GHz
- Antenas
  - Importancia de la antena usada y su orientación

IEEE 802.11 - Estándares

Standard	Scope
IEEE 802.11	Medium access control (MAC): One common MAC for WLAN applications
	Physical layer: Infrared at 1 and 2 Mbps
	Physical layer: 2.4-GHz FHSS at 1 and 2 Mbps
	Physical layer: 2.4-GHz DSSS at 1 and 2 Mbps
IEEE 802.11a	Physical layer: 5-GHz OFDM at rates from 6 to 54 Mbps
IEEE 802.11b	Physical layer: 2.4-GHz DSSS at 5.5 and 11 Mbps
IEEE 802.11c	Bridge operation at 802.11 MAC layer
IEEE 802.11d	Physical layer: Extend operation of 802.11 WLANs to new regulatory domai (countries)
IEEE 802.11e	MAC: Enhance to improve quality of service and enhance security mechanis
IEEE 802.11f	Recommended practices for multivendor access point interoperability
IEEE 802.11g	Physical layer: Extend 802.11b to data rates >20 Mbps
IEEE 802.11h	Physical/MAC: Enhance IEEE 802.11a to add indoor and outdoor channel selection and to improve spectrum and transmit power management
IEEE 802.11i	MAC: Enhance security and authentication mechanisms
IEEE 802.11j	Physical: Enhance IEEE 802.11a to conform to Japanese requirements
IEEE 802.11k	Radio resource measurement enhancements to provide interface to higher la for radio and network measurements
IEEE 802.11m	Maintenance of IEEE 802.11-1999 standard with technical and editorial corrections
IEEE 802.11n	Physical/MAC: Enhancements to enable higher throughput
IEEE 802.11p	Physical/MAC: Wireless access in vehicular environments
IEEE 802.11r	Physical/MAC: Fast roaming (fast BSS transition)
IEEE 802.11s	Physical/MAC: ESS mesh networking
IEEE 802.11,2	Recommended practice for the Evaluation of 802.11 wireless performance
IEEE 802.11u	Physical/MAC: Interworking with external networks

Pila de Protocolos 802.11

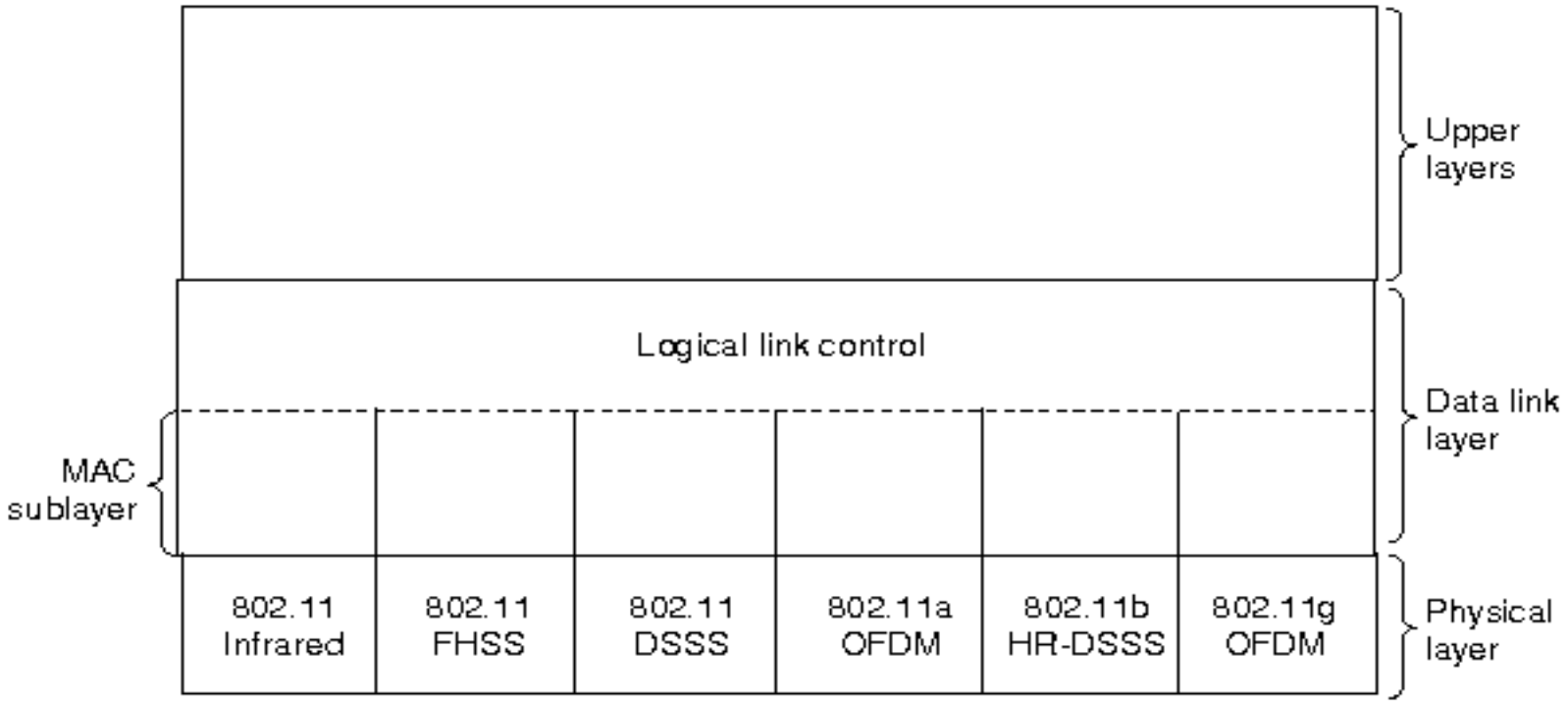


Fig. 4-25. Part of the 802.11 protocol stack.

IEEE 802.11 - Capa Física

	802.11	802.11a	802.11b	802.11g
Available bandwidth	83.5 MHz	300 MHz	83.5 MHz	83.5 MHz
Unlicensed frequency of operation	2.4 - 2.4835 GHz DSSS, FHSS	5.15 - 5.35 GHz OFDM 5.725 - 5.825 GHz OFDM	2.4 - 2.4835 GHz DSSS	2.4 - 2.4835 GHz DSSS, OFDM
Number of non-overlapping channels	3 (indoor/outdoor)	4 indoor 4 (indoor/outdoor) 4 outdoor	3 (indoor/outdoor)	3 (indoor/outdoor)
Data rate per channel	1, 2 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 11 Mbps	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
Compatibility	802.11	Wi-Fi5	Wi-Fi	Wi-Fi at 11 Mbps and below

IEEE 802.11 - FHSS

- E. E. por Salto de Frecuencia
  - banda ISM 2,400-2,495 GHz dividida en 95 canales de 1MHz: el 1º (2,401GHz), ...
  - en Europa se usan del 2 al 79
  - la señal salta entre múltiples canales basándose en una secuencia pseudo-aleatoria (pseudo-ruido) establecida en el estándar
  - el tiempo de permanencia es de unos 0,4 segundos y el salto dura menos de 224 microsegundos
- Velocidad de 1 y 2 Mbps
- Modulación:
  - BFSK para 1 Mbps
  - MFSK-4 para 2 Mbps

