Servicios de la capa de enlace

Framing

Una entidad de la capa de Enlace en un emisor recibe una **PDU de la capa de Red, o paquete**, y crea una PDU de la capa de Enlace (**frame, marco o trama**) que la contiene. El frame puede incluir direcciones de enlace en la cabecera o **header** y un campo de cola o **trailer** de redundancia para control de integridad del frame.

En el lado del receptor, la capa de Enlace reconoce el frame, determinando dónde comienza y termina, separando los campos de header y trailer y entregando su contenido a la capa de Red.

Control de acceso al medio

Ciertas clases de enlace pueden requerir reglas de arbitrado de acceso al medio. Un protocolo de acceso al medio define cuál, de entre todos los nodos conectados, podrá acceder al medio en cada momento para transmitir sus datos.

Entrega confiable

Algunas tecnologías de enlace ofrecen un mecanismo de confiabilidad que asegura el reenvío de los frames con condiciones de error, faltantes o desordenados.

Control de flujo

Ciertas clases de enlaces ofrecen un mecanismo de control de flujo que asegura no saturar a la entidad receptora. Este control de flujo afecta exclusivamente a la transmisión entre dos nodos adyacentes, es decir, pertenecientes al mismo enlace. Lo implementan algunas tecnologías de enlaces punto-a-punto, en particular, las de modems o de interfaces inalámbricas.

Detección y corrección de errores

En algunos enlaces, la tasa de error es sumamente baja y no se justifica aumentar la complejidad de la transmisión de datos con un mecanismo de detección de errores. En esos casos, la instancia de control de integridad que aportan las capas superiores (función de **checksum** de IP, UDP y TCP) es suficiente. Sin embargo, en otros casos, más propensos a errores que otros, es preferible contar con un mecanismo de detección de errores que asegure la integridad a nivel de enlace, entre puntos adyacentes, porque la recuperación de errores ocurridos en un segmento arbitrario de un camino largo puede ser muy costosa.

Preguntas

- ¿Cuáles son las diferencias en las funciones de control de flujo de la capa de Enlace y de Transporte?
- ¿Cuáles son las diferencias en las funciones de detección y corrección de errores de la capa de Enlace y de Transporte?

Detección y corrección de errores

En las PDU de las capas de Transporte y de Red encontramos el campo de Internet Checksum o suma de control para verificación de la integridad de las PDU. En la capa de Enlace, las funciones de control de errores son más sofisticadas y pueden detectar (y aun corregir) errores de uno o varios bits.

Esquemas de detección de errores

- Bits de paridad
- Métodos de sumas de control (Checksums)
- Control de redundancia cíclico (Cyclic Redundancy Check, CRC)

Enlaces

- Punto a punto (point-to-point)

  Enlaces de fibra óptica, enlaces inalámbricos direccionales (microondas, satelitales)

- De acceso múltiple o de difusión (broadcast)

  Todos los nodos del enlace están conectados al mismo canal de difusión compartido. Cableado de cobre en LANs, WiFi.

Protocolos de acceso múltiple

Cuando los medios son compartidos, es posible que dos o más nodos comiencen una transmisión al mismo tiempo, haciendo que los frames emitidos colisionen. El efecto de una colisión es corromper los frames que colisionan (hacerlos irreconocibles para la entidad de Enlace que debe recibirlas). Por este motivo es necesaria alguna forma de coordinación para reducir o eliminar la probabilidad de colisiones. Esta función de la capa de Enlace se llama control de acceso al medio (Medium Access Control, abreviado MAC).

Características deseables de un protocolo de acceso múltiple

- Equitativo

  Cuando haya M nodos que tienen datos para enviar compartiendo un canal de capacidad R, cada nodo deberá poder lograr en promedio una tasa de transferencia de R/M.

- Descentralizado

  Si existiera un único coordinador del acceso al medio, éste podría convertirse en un **cuello de botella** y en un **punto único de falla**. Un protocolo de acceso al medio descentralizado es aquel donde la decisión de cuál nodo será el siguiente en acceder es tomada en forma colaborativa por todos los nodos del enlace.

