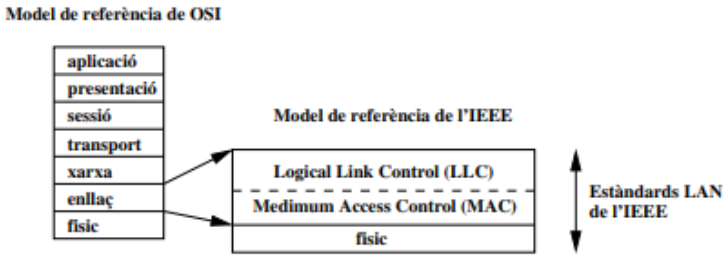
Tema 3: LAN

3.1 Introducció

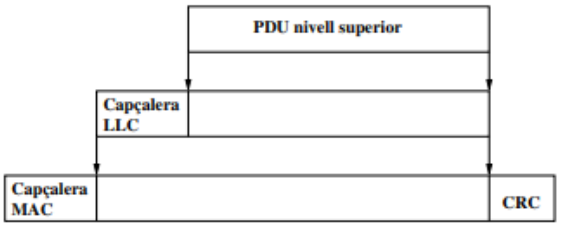
- WAN: Red con switches con topología de malla. Su objetivo es la escalabilidad.
- LAN: Una red multiacceso con medios compartidos. El protocolo MAC es necesario.

3.2 IEEE LAN Architecture

IEEE ha estat l'organisme capdavanter en l'estandardització dels sistemes LANs. Tots els estàndards desenvolupats per aquesta empresa tenen el prefix 802. L'IEEE va definir el model de referència; en aquest model el nivell del model de referència OSI es divideix en dos subnivells:



Definirem l'acrònim PDU com a Protocol Unit Data. Aquest nom es va introduir en el model de referència OSI per referir-se a les estructures de dades que fa servir cada nivell. El CRC que afegeix el nivell MAC serveix pel control d'errors.

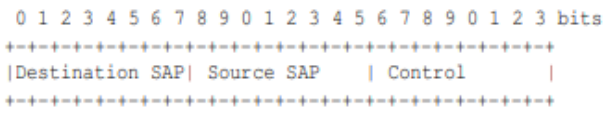


3.2.1 Logical Link Control

El subnivell LLC defineix la interfície de nivell superior. L'estàndard defineix tres tipus de serveis:

1) No orientats a connexió.
2) Orientats a connexió.
3) Confirmats i no orientats a connexió.

L'estàndard es refereix als camps Destination SAP (DSAP) i Source SAP (SSAP) com a "adreces LLC". L'acronim SAP vol dir Service Access Point, aquest nom fa referència a "punt de comunicació" entre nivells. Malgrat que en el LLC, el SAP té un significat anàleg al camp de protocol de la capçalera IP (identifica el nivell superior on ha de lliurar-se el contingut de la trama. El camp de control identifica el tipus de comanda, segons el tipus, pot tenir un o dos bytes.

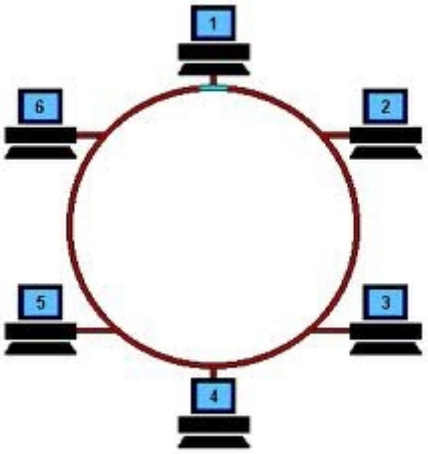


3.3 Ethernet

La tecnología Ethernet es la líder en LAN. Hay muchos estándares con diferentes transmisiones de medios y diferentes bitrates.

