Capa de Enlace

La capa de enlace de datos tiene la responsabilidad de transferir datagramas desde un nodo al nodo adyacente a través de un enlace.

El paquete de capa 2 es un frame o trama, encapsula un datagrama (de capa de red).

Enlace - Terminología

Los datagramas son transferidos por diferentes protocolos de enlace en diferentes enlaces:

- Por ejemplo: Ethernet en primer enlace, Frame Relay (para redes de Circuitos Virtuales) en enlaces intermedios, 802.11 (WiFi) en último enlace.

Cada protocolo de enlace provee servicios diferentes:

- Por ejemplo: puede o no proveer transferencia confiable sobre el enlace.

Enlace - Servicios 1/2

Los siguientes servicios son provisto por la capa de enlace, aunque por lo general y dependiendo de la tecnología con la que opera algunos de ellos no se implementan.

Entramado:

- Encapsula el datagrama en trama, agregando encabezados y acoplados (header & trailer): Le agrega un encabezado con información necesaria como otras capas, pero también un acoplado con información de seguridad como un código CRC.

- Acceso al medio si se trata de un acceso compartido: si el medio es compartido como el aire, hay que utilizar políticas para el uso y para los posibles problemas de interferencias o errores por colisión.

- Dirección “MAC” usada en encabezados de tramas para identificar fuente y destino: utiliza direcciones para los casos de redes de difusión. Las más famosas son las direcciones MAC de Ethernet.

Entrega confiable entre nodos adyacentes:

- Se implementa mediante reconocimientos y retransmisiones
- Raramente usado en enlaces de bajo error de bits (como fibra, algunos pares de cobre trenzados)
- Enlaces inalámbricos: alta tasa de errores

Control de flujo:

- Para evitar que el nodo emisor abrume al nodo receptor

Enlace - Servicios 2/2

Detección de errores:

- Errores causados por atenuación de señal y ruido.
- Receptor detecta presencia de errores:
  - El nodo transmisor agrega bits de detección de errores a la trama y el nodo receptor realiza una comprobación de errores.
  - La detección se implementa por Hardware.
  - Si se detecta un error, se le pide al transmisor: retransmisión o descartar la trama

Corrección de errores:

- Receptor identifica y corrige error(es) de bit(s) sin solicitar retransmisión
- Half-duplex and full-duplex
  - Con la transmisión full-duplex, los nodos de ambos extremos de un enlace pueden transmitir paquetes al mismo tiempo.
  - Con la transmisión semiduplex un mismo nodo no puede transmitir y recibir al mismo tiempo

Enlace - Adaptadores

La capa de enlace es implementada en un adaptador (NIC)

- Tarjetas Ethernet, PCMCI, o Wifi

Lado transmisor

- Encapsula el datagrama en una trama
- Agrega bits de chequeo de errores, control de flujo, etc

Lado receptor

- Busca errores, control de flujo, etc.
- Extrae el datagrama y lo pasa al nodo receptor

El adaptador es semi-autónomo, ya que la funcionalidad principal del protocolo de esta capa está implementada en el driver del adaptador: control de errores y de flujo, recepción de la trama desde la red, etc.

Enlace – Tipos de acceso

Dos tipos de enlaces

Punto-a-apunto

- PPP para acceso discado
- Enlaces punto-a-punto entre switch Ethernet y host (computador)

Difusión (broadcast - cable o medio compartido)

- Ethernet tradicional
- Flujo de subida en HFC (Hybrid Fiber Coax)
- 802.11 WiFi

Direcciones MAC

Dirección MAC (o LAN o física o Ethernet):

- No son los nodos (es decir, los hosts o routers) los que tienen asignadas direcciones de la capa de enlace, sino que las direcciones de la capa de enlace se asignan a los adaptadores instalados en cada nodo. Es decir, cada placa de red.

- Son usadas para conducir un datagrama a otra interfaz físicamente conectada (en la misma red)

- Son de 48 bits (en mayoría de LANs) están grabadas en una ROM de la tarjeta adaptadora .

- Nunca puede haber dos adaptadores con la misma dirección.

- IEEE se encarga de gestionar el espacio de direcciones MAC; y cuando una empresa quiere fabricar adaptadores de red, compra por un precio fijado una parte del espacio de direcciones.

MACs en la red

las direcciones MACs son únicas en la red y únicas en el mundo.

Hay una dirección particular que es la dirección de broadcast o difusión que hace referencia a todas las placas de la red.

FF:FF:FF:FF:FF:FF:FF

Cuando un adaptador de un emisor quiere enviar una trama a otro adaptador de destino, inserta la dirección MAC del destino en la trama y luego la envía a través de la red LAN.

Si la red LAN es una LAN de difusión (como por ejemplo, 802.11 o Ethernet), la trama será recibida y procesada por todos los demás adaptadores de la LAN.

