Clasificación de redes

Redes

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Clasificación de Redes

Existen diversas formas de clasificar redes: según su tecnología de transmisión, según su escala, según el flujo de datos y según su topología. Analicemos cada uno de las clasificaciones ejemplificando el uso de cada tipo de red.

Según su tecnología de transmisión

Las transmisiones pueden ser punto a punto o por difusión. Una transmisión punto a punto es aquella en la que solo dos dispositivos intercambian datos entre si. Por ejemplo, transmitir una foto entre dos celulares utilizando Bluetooth es un ejemplo de transmisión punto a punto.

Cuando un dispositivo transmite información a múltiples destinatarios se habla de difusión o broadcast. Un canal de televisión o una emisora de radio utilizan este tipo de transmisión: un emisor, múltiples televidentes u oyentes.

Según su escala

Se clasifica a las redes según su tamaño o grado de cobertura. Las de menor cobertura se denomina redes de área personal o PAN (Personal Area Network) y su alcance está en el orden de algunos metros. Por ejemplo, una red entre una computadora y un parlante Bluetooth.

Las siguientes redes en la escala se denominan Redes de área local o LAN (Local Area Networks), las cuales tienen coberturas que van desde los 10 a los 1000 metros. Ejemplos típicos son una red de computadoras dentro de una oficina, un aula o en nuestro hogar. Actualmente a este tipo de redes se conectan no solo computadoras, sino Tablets, Smartphones, SmarTV, impresoras, máquinas de foto, aires acondicionados, heladeras, etc.

Las redes de área metropolitana o MAN (Metropolitan Area Networks) tienen cobertura en el orden de los 10Km. Se puede considerar la red de un provedor de servicio de Internet en una ciudad como un tipo de red MAN.

Finalmente, las redes con mayor cobertura se denominan Redes de área amplia o WAN (Wide Area Network). Estas redes cubre grandes regiones como por ejemplo paises o un continente entero. Son ejemplos de redes WAN las redes de las compañías telefónicas o de televisión por cable que ofrecen cobertura nacional o regional.

Internet es un tipo de red que cubre todo el mundo. Esta red se compone de muchas redes WAN, MAN y LAN que se interconectan entre si gracias a la estandarización de los protocolos.

Según su flujo de datos

Existen tres tipos de flujos de datos:

- Simplex: cuando en un enlace entre dos dispositivos uno solo puede transmitir información mientras que el otro recibirla.
- Half-duplex: en este caso, los dos dispositivos pueden transmitir información pero no en forma simultánea.
- Full-duplex: ambos dispositivos pueden transmitir información en forma simultánea.

Algunos sistemas por su objetivo requieren uno u otro flujo de datos. Por ejemplo, una emisora de radio no necesita que los receptores le envíen información ya que su objetivo principal es transmitir música o la voz humana sin necesidad de respuesta. Sin embargo en el caso de transmisión de datos entre computadoras, siempre es deseable que la modalidad sea full duplex para incrementar la velocidad.

Según su topología

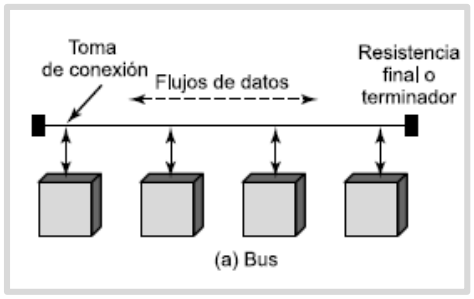
Una interesante clasificación de las redes es según su topología, es decir, cómo están física o lógicamente construídas. Cuando se habla de topología física, se tienen en cuenta las conexiones físicas entre dispositivos, por ejemplo con cable de cobre. En cambio la topología lógica define la forma en que los diferentes dispositivos de la red se comunican entre si más alla de su conexión física.

Antes de estudiar las diferentes topologías, es necesario aclarar que no hay alguna topología mejor que otra, sino que cada una tiene ventajas y desventajas que permiten que sea elegida para determinado tipo de red. Además, existe la posibilidad de usar más de una topología en una red, lo que se denomina topología híbrida.

Topología Bus

Esta topología se utilizaba en antiguas redes LAN Ethernet con cable coaxial, pero cayó en desuso debido al mejor desempeño de los cables de cobre. Actualmente es utilizada en redes HFC (híbridas fibra óptica cable coaxial) por parte de empresas de televisión por cable, en el tramo final coaxial.

Figura 1: Topología Bus



Fuente: Stallings, 2007, p. 485

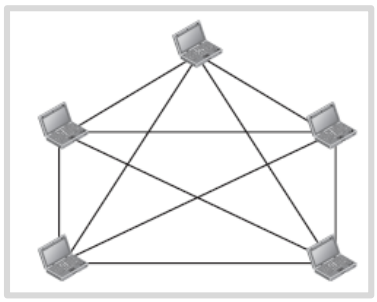
Se utiliza un cable troncal de gran extensión y todos los dispositivos que se quieren conectar a la red se conectan a ese troncal. Debido a la utilización de este troncal, la instalación es sencilla y el costo total de los cables es mas bajo que en otras topologías.

Sin embargo presenta algunos inconvenientes. Cuando hay alguna rotura en el algún tramo del cable, toda la red queda sin servicio. No es sencillo encontrar fallas debido a esta problemática.

Topología Malla

Existen dos versiones de esta topología: la malla total (Full Mesh) y la malla parcial (Partial Mesh). En una Malla total, todos los dispositivos que forman la red tienen un enlace dedicado al resto de los dispositivos. En una malla parcial, no todos los dispositivos cumplen ese requisito.

