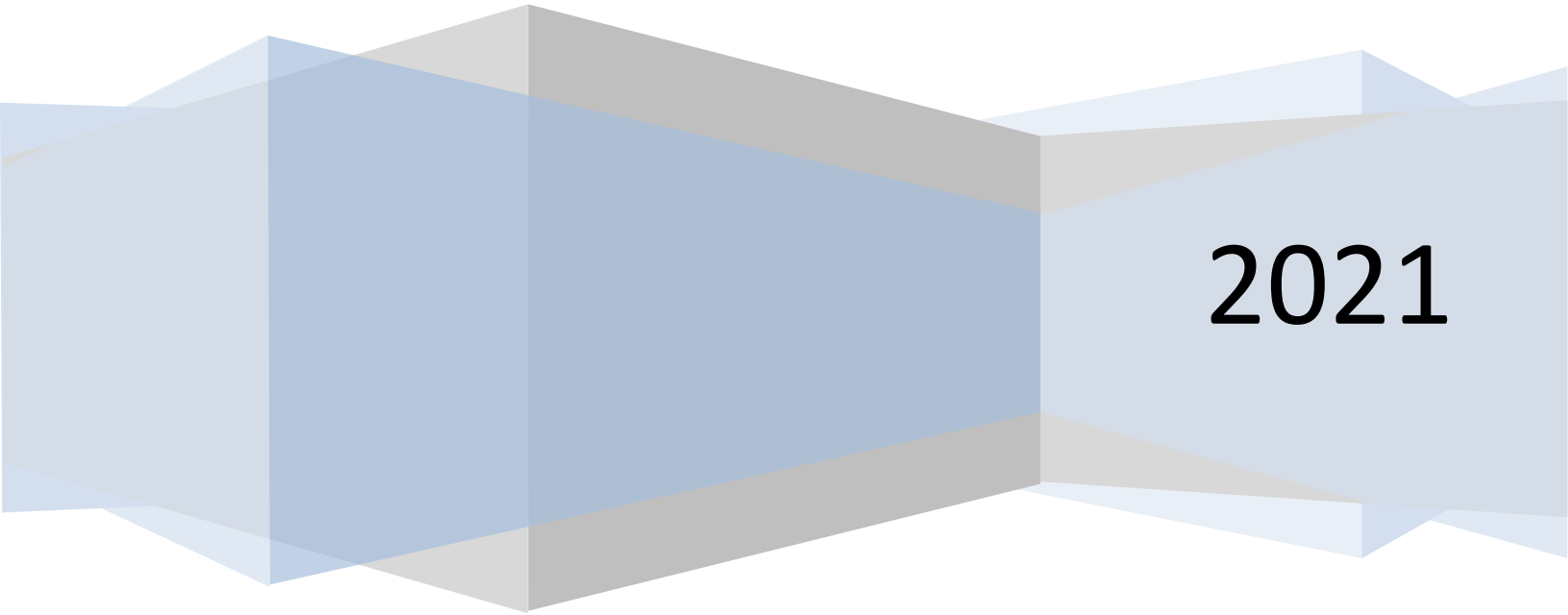
UNIVERSIDAD NACIONAL DE LA MATANZA

ARQUITECTURA DE COMUNICACIONES

Redes y Protocolo TCP/IP

Ing. Anibal Pose



2021

HISTORIA DE LAS REDES LOCALES

Una red de área local, o red local, es la interconexión de varios ordenadores y periféricos. (LAN es la abreviatura inglesa de Local Area Network, 'red de área local'). Su extensión esta limitada físicamente a un edificio o a un entorno de pocos kilómetros. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

En épocas anteriores a los ordenadores personales, una empresa podía tener solamente un ordenador central, accediendo los usuarios a éste mediante terminales de ordenador con un cable simple de baja velocidad. Las redes como SNA de IBM (Arquitectura de Red de Sistemas) fueron diseñadas para unir terminales u ordenadores centrales a sitios remotos con líneas alquiladas. Las primeras LAN fueron creadas a finales de los años 1970 y se solían crear líneas de alta velocidad para conectar grandes ordenadores centrales a un solo lugar. Muchos de los sistemas fiables creados en esta época, como Ethernet y ARCNET, fueron los más populares.

En 1972 comenzó el desarrollo de una tecnología de redes conocida como Ethernet Experimental- El sistema Ethernet desarrollado, conocido en ese entonces como red ALTO ALOHA, fue la primera red de área local (LAN) para computadoras personales (PCs). Esta re d funcionó por primera vez en mayo de 1973 a una velocidad de 2.94Mb/s. Las especificaciones formales de Ethernet de 10 Mb/s fueron desarrolladas en conjunto por las corporaciones Xerox, Digital (DEC) e Intel, y se publicó en el año 1980. Estas especificaciones son conocidas como el estándar DEC-Intel-Xerox (DIX), el libro azul de Ethernet. Este documento hizo de Ethernet experimental operando a 10 Mb/s un estándar abierto. La tecnología Ethernet fue adoptada para su estandarización por el comité de redes l ocales (LAN) de la IEEE como IEEE 802.3. El estándar IEEE 802.3 fue publicado por primera vez en 1985. El estándar IEEE 802.3 provee un sistema tipo Ethernet basado, pero no idéntico, al estándar DIX original. El nombre correcto para esta tecnología es IEEE 802.3 CSMA/CD, pero casi siempre es referido como Ethernet. IEEE 802.3 Ethernet fue adoptado por la organización internacional de estandarización (ISO), haciendo de un estándar de redes internacional. Ethernet continuó

evolucionando en respuesta a los cambios en tecnología y necesidades de los usuarios. Desde 1985, el estándar IEEE 802.3 se actualizó para incluir nuevas tecnologías. Por ejemplo, el estándar 10BASE-T fue aprobado en 1990, el estándar 100BASE-T fue aprobado en 1995 y Gigabit Ethernet sobre fibra fue aprobado en 1998. Ethernet es una tecnología de redes ampliamente aceptada con conexiones disponibles para PCs, estaciones de trabajo científicas y de alta desempeño, mini computadoras y sistemas mainframe.

CLASIFICACIONES DE REDES

Existen distintas clasificaciones de las redes informáticas, de las cuales veremos dos:

Por su extensión.

Por su jerarquía.

Por su topología.

Clasificación redes por extensión

Según la extensión máxima entre los nodos o componentes de la red, no entre solamente 2 terminales, sino como máxima, entre los más extremos.

LAN (Local Area Network o Red De área Local)

MAN (Metropolitan Area Network o Red de Área Metropolitana)

WAN (Wide Area Network o Red de Área Extensa)

LAN (Local Area Network o Red De área Local)

Es una red que cubre una extensión reducida como una empresa, una universidad, un colegio, una casa, etc. No habrá por lo general dos ordenadores que disten entre si más de dos kilómetros. La extensión máxima de esta red será de hasta dos kilómetros. La mayoría de las redes LAN están conectadas por medio de cables y tarjetas de red, una en cada equipo, aunque hoy día se están utilizando las llamadas redes inalámbricas, que son las que la señal viaja por el aire.

MAN (Metropolitan Area Network o Red de Área Metropolitana)

Las redes de área metropolitana cubren extensiones mayores como pueden ser una ciudad o un distrito. Mediante la interconexión de redes LAN se distribuyen la informática a los diferentes puntos del distrito. Bibliotecas, universidades u organismos oficiales suelen interconectarse mediante este tipo de redes. La extensión de estas redes puede ser de hasta 100 kilómetros.

WAN (Wide Area Network o Red de Área Extensa)

Las redes de área extensa cubren grandes regiones geográficas como un país, un continente o incluso el mundo.

Con el uso de una WAN se puede conectar desde España con Japón sin tener que pagar enormes cantidades de teléfono. La implementación de una red de área extensa es muy complicada. La extensión de este tipo de red supera los 100 kilómetros. El mejor ejemplo de una red de área extensa es Internet.

Clasificación de redes por jerarquías

Ordenadas o clasificadas según su jerarquía o relación funcional entre los nodos o componentes de la red.

Cliente / Servidor

Par a par (peer to peer)

Cliente / Servidor

Las redes Cliente/Servidor se usan en entornos LAN mayores, incluyendo colegios y universidades. En este enfoque de la conectividad, la red se compone de uno o más servidores especializados y varios clientes diferentes, los servidores están diseñados para proporcionar servicios centralizados y los clientes son los diferentes nodos en la red. En un entorno Cliente/Servidor, las PCs conectadas a la red puede llamarse clientes, nodos o estaciones de trabajo; existe poca diferencia técnica entre los tres términos en este tipo de red.

Muchos tipos diferentes de servidores se pueden usar en una red Cliente/Servidor. Estos servidores se agregan a la red conforme lo dictan las necesidades de ésta. Tipos comunes de servidores incluyen los siguientes:

Servidor de archivo. Esta computadora está dedicada a proporcionar almacena-miento y administración centralizados de archivos.

Servidor de impresión. Esta computadora está dedicada a proporcionar servicios de impresión centralizados.

Servidor de comunicaciones. Esta computadora está dedicada a proporcionar servicios de módem, fax y correo electrónico.

Servidor de base de datos. Esta computadora está dedicada a ejecutar un programa de base de datos centralizado.

Como mínimo, una red de este tipo tendrá un servidor de archivos, agregándose otros servicios conforme crezcan y desarrollen las necesidades de la empresa.

En muchas formas, el enfoque de Cliente/Servidor para la conectividad es un enfoque de arriba hacia abajo; los servidores proporcionan los servidores centralizados para la red entera. Aunque este enfoque es muy eficaz, tiene sus desventajas. Quizá la mayor desventaja es que si un servidor falla (por cualquier razón), la red entera falla en relación con ese recurso. Por ejemplo, si un servidor de impresión no está disponible, no hay forma de imprimir a través de la red hasta de una impresora local, si hay una disponible). Debido a que es un asunto crítico mantener un funcionamiento la red, la mayor parte de los entornos que usan un enfoque Cliente/Servidor confían en una persona, o el jefe del departamento, se conoce como administrador de la red. Esta persona debe ser muy competente en lo relacionado con la conectividad y tener una compresión de la forma como lo relacionado con la conectividad y tener una compresión de la forma como encajan todas las piezas de la red. El administrador de la red- y los costos de una empresa que financia a esta persona- es la razón por la que el enfoque cliente/servidor se usa de manera compón sólo en redes grandes.