Cada adaptador que reciba la trama comprobará si la dirección MAC de destino contenida en la trama se corresponde con su propia dirección MAC.

- Si corresponde, el adaptador extraerá el datagrama incluido en la trama y lo pasará hacia arriba por la pila de protocolos

- Si no corresponde, el adaptador descarta la trama, sin pasar el datagrama de la capa de red hacia arriba por la pila de protocolos.

- De este modo, sólo el nodo de destino será interrumpido cuando se reciba la trama.

ARP – Address Resolution Protocol

Cuando se quiere establecer una comunicación, por lo general se utiliza un nombre que mediante resolución (local o DNS) se traduce en una dirección IP.

En una red de difusión que posee direcciones físicas es muy complicado conocer a todos los dispositivos conectados. Entonces cómo averiguar las direcciones físicas conociendo una IP.

Cada nodo IP (host o router) de la LAN tiene una tabla ARP

Tabla ARP: mapean direcciones IP/MAC para algunos nodos de la LAN

```
---------------------------------
| IP address | MAC address | TTL |
---------------------------------
```

TTL (time to live): tiempo de expiración para el mapeo (típicamente 20').

ARP resuelve direcciones IP sólo para los nodos de una misma subred.

Funcionamiento:

Si el nodo 237.196.7.78 quiere enviar un datagrama a otro nodo en la subred, entonces necesita obtener la dirección MAC correspondiente a la dirección IP, del nodo destino

- Si el emisor tiene una entrada en su tabla ART una entrada para la dirección IP del nodo destino, puede enviar el datagrama.

- Si el emisor no tiene una entrada, entonces debe enviar un paquete ARP, incluyendo las direcciones MAC e IP del emisor y el receptor, a la dirección de difusión MAC, FF-FF-FF-FF-FF-FF.

- La trama que contiene la consulta ARP es recibida por todos los demás adaptadores existentes en la subred.

- Cada nodo comprueba si su dirección IP corresponde a la dirección IP de destino del paquete ARP.

- El único nodo en el que se produzca la coincidencia devolverá al nodo que ha realizado la consulta una respuesta ARP con la correspondencia deseada.

- Ahora el emisor podrá actualizar su tabla ARP y enviar su datagrama IP

Ruteo a otra LAN

Si el nodo destino se encuentra en otra subred, entonces ejecuta el ARP pero con la IP del gateway.

Una vez que averigua la MAC del router, le manda el datagrama la router. La dirección MAC destino será la del router, la MAC origen la del nodo emisor, la IP destino será la del nodo receptor y la IP origen la del nodo emisor.

El datagrama llega al router donde se analiza la IP destino, como no coincide con alguna del router, el paquete necesita ser reenviado.

Supongamos que el router está conectado a otra subred ethernet y el nodo destino se encuentra allí.

Para hacer la entrega el router debe ejecutar el ARP para averiguar la MAC del destino y poder entregar el datagrama.

Cuando averigua la MAC destino arma un paquete con la MAC destino que es la del destino, su propia MAC como origen, la IP del destino y la IP del nodo origen (ojo, no del router porque no es quién se quiere comunicar con el destino).

Siguiendo el ejemplo:

- A crea datagrama con IP fuente A y IP destino B
- A usa ARP para obtener la MAC de R para la interfaz 111.111.111.110
- A crea una trama enlace de datos con dirección MAC de R como destino y su MAC como origen. Los datos de la trama contienen el datagrama IP de A a B
- El adaptador de A envía la trama
- El adaptador de R recibe la trama
- R saca el datagrama IP de la trama Ethernet, y ve que el destino es B
- R usa ARP para obtener la dirección MAC de B
- R crea la trama con dirección MAC destino B, dirección MAC origen R de la interface 222.222.222.220, incluye el datagrama IP de A para B; y lo envía a B

Ethernet

Es un estándar de redes de área local para computadores, por sus siglas en español Acceso Múltiple con Escucha de Portadora y Detección de Colisiones (CSMA/CD).

Su nombre procede del concepto físico de éter (ether, en inglés). Ethernet define las características de cableado y señalización; de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI.

Ethernet se tomó como base para la redacción del estándar internacional IEEE 802.3, siendo usualmente tomados como sinónimos. Se diferencian en uno de los campos de la trama de datos. Sin embargo, las tramas Ethernet e IEEE 802.3 pueden coexistir en la misma zona.

Si bien IEEE 802.3 y Ethernet son similares, las diferencias entre ellos son sutiles.

Todas las versiones de Ethernet son similares en la arquitectura de acceso al medio múltiple con detección de errores, CSMA/CD. Sin embargo, el estándar IEEE 802.3 ahora soporta múltiples medios en la capa física.

