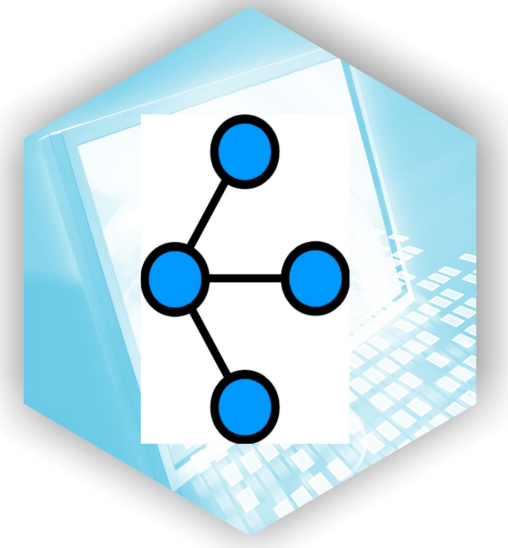
Centro de Educación

Manual de Introducción a Redes TCP/IP



Introducción a Redes TCP/IP

Versión: 1.0
Revisor diagramación: Unidad Apoyo de Diseño y Gestión Documental
Fecha de revisión:13/05/2015

Autores: Ing. Sergio Blanco
Ing. Marcelo Sosa

Índice

Introducción a las redes de computadoras

Definición

Se definirá "red de computadoras" a un conjunto de computadoras autónomas interconectadas con el fin de intercambiar información y permitir el uso compartido de recursos (impresoras, archivos, etc.). Se dice que dos computadoras están interconectadas si pueden intercambiar información y compartir recursos.

Motivaciones

Algunas de las motivaciones para crear la primer red de computadoras fueron:

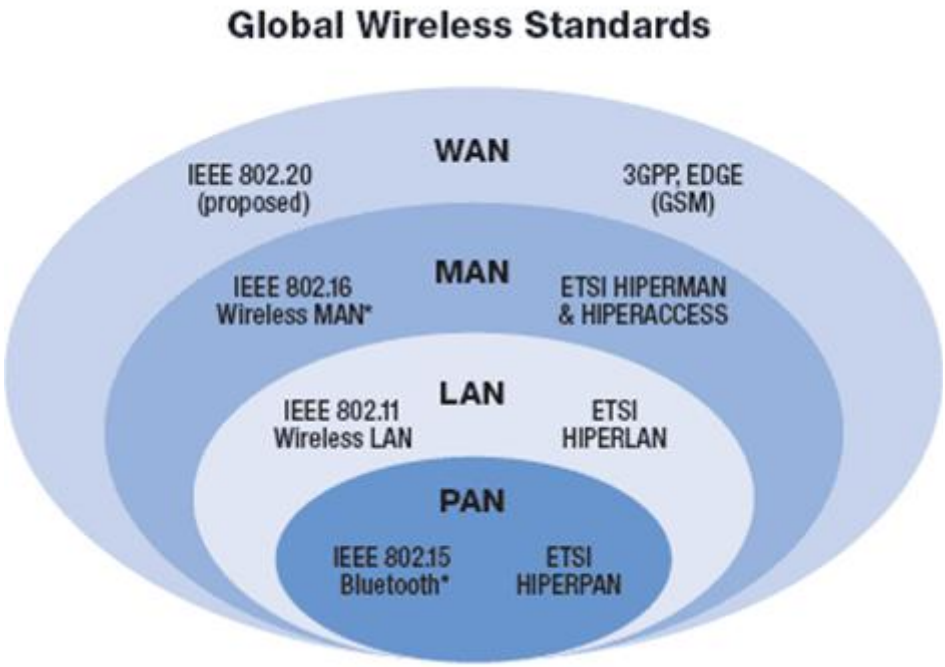
1. Permitir a los empleados de una empresa la posibilidad de intercambiar archivos entre las distintas computadoras sin necesidad de utilizar, disquetes, CDs, etc., y sin tener que abandonar el puesto de trabajo.

2. Debido a que los empleados de la empresa podrían necesitar trabajar con su computadora en distintas oficinas, una posible solución es que análogamente a la red eléctrica, sólo se necesite conectar la misma a un enchufe, independiente de cual sea la oficina en la que se encuentre el empleado.

Clasificación de Redes

Por tamaño

Una posible clasificación de la redes es por su tamaño debido a que según el tamaño de la red el diseño de la misma puede variar. Así obtenemos la clasificación de las redes en redes LAN, WAN y MAN.



Redes LAN

Las redes de área local, generalmente llamadas LAN (Local Area Networks), son redes de propiedad privada que operan dentro de un solo edificio o en edificios cercanos. Las redes LAN se utilizan ampliamente para conectar computadoras personales y electrodomésticos con el fin de compartir recursos (por ejemplo, impresoras) e intercambiar información. Estas redes tienen distancias cortas entre los nodos (dispositivos conectados), lo que les permite alcanzar altas velocidades de transmisión a costos moderados. Como ejemplo, la red en la que no encontramos cuando llegamos a trabajar a nuestra oficina es una red LAN.

Redes WAN

Una Red de Área Amplia, o WAN (Wide Area Network), abarca una extensa área geográfica, como ser un país o continente, un ejemplo de esto son las empresas con varias sucursales interconectadas. Sus velocidades de transmisión son menores que las LAN.

Redes MAN

Una Red de Área Metropolitana, o MAN (Metropolitan Area Network), cubre ciudades o zonas comerciales.

Por Forma de trabajo

Cliente Servidor

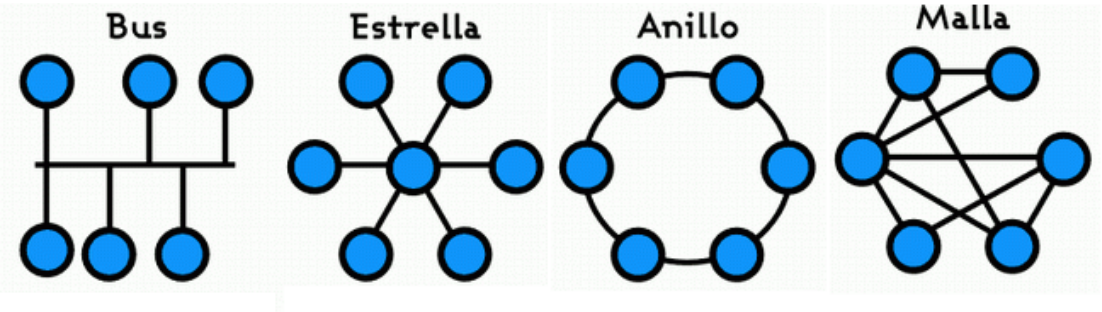
Una computadora es un cliente cuando usa recursos e información de otra computadora de la red, y es un servidor cuando tiene como única función ofrecer sus recursos e información a otro dispositivo de la red. Por ejemplo los servidores de páginas web.

Entre Iguales

Cualquiera de los dispositivos conectados puede actuar como cliente y como servidor, proporcionando recursos y utilizando recursos de otros dispositivos. Como ejemplo de aplicaciones en este tipo de redes tenemos las conocidas como eMule, Kazaa, etc., en las cuales cualquiera de los usuarios que participar con su computadora es servidor y cliente a la misma vez ya que sobre estas redes se comparten los diferentes archivos entre sus usuarios ofreciendo la posibilidad de solicitar y brindar información entre todos.

Clasificación por topología

La topología de red es la forma en que está diseñada la red, en el plano físico o lógico. La topología de red la determina únicamente la configuración de las conexiones entre nodos. La distancia entre los nodos, las interconexiones físicas, las tasas de transmisión y los tipos de señales no pertenecen a la topología de la red, aunque pueden verse afectados por la misma.



Bus

Todas las computadoras se conectan a un único cable que propaga las señales en ambas direcciones.

Estrella

Todas las computadoras se conectan a un circuito central llamado concentrador (o HUB) que recibe la señal enviada y la hace llegar al resto.

Anillo

Las computadoras se conectan secuencialmente unas a otras formando un anillo cerrado. Cuando una computadora transmite una señal a otra, le entrega la información a la siguiente y así hasta que llega a destino.

Malla

Cada nodo está conectado a todos los nodos. De esta manera es posible llevar los mensajes de un nodo a otro por distintos caminos.

Topología física y lógica

Dentro del concepto de topología se pueden diferenciar dos aspectos bien marcados, la topología física y la topología lógica.

Mientras la topología física se refiere a la disposición física de los dispositivos de red y su cableado, la topología lógica se refiere al trayecto seguido por las señales a través de la topología física. Esto es una red puede estar conectada con determinada topología física y funcionar mediante una topología lógica diferente. Un ejemplo de esto que se vera más adelante es la conexión ethernet mediante HUB, que se conecta físicamente en estrella, pero funciona lógicamente como bus.

Modelo teórico de capas

Por mucho tiempo se desarrollaron redes utilizando hardware y software incompatibles entre si, en su gran mayoría eran propietarios y por tanto controlados por organizaciones, resultando dificultosa su interconexión. Para tratar de solucionar el problema la ISO desarrolló un modelo abierto y dividido en capas que facilitó la implantación de redes interoperables y de fácil comunicación entre ellas. Tiempo después, el Departamento de Defensa de EEUU creó el modelo TCP/IP.
El modelo OSI, creó una referencia para entender como viajan los datos desde una aplicación en un PC hacia otra en otro PC, pasando por redes intermedias con diferentes medios de comunicación, tipos de dispositivos, sistemas operativos, etc.

Por qué un modelo en capas:

- Permite dividir la complejidad de una comunicación de un equipo a otro en partes simples
- Permite la interoperatividad de distintos fabricantes
- Permite la normalización de tecnologías
- Permite la evolución independiente de cada capa

Protocolo

Un Protocolo de Comunicación es un conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación entre las entidades que forman parte de una red.
En Informática y Telecomunicaciones, un protocolo es una convención, o estándar, o acuerdo entre partes que regula la conexión, la comunicación y la transferencia de datos entre dos sistemas.
En su forma más simple, un protocolo se puede definir como las reglas que gobiernan la semántica (significado de lo que se comunica), la sintaxis (forma en que se expresa) y la sincronización (quién y cuándo transmite) de la comunicación.