IEEE 802.11 - DSSS

- E. E. de Secuencia Directa
- Banda ISM 2.4 GHz a 1 y 2 Mbps
- Depende de ancho de banda asignado por los distintas regulaciones nacionales
  - banda ISM 2,412-2,484GHz en 14 canales de 5MHz
  - se usan 13 canales en Europa (11 en USA y 14 en Japón)
  - por cada canal la energía se propaga en una banda de 22MHz, por lo que debemos asignar las redes solapadas a canales suficientemente separados (p.e., 1, 6 y 11)
- Multiplexión:
  - cada bit se transmite como 11 chips (secuencia Barker)
- Modulación:
  - DBPSK para 1Mbps
  - DQPSK para 2Mbps

IEEE 802.11a

- Usa la banda ISM de 5GHz
- Multiplexión:
  - OFDM (*orthogonal FDM*): FDM de canales superpuestos entre los que se reparte la transmisión de los bits
  - canales de 20 Mhz compuesto por 52 subportadoras (48 de datos y 4 piloto) separadas por 0,3125MHz
  - cada canal usa códigos de convolución para corregir errores hacia delante (FEC)
- Modulación:
  - cada subportadora puede usar BPSK, QPSK, 16QAM o 64QAM
- Velocidades de 6, 9, 12, 18, 36, 48 y 54 Mbps

IEEE 802.11b

- Usa la banda de 2.4GHz
  - 14 canales de 5MHz
- Extensión de DSSS:
  - usa CCK (*Complementary Code Keying*) en vez de las secuencias Barker
  - que da una tasa de datos mayor con el mismo ancho de banda y tasa de chips
- Ancho de banda de la transmisión por canal de 22MHz
  - hay solapamiento entre canales, se deben dejar al menos 4 libres
- Tasas de datos de 1, 2, 5.5 y 11 Mbps

IEEE 802.11g

- Opera en la banda de 2.4GHz
- Extensión de alta velocidad del 11b (compatible)
- Combina los esquemas de las capas físicas usadas en 802.11, 11b y 11a (OFDM) para proporcionar servicios a distintas tasas de datos
- 14 canales solapados y tasas de datos de 1, 2, 5.5 y 11 Mbps y 6, 9, 12, 18, 36, 48 y 54 Mbps
  - hay solapamiento entre canales, se deben dejar al menos 4 libres

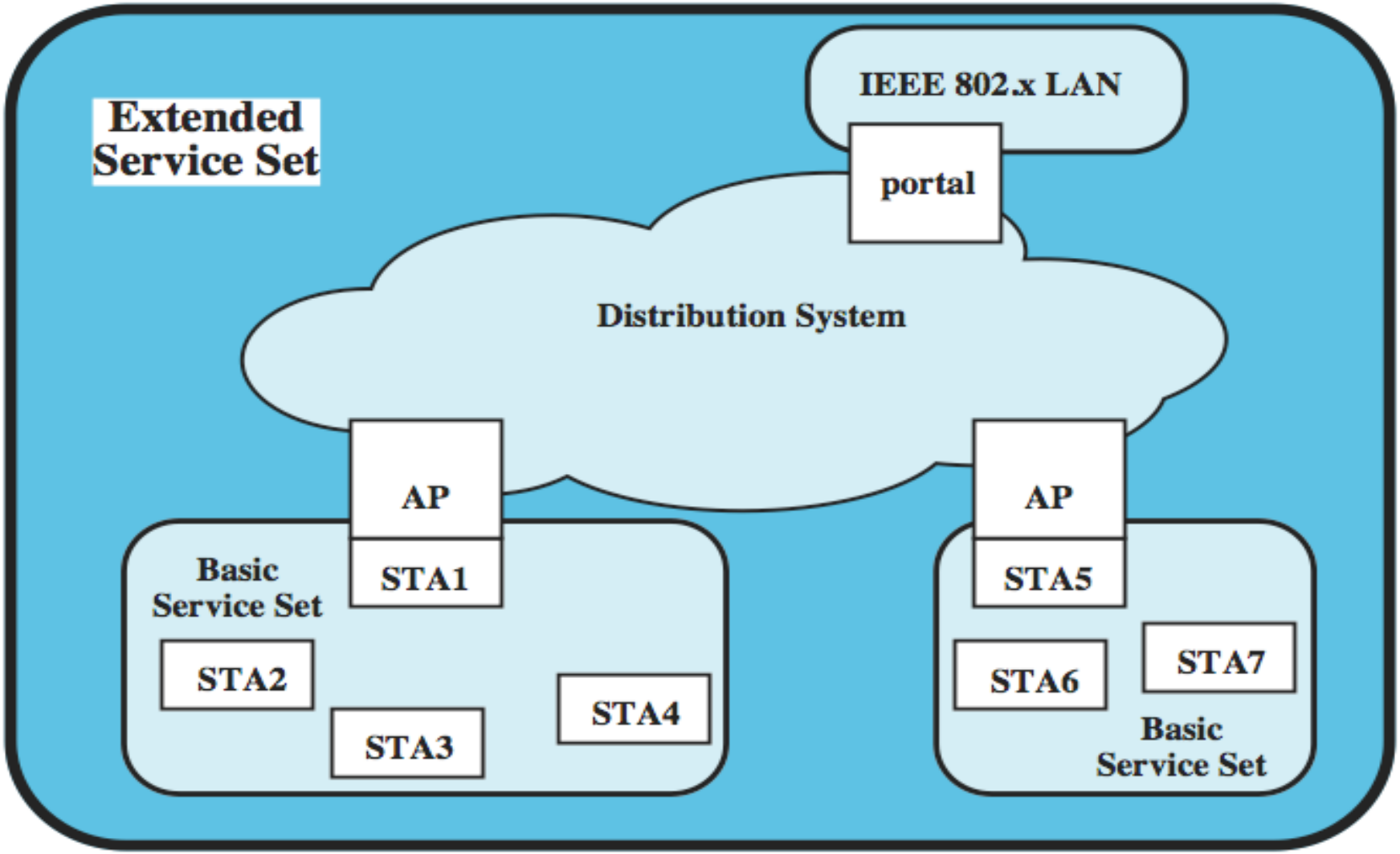
Tasa de datos vs distancia (m)

Data Rate (Mbps)	802.11b	802.11a	802.11g
1	90+	—	90+
2	75	—	75
5.5(b)/6(a/g)	60	60+	65
9	—	50	55
11(b)/12(a/g)	50	45	50
18	—	40	50
24	—	30	45
36	—	25	35
48	—	15	25
54	—	10	20

IEEE 802.11 - Terminología

Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations
Basic service set (BSS)	A set of stations controlled by a single coordination function
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs
Distribution system (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entites using the services of the physical layer
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer

IEEE 802.11- Arquitectura



STA = station
AP = access point

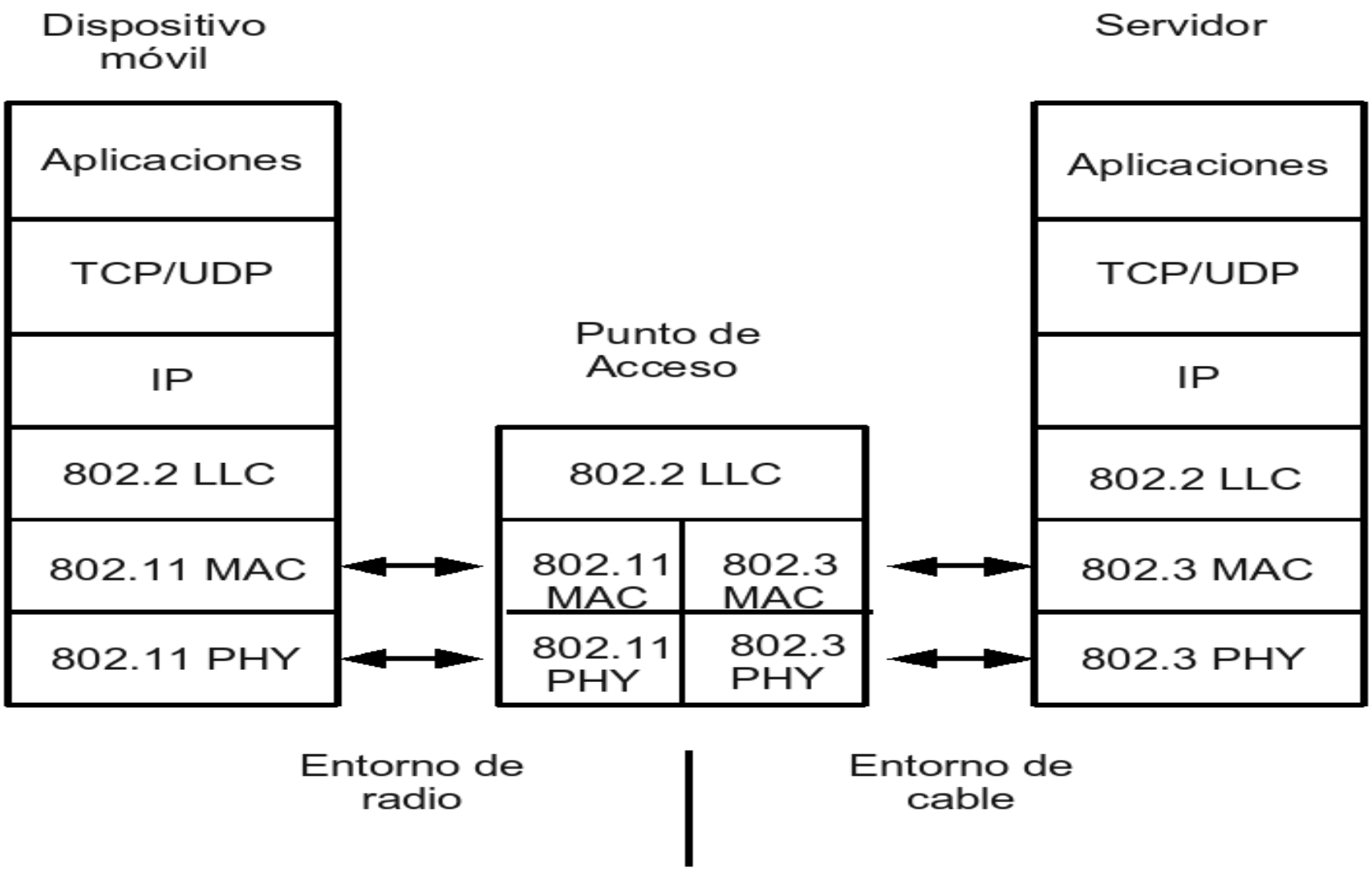
IEEE 802.11 - BSS

- **BSS** (*basic service set*) es un conjunto de estaciones que se comunican entre sí. Hay 2 tipos:
  - **BSS Independiente** (IBSS) o en modo *adhoc* o sin punto de acceso: todos los nodos se comunican directamente entre sí y deben encontrarse al alcance directo unos de otros.
  - **BSS de Infraestructura** (BSS) o con punto de acceso, de manera que los nodos que lo forman no tienen que estar unos al alcance directo de los otros.
- En un BSS todas las tramas entre nodos pasan por el AP, permitiendo cosas como:
  - comunicación entre nodos que no '*se ven*'
  - ahorro de energía, guardando las tramas a nodos que están *hibernando*
- Unidad mínima para construir WLANs multiceldas identificadas por un ESSID
- Puede conectar con un sistema de distribución (DS) troncal a través del AP mediante conexión alámbrica o inalámbricas (WDS)

IEEE 802.11 - ESS

- ESS (*Extended Service Set*): formado por uno o más BSSs interconectados por un [W]DS:
  - los nodos en un ESS se comunican entre sí aunque estén en distintas BSSs, incluso en movimiento
  - los APs actúan como puentes, **creando un mismo dominio de difusión** a través del DS
- Presenta un conjunto de BSSs como único
  - todos los BSSs deben tener el mismo SSID, que también identifica al ESS
- Configuraciones avanzadas (usando VLAN):
  - AP *isolation* (aislante): impide que sus nodos asociados '*se vean*' entre sí
  - AP virtuales: creación de distintos BSS/ESS en un mismo dispositivo AP

Esquema de un Punto de Acceso



802.11 – Tabla de Servicios

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Dissassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassocation	Distribution system	MSDU delivery

Autenticación

- **Tras el escaneado pasivo o activo** (***probe request*** con o sin SSID), un **nodo se asocia a un BSS** usando los parámetros compatibles anunciados por el AP en las
  - tramas ***beacon*** (cada 10-100s) o ***probe response***
- La **autenticación** se usa para establecer la identidad de la estación. Hay dos niveles:
  - **802.11**: **obligatoria antes de la asociación**
  - **802.1X**: **robusta, opcional y posterior a la asociación**
- **802.11** requiere que un nodo establezca su identidad antes de asociarse. 2 sistemas:
  - **abierto**: basta con enviar la MAC (¿es fiable el filtrado MAC?)
  - **de clave compartida** (**WEP**): el AP desafía al nodo a que cifre un mensaje con la clave (no usar nunca!!!)
- **802.11i** recomienda el uso de **s. abierto** + **802.1X**:
  - ofrece autenticación de la capa de enlace y de usuario, no sólo de la estación
  - **WPA2** implementación de la industria (**WPA,** transición)