Ethernet proporciona servicios correspondientes a las capas 1 y 2 del modelo OSI.

IEEE 802.3 especifica la capa física (Capa 1) y la parte de acceso-canal de la capa de enlace (Capa 2), pero no define un protocolo de control de enlace lógico.

Otras diferencias son: la velocidad de transmisión, el método de señalamiento y la longitud máxima del cableado.

Tecnología LAN cableada “dominante” :

- Barata!
- Más simple y barata que LANs con token ring (desarrollada por IBM en los años 1970 con topología física en anillo y técnica de acceso de paso de testigo) y ATM (Modo de Transferencia Asíncrona- ofrece un servicio orientado a conexión)
- Avanza en velocidad: 10 Mbps – 10 Gbps

Servicios:

- Sin conexión: No hay handshaking entre adaptadores.

- No confiable: Receptor no envía acks o nacks al adaptador transmisor

- Flujo de datagramas pasado a la capa de red puede tener vacíos

- Los vacíos son llenados si la aplicación está usando TCP (ya que el host B no confirmará los datos contenidos en las tramas descartadas, obligando a TCP en el host A a realizar retransmisiones).

- De otra manera, si falta algún fragmento, IP no podrá reensamblar el datagrama y lo descarta. Si la ausencia es de un datagrama completo la aplicación notará el vacío.

Ethernet - 10base5

Las LAN 10Base5 están compuestas por los siguientes componentes de hardware:

- Un cable coaxial grueso que no exceda de 500 metros de longitud total
- Dos resistencias terminadoras para proporcionar terminación eléctrica a cada extremo del coaxial
- Transceptores de tipo "tap" para conectar dispositivos al cable grueso con el espaciado prescrito
- Un cable AUI para conectar la Tarjeta de Interfaz de Red desde el dispositivo al transceptor
- Tarjetas de Interfaz de Red 10Base5 para cada dispositivo de la red

Ethernet - 10base2

Las LAN 10Base2 están compuestas por los componentes de hardware siguientes:

- Una cable coaxial delgado cuya longitud no supere los 200 metros
- Dos resistencias terminadoras que proporcionan terminación eléctrica a cada extremo del cable coaxial
- Conectores "T" para interrumpir el coaxial e insertar una conexión para cada dispositivo con los espacios adecuados
- Tarjetas de Interfaz de Red 10Base2 para cada dispositivo

Ethernet - 10baseT

Las LAN 10BaseT se componen del hardware siguiente:

- Un Concentrador de Cableado
- Un cable de Par Trenzado No Apantallado (UTP) de 4 conductores, con una longitud máxima de 100 metros, para conectar la Tarjeta de Interfaz de Red del dispositivo al Concentrador

- Tarjetas de Interfaz de Red 10BaseT para cada dispositivo

Ethernet – 100base(x) y 1000base(x)

Hay variantes en cuanto a las velocidades pero sobre cables de par trenzado y fibra óptica.

Topología estrella

En los 90 la mayoría de las redes LAN habían sido reemplazadas por LANs Ethernet, utilizando topología estrella basada en concentradores: hubs o switchs

Los hosts (y los routers) están directamente conectados a un concentrador mediante un cable de cobre de par trenzado.

Hub:

Es un dispositivo de la capa física que actúa sobre los bits individuales en lugar de sobre las tramas.

Cuando un hub recibe un bit en una de sus interfaces, envía una copia al resto de sus interfaces.

Si un hub recibe tramas procedentes de dos interfaces distintas al mismo tiempo, se produce una colisión y los nodos que crean las tramas tendrán que retransmitirlas.

Cabe aclarar que el hub no tiene inteligencia alguna, solo recibe una señal eléctrica por un puerto, la realza y la emite por el resto de los puertos.

Si dos o más host transmiten a la vez, sus señales se interfieren entre sí porque el hub crea un solo dominio de colisión

Switch:

A principios de la década de 2000 Ethernet experimentó una cambio evolutivo aún mayor.

Las instalaciones Ethernet continuaron utilizando una topología en estrella, pero el concentrador central fue reemplazado por un conmutador (switch).

Un switch no es sólo un dispositivo sin colisiones, sino que también lleva a cabo la conmutación de paquetes mediante un almacenamiento y reenvío.

A diferencia de los routers, que operan hasta la capa 3, un switch opera sólo hasta la capa 2.

Según el switch va recibiendo tramas se van creando entradas en la tabla donde se asocia a un puerto una dirección MAC. Cuando se inicia un switch su tabla de direcciones MAC está vacía.

