Propósito de la capa de enlace de datos.

La capa de enlace de datos.

La capa de enlace de datos del modelo OSI (Capa 2), como se muestra en la figura 1, es responsable de lo siguiente:

- Permite a las capas superiores acceder a los medios.
- Acepta paquetes de la capa 3 y los empaqueta en tramas.
- Prepara los datos de red para la red física.
- Controla la forma en que los datos se colocan y reciben en los medios.
- Intercambia tramas entre los nodos en un medio de red físico, como UTP o fibra óptica.
- Recibe y dirige paquetes a un protocolo de capa superior.
- Lleva a cabo la detección de errores

La notación de la capa 2 para los dispositivos de red conectados a un medio común se denomina “nodo”. Los nodos crean y reenvían tramas. Como se muestra en la figura 2, la capa de enlace de datos OSI es responsable del intercambio de tramas Ethernet entre los nodos de origen y de destino a través de un medio de red físico.

La capa de enlace de datos separa de manera eficaz las transiciones de medios que ocurren a medida que el paquete se reenvía desde los procesos de comunicación de las capas superiores. La capa de enlace de datos recibe paquetes de un protocolo de capa superior y los dirige a un protocolo de las mismas características, en este caso, IPv4 o IPv6. Este protocolo de capa superior no necesita saber qué medios utiliza la comunicación.

Subcapas de enlace de datos.

La capa de enlace de datos se divide en dos subcapas:

- **Control de enlace lógico (LLC):** esta subcapa superior se comunica con la capa de red. Coloca en la trama información que identifica qué protocolo de capa de red se utiliza para la trama. Esta información permite que varios protocolos de la Capa 3, tales como IPv4 e IPv6, utilicen la misma interfaz de red y los mismos medios.
- **Control de acceso al medio (MAC):** se trata de la subcapa inferior, que define los procesos de acceso al medio que realiza el hardware. Proporciona direccionamiento de la capa de enlace de datos y acceso a varias tecnologías de red.

En la figura, se muestra la forma en que la capa de enlace de datos se divide en las subcapas LLC y MAC. La subcapa LLC se comunica con la capa de red, mientras que la subcapa MAC admite diversas tecnologías de acceso de red. Por

ejemplo, la subcapa MAC se comunica con la tecnología LAN Ethernet para enviar y recibir las tramas a través de cables de cobre o de fibra óptica. La subcapa MAC también se comunica con tecnologías inalámbricas como Wi-Fi y Bluetooth para enviar y recibir tramas en forma inalámbrica.

Control de acceso al medio.

Los protocolos de la Capa 2 especifican la encapsulamiento de un paquete en una trama y las técnicas para colocar y sacar el paquete encapsulado de cada medio. La técnica utilizada para colocar y sacar la trama de los medios se llama método de control de acceso al medio.

A medida que los paquetes se transfieren del host de origen al host de destino, generalmente deben atravesar diferentes redes físicas. Estas redes físicas pueden constar de diferentes tipos de medios físicos, como cables de cobre, fibra óptica y tecnología inalámbrica compuesta por señales electromagnéticas, frecuencias de radio y microondas, y enlaces satelitales.

Sin la capa de enlace de datos, un protocolo de capa de red, tal como IP, tendría que tomar medidas para conectarse con todos los tipos de medios que pudieran existir a lo largo de la ruta de envío. Más aún, IP debería adaptarse cada vez que se desarrolle una nueva tecnología de red o medio. Este proceso dificultaría la innovación y desarrollo de protocolos y medios de red. Este es un motivo clave para usar un método en capas en interconexión de redes.

En la figura, se proporciona un ejemplo de una PC en París que se conecta a una PC portátil en Japón. Si bien los dos hosts se comunican exclusivamente mediante el protocolo IP, es probable que se utilicen numerosos protocolos de capa de enlace de datos para transportar los paquetes IP a través de diferentes tipos de redes LAN y WAN. Cada transición a un router puede requerir un protocolo de capa de enlace de datos diferente para el transporte a un medio nuevo.

Provisión de acceso a los medios.

Durante una misma comunicación, pueden ser necesarios distintos métodos de control de acceso al medio. Cada entorno de red que los paquetes encuentran cuando viajan desde un host local hasta un host remoto puede tener características diferentes. Por ejemplo, una LAN Ethernet consta de muchos hosts que compiten por acceder al medio de red. Los enlaces seriales constan de una conexión directa entre dos dispositivos únicamente.

Las interfaces del router encapsulan el paquete en la trama correspondiente, y se utiliza un método de control de acceso al medio adecuado para acceder a cada enlace. En cualquier intercambio de paquetes de capas de red, puede haber muchas transiciones de medios y capa de enlace de datos.

En cada salto a lo largo de la ruta, los routers realizan lo siguiente:

- Aceptan una trama proveniente de un medio.

- Desencapsulan la trama.
- Vuelven a encapsular el paquete en una trama nueva.
- Reenvían la nueva trama adecuada al medio de ese segmento de la red física.

El router de la figura tiene una interfaz Ethernet para conectarse a la LAN y una interfaz serial para conectarse a la WAN. A medida que el router procesa tramas, utilizará los servicios de la capa de enlace de datos para recibir la trama desde un medio, desencapsularlo en la PDU de la Capa 3, volver a encapsular la PDU en una trama nueva y colocar la trama en el medio del siguiente enlace de la red.

Topologias.

Control de acceso a los medios.

La regulación de la ubicación de las tramas de datos en los medios se encuentra bajo el control de la subcapa de control de acceso al medio.

El control de acceso a los medios es el equivalente a las reglas de tráfico que regulan la entrada de vehículos a una autopista. La ausencia de un control de acceso a los medios sería el equivalente a vehículos que ignoran el resto del tráfico e ingresan al camino sin tener en cuenta a los otros vehículos. Sin embargo, no todos los caminos y entradas son iguales. El tráfico puede ingresar a un camino confluyendo, esperando su turno en una señal de parada o respetando el semáforo. Un conductor sigue un conjunto de reglas diferente para cada tipo de entrada.

De la misma manera, hay diferentes métodos para regular la colocación de tramas en los medios. Los protocolos en la capa de enlace de datos definen las reglas de acceso a los diferentes medios. Estas técnicas de control de acceso a los medios definen si los nodos comparten los medios y de qué manera lo hacen.

El método real de control de acceso al medio utilizado depende de lo siguiente:

- **Topología:** cómo se muestra la conexión entre los nodos a la capa de enlace de datos.
- **Uso compartido de medios:** de qué modo los nodos comparten los medios. El uso compartido de los medios puede ser punto a punto, como en las conexiones WAN, o compartido, como en las redes LAN.

Topologías física y lógica.

La topología de una red es la configuración o relación de los dispositivos de red y las interconexiones entre ellos. Las topologías LAN y WAN se pueden ver de dos maneras:

- Topología física: se refiere a las conexiones físicas e identifica cómo se interconectan los terminales y dispositivos de infraestructura, como los routers, los switches y los puntos de acceso inalámbrico. Las topologías físicas generalmente son punto a punto o en estrella. Vea la Figura 1.
- Topología lógica: se refiere a la forma en que una red transfiere tramas de un nodo al siguiente. Esta disposición consta de conexiones virtuales entre los nodos de una red. Los protocolos de capa de enlace de datos definen estas rutas de señales lógicas. La topología lógica de los enlaces punto a punto es relativamente simple, mientras que los medios compartidos ofrecen métodos de control de acceso al medio diferentes. Vea la Figura 2.

La capa de enlace de datos "ve" la topología lógica de una red al controlar el acceso de datos a los medios. Es la topología lógica la que influye en el tipo de trama de red y control de acceso a los medios que se utilizan.

Topologías de WAN.

Topologías físicas de WAN comunes.

