Redes de área local

Federico Reina Toranzo
Juan Antonio Ruiz Rivas

CONTENIDOS

Teoría de la comunicación

Elementos de un sistema de comunicación

Los elementos que integran un sistema de comunicación son:

- Fuente o mensaje
- Emisor
- Medio o canal
- Receptor

El mensaje

Es la información que tratamos de transmitir, puede ser analógica o digital.

Lo importante es que llegue íntegro y con fidelidad.

El emisor

Sujeto que envía el mensaje.

Prepara la información para que pueda ser enviada por el canal, tanto en calidad (adecuación a la naturaleza del canal) como en cantidad (amplificando la señal).

La transmisión puede realizarse

- **en banda base**, o sea, en la banda de frecuencia propia de la señal, el ejemplo más claro es el habla.
- **modulando,** es decir, traspasando la información de su frecuencia propia a otra de rango distinto, esto nos va a permitir adecuar la señal a la naturaleza del canal y además nos posibilita el **multiplexar** el canal, con lo cual varios usuarios podrán usarlo a la vez.

El medio

Es el elemento a través del cual se envía la información del emisor al receptor.

Desgraciadamente el medio puede introducir en la comunicación:

- Distorsiones.
- Atenuaciones (pérdida de señal).
- Ruido (interferencias).

Dos características importantes del medio son:

- Velocidad de transmisión, se mide en bits por segundo.
- Ancho de banda, que es el rango de frecuencias en el que opera la señal. Por ejemplo la red telefónica opera entre 300 y 3400 Hz, la televisión tiene un ancho de banda de 5'5 MHz.

El receptor

Tendrá que demodular la señal, limpiarla y recuperar de nuevo el mensaje original.

Redes LAN, MAN y WAN

Un criterio para clasificar redes de ordenadores es el que se basa en su extensión geográfica, es en este sentido en el que hablamos de redes LAN, MAN y WAN, aunque esta documentación se centra en las redes de área local (LAN), nos dará una mejor perspectiva el conocer los otros dos tipos: MAN y WAN.

Redes de Área Local (LAN)

Son redes de propiedad privada, de hasta unos cuantos kilómetros de extensión. Por ejemplo una oficina o un centro educativo.

Se usan para conectar computadoras personales o estaciones de trabajo, con objeto de compartir recursos e intercambiar información.

Están restringidas en tamaño, lo cual significa que el tiempo de transmisión, en el peor de los casos, se conoce, lo que permite cierto tipo de diseños (deterministas) que de otro modo podrían resultar ineficientes. Además, simplifica la administración de la red.

Suelen emplear tecnología de difusión mediante un cable sencillo al que están conectadas todas las máquinas.

Operan a velocidades entre 10 y 100 Mbps.

Tienen bajo retardo y experimentan pocos errores.

Redes de Área Metropolitana (MAN)

Son una versión mayor de la LAN y utilizan una tecnología muy similar. Actualmente esta clasificación ha caído en desuso, normalmente sólo distinguiremos entre redes LAN y WAN.

Redes de Área Amplia (WAN)

Son redes que se extienden sobre un área geográfica extensa. Contiene una colección de máquinas dedicadas a ejecutar los programas de usuarios (hosts). Estos están conectados por la red que lleva los mensajes de un host a otro. Estas LAN de host acceden a la subred de la WAN por un router. Suelen ser por tanto redes punto a punto.

La subred tiene varios elementos:

- Líneas de comunicación: Mueven bits de una máquina a otra.
- Elementos de conmutación: Máquinas especializadas que conectan dos o más líneas de transmisión. Se suelen llamar encaminadores o routers.

Cada host está después conectado a una LAN en la cual está el encaminador que se encarga de enviar la información por la subred.

Una WAN contiene numerosos cables conectados a un par de encaminadores. Si dos encaminadores que no comparten cable desean comunicarse, han de hacerlo a través de encaminadores intermedios. El paquete se recibe completo en cada uno de los intermedios y se almacena allí hasta que la línea de salida requerida esté libre.

Se pueden establecer WAN en sistemas de satélite o de radio en tierra en los que cada encaminador tiene una antena con la cual poder enviar y recibir la información. Por su naturaleza, las redes de satélite serán de difusión.

Tipología de las redes de área local.

Hay muchos parámetros que conforman la arquitectura de una red de área local, aquí veremos algunos de ellos.

- **Según la técnica de transmisión**: redes de difusión y redes punto a punto.
- **Según método de acceso al medio:** CSMA y Token.
- **Por su topología o disposición en el espacio**: estrella, bus, anillo y mixtas.

Técnicas de transmisión

Redes de difusión

Tienen un solo canal de comunicación compartido por todas las máquinas, en principio todas las máquinas podrían "ver" toda la información, pero hay un "código" que especifica a quien va dirigida.

