Ethernet

Procolo 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** conectado 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 al concentrador. A principios de la década de 2000, se cambió el concentrador po un **conmutador**, aportando una mayor velocidad efectiva. Va desde 10 Mbps hasta 10 Gbps hoy en día, todo sobre la misma trama Ethernet. Facilita la interconexión.

CSMA

En las redes LAN, y de radio, el retardo de programación 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 instantaneamente.
- Si las estaciones pueden saber que otra estación está transmitiendo, esperan para evitar la colisión.
- Sólo habrá colosiones cuando dos estaciones empiecen a transmitir casi simultáneamente. Esta técnica se denomina de acceso múltiple sensible a la portada o Carrier Sense Multiple Access, CSMA. Una estación escucha al medio antes de transmitir, si está ocupado, espera, sino, transmite. Si dos estaciones intentan transmitir casi al mismo tiempo se produce una colisión, es necesario una confirmación del receptor que también debe competir por el cana. 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.

CSMA/CD

En CSMA, si colisionan dos tramas, el medio está inutilizado durante la transmisión de esas tramas. Continuar escuchando el canal mientras dura la transmisión (**Collision Detection**), no necesito recibir confirmación. Si el medio está libre, transmite, sino, continua escuchando hasta que esté libre, 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.

- Tras cada colisión, sobre la misma trama, el tiempo de espera se dublica.
- Tras N intentos no se transmite más y se genera un mensaje de error.
- Si se congestiona el sistema, las estaciones deben esperar más y más para liberar al medio. El tiempo de detectar una colisión es <= dos veces el retardo de programación extremo a extremo. Una trama debe ser suficientemente larga para detectar la colisión antes de que acabe su transmisión.
- 2500 m. Aproximadamente 25msegs de propagación.
- Tº detección colisión = 25 msegs x 2 = 50 msegs
- Enviar 64 bytes a 10 Mbps -> 64 x 8 / 10 Mbps = 51.2msegs

Trama

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

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 puede ser una dirección única, de grupo o global. Tipo: indica el tipo de protocolo utilizado en el campo de datos. En la cabecera IEEE 802.3 el campo Tipo indica la longitud (si <= 1500) o el tipo (si > 1535). Datos: máximo 15000 bytes. Relleno: bytes añadidos para garantizar que la técnica de detección de colisiones pueda operar correctamente, mínimo 46 bytes. Frame Check Sequence, FCS: cógido CRC de detección de errores, incluye todos los campos, excepto el preámbulo, el SFD y el FCS.

WiFi

Los sistemas inalámbricos se destacan por su movilidad y flexibilidad. Aunque no reemplazan completamente a las redes "tradicionales" (como aquellas basadas en servidores o dispositivos estáticos), ofrecen conectividad con ciertas limitaciones, especialmente en cuanto al ancho de banda. Uno de los principales estándares de redes inalámbricas es WiFi, basado en la norma IEEE 802.11 (más información). Además del WiFi, existen otros sistemas de transmisión inalámbrica, como los basados en redes móviles (GSM, GPRS, UMTS –3G–, 4G, 5G), así como tecnologías como Bluetooth o WiMAX. Elementos clave de una red inalámbrica:

- Red de infraestructura: Parte lógica del estándar 802.11 que permite enviar tramas a su destino. No está ligada a una tecnología específica, aunque normalmente se utiliza Ethernet. **Punto de acceso**: Dispositivo encargado de enviar y recibir tramas de los equipos inalámbricos conectados. **Medio inalámbrico**: Utiliza ondas de radiofrecuencia para la transmisión de datos. **Equipo inalámbrico**: Dispositivos con capacidad para conectarse a redes inalámbricas, como portátiles, tabletas o teléfonos móviles. **Basic Service Set, BSS**: grupo de estaciones que se comunican entre sí.
- BSS indpendiente, o ad-hoc: se cominican directamente.
    - Grupo reducido
    - Carácter temporal
- BSS infraestructura: usan un punto de acceso.
    - Comunicaciones entre estaciones móviles pasan por el pnto 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. **Service Set Identifier, SSID**: 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. Seguridad:
- Filtrado MAC
- Login y password, sobre un servidor de autentificación. 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. ¿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 repetición. Solución al problema de los nodos ocultos: RTS/CTS.
- Cuando un emisor quiere transmitir, primero envía un Request To Send, RTS, indicando el tiempo total que necesita.
- Cuando el PA recibe el RTS, responde con un Clear To Send, CTS, indicando el tiempo restante que tiene reservado en el canal. El emisor sabe que tiene el canal disponible y 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, que son tramas cortas. Desventajas: Introduce un retardo y consume recursos del canal. Es opcional-

WiFi: Seguridad

Las redes WiFi transmiten datos a través del aire, lo que las hace especialmente vulnerables a escuchas no autorizadas. Aunque esta vulnerabilidad también existe en redes cableadas, en el caso de las redes inalámbricas se requieren mecanismos de seguridad adicionales. Evolución de los mecanismos de seguridad:

- En un inicio se utilizaba WEP (Wired Equivalent Privacy), pero debido a sus debilidades, fue reemplazado por la familia WPA: WPA, WPA2 y WPA3. Principales protocolos de seguridad: **WEP (Wired Equivalent Privacy)**:
- Utiliza una clave estática, hoy considerada insegura y fácil de romper.
- Es eficiente en términos computacionales (usa claves de 64 a 128 bits).
- Fue exportable internacionalmente y su uso era opcional.
- Usaba el algoritmo RC4 para cifrado y CRC-32 para verificación de integridad. **WPA (WiFi Protected Access)**:
- Introduce TKIP (Temporal Key Integrity Protocol), que cambia las claves de cifrado de forma dinámica durante el uso.
- Incluye MIC (Message Integrity Check) para verificar la integridad de los mensajes. **WPA2**:
- Utiliza el estándar AES para cifrado y CCMP para garantizar la integridad.
- Es un método más seguro que WPA, utilizando claves de 128 bits. **WPA3**:
- Es el método más seguro actualmente, con claves de 192 bits.
- Ofrece mayor protección, incluso si se utilizan contraseñas simples.
- A diferencia de versiones anteriores, la contraseña inicial no se utiliza para derivar directamente las claves. Incluso si esta es descubierta, no se pueden recuperar las claves de sesión.