Por lo general, las WAN se interconectan mediante las siguientes topologías físicas:

- **Punto a punto:** esta es la topología más simple, que consta de un enlace permanente entre dos terminales. Por este motivo, es una topología de WAN muy popular.
- **Hub-and-spoke:** es una versión WAN de la topología en estrella, en la que un sitio central interconecta sitios de sucursal mediante enlaces punto a punto.
- **Malla:** esta topología proporciona alta disponibilidad, pero requiere que cada sistema final esté interconectado con todos los demás sistemas. Por lo tanto, los costos administrativos y físicos pueden ser importantes. Básicamente, cada enlace es un enlace punto a punto al otro nodo.

En la figura, se muestran las tres topologías físicas de WAN comunes.

Una híbrida es una variación o una combinación de cualquiera de las topologías mencionadas. Por ejemplo, una malla parcial es una topología híbrida en que se interconectan algunos terminales, aunque no todos.

Topología física punto a punto.

Las topologías físicas punto a punto conectan dos nodos directamente, como se muestra en la figura.

En esta disposición, los dos nodos no tienen que compartir los medios con otros hosts. Además, un nodo no tiene que determinar si una trama entrante está destinada a él o a otro nodo. Por lo tanto, los protocolos de enlace de datos lógicos pueden ser muy simples, dado que todas las tramas en los medios solo pueden transferirse entre los dos nodos. El nodo en un extremo coloca las tramas en los medios y el nodo en el otro extremo las saca de los medios del circuito punto a punto.

Topología lógica punto a punto.

Los nodos de los extremos que se comunican en una red punto a punto pueden estar conectados físicamente a través de una cantidad de dispositivos intermediarios. Sin embargo, el uso de dispositivos físicos en la red no afecta la topología lógica.

Como se muestra en la figura 1, los nodos de origen y destino pueden estar conectados indirectamente entre sí a través de una distancia geográfica. En algunos casos, la conexión lógica entre nodos forma lo que se llama un circuito virtual. Un circuito virtual es una conexión lógica creada dentro de una red entre dos dispositivos de red. Los dos nodos en cada extremo del circuito virtual intercambian las tramas entre sí. Esto ocurre incluso si las tramas están dirigidas a través de dispositivos intermediarios, como se muestra en la figura 2. Los circuitos virtuales son construcciones de comunicación lógicas utilizadas por algunas tecnologías de la Capa 2.

El método de acceso al medio utilizado por el protocolo de enlace de datos se determina por la topología lógica punto a punto, no la topología física. Esto significa que la conexión lógica de punto a punto entre dos nodos puede no ser necesariamente entre dos nodos físicos en cada extremo de un enlace físico único

Topologías de LAN.

Topologías físicas de LAN.

La topología física define cómo se interconectan físicamente los sistemas finales. En las redes LAN de medios compartidos, los terminales se pueden interconectar mediante las siguientes topologías físicas:

- **Estrella:** los dispositivos finales se conectan a un dispositivo intermediario central. Las primeras topologías en estrella interconectaban terminales mediante concentradores. Sin embargo, en la actualidad estas topologías utilizan switches. La topología en estrella es fácil de instalar, muy escalable (es fácil agregar y quitar dispositivos finales) y de fácil resolución de problemas.
- **Estrella extendida o híbrida:** en una topología en estrella extendida, dispositivos intermediarios centrales interconectan otras topologías en estrella. Una estrella extendida es un ejemplo de una topología híbrida.
- **Bus:** todos los sistemas finales se encadenan entre sí y terminan de algún modo en cada extremo. No se requieren dispositivos de infraestructura, como switches, para interconectar los terminales. Las topologías de bus con cables coaxiales se utilizaban en las antiguas redes Ethernet, porque eran económicas y fáciles de configurar.
- **Anillo:** los sistemas finales se conectan a su respectivo vecino y forman un anillo. A diferencia de la topología de bus, la de anillo no necesita tener una terminación. Las topologías de anillo se utilizaban en las antiguas redes de interfaz de datos distribuida por fibra (FDDI) y redes de Token Ring.

En la figura, se muestra cómo se interconectan los terminales en las redes LAN. Es común que una línea recta en un gráfico de redes represente una red LAN Ethernet que incluye una estrella simple y una estrella extendida.

. Half duplex y Full duplex.

Las comunicaciones dúplex refieren a la dirección en la que se transmiten los datos entre dos dispositivos. Las comunicaciones half-duplex limitan el intercambio de datos a una dirección a la vez, mientras que el dúplex completo permite el envío y recepción de datos simultáneo.

- **Comunicación half-duplex:** los dos dispositivos pueden transmitir y recibir en los medios pero no pueden hacerlo simultáneamente. El modo half-duplex se utiliza en topologías de bus antiguas y en directorios externos. Las redes WLAN también operan en half-duplex. Half-duplex también permite que solo un dispositivo envíe o reciba a la ve en el medio compartido, y se utiliza con métodos de acceso por contención. En la figura 1, se muestra la comunicación half-duplex.

- **Comunicación de dúplex completo:** los dos dispositivos pueden transmitir y recibir en los medios al mismo tiempo. La capa de enlace de datos supone que los medios están disponibles para transmitir para ambos nodos en cualquier momento. Los switches Ethernet operan en el modo de dúplex completo de forma predeterminada, pero pueden funcionar en half-duplex si se conectan a un dispositivo como un dispositivo externo. En la figura 2, se muestra la comunicación de dúplex completo.

Es importante que dos interfaces interconectadas, como la NIC de un host y una interfaz en un switch Ethernet, operen con el mismo modo dúplex. De lo contrario, habrá incompatibilidad de dúplex y se generará ineficiencia y latencia en el enlace.

Métodos de control de acceso al medio.

Algunas topologías de red comparten un medio común con varios nodos. Estas se denominan redes de acceso múltiple. Las LAN Ethernet y WLAN son un ejemplo de una red de accesos múltiples. En cualquier momento puede haber una cantidad de dispositivos que intentan enviar y recibir datos utilizando los mismos medios de red.

Algunas redes de acceso múltiple requieren reglas que rijan la forma de compartir los medios físicos. Hay dos métodos básicos de control de acceso al medio para medios compartidos:

- **Acceso por contención:** todos los nodos en half-duplex compiten por el uso del medio, pero solo un dispositivo puede enviar a la vez. Sin embargo, existe un proceso en caso de que más de un dispositivo transmita al mismo tiempo. Las LAN Ethernet que utilizan concentradores y las WLAN son un ejemplo de este tipo de control de acceso. En la figura 1, se muestra el acceso por contención.
- **Acceso controlado:** cada nodo tiene su propio tiempo para utilizar el medio. Estos tipos deterministas de redes no son eficientes porque un dispositivo debe aguardar su turno para acceder al medio. Las LAN de Token Ring antiguo son un ejemplo de este tipo de control de acceso. En la figura 2, se muestra el acceso controlado.

De forma predeterminada, los switches Ethernet funcionan en el modo de dúplex completo. Esto permite que el switch y el dispositivo conectado a dúplex completo envíen y reciban simultáneamente.

Acceso por contención: CSMA/CD.

Las redes WLAN, LAN Ethernet con concentradores y las redes de bus Ethernet antiguas son todos ejemplos de redes de acceso por contención. Todas estas redes funcionan en el modo half-duplex. Esto requiere un proceso para gestionar cuándo puede enviar un dispositivo y qué sucede cuando múltiples dispositivos envían al mismo tiempo.

En las redes LAN Ethernet de half-duplex se utiliza el proceso de acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD). En la Figura 1 se muestra una red LAN Ethernet que utiliza un concentrador. El proceso de CSMA es el siguiente:

1. La PC1 tiene una trama que se debe enviar a la PC3.
2. La NIC de la PC1 debe determinar si alguien está transmitiendo en el medio. Si no detecta un proveedor de señal, en otras palabras, si no recibe transmisiones de otro dispositivo, asumirá que la red está disponible para enviar.
3. La NIC de la PC1 envía la trama de Ethernet, como se muestra en la figura 1:
4. El directorio externo recibe la trama. Un directorio externo también se conoce como repetidor de múltiples puertos. Todos los bits que se reciben de un puerto entrante se regeneran y envían a todos los demás puertos, como se indica en la figura 2.
5. Si otro dispositivo, como una PC2, quiere transmitir, pero está recibiendo una trama, deberá aguardar hasta que el canal esté libre.
6. Todos los dispositivos que están conectados al concentrador reciben la trama. Dado que la trama tiene una dirección destino de enlace de datos para la PC3, solo ese dispositivo aceptará y copiará toda la trama. Las NIC de todos los demás dispositivos ignorarán la trama, como se muestra en la figura 3.