Redes punto a punto

Muchas conexiones entre pares individuales de máquinas.

La información puede pasar por varias máquinas intermedias antes de llegar a su destino.

Se puede llegar por varios caminos, con lo que se hacen muy importantes las rutinas de enrutamiento o ruteo. Es más frecuente en redes MAN y WAN.

Método de acceso al medio

En las redes de difusión es necesario definir una estrategia para saber cuando una máquina puede empezar a transmitir para evitar que dos o más estaciones comiencen a transmitir a la vez (colisiones).

CSMA

Se basa en que cada estación monitoriza o "escucha" el medio para determinar si éste se encuentra disponible para que la estación puede enviar su mensaje, o por el contrario, hay algún otro nodo utilizándolo, en cuyo caso espera a que quede libre.

Token

El método del testigo(token) asegura que todos los nodos van a poder emplear el medio para transmitir en algún momento. Ese momento será cuando el nodo en cuestión reciba un paquete de datos especial denominado testigo. Aquel nodo que se encuentre en posesión del testigo podrá transmitir y recibir información, y una vez haya terminado, volverá a dejar libre el testigo y lo enviará a la próxima estación.

Topología

Se entiende por topología de una red local la distribución física en la que se encuentran dispuestos los ordenadores que la componen. De este modo, existen tres tipos, que podíamos llamar "puros". Son los siguientes:

- Estrella.
- Bus.
- Anillo

Topología en Estrella.

Esta topología se caracteriza por existir en ella un punto central, o más propiamente nodo central, al cual se conectan todos los equipos, de un modo muy similar a los radios de una rueda.

De esta disposición se deduce el inconveniente de esta topología, y es que la máxima vulnerabilidad se encuentra precisamente en el nodo central, ya que si este falla, toda la red fallaría. Este posible fallo en el nodo central, aunque posible, es bastante improbable, debido a la gran seguridad que suele poseer dicho nodo. Sin embargo presenta como principal ventaja una gran modularidad, lo que permite aislar una estación defectuosa con bastante sencillez y sin perjudicar al resto de la red.

Para aumentar el número de estaciones, o nodos, de la red en estrella no es necesario interrumpir, ni siquiera parcialmente la actividad de la red, realizándose la operación casi inmediatamente.

La topología en estrella es empleada en redes Ethernet y ArcNet.

Topología en Bus

En la topología en bus, al contrario que en la topología de Estrella, no existe un nodo central, si no que todos los nodos que componen la red quedan unidos entre sí linealmente, uno a continuación del otro.

El cableado en bus presenta menos problemas logísticos, puesto que no se acumulan montones de cables en torno al nodo central, como ocurriría en un disposición en estrella. Pero, por contra, tiene la desventaja de que un fallo en una parte del cableado detendría el sistema, total o parcialmente, en función del lugar en que se produzca. Es además muy difícil encontrar y diagnosticar las averías que se producen en esta topología.

Debido a que en el bus la información recorre todo el bus bidireccionalmente hasta hallar su destino, la posibilidad de interceptar la información por usuarios no autorizados es superior a la existente en una Red en estrella debido a la modularidad que ésta posee.

La red en bus posee un retardo en la propagación de la información mínimo, debido a que los nodos de la red no deben amplificar la señal, siendo su función pasiva respecto al tráfico de la red. Esta pasividad de los nodos es debida mas bien al método de acceso empleado que a la propia disposición geográfica de los puestos de red. La Red en Bus necesita incluir en ambos extremos del bus, unos dispositivos llamados terminadores, los cuales evitan los posibles rebotes de la señal, introduciendo una impedancia característica (50 Ohm.)

Añadir nuevos puesto a una red en bus, supone detener al menos por tramos, la actividad de la red. Sin embargo es un proceso rápido y sencillo.

Es la topología tradicionalmente usada en redes Ethernet.

Topología en Anillo

El anillo, como su propio nombre indica, consiste en conectar linealmente entre sí todos los ordenadores, en un bucle cerrado. La información se transfiere en un solo sentido a través del anillo, mediante un paquete especial de datos, llamado **testigo**, que se transmite de un nodo a otro, hasta alcanzar el nodo destino.

El cableado de la red en anillo es el más complejo de los tres enumerados, debido por una parte al mayor coste del cable, así como a la necesidad de emplear unos dispositivos denominados Unidades de Acceso Multiestación (MAU) para implementar físicamente el anillo.

A la hora de tratar con fallos y averías, la red en anillo presenta la ventaja de poder derivar partes de la red mediante los MAU's, aislando dichas partes defectuosas del resto de la red mientras se determina el problema. Un fallo, pues, en una parte del cableado de una red en anillo, no debe detener toda la red. La adición de nuevas estaciones no supone una complicación excesiva, puesto que una vez más los MAU's aíslan las partes a añadir hasta que se hallan listas, no siendo necesario detener toda la red para añadir nuevas estaciones.