Figura 2: Topología Malla



Fuente: Forouzan, 2013, p. 10

Conectar todos los dispositivos entre sí presenta un gran desafío: a medida que se agregan dispositivos, crece en forma exponensial el número de enlaces. Para calcular este número, utilizar la siguiente expresión: $E = n(n-1)\div$, donde E es el número de enlaces, y n el número de nodos o dispositivos. La gran ventaja de esta topología es que para alcanzar a

cualquier dispositivo de la red se utiliza un enlace dedicado. Además si falla un enlace, es posible acceder por cualquier otro camino.

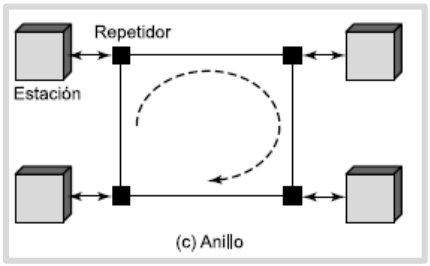
Las desventajas están relacionadas a la cantidad de cable necesario y su costo asociado.

Esta topología se utiliza para redes de tamaño reducido con dispositivos críticos.

Topología Anillo

Esta topología toma su nombre del hecho de que cada dispositivo se conecta a otros dos formando un anillo. Si hay una falla en algún enlace la red queda inaccesible; sin embargo, para evitar este problema se construyen anillos dobles o redundantes. La instalación de un anillo es sencilla y resulta económica cuando se unen grandes distancias, como por ejemplo las centrales y hubs de una red de televisión por cable.

Figura 3: Topología Anillo

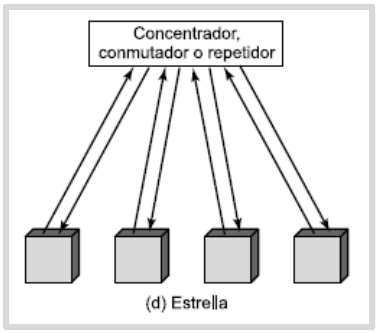


Fuente: Stallings, 2007, p. 485

Topología Estrella

Topología dominante en redes LAN Ethernet, se basa en la utilización de un nodo central (Switch). Cada dispositivo se conecta al nodo mediante un enlace dedicado. Si bien se requiere más cable que en otras topologías, es muy sencillo detectar una falla, y solo el dispositivo cuyo enlace se ve afectado queda fuera de la red.

Figura 4: Topología Estrella



Fuente: Stallings, 2007, p. 485

Referencias

Stallings, W (2004). Introducción a las comunicaciones de datos y redes en *Comunicaciones y Redes de Computadoras.* Madrid: Editorial Pearson Education

Forouzan, B (2013). Introduction en *Data Communications AND Networking.* Estados Unidos: McGraw-Hill

Modelos de referencia

Redes

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Modelos de referencia

El modelo TCP/IP permitió el desarrollo actual de las redes de datos e Internet.

A diferencia de las primeras redes en donde el diseño estaba orientado al hardware, desde hace varias décadas el diseño está orientado al software. Además, para simplificarlo, se decidió crear un modelo de capas en donde cada una de estas capas realiza su función específica e interactúa con otra u otras.

La ventaja de este modelo es que se dividen las tareas de la red y no es necesario que algún protocolo perteneciente a alguna capa conozca los detalles del resto; solo se centra en su función, y los demás protocolos de las demás capas en el propio. Por cierto, un protocolo es un conjunto de reglas que deben seguirse. Si los dispositivos de una red no se ponen de acuerdo en como transmitir datos, el intercambio no sería posible.

Puedes encontrar una excelente analogía del modelo de capas en la página 27 del libro Redes de Computadoras.

El modelo OSI

El modelo OSI (Open System Interconnection ó Interconexión de sistemas abiertos) es un modelo de referencia creado por la ISO (organización internacional de estándares).

Es un modelo que surgió luego del stack de protocolos TCP/IP que también analizaremos. Como TCP/IP ya estaba implementado, el modelo OSI no logró definir protocolos para ciertas capas por lo que en la prácica no llegó a implementarse y solo sirve como referencia.

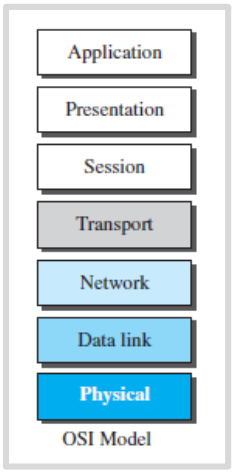
En la figura 1 se oberva el modelo de 7 capas con el nombre en inglés de cada una de ellas. También es muy común referirse a cada capa por su número, que comienza en capa 1 para la capa física, hasta llegar a la capa 7 o aplicación.

Resumen de funciones de cada capa:

- Capa 1 (Física): determinar que valores de señal representan un 1 binario y un 0 binario y cuál es la duración de cada bit. Si la transmisión será half o full dúplex, como son las interfaces.
- Capa 2 (Enlace de datos): si bien los bits viajan por el cable uno tras otro, esta capa forma lo que se denomina trama. Una agrupación lógica que es comprendida por el transmisor y el receptor. Esta capa además detecta y corrige errores, y puede realizar control de flujo, es decir, evita saturar al receptor si este es más lento que el transmisor o le avisa al transmisor que puede incrementar la velocidad.