Si dos dispositivos transmiten al mismo tiempo, se produce una colisión. Los dos dispositivos detectarán la colisión en la red, es decir, la detección de colisión (CD). Esto se logra mediante la comparación de los datos transmitidos con los datos recibidos que realiza la NIC o bien mediante el reconocimiento de la amplitud de señal si esta es más alta de lo normal en los medios. Los datos enviados por ambos dispositivos se dañarán y deberán enviarse nuevamente.

Acceso por contención: CSMA/CA.

Otra forma de CSM que utilizan las redes WLAN del IEEE 802.11 es el acceso múltiple por detección de portadora con prevención de colisiones (CSMA/CA). CSMA/CA utiliza un método similar a CSMA/CD para detectar si el medio está libre. CSMA/CA también utiliza técnicas adicionales. CSMA/CA no detecta colisiones pero intenta evitarlas ya que aguarda antes de transmitir. Cada

dispositivo que transmite incluye la duración que necesita para la transmisión. Todos los demás dispositivos inalámbricos reciben esta información y saben por cuanto tiempo el medio no estará disponible, como se muestra en la figura. Luego de que un dispositivos inalámbricos envía una trama 802.11, el receptor devuelve un acuso de recibo para que el emisor sepa que se recibió la trama.

Ya sea que es una red LAN Ethernet con concentradores o una red WLAN, los sistemas por contención no escalan bien bajo un uso intensivo de los medios. Es importante tener en cuenta que las redes LAN Ethernet con switches no utilizan sistemas por contención porque el switch y la NIC de host operan en el modo de dúplex completo.

Trama de enlace de datos.

La trama.

La capa de enlace de datos prepara los paquetes para su transporte a través de los medios locales encapsulándolos con un encabezado y un tráiler para crear una trama. La descripción de una trama es un elemento clave de cada protocolo de capa de enlace de datos. Si bien existen muchos protocolos de capa de enlace de datos diferentes que describen las tramas de la capa de enlace de datos, cada tipo de trama tiene tres partes básicas:

- Encabezado
- Datos
- Tráiler

Todos los protocolos de capa de enlace de datos encapsulan la PDU de la Capa 3 dentro del campo de datos de la trama. Sin embargo, la estructura de la trama y los campos contenidos en el encabezado y tráiler varían de acuerdo con el protocolo.

No hay una estructura de trama que cumpla con las necesidades de todos los transportes de datos a través de todos los tipos de medios. Según el entorno, la cantidad de información de control que se necesita en la trama varía para cumplir con los requisitos de control de acceso al medio de la topología lógica y de los medios.

Como se muestra en la figura, un entorno frágil requiere más control.

Campos de trama.

El tramado rompe la transmisión en agrupaciones descifrables, con la información de control insertada en el encabezado y tráiler como valores en campos diferentes. Este formato brinda a las señales físicas una estructura que pueden recibir los nodos y que se puede decodificar en paquetes en el destino.

Como se muestra en la figura, los tipos de campos de trama genéricos incluyen lo siguiente:

- Indicadores de arranque y detención de trama: se utilizan para identificar los límites de comienzo y finalización de la trama.
- **Direccionamiento:** indica los nodos de origen y destino en los medios.
- **Tipo:** identifica el protocolo de capa 3 en el campo de datos.
- **Control:** identifica los servicios especiales de control de flujo, como calidad de servicio (QoS). QoS se utiliza para dar prioridad de reenvío a ciertos tipos de mensajes. Las tramas de enlace de datos que llevan paquetes de voz sobre IP (VoIP) suelen recibir prioridad porque son sensibles a demoras.
- **Datos:** incluye el contenido de la trama (es decir, el encabezado del paquete, el encabezado del segmento y los datos).
- **Detección de errores:** estos campos de trama se utilizan para la detección de errores y se incluyen después de los datos para formar el tráiler.

. Dirección de Capa 2.

La capa de enlace de datos proporciona direccionamiento que es utilizado para transportar una trama a través de los medios locales compartidos. Las direcciones de dispositivo en esta capa se llaman direcciones físicas. El direccionamiento de la capa de enlace de datos está contenido en el encabezado de la trama y especifica el nodo de destino de la trama en la red local. El encabezado de la trama también puede contener la dirección de origen de la trama.

A diferencia de las direcciones lógicas de la Capa 3, que son jerárquicas, las direcciones físicas no indican en qué red está ubicado el dispositivo. En cambio, la dirección física es única para un dispositivo en particular. Si el dispositivo se traslada a otra red o subred, sigue funcionando con la misma dirección física de la Capa 2.

Las figuras 1 a 3 muestran la función de las direcciones de la capa 2 y capa 3. A medida que el paquete IP se mueve de host a router, de router a router y, finalmente, de router a host, es encapsulado en una nueva trama de enlace de datos, en cada punto del recorrido. Cada trama de enlace de datos contiene la dirección de origen de enlace de datos de la tarjeta NIC que envía la trama y la dirección de destino de enlace de datos de la tarjeta NIC que recibe la trama.

No se puede utilizar una dirección específica de un dispositivo y no jerárquica para localizar un dispositivo en grandes redes o de Internet. Eso sería como intentar localizar una casa específica en todo el mundo, sin más datos que el nombre de la calle y el número de la casa. Sin embargo, la dirección física se puede usar para localizar un dispositivo dentro de un área limitada. Por este motivo, la dirección de la capa de enlace de datos solo se utiliza para entregas locales. Las direcciones en esta capa no tienen significado más allá de la red local. Compare esto con la Capa 3, en donde las direcciones en el encabezado del paquete pasan del host de

origen al host de destino, sin tener en cuenta la cantidad de saltos de redes a lo largo de la ruta.

Si los datos deben pasar a otro segmento de red, se necesita un dispositivo intermediario, como un router. El router debe aceptar la trama según la dirección física y desencapsularla para examinar la dirección jerárquica, o dirección IP. Con la dirección IP, el router puede determinar la ubicación de red del dispositivo de destino y el mejor camino para llegar a él. Una vez que sabe adónde reenviar el paquete, el router crea una nueva trama para el paquete, y la nueva trama se envía al segmento de red siguiente hacia el destino final.

Tramas LAN y WAN.

En una red TCP/IP, todos los protocolos de capa 2 del modelo OSI funcionan con la dirección IP en la capa 3. Sin embargo, el protocolo de capa 2 específicos que se utilice depende de la topología lógica y de los medios físicos.

Cada protocolo realiza el control de acceso a los medios para las topologías lógicas de Capa 2 que se especifican. Esto significa que una cantidad de diferentes dispositivos de red puede actuar como nodos que operan en la capa de enlace de datos al implementar estos protocolos. Estos dispositivos incluyen las tarjetas de interfaz de red en PC, así como las interfaces en routers y en switches de la Capa 2.

El protocolo de la Capa 2 que se utiliza para una topología de red particular está determinado por la tecnología utilizada para implementar esa topología. La tecnología está, a su vez, determinada por el tamaño de la red, en términos de cantidad de hosts y alcance geográfico y los servicios que se proveerán a través de la red.

En general, las redes LAN utilizan una tecnología de ancho de banda elevado que es capaz de admitir una gran cantidad de hosts. El área geográfica relativamente pequeña de una LAN (un único edificio o un campus de varios edificios) y su alta densidad de usuarios hacen que esta tecnología sea rentable.

Sin embargo, utilizar una tecnología de ancho de banda alto no es generalmente rentable para redes de área extensa que cubren grandes áreas geográficas (varias ciudades, por ejemplo). El costo de los enlaces físicos de larga distancia y la tecnología utilizada para transportar las señales a través de esas distancias, generalmente, ocasiona una menor capacidad de ancho de banda.

La diferencia de ancho de banda normalmente produce el uso de diferentes protocolos para las LAN y las WAN.