- Simple

Categorías de protocolos de acceso múltiple

Protocolos de particionamiento de canal

- TDM (Time Division Multiplexing)
- FDM (Frequency Division Multiplexing)

De toma de turnos

- Token Passing (Token Bus, Token Ring)

De acceso aleatorio

- ALOHA
- CSMA
- Ethernet

Direccionamiento de Enlace

Así como las direcciones IP corresponden a la capa de Red, existe un espacio de direcciones propio de la capa de Enlace.

- Las direcciones IP públicas son alcanzables desde cualquier punto de Internet. En cambio, las direcciones de la capa de Enlace sólo son visibles en el ámbito de un enlace.
- Las direcciones de enlace están fijas a los dispositivos de comunicaciones o interfaces y viajan con ellos. Cuando un dispositivo cambia de red, cambia de dirección IP pero conserva su dirección de Enlace. Una analogía válida relacionaría la dirección MAC con el DNI de una persona, y la dirección IP con el domicilio postal.
- Las direcciones IP tienen una estructura jerárquica, porque expresan un número de red o subred, y un número de host contenido en esa red. El espacio de direcciones de Enlace es plano.

En una LAN, los dispositivos de hardware, o interfaces, están configurados por el fabricante con direcciones de hardware o **direcciones MAC**. Las direcciones MAC están compuestas por seis octetos y suelen escribirse en notación hexadecimal (como, por ejemplo, **1A:23:F9:CD:06:9B**). Este formato aplica a las direcciones MAC en redes Ethernet, Token Ring, y WiFi. Otras tecnologías de capa de Enlace pueden tener direcciones conformadas de otra manera.

Una dirección MAC se separa en dos componentes: los tres primeros octetos (Organizational Unique Identifier, OUI) son asignados por IEEE a los fabricantes de dispositivos en forma única. Cada fabricante recibe su OUI y administra los tres restantes octetos a conveniencia, de modo de no liberar al mercado dos dispositivos con la misma dirección.

Las direcciones MAC destino y origen (en ese orden) aparecen en la cabecera de todos los frames emitidos. En un medio compartido, cuando una estación gana el canal, comienza a transmitir su frame, el cual se difunde por el medio y alcanza a todas las estaciones. Sólo la estación cuya dirección física coincide con la dirección destino del frame lo procesa, extrayendo la PDU de capa de Red contenida y elevándola a la entidad de Red de ese nodo. Todas las demás estaciones simplemente descartan el frame.

Sin embargo, existe una dirección de capa de Enlace especial, la **dirección de broadcast**, que es reconocida como propia por todos los nodos de la red.

Cuando un frame contiene como dirección destino la dirección de broadcast (**FF:FF:FF:FF:FF:FF**), todos los nodos que reciben el frame lo procesan como si fuera dirigido a ellos. Los frames de broadcast son importantes en muchos protocolos que necesitan distribuir información o hacer consultas en toda la LAN.

Interfaz entre capas de Red y de Enlace

Cada vez que un host necesita hacer llegar paquetes a otro nodo destino, debe conocer la dirección IP de ese destino para poder iniciar la solicitud a la entidad de capa de Red emisora. Esta dirección IP destino puede ser conocida de antemano por la aplicación, o puede haber sido el resultado de una traducción de nombres pedida a un servidor DNS.

Esta dirección IP es toda la información que tiene la entidad de Red emisora para hacer llegar su paquete a destino. Cuando la entidad de Red recibe la orden de emitir el paquete, debe determinar **si el destino se encuentra en la misma red, o en una red diferente**. La respuesta a esta pregunta es fundamental para que la capa de Enlace pueda construir correctamente el frame que transportará ese paquete.

Para responder esta pregunta, la capa de Red utiliza la **tabla de ruteo** o tabla de reenvío del host origen para encontrar una ruta al destino.

Se distinguen dos casos:

1. Si la ruta elegida dice que la red del destino está directamente conectada al host, se debe construir un frame con la dirección destino igual a la dirección MAC del nodo destino.
2. Si la ruta elegida dice que la red del destino **no es la misma que la del host**, entonces esa red está más allá de un cierto router; y se debe construir un frame con la dirección destino igual **a la dirección MAC del router**.

En el caso 1, la entrega del paquete es local al ámbito de enlace, porque origen y destino están en la misma red. En cambio, en el caso 2, se necesita el servicio de un router que se encargue de transportar el paquete más allá de la red de origen.