Servicio

Un servicio es un conjunto de operaciones. Cada capa del modelo tiene como cometido brindar un servicio a la capa que está encima de ella, y consumir servicios de la capa debajo de ella. Para ello se definen puntos de interconexión, para que las capas tengan acceso a dichos servicios.

Interfaz

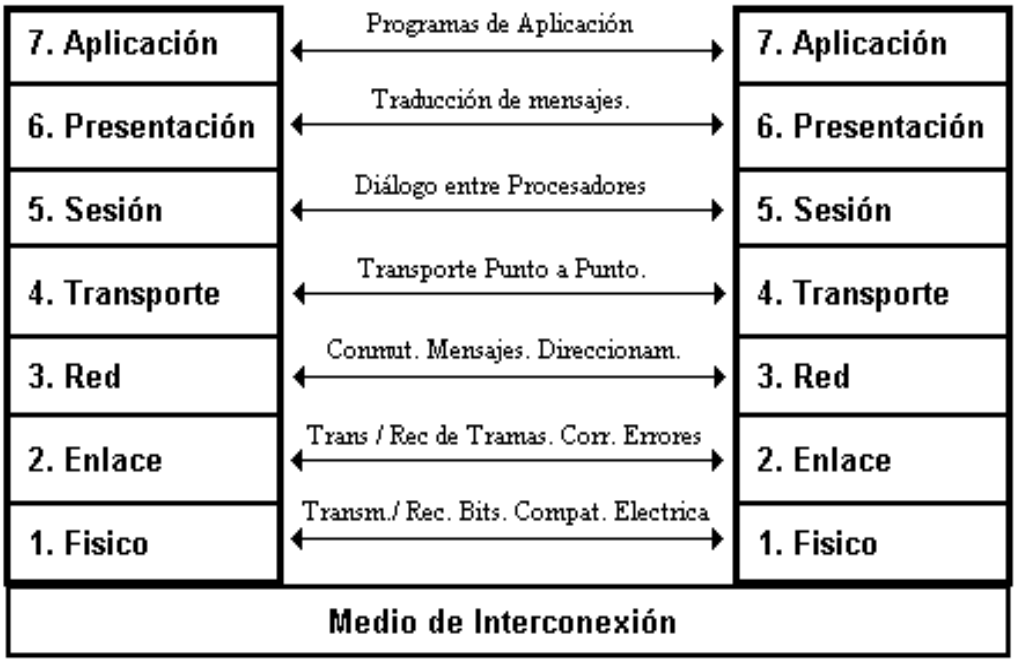
Una interfaz es un límite compartido a través del cual dos componentes diferentes de un sistema de computadoras intercambian información.

Entidades pares

A su vez, para que la información pueda llegar hasta el destino, cada capa del modelo intercambia información con la capa al mismo nivel en el destino. Esta comunicación se denomina, comunicación entre capas o entidades pares.

Modelo OSI de siete capas

El modelo OSI se basa en una propuesta desarrollada por la Organización Internacional de Normas (ISO) como el primer paso hacia la estandarización internacional, y se compone de siete capas, que se analizan a continuación.



Capa de aplicación

Es la capa que suministra servicios a las aplicaciones del usuario.

Capa de presentación

La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común.

Capa de sesión

Como su nombre lo implica, la capa de sesión establece, administra y finaliza las sesiones entre dos hosts que se están comunicando.

Capa de transporte

La capa de transporte segmenta los datos originados en el host emisor y los re-ensambla en una corriente de datos dentro del sistema del host receptor.

Capa de red

La capa de red es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas.

Capa de enlace de datos

La capa de enlace de datos proporciona un tránsito de datos confiable a través de un enlace físico.

Capa física

La capa física se relaciona con la transmisión de bits puros a través de un canal de transmisión.

El Modelo TCP/IP y el modelo híbrido

TCP/IP

El modelo TCP/IP está compuesto de cuatro capas, las cuales son:

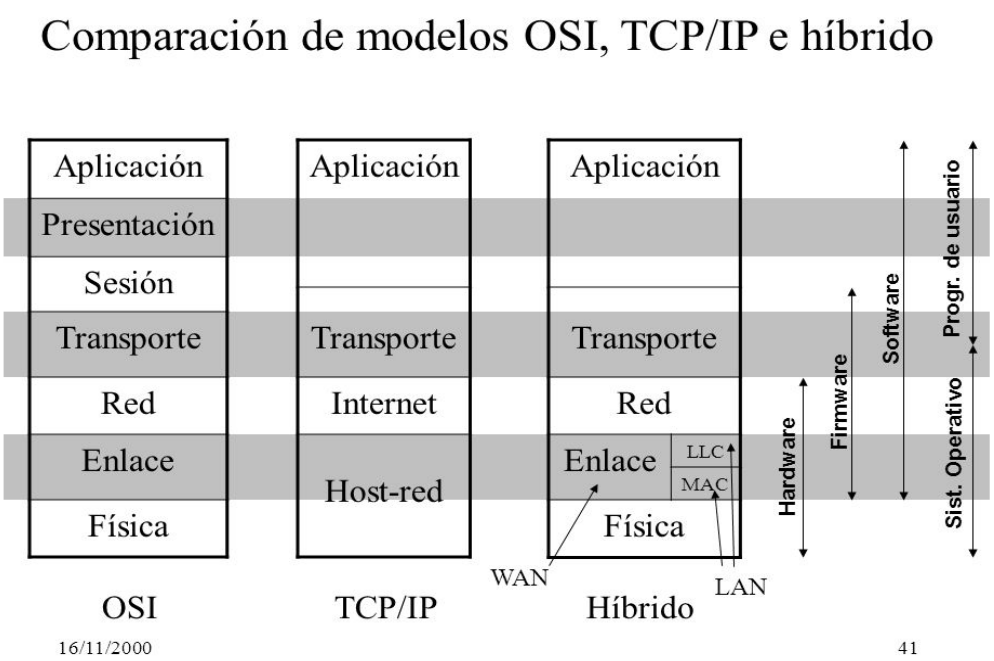
- La capa de aplicación
- La capa de transporte
- La capa de Internet
- La capa de red

Este modelo es el que sirvió para el desarrollo de Internet y el modelo OSI se utiliza como referencia teórica.

Modelo Híbrido

También existe un modelo híbrido, que es el se usa habitualmente. Este está compuesto de cinco capas, las cuales son:

- La capa de aplicación
- La capa de transporte
- La capa de red
- La capa de enlace
- La capa física



Teniendo en cuenta el modelo híbrido, cuando un PC u otro equipo quiere enviar información a otro, los datos deben atravesar cada una de las capas del modelos, tanto en el origen como en el destino. En este proceso, a la información original se le agrega datos que son de utilidad para cada uno de los protocolos que se ejecutan en las capas del modelo. Este proceso de denomina encapsulamiento de datos. A continuación se describen la información más importante que se agrega en cada capa:

- Los datos provenientes de una aplicación del usuario en la capa de transporte se le agrega información como ser el puerto de origen y de destino. Esa unidad de información resultante se denomina segmento.
- A su vez, a dichos segmentos se le agrega información, entre otras cosas, de direccionamiento y se convierten en paquetes.
- Luego, en la capa de enlace de datos, los paquetes se convierten en frames y se adaptan al medio.
- Por último, los frames se convierte en un flujo de bits que se transmite por un medio de comunicación.

Protocolos por capa

- **En capa de aplicación**
  - Hypertext Transfer protocol - HTTP (Protocolo de transferencia de hipertexto)
  - File Transfer Protocol - FTP (Protocolo de transporte de archivos)
  - Domain Name Service - DNS (Servicio de nombre de dominio)

- **En capa de transporte**
  - Transport Control Protocol – TCP (Protocolo de control de transmisión)
  - UDP
  - En capa de red
  - Internet Protocol – IP (Protocolo Internet)

- **En capa de enlace**
  - Ethernet

Capa Física

La función de la capa física es definir todos los detalles para transmitir los bits desde un dispositivo a otro. Por ejemplo la longitud máxima permitida por cada tipo de cable, cantidad de hilos por cada cable, la forma de los conectores, la función de cada uno de los pines de los conectores, o determinar que medios de transmisión utilizar.

Medios de transmisión guiados

Los tipos de medios de transmisión guiados son son aquellos que utilizan un medio sólido para la transmisión, como ser cables coaxiales, pares de cobre o fibra óptica.

Elección del medio adecuado

Para elegir el tipo de medio adecuado se deben considerar aspectos tales como el tipo de dispositivos conectados, la carga de la red, la distancia máxima entre Switches y Pcs, los niveles de interferencia (EMI) presentes, así como requerimientos de seguridad, posibles cambios en el/los equipo/s y otros factores relativos al costo, reusabilidad y tiempo de vida de la red.

Cables coaxiales

Un cable coaxial consiste en alambre de cobre rígido como núcleo, rodeado por un material aislante. El aislante está forrado de un conductor cilíndrico, que por lo general es una malla de tejido fuertemente trenzado. El conductor externo está cubierto con una funda protectora de plástico.

Cables de par trenzados

El estándar donde se especifican las distancias máximas para cableados estructurado (pares trenzados) es la ISO/IEC IS 11801
Los Cables de par trenzado se clasifican según:

1. STP (Shielded Twisted Pair – Par trenzado apantallado).
2. FTP (Foil Screened cable) – Cable Recubierto con lámina de aluminio.
3. UTP (Unshielded Twisted Pair – Par trenzado NO apantallado).