Los protocolos de la capa de enlace de datos incluyen:

- Ethernet
- 802.11 inalámbrico
- Protocolo punto a punto (PPP)
- HDLC

- Frame Relay

Trama de Ethernet.

Encapsulamiento de Ethernet.

Ethernet es la tecnología LAN más utilizada hoy en día.

Ethernet funciona en la capa de enlace de datos y en la capa física. Es una familia de tecnologías de red que se definen en los estándares IEEE 802.2 y 802.3. Ethernet admite los siguientes anchos de banda de datos:

- 0 Mb/s
- 100 Mb/s
- 1000 Mb/s (1 Gb/s)
- 10 000 Mb/s (10 Gb/s)
- 40 000 Mb/s (40 Gb/s)
- 100 000 Mb/s (100 Gb/s)

Como se muestra en la figura 1, los estándares de Ethernet definen tanto los protocolos de capa 2 como las tecnologías de capa 1. Para los protocolos de capa 2, como con todos los estándares IEEE 802, Ethernet depende de ambas subcapas individuales de la capa de enlace de datos para funcionar: la subcapa de control de enlace lógico (LLC) y la subcapa MAC

Subcapa LLC

La subcapa LLC de Ethernet maneja la comunicación entre las capas superiores e inferiores. Generalmente, esto sucede entre el software de red y el hardware del dispositivo. La subcapa LLC toma los datos del protocolo de la red, que generalmente son un paquete IPv4, y agrega información de control para ayudar a distribuir el paquete al nodo de destino. El LLC se utiliza para la comunicación con las capas superiores de la aplicación y para la transición del paquete hacia las capas inferiores con fines de distribución.

El LLC se implementa en el software, y su implementación es independiente del hardware. En una computadora, el LLC se puede considerar el software del controlador de la NIC. El controlador de la NIC es un programa que interactúa directamente con el hardware de la NIC para trasladar los datos entre la subcapa MAC y los medios físicos.

Subcapa MAC

La subcapa MAC es la subcapa inferior de la capa de enlace de datos y se implementa mediante hardware, generalmente, en la NIC de la computadora. Los

datos específicos se detallan en los estándares IEEE 802.3. En la figura 2, se detallan los estándares IEEE de Ethernet comunes.

. Subcapa MAC.

Como se muestra en la ilustración, la subcapa MAC de Ethernet tiene dos tareas principales:

- Encapsulamiento de datos
- Control de acceso al medio

Encapsulamiento de datos

El proceso de encapsulamiento de datos incluye el armado de tramas antes de la transmisión y el desarmado de tramas en el momento de la recepción. Para armar la trama, la capa MAC agrega un encabezado y un tráiler a la PDU de la capa de red.

El encapsulamiento de datos proporciona tres funciones principales:

Delimitación de tramas: el proceso de entramado proporciona delimitadores importantes que se utilizan para identificar un grupo de bits que componen una trama. Estos bits delimitadores proporcionan sincronización entre los nodos de transmisión y de recepción. **Direccionamiento:** el proceso de encapsulamiento contiene la PDU de capa 3 y también proporciona direccionamiento de la capa de enlace de datos. **Detección de errores:** cada trama contiene un tráiler utilizado para detectar errores de transmisión

La utilización de tramas facilita la transmisión de bits a medida que se colocan en los medios y en la agrupación de bits en el nodo receptor.

Control de acceso al medio

La segunda tarea de la subcapa MAC es el control de acceso al medio. El control de acceso al medio es responsable de colocar las tramas en los medios y de quitarlas de ellos. Como su nombre lo indica, controla el acceso a los medios. Esta subcapa se comunica directamente con la capa física.

La topología lógica subyacente de Ethernet es un bus de acceso múltiple, por lo que todos los nodos (dispositivos) de un único segmento de red comparten el medio. Ethernet es un método de red de contienda. En un método de contienda, cualquier dispositivo puede intentar transmitir datos a través del medio compartido siempre que tenga datos que enviar. Para detectar y resolver colisiones, se utiliza el proceso de acceso múltiple por detección de portadora con detección de colisiones (CSMA/CD) en las LAN Ethernet de dúplex medio. Las LAN Ethernet

actuales utilizan switches de dúplex completo, que permiten que varios dispositivos envíen y reciban datos en simultáneo y sin colisiones.

Evolución de Ethernet.

Desde la creación de Ethernet en 1973, los estándares evolucionaron para especificar versiones más rápidas y flexibles de la tecnología. Esta capacidad de Ethernet de mejorar con el tiempo es una de las principales razones por las que su uso está tan difundido. Las primeras versiones de Ethernet eran relativamente lentas, con una velocidad de 10 Mbps, mientras que las más recientes funcionan a 10 Gbps e, incluso, más rápido.

En la capa de enlace de datos, la estructura de la trama es casi idéntica para todas las velocidades de Ethernet. La estructura de la trama de Ethernet agrega encabezados y tráilers alrededor de la PDU de capa 3 para encapsular el mensaje que se envía, como se muestra en la figura 1.

Ethernet II es el formato de trama de Ethernet utilizado en las redes TCP/IP.

Campos de trama de Ethernet.

El tamaño mínimo de trama de Ethernet es de 64 bytes, y el máximo es de 1518 bytes. Esto incluye todos los bytes del campo "Dirección MAC de destino" hasta el campo "Secuencia de verificación de trama (FCS)" inclusive. El campo "Preámbulo" no se incluye al describir el tamaño de una trama.

Cualquier trama de menos de 64 bytes de longitud se considera un fragmento de colisión o una trama corta, y es descartada automáticamente por las estaciones receptoras. Las tramas de más de 1500 bytes de datos se consideran "jumbos" o tramas bebés gigantes.

Si el tamaño de una trama transmitida es menor que el mínimo o mayor que el máximo, el dispositivo receptor descarta la trama. Es posible que las tramas descartadas se originen en colisiones u otras señales no deseadas y, por lo tanto, se consideran no válidas.

En la ilustración, haga clic en cada campo de la trama de Ethernet para leer más acerca de su función.

Campo "Preambulo" y "Delimitador de inicio de trama"

Los campos Preámbulo (7 bytes) y Delimitador de inicio de trama (SFD), también llamado "inicio de trama" (1 byte), se utilizan para la sincronización entre los dispositivos emisores y receptores. Estos ocho primeros bytes de la trama se utilizan para captar la atención de los nodos receptores. Básicamente, los primeros bytes le indican al receptor que se prepare para recibir una trama nueva.

Campo Dirección MAC de destino

Este campo de 6 bytes es el identificador del destinatario deseado. Como recordará, la capa 2 utiliza esta dirección para ayudar a los dispositivos a

determinar si la trama está dirigida a ellos. La dirección de la trama se compara con la dirección MAC del dispositivo. Si coinciden, el dispositivo acepta la trama. Puede ser una dirección de unidifusión, de multidifusión o de difusión.

Campo Dirección MAC de origen

Este campo de 6 bytes identifica la NIC o la interfaz de origen de la trama. Debe ser una dirección de unidifusión.

Campo EtherType

Este campo de 2 bytes identifica el protocolo de capa superior encapsulado en la trama de Ethernet. Los valores comunes son, en hexadecimal, "0x800" para IPv4, "0x86DD" para IPv6 y "0x806" para ARP.

Campo de datos

Este campo (de 46 a 1500 bytes) contiene los datos encapsulados de una capa superior, que es una PDU de capa 3 o, más comúnmente, un paquete IPv4. Todas las tramas deben tener, al menos, 64 bytes de longitud. Si se encapsula un paquete pequeño, se utilizan bits adicionales (llamados "relleno") para aumentar el tamaño de la trama al tamaño mínimo.

Campo Secuencia de verificación de trama

El campo Secuencia de verificación de trama (FCS) (4 bytes) se utiliza para detectar errores en la trama. Utiliza una comprobación cíclica de redundancia (CRC). El dispositivo emisor incluye los resultados de una CRC en el campo FCS de la trama. El dispositivo receptor recibe la trama y genera una CRC para buscar errores. Si los cálculos coinciden, significa que no se produjo ningún error. Los cálculos que no coinciden indican que los datos cambiaron y, por consiguiente, se descarta la trama. Un cambio en los datos podría ser consecuencia de una interrupción de las señales eléctricas que representan los bits.