Privacidad

- La **privacidad** permite trasmitir los datos de forma confidencial mediante el uso de criptografía.
- En **802.11 abierto** o **de clave compartida** se puede recurrir a **WEP** para cifrar los datos:
  - *Wired Equivalent Privacy*
  - *¿Privacidad Equivalente a red Alámbrica? ... mentira podría*
- Se recomienda usar **802.11i**, que integra la autenticación 802.1X junto con la posibilidad de utilizar fuertes sistemas de cifrado y de integridad del mensaje
- Ver en el wikilibro
- WPS (Wi-Fi Protected Setup)

Asociación

- Tras la autenticación, un nodo se asocia al AP para que el DS pueda registrar su ubicación
  - sólo en modo infraestructura y a un único AP
  - el AP asigna un identificador (AID) a cada nodo, un nodo no asociado “no está en la red”
- Dos servicios relacionados con este requerimiento:
  - **Reasociación**, mueve una asociación a otro AP
  - **Disociación**, por parte de la estación o el AP
- Se produce en un intercambio de 3
  - el nodo envía una **petición de asociación**; si no está autenticada, recibe una anulación de autenticación
  - el AP, tras procesarla (p.e., ¿suficiente memoria?), responde con 0 (éxito) y un **ID de asociación** o con !=0
  - el AP inicia el procesamiento de tramas para el nodo a través de DS, guardándolas cuando esté en modo de ahorro de energía

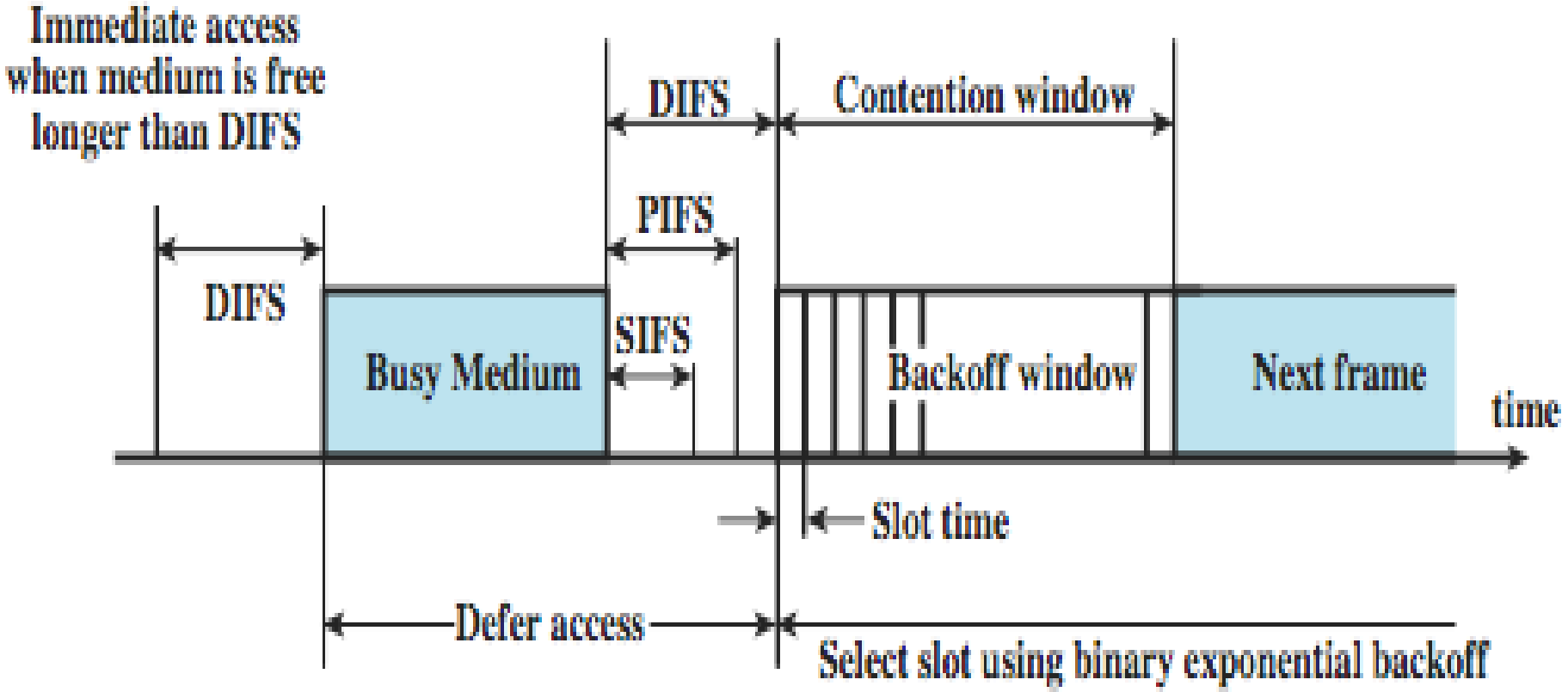
Distribución e integración

- Servicio de **distribución**
  - usado por las estaciones para intercambiar tramas MAC cuando la trama debe atravesar un DS
  - si las estaciones están en la misma BSS, el servicio de distribución atraviesa únicamente el AP de su BSS
  - en modo infraestructura los nodos no se envían tramas directamente, sino estas pasan siempre por el AP
- Servicio de **integración**
  - habilita la transferencia de datos entre una estación 802.11 y otra LAN 802._ , formando una única red integrada

IEEE 802.11 - CAPA M.A.C.

- La capa MAC cubre tres áreas funcionales:
  - entregas fiables de datos en un enlace RF
  - acceso a una red de límites difusos (estaciones ocultas)
  - seguridad en un medio público y remoto
- Proporciona tres tipos de servicios:
  - asíncrono o con contienda (*distributed coordination function* o **DCF**): redes *ad hoc* y en infraestructura
  - síncrono o sin contienda (*point coordination function* o **PCF**): sólo en redes en infraestructura
  - híbrido (**HCF**): ofrece QoS (802.11e / WMM, de 2005)
- Estos se pueden emplear simultáneamente, para ello se definen tres tiempos de espera: SIFS, PIFS (tras el cual se puede usar PCF) y DIFS (*idem* con DCF)
- La ocupación del medio con detección física y virtual
  - NAV, un campo de las tramas con la cantidad de tiempo que se va a reservar el medio