Cuando un equipo envía una trama a otro, el switch sabe por que puerto ha recibido la trama. Además, el switch obtiene la dirección MAC del equipo origen analizando la trama y crea una entrada en la tabla de direcciones MAC con la tupla (puerto, dirección MAC). Al no saber desde que puerto se puede llegar hasta la dirección MAC destino, el switch envía la trama a todos los demás puertos, menos al puerto por donde recibió la trama (ver la figura, donde el PC1 envía una trama y la tabla de direcciones MAC está vacía).

Cuando el equipo destino de la trama responde con otra trama, el switch obtiene la dirección MAC origen de la trama respuesta e inserta en la tabla de direcciones MAC la tupla correspondiente al puerto y dirección MAC origen. Desde este momento y debido a que el switch ahora conoce a que puerto está conectado el equipo destino de la trama y sólo la envía por ese puerto, los equipos origen y destino pueden tener una comunicación punto a punto, sin que otros equipos puedan visualizar su tráfico o provocar colisiones entre ellos.

Cuando el equipo emisor y receptor detienen su comunicación por cierto tiempo, el switch puede borrar sus entradas de la tabla de direcciones, para tener luego que registrarlos cuando se comuniquen nuevamente y tener siempre actualizada su tabla. Esto garantiza el normal funcionamiento ante cambios constantes de los equipos de red.

Un equipo conectado directamente a un puerto de un switch provoca que el switch almacene su dirección MAC. En el caso de conectar dos switchs o un switch y un hub, cada switch aprenderá las direcciones MAC de los dispositivos accesibles por sus puertos, por lo tanto en el puerto de interconexión se almacenan las MAC de los dispositivos conectados al otro hub o switch.

A diferencia de un hub, un switch aísla las colisiones existentes en un segmento de red creando diferentes dominios de colisión.

Estructura de la Trama

- Campos Preámbulo y Delimitador de inicio de trama Los campos Preámbulo (7 bytes) y Delimitador de inicio de trama (SFD) (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 El campo Dirección MAC de destino (6 bytes) es el identificador del receptor deseado. La dirección de la trama se compara con la dirección MAC del dispositivo. Si coinciden, el dispositivo acepta la trama.

- Campo Dirección MAC de origen El campo Dirección MAC de origen (6 bytes) identifica la NIC o interfaz de origen de la trama.

- Campo Longitud/tipo Para todos los estándares IEEE 802.3 anteriores a 1997,.el campo Longitud define la longitud exacta del campo de datos de la trama. Esto se utiliza posteriormente como parte de la FCS para garantizar que el mensaje se reciba adecuadamente. Si el objetivo de un campo es designar un tipo como en Ethernet II, el campo Tipo describe cuál es el protocolo que se implementa.

- Campos Datos y Pad. Los campos Datos y Pad (de 46 a 1500 bytes) contienen los datos encapsulados de una capa superior, que es una PDU de Capa 3 genérica o, con mayor frecuencia, un paquete IPv4. Todas las tramas deben tener al menos 64 bytes de longitud. Si se encapsula un paquete pequeño, el Pad se utiliza para incrementar el tamaño de la trama hasta alcanzar el 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.

Switchs vs Routers

Ambos son dispositivos de almacenamiento y reenvío pero operan en capas diferentes.

El router opera en capa 3, capa de red, ya que su principal función es el ruteo y forwarding de paquetes. Para cumplir estas funciones utiliza las direcciones IP.

El switch es un dispositivo de capa 2, capa de enlace, ya que trabaja con direcciones MACs.

Cabe aclarar que en la actualidad hay switchs de capa 3 que implementan funciones de capa de red. Sin embargo a fines educativos vamos a quedarnos con la función principal que es en capa de enlace.

Ambos dispositivos implementan todas las capas del modelo TCP/IP ya que necesitan aplicaciones para su configuración, administración y monitoreo. Pueden ser accedidos en forma remota. Pero nos interesan hasta la capa que implementan según sus funciones principales.

Preguntas de Repaso

- ¿A quién le provee servicios la capa de Enlace?
- ¿Las direcciones MACs son únicas en la red local pero se pueden repetir en el resto de internet?

- ¿Porqué es necesario el protocolo ARP en la red Ethernet?
- ¿Cómo detecta errores la capa de Enlace en la red Ethernet?
- ¿Los routers y los switchs porqué no implementan la capa de aplicación?

Capa de Red

La capa de Red es la que hace posible que la interconexión de muchas redes pueda verse como una única red.

Capa de Red - Definición

La capa de red es la encargada de proporcionar conectividad y selección de ruta entre hosts que pueden estar en la misma red local o en diferentes redes.

Lo logra utilizando un esquema de direcciones como IPv4 o IPv6, sumados a los protocolos IP, ICMP, los de ruteo y otros más. Para entender el concepto, imaginemos que se pudiera crear una gran red ethernet y que las direcciones MAC fueran las IP. Pero, en la realidad tenemos muchas redes heterogéneas, como la ethernet cableada, WiFi, la red de celulares, satélite, etc. Con las direcciones IP las tornamos homogéneas. Recordar que la información más importante que maneja la capa de red son las direcciones IP.