STP

Los cables STP están embutidos en una malla metálica global y tiene una pantalla individual por cada par trenzado, lo que los hace más inmunes a la interferencia, aunque asociado a un costo mas elevado y a una mayor complejidad de instalación al ser más grueso y menos flexible.

FTP

Los cables FTP están compuestos por 4 pares trenzados rodeados por una pantalla metálica, lo que lo hace mas compacto que el STP.

UTP

Las principales características del UTP son su precio y la facilidad de instalación. Además permiten velocidades de datos de hasta 1 Gbps. Son los más utilizados en redes LAN.

Categorías Cables UTP

Las categorías son definidas en los estándares ISO/IEC IS 11801 y TIA/EIA 568B.

TIA/EIA se refiere tanto al componente como a la performance punta a punta como categoría, en cambio el estándar ISO/IEC se refiere a los componentes como categoría y a la performance como clase. A continuación hay una tabla de las categorías, su uso y ancho de banda máximo.

Cuadro 1. Categorías del cable par trenzado UTP

Categoría	Uso	Ancho de Banda
CAT 1	Voz solamente (cable telefónico)	-
CAT 2	Datos hasta 4 Mbps (Localtalk, Apple)	-
CAT 3	Datos hasta 10 Mbps (Ethernet 10Base-T)	16 MHz
CAT 4	Datos hasta 20 Mbps (Token Ring)	20 MHz
CAT 5	Datos hasta 100 Mbps (FastEthernet 100Base-T)	100 Mhz
CAT 5e	Datos hasta 1000 Mbps (Gigabit Ethernet 1000Base-T)	100 MHz
CAT 6	Datos hasta 10 Gigabits (10GBase-T)	250 MHz

**Todas las especificaciones están acotadas a 100 metros*

Conectores UTP

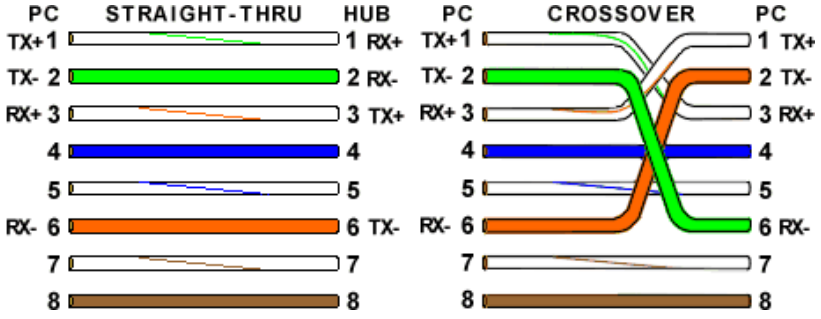
RJ-45

El conector RJ45, es el conector típicamente usado en redes Ethernet. Tienen 8 pines, donde el 1 y 2 son usados para transmisión de datos y los pines 3 y 6 son usados para la recepción de datos.

RJ-45 Cruzado

Los "Crossover Ethernet Cable" se utilizan para comunicar directamente dos PCs o Hubs, en cambio los "Straight-through cable" se utiliza para conectar un PC con un Hub/Switch.

En la actualidad muchas de las tarjetas de red reconocen si necesitan un cable cruzado y "se cruzan" para poder utilizar cables RJ-45 normales.



Fibra óptica

Las fibras ópticas en mono-modo llegan a trasmitir datos a una velocidad de más de 50 Gbps hasta 100 Km. sin amplificar. El rayo de luz cuando pasa de un medio a otro se refracta según el ángulo de incidencia y depende de las propiedades de ambos medios. Si el ángulo con que incide el rayo de luz es mayor que un cierto ángulo crítico, entonces el rayo queda atrapado dentro de la fibra y no se pierde energía.

Si el diámetro de la fibra se reduce a unas cuantas longitudes de onda de luz, se transforma en una guía de onda y la luz se propaga en línea recta sin rebotar, dando como resultado a la fibra mono-modo. De esta forma se alcanza mayores distancias pero el costo es mayor.

Las conexiones de fibra pueden incluir dos hilos de fibra, uno para transmisión y otro para recepción, o como en el caso de FTTH una sola fibra que transmite en una longitud de onda y recibe en otra.

Conectores de Fibra Óptica

Existen varios conectores de fibra, entre los mas usados están el ST, SC y LC.

Transmisión WAN

Cuando los puntos a conectar son muy distantes, Ethernet no soporta cables para tal distancia. Además hay que tener permiso para por ejemplo enterrar los cables en una ciudad. Esta es la diferencia entre una LAN y una WAN. La LAN se utiliza en un edificio o un complejo, utilizando si es necesario un tendido de fibra óptica. Para implementar una WAN se necesita tener derechos de pasar los cables bajo tierra atravesando ciudades, etc. Las empresas que necesitan utilizar éstas líneas de larga distancia las arriendan "leased line". Ejemplo: a Antel. La empresa propietaria de la WAN.

Capa de enlace de datos

La tarea de la capa de enlace de datos es convertir el flujo de bits en bruto ofrecido por la capa física en un flujo de tramas para que la capa de red lo utilice. La capa de enlace puede presentar este flujo con niveles variables de confiabilidad, desde un servicio sin conexión ni confirmación de recepción hasta un servicio confiable, orientado a conexión.

Funciones de la capa de enlace

En la "capa 2" se definen Protocolos y estándares utilizados para controlar la transmisión de datos a través de la capa física. Se definen muchas funciones cuyos detalles de la implementación de los protocolos va a depender del tipo de red de capa física. Independiente del tipo de red física, todos los protocolos realizan las siguientes funciones:

Arbitraje

Existen protocolos en la capa de enlace que permite arbitrar la utilización de la red física para evitar o recuperarse de las colisiones (un análogo a como las reglas de transito aplican al transito urbano). En una red Ethernet, el algoritmo de arbitraje utilizado es el CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

Direccionamiento

Los protocolos de enlaces de datos definen las direcciones para asegurar que escuche y reciba los datos el dispositivo al cual le fue enviado. Se le pone en el "Header" del frame la dirección indicada. Cada protocolo de enlace define su propio estructura de direcciones (que debe de ser única).

Ejemplo: Ethernet utiliza MAC con 6 bytes, y Frame Relay utiliza DLCI con 10 bits.

Detección de Errores

Los protocolos de enlace necesitan una función que detecte si ocurrieron errores en los datos transmitidos. La mayoría de los protocolos utilizan FCS (Frame Check Sequence) or CRC (Cyclical Redundancy Check) como algoritmo para detectar errores. La recuperación de los datos no se realiza en la capa de enlace, sino que se implementa en la capa de Transporte (TCP). Para eso, se identifican los datos encapsulados.

Identificación de tipo de encapsulado

Por ejemplo se utiliza el protocolo LLC que cuenta con un campo "header" que indica el tipo de datos que tiene empaquetado, permitiendo así que sea dirigido como corresponde.

Ethernet

Ethernet, es una familia de protocolos de capa física y capa de enlace. La primera Ethernet surgió como "DIX Ethernet" (DEC, Intel, Xerox). En 1980 IEEE estandarizó la primera versión de Ethernet.

La Ethernet clásica utiliza el algoritmo CSMA/CD persistente. Este descriptor tan sólo significa que las estaciones "escuchan" el medio cuando tienen una trama que desean enviar, y la envían tan pronto como el medio está inactivo. Monitorean el canal por si hay colisiones al momento en que envían. Si hay una colisión, abortan la transmisión con una señal de bloqueo corta y vuelven a transmitir después de un intervalo aleatorio.

Si no hay colisión, el emisor supone que la trama se entregó con éxito, ya que ni CSMA/CD ni Ethernet proveen confirmaciones de recepción. Esta elección es apropiada para los canales de cable de cobre y de fibra óptica que tienen tasas de error bajas, y cualquier error que ocurra debe entonces detectarse mediante la CRC y recuperarse en las capas superiores.

Ethernet utiliza los protocolos MAC (Media Access Control) – IEEE 802.3, y LLC (Logical Link Control) – IEEE 802.2 de capa de enlace.

10Base5 y 10Base2

Las redes 10BASE5 y 10BASE2 difieren en detalles del cableado. En ambas redes NO existen Hubs, Switch, etc., solo consisten de tarjetas Ethernet en los PCs y el cableado. Los cables crean un bus común que es compartido entre todos los dispositivos de la red. Cuando un dispositivo quiere enviar bits a otro dispositivo, transmite la señal eléctrica que se propaga por toda la red y son escuchados todos los dispositivos.

10BaseT

Las redes 10BASE-T Utilizan un Hub, cuentan con una topologia física en estrella aunque lógicamente funciona como un Bus, tiene mayor disponibilidad respecto a las 10BASE2 y 10BASE5 ya que si cae el cable entre un PC y el Hub el resto de las conexiones siguen disponibles. Como el

Hub repite todo lo que escucha, continua el mismo concepto de compartir el canal físico.

HUB

Un HUB es un dispositivo que permite conectar varias PC en forma independiente sin alterar las conexiones existentes, su funcionamiento es el siguiente:

1. La tarjeta de red del "PC1" envía un frame
2. La tarjeta de red envía el frame en loop internamente hacia el receptor
3. El Hub recibe el frame
4. El cableado interno del Hub propaga la señal eléctrica a todos los otros puertos del Hub.
5. La señal se repite a cada uno de los otros dispositivos conectados al Hub

Si ahora otro PC "PC2" envía un frame al mismo tiempo, entonces el Hub repite ambas señales superpuestas a todas las NIC (tarjetas de red). Las PC1 y PC2 detectan la colisión y esperan un tiempo aleatorio para enviar nuevamente el frame.

Colisiones

Con la utilización de Hubs, no se alcanza el 100% de utilización en la red y la performance se degrada al aumentar la utilización, ya que continúa habiendo colisiones (y estas aumentan con la cantidad de conexiones) y se sigue utilizando el algoritmo CSMA/CD.
Se define dominio de colisiones, como el conjunto de dispositivos cuyos frames pueden colisionar, por lo que una solución al problema anterior es un dispositivo lo suficientemente inteligente como para evitar o disminuir las colisiones restringiendo el dominio de colisiones y dejar de utilizar el algoritmo CSMA/CD.