IEEE 802.11 MAC - Tiempos

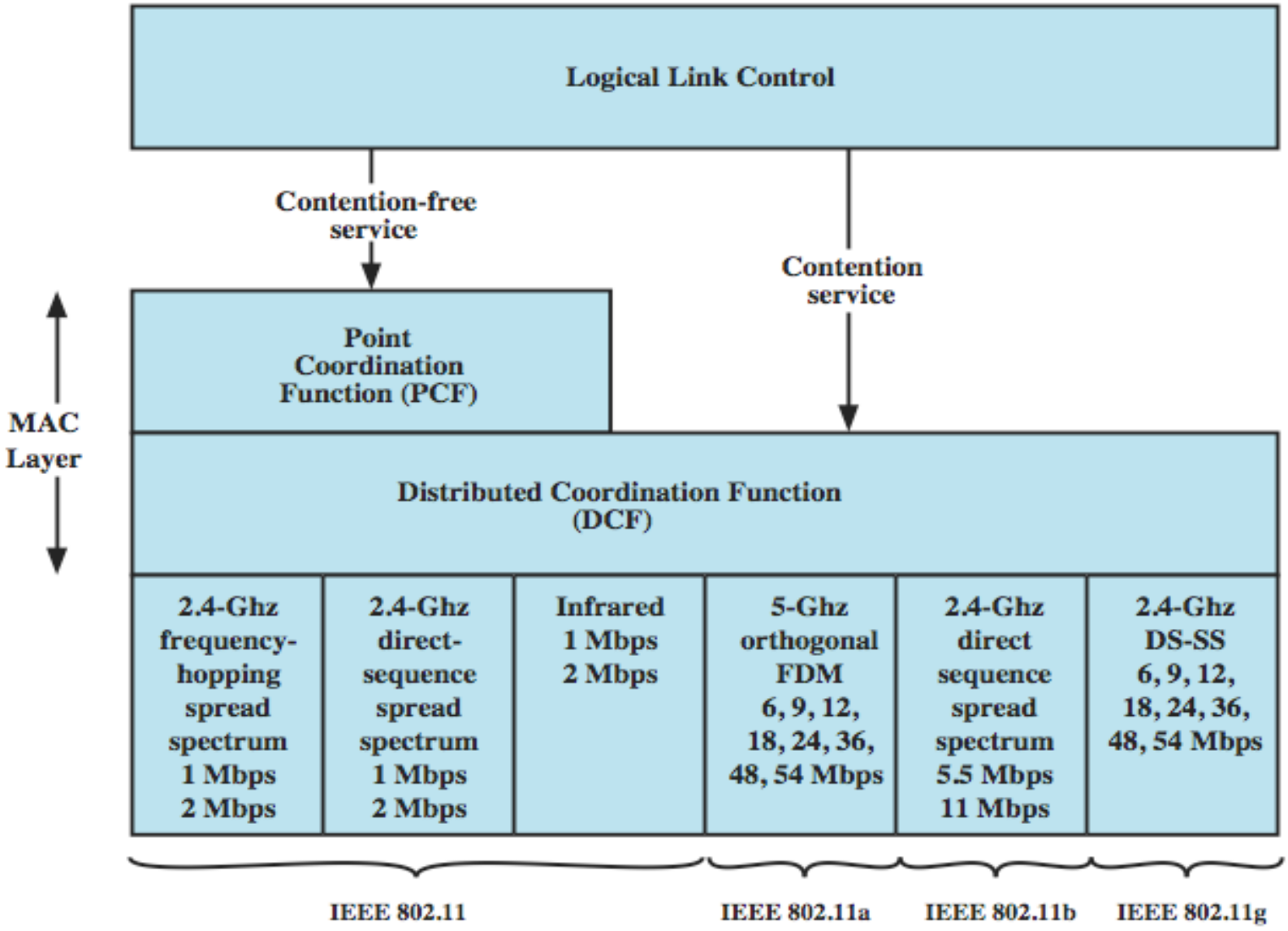


(a) Basic Access Method

Valores de prioridad IFS

- Se establecen distintas prioridades para distintos tipos de tráfico: primero, el de mayor prioridad.
- SIFS (*Short InterFrame Spacing*)
  - tras este periodo pueden iniciarse las transmisiones de prioridad más alta como la tramas CTS, ACK, el segundo y siguientes fragmentos de una trama y la respuesta a una trama de sondeo en periodo sin contienda (PCF)
- PIFS (Pcf IFS)
  - tras este periodo las estaciones pueden ocupar el medio con datos a transmitir **sin contienda**
- DIFS (Dcf IFS)
  - tras este periodo de tiempo las estaciones pueden contender por el acceso al medio
  - los nodos pueden tener un acceso inmediato al medio si este está libre durante un periodo de tiempo más largo que DIFS

MAC - Arquitectura



DCF con CSMA/CA

- Permite a varios nodos interactuar sin control central, solo escuchando la portadora física y virtual (NAV)
- Si el medio está libre un tiempo > DIFS, transmite
- Si el medio está ocupado, espera a que esté libre un tiempo > DIFS y hace la *demora exponencial*:
  - pone en marcha un temporizador de espera aleatorio dentro de un intervalo llamado *ventana de contienda*, que crece 2^n cada vez que hay una colisión hasta un máximo (~ c. física)
  - si éste llega a cero y el medio no se ha ocupado, transmite
  - si se ocupa antes, espera otro DIFS conservando el mismo valor que tenía el temporizador cuando se ocupó
  - la ventana se reinicia cuando se transmite con éxito o se alcanza el máximo de reintentos
- El transmisor espera a recibir ACK, que el receptor envía en el siguiente periodo SIFS (intercambio atómico de tramas)
- Si no se confirma, se retransmite (hasta máx. de reintentos)
- Las tramas se fragmentan cuando superan un cierto umbral, p.e. para reducir los errores (*Fragmentation Threshold*)