Ejemplo

Sea host A con la dirección IP 170.210.80.14/26, y cuyo router por defecto es R, con dirección 170.210.80.1. Supongamos que este host A hace ping, o cualquier otro tipo de tráfico basado en IP, hacia otro host B.

1. Si la dirección del host B fuera, por ejemplo, 170.210.80.8, entonces la entidad de Red del host A, aplicando la máscara de 26 bits de su configuración a la dirección destino de B, encontraría que la red destino es la misma que la red origen, ya que **dirección(A) AND máscara = dirección(B) AND máscara**. La entrega será local. Se encapsulará el paquete en un frame con la dirección MAC del host B y será enviado por la red.
2. Si la dirección del host B fuera, en cambio, 200.15.1.7, entonces la entidad de Red del host A determinará que la red destino **es otra**; y necesariamente la entrega deberá hacerse a través del router R. Se encapsulará el paquete en un frame con la dirección MAC **del router R** y este frame será enviado por la red. La interfaz del router R será la que procese el frame, extraiga el paquete, y lo someta al proceso de reenvío habitual que realizan los routers.

Protocolo ARP

El protocolo de resolución de direcciones (Address Resolution Protocol, ARP) es el que relaciona la capa de Red con la capa de Enlace. Es el mecanismo que permite averiguar la dirección MAC de un nodo a quien se dirige un paquete.

Para generar el frame que transporte un paquete se necesita la dirección MAC de un segundo nodo, ya sea la del destinatario final (si se encuentra en la red local), o la del router intermedio (si el destinatario se encuentra en una red remota). ¿Cómo se obtiene esta dirección MAC? Aquí es donde interviene el protocolo ARP.

Cuando la capa de Red del host A decida de quién es la dirección MAC que necesita (la de B o la de R), el protocolo ARP emitirá un frame de broadcast conteniendo una **consulta ARP**, la cual, básicamente, dice "¿De quién es la dirección IP X.X.X.X?". Como el frame es emitido con destino a la dirección de broadcast, todos los nodos de la red lo procesarán. Aquel que esté configurado con la dirección IP presentada en la consulta emitirá una **respuesta ARP** dirigida al nodo A, y esta respuesta ARP contendrá la dirección MAC buscada. A partir de aquí el nodo A puede terminar de construir el frame y enviarlo a la red.

Este tráfico ARP, aunque necesario, introduce una cierta demora y una cierta carga en la red. Para minimizar estos inconvenientes, y como es sumamente probable que se vuelva a necesitar esta dirección MAC para el tráfico siguiente, esta relación **dirección IP-dirección MAC** recientemente averiguada se guarda en una cache, la **tabla ARP** del host. Eventualmente el tiempo de vida de esta entrada expirará, y la entrada será borrada de la tabla.

La tabla arp puede consultarse con el comando arp -a.

Ethernet

El formato de los frames Ethernet incluye:

- Un **preámbulo** o campo de sincronización, de 8 bytes, que sirve para que el receptor ajuste el reloj de su interfaz de manera de reconocer correctamente el resto de los bits.
- Las **direcciones MAC destino y origen** del frame, cada una de 6 bytes.
- Un campo **tipo** de 2 bytes, que especifica qué contenido transporta el frame, y por lo tanto qué entidad de capa superior debe recibir ese contenido en el receptor.
- Un campo de **datos** o carga útil, de entre 46 y 1500 bytes, que contiene la PDU de la capa usuaria (habitualmente un paquete IP).
- Y un trailer llamado **Frame Check Sequence (FCS)** conteniendo el CRC aplicado al frame por el emisor.

CSMA/CD

La sigla **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)** identifica al protocolo de acceso al medio de la tecnología Ethernet. Se trata de un protocolo de acceso aleatorio inspirado en **ALOHA**, una red de radio creada para la Universidad de Hawaii en los años 70.