Ejemplos de puestas en práctica de redes cliente/servidor incluyen Novell NetWare, Windows NT Server y LAN Manager.

Redes Par a par (peer to peer, punto a punto)

En un entorno de conectividad de punto a punto no hay servidores centralizados. En un lugar, cada nodo en la red proporciona servidores a los que pueden tener acceso otros nodos en la red. Por ejemplo, un nodo puede tener una impresora que pueden usar otros nodos, en tanto que un nodo diferente puede tener archivos de datos a disposición de otros usuarios de la red.

La conectividad de punto a punto se usa de manera tradicional para redes o grupos de trabajo menores. Por ejemplo un salón de clase, si no está conectado a una red mayor, puede usar el enfoque de red de punto. Este enfoque elimina varias de las desventajas inherentes en el enfoque Cliente/Servidor. Por ejemplo, si una de las computadoras en la red falla, no se desactiva la red completa. Por su puesto, los recursos compartidos por ese nodo no están disponibles, pero pueden usarse servicios alternativos por medio de otros nodos en la red. Además, de manera característica no es necesario un administrador de red porque cada persona que usa la red, por lo general mantiene su propia máquina y administra sus propios recursos compartidos.

Ejemplos de redes de punto incluyen Windows 95, Windows para Trabajo en Grupo, LANtastic y 10Net.

Protocolos de comunicación

Así como nosotros las personas podemos hablar en distintos idiomas, las computadoras pueden comunicarse con otros equipos con diferentes "lenguajes". A estos lenguajes se les llama Protocolos de comunicación, y son los encargados de regir en proceso de comunicación. Son un conjunto de reglas que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red Son normas y reglamentos que se encargarán de administrar el empaquetado del mensaje, la salida del mensaje desde el emisor, cómo viajará el mensaje a través del canal o medio, como lo recibirá el receptor, la respuesta que nos devolverá el receptor al recibir el mensaje, etc.

Cabe aclarar que para que dos computadoras se entiendan deben tener el mismo protocolo instalado en cada una.

Más específica o técnicamente hablando, establecen aspectos tales como:

Las secuencias posibles de mensaje que pueden arribar durante el proceso de la comunicación.

La sintaxis de los mensajes intercambiados.

Estrategias para corregir los casos de error.

Estrategias para asegurar la seguridad (autenticación, encriptación).

EL MODELO DE REFERENCIA OSI

Es aquí donde el Modelo de Referencia de Interconexión de Sistemas Abiertos cobra la importancia que merece, al permitir que sistemas de cómputo disímiles se interconecten e inter operen, gracias a reglas preestablecidas que deben ir cumpliéndose nivel a nivel para su total desempeño logrando el concepto de Internet Working (Este concepto da la idea de sistemas abiertos, y es donde las compuertas tienen lugar cubriendo desde los niveles mas bajos de conectividad hasta esquemas de conversión de protocolos que requieren de un alto grado de integración.

Concepto de Modelo OSI

El Modelo de Referencia de Interconexión de Sistemas Abiertos, conocido mundialmente como Modelo OSI (Open System Interconnection), fue creado por la ISO (Organización Estándar Internacional) y en él pueden modelarse o referenciarse diversos dispositivos que reglamenta la ITU (Unión de Telecomunicación Internacional), con el fin de poner orden entre todos los sistemas y componentes requeridos en la transmisión de datos, además de simplificar la interrelación entre fabricantes. Así, todo dispositivo de cómputo y telecomunicaciones podrá ser referenciado al modelo y por ende concebido como parte de un sistema interdependiente con características muy precisas en cada nivel.

Esta idea da la pauta para comprender que el modelo OSI existe potencialmente en todo sistema de cómputo y telecomunicaciones, pero que

solo cobra importancia al momento de concebir o llevar a cabo la transmisión de datos.

El Modelo OSI cuenta con 7 capas o niveles:

- Nivel de Aplicación
- Nivel de Presentación
- Nivel de Sesión
- Nivel de Transporte
- Nivel de Red
- Nivel de Enlace de Datos
- Nivel Físico

Nivel de Aplicación

Es el nivel más cercano al usuario y a diferencia de los demás niveles, por ser el más alto o el último, no proporciona un servicio a ningún otro nivel.

Cuando se habla de aplicaciones lo primero que viene a la mente son las aplicaciones que procesamos, es decir, nuestra base de datos, una hoja de cálculo, un archivo de texto, etc., lo cual tiene sentido ya que son las aplicaciones que finalmente deseamos transmitir. Sin embargo, en el contexto del Modelo de Referencia de Interconexión de Sistemas Abiertos, al hablar del nivel de Aplicación no nos estamos refiriendo a las aplicaciones que acabamos de citar. En OSI el nivel de aplicación se refiere a las aplicaciones de red que vamos a utilizar para transportar las aplicaciones del usuario.

FTP (File Transfer Protocol), Mail, Rlogin, Telnet, son entre otras las aplicaciones incluidas en el nivel 7 del modelo OSI y sólo cobran vida al momento de requerir una comunicación entre dos entidades.

En Resumen se puede decir que la capa de Aplicación se dice que es una sesión específica de aplicación (API), es decir, son los programas que ve el usuario.

Nivel de Presentación

Se refiere a la forma en que los datos son representados en una computadora. Proporciona conversión de códigos y reformateo de datos de la aplicación del usuario. Es sabido que la información es procesada en forma binaria y en este nivel se llevan a cabo las adaptaciones necesarias para que pueda ser presentada de una manera mas accesible.

Códigos como ASCII (American Standard Code for Information Interchange) y EBCDIC (Extended Binary Coded Decimal Interchange Code), que permiten interpretar los datos binarios en caracteres que puedan ser fácilmente manejados, tienen su posicionamiento en el nivel de presentación del modelo OSI.

Nivel de Sesión

Este nivel es el encargado de proveer servicios de conexión entre las aplicaciones, tales como iniciar, mantener y finalizar una sesión. Establece, mantiene, sincroniza y administra el diálogo entre aplicaciones remotas.

Cuando establecemos una comunicación y que se nos solicita un comando como login, estamos iniciando una sesión con un host remoto y podemos referenciar esta función con el nivel de sesión del modelo OSI. Del mismo modo, cuando se nos notifica de una suspensión en el proceso de impresión por falta de papel en la impresora, es el nivel de sesión el encargado de notificarnos de esto y de todo lo relacionado con la administración de la sesión.

Nivel de Transporte

En este nivel se realiza y se garantiza la calidad de la comunicación, ya que asegura la integridad de los datos. Es aquí donde se realizan las retransmisiones cuando la información fue corrompida o porque alguna trama (del nivel 2) detectó errores en el formato y se requiere volver a enviar el paquete o datagrama.

El nivel de transporte notifica a las capas superiores si se está logrando la calidad requerida. Este nivel utiliza reconocimientos, números de secuencia y control de flujo.

Los protocolos TCP (Transmisión Control Protocol) y UDP (User Datagram Protocol) son característicos del nivel del transporte del modelo OSI, al igual que SPX (Sequenced Packet Exchange) de Novell.

En Resumen se dice que la capa de Transporte es la integridad de datos de extremo a extremo o sea que se encarga el flujo de datos del transmisor al receptor verificando la integridad de los mismos por medio de algoritmos de detección y corrección de errores, la capa de Red es la encargada de la información de enrutador e interceptores y aquella que maneja el Hardware (HW), ruteadores, puentes, multiplexores para mejorar el enrutamiento de los paquetes.

Enlace de Datos

Conocido también como nivel de Trama (Frame) o Marco, es el encargado de preparar la información codificada en forma binaria en formatos previamente definidos por el protocolo a utilizar.

Tiene su aplicación en el contexto de redes WAN y LAN ya que como se estableció previamente la transmisión de datos no es mas que el envió en forma ordenada de bits de información. Podríamos de hecho concebir a ésta como una cadena de bits que marchan en una fila inmensa (para el caso de transmisiones seriales), cadena que carece de significado hasta el momento en que las señales binarias se agrupan bajo reglas, a fin de permitir su interpretación en el lado receptor de una manera constante.

Este nivel ensambla los datos en tramas y las transmite a través del medio (LAN o WAN). Es el encargado de ofrecer un control de flujo entre tramas, así como un sencillo mecanismo para detectar errores. Es en este nivel y mediante algoritmos como CRC (Cyclic Redundancy Check), donde se podrá validar la integridad física de la trama; mas no será corregida a este nivel sino que se le notificará al transmisor para su retransmisión.

En Resumen se puede decir que la capa de Enlace de Datos es aquella que transmite la información como grupos de bits, o sea que transforma los bits en frames o paquetes por lo cual si recibimos se espera en conjunto de señales para convertirlos en caracteres en cambio si se manda se convierte directamente cada carácter en señales ya sean digitales o analógicos.

Nivel Físico

Es el primer nivel del modelo OSI y en él se definen y reglamentan todas las características físicas-mecánicas y eléctricas que debe cumplir el sistema para poder operar. Como es el nivel más bajo, es el que se va a encargar de las comunicaciones físicas entre dispositivos y de cuidar su correcta operación. Es

bien sabido que la información computarizada es procesada y transmitida en forma digital siendo esta de bits: 1 y 0. Por lo que, toda aplicación que se desee enviar, será transmitida en forma serial mediante la representación de unos y ceros.

En este nivel, se encuentran reglamentadas las interfaces de sistemas de cómputo y telecomunicaciones (RS-232 o V.24, V.35) además de los tipos de conectores o ensambles mecánicos asociados a las interfaces (DB-24 y RJ-45 para RS-232 o V.24, así como Coaxial 75 ohms para G703)

En Resumen se dice que la capa Físico transmite el flujo de bits sobre un medio físico y aquella que representa el cableado, las tarjetas y las señales de los dispositivos.

Modelo TCP/IP

Introducción

Internet se desarrolló para brindar una red de comunicación que pudiera continuar funcionando en tiempos de guerra. Aunque la Internet ha evolucionado en formas muy diferentes a las imaginadas por sus arquitectos, todavía se basa en un conjunto de protocolos TCP/IP. El diseño de TCP/IP es ideal para la poderosa y descentralizada red que es Internet.

Es muy útil conocer los modelos OSI y TCP/IP para comprender como se produce la comunicación de los distintos dispositivos. Cada modelo ofrece su propia estructura para explicar cómo funciona una red, pero los dos comparten muchas características.