Estación oculta y expuesta

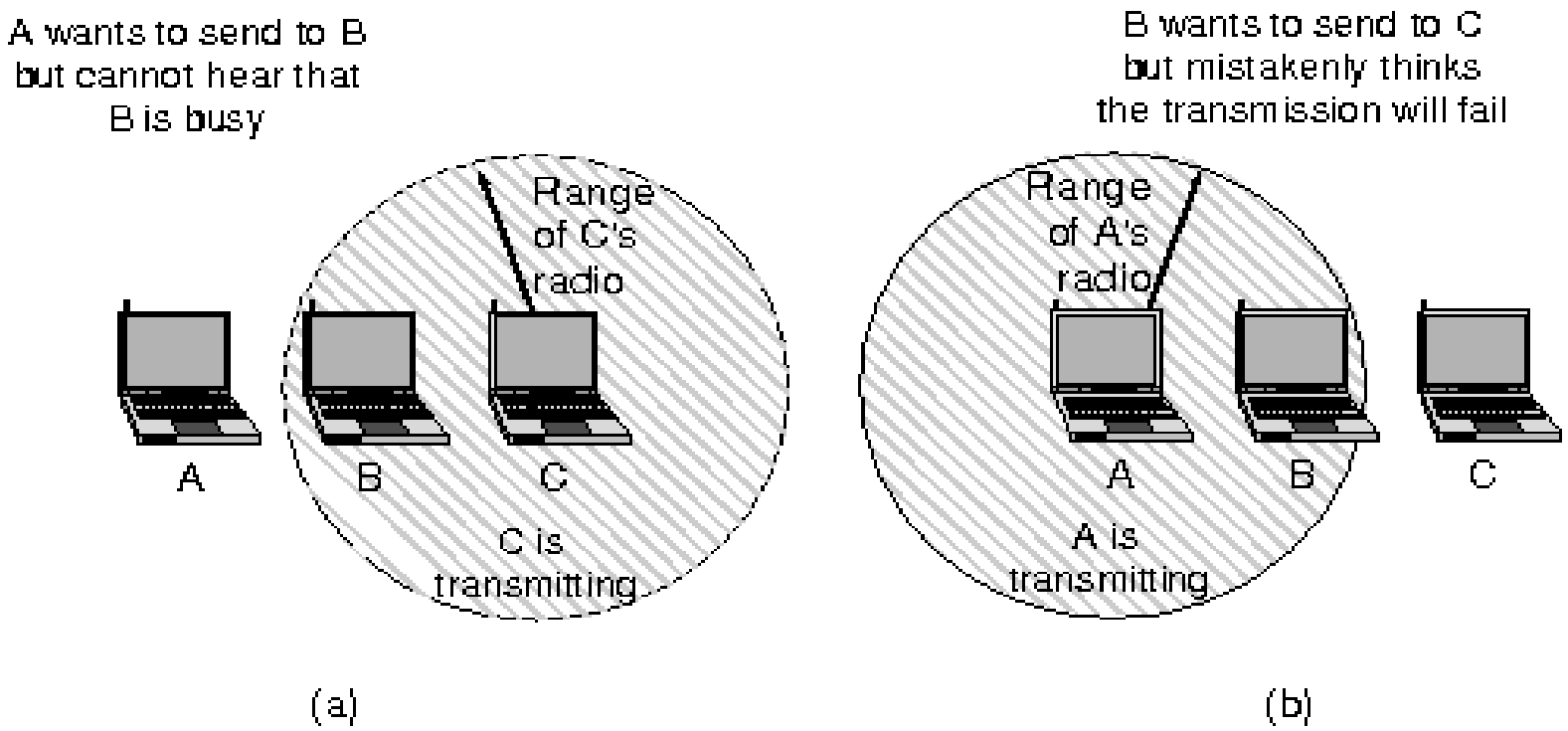


Fig. 4-26. (a) The hidden station problem. (b) The exposed station problem.

DCF con intercambio RTS/CTS

- Para evitar el problema de la estación oculta, garantizando la reserva del medio y una transmisión sin interrupciones
- **Intercambio de 4 tramas** para una mejor fiabilidad
  - la fuente envía una trama RTS (*Request to Send*) al destino con la duración de la transmisión (NAV)
  - el destino responde con CTS (*Clear to Send*) y su NAV
  - después de recibir CTS, la fuente envía los datos
  - el destino responde con ACK
- **RTS** alerta a todas las estaciones al alcance de la fuente de que se inicia un intercambio
- **CTS** alerta a todas las estaciones al alcance del destino
- **En los nodos** se puede establecer una longitud de trama a partir de la cual se usa RTS/CTS (RTS *Threshold*) si se detectan exceso de colisiones por estaciones ocultas
  - no en el A.P., ya que para este no hay estaciones ocultas

Intercambio - Esquema

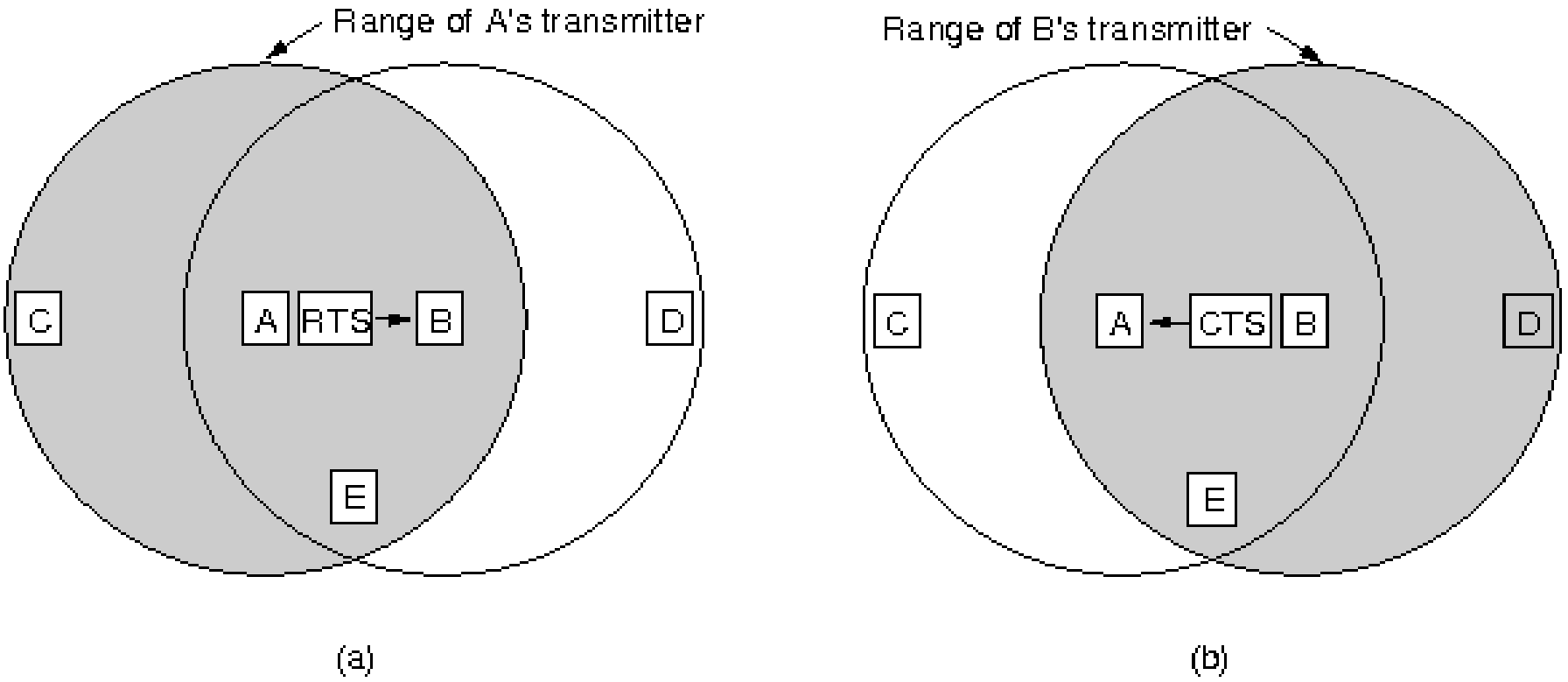


Fig. 4-12. The MACA protocol. (a) *A* sending an RTS to *B*. (b) *B* responding with a CTS to *A*.