En Ethernet, los nodos comparten un medio, como un **bus** o un repetidor multivía (un **hub**), y su tráfico puede sufrir colisiones. La filosofía de Ethernet es tratar de evitar que estas colisiones se produzcan, y cuando ocurren, recuperarse de ellas. Para esto, los nodos aplican las reglas de CSMA/CD. Esta técnica replica aproximadamente la conducta de dos personas que tratan de no interrumpirse durante una conversación, en cuyo caso esperan un tiempo antes de volver a hablar:

- Antes de transmitir, un nodo sensa el canal. Si está ocupado, espera a que se desocupe.
- Cuando un nodo que desea transmitir encuentra el canal desocupado, comienza a transmitir, sensando simultáneamente el canal, para controlar que el estado eléctrico del medio coincida con lo que está transmitiendo.
- Si, dentro del tiempo que tarda en emitir los primeros **512 bits** (conocido como **ventana de colisión**) no se encuentran problemas, considera ganado el canal según el protocolo de acceso al medio, y continúa la emisión del frame hasta el final.
- Si en algún momento la lectura del medio no corresponde a lo que se está transmitiendo, se ha detectado una colisión. En ese caso, el nodo emite una señal llamada de **jam** para indicar al resto de los nodos que ha ocurrido una colisión, y entra en un procedimiento de recuperación de la colisión llamado **backoff exponencial**.

- Para esto toma un número aleatorio entero K, que puede valer 0 o 1, espera una cantidad de tiempo igual a **K * ventana de colisión**, y vuelve a transmitir.
- Si vuelve a producirse colisión, elige un nuevo entero aleatorio K esta vez entre 0 y 3, y nuevamente espera un nuevo intervalo de tiempo igual a K * ventana de colisión.
- Cada vez que vuelva a ocurrir una colisión, el nuevo valor aleatorio de K estará en [0, 2^c-1] donde c es el número de ciclo.
- El ciclo se repite hasta 16 veces. Si al cabo de 16 ciclos de backoff se ha sufrido colisión en todos los intentos, se declara que la transmisión ha fallado.

Al momento de elegir cuánto tiempo esperar para retransmitir, la estrategia del backoff exponencial apunta a encontrar un equilibrio entre dos extremos. Si el tiempo de espera fuera muy corto, la probabilidad de una segunda colisión aumentaría. Si fuera demasiado largo, se desperdiciaría mucho tiempo de uso del canal en la resolución de la colisión, y así se reduciría el throughput de la red. Al ir aumentando el intervalo de donde se extraen los números aleatorios, la probabilidad de que coincidan los tiempos esperados por ambos nodos va decreciendo exponencialmente.

Bridges

En un medio de acceso múltiple, y en ausencia de un sistema de acceso al medio como los de división de canal, o de toma de turnos, pueden ocurrir colisiones. Todos los hosts que puedan verse involucrados en una colisión forman un **dominio de colisión**. Si el dominio de colisión es grande (con muchos hosts), las colisiones pueden reducir notablemente el rendimiento de la red.

Un **bridge**, o puente, es un dispositivo que divide los **dominios de colisión**, para hacerlos más pequeños, es decir, integrados por **menos** hosts. Al existir menor cantidad de hosts en un dominio de colisión, la probabilidad de colisiones será menor y se podrá reducir el gasto de ancho de banda en la ocurrencia y recuperación de las colisiones.

Aprendizaje

Un bridge funciona en la capa de Enlace, ya que es capaz de reconocer frames e interpretar direcciones MAC. Cuenta con dos o más interfaces, conectadas a diferentes segmentos de un medio de acceso múltiple, y una **tabla de direcciones MAC**, en memoria, asociada a cada interfaz. Inicialmente, la tabla

de cada interfaz está vacía; pero al recibir tráfico, el bridge **aprende** qué estaciones se encuentran sobre cada segmento de red conectado. Las interfaces del bridge se disponen en **modo promiscuo**, es decir, pueden procesar frames cuyas direcciones MAC destino **no sean las del bridge**.

Para cada frame que ingrese por una interfaz, el bridge tomará nota de cuál es la dirección MAC **origen** del frame, y la agregará a la tabla de direcciones MAC asociada con esa interfaz. De esta forma, el bridge estará registrando que la estación con esa dirección MAC es adyacente a la interfaz en cuestión. Al cabo de algún tiempo, el bridge habrá construido una especie de mapa que indicará sobre cuál interfaz se ubica cada host de la red. Este aprendizaje es automático y resulta transparente a los usuarios. El bridge funcionará sin ninguna configuración, y, si bien sus interfaces tienen direcciones MAC, nunca necesitarán ser direccionadas por ningún tráfico de los usuarios.