3.3.1 Tipos de MAC

- **Token Passing**: El tipo de acceso está regulado por un testimonio. Solo un host puede transmitir a la vez (el que tiene el token). Mientras un host transmite el token, los otros hosts de la red esperan en silencio. El token se va pasando cada X tiempo al siguiente host, típicamente después de la transmisión de una trama. Ejemplos: FDDI y Token-Ring. Una buena analogía sería un grupo de personas pasando el turno de palabra (Talking Pillow from Breaking Bad).



- **Random:** No hay token y cada host transmite cuando quiere. Hay una probabilidad de colisión y en caso de colisión, el frame se vuelve a transmitir después de un tiempo random de *backoff*. Para que sea equitativo, las distintas estaciones han de tener el mismo generador para el tiempo. Ejemplo: Ethernet.

N(T): Media del nombre de frames que se envían desde cualquier estación a la red sin colisionar en un tiempo T.
C(T): Número de tramas que colisionan durante un tiempo T.
t_t:Media del tiempo de transmisión de tramas.
E: Eficiencia de la red
G: Carga de oferta

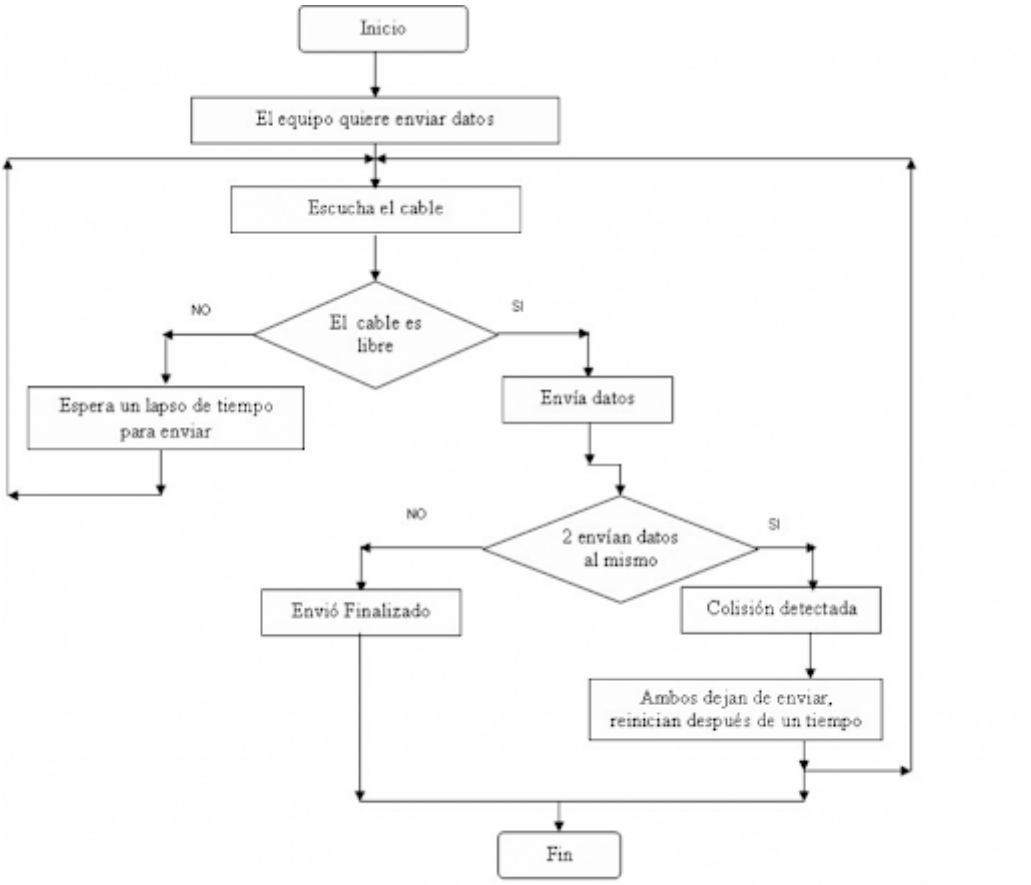
$$E = N\frac{N(T)t_t}{T} = \frac{bits\ enviados \cdot tiempo\ de\ transmisión}{T}$$