Todo dispositivo conectado a Internet que desee comunicarse con otros dispositivos en línea debe tener un identificador exclusivo. El identificador se denomina dirección IP. Una dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI.

IPv4, la versión actual de IP, se diseñó antes de que se produjera la explosión de internet, lo que produjo una gran demanda de direcciones IP, que hizo que las cuatro mil millones de direcciones posibles fueran insuficientes. La división en subredes, la Traducción de direcciones en red (NAT) y el direccionamiento privado se utilizan para extender el direccionamiento IP sin agotar el suministro.

El TCP/IP es la base de Internet, y sirve para comunicar todo tipo de dispositivos, computadoras que utilizan diferentes sistemas operativos, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN). TCP/IP fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en ARPANET, una red de área extensa del departamento de defensa.

Familia de protocolos TCP/IP

Existen diversos protocolos dentro de la arquitectura TCP/IP, sobre todo a nivel de aplicación

5	Aplicación	ej. HTTP, FTP, DNS *(protocolos de enrutamiento como BGP y RIP, que por varias razones funcionen sobre TCP y UDP respectivamente, son considerados parte del nivel de red)*
4	Transporte	ej. TCP, UDP, RTP, SCTP *(protocolos de enrutamiento como OSPF, que funcionen sobre IP, son considerados parte del nivel de Internet)*
3	Internet	Para TCP/IP este es el Protocolo de Internet (IP) *(protocolos requeridos como ICMP e IGMP funcionan sobre IP, pero todavía se pueden considerar parte del nivel de red; ARP no funciona sobre IP)*
2	Enlace	ej. Ethernet, Token Ring, PPP, HDLC, Frame Relay, RDSI, ATM, IEEE 802.11, FDDI
1	Físico	ej. medio físico, y técnicas de codificación, T1, E1

Resumen comparativo entre el modelo OSI y el modelo TCP/IP

Los protocolos que forman la suite de protocolos TCP/IP pueden describirse en términos del modelo de referencia OSI.

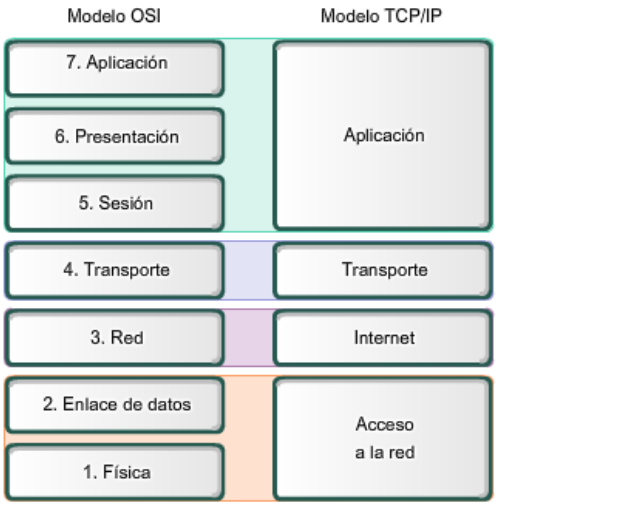
Las similitudes incluyen:

- Ambos se dividen en capas.
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.
- Ambos tienen capas de transporte y de red similares.
- Ambos modelos deben ser conocidos por los profesionales de redes.
- Ambos suponen que se conmutan paquetes. Esto significa que los paquetes individuales pueden usar rutas diferentes para llegar al mismo destino. Esto se contrasta con las redes conmutadas por circuito, en las que todos los paquetes toman la misma ruta.

Las diferencias incluyen:

- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación.
- TCP/IP combina la capa de enlace de datos y la capa física del modelo OSI en la capa de acceso de red.
- TCP/IP parece ser más simple porque tiene menos capas.
- Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló la Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. En comparación, por lo general las redes no se desarrollan a partir del protocolo OSI, aunque el modelo OSI se usa como guía.

Comparación del modelo OSI con el modelo TCP/IP



Las semejanzas claves están en la capa de Red y de Transporte.

CAPA FISICA DE UNA RED LAN

Antes de distinguir los distintos tipos de cableado, es importante hablar de los distintos medios de transmisión que nos podemos encontrar. Estos medios de transmisión se clasifican en guiados y no guiados.

Los primeros son aquellos que utilizan un medio sólido (un cable) para la transmisión. Los medios no guiados utilizan el aire para transportar los datos: son los medios inalámbricos.

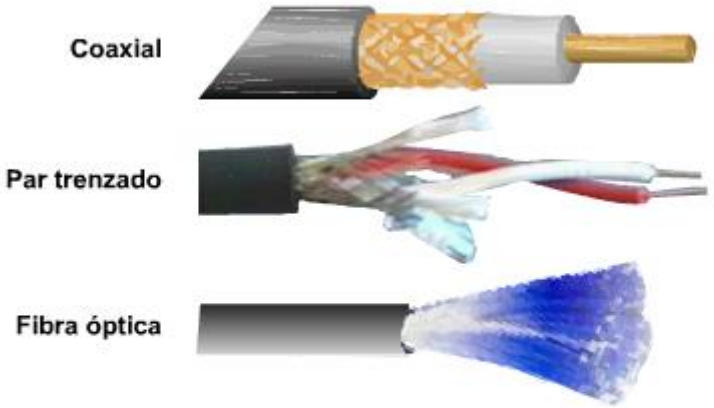
Los cables, medios guiados, transmiten impulsos eléctricos o lumínicos. Los bits se transforman en la tarjeta de red y se convierten en señales eléctricas o lumínicas específicas y determinadas por el protocolo que implemente esa red.

Podemos considerar tres tipos de medios distintos :

Cable coaxial

Par trenzado.

Fibra óptica.



Tipos de cables:
Los cables son los medios guiados por excelencia. Su configuración está ideada para mejorar la integridad de los datos y la velocidad de transmisión

La velocidad de transmisión, el alcance y la calidad (ausencia de ruidos e interferencias) son los 3 elementos que caracterizan este tipo de medio. La evolución de esta tecnología ha estado orientada por la optimización de estas tres variables.

Uno de los principales problemas de la transmisión de un flujo de datos por un cable eléctrico consiste en el campo magnético que se genera por el hecho de la circulación de los electrones. Este fenómeno es conocido como inducción electromagnética. La existencia de un campo magnético alrededor de un cable va a generar interferencias en los cables próximos debido a este mismo fenómeno.

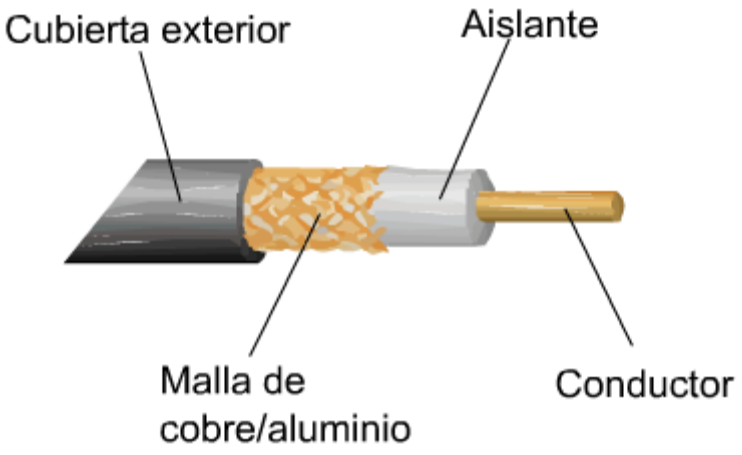
Cada uno de estos tipos de cable aporta una solución a los tres problemas definidos anteriormente. El cable coaxial, con su malla exterior, proporciona una pantalla para las interferencias, el cable de par trenzado permite que los campos electromagnéticos generados por la corriente eléctrica se acoplen y se evite así la interferencia.

Del mismo modo que se ha tratado de solucionar el problema del acoplamiento de la señal se han buscado soluciones para disminuir la atenuación que sufre ésta según va circulando por el cable y que es mayor cuanta más distancia debe recorrer, por lo que este factor limita considerablemente la longitud de cable que se puede instalar sin regenerar la señal. Generalmente, en los cables de cobre un mayor grosor del conductor

hace que la atenuación sea menor; sin embargo, la solución mejor a este problema es el cable de fibra óptica.

Cable coaxial

La denominación de este cable proviene de su peculiar estructura en la que los dos conductores comparten un mismo eje, no se sitúan uno al lado del otro sino que uno de los conductores envuelve al otro.El cable coaxial es similar al cable utilizado en las antenas de televisión: un hilo de cobre en la parte central rodeado por una malla metálica y separados ambos elementos conductores por un cilindro de plástico, protegidos por una cubierta exterior.



Estructura de un cable:
Estructura básica de un cable coaxial en la que se muestran los conductores y aislantes que lo constituyen

*Este medio ya no se utiliza de forma habitual en las redes LAN.

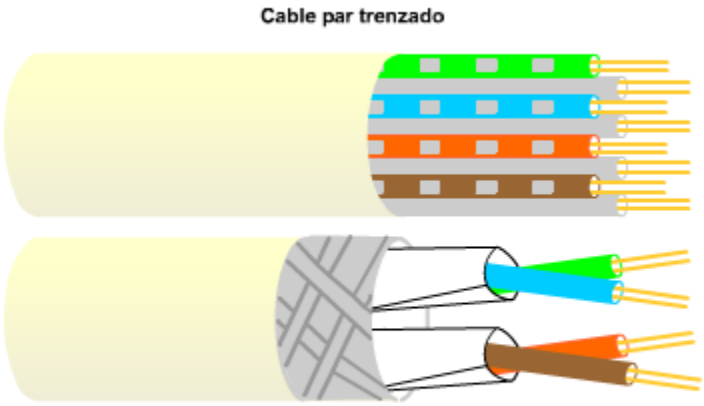
Cable par trenzado.

El par trenzado es parecido al cable telefónico, consta de 8 hilos trenzados dos a dos identificados por colores para facilitar su instalación. Se trenza con el propósito de reducir interferencias. Dependiendo del número de trenzas por unidad de longitud, los cables de par trenzado se clasifican en categorías. A mayor número de trenzas, se obtiene una mayor velocidad de transferencia gracias a que se provocan menores interferencias.