Dos buenos ejemplos de red en anillo serían Token-Ring y FDDI (fibra óptica)

Topologías híbridas.

Son las más frecuentes y se derivan de la unión de topologías “puras”: estrella-estrella, bus-estrella, etc.

El modelo OSI

Una de las necesidades más acuciantes de un sistema de comunicaciones es el establecimientos de estándares, sin ellos sólo podrían comunicarse entre si equipos del mismo fabricante y que usaran la misma tecnología.

La conexión entre equipos electrónicos se ha ido estandarizando paulatinamente siendo la redes telefónicas las pioneras en este campo. Por ejemplo la histórica CCITT definió los estándares de telefonía: PSTN, PSDN e ISDN.

Otros organismos internacionales que generan normas relativas a las telecomunicaciones son: ITU-TSS (antes CCITT), ANSI, IEEE e ISO

La ISO (International Organisation for Standarisation) ha generado una gran variedad de estándares, siendo uno de ellos la norma ISO-7494 que define el modelo OSI, este modelo nos ayudará a comprender mejor el funcionamiento de las redes de ordenadores.

El modelo OSI no garantiza la comunicación entre equipos pero pone las bases para una mejor estructuración de los protocolos de comunicación. Tampoco existe ningún sistema de comunicaciones que los siga estrictamente, siendo la familia de protocolos TCP/IP la que más se acerca.

El modelo OSI describe siete niveles para facilitar los interfaces de conexión entre sistemas abiertos, en la página siguiente puedes verlo con más detalle.

Nivel	Nombre	Función	Dispositivos y protocolos
1	Físico	Se ocupa de la transmisión del flujo de bits a través del medio.	Cables, tarjetas y repetidores (hub). RS-232, X.21.
2	Enlace	Divide el flujo de bits en unidades con formato (tramas) intercambiando estas unidades mediante el empleo de protocolos.	Puentes (bridges). HDLC y LLC.
3	Red	Establece las comunicaciones y determina el camino que tomarán los datos en la red.	Encaminador(router). IP, IPX.
4	Transporte	La función de este nivel es asegurar que el receptor reciba exactamente la misma información que ha querido enviar el emisor, y a veces asegura al emisor que el receptor ha recibido la información que le ha sido enviada. Envía de nuevo lo que no haya llegado correctamente.	Pasarela (gateway). UDP, TCP, SPX.
5	Sesión	Establece la comunicación entre las aplicaciones, la mantiene y la finaliza en el momento adecuado. Proporciona los pasos necesarios para entrar en un sistema utilizando otro. Permite a un mismo usuario, realizar y mantener diferentes conexiones a la vez (sesiones).	Pasarela.
6	Presentación	Conversión entre distintas representaciones de datos y entre terminales y organizaciones de sistemas de ficheros con características diferentes.	Pasarela. Compresión, encriptado, VT100.
7	Aplicación	Este nivel proporciona unos servicios estandarizados para poder realizar unas funciones especificas en la red. Las personas que utilizan las aplicaciones hacen una petición de un servicio (por ejemplo un envío de un fichero). Esta aplicación utiliza un servicio que le ofrece el nivel de aplicación para poder realizar el trabajo que se le ha encomendado (enviar el fichero).	X.400

La comunicación según el modelo OSI siempre se realizará entre dos sistemas. Supongamos que la información se genera en el nivel 7 de uno de ellos, y desciende por el resto de los niveles hasta llegar al nivel 1, que es el correspondiente al medio de transmisión (por ejemplo el cable de red) y llega hasta el nivel 1 del otro sistema, donde va ascendiendo hasta alcanzar el nivel 7. En este proceso, cada uno de los niveles va añadiendo a los datos a transmitir la información de control relativa a su nivel, de forma que los datos originales van siendo recubiertos por capas datos de control.

De forma análoga, al ser recibido dicho paquete en el otro sistema, según va ascendiendo del nivel 1 al 7, va dejando en cada nivel los datos añadidos por el nivel equivalente del otro sistema, hasta quedar únicamente los datos a transmitir. La forma, pues de enviar información en el modelo OSI tiene una cierta similitud con enviar un paquete de regalo a una persona, donde se ponen una serie de papeles de envoltorio, una o más cajas, hasta llegar al regalo en sí.

Emisor	Paquete	Receptor
Aplicación	C7 Datos	Aplicación
Presentación	C6 C7 Datos	Presentación
Sesión	C5 C6 C7 Datos	Sesión
Transporte	C4 C5 C6 C7 Datos	Transporte
Red	C3 C4 C5 C6 C7 Datos	Red
Enlace	C2 C3 C4 C5 C6 C7 Datos	Enlace
Físico	C2 C3 C4 C5 C6 C7 Datos	Físico

C7-C2 : Datos de control específicos de cada nivel.