$$G = \frac{(N(T)+C(T))_t}{T}$$

3.3.2 Carrier Sense Multiple Access / Collision Detection (CSMA/CD)

A diferencia de Aloha, CSMA consiste en escuchar
Es una dirección aleatoria de MAC donde las estaciones escuchan el medio (carrier sense) antes de transmitir. Cuando el medio está libre el frame se transmite inmediatamente y el medio detecta las colisiones.

En caso de colisión, el frame se retransmite después de un tiempo aleatorio (*backoff*).



3.3.3 Ethernet Half-Duplex and Full-Duplex

- **Half duplex:** Usando CSMA/CD solo un NIC puede ser transmitido simultáneamente en el medio.
- **Full-duplex:** Cuando 2 Ethernet NIC se conectan point2point algunos estándares de Ethernet permiten una transmisión Full-Duplex

Los NIC de Ethernet tienen un mecanismo de auto-negociación para detectar la disponibilidad de full-duplex.
En el modo full-duplex se desactiva CSMA/CD ya que no pueden ocurrir las colisiones.

3.3.4 Ethernet Frames

- Ethernet II

Preamble (8 bytes)	Dest MAC (6 bytes)	Src MAC (6 bytes)	Frame Type (2 bytes)	Payload (46-1500 bytes)	CRC (4 bytes)

- IEEE 802.3

Preamble (8 bytes)	Dest MAC (6 bytes)	Src MAC (6 bytes)	Length of Frame (2 bytes)	Payload (46-1500 bytes)	CRC (4 bytes)

Preamble: Da tiempo a detectar, sincronizar y empezar la recepción
Type: Identifica el protocolo de capa superior (IP, ARP, … RFC 1700, Assigned Numbers)
Este valor es siempre > 1500.
Length: Payload size (0-1500)

IEEE Sub-Networking Access Protocol (SNAP)

Permite la especificación de protocolos y de identificadores privados de proveedor. No está soportado por el campo de 8 bit 802.2 Service Access Point (SAP).
Se usa para encapsular los protocolos TCP/IP en el IEEE 802.2 (LLC) con OUI=0x000000 y el tipo es igual al RFC 1700 (usado por DIX).

3.4 Ethernet Switches

3.4.1 Introducción Ethernet Switches

Nos encontramos con el problema de Hub, que surge de la multiple conexión de estaciones que colisionan. La solución al error será el uso de Ethernet Switches (o puentes).

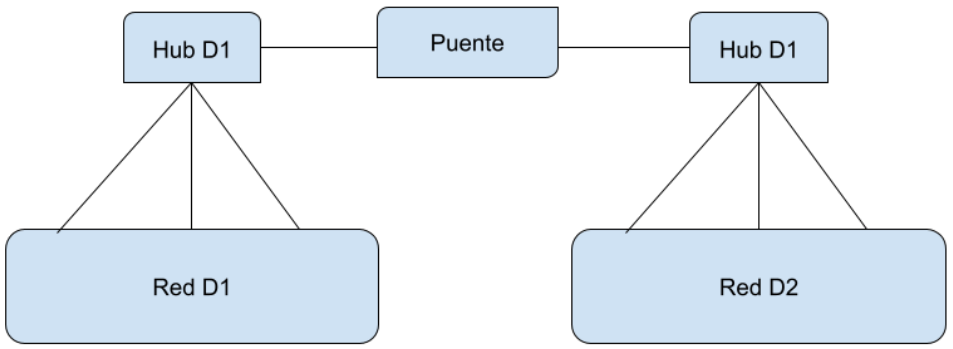
3.4.2 Puentes Ethernet

- Son dispositivos de capa 2, es decir, de tipo “plug and play” y no necesita configuración inicial. En cada puerto tenemos un NIC en modo “promiscuo”, es decir, que captura todos los frames.