Switches

Un Switch (o puente) trata a cada puerto físico individual como un bus separado y contiene buffers de memoria, tal que, si dos PCs envían un frame al mismo tiempo, el Switch reenvía uno hacia el destino especificado y mantiene en memoria al otro frame hasta que el primero haya sido recibido. De esta forma las colisiones pueden ser evitadas. El Switch en

diferencia con el Hub, "solo" reenvía el frame por el puerto donde se encuentra conectado el dispositivo al que se le envía el frame.

Half Duplex / Full Duplex

Cuando un dispositivo en una Ethernet original que no utiliza Switch, necesita enviar un frame, tiene que esperar el momento en que no esté recibiendo un frame, de lo contrario se produciría una colisión (Half Duplex)

Las redes Ethernet que utilizan Switch, permiten enviar múltiples frames sobre diferentes puertos al mismo tiempo. Además, estando conectado un solo dispositivo a un puerto, dicho dispositivo puede enviar y recibir frames al mismo tiempo (Full Duplex). Esto significa que la NIC permite enviar y recibir frames al mismo tiempo.

Direccionamiento

En Ethernet se puede direccionar a un único dispositivo (UNICAST) o a un grupo (MULTICAST).

La dirección de una NIC tiene una longitud de 6 bytes que usualmente está escrita en hexadecimal separada de a 4 dígitos (Ejemplo:0000.0C13.4586).

Contrapuesto a la UNICAST se encuentran las direcciones "Group Address" que incluyen las BROADCAST y MULTICAST. Las direcciones UNICAST se utilizan para identificar tanto al que envía como al que recibe el frame.

En el Header del frame se encuentran dos campos, uno con la dirección del origen, y otro con la dirección del destino. Las direcciones son conocidas como MAC Address y su nombre se debe a que en el protocolo MAC (IEE 802.3) se definen los detalles del direccionamiento de Ethernet. Se requiere que la MAC Address sea única. La dirección MAC es grabada en memoria ROM dentro de la tarjeta.

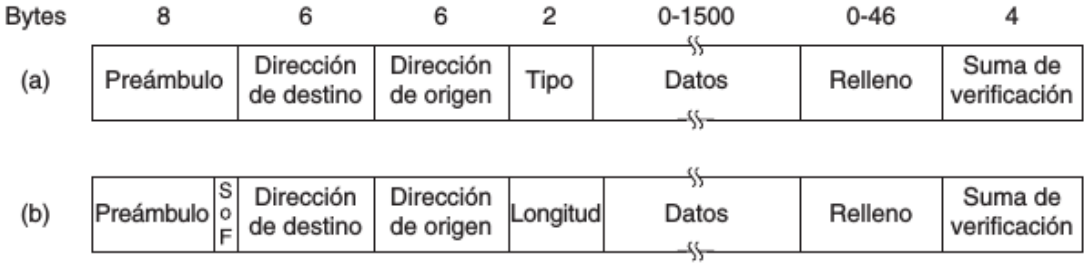
La primera mitad de la dirección identifica al fabricante (OUI). La segunda mitad identifica a una tarjeta en particular, con un número que el fabricante no haya utilizado.

- GROUP ADDRESSES: Identifican más de una tarjeta de red y se subdividen en dos categorías: BROADCAST ADDRESSES y MULTICAST ADDRESSES
- BROADCAST ADDRESSES: Indica que todos los dispositivos de la LAN pueden procesar el frame. El valor es FFFF.FFFF.FFFF.FFFF
- MULTICAST ADDRESSES: Es una dirección utilizada para que solo un subgrupo de los dispositivos de una LAN reciban el frame.

El protocolo IP utiliza Multicast addresses, y cuando está sobre una LAN Ethernet utiliza la MAC address que tiene el formato: "0100.5exx.xxxx" donde las x pueden tomar cualquier valor.

Trama de Ethernet

El Framing (o trama) le da un significado a cada uno de los bits transmitidos en un frame. Cuando un dispositivo recibe una trama en la capa física, ésta no interpreta dichos bits, sino que se lo pasa a la capa de enlace quien conoce el significado de cada uno de los bits. Por ejemplo la IEEE 802.3 define la ubicación de los campos (conjunto de bits) dentro del flujo de bits de un frame.



(a) Trama Ethernet DIX (b) Trama Ethernet 802.3

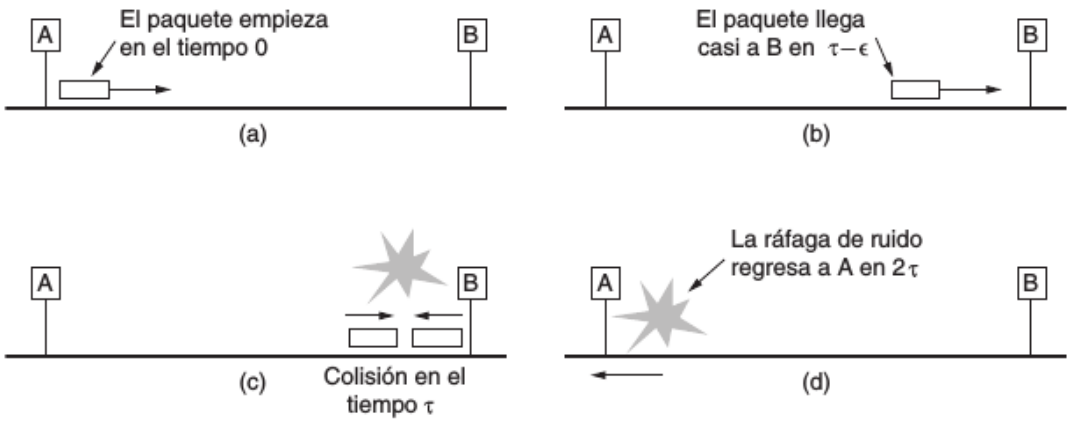
El formato utilizado para enviar tramas se muestra en la figura anterior. Primero viene un Preámbulo de 8 bytes, cada uno de los cuales contiene el patrón de bits 10101010 (con la excepción del último byte, en el que los últimos 2 bits se establecen a 11). Este último byte se llama delimitador de Inicio de trama en el 802.3. Los últimos dos bits indican al receptor que está a punto de empezar el resto de la trama.

Después vienen dos direcciones, una para el destino y una para el origen (en un analogo a una carta postal donde se fija el destinatario y el remitente), cada una de ellas tiene una longitud de 6 bytes. El primer bit transmitido de la dirección de destino es un 0 para direcciones ordinarias y un 1 para direcciones de grupo. La dirección especial que consiste únicamente en bits 1 está reservada para difusión (BROADCAST). Una trama que contiene sólo bits 1 en el campo de destino se acepta en todas las estaciones de la red. La multidifusión es más selectiva, pero involucra el manejo de grupos para definir qué estaciones están en un grupo. Por el contrario, la difusión no hace ninguna diferencia entre las estaciones, por lo que no requiere manejo de grupos.

Una característica interesante de las direcciones de origen de las estaciones es que son globalmente únicas; el IEEE las asigna de manera central para asegurar que no haya dos estaciones en el mundo con la misma dirección.
A continuación está el campo Tipo o Longitud, dependiendo de si la trama es Ethernet o IEEE 802.3. Ethernet usa un campo Tipo para indicar al receptor qué hacer con la trama. Es posible utilizar múltiples protocolos de capa de red al mismo tiempo en la misma máquina, por lo que cuando llega una trama de Ethernet, el sistema operativo tiene que saber a cuál entregarle la trama. El campo Tipo especifica a qué proceso darle la trama. Por ejemplo, un código de tipo de 0x0800 significa que los datos contienen un paquete IPv4.

Después están los datos, de hasta 1500 bytes, además de haber una longitud de trama máxima, también hay una longitud mínima. Si bien algunas veces un campo de datos de 0 bytes es útil, causa problemas. Cuando un transceptor detecta una colisión, trunca la trama actual, lo que significa que los bits perdidos y las piezas de las tramas aparecen todo el tiempo en el cable. Para que Ethernet pueda distinguir con facilidad las tramas válidas de lo inservible, necesita que dichas tramas tengan una longitud de por lo menos 64 bytes, de la dirección de destino a la suma de verificación, incluyendo ambas. Si la porción de datos de una trama es menor que 46 bytes, el campo de Relleno se utiliza para completar la trama al tamaño mínimo.

Otra razón para tener una trama de longitud mínima es evitar que una estación complete la transmisión de una trama corta antes de que el primer bit llegue al extremo más alejado del cable, donde podría tener una colisión con otra trama. Para agregar algún margen de seguridad, este número se redondeó a 512 bits o 64 bytes. Este problema se ilustra en la figura a continuación.



El campo final de es la Suma de verificación. Esta CRC es un código de detección de errores que se utiliza para determinar si los bits de la trama se recibieron correctamente. Sólo realiza detección de errores y la trama se desecha si se detecta uno.

Fast Ethernet

Se definió en el estándar IEEE 802.u y mantiene muchas de las características de la IEEE.3 Aunque existe el algoritmo CSMA/CD, se puede deshabilitar cuando se utiliza una topología punto a punto Full Duplex. Utiliza el mismo Header y Trailer que el 802.3 (MAC) y 802.2 (LLC) Permite una amplia variedad en el cableado, tal como fibra óptica single y multimodo.

El diseño 100BASE-TX utiliza un cableado UTP Categoría 5, mientras que 100BASE-T4 utiliza categoría 3 (difiere en que el T4 requiere 4 pares trenzados mientras que el TX requiere solo 2 pares la cantidad de pares). Ambos se conocen en conjunto como 100BASE-T. El diseño con fibra óptica 100BASE-FX utiliza dos filamentos de fibra multimodo llegando a una distancia de hasta 2 km.