Los niveles OSI se entienden entre ellos, es decir, el nivel 5 enviará información al nivel 5 del otro sistema (lógicamente, para alcanzar el nivel 5 del otro sistema debe recorrer los niveles 4 al 1 de su propio sistema y el 1 al 4 del otro), de manera que la comunicación siempre se establece entre niveles iguales, a las normas de comunicación entre niveles iguales es a lo que llamaremos **protocolos**. Este mecanismo asegura la modularidad del conjunto, ya que cada nivel es independiente de las funciones del resto, lo cual garantiza que a la hora de modificar las funciones de un determinado nivel no sea necesario reescribir todo el conjunto.

En las familias de protocolos más utilizadas en redes de ordenadores (TCP/IP, IPX/SPX, etc.) nos encontraremos a menudo funciones de diferentes niveles en un solo nivel, debido a que la mayoría de ellos fueron desarrollados antes que el modelo OSI.

Medios de transmisión.

Medios magneto-ópticos.

Los disquetes, zips y en general los medios removibles, los podemos llevar de un sitio a otro.

Par trenzado.

Grosor de 1mm.

El ancho de banda depende del grosor y de la distancia.

Velocidad del orden de 10-100 Mbps.

Categorías de cable par trenzado:

- **STP** (apantallado): 2 pares de hilo, recubierto por malla.
- **UTP** (no apantallado): 4 pares de hilos.
  - **Categoría 3:** van de 4 en 4 (8 cables), alcanzando 30 Mbps .
  - **Categoría 5:** más retorcidos y mejor aislante (teflón), alcanzando 100 Mbps .

Cable coaxial.

Los hay de 2 impedancias:

- **75 ohmios**: banda ancha, utilizado en TV, distintos canales, 300MHz.
- **50 ohmios**: banda base, utilizado en Ethernet, un canal.
  - **10BASE5:** coaxial grueso, 500 metros, 10Mbps, conector “N”.
  - **10BASE2:** coaxial fino, 185 metros, 10 Mbps, conector “BNC”.

Fibra óptica.

Se necesita una fuente de luz: láser o LED.

Se transmite por fibra y se capta por foto diodos.

La topología típica es el anillo

Alcanza un ancho de banda de 30000GHz .

Sólo necesita repetidores cada 30 kms.

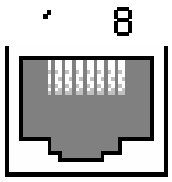
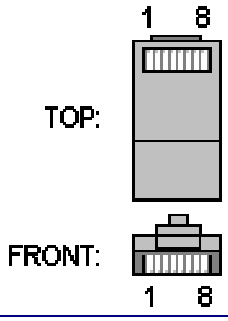
No hay interferencias.

Pesa 8 veces menos que el cable par trenzado.

El cable y los conectores vistos bajo la norma Ethernet 802.3

	Tipo de cable	Conexión	Longitud máxima	Nº max. de estaciones	Observaciones
10 base 5	Coaxial grueso, 50 ohmios, o cable amarillo,	Conectores tipo vampiro	500 m	100	Líneas acabadas en una impedancia del mismo valor que la Z característica, Líneas libres acabadas en tapones para evitar los rebotes
10 base 2	Coaxial fino, 50 ohmios RG58	BNC	185 m	30	conexión por "T" [Problema: hay que abrir la red] Líneas libres acabadas en tapones para evitar los rebotes
10 base T	Par trenzado	RJ-45(ISO 8877).	100 m		Hub: Bus lógico en una caja y todas las estaciones colgando
100 base T	UTP categoría 5				

Numeración del conector RJ45

Hembra	Macho
Visto de frente	Conector visto de frente y desde arriba
	

Ethernet 10Base-T (T568B colores)

RJ45		Código	Utilidad	Pares
1	Blanco/Naranja o el blanco del par naranja	T2	Txdata +	PAR 2
2	Naranja o naranja/blanco	R2	TxData -	
3	Blanco/verde o el blanco del par verde	T3	RecvData +	PAR 3
4	Azul o azul/blanco	R1		PAR 1
5	Blanco/Naranja o el blanco del par naranja	T1		
6	Verde o verde/blanco	R3	RecvData -	
7	Blanco/marrón o el blanco del par marrón	T4		PAR 4
8	Marrón o marrón/blanco	R4		

Pares usados según norma

ATM 155Mbps usa los pares 2 y 4 (pins 1-2, 7-8)

Ethernet 10Base - T4 usa los pares 2 y 3 (pins 1-2, 3-6)

Ethernet 100Base-T4 usa los pares 2 y 3 (4T+) (pins 1-2, 3-6)

Ethernet 100Base-T8 usa los pares 1,2,3 y 4 (pins 4-5, 1-2, 3-6, 7-8)

Cable usado según norma

Categoría	Velocidad	Donde se usa
1	No entra dentro de los criterios de la norma	
2	Hasta 1 MHz	Para telefonía
3	Hasta 16 MHz	Ethernet 10Base-T
4	Hasta 20 MHz	Token-Ring, 10Base-T
5	Hasta 100 MHz	100Base-T, 10Base-T

Componentes de una red.