Los cables par trenzado pueden ser a su vez de dos tipos:

UTP (Unshielded Twisted Pair, par trenzado no mallado)

STP (Shielded Twisted Pair, par trenzado mallado)



Par trenzado:
Puede estar constituido, según el tipo, por cuatro o dos pares de cables. En primer caso es un cable UTP y en el segundo STP

Los cables sin apantallado son los más utilizados debido a su bajo coste y facilidad de instalación. Los cables STP están embutidos en una malla metálica que reduce las interferencias y mejora las características de la transmisión. Sin embargo, tienen un coste elevado y al ser más gruesos son más complicados de instalar.

El cable UTP

El cable de par trenzado se divide en categorías y ofrece una serie de prestaciones en función del número de trenzas que se han aplicado a los pares.

Categoría 3, hasta 16 Mhz: Telefonía de voz, 10Base-T Ethernet y Token ring a 4 Mbs

Categoría 4, hasta 20 Mhz: Token Ring a 16 Mbs.

Categoría 5, hasta 100 Mhz: Ethernet 100Base-TX

Categoría 5e, hasta 100 Mhz: Gigabit Ethernet

Categoría 6, hasta 250 Mhz.

Disposición de los hilos en un conector RJ45

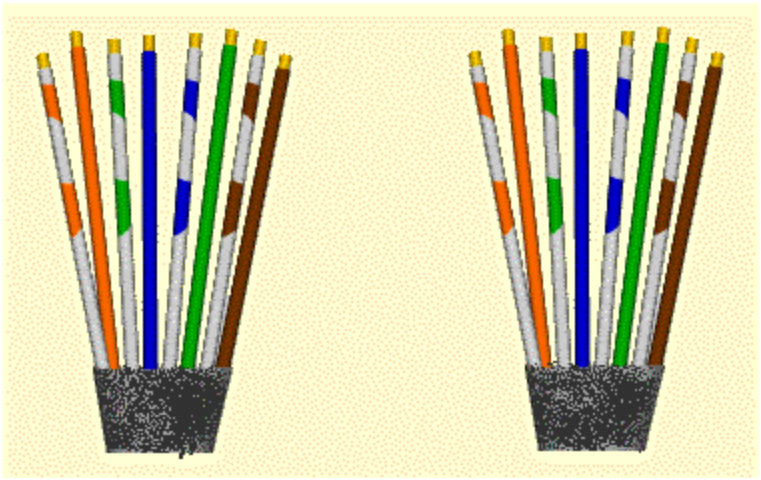
Aunque podríamos disponer como quisiéramos el orden de los cables, siempre y cuando todos los cables que engastemos mantengan el mismo orden en los extremos, y no tendríamos ningún problema de comunicación, existen normativas oficiales sobre el orden que ha de utilizarse en instalaciones certificadas.

La Norma EIA/TIA 568B RJ45: en donde se fija el estándar de cableado (requerimientos mecánicos y eléctricos, y componentes), normas desarrolladas por la *Electronics Industry Association* (EIA) y la *Telecomunications Industry Association* (TIA). El estándar 568B se conoce también como AT&T.

En este apartado describiremos la disposición en un par trenzado para interconectar varios equipos con un concentrador. En el caso de que quisiéramos unir dos ordenadores y no tuviéramos un concentrador deberíamos elaborar un cable cruzado; algo que veremos en el módulo 5.

La especificación IEEE para Ethernet 10/100 Base T Ethernet requiere usar sólo dos pares trenzados, un par es conectado a los pines 1 y 2, y el segundo a los pines 3 y 6. De acuerdo con la Norma EIA/TIA 568B RJ45 sólo el par Blanco/Naranja y Naranja, y el Par Blanco/Verde y Verde son los únicos usados para datos en 10 Base T. Los dos primeros sirven para la emisión de datos y los otros dos para la recepción.

RJ45	COLOR	RJ45	Función
1	Blanco/Naranja	1	Transmite
2	Naranja	2	Transmite
3	Blanco/Verde	3	Recibe
4	Azul	4	
5	Blanco/Azul	5	
6	Verde	6	Recibe
7	Blanco/Marrón	7	
8	*Marrón*	*8*	



Este es el orden en el que veremos los hilos al engastarlos en un conector RJ45, en los dos extremos veremos la misma disposición de los hilos. La posición de la pestaña del conector será hacia abajo. Hemos de recordar que la longitud del cable no debe exceder los 90 metros (aunque puede llegar hasta los 100 metros).

Cable de fibra óptica

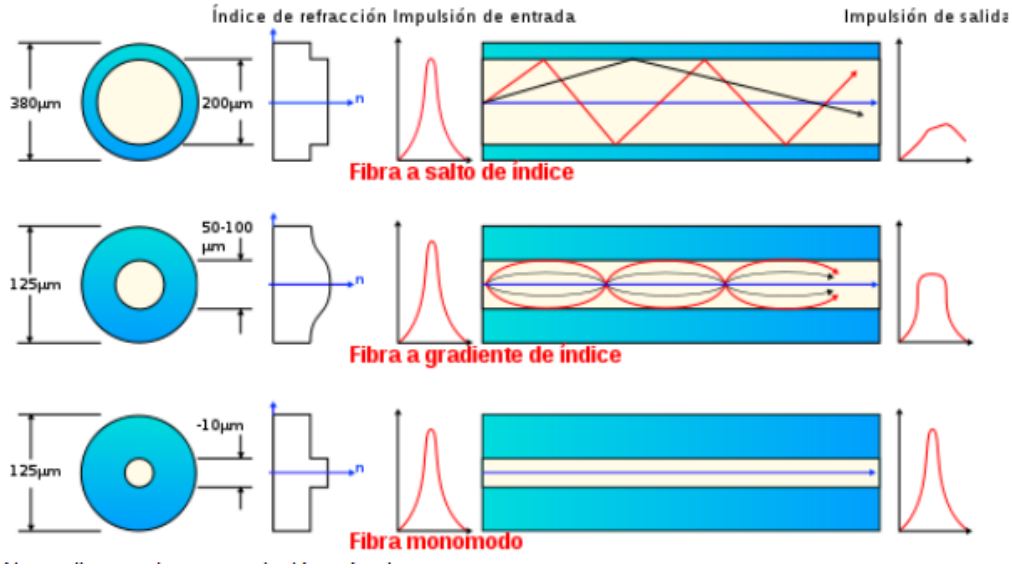
En los cables de fibra óptica la información se transmite en forma de pulsos de luz. En un extremo del cable se coloca un diodo luminoso (LED) o bien un láser, que emite la señal luminosa. Al otro extremo se sitúa un detector de luz. Este cable permite que la atenuación sea mínima y que no se produzca la interferencia de campos magnéticos, de manera que la longitud a la que se pueden transmitir los datos empleando un solo cable y la cantidad y velocidad en que se hace sea muy alta.

El medio de transmisión consiste básicamente en dos cilindros coaxiales de vidrios transparentes y de diámetros muy pequeños. El cilindro interior se denomina núcleo y el exterior se denomina envoltura, siendo el índice de refracción del núcleo algo mayor que el de la envoltura. En la superficie de separación entre el núcleo y la envoltura se produce un fenómeno de reflexión total de la luz, debido a la diferencia en el índice de refracción. Como consecuencia de esta estructura óptica todos los rayos de luz que se reflejan totalmente en dicha superficie se transmiten guiados a lo largo del núcleo de la fibra. Este conjunto está envuelto por una capa protectora.

Existen dos formas de transmisión:

Monomodo: La luz, generada por un laser, viaja por el núcleo sin reflejarse en las paredes, presentando una única longitud de onda.. El cable empleado es grueso y apenas si se puede emplear en instalaciones LAN debido a que soporta muy bajo ángulo de curvatura.

Multimodo: La luz es producida por un led y viaja reflejándose en las paredes del cable transportando múltiples longitudes de onda.



CAPA DE ENLACE - ETHERNET

Ethernet es el medio más común que nos encontramos en una Red de Área Local (LAN). Conviven dos implementaciones muy parecidas, la Ethernet y la norma de IEEE 802.3, que está basada en la anterior. Ethernet es una especificación LAN de "banda base" Que operaba a 10 Mbps utilizando un protocolo de acceso múltiple al medio conocido como CSMA/CD (Carrier Sense Multiple Access/Collition Detect) sobre un cable coaxial.

Ethernet fue creado en Xerox en los años 70, pero el término es usualmente referido para todas las LAN CSMA/CD. La especificación IEEE 802.3 fue desarrollada en 1980 basada sobre la tecnología original Ethernet. La versión

2.0 de Ethernet fue desarrollada conjuntamente por DEC (Digital Equipment Corporation), Intel, y Xerox y es compatible con el estándar IEEE 802.3. El estándar IEEE 802.3 provee una gran variedad de opciones de cableado. Tanto Ethernet como IEEE 802.3 se implementan normalmente en la tarjeta de red.

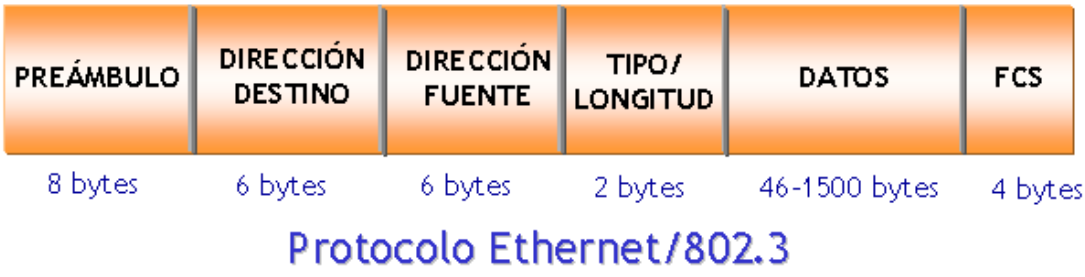
Direcciones MAC

Todos los interfaces compatibles Ethernet/802.3 poseen una Dirección MAC o Dirección Hardware única en el mundo, de 48 bits (o lo que es lo mismo, 6 bytes) de longitud. Cada fabricante de equipos ethernet tiene asignado un rango de direcciones, y es responsabilidad de éste asignar una dirección distinta a cada tarjeta de red. Las direcciones MAC están almacenadas en una pequeña memoria que poseen las tarjetas de red.

Las direcciones MAC se representan en hexadecimal con el siguiente formato: XX:XX:XX:XX:XX:XX.

