Bloque V: El nivel de enlace

Tema 12: Tecnologías del nivel de enlace

Índice

- Bloque V: El nivel de enlace
  - Tema 12: Tecnologías del nivel de enlace
    - Introducción
    - Ethernet
      - CSMA/CD
      - Trama
      - Conmutadores
    - WiFi
      - Introducción
      - Capa física
      - CSMA/CA
      - Seguridad

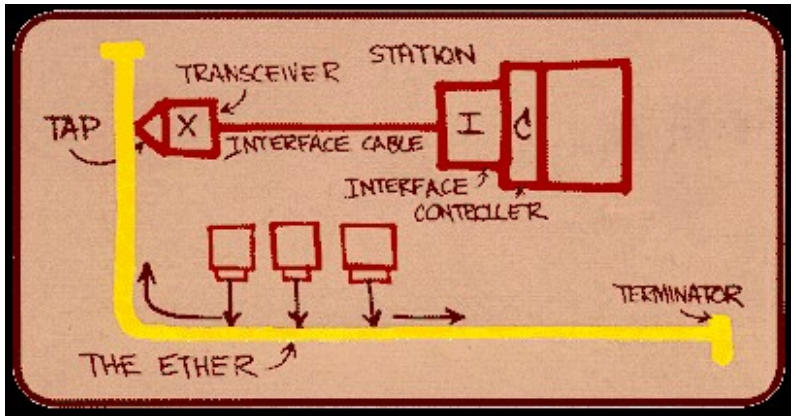
- **Lecturas recomendadas:**
  - Capítulo 5, secciones 5.3, 5.5, 5.6 y 5.7, de “Redes de Computadores: Un enfoque descendente”. James F. Kurose, Keith W. Ross. Addison Wesley.
  - Capítulo 6, secciones 6.1 y 6.3, de “Redes de Computadores: Un enfoque descendente”. James F. Kurose, Keith W. Ross. Addison Wesley.

Introducción

- Tecnologías punto a punto: un (único) emisor en un extremo y un (único) receptor en el otro extremo.
- Tecnologías de broadcast → Problema del acceso múltiple: coordinar el acceso de múltiples emisores y receptores a un canal de difusión compartido.
- Colisión: dos transmiten simultáneamente (total o parcialmente) → Los receptores no son capaces de recuperar el mensaje transmitido.
- Requisitos protocolos de acceso múltiple (canal a R bps):
  - Si sólo hay un nodo → Que transmita a R bps.
  - Si hay N nodos → De media, que transmitan a R/N bps.
  - Protocolo descentralizado y simple.
- Tipos de protocolos de acceso múltiple:
  - Protocolos de particionamiento del canal: https://www.youtube.com/watch?v=kZ3V_sIXiI0&t=12s
  - Protocolos de turnos: https://www.youtube.com/watch?v=hOkE-0RG9vo
  - Protocolos de acceso aleatorio: https://www.youtube.com/watch?v=7aSkJCUDAes

Ethernet

- Protocolo de acceso aleatorio para canales de difusión.
- Se inventó a mediados de los 70 y se basaba en una topología en bus, con un cable **coaxial** conectando a todos los nodos.



- A mediados de los 90 se pasó a una topología en estrella basada en **concentradores** (hubs). Los equipos se conectaban con un cable de cobre de par trenzado (RJ-45) al concentrador.
- A principios de la década de 2000, se cambió el concentrador por un **conmutador** → Mayor velocidad efectiva.
- Va desde 10 Mbps hasta 10 Gbps hoy en día, todo sobre la misma trama Ethernet → Facilita la interconexión.

- Precursoras: ALOHA y ALOHA ranurado

Ethernet: CSMA

- En las redes LAN (y de radio) el retardo de propagación entre las estaciones es mucho más pequeño que el tiempo de transmisión de las tramas:
  - Cuando una estación transmite una trama → El resto lo saben casi instantáneamente.
  - Si las estaciones pueden saber que otra estación está transmitiendo → Esperan para evitar la colisión.
  - Sólo habrá colisiones cuando dos estaciones empiecen a transmitir casi simultáneamente.
- Esta técnica se denomina de acceso múltiple sensible a la portadora (Carrier Sense Multiple Access): una estación escucha el medio antes de transmitir
  - Si está ocupado → Espera
  - Si está libre → Transmite
- Si dos estaciones intentan transmitir casi al mismo tiempo → Colisión
  - Es necesario una confirmación del receptor que también debe competir por el canal.
- Tiempo de espera después de una colisión:
  - CSMA 1-persistente: espera hasta que el canal esté libre y después transmite. Se produce colisión si hay dos o más estaciones esperando.