Dentro de lo que son componentes de una red vamos a distinguir entre equipos de red, cableados y conectores a la misma; y, dentro de los equipos de red, también vamos a hacer una subdivisión en equipos que interconectan redes y equipos conectados a un segmento de las mismas.

Equipos que interconectan redes.

Repetidores.

Los repetidores son equipos que trabajan a nivel 1 de la pila OSI, es decir, repiten todas las señales de un segmento a otro a nivel eléctrico.

Se utilizan para resolver los problemas de longitudes máximas de los segmentos de red (su función es extender una red Ethernet más allá de un segmento). No obstante, hay que tener en cuenta que, al retransmitir todas las señales de un segmento a otro, también retransmitirán las colisiones. Estos equipos sólo aíslan entre los segmentos los problemas eléctricos que pudieran existir en algunos de ellos.

El número máximo de repetidores en cascada es de cuatro, pero con la condición de que los segmentos 2 y 4 sean IRL, es decir, que no tengan ningún equipo conectado que no sean los repetidores. En caso contrario, el número máximo es de 2, interconectando 3 segmentos de red.

El repetidor tiene dos puertas que conectan dos segmentos Ethernet por medio de transceivers (instalando diferentes transceivers es posible interconectar dos segmentos de diferentes medios físicos) y cables drop.

El repetidor tiene como mínimo una salida Ethernet para el cable amarillo y otra para teléfono.

Con un repetidor modular se pude centralizar y estructurar todo el cableado de un edificio, con diferentes medios, adecuados según el entorno, y las conexiones al exterior.

Un Concentrador es un equipo igual a un multiport repeater pero con salida RJ-45.

Los repetidores con buffers es la unión de dos redes por una línea serie mediante una pareja de repetidores.

Puentes o Bridges.

Estos equipos se utilizan asimismo para interconectar segmentos de red, (amplía una red que ha llegado a su máximo, ya sea por distancia o por el número de equipos) y se utilizan cuando el tráfico no es excesivamente alto en las redes pero interesa aislar las colisiones que se produzcan en los segmentos interconectados entre sí.

Los bridges trabajan en el nivel 2 de OSI, con direcciones físicas, por lo que filtra tráfico de un segmento a otro.

Esto lo hace de la siguiente forma: Escucha los paquetes que pasan por la red y va configurando una tabla de direcciones físicas de equipos que tiene a un lado y otro (generalmente tienen una tabla dinámica), de tal forma que cuando escucha en un segmento

un paquete de información que va dirigido a ese mismo segmento no lo pasa al otro, y viceversa.

No filtra los broadcasts, que son paquetes genéricos que lanzan los equipos a la red para que algún otro les responda, aunque puede impedir el paso de determinados tipos de broadcast. Esto es típico para solicitar las cargas de software, por ejemplo. Por tanto, al interconectar segmentos de red con bridges, podemos tener problemas de tormentas de broadcasts, de saturación del puente por sobrecarga de tráfico, etc.

El número máximo de puentes en cascada es de siete; no pueden existir bucles o lazos activos, es decir, si hay caminos redundantes para ir de un equipo a otro, sólo uno de ellos debe estar activo, mientras que el redundante debe ser de backup. Para esto, cuando se está haciendo bridging en las redes, se usa el algoritmo de spanning-tree, mediante el cual se deshacen los bucles de los caminos redundantes.

Las posibles colisiones no se transmiten de un lado a otro de la red. El bridge sólo deja pasar los datos que van a un equipo que él conoce.

El bridge generalmente tiene una tabla dinámica, aíslan las colisiones, **pero no filtran protocolos**.

El bridge trabaja en el nivel 2 de OSI y aísla las colisiones

La primera vez que llega un paquete al bridge lo transmitirá, pero aprende (ya que, si el paquete no lo coge nadie, significa que no está).

El peligro de los bridges es cuando hay exceso de broadcast y se colapsa la red. A esto se le llama tormenta de broadcast, y se produce porque un equipo está pidiendo ayuda (falla).

Routers.

Estos equipos trabajan a nivel 3 de la pila OSI, es decir pueden filtrar protocolos y direcciones a la vez. Los equipos de la red saben que existe un router y le envían los paquetes directamente a él cuando se trate de equipos en otro segmento.