Por ejemplo, 00-40-05-7F-CE-85, sería una dirección MAC válida Conviene decir que las direcciones MAC solamente sirven para comunicarse en un mismo medio físico, como por ejemplo, una Red de Área Local (LAN). Cuando hay que comunicarse con un dispositivo que no pertenece a esa LAN, entran en juego el nivel de red y las direcciones lógicas.

Estructura de la trama Ethernet



Protocolo Ethernet/802.3

Detalle de la estructura de la trama Ethernet/802.3

Preámbulo: (64 bits) El paquete comienza con una secuencia de unos y ceros alternados (de 56 bits en 802.3 ó de 62 bits en Ethernet), que se completa hasta 64 bits en ambos casos. El preámbulo recibido en la red no es pasado por la tarjeta de red hasta el sistema.

Dirección de Destino: (6 bytes) La dirección de destino (DD) es de 48 bits (6 bytes) de tamaño, de la cual se transmite primero el bit menos significativo. La DD es utilizada por la tarjeta del sistema receptor, para determinar si el paquete entrante es para él. Si el sistema receptor detecta una correspondencia entre su dirección MAC y la dirección que viene en el campo DD, recogerá el paquete. Los otros sistemas, a los que no se dirige la trama, ignorarán el resto del paquete.

Las direcciones de destino pueden ser:

1. Individual (física): El campo DD contiene una dirección única e individual asignada a un nodo en la red. Es decir, una dirección MAC de una tarjeta de la red.

2. Broadcast (difusión): El campo DD está formado todo por unos. Es una dirección especial y todos los dispositivos MAC de la red deberán recibir el mensaje de broadcast.

Dirección Fuente: (6 bytes) La dirección fuente (DF) es de 48 bits (6 bytes) de tamaño, transmitiéndose primero el bit menos significativo. El campo DF lo provee la MAC de la tarjeta emisora, la cual inserta su propia dirección física en este campo al transmitirse la trama, indicando que fue la estación origen. Los formatos de direcciones tipo broadcast son ilegales en el campo DF.

Longitud/Tipo: (2 bytes) El campo Longitud (en 802.3) o Tipo (en Ethernet) de 2 bytes va tras el campo DF. La elección de escoger Longitud o Tipo es dependiente de si la trama es 802.3 o Ethernet.

Datos: (46 - 1500 bytes) Este campo contiene los datos (la información útil que es transferida) cuyo tamaño varía de 56 a 1.500 bytes.

FCS (Frame Check Sequence): (4 bytes) Contiene el valor del algotimo CRC (Cyclic Redundancy Check) de 32 bits de la trama completa. El CRC es calculado por la estación emisora sobre los campos DD, DF, Longitud/Tipo y Datos y es anexado en los últimos 4 bytes de la trama. El mismo algoritmo

CRC es utilizado por la estación receptora para calcular el valor CRC en la trama recibida. El valor calculado por el receptor es comparado con el valor que fue puesto en el campo FCS por la estación emisora, obteniendo un mecanismo de detección de errores en caso de datos corruptos.

Protocolo CSMA/CD.

Expliquemos cómo funciona el protocolo de acceso al medio CSMA/CD. Son las siglas de Carrier Sense, Multiple Access with Collision Detect.

El problema que pretende resolver es cómo acceden a un medio compartido (el cable de red) varios ordenadores. Otro protocolo de acceso al medio es el Paso de Testigo, en donde solamente la estación que disponga del token puede transmitir en ese momento.

El protocolo CSMA/CD funciona de la siguiente forma. Cuando un ordenador necesita transmitir información, la tarjeta de red (que es donde se implementa el protocolo como dijimos antes) escucha en el cable, de forma parecida a como los indios del Oeste Americano escuchaban si venía un tren por la vía, pegando la oreja al raíl. Si está pasando información, tiene que esperarse durante un tiempo aleatorio. Si no pasa información en ese momento, puede transmitir. Hasta aquí la parte de Acceso Múltiple con Detección de Portadora. Poner la oreja y ver que no pasa nadie.

Puede ocurrir que dos estaciones hayan hecho lo mismo: escuchar, ver que no emitía nadie, y emitir ellas, produciéndose lo que se conoce como colisión. Para resolver el conflicto, lo que hace cada estación es emitir y quedarse un momento escuchando, por si se ha producido una colisión. Si se ha producido una colisión, cada estación da por no emitida la trama y espera un tiempo aleatorio para volver a intentarlo.

CAPA DE RED - IP

IP es el protocolo que oculta la red física subyacente creando una vista de red virtual. Es un protocolo de entrega de paquetes no fiable y no orientado a conexión, y se puede decir que aplica la ley del mínimo esfuerzo. No aporta

fiabilidad, control de flujo o recuperación de errores. Los paquetes (datagramas) que envía IP se pueden perder, desordenarse, o incluso duplicarse, e IP no manejará estas situaciones. El proporcionar estos servicios depende de protocolos superiores. IP asume pocas cosas de las capas inferiores, sólo que los datagramas "probablemente" serán transportados a la estación de destino.

La versión actual es la IP versión 4 (IPv4). Desde mediados de los años 90 se escucha que será sustituida por la nueva generación IPv6, pero diversos factores han hecho que no se haya producido dicha sustitución.

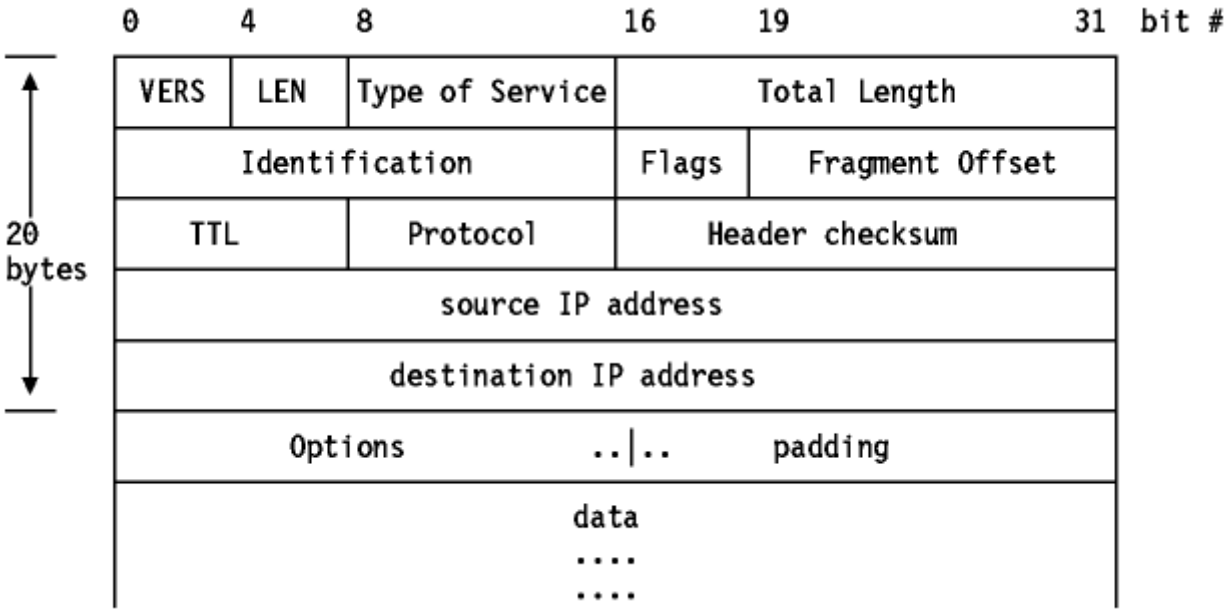
1.- IPv4 ha ido desarrollando mecanismos para resolver sus deficiencias, como el agotamiento de direcciones IP contrarrestado con el uso de direccionamiento privado, o la aparición de protocolos como SSL para añadirle la seguridad de la que carecía.

2.- IPv6 ha tardado en desarrollarse y probarse más de lo esperado, además de no proveer mecanismos suaves de evolución. Por ejemplo, al pasar de redes Ethernet a 10 Mbps a redes de 100 Mbps, el cambio en la mayoría de los sitios casi ha sido imperceptible.

3.- Las empresas y organismos han sentido pereza ante el cambio: si lo que tengo me funciona, porqué voy a cambiarlo, unido a la mayor complejidad de IPv6 que necesitará una formación y entrenamiento.

Hablaremos por tanto, todavía de IPv4.

Estructura del datagrama IP: El datagrama IP es la unidad de transferencia en la pila IP. Tiene una cabecera con información para IP, y su carga de datos para los protocolos superiores. La cabecera del datagrama IP es de un mínimo de 20 bytes de longitud:



En la En la figura se muestra la estructura del datagrama IP, donde:

VERS: La versión del protocolo IP. La versión actual es la 4. La 5 es experimental y la 6 es la nueva generación IPv6.

LEN: La longitud de la cabecera IP contada en cantidades de 32 bits. No incluye el campo de datos.

Type of Service: El tipo de servicio es una indicación de la calidad del servicio solicitado para este datagrama IP.

Total Length: La longitud total del datagrama, cabecera y datos, especificada en bytes.

Identification: Un número único que asigna el emisor para ayudar a reensamblar un datagrama fragmentado. Los fragmentos de un datagrama tendrán el mismo número de identificación.

Flags: Varios flags de control. Donde:

0 está reservado, debe ser cero
DF: No fragmentar (Don't Fragment): con 0 se permite la fragmentación, con 1 no.

MF: Más fragmentos (More fragments): 0 significa que se trata del último fragmento del datagrama, 1 que no es el último.

Fragment Offset: Usado con datagramas fragmentados, para ayudar al reensamblado de todo el datagrama. El valor es el número de partes de 64 bits (no se cuentan los bytes de la cabecera) contenidas en fragmentos anteriores. En el primer (o único) fragmento el valor es siempre cero.

Time to Live: Especifica el tiempo (en saltos de router) que se le permite viajar a este datagrama. Cada "router" por el que pase este datagrama ha de sustraer uno de este campo. Cuando el valor alcanza cero, se asume que este datagrama ha estado viajando sin llegar a su destino por alguna razón y se desecha. El valor inicial lo deberá fijar el protocolo de alto nivel que crea el datagrama.

Protocol Number: Indica el protocolo de alto nivel al que IP deberá entregar los datos del datagrama.