Ethernet: CSMA/CD

- En CSMA, si colisionan dos tramas → El medio está inutilizado durante la transmisión de esas tramas.
- Mejora: continuar escuchando el canal mientras dura la transmisión (**Collision Detection**) → No necesito recibir confirmación.

- Si el medio está libre → Transmite.
- Si no, continua escuchando hasta que esté libre → Transmite.
- Si se detecta una colisión durante la transmisión → Se transmite una señal corta de alerta y se corta la transmisión.
- Se espera un tiempo aleatorio, y después se intenta transmitir de nuevo (exponential backoff):
  - Tras cada colisión (sobre la misma trama) el tiempo de espera se duplica (1 seg, 2, 4, 8, 16, 32, …)
  - Tras N intentos, no se retransmite más y se genera un mensaje de error.
  - Si se congestiona el sistema → Las estaciones deben esperar más y más para liberar al medio.

Ethernet: CSMA/CD

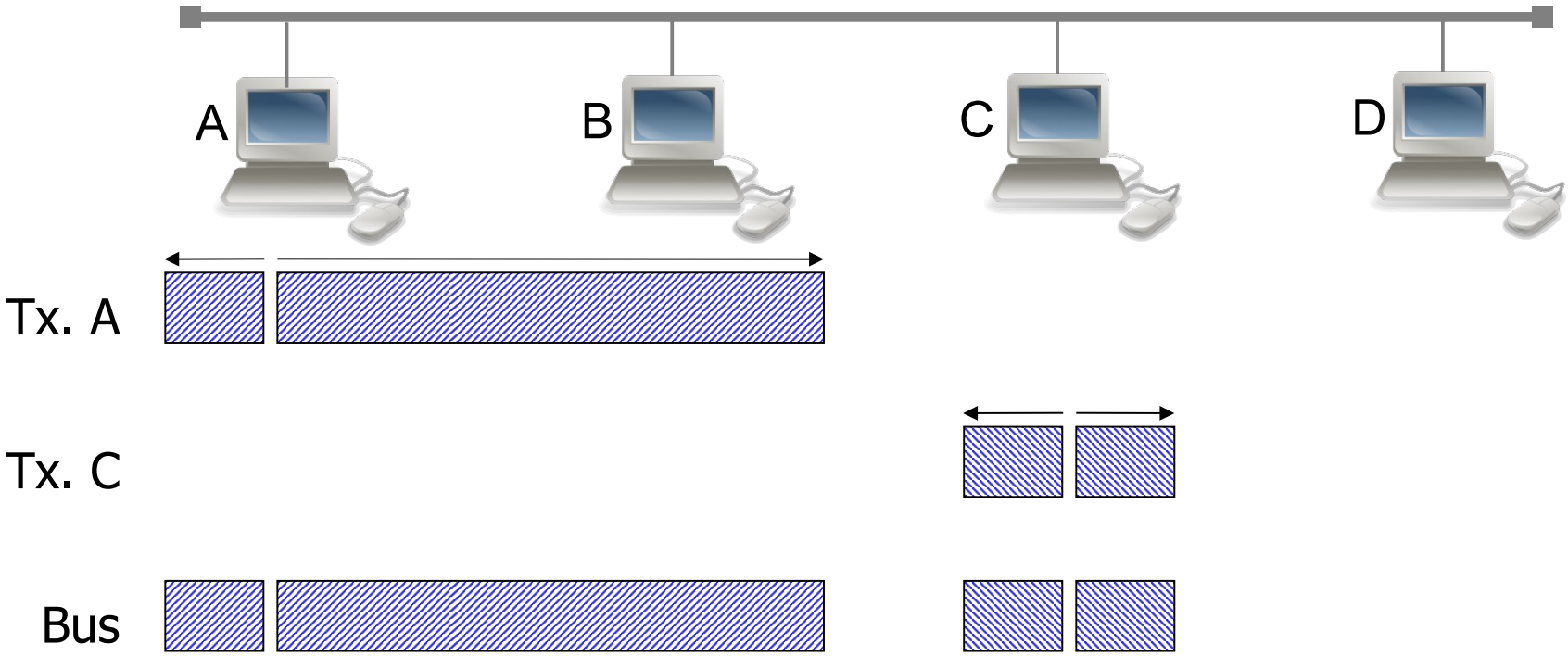
Tx. A

Tx. C

Bus

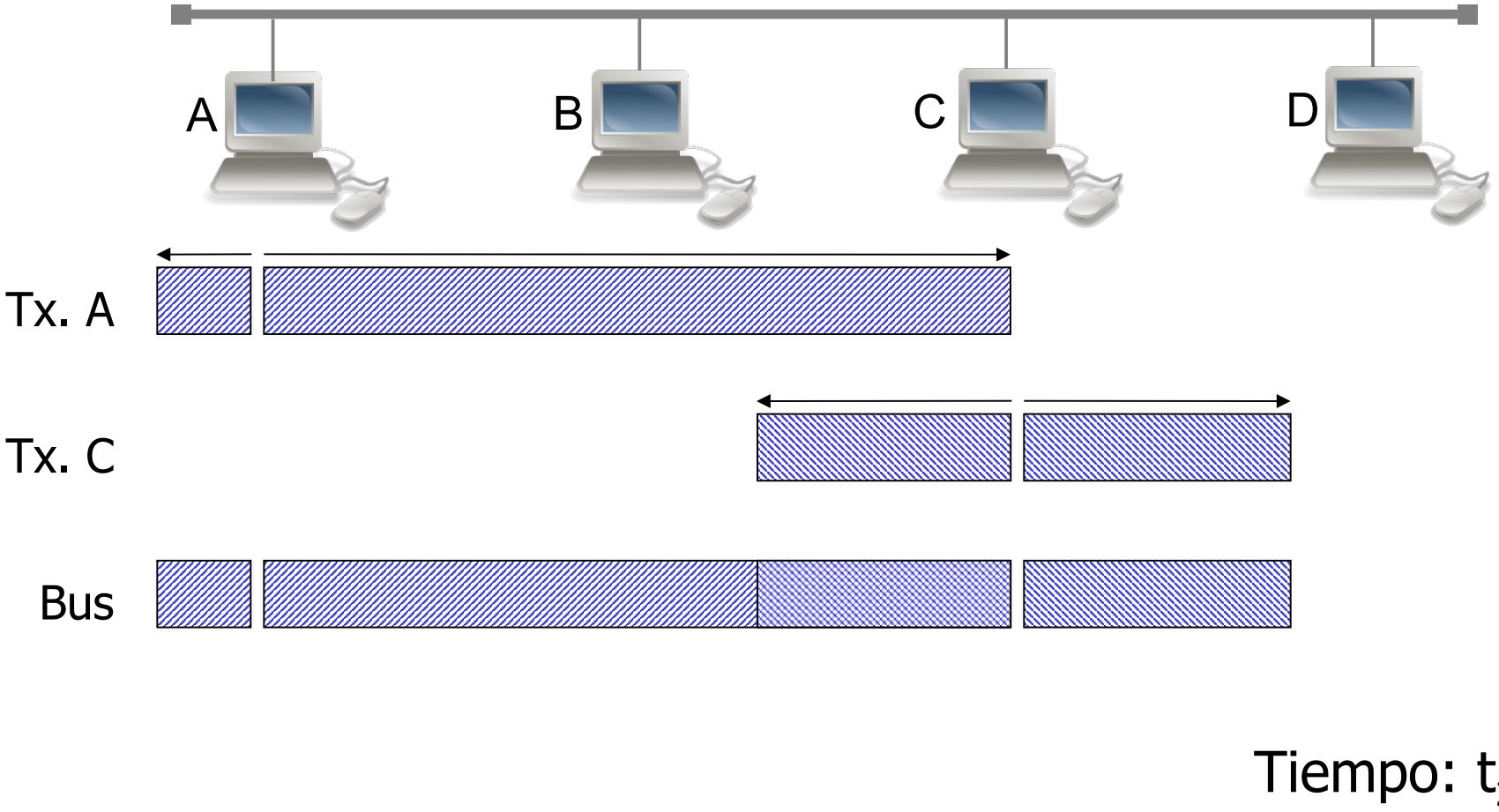
Tiempo: t_0

Ethernet: CSMA/CD

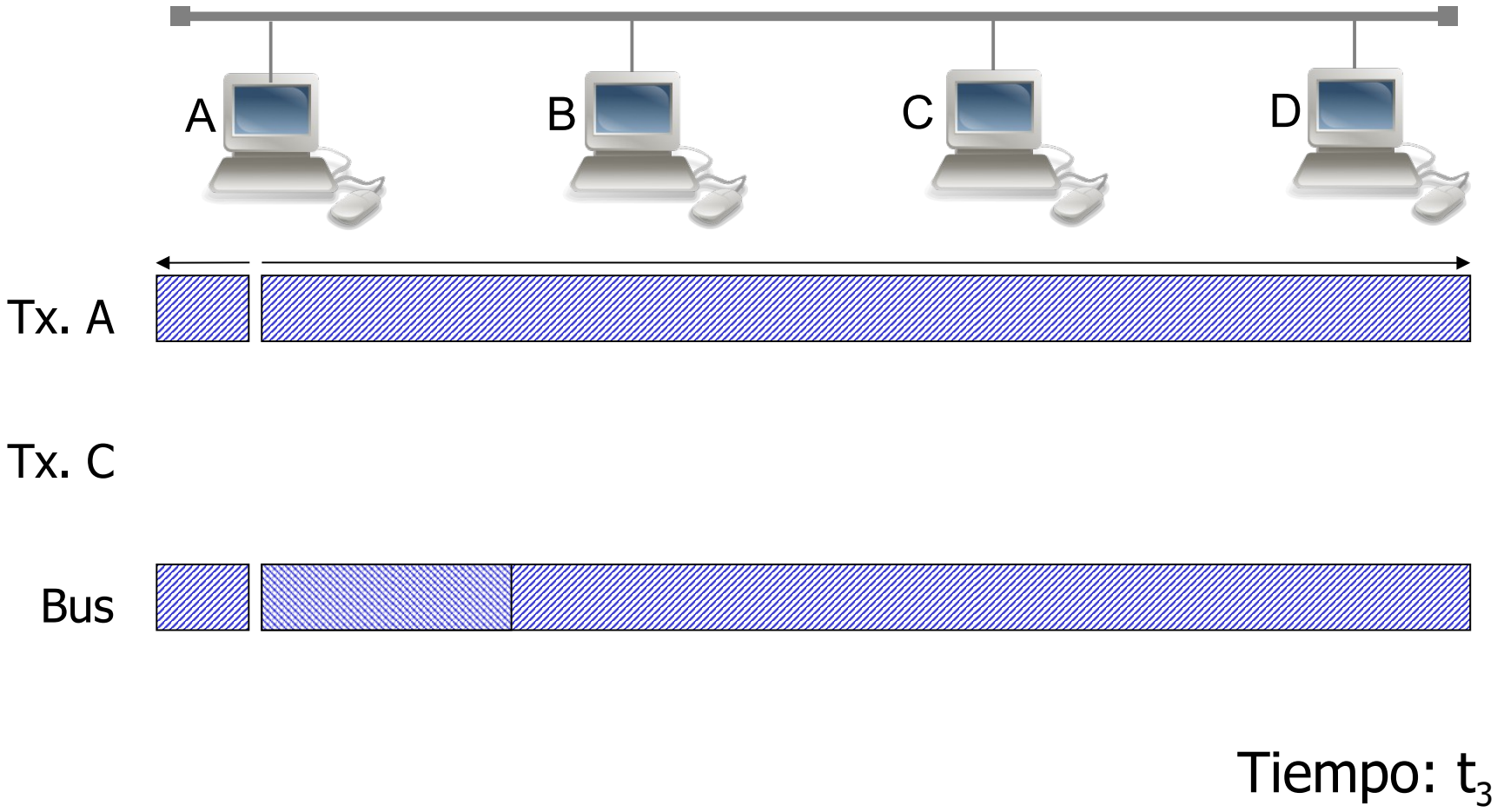


Tiempo: t_1

Ethernet: CSMA/CD



Ethernet: CSMA/CD



Ethernet: CSMA/CD

- ¿Cuánto tiempo se tarda en detectar una colisión, en el peor de los casos?
  - A transmite.
  - Justo antes de que llegue a D, D empieza a transmitir.
  - Casi inmediatamente → D detecta la colisión.
  - Pero la colisión se debe propagar hasta volver a A.
- El tiempo en detectar una colisión es <= dos veces el retardo de propagación extremo a extremo.
- Una trama debe ser suficientemente larga para detectar la colisión antes de que acabe su transmisión → Tamaño mínimo de trama (64 bytes) y tamaño máximo del medio (2500 m).