- Capa 3 (Red): esta capa forma otra agrupación de bits denominada Paquete, la cual se encapsula luego en la trama de la capa 2. La función principal es llevar estos paquetes desde el origen hasta el destino, pasando por diversos nodos intermedios. Esta capa realiza control de congestión. Finalmente, esta capa resuelve problemas relacionados a la interconexión de redes heterogéneas.
- Capa 4 (Transporte): Se determina, según el protocolo utilizado, si el servicio será orientado o no a la conexión. De forma similar a las capas 3 y 2, forma un PDU (Unidad de datos de protocolo) que luego es encapsulado en un paquete de capa 3.
- Capa 5 (Sesión): define la sincronización entre dispositivos de la red.
- Capa 6 (Presentación): permite la comunicación cuando dos dispositivos utilizan diferentes tipos de representaciones en los datos que van a intercambiar.
- Capa 7 (Aplicación): es la capa más cercana al usuario en donde se definen protocolos que son utilizados por las aplicaciones de red. Por ejemplo, un protocolo para enviar y recibir correo electrónico.

Figura 1: Modelo OSI



Fuente: Forouzan, 2014, p. 45

El conjunto de protocolos TCP/IP

TCP/IP es similar a OSI ya que utiliza el modelo de capas. Su nombre surge de dos protocolos utilizados muy importantes: el protocolo TCP y el IP. Originalmente se definió como un modelo de 4 capas (Data-Link, Internet, Transport y Application), aunque actualmente se lo piensa como de cinco.

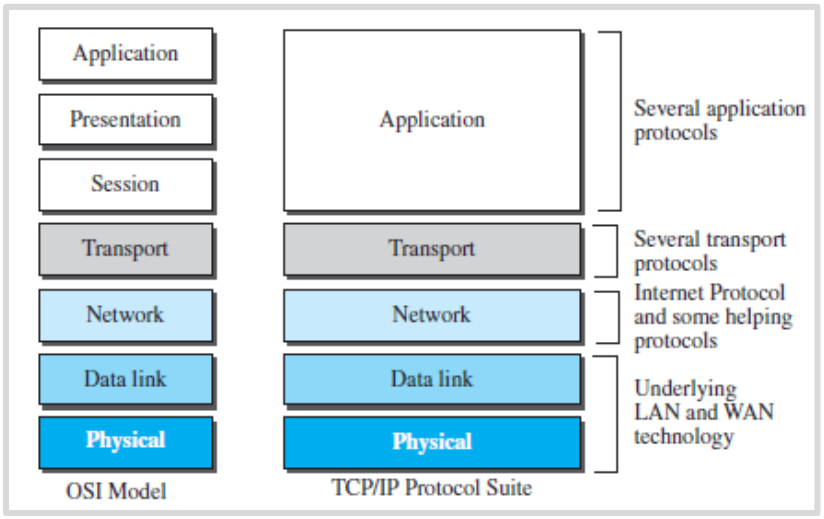
- Capa física: esta capa se encarga de la transmisión de bits y se puede pensar que interactúa con una capa inferior oculta, la cual sería el medio de transmisión.

- Capa enlace de datos: no define un único protocolo, sino que soporta todos los posibles de este nivel mientras cumplan el requisito de formar una trama y ser capaces de enviarlas al destinatario en el mismo segmento de red. El dispositivo denominado Switch funciona en esta capa, ya que es capaz de recibir las tramas y enviarlas al destino indicado.
- Capa de red o Internet: similar a la capa 3 del modelo OSI. Aquí se define el protocolo IP (Internet Protocol) el cual define cuál es el formato del paquete, es decir, su tamaño, su encabezado y los campos que lo componen. Este protocolo se define como "no orientado a la conexión" lo que significa que no garantiza que los paquetes lleguen a destino, aunque hará su mejor esfuerzo. Tampoco realiza controles de flujo, errores o congestión, dejando estos controles a cargo de la capa superior. Los dispositivos denominados Routers o enrutadores se encargan de encaminar los paquetes para que estos atraviesen diferentes redes y lleguen a destino.
- Capa de transporte: aquí se definen protocolos que toman los datos de la capa de aplicación, los dividen en una unidad propia del protocolo (segmento o datagrama de usuario) la cual es encapsulada en los paquetes IP. Existe diversidad de protocolos, cada uno diseñado para un tipo de servicio particular. Por ejemplo, TCP realizar control de flujo y congestión, y puede detectar cuando los segmentos no llegan a destino y retransmitirlos. UDP en cambio no realizar ninguna de estas operaciones. A simple vista uno pensaría ¿para qué utilizar UDP? La respuesta es que hay aplicaciones, como por ejemplo las transmisiones de Voz, en donde retransmitir paquetes sería contraproducente por lo que es mejor descartarlos.
- Capa de aplicación: En esta capa se realiza una comunicación "proceso a proceso" entre computadoras, es decir entre los diferentes programas de aplicación. Por ejemplo, cuando visitamos una página web, utilizamos el protocolo HTTP, cuando enviamos y recibimos correos electrónicos utilizamos SMTP y POP.

Comparación OSI – TCP/IP

Si bien TCP/IP se implementa en la práctica y OSI quedó relegado a ser un modelo de referencia teórico, es común referirse a las capas del modelo OSI cuando se habla de algún protocolo de TCP/IP. En la figura 2 puede verse la relación entre capas de los dos modelos.