Algunos valores son:

0 Reservado
1 ICMP (Internet Control Message Protocol)
2 IGMP (Internet Group Management Protocol)
3 GGP (Gateway-to-Gateway Protocol)
4 IP (IP encapsulation)
5 Flujo (Stream)
6 TCP (Transmission Control)
8 EGP (Exterior Gateway Protocol)
17 UDP (User Datagram)
89 OSPF (Open Shortest Path First).

Header Checksum: Es el checksum de la cabecera. Si su comprobación no es válida, el datagrama se desecha, ya que al menos un bit de la cabecera está corrupto, y el datagrama podría haber llegado al destino equivocado. No tenemos la seguridad de que lo que esté mal sean las direcciones.

Source IP Address: La dirección IP de 32 bits del host emisor.

Destination IP Address: La dirección IP de 32 bits del host receptor.

Options: No requiere que toda implementación de IP sea capaz de generar opciones en los datagramas que crea, pero sí que sea capaz de procesar datagramas que contengan opciones. El campo "Options" (opciones) tiene longitud variable. Puede haber cero o más opciones

Direcciones IP

Las direcciones TCP/IP pueden ser simbólicas o numéricas. La forma simbólica es más fácil de leer y recordar por las personas, por ejemplo: www.iesjuandelacierva.com. La forma numérica es un número binario sin signo de 32 bits, habitualmente expresado en forma de números decimales separados por puntos. Por ejemplo, 150.214.5.11 es una dirección numérica.

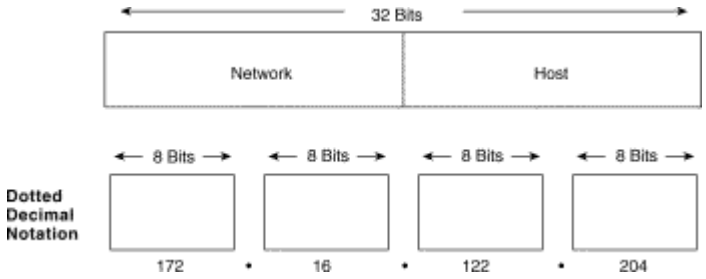
La forma numérica es usada por las máquinas porque es más eficiente y es la que utilizan los protocolos de nivel de red. La función de correspondencia entre los dos tipos de direcciones, la simbólica y la numérica, la realiza el sistema de DNS (Domain Name System). A partir de ahora, nos referiremos a la forma numérica, cuando hablemos de dirección IP.

Las direcciones IP son números de 32 bits, habitualmente expresados como cuatro valores decimales separados por puntos. El formato binario para la dirección IP 128.2.7.9 es:

10000000 00000010 00000111 00001001.

Cada interfaz de una máquina conectada a una red TCP/IP tiene asignada una dirección IP. Por interfaz de red entendemos el dispositivo que nos une a la red, como una tarjeta de red o un módem. Dos nodos conectados a una misma red no pueden tener la misma dirección IP. Todas las máquinas conectadas a una misma red poseen direciones IP con los primeros bits iguales (bits de red), mientras que los bits restantes son los que identifican a cada máquina concreta dentro de esa red.

Las máquinas que pertenecen a una misma red IP, pueden comunicarse directamente unas con otras. Para comunicarse con máquinas de una red IP diferente, deben hacerlo mediante mecanismos de interconexión como routers, proxys o gateways.



A la parte de la dirección IP que es común a todas las direcciones que se encuentran en una red IP, se le llama laparte de la red (network). Los bits restantes son llamadosparte del puesto (o de host).

El tamaño de la parte dedicada al puesto depende del tamaño de la red. Entre estas dos partes deben completar los 32 bits. Para satisfacer diferentes necesidades, se han definido varias clases de redes, fijando diferentes sitios donde dividir la dirección IP. Las clases de redes se dividen en las siguientes:

Clase A:

Comprende redes desde 1.0.0.0 hasta 127.0.0.0. El número de red está contenido en el primer octeto (byte). Esta clase ofrece una parte para el puesto de 24 bits, permitiendo aproximadamente 1,6 millones de puestos por red.

Clase B:

Comprende las redes desde 128.0.0.0 hasta 191.255.0.0; el número de red está en los dos primeros octetos. Esta clase permite 16.320 redes con 65.024 puestos cada una.

Clase C:

Van desde 192.0.0.0 hasta 223.255.255.0, con el número de red contenido en los tres primeros octetos. Esta clase permite cerca de 2 millones de redes con 254 puestos cada una.

Clases D, E, y F:

Las direcciones que están en el rango de 224.0.0.0 hasta 254.0.0.0 son experimentales o están reservadas para uso con propósitos especiales. IP Multicast, un servicio que permite trasmitir información a muchos puntos en una internet a la vez, tiene direcciones dentro de este rango.

Al número de bits que comparten todas las direcciones de una red se le llama máscara de red (netmask), y su papel es determinar qué direcciones pertenecen a la red y cuáles no. Veámoslo con un ejemplo.

	Decimal	Binario
Dirección de puesto	192.168.1.5	11000000.10101000.00000001.00000101
Máscara de red	255.255.255.0	11111111.11111111.11111111.00000000
Parte de red	192.168.1.	11000000.10101000.00000001.
Parte de puesto	.5	.00000101
Dirección de red	192.168.1.0	11000000.10101000.00000001.00000000
Dirección de difusión	192.168.1.255	11000000.10101000.00000001.11111111

Una dirección de puesto IP (192.168.1.5) a la que se aplique una operación "and"de bits con su máscara de red (255.255.255.0), nos dará la dirección de la red a la que pertenece (192.168.1.0). La dirección de red será el menor número de dirección IP dentro del rango de la red porque tiene la parte de puesto toda con ceros.

Una red IP queda definida por la dirección de la red y la máscara de la red. La notación que se usa para referirnos a dicha tupla es dirección de red/máscara de red (192.168.1.0/255.255.255.0) o dirección de red/número de bits de red (192.168.1.0/24).

En esta red, para la parte de puesto han quedado 8 bits, que nos darán 2^8 = 256 direcciones posibles.

Siempre hay que quitar dos direcciones especiales, que son la dirección de la red (todo a ceros) y la dirección de broadcast (todo a unos). Entonces, quedarán 254 direccciones posibles para puestos dentro de la red. La dirección de difusión (broadcast) es una dirección especial a la que escucha cada máquina en la red IP, además de a la suya propia. Esta dirección es a la que se envían los paquetes de datos si se supone que todas las máquinas de la red lo deben recibir.

Ciertos tipos de datos, como la información de encaminamiento y los mensajes de aviso son transmitidos a la dirección de difusión para que cada estación en la red pueda recibirlo simultáneamente. Para ello se utiliza la dirección más alta posible en la red, conseguida con la parte de red a la que se

añade el resto de bits (de la parte de puesto) todos con valor a uno (1). En el ejemplo anterior sería 192.168.1.255.

Desde el punto de vista de su accesibilidad, podemos clasificar las direcciones IP en:

Direcciones IP públicas: aquellas que son visibles por todos los puestos conectados a Internet. Para que una máquina sea visible desde Internet debe tener asignada obligatoriamente una dirección IP pública, y no puede haber dos puestos con la misma dirección IP pública.

Direcciones IP privadas: aquellas que son visibles únicamente por los puestos de su propia red privada. Los puestos con direcciones IP privadas no son visibles desde Internet, por lo que si quieren alir a ésta deben hacerlo a través de un router o un proxy. Las direcciones IP privadas se utilizan en redes de empresas, organismos, centros para interconectar los puestos de trabajo. Se definen en el RFC30 1918, que ha sustituido al RFC 1597.

Si estamos construyendo una red privada y no tenemos intención de conectar nunca esa red a Internet entonces podríamos elegir las direcciones que queramos, pues no vamos a colisionar con nadie, sin embargo, es buena práctica utilizar direcciones privadas por si en el futuro nos conectáramos. Estas direcciones son:

Dirección	Bits de red	Máscara de red	Número de redes
10.0.0.0	8	10.255.255.255	1 de clase A
172.16.0.0	12	172.31.255.255	16 de clase B
192.168.0.0	16	192.168.255.255	256 de clase C

Estas direcciones no se corresponden con las de ninguna máquina en Internet y no se encaminarán a través de los "routers" de Internet. Podremos utilizarlas de forma interna, con la ventaja de que si conectamos mediante un proveedor a Internet, nuestras direcciones no coincidirán con las de ninguna máquina de Internet.

En este caso, puede que haya multitud de equipos en redes distintas con estas mismas direcciones IP, pero como estas direcciones no se "rutean" no hay por qué coordinar su uso. En el caso de que se conecten a Internet, se habilitan mecanismos como la traducción de direccciones (NAT) o el uso de intermediarios (proxys) para que las direcciones que salgan a Internet sean direcciones válidas.

También la dirección 127.0.0.1, denominada de bucle local (loopback), es una dirección especial, que como veremos utiliza la propia máquina para acceder a sus procesos locales.

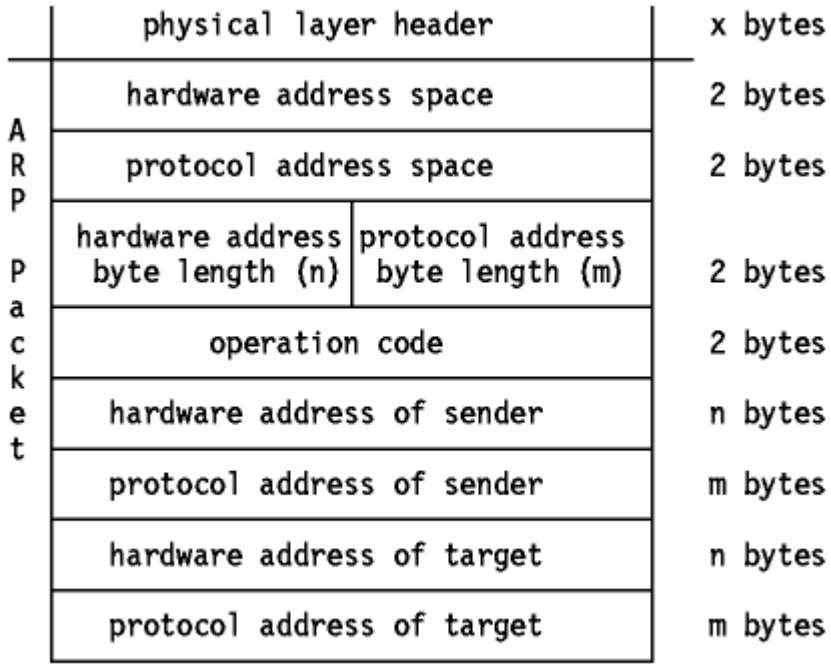
Protocolo ARP

En una red física, los hosts individuales se conocen en la red a través de su dirección física. Los protocolos de más alto nivel direccionan a los hosts de destino con una dirección lógica. Cuando se quiere enviar un mensaje a una dirección IP de destino que se encuentra en nuestra red, 172.26.0.5, el manejador de dispositivo físico no sabe a qué dirección MAC enviarla.