  - 2500 m → Aprox. 25 μsegs de retardo de propagación.
  - Tº detección colisión = 25 μsegs x 2 = 50 μsegs.
  - Enviar 64 bytes a 10 Mbps ⇒ 64 x 8 / 10 Mbps = 51.2 μsegs.

- https://media.pearsoncmg.com/aw/ecs_kurose_compnetwork_7/cw/content/interactiveanimations/csma-cd/index.html

Ethernet: Trama

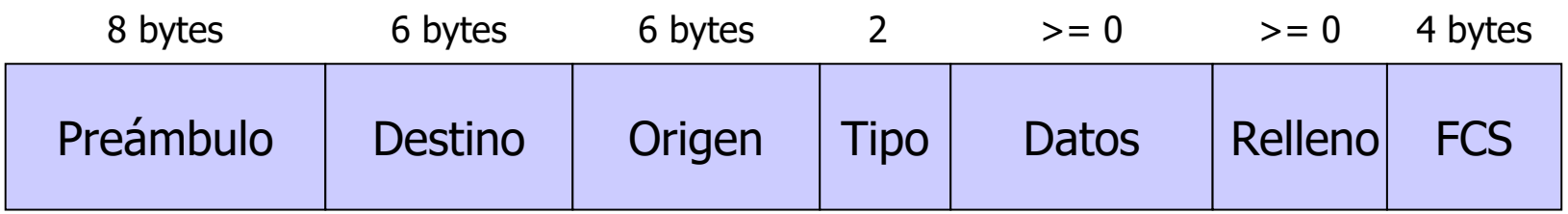
- Ethernet:
  - Estándar definido por Xerox en 1982
  - Método de acceso: CSMA/CD 1-persistente
  - 10 Mbps

8 bytes	6 bytes	6 bytes	2	>= 0	>= 0	4 bytes
Preámbulo	Destino	Origen	Tipo	Datos	Relleno	FCS

- IEEE 802.3
  - Estándar propuesto por la IEEE sobre el estándar Ethernet.

7 bytes	1	6 bytes	6 bytes	2	>= 0	>= 0	4 bytes
Preámbulo	SFD	Destino	Origen	Long.	Datos	Relleno	FCS