- Para descubrir la MAC presente en cada puerto, se usa la dirección de origen. Cada entrada tiene, por tanto, la MAC y el número de los puertos.

- Para decidir si un frame tiene que ser transmitido por un puerto u otro, se usa la dirección de destino.

3.4.2.1 Funcionamiento



- Si se recibe un fragmento cuya dirección de origen no se encuentra en la tabla de MACs, se añade (**learning** bridge).

- Si se recibe un frame de D1 con una dirección que se encuentra en D2, no está en la tabla, o es en broadcast, se envía a D2. Esto es conocido como **flooding**.

- Si se recibe un frame de D1 con una dirección a la misma red D1, se descarta. Esto se conoce como **filtering**.

- Las entradas tienen un tiempo de muerte, que se actualiza (vuelve al max) cada vez que se usa una entrada. Si el tiempo llega a 0, se descarta esa entrada de la tabla.

3.4.2.2 Ventajas

Mediante el uso de puentes, podemos garantizar que habrá muchísimos menos fallos de colisión, y que los clientes de D1 y D2 podrán mandar frames de forma simultánea a sus servidores.

3.4.3 Switches Ethernet

3.4.3.1 Funcionamiento

Es equivalente a un puente de multiport.

- Si se recibe un frame con una dirección de origen que no esté en la tabla, se añade.

- Si se recibe un frame con una dirección de destino que no esté en la tabla o que sea multicast (o broadcast), se copia el frame en los buffers de transmisión de todos los demás puertos. Esto se conoce como **flooding**.

- Si se recibe un fragmento con una dirección con otro puerto, se cambia (mediante el switch) ASAP al buffer de transmisión del nuevo puerto.

- Si se recibe un frame con una dirección de destino de otra estación por el mismo puerto, se descarta. Esto se conoce como **filtering**.

3.4.3.2 Capacidades

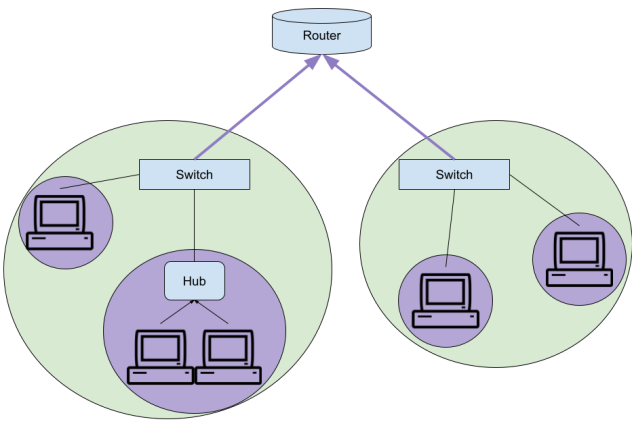
- Cada puerto es un dominio de colisiones distinto, así que se generan muchas menos colisiones.

- Los puertos:
  - Pueden ser a la vez transmisión y recepción.
  - Pueden tener distintos bitrates.
  - Pueden ser full-duplex (útil si solo hay un host conectado)

- Se puede incrementar el bitrate mediante agregación de links, que funcionarán como uno solo.

- Toda estación sólo puede capturar el tráfico de su dominio de colisión, aportando así seguridad entre dominios.

3.4.3.3 Dominios de broadcast y de colisión



Dominios de broadcast: Son el set de estaciones que recibirán un frame en broadcast mandado por cualquiera de ellos. A no ser que se use VirtualLAN, un switch nunca separa en dominios de broadcast. Los routers siempre separaran en dominios de broadcast. Conocer el dominio de broadcast nos facilita el uso de saltos en un hop mediante ARP.
Dominios de colisión: Todas las diferentes salidas desde un switch.