Direcciones MAC de Ethernet.

Dirección MAC y hexadecimal.

Una dirección MAC de Ethernet es un valor binario de 48 bits expresado como 12 dígitos hexadecimales (4 bits por dígito hexadecimal).

Así como el sistema decimal es un sistema numérico de base 10, el sistema hexadecimal es un sistema de base 16. El sistema numérico de base 16 utiliza los número del 0 al 9 y las letras de la A a la F. En la figura 1, se muestran los valores decimales y hexadecimales equivalentes para los números binarios del 0000 al 1111. Es más fácil expresar un valor como un único dígito hexadecimal que como cuatro bits binarios.

Dado que 8 bits (1 byte) es un método de agrupación binaria común, los números binarios del 00000000 al 11111111 se pueden representar en hexadecimal como el rango del 00 al FF, como se muestra en la figura 2. Los ceros iniciales se muestran siempre para completar la representación de 8 bits. Por ejemplo, el valor binario "0000 1010" se muestra en hexadecimal como "0A".

Nota: es importante distinguir los valores hexadecimales de los valores decimales con respecto a los caracteres del 0 al 9, como se muestra en la ilustración.

Representación de valores hexadecimales

Generalmente, el sistema hexadecimal se representa por escrito por medio del valor precedido por "0x" (por ejemplo, "0x73") o de un subíndice 16. En ocasiones menos frecuentes, puede estar seguido por una H (por ejemplo, "73H"). Sin embargo, y debido a que el texto en subíndice no se reconoce en entornos de línea de comandos o de programación, la representación técnica de un valor hexadecimal es precedida por "0x" (cero X). Por lo tanto, los ejemplos anteriores deberían mostrarse como "0x0A" y "0x73", respectivamente.

El valor hexadecimal se utiliza para representar las direcciones MAC de Ethernet y las direcciones IP versión 6.

Conversiones hexadecimales

Las conversiones numéricas entre valores decimales y hexadecimales son simples, pero no siempre es conveniente dividir o multiplicar por 16. Si es necesario realizar dichas conversiones, generalmente, es más fácil convertir el valor decimal o hexadecimal a un valor binario y, a continuación, convertir ese valor binario a un valor decimal o hexadecimal, según corresponda.

Dirección MAC: Identidad de Ethernet.

En Ethernet, cada dispositivo de red está conectado al mismo medio compartido. En el pasado, Ethernet era, en mayor medida, una topología de dúplex medio que utilizaba un bus de acceso múltiple o, más recientemente, hubs Ethernet. Es decir que todos los nodos recibían cada trama transmitida. Para evitar la sobrecarga excesiva que implicaba el procesamiento de cada trama, se crearon las direcciones MAC a fin de identificar el origen y el destino reales. El direccionamiento MAC proporciona un método de identificación de dispositivos en el nivel inferior del modelo OSI. Aunque actualmente Ethernet utiliza NIC y switches de dúplex completo, todavía es posible que un dispositivo que no es el destino deseado reciba una trama de Ethernet.

Estructura de la dirección MAC

El valor de la dirección MAC es el resultado directo de las normas implementadas por el IEEE para proveedores con el objetivo de garantizar direcciones únicas para cada dispositivo Ethernet. Las normas establecidas por el IEEE obligan a los proveedores de dispositivos Ethernet a registrarse en el IEEE. El IEEE asigna al proveedor un código de 3 bytes (24 bits), llamado "identificador único de organización (OUI)".

El IEEE requiere que un proveedor siga dos sencillas reglas, como se muestra en la ilustración:

- Todas las direcciones MAC asignadas a una NIC o a otro dispositivo Ethernet deben utilizar el OUI que se le asignó a dicho proveedor como los tres primeros bytes.
- Todas las direcciones MAC con el mismo OUI deben tener asignado un valor único en los tres últimos bytes.

Nota: es posible que existan direcciones MAC duplicadas debido a errores de fabricación o en algunos métodos de implementación de máquinas virtuales. En cualquier caso, será necesario modificar la dirección MAC con una nueva NIC o en el software

Procesamiento de tramas.

A menudo, la dirección MAC se conoce como "dirección física (BIA)" porque, históricamente, esta dirección se graba de manera física en la memoria de solo lectura (ROM) de la NIC. Es decir que la dirección está codificada en el chip de la ROM de manera permanente.

Nota: en las NIC y los sistemas operativos de PC modernos, es posible cambiar la dirección MAC en el software. Esto es útil cuando se intenta acceder a una red

filtrada por BIA. En consecuencia, el filtrado o el control de tráfico basado en la dirección MAC ya no son tan seguros.

Cuando la computadora arranca, lo primero que hace la NIC es copiar la dirección MAC de la ROM a la RAM. Cuando un dispositivo reenvía un mensaje a una red Ethernet, adjunta la información del encabezado a la trama. La información del encabezado contiene las direcciones MAC de origen y de destino.

En la animación, haga clic en Reproducir para ver el proceso de reenvío de tramas. Cuando una NIC recibe una trama de Ethernet, examina la dirección MAC de destino para ver si coincide con la dirección MAC física del dispositivo almacenada en la RAM. Si no hay coincidencia, el dispositivo descarta la trama. Si hay coincidencia, envía la trama a las capas OSI, donde ocurre el proceso de desencapsulamiento.

Nota: las NIC Ethernet también aceptan tramas si la dirección MAC de destino es un grupo de difusión o de multidifusión del cual es miembro el host.

Cualquier dispositivo que pueda ser el origen o el destino de una trama de Ethernet debe tener asignada una dirección MAC. Esto incluye estaciones de trabajo, servidores, impresoras, dispositivos móviles y routers.

Representaciones de la dirección MAC.

En un host de Windows, se puede utilizar el comando ipconfig /all para identificar la dirección MAC de un adaptador Ethernet. En la figura 1, observe que se indica en la pantalla que la dirección física (MAC) de la computadora es 00-18-DE-DD-A7-B2. Si tiene acceso, le sugerimos intentar esto en su propia computadora. En un host Mac o Linux, se utiliza el comando ipconfig.

Según el dispositivo y el sistema operativo, puede ver varias representaciones de direcciones MAC, como se muestra en la figura 2. Los routers y switches Cisco utilizan el formato XXXX.XXXX.XXXX, en el que X es un carácter hexadecimal

Dirección MAC de unidifusión.

En Ethernet, se utilizan diferentes direcciones MAC para las comunicaciones de unidifusión, difusión y multidifusión de capa 2.

Una dirección MAC de unidifusión es la dirección única utilizada cuando se envía una trama desde un único dispositivo transmisor hacia un único dispositivo receptor.

En el ejemplo de la animación, un host con la dirección IPv4 192.168.1.5 (origen) solicita una página web del servidor en la dirección IPv4 de unidifusión 192.168.1.200. Para que un paquete de unidifusión se envíe y se reciba, la

dirección IP de destino debe estar incluida en el encabezado del paquete IP. Además, el encabezado de la trama de Ethernet también debe contener una dirección MAC de destino correspondiente. Las direcciones IP y MAC se combinan para la distribución de datos a un host de destino específico.

El proceso que un host de origen utiliza para determinar la dirección MAC de destino se conoce como "protocolo de resolución de direcciones (ARP)". El ARP se analiza más adelante en este capítulo.

Aunque la dirección MAC de destino puede ser una dirección de unidifusión, difusión o multidifusión, la dirección MAC de origen siempre debe ser de unidifusión.

Dirección MAC de difusión.

Los paquetes de difusión tienen una dirección IPv4 de destino que contiene solo números uno (1) en la porción de host. Esta numeración en la dirección significa que todos los hosts de esa red local (dominio de difusión) recibirán y procesarán el paquete. Muchos protocolos de red, como DHCP y ARP, utilizan la difusión.