Ethernet: Trama

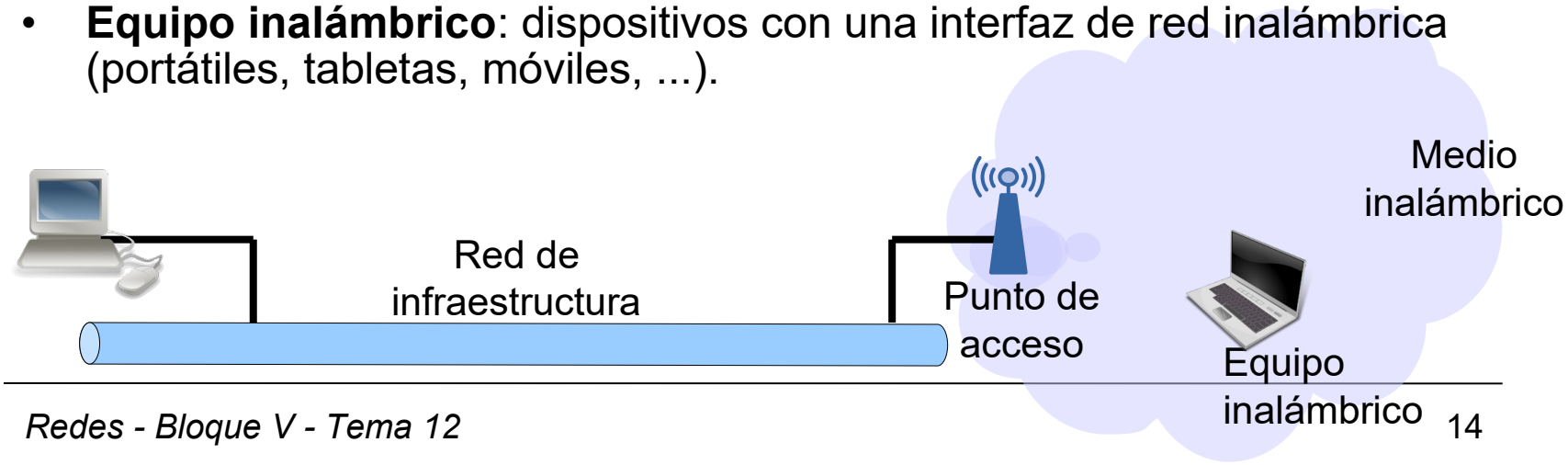


- Preámbulo: patrón de 8 bytes, con 0's y 1's alternados, para sincronizar el emisor y el receptor:
  - El último byte es 01010111.
  - El receptor puede localizar el primer bit del resto de la trama.
- Dirección destino: puede ser una dirección única, de grupo o global.
- Dirección origen
- Tipo: indica el tipo de protocolo utilizado en el campo de datos.
  - En la cabecera IEEE 802.3 el campo Longitud indica la longitud (si <= 1500) o el tipo (si > 1535).
- Datos: máximo 1500 bytes