Figura 3: Encapsulación y desencapsulación de la información



Fuente: Forouzan, 2014, p. 45

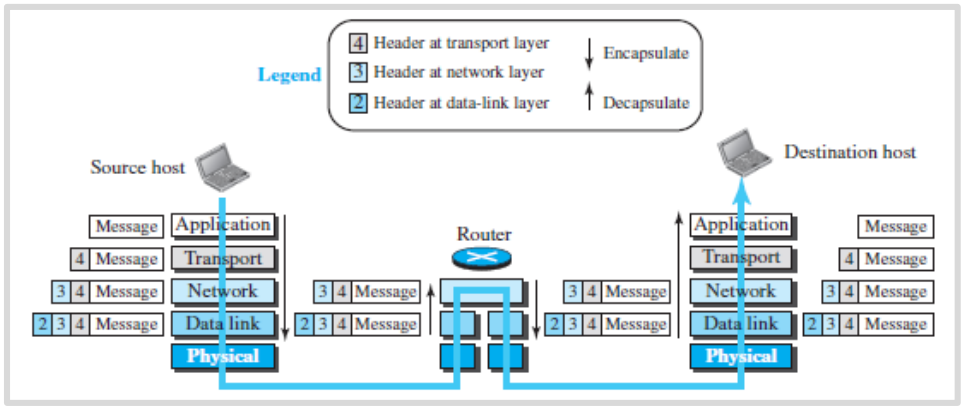
Una tecnología LAN muy popular que trabaja tantos en las capas físicas como enlace de datos se denomina Ethernet. Analizaremos Ethernet y su evolución en este mismo módulo.

Encapsulación y desencapsulación

En la figura 3 se observa un esquema de dos computadoras (origen y destino) y un Router que interconecta dos redes. El mensaje originado por la computadora de origen se va encapsulando a medida que desciende por las diferentes capas y cada una le agrega su encabezado. Este encabezado consiste en un número de campos que cumplen diversas funciones como almacenar las direcciones de origen y destino, una suma de verificación y otros datos que estudiaremos y que hacen posible que los paquetes lleguen a destino.

En El Router, solo se desencapsula hasta la capa 3 para obtener datos necesarios para que el equipo tome la decisión de ruta correcta, y luego es nuevamente encapsulado. Finalmente, la computadora de destino recibe la trama y comienza el desencapsulado hasta obtener el mensaje original.

Figura 4: Encapsulación y desencapsulación de la información



Fuente: Forouzan, 2014, p. 41

Este proceso agrega información al mensaje original la cual "consume" parte de la capacidad que puedan tener los enlaces entre dispositivos. Esta consecuencia se denomina "packet overhead" y depende de dos factores: la longitud total del paquete y la longitud del encabezado.

Si dos paquetes tienen la misma longitud de encabezado, pero el paquete A lleva un mensaje de mayor tamaño que el paquete B, el overhead de este último será mayor. Esto significa que la capacidad de la red se está utilizando menos eficientemente que con el paquete A.

Referencias

Stallings, W (2004). Introducción a las comunicaciones de datos y redes en *Comunicaciones y Redes de Computadoras.* Madrid: Editorial Pearson Education

Forouzan, B (2013). Introduction en *Data Communications AND Networking.* Estados Unidos: McGraw-Hill

Acceso al medio

Redes

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Acceso al medio

La capa física del modelo OSI se encarga de la transmisión de bits de un extremo a otro. Esta capa se basa en diversos medios de transmisión como pueden ser el cable UTP, el cable coaxial, la fibra óptica o las radiocomunicaciones. Ninguno de estos medios está libre de errores. Estos errores se producen debido a la problemática del ruido o por interferencias.

Si bien los medios son construídos para minimizar los errores, estos siempre están presentes, y la capa 1 nada puede hacer con ellos, ni siquiera reconocerlos. Es por ello que deja este interesante trabajo a su capa inmediata superior: la capa de enlace de datos.

Diversas funciones se llevan a cabo en la capa de enlace además de detectar o detectar y corregir errrores: se forman tramas que agrupan a todos los bits provenientes de la capa superior, se les agrega un encabezado con información que hace posible que estas tramas sean interpretadas y lleguen al destinatario correcto, y se introducen códigos para detectar o corregir errores.

Cuando las redes son de difusión, se debe establecer un mecanismo para que todos los dispositivos puedan ser capaces de transmitir y recibir información sin interferirse entre sí. Para este propósito, los protocolos definen una subcapa dentro de la capa 2 denominada "subcapa de control de acceso al medio".

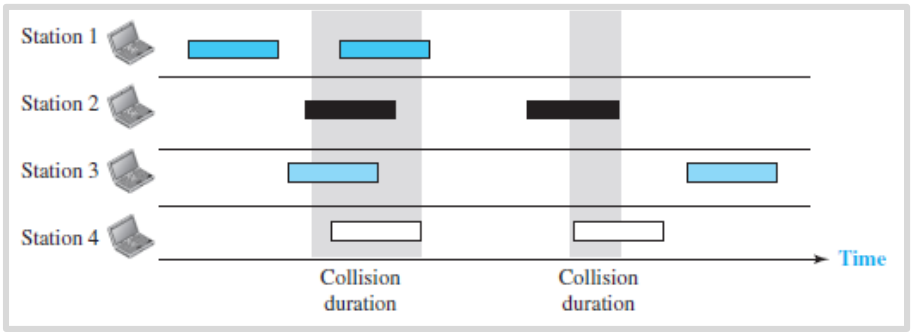
Analicemos la evolución de los protocolos utilizados en redes de difusión.

ALOHA puro

El método usado por ALOHA puro es muy simple y en la actualidad puede parecer sorprendentemente malo, pero al momento de su creación (1970) resultaba eficiente para las necesidades de la época.