Nombre	Cable	Segmento máximo	Ventajas
100Base-T4	Par trenzado	100 m	Utiliza UTP categoría 3.
100Base-TX	Par trenzado	100 m	Full-dúplex a 100 Mbps (UTP cat 5).
100Base-FX	Fibra óptica	2000 m	Full-dúplex a 100 Mbps; distancias largas.

Giga Ethernet

Se define en el estándar IEEE 802.3z para fibra óptica. Mantiene muchas características de las Ethernet anteriores. CSMA/CD aún es utilizado, pero puede ser deshabilitado. Utilizan el mismo Header y Trailer que las Ethernet más viejas. Uso más frecuente: entre Switches, Switches y Routers, o Switches y Servidores. La gran diferencia es la velocidad más rápida de 1 Gbps (1000 Mbps).

Nombre	Cable	Segmento máximo	Ventajas
1000Base-SX	Fibra óptica	550 m	Fibra multimodo (50, 62.5 micras)
1000Base-LX	Fibra óptica	5000 m	Monomodo (10 µ) o multimodo (50, 62.5µ)
1000Base-CX	2 pares de STP	25 m	Par trenzado blindado
1000Base-T	4 pares de UTP	100 m	UTP estándar categoría 5

1000BASE-LX utiliza fibra óptica y si utiliza multimodo llega hasta una distancia de 550 metros, mientras que si utiliza modo simple puede llegar hasta una distancia de 5 km. 1000BASE-SX utiliza fibra óptica multimodo llega hasta una distancia de 550 metros. 1000BASE-CX utiliza dos pares STP llegando a 25 metros. 1000Base-T utiliza cuatro pares UTP categoría 5 alcanzando los 100 metros.

Capa de Red

Si las redes fueran puramente de capa 2 no serían escalables, dado que existiría una única gran red que tendría los siguientes problemas:

- Dominios de colisión muy grandes
- Tormentas de broadcast
- Problemas de Seguridad
- Problemas de escalabilidad

Los dominios de colisión muy grandes congestionan las redes e impiden las comunicaciones, ya se estudió en el capitulo anterior que este problema se puede resolver utilizando una red de capa 2 switcheada. Por otro lado, aún subsiste el problema que generan los broadcast Ethernet en la red, dado que los mismos se envían a todos los dispositivos y la suma de todos los broadcast generados, por las aplicaciones, congestionan los enlaces impidiendo las comunicaciones.

También por motivos de seguridad es importante agrupar equipos y separarlos de otros. Por tanto, es necesario un protocolo en una capa superior que soluciones estos problemas y permita escalabilidad.
Si una red tuviera un esquema de direccionamiento plano, como es Ethernet, sería poco eficiente buscar un equipo en particular. Entonces, para que la misma sea eficiente, se definen jerarquías que faciliten las búsquedas. Para ello, en el protocolo IP existen subredes que permiten agrupar los equipos de forma análoga a lo que es el sistema telefónico, donde con los primeros números telefónicos (característica) se puede saber a que localidad pertenece.

Routers

Los router son dispositivos que operan a nivel de capa de red y cuyas funciones son:

- Interconectar subredes – los router tienen interfaces que permiten conectarse a los distintos tipos de redes y permiten el intercambio de información entre estas.
- Determinar la mejor ruta para el flujo información – para esto los routers ejecutan aplicaciones que se llaman protocolos de ruteo, que les permiten tener información del estado de todas las posibles rutas para llegar hacia los destinos y a partir de ellas determinar cual o cuales son las mejores. Para esto es fundamental el esquema

jerárquico, lo cual permite identificar en que red se encuentra el equipo de destino basándose solo en la porción de subred.

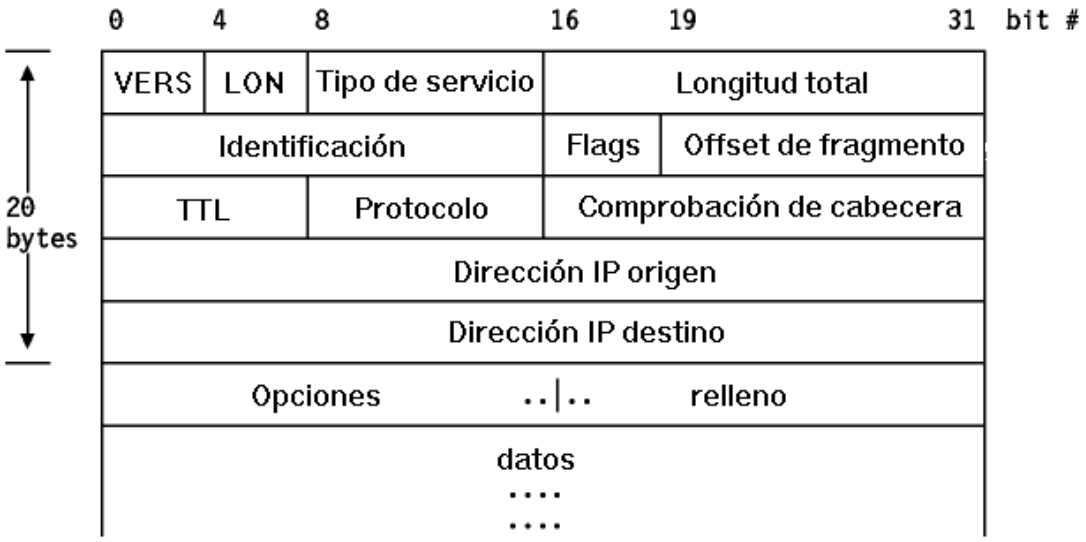
- Detener los broadcast generados por las distintas aplicaciones. Muchos servicios realizan periódicamente broadcast anunciándose, estos broadcast llegan a todos los equipos de una red. Cuanto mayor sea el número de equipos, en una red, mayor será el trafico de broadcast y por tanto habrá más congestiones. Por tal motivo, los diseñadores de red deben reducir el tamaño de los dominios de broadcast, para ello se pueden utilizar routers.

Protocolo IP

El protocolo IP es el que se usa en la capa 3 y se popularizo dado que es el utilizado en Internet. A medida que la información fluye por las distintas capas del modelo OSI, los datos se encapsulan en cada capa. En particular en la capa de red, los datos se encapsulan en paquetes en donde se les agrega un encabezado que incluye información de dirección de origen y de destino, entre otras cosas.

En la figura a continuación se muestran el formato del paquete IP (versión 4), los campos más importantes son:

- Dirección IP de origen (32 bits)
- Dirección IP de destino (32 bits)
- Type of service (ToS) – Tipo de servicio
- Time To Live (TTL) – Tiempo de vida



Direccionamiento IPv4

Las direcciones IPv4 (IP versión 4) tienen una longitud de 32 bits, generalmente estos se convierten a decimal y se representan utilizando 4 números, del 0 al 255, separados por puntos. Por tanto, las direcciones IP válidas van desde 0.0.0.0 al 255.255.255.255.

Toda dirección IP consta de dos partes una parte de red y otra parte de host. La parte de red es la que permite la agrupación jerárquica de los equipos y el resto es la que determina cuantos equipos puede haber en esa red.

Para hallar cual es la porción de red y cual es la de host en una dirección IP existe la máscara de red que también tiene un largo de 32 bits y se representan de igual manera que las direcciones de host. Los bits unos en la máscara indican la porción de red, mientras que los ceros la de host. Si dos equipos tienen la misma mascara y coincide su dirección de red, entonces están en la misma red.

Una forma de notación alterna a notar la dirección de host y la mascara es la notación CIDR que permite identificar la mascara haciendo referencia a cuantos de los bits de una dirección se utilizan para la mascara. Por ejemplo en una dirección /8, implica una máscara 255.0.0.0.

Direcciones de Red y Broadcast

Dentro de toda red hay dos direcciones que están reservadas y no se pueden asignar a ningún equipo, ellas son la dirección de red y la de broadcast.

- La dirección de red identifica a la red y tiene la particularidad que en la parte de host todos los bits son cero.
- La dirección de broadcast tiene todos los bits en unos en la parte de host y permite enviar un paquete a todos los equipos de una red.

A modo de ejemplo, en la red 192.168.3.0 con mascara 255.255.255.0, la dirección de red es 192.168.3.0 y la de broadcast es 192.168.3.255. Para hallar la cantidad de direcciones que se pueden utilizar se puede usara la regla de "cantidad de equipos = 2 *n - 2" donde n es la cantidad de bits de la porción de host.

Clases IPv4

Las direcciones IP se dividen en varias clases de acuerdo al largo de su dirección de red. Las clases más conocidas son:

- A van desde la dirección 0.0.0.0 hasta la 126.255.255.255 con mascara 255.0.0.0 (/8)
- B van desde la dirección 128.0.0.0 hasta la 191.255.255.255 con mascara 255.255.0.0 (/16)
- C van desde la dirección 192.0.0.0 hasta la 223.255.255.255 con mascara 255.255.255.0 (/24)

CLASE	DIRECCIONES DISPONIBLES		CANTIDAD DE REDES	CANTIDAD DE HOSTS	APLICACIÓN
	DESDE	HASTA			
A	0.0.0.0	127.255.255.255	128*	16.777.214	Redes grandes
B	128.0.0.0	191.255.255.255	16.384	65.534	Redes medianas
C	192.0.0.0	223.255.255.255	2.097.152	254	Redes pequeñas
D	224.0.0.0	239.255.255.255	no aplica	no aplica	Multicast
E	240.0.0.0	255.255.255.255	no aplica	no aplica	Investigación

* El intervalo 127.0.0.0 a 127.255.255.255 está reservado como dirección loopback y no se utiliza.