- Relleno: bytes añadidos para garantizar que la técnica de detección de colisiones pueda operar correctamente (mínimo 46 bytes)
- FCS (Frame Check Sequence): código CRC de detección de errores (incluye todos los campos, excepto el preámbulo, el SFD y el FCS).

WiFi: Introducción

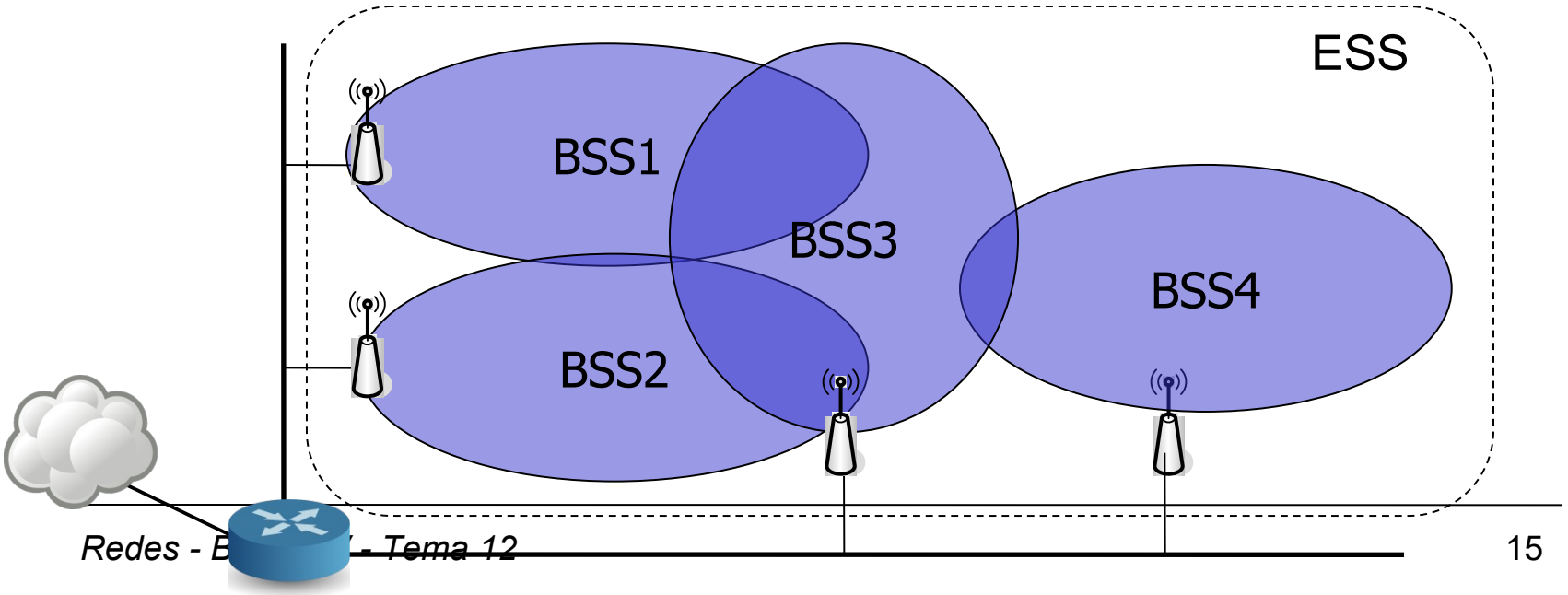
- Características de los sistemas de transmisión inalámbrica: movilidad y flexibilidad.
- No son un sustituto de las redes “tradicionales”: equipos estáticos (i.e. servidores) y velocidad limitada por el ancho de banda.
- Estándares WiFi: https://www.wi-fi.org/discover-wi-fi