3.4.3.4 Control de Flow

Consiste en adaptar la velocidad a la que el switch recibe los frames y la velocidad a la que los manda. Si no se usa, podría causar pérdida de frames por culpa del overflow de los buffers.

Técnicas de control de flow:

- Jabber signal (Half duplex): El switch manda una señal al puerto cuya velocidad tiene que ser rebajada.
- Pause frames (Full duplex): El switch manda frames de pausa, que tienen un entero (2 bytes) que indica el tiempo (en 512 bits) que el NICs que reciben el frame tienen que estar pausados.

3.4.3.4.1 Problemas

Puede introducir ineficiencia al sistema.

- Si tenemos dos hosts a velocidades de transmisión muy distantes (P.ej: 10Mbps - 100Mbps), el lento podría mandar un flow control de pause frames que causaría que la transmisión de los frames del rápido también tuvieran que esperarse, reduciendo su poder de transmisión.

Si no se especifica otra cosa, se entenderá que trabajamos siempre en control de flow ideal, donde no se generan problemas.

3.4.3.5 Compartición de bitrate

- Hub: Si el hub crea un cuello de botella para los puertos activos, la capacidad (bitrate) se compartirá de forma igual entre todos los puertos.
- Switch: Si un puerto es el causante del cuello de botella, el bitrate se reparte entre todos los puertos que quieran comunicarse con el causante.

3.4.3.6 Spanning Tree Protocol (STP 802.1D)

- El principio básico de enrutado de capa 2 de los switches se basa en tener un único puerto para mandar frames a un destino, así que no se permiten ciclos.

- Los ciclos pueden aparecer si:
    - Se introducen por accidente (no me jodasxd)
    - Se tienen caminos redundantes para “reducir fallos”.

- Si se introducen ciclos sin controlar, se produce una lluvia de broadcasts, que bloqueará la red.

Por tanto, el objetivo del STP es crear un árbol (STP-tree) con caminos óptimos (libre de ciclos porque es un árbol). Todos los puertos que quedan apartados del STP-tree, se bloquean para evitar los ciclos.
Los switches mandan mensajes 802.1D a sus vecinos para ir construyendo el árbol. Si por algún fallo cambia la topología, se construirá uno nuevo.

3.4.3.7 Virtual LANs (VLANs)

El objetivo es agrupar distintos dominios de broadcast en una sola red.

- Cada puerto del switch pertenece a una VLAN (P.ej: Todos los puertos 1 serán la Red A, todos los puertos 2 serán la red B, en todos los switches.)
- El switch aisla las VLANs, es decir, el flooding se hace en función de las VLANs (P.ej: todos los puertos 1 de todos los switches).
- Se necesitará un router para distribuir los datos entre las VLANs, dado que cada switch tiene N VLANs conectadas a él.

3.4.3.7.1 Ventajas

- Generan flexibilidad en el posicionamiento de los dispositivos físicos.
- Facilita el aumento en tamaño de la red.
- Facilita la gestión de la red, dado que es mucho más sencillo añadir redes, cambiar hosts de LAN, etc.

Dado que cada VLAN tiene un dominio de broadcast distinto, se usará un STP-tree distinto para cada VLAN.

3.4.3.7.2 Trunk (Puerto troncal)

- Un puerto configurado para truncado pertenece a varias, o todas, las VLANs del sistema.
- Todo el tráfico de frames mandado a una VLAN pasará por el truncado.
- Para separar el tráfico de distintas VLAN dentro de un truncado, se usan TAGs.

Nota del editor: Debe entenderse como un puerto para dominarlos a todos. Este puerto controla el tráfico de varias VLANs conectadas al mismo switch. Es decir, como un switch puede tener varias Virtual LANs, para comunicarse con el router tendrá que haber puertos troncales para llevar tráfico de todas hacia él sin ser ese puerto de ninguna VLAN en concreto.