802.11 MAC – Formato de trama

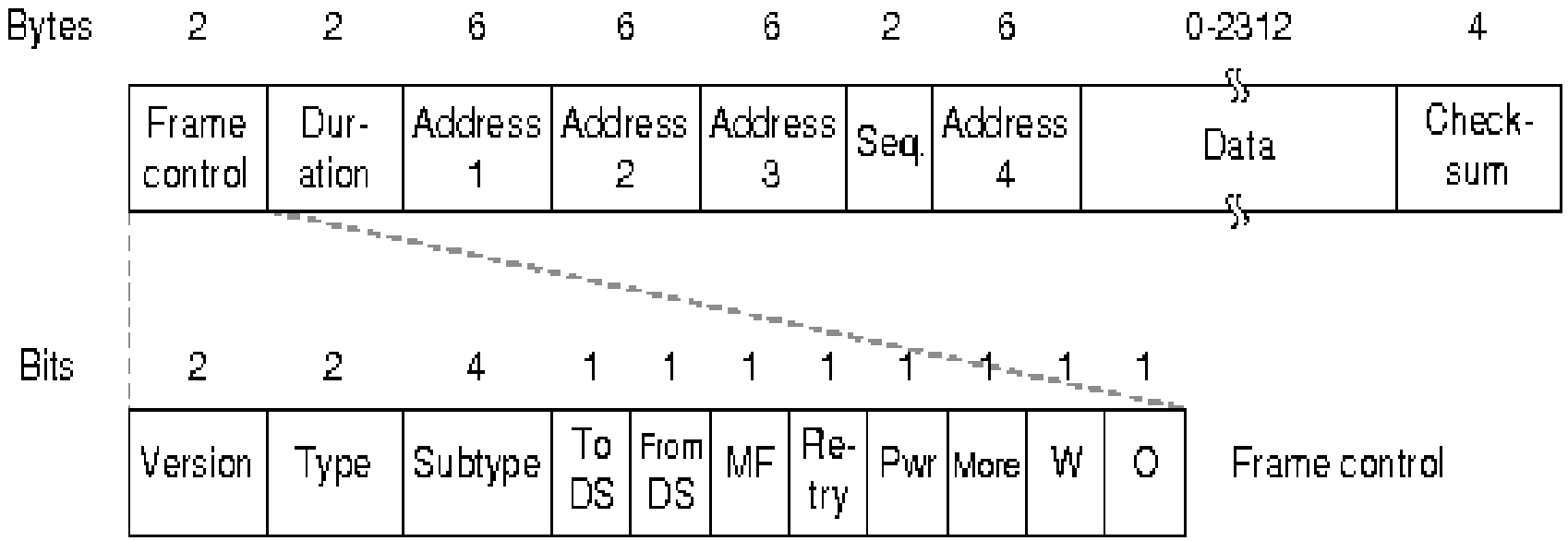


Fig. 4-30. The 802.11 data frame.

802.11 MAC – Trama (1)

- Existen tres clases distintas de tramas MAC: Datos, Control y Gestión
- Las tramas tienen los siguientes campos
  - control de trama (2B), formado por 11 subcampos
    - Versión de protocolo (2b)
    - Tipo (2b): datos, control o gestión
    - Subtipo (4b): Datos / RTS, CTS, ACK / *Beacon* ...
    - ToDS (1b) y FromDS (1b): (=1 si datos y modo infraestr.)
    - Más Fragmentos (1b)
    - Reintento (1b)
    - Gestión de energía (1b), tras terminar la operación
    - Más datos (1b), guardados en el AP para el nodo
    - Trama protegida (WEP) (1b), la trama cambia ligeramente
    - En orden (1b)

802.11 MAC – Trama (2)

- Duración/ID (2B), depende de los bits 15/14
  - si el bit 15 = 0, se usa para establecer el NAV (*Network Allocator Vector*) o nº de microsegundos que se espera que permanezca ocupado el medio para la transmisión en curso ==> escucha virtual de la portadora
  - si el bit 15 = 1/ bit 14 = 0, tramas CFP (sin contienda)
  - si el bit 15 = 1/bit 14 = 1, trama PS-*Poll*, sondeo de ahorro de energía al A.P. para asegurarse que no se pierde ninguna trama (se le añade el ID de asociación)
- Dirección de 1 a 4 (x6B), normalmente 3 direcciones
  - dirección de destino, origen, receptor, transmisor
- Control de secuencia (2B), no en las tramas de control
  - nº fragmento (4b) y nº secuencia (12b)
- Datos (0-2312B)
- FCS (6B), secuencia de comprobación de trama
- Máximo Total: 2346B

WPANs – IEEE 802.15

- *Wireless Personal Area Network* o *Piconets adhoc*
  - un dispositivo actúa como maestro y el resto de esclavos
  - distancias de unos 10m
- adecuado para aplicaciones como conexiones esporádicas entre dispositivos móviles y de periféricos
- se usa transmisiones de radio de corto alcance, como *bluetooth*
- se estandarizan en el IEEE 802.15:
  - 802.15.1: *Bluetooth*
  - 802.15.2: Coexistencia con WLANs
  - 802.15.3: Alta velocidad (11 a 55 Mbps)
  - 802.15.4: Baja velocidad, consumo y complejidad
  - 802.15.5: Interconexión en malla

IEEE 802.15.1 – Bluetooth (1)

- *Bluetooth* es un estándar abierto publicado por el *B. Special Interest Group* (Ericsson, IBM, Nokia, Intel, Toshiba...)
- El comité 802.15 estandariza sólo las capas física y de enlace de datos, el resto queda fuera de su alcance

IEEE 802.15.1 – Bluetooth (2)

- La arquitectura está formada por una unidad básica llamada *piconet* formada por un maestro y hasta 7 esclavos activos
  - en una *piconet* puede haber hasta 255 nodos estacionados, estando los no activos en estado de bajo consumo hasta que el maestro lo vuelva a activar
  - las *piconets* se pueden conectar mediante un nodo puente, formando una *scatternet*
- Es un sistema TDM controlado por el reloj del maestro, en el que no hay comunicación directa esclavo esclavo
- Sobre las capas 802.15 se define los perfiles de aplicación: auriculares, acceso LAN, sync, fax, transferencia de archivos ...