Para resolver este problema, se suministra un protocolo (el ARP) que traducirá la dirección IP a la dirección física del host de destino. No es un protocolo que transporte datos, sino que tiene un propósito específico: asociar direcciones lógicas con direcciones físicas.

Existe un protocolo, el RARP (Reverse ARP) cuyo propósito es el complementario: sabiendo una dirección física, obtener la dirección lógica que le corresponde. Se utiliza cuando tenemos un dispositivo (una impresora, por ejemplo) que debe arrancar e integrarse en la red con una dirección lógica, y lo único que conoce es su dirección física. En este caso debe existir un servidor (con el protocolo DHCP o bootp) que se encargue de gestionar estas asignaciones.

Veamos cómo funciona el protoolo ARP. Utiliza una tabla (llamada caché ARP) para realizar esta traducción. Cuando la dirección física no se encuentra en la caché ARP, se envía un broadcast a la red, con un formato especial llamado petición ARP. Si una de las máquinas en la red reconoce su propia dirección IP en la petición, devolverá una respuesta ARP al host que la solicitó. La respuesta contendrá la dirección física del hardware, así como información de encaminamiento (si el paquete ha atravesado puentes durante su trayecto). Tanto esta dirección como la ruta se almacenan en la caché del host solicitante. Todos los posteriores datagramas enviados a esta dirección IP se podrán asociar a la dirección física correspondiente, que será la que utilice el manejador de dispositivo para mandar el datagrama a la red.



Este es el formato del paquete ARP, donde tras la cabecera de la capa física vienen:

Hardware address space: Especifica el tipo de hardware; ejemplos son Ethernet o Packet Radio.

Protocol address space: Especifica el tipo de protocolo, el mismo que en el campo de tipo EtherType en la cabecera de IEEE 802.

Hardware address length: Especifica la longitud (en bytes) de la dirección hardware del paquete.
Para Ethernet e IEEE 802.3 será de 6 bytes.

Protocol address length: Especifica la longitud (en bytes) de la dirección lógica. Para IP será de 4 bytes.

Operation code: Especifica el tipo de operación ARP.

Source/target hardware address: Contiene las direcciones físicas hardware. En IEEE 802.3 son direcciones de 48 bits.

Source/target protocol address: Contiene las direcciones lógicas. En TCP/IP son direcciones IP de 32 bits.

Para el paquete de solicitud, la dirección hardware de destino es el único campo indefinido del paquete, que es el que pretende obtener.

El host solicitante recibirá la respuesta ARP, y seguirá el proceso ya comentado para tratarla. Como resultado, la tripleta <tipo de protocolo, dirección de protocolo, dirección hardware> para el host en cuestión se añadirá a la caché ARP. La próxima vez que un protocolo de nivel superior quiera enviar un paquete a ese host, el módulo de ARP encontrará la dirección hardware, a la que se enviará el paquete.

Ejemplo: Mediante el comando arp podemos mostrar la caché arp en un sistema linux:

```
[root@llocalhost]# arp -e
Address HWtype HWaddress Flags Mask Iface
172.26.0.1 ether 00:01:38:11:D6:03 C eth0
```

Capa de transporte del protocolo TCP-IP

Protocolo TCP

La capa de transporte ofrece a la capa de aplicación dos servicios: un servicio orientado a conexión protocolo TCP "Transmition Control Protocol" y un servicio no orientado a conexión protocolo UDP "User Datagram Protocol". La unidad de envío o recepción datos del protocolo TCP se conoce con el nombre de segmento TCP y la unidad de envío o recepción de datos del protocolo UDP es conocido como datagrama UDP.

La función protocolo TCP consiste en ofrecer un servicio de envío y recepción de datos orientado a conexión que sea seguro y que goce de los siguientes mecanismos:

-. Multiplexamiento.

-. Conexiones.

-. Fiabilidad.

-. Control de flujo y congestión.

Macanismo de Multiplexamiento

El mecanismo de multiplexamiento consiste en que más de una aplicación pueda utilizar los servicios del protocolo TCP. El protocolo TCP hace uso de los parámetros de control: Puerto destino y Puerto origen incluidos en una cabecera TCP y los parámetros de control: Dirección IP Destino y Dirección IP Origen incluidos en una cabecera IP con el fin de satisfacer el mecanismo de multiplexamiento.

Cuando los números de puerto son concatenados con las direcciones IP de la capa de enrutamiento, conforman lo que se denomina un conector "socket". Un par de conectores identifica de forma única la conexión bidireccional entre una aplicación cliente y una aplicación servidor.

Los puertos de las aplicaciones que ofrecen servicios a las aplicaciones clientes han sido estandarizados y se conocen con el nombre de "puertos bien conocidos". La organización que controla y estandariza el número de un puerto es la IANA "Internet Assigned Numbers Authority".

El número de puerto de una aplicación está definido por un registro de 16 bit "parámetro de control Puerto destino y/o puerto origen", esto implica un rango de puertos que va de 0 a 65535 puertos. El rango de puertos que va de 0 a 1023 son conocidos con el nombre de puertos privilegiados. Los procesos que hacen uso de estos puertos son ejecutados con privilegio root.

En un encabezado TCP el número de puerto que refleja el parámetro puerto origen es el número de puerto de la aplicación que está enviando los datos. Y el número de puerto que refleja el parámetro puerto destino es el número de puerto de la aplicación destino.

Mecanismo de conexión:

Como el protocolo TCP es un protocolo orientado a conexión, es necesario iniciar y mantener la información del estado para cada conexión TCP. Cada conexión queda identificada de forma única por un par de conectores que corresponden con sus dos extremos "Socket".

Cuando dos procesos "cliente/servidor" desean comunicarse, el protocolo TCP debe establecer primero una conexión (inicializar la información de estado en cada lado) y cuando la comunicación se ha completado, la conexión se termina con la intención de liberar recursos en el sistema.

Como las conexiones tienen que establecerse entre "computadoras, enrutadores, etc." y sobre un servicio no orientado a conexión ofrecido por la capa de enrutamiento, el protocolo TCP utiliza un mecanismo de acuerdo que usa números de secuencia para la inicialización de las conexiones.

Mecanismo de fiabilidad

Con el fin de poder recuperar los datos que se corrompan, pierdan, dupliquen o se entreguen desordenados por los servicios de la capa de enrutamiento, el protocolo TCP está diseñado para satisfacer los principios de un protocolo orientado a conexión, es decir; que por cada segmento enviado por el emisor este debe recibir un número de acuse de recibido enviado por el receptor.

Es importante resaltar que no existe ninguna restricción en el protocolo TCP sobre el hecho de reutilizar más de una vez una misma conexión. Como hemos explicado anteriormente una conexión se define por un par de conectores "Sockets". Cualquier nueva instancia de una conexión será referida como una encarnación de la conexión. ¿Cómo el protocolo TCP identifica los segmentos duplicados de encarnaciones previas?. Esta condición es posible si la conexión presenta momentos de inestabilidad, es decir; que una conexión se abre y se cierra varias veces de forma contínua debido a la inestabilidad en la línea de transmisión o por falta de recursos en el sistema.

Para evitar que el protocolo TCP se confunda, se debe evitar que los segmentos de una encarnación utilicen los números de secuencia que posiblemente estén siendo utilizados por el protocolo TCP por una encarnación anterior. Para asegurarnos de esto es necesario que cuando se creen nuevas conexiones, el protocolo TCP haga uso de un generador de números iniciales de secuencia (ISN, 'initial sequence number') para eligir un nuevo ISN de 32 bits por cada conexión nueva. Este generador está asociado a un reloj de 32 bit, cuyo bit menos significativo se incrementa aproximadamente cada 4 microsegundos. Esto implica que un número inicial de secuencia rote aproximadamente cada 4.55 horas. Partiendo de esta premisa queda razonablemente explícito suponer que los números de secuencia iniciales serán únicos durante el proceso de sincronización de una conexión ya que cada implementación del protocolo TCP tiene que elegir un valor que determine el tiempo de vida máximo de un segmento en la red "Maximun Segment Life MSL". Si este tiempo de vida es mayor que el definido, el protocolo TCP descarta el segmento.

Cada que vez que el protocolo TCP cierra una conexión o envia el último número de acuse de recibo, el protocolo TCP debe de dejar activa la conexión por un tiempo igual a dos veces el tiempo de vida máximo de un segmento. Con esta acción se asegura que el último número de acuse recibido es procesado por el protocolo TCP. Este tiempo varía entre sistemas operativos.

El protocolo TCP trata a la corrupción de datos con el uso del parámetro de control Suma de control "Checksum" por cada segmento transmitido, comprobándose en el receptor y descartando los segmentos dañados. El campo "Suma de control" es el complemento "a uno" de 16 bits de la suma de los complementos "a uno" de todas las palabras de 16 bits de la cabecera y del texto. Si un segmento contiene un número impar de octetos de cabecera y texto, el último octeto se rellena con ceros a la derecha para formar una palabra de 16 bits con el propósito de calcular la suma de control. En el cálculo de la suma de control, el propio campo suma de control se considera formado por ceros. La suma de control también incluye una pseudocabecera de 96 bits prefijada imaginariamente a la cabecera TCP ver figura 1.4. Esta pseudocabecera contiene la dirección de origen, la dirección de destino, el protocolo, y la longitud del segmento de TCP. Esto proporciona una protección ante segmentos mal encaminados. Esta información es transportada por el

protocolo de internet y es transferida a través de la interfaz TCP/Red en los argumentos o en los resultados de las llamadas de TCP a IP.