¿Cuándo pueden transmitir los dispositivos de una red que utiliza un medio compartido? Simplemente cuando tengan algo que enviar.
La eficiencia es muy baja como se observa en la figura 1. Solo dos tramas llegan a destino en forma exitosa: la primera enviada por la estación 1, y la tercera enviada por la estación 3. Todas las demás sufrieron colisiones, es decir, se interfirieron y la información fue destruída. Cuando se produce una colisión, se espera un tiempo aleatorio para retransmitir para evitar una casi segura segunda colisión.

Figura 1: ALOHA puro



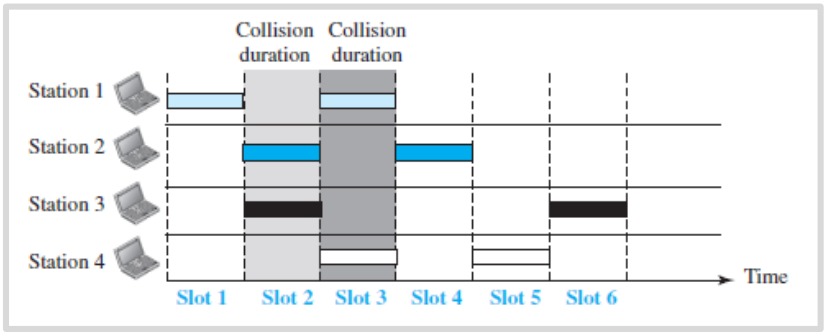
Fuente: Forouzan, 2014, p. 327

ALOHA ranurado

Este método mejora al anterior simplemente dividiendo el tiempo en slots o ranuras. Antes cada estación podría transmitir en cualquier momento, en cambio con el nuevo método solo pueden transmitir cuando comienza un nuevo slot.

Si bien no se eliminan las colisiones ya que dos o más estaciones pueden tener datos para transmitir cuando comienza un slot, se reduce el tiempo de vulnerabilidad a la mitad en relación a ALOHA.

Figura 2: ALOHA ranurado



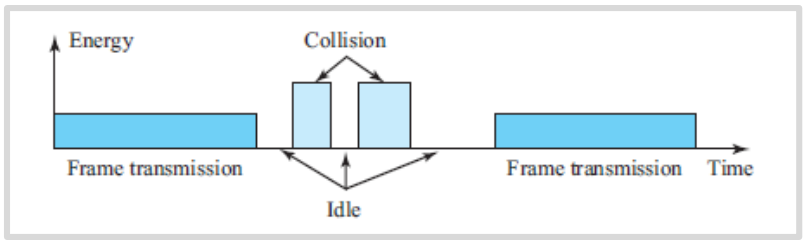
Fuente: Forouzan, 2014, p. 330

CSMA

CSMA significa acceso múltiple con detección de portadora. Como el nombre lo indica, a diferencia de los métodos ALOHA donde las estaciones solo eran capaces de enviar sus tramas en cualquier momento o al inicio de una trama, en este caso las estaciones hacen un sensado del medio. Esto significa que antes de transmitir, las estaciones escuchan el medio y pueden darse cuenta

si otra estación está transmitiendo o si una colisión ocurre. Lo hacen al detectar el nivel de tensión. Los 3 casos se observan en la figura 3.

Figura 3: Niveles de tensión



Fuente: Forouzan, 2014, p. 337

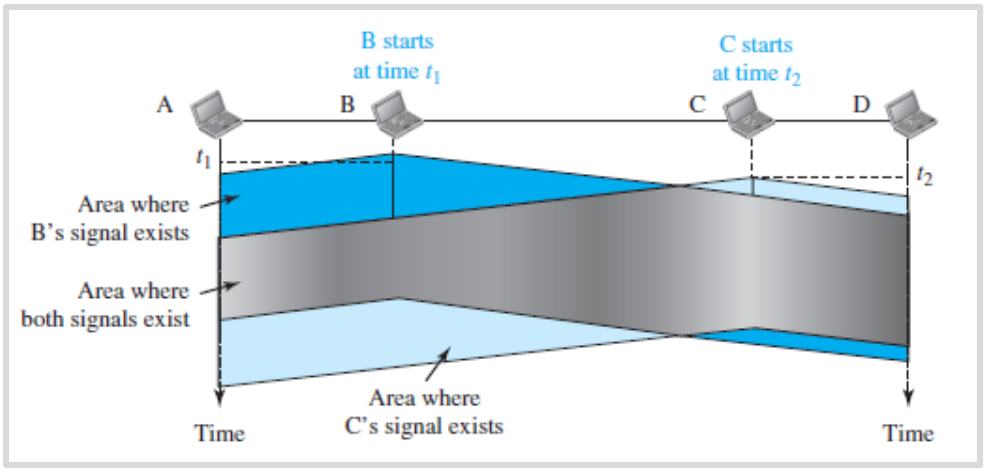
¿Esto significa que se eliminan las colisiones? Lamentablemente no es posible eliminarlas debido a una problemática relacionada a la distancia.

Consideremos la figura 4 para analizar el problema.

La computadora B está escuchando el canal en el momento t1 y como no detecta señales, transmite su trama al medio compartido. La información no viaja instantáneamente, sino que existe una demora por el tiempo de propagación de las señales, dependiente de la distancia y del medio utilizado.
Entonces, en el momento t2 la estación C se encuentran sensando el canal, y si bien la estación B ya está transmitiendo no le es posible detectar tal situación y por lo tanto transmite su trama.