Subredes

Dado que la división inicial de clases es poco eficiente a la hora de asignar direcciones, se crearon las subredes. Las mismas permiten administrar de forma más flexible las direcciones IP. Para crear una dirección de subred, se pide "prestados" bits del campo de host y los designa como campo de subred. A modo de ejemplo, para la clase C 192.168.3.0 / 24 en la que se puede crear una red de 253 equipos se puede tener por ejemplo, si pedimos prestado un bit, 2 redes de 125 equipos y en este caso las redes son 192.168.3.0/25 y 192.168.3.128/25.

Direcciones Privadas

A fin de aprovechar mejor las direcciones IP, se definen rangos de direcciones para redes privadas, estas direcciones no se utilizan en la red pública (ej. Internet), y se pueden repetir en diferentes redes privadas:

- 10.0.0.0 – 10.255.255.255/8
- 172.16.0.0 – 172.31.255.255/12
- 192.168.0.0 – 172.168.255.255/16

NAT

NAT surge como una forma "momentánea" de solucionar el problema de insuficiente capacidad de direccionamiento en IPv4. NAT utiliza una (o unas pocas) direcciones públicas para identificar la red del exterior y se utilizan direcciones privadas para identificar cada uno de los Pcs.

Para el camino hacia la red pública NAT coloca en la dirección de origen, la dirección publica que posee y en el destino la dirección publica del destino, Además le asigna un puerto a la comunicación con el PC de la red privada para identificar después a que dirección IP privada traducir los paquetes que se le envían a esta PC.

Direcciones en IPv6

Debido al incremento de dispositivos conectados a internet y a la convergencia de otras tecnologías de comunicación a IP, las direcciones IP públicas se fueron haciendo escasas, por lo que surgió la necesidad de adaptar el protocolo IP y surgió el protocolo IPv6.

Las direcciones IPv6 están basadas en 128 bits lo que da un espacio en IPv6 mucho mas extenso que en IPv4, y puesto que es difícil definir el espacio con notación decimal, IPv6 se compone de ocho secciones de 16 bits, separadas por dos puntos (:) expresadas con notación hexadecimal (16 diferentes caracteres: 0-9 y a-f).

Ejemplo de una dirección IPv6: 2607 : f0d0 : 4545 : 3 : 200 : f8ff : fe21 : 67cf.

Asignación de direcciones IP

A la hora de asignar direcciones IP a los equipos hay dos formas de hacerlo:

- Estáticamente - Para ello el administrador de la red debe configurar cada uno de los equipos y mantener registros de esas asignaciones.
- Dinámicamente - El protocolo más utilizado para asignar direcciones IP en forma dinámica o centralizada es el protocolo DHCP. Para ello se configura los equipos para que cuando se prendan realicen un broadcast solicitando una dirección IP. Este pedido es contestado por un servidor de DHCP y no sólo le asigna la dirección IP sino que además puede asignar el gateway por defecto, dirección IP del servidor de nombres, entre otros. En este caso, el trabajo del

administrador se restringe a configurar el servidor central y las Pcs para que obtengan automáticamente la dirección IP.

Protocolo ARP

Para que un equipo le pueda enviar un paquete a otro debe conocer su dirección IP y su dirección MAC. Pero lo que se conoce es sólo su dirección IP y se debe obtener la dirección Mac del equipo destino. Para ello existe el protocolo ARP, que dada una IP, realiza un broadcast preguntado quien tiene una cierta IP. Cuando el equipo de destino responde el pedido, se obtiene la MAC de destino.

A medida que los equipos reciben respuestas a peticiones ARP, se va cargando una tabla que se denomina Tabla de ARP. En la misma se guarda la asociación de IP con dirección MAC.

P*uede consultar la tabla ARP en su equipo con el comando arp -a.*

Para la comunicación de dos equipos en diferentes subredes, deben tener configurado un gateway por defecto (por lo general es la dirección IP del router que se conecta a su subred).

Cuando un equipo tiene un paquete para enviar a un destino, este verifica si la dirección está dentro de su subred, si está lo envía directamente, y sino se lo envía al gateway por defecto y el router sabrá como encaminar el paquete hacia su destino.

Protocolo ICMP

"El Protocolo de Control de Mensajes de Internet o ICMP es el subprotocolo de diagnóstico y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado ICMP difiere del propósito de TCP y UDP ya que generalmente no se utiliza directamente por las aplicaciones de usuario en la red. La única excepción es la herramienta ping y traceroute, que envían mensajes de petición Echo ICMP (y recibe mensajes de respuesta Echo) para determinar si un host está disponible, el tiempo que le toma a los paquetes en ir y regresar a ese host y cantidad de hosts por los que pasa."

Protocolos de Routeo

Una de las funciones de la capa 3 del modelo OSI es encontrar el mejor camino, para los paquetes, hacia las redes de destino. Para poder tomar decisiones los router deben tener conocimiento de las redes que existen y por donde llegar a ellas. Esta información se puede obtener de dos formas, estáticamente o dinámicamente. En esta última, los routers intercambian información para elegir las mejores rutas. En este capítulo se estudiará:

- El proceso de routeo en un router
- Los protocolos routing estático y dinámico
- Por último, se realizará una breve explicación del protocolo RIP

Cuando llega un paquete a un router, éste debe realizar el enrutamiento del paquete que consta de varias partes:

1. El router examina la cabecera IP y determina cual es la dirección de destino.
2. Busca en la tabla de ruteo si existe una entrada que coincida con esa IP. Para ello, se ordena la tabla de ruteo empezando con las entradas con máscara más larga hasta las cortas.
3. Si coincide, se conmuta hacia la interfaz de salida y se encapsula utilizando la capa de enlace correspondiente. Si no, el destino es inalcanzable se descarta el paquete.

Los protocolos de routing son los que permite a los routers tener un mapa de las redes que existen y de cómo es la mejor forma de llegar a ellas.

La información de las red existentes se puede obtener mediante el intercambio de información con sus vecinos. Esto le permite saber, al router, que red está por cada interfaz y que distancia. Cada protocolo implementa su concepto de distancia, por ejemplo para RIP la distancia son saltos de routers, OSPF toma en cuenta el ancho de banda del enlace.
Luego de intercambiar información, con los mejores valores obtenidos, el router crea una tabla de ruteo en donde se asocian redes de destino con interfaces de salida.

A medida que se producen cambios de topología en la red, los routers propagan estos acontecimientos de forma de poder adaptarse a los cambios y utilizar las mejores rutas hacia los destinos.
La tabla de ruteo le permite al router identificar para cada red de destino cuál va ser la interfaz por la que va a sacar el paquete. Esta tabla contiene las mejores rutas hacia los destinos.

La información en la tabla de ruteo se puede llenar de dos formas:

- Estáticamente – el administrador de la red las configura manualmente.
- Dinámicamente – En la red hay un protocolo de ruteo que se encarga de recabar y procesar esta información.

Se utiliza el enrutamiento estático en las siguientes circunstancias:

- Desea controlar la que el router utilizará para cierta red
- Cuando existe una única red hacia un destino
- No se quiere recargar el procesamiento ni la memoria del router
- No se quiere consumir ancho de banda con información de routing

El enrutamiento dinámico, se produce cuando los routers se envían entre sí mensajes periódicos de actualización de enrutamiento. Cada vez que un router recibe un mensaje que contiene nueva información, vuelve a calcular una nueva mejor ruta y envía esta nueva información actualizada a los demás routers. Al usar el enrutamiento dinámico, los routers se pueden adaptar a los cambios en las condiciones de las redes.

El enrutamiento dinámico elimina la necesidad de que los administradores o los fabricantes de la red introduzcan información en las tablas de enrutamiento de forma manual. Funciona mejor cuando el ancho de banda y las grandes cantidades de tráfico de red no constituyen un problema. RIP, EIGRP y OSPF son todos ejemplos de protocolos de enrutamiento dinámico, ya que permiten que este proceso se lleve a cabo.

Protocolo RIP

RIP es un protocolo dinámico de routing que tiene como métrica los saltos de router. Por tanto, si se realiza una publicación diciendo que una red esta x saltos, entonces esto quiere decir que hay que atravesar x routers para llegar al destino.

Al iniciar el protocolo, cada router anuncia por sus interfaces las redes las que tienen directamente conectadas. Esta información llega a sus vecinos, los cuales agregan un salto a la métrica, recalculan las mejores rutas y las anuncian nuevamente.

En régimen, cada router periódicamente recibe anuncios de sus vecinos, estos les agregan la métrica, recalculan las mejores rutas y lo vuelve a anunciar a sus vecinos, por eso es la denominación de vector distancia.
Hay que tener en cuenta que si hay múltiples rutas hacia un destino RIP selecciona la ruta que tiene el menor número de saltos. Sin embargo, dado que el número de saltos es la única métrica de enrutamiento que usa RIP para determinar cuál es la mejor ruta, esta no necesariamente es la ruta más rápida.

Protocolo OSPF

Open Shortest Path first (OSPF) es un protocolo de routing link-state no propietario, esto quiere decir principalmente dos cosas: Primero que es de libre uso y suele estar soportados por la mayoría de los equipos destinados a ofrecer servicios a la red y Segundo el ser un link-state quiere decir que a diferencia de RIP o IGRP que son Distance-vector, no mandan continuamente la tabla de rutas a sus vecinos sino que solo lo hacen cuando hay cambios en la topología de red, de esta forma se evita el consumo de ancho de banda innecesario.

A diferencia de RIP que utiliza como costo la distancia en saltos a cada uno de los destinos para cada ruta, OSPF utiliza información del estado de enlace, con lo cual hace uso de características como la latencia, capacidad, edad del enlace, etc.

En un cambio de topología OSPF envía el cambio inmediatamente de forma que la convergencia de la red es mas rápida que en los distance-vector donde depende de timers asignados, de forma que en un link-state el tiempo de convergencia puede ser de 4 o 5 segundos según la red en RIP puede se de 180 segundos.