Además los routers pueden interconectar redes distintas entre sí; eligen el mejor camino para enviar la información, balancean tráfico entre líneas, etc.

El router trabaja con tablas de encaminamiento o enrutado con la información que generan los protocolos, deciden si hay que enviar un paquete o no, deciden cual es la mejor ruta para enviar un paquete o no, deciden cual es la mejor ruta para enviar la información de un equipo a otro, pueden contener filtros a distintos niveles, etc.

Poseen una entrada con múltiples conexiones a segmentos remotos, garantizan la fiabilidad de los datos y permiten un mayor control del tráfico de la red. Su método de funcionamiento es el encapsulado de paquetes.

Para interconectar un nuevo segmento a nuestra red, sólo hace falta instalar un router que proporcionará los enlaces con todos los elementos conectados.

Gateways.

También llamados traductores de protocolos, son equipos que se encargan, como su nombre indica, a servir de intermediario entre los distintos protocolos de comunicaciones para facilitar la interconexión de equipos distintos entre sí.

Su forma de funcionar es que tienen duplicada la pila OSI, es decir, la correspondiente a un protocolo y, paralelamente, la del otro protocolo. Reciben los datos encapsulados de un protocolo, los van desencapsulando hasta el nivel más alto, para posteriormente ir encapsulando los datos en el otro protocolo desde el nivel más alto al nivel más bajo, y vuelven a dejar la información en la red, pero ya traducida.

Los gateways también pueden interconectar redes entre sí.

Equipos de red conectados a un segmento.

Transceivers.

Son equipos que son una combinación de transmisor/receptor de información. El transceiver transmite paquetes de datos desde el controlador al bus y viceversa.

En una ethernet, los transceivers se desconectan cuando el equipo al que están conectados no está funcionando, sin afectar para nada al comportamiento de la red.

Multitransceivers.

Son transceivers que permiten la conexión de más de un equipo a la red en el mismo sitio, es decir, tienen varias salidas para equipos.

Multiport-transceivers.

Son equipos que van conectados a un transceiver y que tienen varias puertas de salida para equipos. La única limitación que tienen es que mediante estos equipos no se pueden interconectar equipos que conecten redes entre sí.

Fan-out.

Estos equipos van conectados a un transceiver, y permiten dividir la señal del mismo a varios equipos. Su limitación estriba en que la longitud de los cables que vayan a los equipos es menor , porque no regeneran la señal, a diferencia de los multiport-transceivers.

El fan-out permite conectar hasta ocho DTE's utilizando un sólo transceiver. Poniendo un fan-out en cascada de dos niveles, se podría conseguir hasta 64 DTE's con un transceiver conectado a la red.

El fan-out puede configurar una red de hasta ocho estaciones sin usar cable ethernet ni transceivers, por medio de un fan-out, funcionando así de modo aislado.

La longitud del cable AUI, desde l segmento al DTE se reduce a 40m. si hay un fan-out en medio.

Multiport-repeaters.

Son equipos que van conectados a red, dando en cada una de sus múltiples salidas señal de red regenerada. Entre sí mismos se comportan como un segmento de red.

El multiport cuenta como un repetidor. Tiene salida AUI o BNC y es parecido al fan-out, pero en cada una de sus salidas regenera señal. Es un repetidor.

Servidores de Terminales.

Son equipos que van conectados a la red, y en sus salidas generan una señal para un terminal, tanto síncrono como asíncrono, desde el cual se podrá establecer una sesión con un equipo o host.

El servidor de terminales es un dispositivo configurado para integrar terminales "tontas" o PCs por interface serie con un emulador de terminales. Puede utilizar los protocolos TCP/IP y LAT para una red ethernet, y se puede acceder a cualquier ordenador que soporte TCP/IP o LAT (DECnet).

Protocolos TCP/IP

Protocolos de comunicaciones.

Los protocolos que se utilizan en las comunicaciones son una serie de normas que deben aportar las siguientes funcionalidades:

- Permitir localizar un ordenador de forma inequívoca.
- Permitir realizar una conexión con otro ordenador.
- Permitir intercambiar información entre ordenadores de forma segura, independiente del tipo de maquinas que estén conectadas (PC, Mac,AS-400...).
- Abstraer a los usuarios de los enlaces utilizados (red telefónica, radioenlaces, satélite...) para el intercambio de información.
- Permitir liberar la conexión de forma ordenada.

Debido a la gran complejidad que conlleva la interconexión de ordenadores, se ha tenido que dividir todos los procesos necesarios para realizar las conexiones en diferentes niveles. Cada nivel se ha creado para dar una solución a un tipo de problema particular dentro de la conexión. Cada nivel tendrá asociado un protocolo, el cual entenderán todas las partes que formen parte de la conexión.