Finalmente se produce la colisión de tramas destruyéndose la información. El tiempo de vulnerabilidad (es decir, el tiempo en que pueden producirse las colisiones) es igual al tiempo de propagación de la trama.

Figura 4: Colisión en CSMA



Fuente: Forouzan, 2014, p. 332

Cuando se utiliza CSMA, las estaciones detectan el canal libre y transmiten. Cuando detectan que el canal se encuentra ocupado pueden utilizar diversos métodos.

CSMA Persistente-1

Se denomina persistente 1 porque en el preciso momento en que una estación detecta que el canal está libre, transmite su trama con probabilidad 1. Hay grandes chances de que ocurra una colisión ya que todas las estaciones se comportan de igual manera y pueden comenzar a transmitir casi en simultáneo.

La persistencia se da porque los dispositivos sensan continuamente buscando transmitir apenas el canal se desocupe.

CSMA no persistente

Este método difiere del CSMA Persistente-1 ya que los dispositivos no sensan de manera permanente, sino que esperan un tiempo aleatorio cuando detectan el canal ocupado. Como la probabilidad de que dos estaciones hayan esperado el mismo tiempo aleatorio para transmitir es muy baja, se reducen las chances de colisiones.

La desventaja es que se reduce el rendimiento, ya que el canal puede permanecer libre debido a que los dispositivos se encuentran esperando sus tiempos aleatorios.

CSMA Persistente-p

Este método se usa en canales que utilizan slots o ranuras y combina las ventajas de los dos anteriores. Cuando una estacion detecta que el canal

está libre transmite su trama con probabilidad p. Luego espera el inicio del sigiuente slot y vuelve a chequear el estado del canal. Aquí pueden suceder dos cosas:

- El canal está libre, entonces, volver al paso anterior y transmitir con probabilidad p.
- El canal está ocupado, entonces actuar como si hubiera ocurrido una colisión y activar un mecanismo de espera.

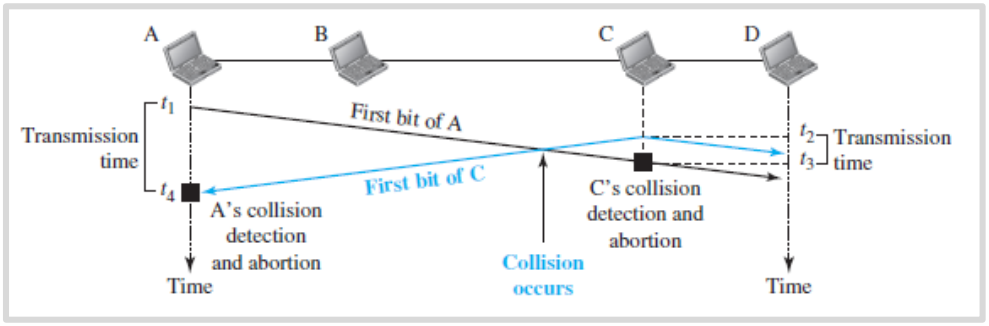
CSMA/CD

CSMA mejora el rendimiento al permitir que los dispositivos escuchen el canal en lugar de transmitir sus tramas sin importar lo que hagan los demás. Pero todavía existen un problema: ¿qué hacer cuando se produce una colisión?

Hasta el momento las estaciones simplemente continuaban transmitiendo sus tramas aun luego de la colisión. EL método CSMA/CD (con detección de colisiones) mejora esta situación haciendo que un dispositivo que detecta una colisión, pare de transmitir su trama.

Analicemos la situación consierando la figura 5. A detecta el canal libre en el momento t1 y transmite su trama. C detecta el canal libre en t2, ya que aun no ha llegado el primer bit de la trama de A, y transmite su trama. Luego de un tiempo y en una distancia intermedia se produce la colisión, la cual es advertida por A en el momento t4 y por C en el momento t3. En esos momentos A y C dejan de transmitir y liberan el canal.

Figura 5: Colisión en CSMA



Fuente: Forouzan, 2014, p. 335

Detectar colisiones y dejar de transmitir mejora el rendimiento al liberar el canal antes, pero para que este método funcione debe haber ciertas restricciones en cuanto al tamaño mínimo de trama.

Para profundizar tus conocimientos y leer sobre otras técnicas de acceso, te recomiendo consultar el capítulo 4 del libro Redes de Computadoras, de Tanenbaum.

Otros protocolos

Existen otros tipos de protocolos utilizados principalmente en redes inalámbricas. Puede profundizar tus conocimientos sobre protocolso MACA y MACAW (Acceso múltiple con prevensión de colisiones y Acceso múltiple con prevensión de colisiones inalámbrico) en el capítulo 4 del libro Redes de Computadoras de Tanenbaum. Además, como este último protocolo tiene aún sus limitaciones, puede consultar este docuemnto y pensar como podría mejorarse:
http://web.mit.edu/6.263/www/MACAW.pdf

Referencias

Tanenbaum, A (2012). La subcapa de control de acceso al medio en Redes *de Computadoras.* Madrid: Editorial Pearson Education

Forouzan, B (2013). Data Link Layer: Ethernet en *Data Communications AND Networking.* Estados Unidos: McGraw-Hill

Ethernet

Redes

UNIVERSIDAD SIGLO 21 | MIEMBRO DE LA RED ILUMNO

Ethernet

Los estándares IEEE 802.3 / Ethernet son utilizados en forma masivas en redes de área local (LAN).

La tecnología Ethernet fue una de tantas otras tecnologías que surgieron en los comienzos de las redes LAN (otras son token ring, token bus, FDDI) pero es la que a lo largo del tiempo ha logrado convertirse en el estándar de este tipo de redes.