Filtrado

Para cada frame que ingrese, el bridge además buscará la dirección MAC **destino** de ese frame en las tablas de sus diferentes interfaces. Pueden ocurrir cuatro situaciones:

1. La dirección destino no se encuentra en ninguna de las tablas, posiblemente porque el host destino aún no ha efectuado ninguna clase de tráfico. En este caso el bridge **copia el frame en todas sus demás interfaces**, es decir, **inunda** sus interfaces con ese frame.
2. La dirección destino se encuentra en la tabla **de la misma interfaz por la cual ingresó el frame**. En ese caso, tanto la estación origen como la estación destino están ubicadas sobre un mismo segmento de red, y no tiene sentido reenviar ese frame por ninguna otra interfaz. El frame simplemente **se descarta**, porque el medio de acceso múltiple permitirá que el frame, ya emitido, llegue a la estación destino sin que haga falta ninguna otra acción.
3. La dirección destino se encuentra en la tabla de **una interfaz distinta a la de ingreso**. En este caso el bridge reenvía el frame por la interfaz donde se encuentra el host destino, **y sólo por esa interfaz**, segmentando efectivamente el tráfico de modo que los hosts en los demás segmentos no reciban tráfico irrelevante para ellos.
4. La dirección destino es **la dirección de broadcast**. Este frame le compete, potencialmente, **a todos** los hosts de la red, y por lo tanto **debe inundarse** como en el caso en que no se conoce la ubicación del destino.

El mecanismo descripto, de aprendizaje automático y filtrado de frames, tiene el resultado de dividir los dominios de colisión, puesto que, si ocurriera una colisión

sobre un segmento, el bridge descartaría el frame (porque ha quedado corrupto) y no habría novedad alguna sobre los demás segmentos. Un dominio de colisión de n hosts donde insertáramos un bridge podría quedar dividido en dos dominios de $n/2$ hosts, con una probabilidad de colisiones menor en cada uno de ellos.

Un aspecto interesante de los bridges es que pueden ser construidos de manera que relacionen dominios de colisión implementados sobre diferentes tecnologías de enlace. Así, un bridge puede conectar (y filtrar) segmentos Ethernet, Token Ring, 802.11 (inalámbricos o "WiFi"), etc.

Switches

Un **bridge multivía** es un **switch** o **conmutador**. Se trata de un elemento de conmutación **en capa de Enlace**, de varias interfaces, que realiza **aprendizaje de direcciones MAC y filtrado de frames** por cada una de esas interfaces.

Siendo funcionalmente un bridge, el switch aplica las reglas basadas en direcciones MAC origen y destino para la fase de aprendizaje y para la fase de filtrado. Si ingresa al switch un frame:

- Con dirección MAC origen hasta ahora desconocida, la dirección **se aprenderá** (se almacenará en la tabla de direcciones MAC asociada a esa interfaz).
- Con dirección MAC destino hasta ahora desconocida, la acción será **inundarlo** por todas sus interfaces.
- De broadcast, la acción será **inundarlo** por todas sus interfaces.
- Con direcciones MAC origen y destino conocidas y localizadas en la misma tabla de una interfaz, el frame **se descarta**.
- Con direcciones MAC origen y destino conocidas y localizadas en tablas de diferentes interfaces, el frame será **reenviado sólo** a la interfaz correspondiente.
- . . . corrupto por colisiones, será descartado.

El funcionamiento de la red Ethernet "clásica", tal cual se inventó, corresponde a la descripción del algoritmo CSMA/CD sobre un medio de acceso múltiple único y compartido, como un bus coaxil, o un **hub**. Sin embargo, las redes "Ethernet" modernas se **conmutan**, es decir, se implementan con switches. Aunque las interfaces de los hosts siguen funcionando de la misma manera y el formato de los frames es el mismo, en las redes conmutadas no existen las colisiones.