Como se muestra en la animación, el host de origen envía un paquete de difusión IPv4 a todos los dispositivos de la red. La dirección IPv4 de destino es una dirección de difusión: 192.168.1.255. Cuando el paquete de difusión IPv4 se encapsula en la trama de Ethernet, la dirección MAC de destino es la dirección MAC de difusión FF-FF-FF-FF-FF-FF en hexadecimal (48 números uno en binario).

Dirección MAC de multidifusión.

Las direcciones de multidifusión le permiten a un dispositivo de origen enviar un paquete a un grupo de dispositivos. Una dirección IP de grupo de multidifusión se asigna a los dispositivos que pertenecen a un grupo de multidifusión. El intervalo de direcciones IPv4 de multidifusión va de 224.0.0.0 a 239.255.255.255. El rango de direcciones de multidifusión IPv6 comienza con FF00::/8. Debido a que las direcciones de multidifusión representan un grupo de direcciones (a veces denominado "grupo de hosts"), solo se pueden utilizar como el destino de un paquete. El origen siempre tiene una dirección de unidifusión.

Las direcciones de multidifusión se pueden usar en juegos remotos, donde muchos jugadores se conectan de manera remota para jugar al mismo juego. Otro uso de las direcciones de multidifusión es el aprendizaje a distancia mediante videoconferencias, donde muchos alumnos están conectados a la misma clase.

Al igual que con las direcciones de unidifusión y de difusión, la dirección IP de multidifusión requiere una dirección MAC de multidifusión correspondiente para poder enviar tramas en una red local. La dirección de multidifusión MAC relacionada con una dirección de multidifusión IPv4 es un valor especial que comienza con 01-00-5E en formato hexadecimal. La porción restante de la dirección MAC de multidifusión se crea convirtiendo en seis caracteres

hexadecimales los 23 bits inferiores de la dirección IP del grupo de multidifusión. Para una dirección IPv6, la dirección de multidifusión MAC comienza con 33-33.

Un ejemplo, como se muestra en la animación, es la dirección hexadecimal de multidifusión 01-00-5E-00-00-C8. El último byte (u 8 bits) de la dirección IPv4 224.0.0.200 es el valor decimal 200. La forma más fácil de ver el equivalente hexadecimal es convertirlo en binario con un espacio cada 4 bits: 200 (decimal) = 1100 1000 (binario). Con la tabla de conversión que se presentó antes, podemos convertirlo en hexadecimal: 1100 1000 (binario) = 0xC8 (hexadecimal).

Tabla de direcciones MAC.

Nociones básicas de switches.

Un switch Ethernet de capa 2 utiliza direcciones MAC para tomar decisiones de reenvío. Desconoce por completo qué protocolo se transmite en la porción de datos de la trama, como un paquete IPv4. El switch toma decisiones de reenvío solamente según las direcciones MAC Ethernet de capa 2.

A diferencia de los hubs Ethernet antiguos, que repiten los bits por todos los puertos excepto el de entrada, un switch Ethernet consulta una tabla de direcciones MAC para tomar una decisión de reenvío para cada trama. En la ilustración, se acaba de encender el switch de cuatro puertos. Todavía no conoce las direcciones MAC de las cuatro PC conectadas.

Nota: a veces, la tabla de direcciones MAC se conoce como “tabla de memoria de contenido direccionable (CAM)”. Aunque el término “tabla CAM” es bastante común, en este curso nos referiremos a ella como “tabla de direcciones MAC”.

Tabla de direcciones MAC.

Nociones básicas de switches.

Un switch Ethernet de capa 2 utiliza direcciones MAC para tomar decisiones de reenvío. Desconoce por completo qué protocolo se transmite en la porción de datos de la trama, como un paquete IPv4. El switch toma decisiones de reenvío solamente según las direcciones MAC Ethernet de capa 2.

A diferencia de los hubs Ethernet antiguos, que repiten los bits por todos los puertos excepto el de entrada, un switch Ethernet consulta una tabla de direcciones MAC para tomar una decisión de reenvío para cada trama. En la ilustración, se acaba de encender el switch de cuatro puertos. Todavía no conoce las direcciones MAC de las cuatro PC conectadas.

Nota: a veces, la tabla de direcciones MAC se conoce como “tabla de memoria de contenido direccionable (CAM)”. Aunque el término “tabla CAM” es bastante común, en este curso nos referiremos a ella como “tabla de direcciones MAC”.

Obtención de direcciones MAC.

El switch arma la tabla de direcciones MAC de manera dinámica después de examinar la dirección MAC de origen de las tramas recibidas en un puerto. El switch reenvía las tramas después de buscar una coincidencia entre la dirección MAC de destino de la trama y una entrada de la tabla de direcciones MAC.

El siguiente proceso se realiza para cada trama de Ethernet que ingresa a un switch.

Aprendizaje: Examinar la dirección MAC de origen

Se revisa cada trama que ingresa a un switch para obtener información nueva. Esto se realiza examinando la dirección MAC de origen de la trama y el número de puerto por el que ingresó al switch.

- Si la dirección MAC de origen no existe, se la agrega a la tabla, junto con el número de puerto de entrada. En la figura 1, la PC-A está enviando una trama de Ethernet a la PC-D. El switch agrega a la tabla la dirección MAC de la PC-A.
- Si la dirección MAC de origen existe, el switch actualiza el temporizador de actualización para esa entrada. De manera predeterminada, la mayoría de los switches Ethernet guardan una entrada en la tabla durante cinco minutos

Nota: si la dirección MAC de origen existe en la tabla, pero en un puerto diferente, el switch la trata como una entrada nueva. La entrada se reemplaza con la misma dirección MAC, pero con el número de puerto más actual.

Reenvío: Examinar la dirección MAC de destino

A continuación, si la dirección MAC de destino es una dirección de unidifusión, el switch busca una coincidencia entre la dirección MAC de destino de la trama y una entrada de la tabla de direcciones MAC.

- Si la dirección MAC de destino está en la tabla, reenvía la trama por el puerto especificado.
- Si la dirección MAC de destino no está en la tabla, el switch reenvía la trama por todos los puertos, excepto el de entrada. Esto se conoce como “unidifusión desconocida”. Como se muestra en la figura 2, el switch no tiene la dirección MAC de destino de la PC-D en la tabla, por lo que envía la trama por todos los puertos, excepto el 1.

Nota: si la dirección MAC de destino es de difusión o de multidifusión, la trama también se envía por todos los puertos, excepto el de entrada

Filtrado de tramas.

A medida que un switch recibe tramas de diferentes dispositivos, puede completar la tabla de direcciones MAC examinando la dirección MAC de cada trama. Cuando la tabla de direcciones MAC del switch contiene la dirección MAC de destino, puede filtrar la trama y reenviarla por un solo puerto.

En las figuras 1 y 2, se muestra la PC-D enviando una trama de regreso a la PC-A. En primer lugar, el switch obtiene la dirección MAC de la PC-D. A continuación, como la dirección MAC de la PC-A está en la tabla del switch, este envía la trama solamente por el puerto 1.

En la figura 3, se muestra la PC-A enviando otra trama a la PC-D. La tabla de direcciones MAC ya contiene la dirección MAC de la PC-A, por lo que se restablece el temporizador de actualización para esa entrada. A continuación, como la dirección MAC de la PC-D está en la tabla del switch, este envía la trama solamente por el puerto 4.

.

Métodos de reenvío del switch.

Métodos de reenvío de tramas de los switches Cisco.

Los switches utilizan uno de los siguientes métodos de reenvío para el switching de datos entre puertos de la red

- Switching de almacenamiento y envío
- Switching por método de corte

En la figura 1, se resaltan las diferencias entre estos dos métodos.

En este tipo de switching, cuando el switch recibe la trama, la almacena en los búferes de datos hasta recibir la trama en su totalidad. Durante el proceso de almacenamiento, el switch analiza la trama para buscar información acerca de su destino. En este proceso, el switch también lleva a cabo una verificación de errores utilizando la porción del tráiler de comprobación de redundancia cíclica (CRC) de la trama de Ethernet.