Diferentes empresas han dado diferentes soluciones a la conexión entre ordenadores, implementando diferentes familias de protocolos, y dándole diferentes nombres (DECnet, TCP/IP, IPX/SPX, NETBEUI, etc.).

¿Qué es TCP/IP?

Cuando se habla de TCP/IP , se relaciona automáticamente como el protocolo sobre el que funciona la red Internet . Esto , en cierta forma es cierto , ya que se le llama TCP/IP , a la familia de protocolos que nos permite estar conectados a la red Internet . Este nombre viene dado por los dos protocolos estrella de esta familia :

- El protocolo TCP, funciona en el nivel de transporte del modelo de referencia OSI, proporcionando un transporte fiable de datos.
- El protocolo IP, funciona en el nivel de red del modelo OSI, que nos permite encaminar nuestros datos hacia otras maquinas.

Pero un protocolo de comunicaciones debe solucionar una serie de problemas relacionados con la comunicación entre ordenadores , además de los que proporciona los protocolos TCP e IP .

Arquitectura de protocolos TCP/IP

Para poder solucionar los problemas que van ligados a la comunicación de ordenadores dentro de la red Internet , se tienen que tener en cuenta una serie de particularidades sobre las que ha sido diseñada TCP/IP:

- Los programas de aplicación no tienen conocimiento del hardware que se utilizara para realizar la comunicación (módem, tarjeta de red...)
- La comunicación no esta orientada a la conexión de dos maquinas, eso quiere decir que cada paquete de información es independiente, y puede viajar por caminos diferentes entre dos maquinas.
- La interfaz de usuario debe ser independiente del sistema, así los programas no necesitan saber sobre que tipo de red trabajan.
- El uso de la red no impone ninguna topología en especial (distribución de los distintos ordenadores).

De esta forma, podremos decir, que dos redes están interconectadas, si hay una maquina común que pase información de una red a otra. Además, también podremos decir que una red Internet virtual realizara conexiones entre redes, que ha cambio de pertenecer a la gran red, colaboraran en el trafico de información procedente de una red cualquiera, que necesite de ella para acceder a una red remota. Todo esto independiente de las maquinas que implementen estas funciones, y de los sistemas operativos que estas utilicen .

Descomposición en niveles de TCP/IP.

Toda arquitectura de protocolos se descompone en una serie de niveles , usando como referencia el modelo OSI . Esto se hace para poder dividir el problema global en subproblemas de mas fácil solución .

Al diferencia de OSI , formado por una torre de siete niveles , TCP/IP se descompone en cinco niveles , cuatro niveles software y un nivel hardware . A continuación pasaremos a describir los niveles software , los cuales tienen cierto paralelismo con el modelo OSI.

Nivel de aplicación

Constituye el nivel mas alto de la torre tcp/ip . A diferencia del modelo OSI , se trata de un nivel simple en el que se encuentran las aplicaciones que acceden a servicios disponibles a través de Internet . Estos servicios están sustentados por una serie de protocolos que los proporcionan . Por ejemplo , tenemos el protocolo FTP (File Transfer Protocol), que proporciona los servicios necesarios para la transferencia de ficheros entre dos ordenadores.

Otro servicio, sin el cual no se concibe Internet , es el de correo electrónico, sustentado por el protocolo SMTP (Simple Mail Transfer Protocol) .

Nivel de transporte

Este nivel proporciona una comunicación extremo a extremo entre programas de aplicación. La maquina remota recibe exactamente lo mismo que le envió la maquina origen. En este nivel el emisor divide la información que recibe del nivel de aplicación en paquetes, le añade los datos necesarios para el control de flujo y control de errores , y se los pasa al nivel de red junto con la dirección de destino.

En el receptor este nivel se encarga de ordenar y unir las tramas para generar de nuevo la información original.

Para implementar el nivel de transporte se utilizan dos protocolos :

- **UDP:** proporciona un nivel de transporte no fiable de datagramas, ya que apenas añade información al paquete que envía al nivel inferior, solo la necesaria para la comunicación extremo a extremo. Lo utilizan aplicaciones como NFS y RPC, pero sobre todo se emplea en tareas de control.
- **TCP (Transport Control Protocolo):** es el protocolo que proporciona un transporte fiable de flujo de bits entre aplicaciones. Esta pensado para poder enviar grandes cantidades de información de forma fiable, liberando al programador de aplicaciones de la dificultad de gestionar la fiabilidad de la conexión (retransmisiones, perdidas de paquete, orden en que llegan los paquetes ,duplicados de paquetes, ...) que gestiona el propio protocolo. Pero la complejidad de la gestión de la fiabilidad tiene un coste en eficiencia, ya que para llevar a cabo las gestiones anteriores se tiene que añadir bastante información a los paquetes a enviar. Debido a que los paquetes a enviar tienen un tamaño máximo, como mas información añada el protocolo para su gestión , menos información que proviene de la aplicación podrá contener ese paquete. Por eso, cuando es mas importante la velocidad que la fiabilidad, se utiliza UDP, en cambio TCP asegura la recepción en destino de la información a transmitir.