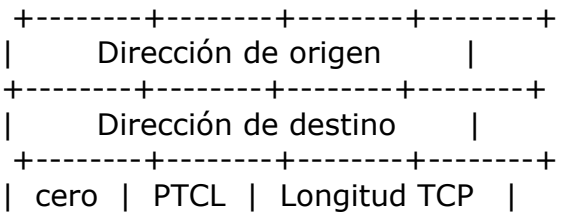


Figura 1.4 Pseudocabecera TCP

La "longitud TCP" consiste en la suma de la longitud de la cabecera de TCP más la de los datos en octetos (esto no es una cantidad transmitida explícitamente, sino que ha de calcularse), y no incluye los 12 octetos de la pseudocabecera.

Mecanismo de cotrol de flujo

El protocolo TCP está diseñado para controlar el envío y recepción de segmentos TCP a fin de evitar momentos de congestión en la red. Las principales técnicas de control de flujo implementadas en el protocolo TCP son:

-. Desplazamiento de ventana "Sliding Window".

-. Comienzo lento "Slow Start" y control de congestión.

La técnica de desplazamiento de ventana es una técnica de control del flujo impuesta por el receptor de segmentos TCP con el fin de evitar momentos de congestión en el computador receptor. Durante el proceso de inicialización de una conexión TCP, el proceso TCP de cada computador da a conocer los parámetros de control ventana y MSS. Con estos dos parámetros el proceso de

envío de segmentos del protocolo TCP puede calcular el máximo número de segmentos que puede recibir el proceso de recepción del protocolo TCP en un momento determinado. El parámetro ventana incluido en una cabecera TCP es un registro de 16 bits y el valor del mismo puede variar durante el envío y recepción de segmentos TCP hasta llegar al punto de que sea igual a cero. Cuando esto ocurre indica que el proceso de recepción de segmentos no está en capacidad de recibir ningún segmento TCP ya que el buffer de recepción se encuentra completamente lleno. Esto obliga al proceso de envío de segmentos TCP del computador remoto no transmitir ningún segmento hasta que el parámetro de control ventana sea mayor o igual a un segmento.

Esta técnica funciona si la conexión TCP se establece en una red local pero cuando la conexión TCP se establece a través de una red WAN los enrutadores pueden experimentar momentos de congestión ya que los mismos interactúan con un servicio de conexión no orientado y la capacidad de envío y recepción de datos de un enlace WAN en la mayoría de los casos es mucho menor que el de una red LAN. Para resolver este inconveniente el protocolo TCP hace uso de la técnicas comienzo lento "Slow Start" y control de congestión. Estas técnicas son técnicas de control de flujo impuestas en el emisor para evitar momentos de congestión en la red.

Las técnicas slow start y control de congestión consisten en que el transmisor de segmentos TCP hace uso de los parámetros de control: ventana de congestión y umbral de congestión. El parámetro de control ventana de congestión es utilizado para calcular el máximo número de segmentos que pueden ser transmitidos por el transmisor en un momento determinado. Y el parámetro umbral de congestión es utilizado para detectar momentos de congestión en la red.

El valor inicial del parámetro congestión de ventana es igual al parámetro MSS y el valor inicial del umbral de congestión es igual a 65535. Por cada número de acuse recibido de cada segmento transmitido el parámetro congestión de ventana se incrementa a un MSS; esto implica un posible crecimiento exponencial de este parámetro.

El máximo número de segmentos TCP que el transmisor puede enviar en un monento dado es seleccionado por el mínimo valor de la comparación de los

parámetros Ventana y Congestión de ventana, es decir; que si el valor del parámetro Ventana es igual a 4096 bytes y el parámetro Congestión de ventana es igual a 2048 bytes. El transmisor de segmentos TCP hará uso del parámetro congestión de ventana para determinar el máximo número de segmentos que pueden ser transmitidos en un momento dado. El crecimiento del parámetro congestión de ventana se detiene hasta que el mismo sea igual al parámetro de control ventana.

Si el transmisor de segmentos TCP detecta un posible momento de congestión en la red debido a que el tiempo de espera de un número de acuse recibido expiró, el protocolo slow start se inicia nuevamente inicializando la ventana de congestión con el valor asignado al MSS y el parámetro umbral de congestión se le asigna un valor igual a la mitad de la ventana de transmisión pero nunca por debejo de dos segmentos. Esto implica que el umbral de congestión es determinado por la siguiente fórmula:

Umbral de congestion = max [2 segmentos, 1 / 2 min(ventana, ventana de congestion)]

Luego la técnica slow start entra en acción hasta que el parámetro congestión de ventana sea mayor que el umbral del congestión. Cuando esto ocurre el crecimiento de la ventana de congestión deja de ser exponencial ya que se incrementa a uno no por cada número de acuse recibido por segmento sino por el grupo de números de acuse recibido del rango de segmentos que son incluidos en la ventana de congestión en ese momento.

Se dice que el protocolo de transmisión TCP se encuentra en el estado slow start si la ventana de congestión es menor o igual al umbral de congestión. Y si la ventana de congestión es mayor que el umbral de congestión se dice que el protocolo de transmisión se encuentra en un estado de control de congestión.

Control de flujo para aplicaciones interactivas

Cuando las aplicaciones interactivas Ejemplo: Telnet hacen uso de los servicios de la capa de transporte por cada caracter a ser enviado, el protocolo TCP crea un segmento TCP de 21 Bytes que al ser encapsulado por la capa de

enrutamiento tenemos un paquete de 41 Bytes. Una vez que este paquete es recibido y procesado, el computador destino envía un paquete IP de 40 bytes, el cual incluye el número de acuse recibido del segmento enviado. Esto implica que por cada caracter a ser enviado se requieren como mínimo de 81 Bytes. Para optimizar esta situación en el receptor muchas de las aplicaciones retardan el envío de los números de acuse recibido o las actualizaciones de ventanas a un tiempo fijo, el cual varía dependiendo de la aplicación TCP. Este retardo se encuentra en el rango de 200mseg - 500mseg. Para el transmisor se hace uso del algoritmo de Nagle el cual consiste en enviar el primer caracter y almacenar en un buffer los posibles nuevos caracteres que serán enviados cuando se reciba el número de acuse recibido del primer caracter.

Tiempo de espera de retransmisión

Debido a la variabilidad de las redes que componen el sistema de redes de la red Internet y la gran cantidad de casos de conexiones TCP, el tiempo de espera de retransmisión se debe determinar dinámicamente ya que el tiempo de ida y vuelta es distinto para cada conexión TCP. Veamos a continuación un procedimiento para determinar un tiempo de espera de retransmisión.

-. Mídase el tiempo transcurrido entre el envío de un octeto de datos con un número de secuencia determinado y la recepción de un acuse de recibo que incluya ese número de secuencia (los segmentos enviados no tienen por qué concordar con los segmentos recibidos). Este tiempo medido es la muestra del tiempo de ida y vuelta 'Round Trip Time' o RTT.

-. Calcular un promedio ponderado del RTT:

-. RTT-Estimado = alpha x RTT-Estimado + Beta * RTT-Muestra. Donde alpha + beta = 1. alpha entre 0.8 y 0.9 y beta entre 0.1 y 0.2.

-. El tiempo de espera de retransmisión => RTO = 2 * RTT-Estimado.

El incoveniente de este algoritmo es que no se distingue entre un Ack del segmento enviado

y un Ack de retransmisión.

Los algoritmos de Karn y Partridge solucionan este problema no tomando muestras del RTT al retransmitir un segmento y duplicando el RTO despues de cada retransmisión.

Opciones

La implementación del protocolo TCP basado en el RFC 793 sólo incluye las opciones: fin de la lista de opciones, no operación y el tamaño máximo del segmento. En el RFC 1323 se definen las siguientes opciones: Factor de posicionamiento de la ventana "Window Scale Factor" y Timestamp.

-. Factor de posicionamiento de la ventana: Está opción es utilizada para incrememtar el parámetro de control ventana de un registro de 16 bits a un registro de 32 bits sin tener que modificar el parámetro de control ventana definido en una cabecera TCP. Esta opción está definida por un registro de tres bytes. En el primer byte se define el tipo de opción que para este caso es igual a tres, en el segundo byte se define el número de bytes de la opción, que para este caso es igual tres bytes, y el último byte define el factor de escala del registro ventana. Es importante mencionar que el valor máximo definido en el RFC 1323 del registro del factor de escala es igual a 14.

Cuando esta opción está presente en la petición inicial de una conexión TCP, el parámetro de control ventana es calculado por la siguiente fórmula:

Ventana con factor de escala = ventana * 2 ^ factor de escala.

Esto implica que el máximo valor del parámetro de control ventana una vez aplicado el factor de escala de una ventana es:

1.073.725.440 Bytes = 65535 * 2 ^ 14.

Esta opción es utilizada para redes de alta velocidad con el fin de evitar el efecto del producto del ancho de banda en una conexión TCP.

-.Timestamp: Esta opción le ofrece al protocolo TCP un mecanismo para calcular el RTT por cada número de acuse recibido. Por cada segmento a ser enviado se registra el momento de envío en el campo de opciones => Timestamp y en el momento de envío del acuse de recibido se registra el momento de envío en el campo de opciones => Timestamp. De esta manera el módulo TCP puede tener un aproximado del RTT.

Este campo debe enviarse en la petición inicial de la conexión TCP. Si esta opción no está presente en una cabecera TCP este mecanismo no se activa.

Routers y Switches

ROUTER

Un router es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador (mediante puentes de red), y que por tanto tienen prefijos de red distintos.

SWITCH

Conmutador (switch) es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada ésta.

Los conmutadores se utilizan cuando se desea conectar múltiples tramos de una red, fusionándolos en una sola red. Al igual que los puentes, dado que funcionan como un filtro en la red y solo retransmiten la información hacia los tramos en los que hay el destinatario de la trama de red, mejoran el rendimiento y la seguridad de las redes de área local (LAN).

HUB

Un HUB, también llamado concentrador, es un aparato que hace de puente al que podemos conectar varios dispositivos, generalmente electrónicos, usando solo una conexión del dispositivo al que queremos conectar estos aparatos, el HUB posee varias entradas y una salida o en algunos casos varias salidas y una entrada. De esta manera podemos conectar a sus entradas varios aparatos y usarlos de uno en uno o todos a la vez. Si es al contrario podemos conectar varios dispositivos de salida y usar la entrada en todas las fuentes de salida o solo en una de ellas.