Protocolos de truncado:

- **Inter-Switch Link** (ISL): Perteneciente a Cisco
- **IEEE-802.1Q**

3.5 Wireless LANs 802.11

3.5.1 Componentes

3.5.1.1 Sistemas de Distribución (DS)

Son usados por los puntos de acceso para intercambiar frames entre ellos y con redes cableadas, que no es un chino enfadado, sino por ejemplo un switch de ethernet.

3.5.1.2 Puntos de acceso (AP)

Los puntos de acceso simplifican la comunicación entre estaciones. Todas esas comunicaciones irán siempre a través del Access Point, que puede tener o no un router asociado.

3.5.1.3 Set básico de servicio (BBS)

- Set de estaciones que se comunican entre ellas.
- Se identifican por:
    - Un identificador de Set de Servicio (SSID) o un nombre de red en menos de 32 caracteres
    - Un identificador de Set Básico de Servicio (BSSID)
- Si la red se compone por más de un BBS, se le llama set extendido de servicio (ESS)

3.5.1.4 MAC

MAC usa CSMA/CA, que a diferencia de CSMA/CD, no usa Collision Detect sinó Collision Avoidance, esperando siempre el tiempo aleatorio de backoff antes de transmitir, y no sólo cuando se colisiona.
No se usa CD, ya que es muy difícil detectar colisiones via wireless, ya que la Tx es mucho más potente que la Rx.

3.5.1.5 Direcciones

Están diseñadas para ser compatibles con Ethernet, usando rangos no solapados.
Un frame puede llegar a tener 4 direcciones y siempre tendremos el BSSID para identificar los frames que son del Set básico de servicio.

3.5.2 Problema del nodo oculto

Pongámonos en la siguiente situación:

- Tenemos un Nodo A que está en rango de AP con un Nodo C.
- El Nodo A y el Nodo B no se comunican entre sí.

Entonces, si A transmite al Access Point (AP), B no puede detectar que hay una transmisión en el sistema mediante Carrier Sense (CS), así que si B transmite, el AP sufrirá una colisión.

3.5.3 RTS/CTS

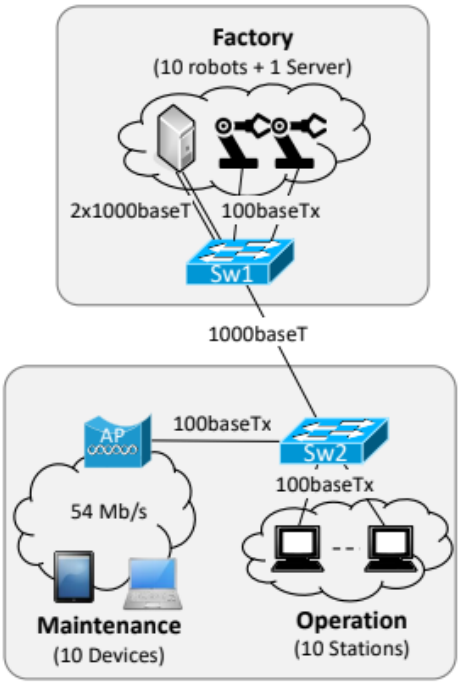
Con el fin de solucionar el problema anterior, tenemos este mecanismo opcional.

- Los RTS se mandan usando acceso básico.
- En cuanto se recibe el RTS/CTS, la estación define el valor del Network Allocation Vector (NAV). Mientras este no sea 0, se seguirá mostrando el medio como ocupado.
- Los RTS/CTS solo se pueden usar en unicast para transmisión (Tx)

- Existe un valor mínimo de tamaño de frames con los que se puede utilizar RTS/CTS.