La CRC utiliza una fórmula matemática basada en la cantidad de bits (números uno) de la trama para determinar si esta tiene algún error. Después de confirmar la integridad de la trama, se la reenvía por el puerto apropiado hacia su destino. Cuando se detecta un error en la trama, el switch la descarta. El proceso de descarte de las tramas con errores reduce el ancho de banda consumido por datos dañados. El switching de almacenamiento y envío se requiere para el análisis de calidad de servicio (QoS) en las redes convergentes, donde se necesita una clasificación de la trama para decidir el orden de prioridad del tráfico. Por ejemplo, los flujos de datos de voz sobre IP deben tener prioridad sobre el tráfico de navegación web.

Haga clic aquí para obtener más información sobre el switching de almacenamiento de envío y por método de corte.

Switching por método de corte.

En este tipo de switching, el switch actúa sobre los datos apenas los recibe, incluso si la transmisión aún no se completó. El switch reúne en el búfer solo la información suficiente de la trama como para leer la dirección MAC de destino y determinar a qué puerto debe reenviar los datos. La dirección MAC de destino se encuentra en los primeros 6 bytes de la trama después del preámbulo. El switch busca la dirección MAC de destino en la tabla de switching, determina el puerto de la interfaz de salida y reenvía la trama a su destino mediante el puerto de switch designado. El switch no lleva a cabo ninguna verificación de errores en la trama.

A continuación, se presentan dos variantes del switching por método de corte:

- **Switching de reenvío rápido:** este método ofrece el nivel de latencia más bajo. El switching de envío rápido reenvía el paquete inmediatamente

después de leer la dirección de destino. Como el switching de reenvío rápido comienza a reenviar el paquete antes de recibirlo por completo, es posible que, a veces, los paquetes se distribuyan con errores. Esto no sucede frecuentemente, y el adaptador de red de destino descarta el paquete defectuoso al recibirlo. En el modo de reenvío rápido, la latencia se mide desde el primer bit recibido hasta el primer bit transmitido. El switching de envío rápido es el método de corte típico.

- **Switching libre de fragmentos:** en este método, el switch almacena los primeros 64 bytes de la trama antes de reenviarla. El switching libre de fragmentos se puede ver como un punto medio entre el switching de almacenamiento y envío, y el switching por método de corte. El motivo por el que el switching libre de fragmentos almacena solamente los primeros 64 bytes de la trama es que la mayoría de los errores y las colisiones de la red se producen en esos primeros 64 bytes. El switching libre de fragmentos intenta mejorar el switching de reenvío rápido al realizar una pequeña verificación de errores en los 64 bytes de la trama para asegurar que no haya ocurrido una colisión antes de reenviarla. Este método de switching es un punto medio entre la alta latencia y la alta integridad del switching de almacenamiento y envío, y la baja latencia y la baja integridad del switching de reenvío rápido.

Algunos switches están configurados para realizar el switching por método de corte en cada puerto hasta alcanzar un umbral de errores definido por el usuario y, luego, cambiar automáticamente al switching de almacenamiento y envío. Si el índice de error está por debajo del umbral, el puerto vuelve automáticamente al switching por método de corte.

Almacenamiento en búfer de memoria en los switches.

Un switch Ethernet puede usar una técnica de almacenamiento en búfer para almacenar tramas antes de enviarlas. El almacenamiento en búfer también se puede utilizar cuando el puerto de destino está ocupado debido a una congestión. En este caso, el switch almacena la trama hasta que se pueda transmitir.

Como se muestra en la ilustración, existen dos métodos de almacenamiento en búfer de memoria: memoria basada en puerto y memoria compartida.

Búfer de memoria basada en puerto

En el búfer de memoria basada en puerto, las tramas se almacenan en colas conectadas a puertos de entrada y de salida específicos. Una trama se transmite al puerto de salida una vez que todas las que están delante de ella en la cola se hayan transmitido correctamente. Es posible que una sola trama demore la transmisión de todas las tramas almacenadas en la memoria debido al tráfico del puerto de destino. Esta demora se produce aunque las demás tramas se puedan transmitir a puertos de destino abiertos.

Búfer de memoria compartida

El búfer de memoria compartida deposita todas las tramas en un búfer de memoria común que comparten todos los puertos del switch. La cantidad de memoria de búfer que requiere un puerto se asigna de forma dinámica. Las tramas que están en el búfer se enlazan de forma dinámica al puerto de destino. Esto permite que se pueda recibir el paquete por un puerto y que se pueda transmitir por otro, sin necesidad de colocarlo en otra cola.

El switch conserva un mapa de enlaces de trama a puerto que indica adónde debe transmitirse el paquete. El enlace se elimina del mapa una vez que la trama se transmite correctamente. La cantidad de tramas almacenadas en el búfer está limitada por el tamaño del búfer de memoria en su totalidad y no se limita a un solo búfer de puerto. Esto permite que se transmitan tramas más grandes y que se descarte una menor cantidad de ellas. Esto es de especial importancia para el switching asimétrico. El switching asimétrico permite diferentes índices de datos en diferentes puertos. Esto permite dedicar un mayor ancho de banda a ciertos puertos, como a un puerto conectado a un servidor.

Configuración del puerto de switch.

Configuración de dúplex y velocidad.

Dos de los parámetros más básicos de un switch son el ancho de banda y los parámetros de dúplex para cada puerto de switch individual. Es fundamental que los parámetros de dúplex y de ancho de banda coincidan entre el puerto de switch y los dispositivos conectados, como una computadora u otro switch.

Existen dos tipos de parámetros de dúplex utilizados para las comunicaciones en una red Ethernet: dúplex medio y dúplex completo.

- **Dúplex completo:** ambos extremos de la conexión pueden enviar y recibir datos simultáneamente.
- **Dúplex medio:** solo uno de los extremos de la conexión puede enviar datos por vez.

La autonegociación es una función optativa que se encuentra en la mayoría de los switches Ethernet y NIC, que permite que dos dispositivos intercambien automáticamente información sobre velocidad y funcionalidades de dúplex. El switch y el dispositivo conectado seleccionan el modo de mayor rendimiento. Si ambos dispositivos tienen la funcionalidad, se selecciona dúplex completo, junto con el ancho de banda común más alto.

Por ejemplo, en la figura 1, la NIC Ethernet de la PC-A puede funcionar en dúplex completo o en dúplex medio, y a 10 Mb/s o 100 Mb/s. La PC-A está conectada al switch S1 en el puerto 1, que puede funcionar en dúplex completo o en dúplex medio, y a 10 Mb/s, 100 Mb/s o 1000 Mb/s (1 Gb/s). Si ambos dispositivos utilizan la autonegociación, el modo de funcionamiento será en dúplex completo y a 100 Mb/s.

Nota: de manera predeterminada, la mayoría de los switches Cisco y NIC Ethernet utilizan la autonegociación para la configuración de velocidad y dúplex. Los puertos Gigabit Ethernet solamente funcionan en dúplex completo.

Incompatibilidad de dúplex

Una de las causas más comunes de problemas de rendimiento en enlaces Ethernet de 10 o 100 Mb/s ocurre cuando un puerto del enlace funciona en dúplex medio, mientras el otro puerto funciona en dúplex completo, como se muestra en la figura 2. Esto sucede cuando uno o ambos puertos de un enlace se restablecen, y el proceso de autonegociación no configura ambos participantes del enlace de la misma manera. También puede ocurrir cuando los usuarios reconfiguran un lado

del enlace y olvidan reconfigurar el otro. Ambos lados de un enlace deben tener activada la autonegociación, o bien ambos deben tenerla desactivada.

MDIX automática.

Además de tener la configuración de dúplex correcta, también es necesario tener definido el tipo de cable correcto para cada puerto. Anteriormente, las conexiones entre dispositivos específicos, como switch a switch, switch a router, switch a host y router a host, requerían el uso de tipos de cable específicos (cruzado o directo). En la actualidad, la mayoría de los dispositivos de switch permiten que el comando mdix auto interface configuration en la CLI active la función de interfaz cruzada dependiente del medio (MDIX) automática.