- **Red de infraestructura**: componente lógico de 802.11 para enviar las tramas a su destino (no se especifica una tecnología particular). Se suele usar Ethernet.
- **Punto de acceso**: responsable de enviar y recibir tramas de un host inalámbrico asociado.
- **Medio inalámbrico**: radio frecuencia.
- **Equipo inalámbrico**: dispositivos con una interfaz de red inalámbrica (portátiles, tabletas, móviles, ...).

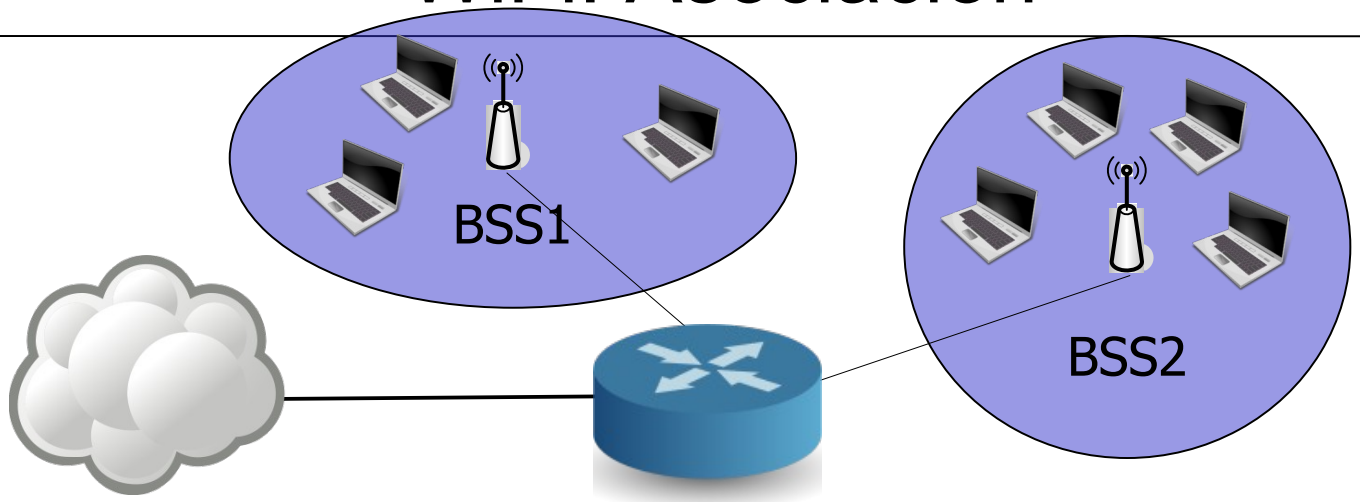


WiFi: Introducción

- **Basic Service Set** (BSS): grupo de estaciones que se comunican entre sí.
  - BSS independiente (o ad-hoc): se comunican directamente.
    - Grupo reducido
    - Carácter temporal (p.e. reunión)
  - BSS infraestructura: usan un punto de acceso.
    - Comunicaciones entre estaciones móviles pasan por el punto de acceso → Una estación se **asocia** a un punto de acceso.
    - Los puntos de acceso envían periódicamente una señal baliza.
    - Distancia de las estaciones al punto de acceso (no entre estaciones).
- **Extended Service Set** (ESS): asociación de BSSs. Se encadenan varias BSSs usando un backbone → Transición BSS.