Capa de Red - Funciones

Las funciones más importantes son:

- reenvío (forwarding)
- enrutamiento (routing)

Cuando un paquete llega a un router por una interface (física o virtual) se analiza con la tabla de ruteo y se determina la interface por la cuál se enviará. El forwarding implica el paso de un paquete de una interface de entrada a otra de salida. Puede que el paquete tenga como destino el propio router, en cuyo caso se pasa a las capas superiores. Un ejemplo es un acceso al router a través de la red para configurarlo.

La otra función importante es el enrutamiento que consiste en utilizar la información de las tablas de ruteo para elegir la interface de salida. Más adelante veremos como se llenan de información estas tablas. Notar que en ningún caso el router tiene información del camino completo de un paquete a menos que sea el próximo host. Los algoritmos de ruteo proporcionan parte de la información contenida en las tablas.

Un algoritmo de enrutamiento es el encargado de aportar información para decidir el enlace de salida por el cuál se transmitirá un paquete.

Capa de Red - Reenvío

Una explicación sencilla sobre reenvío es que los paquetes llegan a un router: este analiza la información de la cabecera, la compara con una estructura de información (tabla de ruteo) y determina por cuál de sus otras interfaces enviará el mensaje.

En la tabla hay patrones de datos asociados a las interfaces.

Capa de Red - Ruteo

Los paquete van “saltando” de router en router pero no se mantiene el estado (Camino) de la comunicación.

Diferentes paquetes de una misma comunicación podrían tomar caminos diferentes a causa de congestión, caída de enlaces, mal funcionamiento de algún dispositivo (Siempre que haya un camino alternativo).

Capa de Red - Componentes

La capa de red en Internet está compuesta por:

- Protocolos de ruteo para
    - selección de ruta.
- Protocolos IP para
    - direccionamiento
    - formato de datagramas
    - manejo de paquetes
- Protocolo ICMP para

        - reportar errores
        - brindar información para el router
- Tabla de Ruteo para
        - elegir enlace de salida

Funcionamiento IP

Un ejemplo de funcionamiento de una conexión usando dos tecnologías de redes físicas diferentes: ethernet y frame relay. La forma de interpretar el gráfico en analizando las capas en forma vertical y horizontal.

Si seguimos la secuencia de **t1** a **t14** vemos como transitan los datos desde un sistema final A (host) al otro B (otro Host).

En el primer host A, la aplicación genera un conjunto de datos y se los pasa a la capa de Transporte. La capa de transporte le agrega un encabezado y la información más importante son los puertos (PORTs) origen y destino que permiten diferenciar a los procesos cliente y servidor que se van a comunicar entre los hosts:

```
------------------------
|  TCP-H  |    Data    |
------------------------
```

Este conjunto, llamado segmento, se pasa a la capa de red la que le agrega su encabezado y tenemos **t1**. La información más importante del encabezado son las IP destino (B) y la IP origen (A):

```
---------------------------------
| IP-H   |  TCP-H  |    Data    |
---------------------------------
```

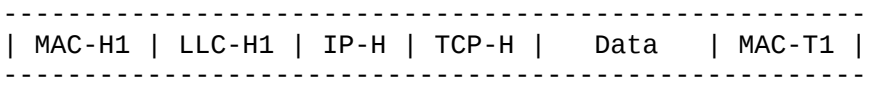
Ahora tenemos un paquete IP que se pasa a la capa de enlace ethernet compuesta por dos capas, la LLC que es la que se comunica con el SW y la MAC con el HW y por supuesto maneja las famosas direcciones MACs, quedando **t2**:

```
-----------------------------------------
| LLC-H1 |  IP-H   |  TCP-H  |    Data    |
-----------------------------------------
```

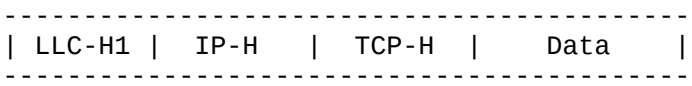
Acá se le agrega un acoplado también y estamos en **t3**.

```
-------------------------------------------------------
| MAC-H1 | LLC-H1 | IP-H | TCP-H |   Data   | MAC-T1 |
-------------------------------------------------------
```

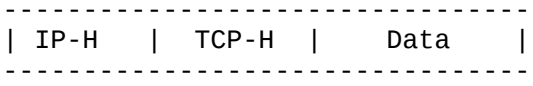
Se envía por la red hasta el router X que comparte la misma tecnología ethernet por un lado, pero que tiene otra del tipo Frame Relay **t4**:



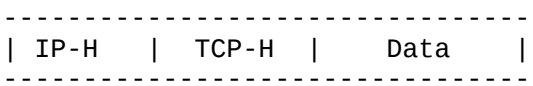
Para arriba **t5**:



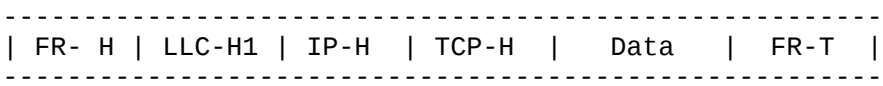
Más arriba a la capa de red del router X **t6**:



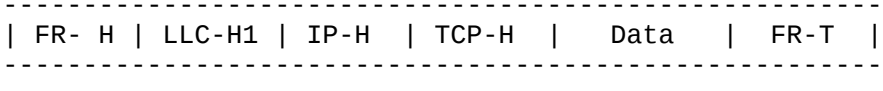
El router analiza la IP destino del encabezado IP y elige por dónde la va a enviar. Si la IP es una de las que tiene X, entonces pasa el paquete a las capas superiores. La ip no es propia **t7**.



En este caso elige la interface Frame Relay que lo conecta con el router Y **t8**:



Se envía a Y y llega **t9**:



Se pasa a la capa de red **t10**:

```
--------------------------------
| IP-H   |  TCP-H  |    Data    |
--------------------------------
```

Se analiza la IP destino como en X y se determina que debe ser enviado a B **t11**:

```
--------------------------------
| IP-H   |  TCP-H  |    Data    |
--------------------------------
```

Se pasa a la capa de enlace y **t12**:

```
-----------------------------------------
| LLC-H2 |  IP-H   |  TCP-H  |    Data    |
-----------------------------------------
```

Notar que los headers (encabezados) tienen el 2 para diferenciarlos de los anteriores ya que acá estamos en otra red ethernet y las MACs son diferentes. También se le agrega un acoplado y estamos en **t13**.

```
-------------------------------------------------
| MAC-H2 | LLC-H1 | IP-H | TCP-H |  Data  | MAC-T2 |
-------------------------------------------------
```

Llega al host B **t14**:

```
-------------------------------------------------
| MAC-H2 | LLC-H1 | IP-H | TCP-H |  Data  | MAC-T2 |
-------------------------------------------------
```

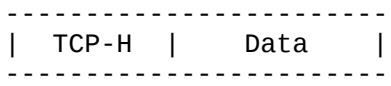
Para arriba **t15**:

```
-----------------------------------------
| LLC-H2 |  IP-H   |  TCP-H  |    Data    |
-----------------------------------------
```

A la capa de red **t16**:

```
--------------------------------
| IP-H   |  TCP-H  |    Data    |
--------------------------------
```

La IP destino es la ip de B entonces se pasa a la capa de Transporte TCP:



Se determina el proceso identificado por el PORT y se entrega los datos a la aplicación.

Ahora, si analizamos la comunicación en forma horizontal como por ejemplo:

t1, t6, t7, t10, t11, t16

Vemos que el conjunto de información, en este caso paquete, se repite para la capa de red en A, X, Y y en B. Los protocolos funcionan en forma horizontal entre las mismas capas de diferentes dispositivos. Los siguientes ejemplos solo involucran 2 t porque son punto a punto directamente conectados.

Datagrama IPv4

El encabezado del datagrama IPv4 está formado por una serie de campos.

Datagrama IPv4 - Campos 1/2

- Versión(4 bits)
    - IPv4 – actual
    - IPv 6
- IHL (Internet header length)(4 bits)
    - En bloques de 32 bits
    - Incluye opciones
- Tipo de servicio (8 bits)
    - Parámetros
- Largo total (16 bits)

    - En octetos

Datagrama IPv4 - Campos 2/2

- Identificación (16 bits)
    - Número de secuencia
    - Con direcciones y protocolo de usuario - único
- Indicadores (Flags)(3bits)
    - Bit más datos
    - No fragmentar
- Desplazamiento del fragmento (13 bits)
- Tiempo de Vida (8 bits)
- Protocolo (8 bits)

Tablas de Ruteo

Las tablas de ruteo se encuentran tanto en los routers como en los hosts. Poseen información para decidir el envío de paquetes. Consta de 4 partes pero algunas pueden no estar presentes.

Tipos de entradas en la tabla de ruteo:

1.- Las redes directamente conectadas.
2.- Redes configuradas en forma estática.
3.- Redes configuradas en forma dinámicas.
4.- Defecto.

La primer parte se completa con información sobre las redes que están directamente conectadas y puede obtenerla de la configuración de las interfaces al arrancar o si se introducen en caliente al configurar una interface.

La última parte es una sola entrada y es la ruta por defecto, comodín, ya que cualquier dirección coincide con ésta.