Una vez que el switch haya aprendido las direcciones MAC de los hosts en la red (según la dirección origen de los frames), comenzará a filtrar los frames (según su dirección destino) haciendo que el tráfico entre dos estaciones **circule sólo entre ellas**. De esta manera creará un camino virtual privado a través de su **switching fabric**, o entramado de conmutación, entre cada par de estaciones

que se comunican. Salvo mal funcionamiento o ataque al switch, ningún otro host de la red puede recibir ese tráfico, por lo cual son una alternativa más segura que los hubs.

Dominio de broadcast

Conectando unos switches a otros en forma de árbol puede formarse una jerarquía de switches. Como cada switch inunda los broadcasts, todos los hosts conectados a una misma jerarquía de switches forman un **dominio de broadcast**. Es decir, cualquier frame de broadcast emitido por cualquiera de los hosts conectados, será recibido por todos los demás.

Spanning Tree Protocol (STP)

Redundancia y tolerancia a fallos

Una topología creada utilizando una jerarquía de switches en árbol tendrá la desventaja de que cada uno de esos switches y enlaces entre ellos resulta un punto único de falla. En redes de misión crítica, normalmente se busca asegurar **tolerancia a fallos**, aplicando alguna forma de **redundancia**. Esto quiere decir que, si duplicamos todos o algunos de los caminos, podremos contar con un camino alternativo para los frames en caso de fallos de switches o de enlaces.

Por este motivo, las topologías tolerantes a fallos ya no corresponden a árboles, sino a grafos que presentan **ciclos**.

Sin embargo, en una topología Ethernet con ciclos, inmediatamente aparecen anomalías:

- Un frame que (por error, o debido a un ataque) sea dirigido a una dirección MAC **que no se encuentre en la red**, será inundado por el primer switch que lo reciba; pero también por el siguiente, y por el siguiente... hasta volver al primer switch, y así infinitamente, cayendo en un ciclo de conmutación que no se romperá nunca, sobrecargando la red y ocupando recursos sin ningún resultado útil.
- Un frame **de broadcast** será inundado, con el mismo efecto.

Protocolo STP

Debido al problema de la inundación, las topologías con ciclos **están prohibidas** en las redes Ethernet. Pero aún puede utilizarse esa redundancia para obtener tolerancia a fallos gracias al protocolo de árbol de expansión o **STP**. Este protocolo está normalizdo por IEEE bajo la denominación **802.1d**.

Todos los bridges (y por lo tanto, todos los switches) deben implementar el protocolo STP. Mediante este protocolo los switches de una topología con ciclos se configuran en un árbol (un grafo sin ciclos) seleccionando y desactivando algunos enlaces. Los hosts siguen quedando todos conectados al mismo dominio de broadcast; sin embargo, ya no hay ciclos de conmutación entre ellos, y en caso de fallo de algún switch o enlace activo, el árbol será reconfigurado de manera de activarse un camino alternativo.

Para configurar su árbol de expansión, los switches intercambian **BPDUs** (unidades de datos de protocolo STP) con sus switches vecinos.

- Las BPDUs contienen un número **BID (Bridge ID)** compuesto por un número de prioridad (por defecto, 32768) seguido de la dirección MAC perteneciente al switch.
- Estas BPDUs llevan una dirección destino **multicast** reservada, gracias a lo cual son inundadas hasta llegar a todos los switches de la topología. En el camino, los switches que atraviesan van agregándoles información.
- El switch con el BID más bajo es elegido el **switch raíz** del árbol.
- Cada switch identifica cuál es la interfaz más cercana al raíz y la considera su **interfaz raíz**.
- Las interfaces que miran a otros switches pasarán a estado **designado** si están más cerca del switch raíz. Emitirán y recibirán BPDUs y frames de datos que circulen por la red.
- Todas las demás interfaces hacia otros switches pasarán a estado **bloqueado**, o desactivado y no emitirán BPDUs ni frames de datos.
- Las interfaces quedan intercambiando BPDUs con los demás switches en forma periódica, para detectar fallos.
- En caso de fallo, se repite el procedimiento de configuración del árbol, reconectándose todos los nodos a la topología a través de caminos alternativos.

El administrador de una topología puede influir en la elección del bridge raíz configurando manualmente la prioridad que compone el BID. Por defecto, sin embargo, el mecanismo es automático y transparente.

Más detalles

- STP
- El protocolo de árbol de expansión (802.1d)