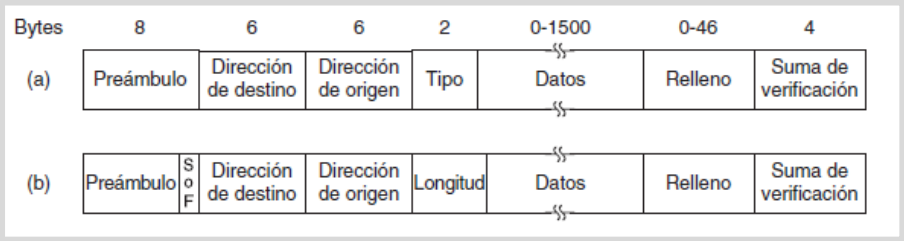
La IEEE estandarizó a Ethernet bajo el número 802.3, y realizó modificaciones mínimas que permiten la compatibilidad entre sí. En la actualidad, es similar hablar de estandar 802.3 o Ethernet.

Ethernet abarca tanto el nivel físico de OSI como el de enlace de datos. Además, en el nivel de enlace se subdivie en dos: Control de acceso al medio (MAC) y Control de Enlace Lógica (LLC).

Subcapa MAC

El objetivo de esta subcapa es controlar el acceso a un medio compartido y formar tramas. La trama Ethernet tiene el formato que se observa en la figura 1. En la figura también puede verse la comparación con la trama 802.3 y la pequeña diferencia.

Figura 1: Modelo OSI



Fuente: Tanenbaum, 2012, p. 242

Las tramas tienen un tamaño mínimo y uno máximo. Si te preguntas por qué, puedes profundizar leyendo la sección 4.3 del libro Redes de Computadoras.

El campo denominado preámbulo permite detectar el comienzo de una trama. Es una secuencia predefinida de unos y ceros durante 8 bytes, la cual no se repite dentro de los datos.
Las direcciones de destino y origen permiten identificar quién debe recibir los datos y procesarlos, y quién no.
El campo tipo anuncia que protocolo va encapsulado en el área de datos. Por ejemplo, si la capa superior trabaja con IP, en ese campo estará el número 0800. En la versión 802.3, el campo Tipo se denomina Longitud y expresa cuantos Bytes tiene en total esa trama.

El campo de datos es variable entre 0 bytes y 1500 bytes. Para mejorar la eficiencia de la red, es conveniente que ese campo esté completo con los 1500 bytes; de lo contrario, el porcentaje de datos transportados en comparación con los bytes de encabezado es inferior.
El campo relleno se utiliza en caso de que la trama no llegue al tamaño mínimo.
Finalmente, el campo suma de verificación almacena una secuencia de bits resultante de aplicar una verificación de redundancia cíclica, la cual le permite al receptor detectar errores de hasta 32 bits.

Para conocer más sobre como funciona el CRC, consultar la sección 3.2 del libro Redes de Computadoras de Tanenbaum.

Direcciones Ethernet

Cada dispositivo que forma parte de una red LAN posee un número identificador denominado dirección Ethernet. Las comunicaciones son posibles porque las tramas contienen los campos dirección de origen y dirección de destino.
Las direcciones Ethernet tienen un tamaño de 48 bits (6 bytes) aunque lo normal es expresarlas en hexadecimal, como por ejemplo: 1B:20:30:FA:FB:00

Del total de 6 bytes, los primeros 3 se denominan "OUI" o identificador único de organizador. Cada fabricante posee un número de OUI. Puedes hacer la prueba localizando el fabricante de tu placa de red ingresando a https://www.wireshark.org/tools/oui-lookup.html y pegando los primeros 3 bytes de tu dirección MAC.

Conocer tu dirección MAC varía de acuerdo al sistema operativo. Por ejemplo en un sistema operativo Windows debes ejecutar *ipconfig /all* y buscar el campo *dirección física*.

Es interesante conocer que la transmisión de esa dirección se hace a nivel de byte enviándose primero el bit menos significativo. Utilizando el ejemplo anterior, el primer byte es 1B, convertido a binario es 00011011.
Ese byte será transmitido de la siguiente forma al cable: 11011000.

Esto puede parecer confuso, pero justamente el bit menos significativo del primer byte indica si el destino es un único dispositivo o varios.

¿Es posible enviar entonces tramas a más de un destinatario?

La respuesta es si. No solo es posible enviar una trama a un dispositivo específico, lo que se denomina **Unicast**, sino que también es posible enviarla a un grupo de destinatarios; en este caso la dirección deberá ser de

Multicast. Para enviar una trama a todos los dispositivos de una LAN, se utiliza una dirección especial denominada de **Broadcast**. Esta dirección contiene todos los bits en 1, resultando ser en código hexadecimal: FF:FF:FF:FF:FF:FF.

Enviar broadcast resulta ineficiente para la red, porque si todo el mundo lo hace la red se congestionará. Sin embargo, que exista la posibilidad de hacerlo es de suma utilidad como estudiaremos en el siguiente módulo.

Control de acceso al medio

Originalmente Ethernet trabajaba en medios compartidos, por lo que era necesario arbitrar sobre quién podía transmitir y quién no, y qué se debía hacer cuando se producía una colisión (situación no deseada que se produce cuando dos estaciones transmiten en simultáneo).

Si bien actualmente las redes LAN son conmutadas, lo cual significa que el enlace entre dos dispositivos es full duplex y las colisiones no pueden producirse, las actualizaciones del estándar poseen compatibilidad hacia atrás, es decir que una nueva versión del estandar es compatible con la anterior y hereda características que se diseñaron debido al control de acceso al medio.