Estas dos partes son las que tienen todos los hosts y sirven para determinar si el envío es a un host local o remoto.

Las dos partes del medio pueden no estar o puede estar alguna de ellas, dependiendo de la complejidad de la red y las interconexiones donde opera el router.

Las estáticas son introducidas o configuradas por los administradores del router y son destinos que el router no conoce. Generalmente son pocas y se dan cuando la red en de tamaño pequeño pero que tiene algunos routers.

Las dinámicas son las que aprende utilizando los protocolos de ruteos codificados en algoritmos. Se utilizan generalmente en sistemas muy interconectados y complejos (corazón de internet).

Cada línea de la tabla de ruteo tiene la siguiente información:

```
-----------------------------------------
|   Red   |  Mask   |   GW  |  Interface  |
-----------------------------------------
```

Rutas 1/4

Veamos en un ejemplo cómo se arman las tablas de ruteo para R1 y R2. Todas las máscaras son /24

R1 está conectado a:

- Red:10.0.3.0 Interface:I0 IP:10.0.3.1
- Red:10.0.2.0 Interface:I2 IP:10.0.2.1
- Red:10.0.4.1 Interface:I1 IP:10.0.4.2

R2 está conectado a:

- Red:10.0.1.0 Interface:I0 IP:10.0.1.1
- Red:10.0.4.0 Interface:I1 IP:10.0.4.1
- Red:200.100.2.0 Interface:I1 IP:200.100.2.1 (Internet)

Rutas 2/4

Así se arman las tablas:

Primero las redes directamente conectadas.

En R1 el la primer entrada colocamos : 10.0.2.0, 24, *, I2. Significa que cuando tenga una dirección IP que reenviar va a aplicar la máscara de la segunda columna y comparar el resultado con la red 10.0.2.0.

Recordar que la IP a evaluar es dirección de host. Si coinciden las direcciones de red entonces hay que enviarla por la interface I2 y no hace falta un gateway.

El proceso de evaluación continúa con la siguiente entrada (fila) y así hasta encontrar una equivalencia (match).

Introducimos las dos siguiente lineas: 10.0.3.0, 24, , *I0 y 10.0.4.0, 24*, , I1.

Para R2 hacemos un proceso similar.

Rutas 3/4

Ahora completamos la ruta default.

Esta entrada en la última posibilidad que tiene una dirección de ser enviada. Entonces necesitamos que haga equivalencia (match) con cualquier red y la máscara 0.0.0.0 es un comodín para eso.

Y también necesitamos enviarle los paquetes a alguien que pueda dirigirlos (gateway, normalmente más arriba en la jerarquía o más cerca de la conexión al resto de las redes).

En el caso de R1 es R2, pero observar que se le envía a la IP de la interface que está en la red que comparten ambos routers y se sale por la interface que está directamente conectada a dicha red.

- Entonces será: Default, 0.0.0.0, 10.0.4.1, I1.

Los paquetes que van a las redes conectadas a R1 se entregan directamente, los que van para internet se envían a R2 para que él lo resuelva.

En el caso de R2 su router default está en internet y vamos a suponer que su dirección es 200.100.2.2.

Rutas 4/4

Es el turno de las direcciones estáticas y dinámicas.

Como la red es pequeña y los routers tienen pocas conexiones con otros routers no se justifica correr protocolos de ruteo y por lo tanto no tendremos entradas dinámicas.

Y las estáticas…

Veamos: con el estado de la tabla hasta acá no podemos resolver ciertas IP.

Supongamos que llega un paquete con la dirección IP 10.0.3.3 desde internet. No coincide con la primer entrada, ni con la segunda, que son las redes conectadas y pasa a la default. El paquete se envía otra vez a internet.

R2 no conoce las redes que están detrás de R1 y hay que agregarlas. Notar que la IP en la columna gateway es la de la interface que R1 tiene conectada a la red que comparten.

En R1 podemos agregamos la red 10.0.1.0 , pero es redundante porque se resuelve con la default.

Interfaces Virtuales

Cuando se instala una red local con subredes se requiere que las subredes estén conectadas por routers y en cableados conectados a dispositivos switchs diferentes.

Suponga que en el aula de máquinas de la biblioteca se quiere instalar tres subredes, las ya mencionadas A, D y E.

Va a haber mayoría de alumnos, un par de docentes y un par de administrativos. Poner un switch para cada grupo o un cableado separado no es rentable. Además los routers incrementan su costo cuando más interfaces tienen.