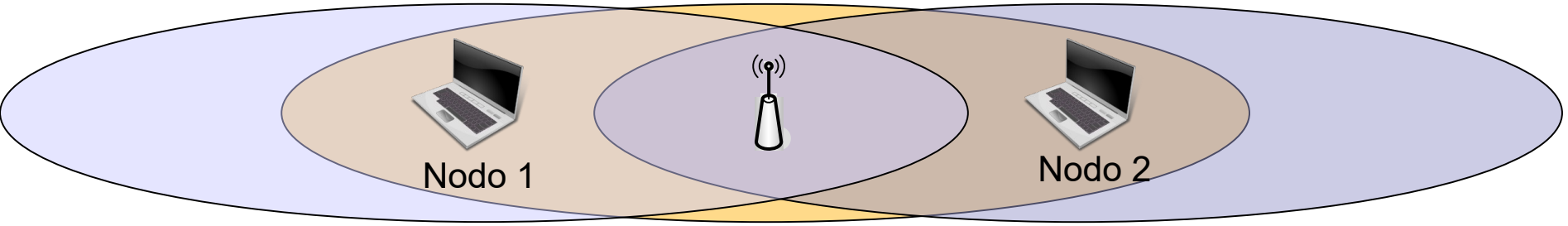
WiFi: Asociación



- **SSID** (Service Set Identifier): identifica la red inalámbrica asociada a un punto de acceso.
- Un equipo móvil debe asociarse con un punto de acceso (PA) → Los puntos de acceso envían periódicamente tramas **baliza** (MAC del PA + SSID).
  - Exploración pasiva: el equipo espera a recibir tramas baliza.
  - Exploración activa: el equipo solicita a los PA que se identifiquen.
- El equipo determina a que punto de acceso asociarse (p.e. mayor potencia).
- Seguridad:
  - Filtrado MAC
  - Login y password, sobre un servidor de autenticación (p.e. RADIUS).
- Después, configuración IP por DHCP.

WiFi: CSMA/CA

- Una vez asociado, el equipo móvil puede transmitir y recibir tramas del PA → Subcapa **MAC** del nivel de enlace.
- Pero, otra vez, tenemos el problema del acceso múltiple → Solución: CSMA/CA (Collision Avoidance).
- ¿Por qué no CSMA/CD?
  - Problema del **nodo oculto** (no todas las estaciones reciben todo).



- CSMA/CA:
  - Cuando una estación empieza a transmitir, transmite la trama completa … haya o no colisión.
  - Necesita un ACK para confirmar recepción.

WiFi: CSMA/CA

- Solución al problema de los nodos ocultos: RTS/CTS.
  - Cuando un emisor quiere transmitir, primero envía un RTS (Request To Send) indicando el tiempo total que necesita.
  - Cuando el PA recibe el RTS, responde con un CTS (Clear To Send) indicando el tiempo restante que tiene reservado el canal → El emisor sabe que tiene el canal disponible + el resto saben que el canal estará ocupado.
- Beneficios:
  - Una trama sólo se enviará después de reservar el canal → Evita colisiones de nodos ocultos.
  - Las colisiones se producen sobre las tramas RTS o CTS → Son tramas cortas.
- Desventajas: introduce un retardo (enviar RTS y CTS) y consume recursos del canal → Es opcional (se establece un umbral de tamaño de trama a partir del cual se usa).
- https://www.ccs-labs.org/teaching/rn/animations/csma/

WiFi: Seguridad

- El aire es un medio compartido → Muy sensible a escuchas.
  - No es muy distinto al cable → hay que alcanzar la misma seguridad.
  - Sin embargo se usan mecanismos adicionales.
- Inicialmente WEP y ahora la familia WPA: WPA, WPA2 y WPA3.
- WEP (Wired Equivalent Privacy):
  - Clave estática → Hoy en día, muy fácil de romper.
  - Computacionalmente eficiente (clave de 64-128 bits).
  - Exportable internacionalmente.
  - Opcional.
  - RC4 para cifrado y CRC-32 para integridad.
- WPA (WiFi Protected Access):
  - Implementa TKIP (Temporal Key Integrity Protocol) para cifrado: cambia dinámicamente las claves según se utiliza el sistema.
  - MIC para integridad.
- WPA2:
  - AES para cifrado y CCMP para integridad.
  - Método más seguro. Clave de 128 bits.
- WPA3:
  - Método más seguro. Clave de 192 bits.
  - Mejor protección, aun con contraseñas simples.
  - La contraseña inicial no se usa para derivar las claves. Aunque la contraseña sea descubierta, las claves de sesión no se pueden obtener.

What is the Internet?

https://www.youtube.com/watch?v=3YqGYvJkxoA