WPANs - Diagrama

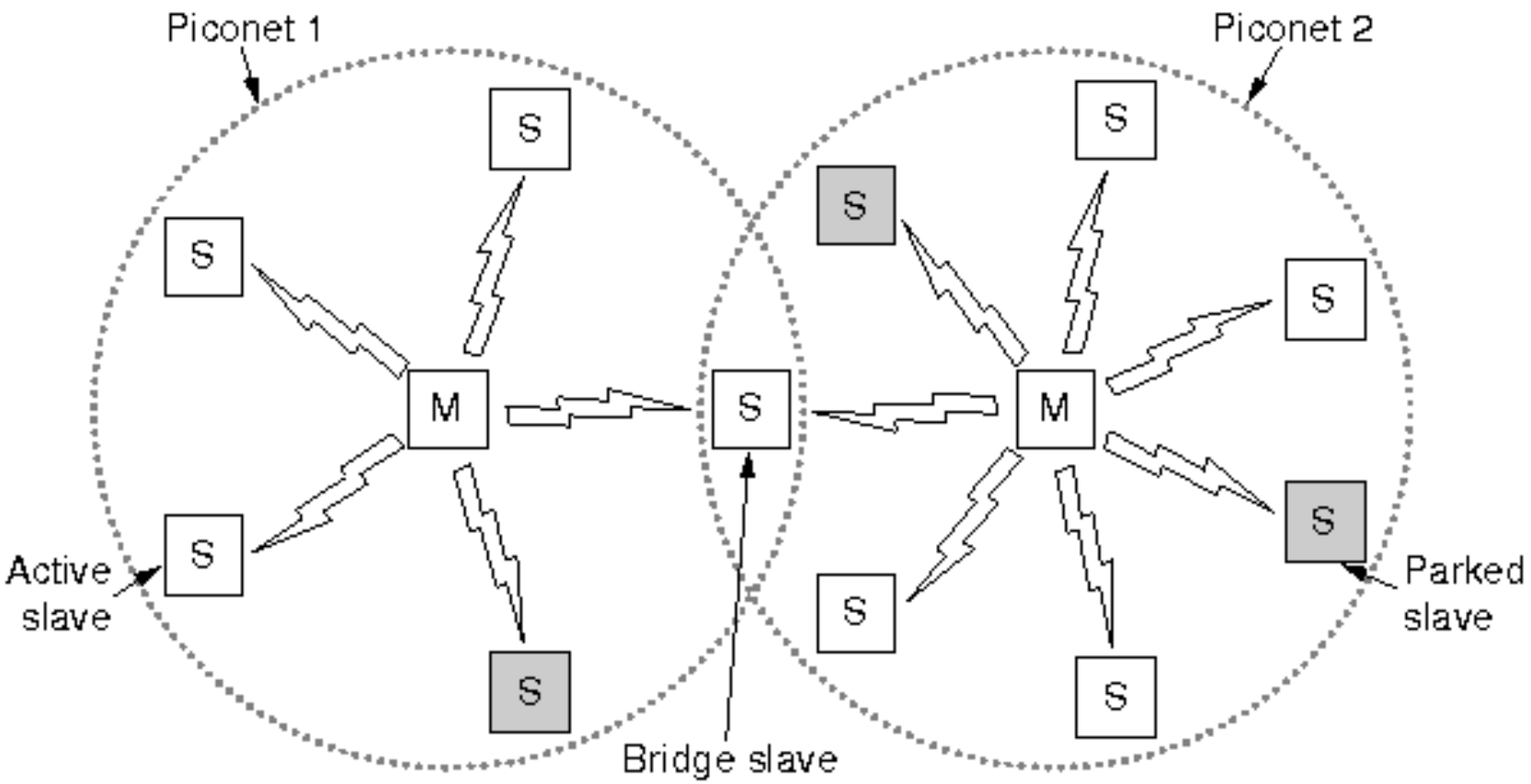


Fig. 4-35. Two piconets can be connected to form a scatternet.

IEEE 802.15.1 - CAPAS

- C. física: interfaz de radio en la banda ISM 2.4GHz
  - Multiplexión:
    - FHSS de 79 canales de 1MHz y 1600 saltos/segundo
    - TDM: mitad para el maestro, mitad para el resto (TDD)
  - Modulación:
    - FSK para 1Mbps
  - Hay tres tipos de transceptores de radio *Bluetooth*:
    - Clase 1: P. max. de 100 mW y alcance de 100m
    - Clase 2: P. max. de 2,5mW y alcance de 10m
    - Clase 3: P. max. de 1mW y alcance de 1 o 2m
- C de banda base (MAC): maneja el envío de tramas
- C L2CAP (LLC): divide paquetes de hasta 64KB en tramas, maneja la calidad de servicio

Bluetooth – Pila de protocolos

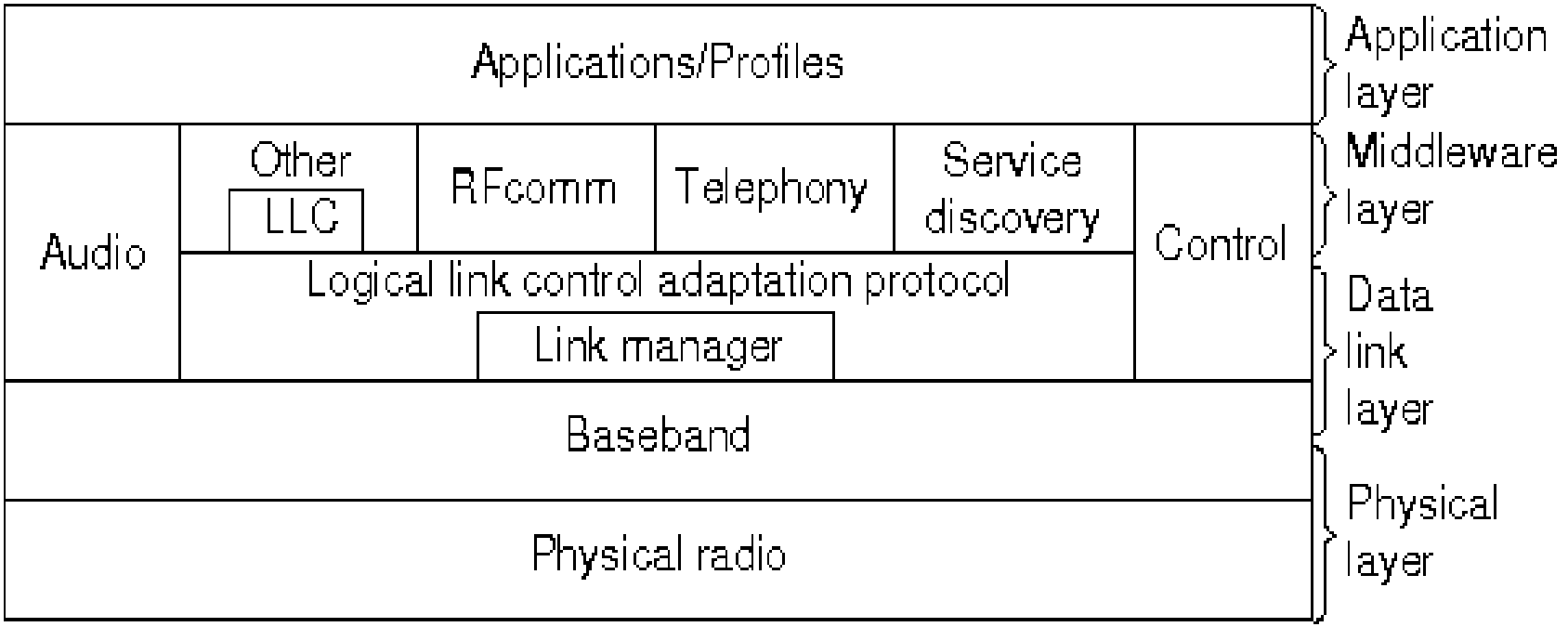


Fig. 4-37. The 802.15 version of the Bluetooth protocol architecture.