3.6 Ejercicios

3.6.1 Ejercicio MAC



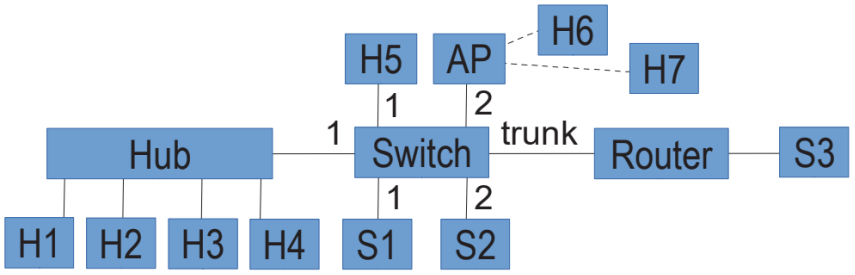
Teniendo en una empresa de fabricación el siguiente sistema, se pide que entres los valores de la siguiente tabla MAC para el Switch Sw2 una vez completadas las siguientes operaciones:

- Los robots están siempre activos y listos para mandar datos a la red de la factoría (donde se sacan las true FACTS).

- Los operarios de Mantenimiento y de Operaciones descargan continuamente datos del servidor de la factoría para chequear el correcto funcionamiento.

MACs aprendidas por Sw2	**Si / No**	**← Por qué?**	**Puerto**
Servidor Factoría	Si	Al descargar datos, viene la MAC desde ese servidor y tiene que pasar por Sw2.	1, por ejemplo
Robots	No	Los robots se comunican únicamente con la factoría, así que no saldrán de Sw1	Ninguno
Mantenimiento	Si	Al descargar datos, Mantenimiento y Operaciones tendrán que mandar su request que pasará por Sw2.	2, por ejemplo
Operaciones	Si		Y, efectivamente, 3

3.6.2 Ejercicio VLAN



An organisation has a network as shown in the figure, and:

- The switch is configured with 2 VLAN 1 and 2 as shown with the numbers by each port.
- PCs are connected via wire (H1-H5) and wireless (H6-H7).
- Server S1 is in VLAN1, and S2 is in VLAN2.
- Server S3 is available to all PCs through the router.
- Assume that all connections are at 100 Mbps and that the configuration is optimal.

3.6.2.1 Complete the list of devices that will receive the following messages:

Broadcast desde H1
H1 enviará broadcast y:

- El hub lo replica a todas sus salidas incluido el Switch.
- El Switch lo mandará a los conectados a la misma VLAN (1) y al Trunk.

Por lo tanto:
H1 → H2, H3, H4, Switch, H5, S1 y Router

Broadcast desde H6
H6 enviará broadcast y:

- El Access Point (AP) lo replicará por sus salidas incluido el Switch.
- El Switch lo mandará a todos los conectados a la misma VLAN (2) y al Trunk.

Por lo tanto:
H6 → H7, AP, Switch, S2, Router

Broadcast desde S3
S3 enviará broadcast y:

- El Router lo recibe pero no replica a nadie más.

Por lo tanto:
S3 → Router

3.6.2.2 Complete the list of devices traversed by an Ethernet frame sent from:

H2 hacia S3: H2 → Hub → H134 & Switch → Router → S3
H5 hacia S2: H5 → Switch → Router → Switch → S2
H7 hacia S1: H7 → AP → Switch → Router → Switch → S1

3.6.2.3 If all PCs (H*) transmit Ethernet frames (unicast) at the maximum rate and continuously from the server belonging to its corresponding VLAN (S1 for VLAN 1 and S2 for VLAN 2), compute the maximum transfer speed achieved by:

Sabemos que todas las conexiones se transmiten a 100 Mbps.

H3 hacia S1:

- Dado que transmiten los 4 del Hub, habrá 25 Mbps en cada salida del Hub, pero 100 Mbps a la salida hacia el Switch.
- H5 manda al Switch también a 100 Mbps.
- No podemos tener una recepción por parte de S1 de 100Mbps si recibimos 200Mbps, por lo tanto habrá que rebajar las entradas desde el Hub y H5 ambas a 50 Mbps.