El método utilizado por la primera versión de Ethernet se denomina Acceso múltiple con sensado de portadora y detección de colisiones. (CSMA/CD). Puedes leer más sobre este método y las particularidades que llevaron a definir un tamaño de trama mínimo en el capítulo 4 del libro “Redes de Computadoras” de Tanenbaum.

Implementaciones

Además de definir como debe ser la trama y como se realizará el control de acceso al medio, Ethernet define que tipo de medio de transmisión y que topologías pueden utilizarse.

La primera versión de Ethernet contemplaba 4 tipos de implementaciones las cuales tienen la siguiente denominación:

- 10Base5
- 10Base2
- 10Base-T
- 10Base-F

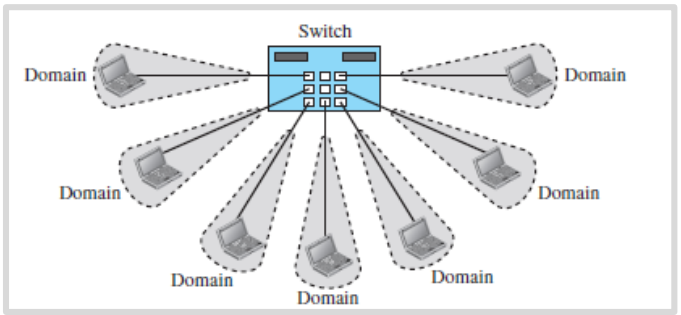
El número 10 hace referencia a la velocidad de transmisión: 10Mbps. La palabra Base significa que se transmiten señales digitales en banda base. El número 5 indica 500 metros de alcance máximo, mientras que el 2 indica 185m, ambas versiones trabajaban sobre cable coaxial grueso y fino respectivamente. Finalmente, las letras T y F indican la utilización de cable UTP y Fibra Óptica respectivamente con distancias máximas de 100 y 2000 metros.

Las implementaciones con cable coaxial utilizaban topología Bus, mientras que el uso de cable UTP o Fibra migró la topología a Estrella. Para interconectar los dispositivos en topología estrella se utilizaban Hubs. Un hub no es mas que un repetidor de señal, con lo cual si una estación transmitía una trama, todas las demás la recibían. Esta situación se denomina "dominio de colisión" lo cual significa que todos los dispositivos forman parte de un dominio donde pueden ocurrir colisiones.

El remplazo de hubs por switches introduzco el concepto de conmutación: ahora los switches poseen inteligencia y en lugar de "repetir" la señal a todas sus salidas, tienen la capacidad de aprender qué dispositivo está conectado en cada interfaz, y de esta forma reenviar la trama solo a esa interfaz. Lo que hacen los switches para poder conmutar es crear una tabla que almacena la MAC que está conectada a cada interfaz. De esta forma los dominios de colisión están ahora reducidos al enlace entre un dispositivo y el puerto del switch, y si la comunicación pasa de ser half-duplex a full-duplex, entonces se elimina por completo la posibilidad de colisiones.

En la figura 2 se observa el esquema de una red LAN, la cual utiliza un switch para interconectar dispositivos con topología estrella. Cada enlace es un dominio de colisión.

Figura 2: Ethernet conmutada



Fuente: Forouzan, 2012, p. 375

Evolución de Ethernet

Las necesidad de velocidad fueron aumentando por lo que se promovieron actualizaciones al estandar original Ethernet capaz de ofrecer velocidades de 10Mbps (20Mbps para Full-duplex).

La primera actualización fue a 100Mbps y se denomina FastEthernet. Esta actualización eliminó la topología Bus y disminuyó la distancia máxima de la red de 2500 a 500 metros para poder ser compatible con el tamaño de trama de Ethernet. Además se cambió la codificación Manchester por sistemas capaces de lograr la velocidad de 100Mbps.

Para profundizar estos cambios, consultar la sección 4.3 del libro Redes de Computadoras de Tanenbaum.

Gigabit Ethernet

La segunda actualización llevó la velocidad a 1000Mbps o 1Gbps manteniendo la compatibilidad con versiones anteriores. Para lograr esta velocidad se introdujeron diversos cambios en la cantidad de pares del cable UTP usados, la distancia máxima de la red y el sistema de codificación.

Figura 1: Implementaciones Gigabit

Implementation	*Medium*	*Medium Length*	*Number of wires*	*Encoding*
10GBase-SR	Fiber 850 nm	300 m	2	64B66B
10GBase-LR	Fiber 1310 nm	10 Km	2	64B66B
10GBase-EW	Fiber 1350 nm	40 Km	2	SONET
10GBase-X4	Fiber 1310 nm	300 m to 10 Km	2	8B10B

Fuente: Forouzan, 2012, p. 383

10Gigabit Ethernet y más

Las actualizaciones continuan debido a las necesidades de mayores velocidades de acceso. Pueden consultarse los diferentes estándares definitivos y en desarrollo:

- 10GigabitEthernet: estándar IEEE 802-3ae
- 40/100GigabitEthernet: estándar IEEE 802.3bm
- TerabitEthernet: estándar IEEE 802.3bs

Referencias

Tanenbaum, A (2012). La subcapa de control de acceso al medio en Redes *de Computadoras.* Madrid: Editorial Pearson Education

Forouzan, B (2013). Wired LANs: Ethernet en *Data Communications AND Networking.* Estados Unidos: McGraw-Hill