Cuando se activa la función de MDIX automática, el switch detecta el tipo de cable conectado al puerto y configura las interfaces de manera adecuada. Por lo tanto, se puede utilizar un cable directo o cruzado para realizar la conexión con un puerto 10/100/1000 de cobre situado en el switch, independientemente del tipo de dispositivo que esté en el otro extremo de la conexión.

Nota: de manera predeterminada, la función MDIX automática se activa en los switches con el software Cisco IOS versión 12.2(18)SE o posterior.

MAC e IP.

Destino en la misma red.

Hay dos direcciones primarias asignadas a un dispositivo en una LAN Ethernet:

- **Dirección física (dirección MAC):** se utiliza para comunicaciones de NIC Ethernet a NIC Ethernet en la misma red.
- **Dirección lógica (dirección IP):** se utiliza para enviar el paquete del origen inicial al destino final.

Las direcciones IP se utilizan para identificar la dirección del origen inicial y del destino final. La dirección IP de destino puede estar en la misma red IP que la de origen o en una red remota.

Nota: la mayoría de las aplicaciones utilizan el sistema de nombres de dominio (DNS) para determinar la dirección IP cuando se les indica un nombre de dominio, como “www.cisco.com”. El DNS se analiza en detalle en otro capítulo.

Las direcciones de capa 2, o físicas, como las direcciones MAC Ethernet, tienen un propósito diferente: se utilizan para distribuir la trama de enlace de datos con el paquete IP encapsulado de una NIC a otra en la misma red. Si la dirección IP de

destino está en la misma red, la dirección MAC de destino es la del dispositivo de destino.

En la ilustración, se muestran las direcciones MAC Ethernet y la dirección IP de la PC-A enviando un paquete IP al servidor de archivos en la misma red.

La trama de Ethernet de capa 2 contiene lo siguiente:

- Dirección MAC de destino: es la dirección MAC de la NIC Ethernet del servidor de archivos.
- **Dirección MAC de origen:** es la dirección MAC de la NIC Ethernet de la PC-A.

El paquete IP de capa 3 contiene lo siguiente:

- **Dirección IP de origen:** es la dirección IP del origen inicial, la PC-A.
- **Dirección IP de destino:** es la dirección IP del destino final, el servidor de archivos.

Red remota de destino.

Cuando la dirección IP de destino está en una red remota, la dirección MAC de destino es la dirección del gateway predeterminado del host (la NIC del router) como se muestra en la ilustración. Si utilizamos una analogía de correo postal, esto sería similar a cuando una persona lleva una carta a la oficina postal local. Todo lo que debe hacer es llevar la carta a la oficina postal. A partir de ese momento, se vuelve responsabilidad de la oficina postal reenviar la carta al destino final.

En la ilustración, se muestran las direcciones MAC Ethernet y las direcciones IPv4 de la PC-A enviando un paquete IP al servidor web en una red remota. Los routers examinan la dirección IPv4 de destino para determinar la mejor ruta para reenviar el paquete IPv4. Esto es similar a la manera en que el servicio postal reenvía el correo según la dirección del destinatario.

Cuando el router recibe una trama de Ethernet, desencapsula la información de capa 2. Por medio de la dirección IP de destino, determina el dispositivo del siguiente salto y desencapsula el paquete IP en una nueva trama de enlace de datos para la interfaz de salida. Junto con cada enlace en una ruta, se encapsula un paquete IP en una trama específica para la tecnología de enlace de datos particular relacionada con ese enlace, como Ethernet. Si el dispositivo del siguiente salto es el destino final, la dirección MAC de destino es la de la NIC Ethernet del dispositivo.

¿Cómo se asocian las direcciones IPv4 de los paquetes IPv4 en un flujo de datos con las direcciones MAC en cada enlace a lo largo de la ruta hacia el destino? Esto se realiza mediante un proceso llamado “protocolo de resolución de direcciones (ARP)”.

ARP.

Introducción ARP.

Recuerde que cada dispositivo que tiene una dirección IP en una red Ethernet también tiene una dirección MAC Ethernet. Cuando un dispositivo envía una trama de Ethernet, esta contiene estas dos direcciones:

- **Dirección MAC de destino:** la dirección MAC de la NIC Ethernet, que es la dirección del destino final o del router.
- **Dirección MAC de origen:** la dirección MAC de la NIC Ethernet del remitente.

Para determinar la dirección MAC de destino, el dispositivo utiliza ARP. ARP proporciona dos funciones básicas:

- Resolución de direcciones IPv4 a direcciones MAC
- Mantenimiento de una tabla de asignaciones

Funciones del ARP.

Resolución de direcciones IPv4 a direcciones MAC

Cuando se envía un paquete a la capa de enlace de datos para encapsularlo en una trama de Ethernet, el dispositivo consulta una tabla en su memoria para encontrar la dirección MAC que está asignada a la dirección IPv4. Esta tabla se denomina "tabla ARP" o "caché ARP". La tabla ARP se almacena en la RAM del dispositivo.

El dispositivo emisor busca en su tabla ARP la dirección IPv4 de destino y la dirección MAC correspondiente.

Si la dirección IPv4 de destino del paquete está en la misma red que la dirección IPv4 de origen, el dispositivo busca la dirección IPv4 de destino en la tabla ARP.

Si la dirección IPv4 de destino está en una red diferente que la dirección IPv4 de origen, el dispositivo busca la dirección IPv4 del gateway predeterminado.

En ambos casos, se realiza una búsqueda de la dirección IPv4 y la dirección MAC correspondiente para el dispositivo.

En cada entrada o fila de la tabla ARP, se enlaza una dirección IPv4 con una dirección MAC. Llamamos "asignación" a la relación entre dos valores; simplemente, se refiere a que puede localizar una dirección IPv4 en la tabla y averiguar la dirección MAC correspondiente. La tabla ARP almacena temporalmente (en caché) la asignación para los dispositivos de la LAN.

Si el dispositivo localiza la dirección IPv4, se utiliza la dirección MAC correspondiente como la dirección MAC de destino de la trama. Si no se encuentra ninguna entrada, el dispositivo envía una solicitud de ARP.

Eliminación de entradas de una tabla ARP.

Para cada dispositivo, un temporizador de memoria caché ARP elimina las entradas de ARP que no se hayan utilizado durante un período especificado. El temporizador varía según el sistema operativo del dispositivo. Por ejemplo, algunos sistemas operativos Windows almacenan entradas de ARP en la memoria caché durante dos minutos, como se muestra en la ilustración.

También se pueden utilizar comandos para eliminar de manera manual todas las entradas de la tabla ARP o algunas de ellas. Después de eliminar una entrada, el proceso de envío de una solicitud de ARP y de recepción de una respuesta de ARP debe ocurrir nuevamente para que se introduzca la asignación en la tabla ARP.

Problemas de ARP.

Difusiones ARP.

Todos los dispositivos de la red local reciben y procesan una solicitud de ARP debido a que es una trama de difusión. En una red comercial típica, estas difusiones tendrían, probablemente, un efecto mínimo en el rendimiento de la red. Sin embargo, si se encendiera una gran cantidad de dispositivos que comenzaran a acceder a los servicios de red al mismo tiempo, el rendimiento podría disminuir durante un breve período, como se muestra en la ilustración. Después de que los dispositivos envían las difusiones ARP iniciales y obtienen las direcciones MAC necesarias, se minimiza cualquier efecto en la red.

Suplantación de ARP.

En algunos casos, el uso de ARP puede ocasionar un riesgo de seguridad potencial conocido como “suplantación de ARP” o “envenenamiento ARP”. Esta es una técnica utilizada por un atacante para responder a una solicitud de ARP de una dirección IPv4 que pertenece a otro dispositivo, como el gateway predeterminado, como se muestra en la ilustración. El atacante envía una respuesta de ARP con su propia dirección MAC. El receptor de la respuesta de ARP agrega la dirección MAC incorrecta a la tabla ARP y envía estos paquetes al atacante.

Los switches de nivel empresarial incluyen técnicas de mitigación conocidas como “inspección dinámica de ARP (DAI)”. La DAI excede el ámbito de este curso.