Por lo tanto, H3 retransmitirá 50(Hub) / 4 (entradas de Hub) = 12.5 Mbps.

H5 hacia S1:

- Siguiendo el mismo razonamiento que en el anterior

Por lo tanto H5 retransmitirá 50Mbps.

H6 hacia S2:

- Al solo haber una entrada al Switch para la VLAN 2, los 100Mbps se mantienen para AP a repartir entre los dos hosts.

Por lo tanto 100 (AP) / 2 (hosts del AP) = 50 Mbps.

3.6.3.4 If all PCs (H*) receive Ethernet frames from their corresponding server in their VLAN, compute the maximum transfer speed they achieve.

Sabemos que todas las conexiones se transmiten a 100 Mbps.

S1 hacia VLAN1:
Al transmitir, se divide entre cuántos van a recibir, por lo tanto:
100 (envío) / 5 (receptores) = 20Mbps

S2 hacia VLAN2:
Al transmitir, se divide entre cuantos van a recibir, por lo tanto:
100 (envío) / 2 (Receptores) = 50Mbps

3.6.3.5 Which MAC addresses will be in the Switch MAC table?

Tendrá todos aquellos que han pasado por ahí, es decir, todos exceptuando S3, ya que tiene un Router entre medio (> Layer 2)

Tema 4: TCP

4.1 Protocolo UDP

4.1.1 Introducción a la capa de Transporte de Internet

La capa de transporte ofrece un canal de comunicación entre aplicaciones, las cuales se identifican en puertos de 16 bits.
Se usan dos protocolos:

- User Datagram Protocol (UDP): Ofrece un servicio de datagrama en el que no se puede confiar pero con poca latencia.
- Transmission Control Protocol (TCP):Ofrece un servicio de confianza a coste de una alta latencia.

Ambos protocolos usan el paradigma cliente-servidor.

4.1.2 Descripción

Servicio de datagramas al igual que IP, por lo tanto:

- No transmite confianza
- No tiene recuperación de errores
- No tiene ACK
- No tiene control de flujo

No tiene un buffer de transmisión, así que cada que escribe, genera un datagrama UDP (PDU).
UDP se usa cuando se quiere tener velocidad de transmisión por encima de la llegada del 100% de paquetes: Transmisión de voz y audio, por ejemplo.

4.1.3 Cabecera UDP

Tiene un tamaño fijo de 8 bytes, el checksum se computa mediante la cabecera, una pseudo-cabecera y el payload.
Debido a la existencia de la pseudo-cabecera, el checksum se tendrá que actualizar si se usa PAT.

4.2 Protocolos ARQ

4.2.1 Introducción

Los protocolos ARQ (Automatic Repeat reQuest), crean un canal de comunicación fiable entre endpoints, añadiendo funcionalidades como:

- Detección de errores
- Recuperación de errores y orden
- Control de flujo

Funcionalidades que le faltaban a UDP.

4.2.1.1 Protocolos basicos

- Stop and Wait
- Go Back N
- Retransmisión selectiva

4.2.1.2 Ingredientes de ARQ

- Orientado a la conexión
- Buffers de transmisión y recepción
- ACK
- Los ACKs se pueden devolver en la dirección opuesta
- Timeouts de Retransmisión (entiendo que esto es flow control)
- Números de secuencia

4.2.2 Asumpciones

- Deberemos centrarnos en la transmisión en una dirección.
- Deberemos asumir que el origen está saturado: Siempre tiene información pendiente de envío.
- Deberemos asumir que trabajamos con full duplex.
- Deberemos asumir que las vacas son esfericas.
- Deberemos asumir las siguientes definiciones:
    - D es la distancia en metros
    - v_p es el bitrate en bps
    - La velocidad de propagación será la división de los dos anteriores.
- Deberemos asumir que trabajamos en una capa genérica donde el emisor manda PDUs de Información y el receptor manda PDUs de ACK.

4.2.3 Protocolo Stop and Wait