Los dispositivo de conexión vienen preparados para poder partirlos en subredes y conectarse al router con un solo troncal a una sola interface. Entonces hay que utilizar interfaces virtuales. La tabla de ruteo podría quedar así:

Destino	Mask	GW	Interface
10.0.1.0	/24	*	I0:0
10.0.2.0	/24	*	I1:0
10.0.3.0	/24	*	I2:0

ICMP 1/2

- Usado por hosts & routers para comunicar información a nivel de la red
    - Reporte de errores: host inalcanzable, o red, o puerto, o protocolo

        - eco request/reply (usado por ping)

- Funcionalidad de Capa de red “sobre” IP:
        - ICMP son llevados por datagramas IP
- Mensajes ICMP: tipo y código de error, más primeros 8 bytes del datagrama que causó el error
- Ejemplo para ping y traceroute

ICMP 2/2

El protocolo ICMP tiene varios códigos y también varios formatos de paquetes.

PING

Packet Internet Groper

- Testear conectividad
- Determinar latencias
- Utiliza paquetes ICMP
- Comando
    - ping ***IP***
    - ping ***Hostname***

Tracert – Traceroute - Tracepath

Verificar Rutas

- Utiliza el ttl
- Comando
        - tracepath ***IP***
        - tracepath ***Hostname***
        - tracert ***IP***
        - tracert ***Hostname***

Veamos el funcionamiento de la herramienta (Son todas similares):

- **Tracert – Traceroute – Tracepath**

En los paquetes IP existe un campo llamado **ttl** (time to live). Este campo tiempo de vida se llena con un valor numérico(8 bits) antes de enviar un paquete.

En teoría indica la cantidad de segundos, pero en la práctica funciona de otra manera.

El paquete sale de un host con un valor que se decrementa en 1 cada vez que pasa un router.

En funcionamiento normal el paquete entra a un router, se determina la interface de salida, se le decrementa el ttl en 1 y se envía.

Pero si hay congestión los paquetes van a para a una cola y luego de un determinado plazo se les decrementa en 1 el ttl. Si la cuenta llega a 0, se envía un mensaje de error al emisor y el paquete se descarta. Esto evita que el paquete quede circulando por la red indefinidamente en caso de un bucle de ruteo y favorece el control de congestión en la red.

Las herramientas estas realizan pings modificando el valor del ttl.

Funcionamiento:

Arranca con ttl=1, envía el paquete y lo recibe el primer router, este lo decrementa y como llega a 0 manda un mensaje de error.

Muestra el resultado.

Luego pone el ttl=2 y envía el nuevo paquete. Este morirá al segundo salto y brindará información sobre el siguiente punto.

Y así continúa incrementando el ttl hasta alcanzar el destino.

A tener en cuenta:

    - Los paquetes pueden tomar diferentes caminos dado que las rutas cambian dinámicamente por los protocolos de ruteo y pueden morir por retraso en alguna cola debido a una posible congestión; o pueden simplemente perderse.

Sin embargo es una herramienta interesante que nos indica que al menos existe un camino (si llega), puede indicarnos un corte en la red o un mal funcionamiento de algún router. Y nos brinda información adicional como tiempos de retardo.

Preguntas de Repaso

- ¿Cuál es la función principal de la capa de Red?
- ¿Cuál es la información más importante que maneja la capa de Red? ¿Porqué?
- ¿Cuál es la diferencia entre **forwarding** y **routing**?
- ¿Porque se dice que los protocolos rigen una comunicación horizontal y no vertical?

Capa Transporte

En la capa de transporte del modelo TCP/IP se implementan los servicios:

- Orientado a Conexión (TCP)
- Sin Conexión (UDP)

Transporte - Servicios 1/2

La función de la capa de transporte es proveer comunicación lógica entre procesos de aplicación que corren en diferentes hosts

Los protocolos de Transporte corren en sistemas finales.

- Emisor: descompone los mensajes de aplicación en segmentos, los pasa a la capa de red
- Receptor: rearma los segmentos en mensajes, los pasa a la capa de aplicación

Más de un protocolo de transporte disponible a las aplicaciones:

- TCP
- UDP

Transporte - Servicios 2/2

- Entrega confiable, en orden (TCP)
    - Control de congestión
    - Control de flujo
    - Establecimiento de conexión
- Entrega no confiable, sin orden (UDP)
    - Extensión simple del IP “best- effort”
- Servicios no disponibles
    - Garantías de retardo
    - Garantías de ancho de banda

Multiplexión

TCP posibilita multiplexar/demultiplexar, es decir, transmitir datos desde diversas aplicaciones en la misma linea o, en otras palabras, ordenar la información que llega en paralelo.

Estas operaciones se realizan empleando el concepto de puertos, es decir, un número vinculado a un tipo de aplicación que, cuando se combina con una dirección IP, permite determinar en forma exclusiva una aplicación que se ejecuta en una máquina determinada.

Preguntas de Repaso

- ¿Qué servicios provee la capa de Transporte?
- ¿Cuál es la información más importante que maneja la capa de Transporte?