Una de las mayores ventaja de OSPF es que permite ruteo jerárquico basado en la elección de la mejor ruta utilizando características del estado de enlace. Este ruteo jerárquico se basa en la definicion de áreas sobre las cuales cierta cantidad de enrutadores y no necesariamente todos los que componen el área deben mantener la información de ruteo dentro del área y algunos pocos de ellos solamente mantienen información de ruteo hacia dentro/fuera del área.

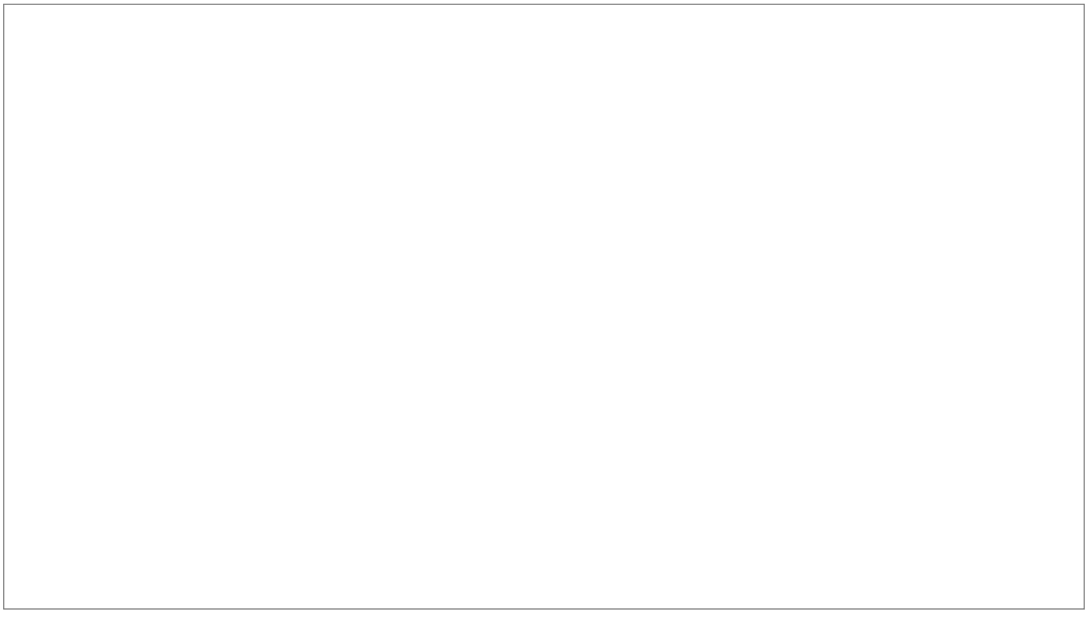
Mediante un mecanismo de inundación (Multicast) toma conocimiento de los vecinos que tiene utilizando mensajes (Hello), una vez establecida la asociación se da lugar a los mensajes LSA (Link State Advertisement) que permiten actualizar el estado de los enlaces de un enrutador y con esto el conocimiento de la topología.

Existen diferentes tipos de LSAs dependiente del tipo de información intercambiada sobre estados de enlaces. Esta es almacenada en la base de datos de estado de enlace que mantiene cada enrutador para el proceso OSPF que está ejecutando.

Tipos de Router en OSPF

Para el encaminamiento entre distintas áreas del AS (encaminamiento inter-área) y desde el AS hacia el exterior (encaminamiento exterior), OSPF utiliza routers especiales que mantienen una información topológica más completa que la del área en la que se sitúan. Así, pueden distinguirse:

Los ABRs (Area Border Routers), que mantienen la información topológica de su área y conectan ésta con el resto de áreas, permitiendo enrutar paquetes a cualquier punto de la red (inter-área routing).



Los ASBRs (Autonomous System Border Routers), que permiten encaminar paquetes fuera del AS (Sistema Autónomo) en que se alojen, es decir, a otras redes conectadas al Sistema Autónomo o resto de Internet (external routing).

Un paquete generado en la red será enviado, de forma jerárquica, a través del área si su destino es conocido por el emisor; al ABR del área correspondiente si el destino es intra-área; este lo enviará al router del área de destino, si este se encuentra en el AS; o al ASBR si el destino del paquete es exterior a la red.

Tipo de áreas

Los sistemas autónomos pueden ser grandes por si mismos y nada sencillos de administrar. OSPF permite dividir estos en áreas numeradas donde un área es una red o un conjunto de redes inmediatas.

Ejemplos de áreas

Área Backbone

El *backbone*, también denominado área cero, forma el núcleo de una red OSPF. Es la única área que debe estar presente en cualquier red OSPF, y mantiene conexión, física o lógica, con todas las demás áreas en que esté particionada la red. La conexión entre un área y el *backbone* se realiza mediante los ABR, que son responsables de la gestión de las rutas no-internas del área (esto es, de las rutas entre el área y el resto de la red).

Área *stub*

Un área *stub* es aquella que no recibe rutas externas. Las rutas externas se definen como rutas que fueron inyectadas en OSPF desde otro protocolo de encaminamiento. Por lo tanto, las rutas de segmento necesitan normalmente apoyarse en las rutas predeterminadas para poder enviar tráfico a rutas fuera del segmento.

Capa de Transporte

Algunas de las funciones más importante de la capa de transporte son: Recuperación de datos, Control de flujo, Segmentación de los datos.
Esta es la primera capa en la que realiza la recuperación de datos que se hayan perdido. En la capa de transporte no sólo se detectan los datos perdidos sino que se recuperan pidiendo su reenvío. Entonces, se garantiza la confiabilidad de los datos (reliability).

El control de flujo pretende disminuir la congestión existente que causan pérdidas de paquetes en la red. Pretende controlar la velocidad entre dos puntos para disminuir dicha congestión.

Dado que la capa de aplicación suele enviar grandes cantidades de datos que no entran en un paquete IP se debe segmentar, o sea dividir en trozos más pequeños cosa que puedan transportarse dentro de un paquete IP.

Puertos de Aplicaciones

Cuando a una computadora le llegan paquetes (la IP Destino del paquete corresponde a la de dicha computadora), se utiliza multiplexación para saber a qué aplicación debe enviarles cada uno de los paquetes, ya sea para un servidor FTP, Web browser u otras aplicaciones. La multiplexación se hace utilizando números de puertos diferentes.
Cada servidor, tal como un servidor web, telnet, ftp, etc., tiene un número de puerto bien conocido. Por otro lado los clientes de estos servidores utilizan un puerto cualquiera que esté libre y no sea de los bien "conocidos". De esta forma con los dos socket, en ambos lados se pueden distinguir en los paquetes cual es el origen y el destino.

Por ejemplo:

- Www (80/tcp 8080/tcp): se utiliza a través del browser y el server, y puede ser utilizado para acceder a un router o un switch habilitando el server en dicho dispositivo.
- DNS (53/udp): donde también existe el server (administrado por personal de red) y el cliente ubicado en cualquier dispositivo que utilice TCP/IP
- SNMP (25/tcp): es un software para el gerenciamiento de los equipos de red, que permite consultar, almacenar, etc., información a cerca de la operación de a red.
- FTP (20/tcp 21/tcp): utilizando un cliente y un server, se utiliza para transferir información entre diferentes dispositivos.

Protocolos orientados a conexión y no orientados a conexión

En el caso de un servicio "Orientado a conexión", antes de la transferencia de datos se debe establecer algún tipo de correlación entre ambos extremos. De lo contrario se considera "Sin conexión".
Un protocolo orientado a conexión necesita intercambios de mensajes antes de comenzar a transferir datos, y el no orientado a conexión no necesita tal intercambio de mensajes al inicio.

En la capa de transporte existen dos protocolos TCP y UDP, donde TCP es orientado a conexión y UDP no es orientado a conexión. Cada aplicación utiliza uno de estos protocolos dependiendo de sus requerimientos.

TCP

Funciones que realiza:

- Recuperación de errores
- Control de flujo utilizando "ventanas"
- Servicio con conexión
- Segmentación de datos
- Multiplexación utilizando puertos

Estas funciones son realizadas en ambas computadoras ubicadas en el extremo, independiente si están en la misma o en otra Ethernet.

Recuperación de errores

La transferencia de datos de manera fiable (reliability), o sea estando seguros que llegan todos los datos que fueron enviados, es utilizado por el protocolo TCP. Para lograrlo TCP enumera los bytes de datos utilizando un campo dentro del Header que contiene la secuencia y el reconocimiento. Para lograr que sea fiable en ambas direcciones se utiliza el campo de número de secuencia de una dirección combinada con el campo de reconocimiento en la dirección opuesta.

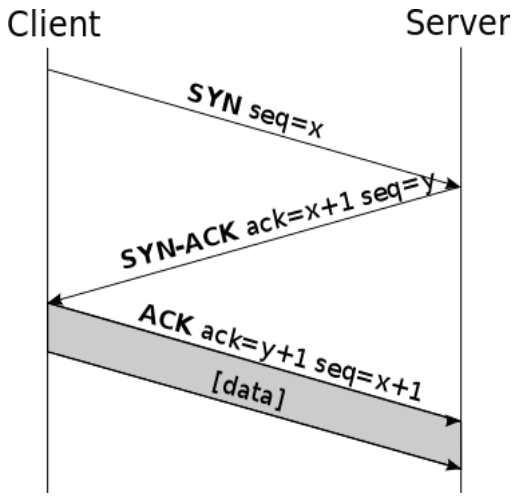
Control de Flujos

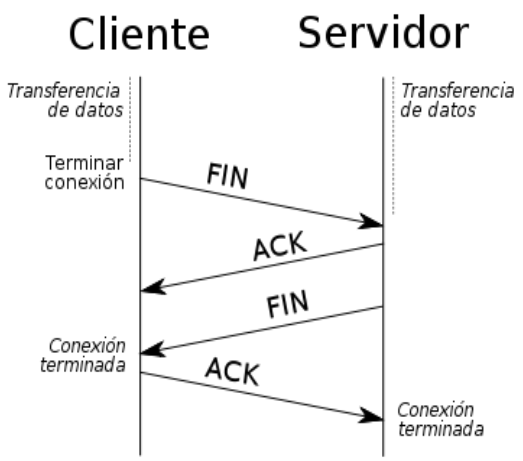
TCP implementa el control de flujo utilizando los dos campos "Sequence" (secuencia) y "ACK" (reconocimiento) y un nuevo campo llamado "Windows" (ventana) El campo "Windows" indica la cantidad máxima de

bytes no reconocidos que pueden estar pendientes e un cierto momento. Esta ventana comienza pequeña y va creciendo hasta que ocurre un error. La ventana desliza (disminuye o aumenta) dependiendo de la performance de la red. Entonces, si la ventana está llena, el que envía espera que le reconozcan los datos y le envíe una nueva ventana. De esta forma se realiza el control de flujo de datos.

Establecimiento de conexión

El lado cliente de una conexión realiza una apertura activa de un puerto enviando un paquete SYN inicial al servidor como parte de la negociación en tres pasos. En el lado del servidor se comprueba si el puerto está abierto. En caso de que se encuentre abierto el puerto, el lado servidor respondería a la petición SYN válida con un paquete SYN/ACK. Finalmente, el cliente debería responderle al servidor con un ACK, completando así la negociación en tres pasos (SYN, SYN/ACK y ACK).





La fase de finalización de la conexión utiliza una negociación en cuatro pasos enviando el segmento FIN y el ACK. Una desconexión típica requiere un par de segmentos FIN y ACK desde cada lado de la conexión.

Segmentación

Las aplicaciones necesitan enviar diferentes cantidades de bytes, desde un único bits a millones. La MTU es el tamaño máximo de datos que entra en una trama Ethernet (un paquete) es de 1500 bytes, por lo que la cantidad de bytes de un segmento deberá ser: 1500 – 20 – 20 (de ambos Headers) <=1460.

UDP

UDP es sin conexión, no hay recuperación de datos erróneos, no utiliza ventanas para controlar el flujo y evitar congestión, y tampoco reordena los datos recibidos. Sin embargo, si cumple con algunas funciones comunes con TCP, tales como transferencia de datos, segmentación y multiplexación utilizando números de puertos. Estas características recién mencionadas hacen al protocolo UDP que tenga mucho menos cantidad de bytes que utilizar para transmitir la misma cantidad de información. También requiere mucho menos cantidad de tiempo de procesamiento.

Aunque no es común, está permitido que dos aplicaciones utilicen el mismo puerto, una para UDP y otra para TCP.

De igual manera los socket serían distintos ya que uno de los tres elementos que los conforman es diferente (TCP, UDP).

Las aplicaciones que utilizan UDP o tienen un grado de tolerancia a la pérdida de datos o por otro lado ellos mismos se encargan de recuperar los datos. Por ejemplo Telnet, utiliza UDP porque no prioriza en la recuperación total de los datos, y el DNS es una aplicación que maneja la recuperación de datos ya que en caso de que la resolución del nombre falle, la petición se realizará nuevamente.

Capa de Aplicación

La capa de aplicación es la capa más cercana al usuario final e interactúa con las aplicaciones de software que se ejecutan el PC.
En este capítulo se mostrará el funcionamiento practico de algunas aplicaciones como ser el caso de:

- HTTP
- Telnet
- FTP

HTTP

El protocolo de transferencia de hipertexto (HTTP, HyperText Transfer Protocol) es el protocolo usado en cada transacción de la Web (WWW). El hipertexto es el contenido de las páginas web, y el protocolo de transferencia es el sistema mediante el cual se envían las peticiones de acceso a una página y la respuesta con el contenido. También sirve el protocolo para enviar información adicional en ambos sentidos, como formularios con campos de texto.

HTTP es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores. Al finalizar la transacción todos los datos se pierden. Por esto se popularizaron las cookies, que son pequeños ficheros guardados en el propio ordenador que puede leer un sitio web al establecer conexión con él, y de esta forma reconocer a un visitante que ya estuvo en ese sitio anteriormente. Gracias a esta identificación, el sitio web puede almacenar gran número de información sobre cada visitante, ofreciéndole así un mejor servicio.

TELNET

Telnet es el nombre de un protocolo (y del programa informático que implementa el cliente) que sirve para acceder mediante una red a otra máquina, para manejarla como si estuviéramos sentados delante de ella.
Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

Sólo sirve para acceder en modo terminal, es decir, sin gráficos, pero fue una herramienta muy útil para arreglar fallos a distancia, sin necesidad de estar físicamente en el mismo sitio que la máquina que los tenía. También

se usaba para consultar datos a distancia, como datos personales en máquinas accesibles por red, información bibliográfica, etc.

Su mayor problema es de seguridad, ya que todos los nombres de usuario y contraseñas necesarias para entrar en las máquinas viajan por la red como texto plano (cadenas de texto sin cifrar). Esto facilita que cualquiera que espíe el tráfico de la red pueda obtener los nombres de usuario y contraseñas, y así acceder él también a todas esas máquinas. Por esta razón dejó de usarse, casi totalmente, hace unos años, cuando apareció y se popularizó el SSH, que puede describirse como una versión cifrada de telnet.

FTP

FTP (File Transfer Protocol) es un protocolo de transferencia de ficheros entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar ficheros desde él o para enviarle nuestros propios archivos independientemente del sistema operativo utilizado en cada equipo. El Servicio FTP es ofrecido por la capa de Aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21.

Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier fichero, se realiza en texto plano sin ningún tipo de encriptación, con lo que un posible atacante lo tiene muy fácil para capturar este tráfico, acceder al servidor, o apropiarse de los ficheros transferidos. Para solucionar este problema son de gran utilidad aplicaciones como scp y sftp, incluidas en el paquete SSH, que permiten transferir ficheros pero cifrando todo el tráfico.

DNS

Cualquier tipo de aplicación que utiliza nombres de dominio para representar direcciones IP utiliza el DNS para traducir ese nombre a la dirección IP correspondiente. Por tanto, el funcionamiento de este sistema es fundamental para la continuidad de una red.

Facilita la comunicación con los equipos en la red, haciendo referencia a nombres en vez de direcciones numéricas, hace la traducción de nombres a

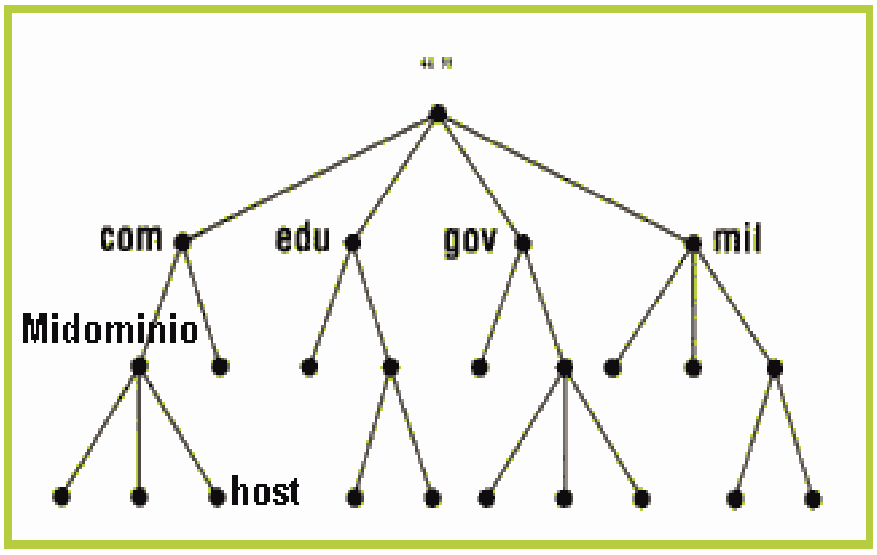
direcciones IP. Es más sencillo recordar la dirección www.antel.com.uy que la IP 190.0.136.230 que le corresponde.

Dominios

Es un conjunto de etiquetas separadas por puntos. El servidor de dominio es un dispositivo de red que administra nombres de dominio y responde a las peticiones de clientes para transformar un nombre de dominio en la dirección IP asociada. El sistema DNS se basa en una jerarquía que crea distintos niveles de servidores DNS. Si un DNS puede traducir un nombre de dominio a su dirección IP asociada, lo hace y devuelve el resultado al cliente. Si no logra traducir la dirección, transfiere la petición al siguiente servidor DNS del sistema. Por tanto, existen dos tipo de consultas:

- Recursivas
- No recursivas

En Internet, el nivel superior de la jerarquía de nombres se administra mediante una organización llamada ICANN (Corporación de Internet para la Asignación de Nombres y Números, del inglés Internet Corporation for Assigned Names and Numbers), la cual se creó para este fin en 1998 como parte del proceso de maduración de Internet, que se convirtió en un asunto económico a nivel mundial.



Los dominios de nivel superior se dividen en dos categorías: genéricos y países. Los dominios genéricos, que se listan en la figura 7-2, incluyen los dominios originales de la década de 1980 y los dominios introducidos

mediante solicitudes a la ICANN. En lo futuro se agregarán otros dominios genéricos de nivel superior. Los dominios de país incluyen una entrada para cada país, como se define en la ISO 3166.

La responsabilidad de la administración de los subárboles. Por ejemplo:

- "." ICAN-IANA
- uy. SECIU
- edu.uy. SECIU
- antel.com.uy. ANTEL
- Fing.edu.uy. Facultad de Ingeniería
- ucu.edu.uy. Universidad Católica

Hay 13 servidores root distribuidos por el mundo, identificados por letras: A B C ... M.

Consulta recursiva

El servidor que responde consultas recursivas de los clientes, realiza todo el trabajo, preguntando a otros servidores, para obtenerla.

Consulta no recursiva

El servidor que responde consultas no recursivas de los clientes, otorga como respuesta la mejor referencia que tenga a otros servidores, a quién este deberá consultar a los efectos de poder obtener la respuesta buscada.