Nivel de red

También recibe el nombre de **nivel Internet**. Coloca la información que le pasa el nivel de transporte en datagramas IP, le añade cabeceras necesaria para su nivel y lo envía al nivel inferior. Es en este nivel donde se emplea el algoritmo de encaminamiento, al recibir un datagrama del nivel inferior decide, en función de su dirección, si debe procesarlo y pasarlo al nivel superior, o bien encaminarlo hacia otra maquina. Para implementar este nivel se utilizan los siguientes protocolos:

- **IP (Internet Protocol):** es un protocolo no orientado a la conexión, con mensajes de un tamaño máximo . Cada datagrama se gestiona de forma independiente, por lo que dos datagramas pueden utilizar diferentes caminos para llegar al mismo destino, provocando que lleguen en diferente orden o bien duplicados. Es un protocolo no fiable , eso quiere decir que no corrige los anteriores problemas, ni tampoco informa de ellos. Este protocolo recibe información del nivel superior y le añade la información necesaria para su gestión (direcciones IP , checksum)
- **ICMP (Internet Control Message Protocol):** proporciona un mecanismo de comunicación de información de control y de errores entre maquinas intermedias por las que viajaran los paquetes de datos . Esto datagramas los suelen emplear las maquinas (gateways, host, ...) para informarse de condiciones especiales en la red, como la existencia de una congestión , la existencia de errores y las posibles peticiones de cambios de ruta. Los mensajes de ICMP están encapsulados en datagramas IP.
- **IGMP (Internet Group Management Protocol):** este protocolo esta íntimamente ligado a IP . Se emplea en maquinas que emplean IP multicast . El IP multicast es una variante de IP que permite emplear datagramas con múltiples destinatarios .

También en este nivel tenemos una serie de protocolos que se encargan de la resolución de direcciones:

- **ARP (Address Resolution Protocol):** cuando una maquina desea ponerse en contacto con otra conoce su dirección IP , entonces necesita un mecanismo dinámico que permite conocer su dirección física . Entonces envía una petición ARP por broadcast (o sea a todas las maquinas). El protocolo establece que solo contestara a la petición , si esta lleva su dirección IP . Por lo tanto solo contestara la maquina que corresponde a la dirección IP buscada , con un mensaje que incluya la dirección física . El software de comunicaciones debe mantener una cache con los pares IP-dirección física . De este modo la siguiente vez que hay que hacer una transmisión a es dirección IP , ya conoceremos la dirección física.
- **RARP (Reverse Address Resolution Protocol):** a veces el problema es al revés, o sea, una máquina solo conoce su dirección física, y desea conocer su dirección lógica. Esto ocurre, por ejemplo, cuando se accede a Internet con una dirección diferente, en el caso de PC que acceden por módem a Internet, y se le asigna una dirección diferente de las que tiene el proveedor sin utilizar. Para solucionar esto se envía por broadcast una petición RARP con su dirección física , para que un servidor pueda darle su correspondencia IP.
- **BOOTP (Bootstrap Protocol):** el protocolo RARP resuelve el problema de la resolución inversa de direcciones, pero para que pueda ser mas eficiente, enviando más información que meramente la dirección IP, se ha creado el protocolo BOOTP. Este además de la dirección IP del solicitante , proporciona información adicional, facilitando la movilidad y el mantenimiento de las maquinas.

Nivel de enlace

Este nivel se limita a recibir datagramas del nivel superior (nivel de red) y transmitirlo al hardware de la red. Pueden usarse diversos protocolos: DLC(IEEE 802.2), Frame Relay, X.25, etc.

La interconexión de diferentes redes genera una red virtual en la que las maquinas se identifican mediante una dirección de red lógica. Sin embargo a la hora de transmitir información por un medio físico se envía y se recibe información de direcciones físicas. Un diseño eficiente implica que una dirección lógica sea independiente de una dirección física, por lo tanto es necesario un mecanismo que relacione las direcciones lógicas con las direcciones físicas. De esta forma podremos cambiar nuestra dirección lógica IP conservando el mismo hardware, del mismo modo podremos cambiar una tarjeta de red, la cual contiene una dirección física, sin tener que cambiar nuestra dirección lógica IP.

Direcciones IP y máscaras de red

En una red TCP/IP los ordenadores se identifican mediante un número que se denomina **dirección IP**. Esta dirección ha de estar dentro del rango de direcciones asignadas al organismo o empresa a la que pertenece, estos rangos son concedidos por un organismo central de Internet, el **NIC** (Network Information Center).

Una dirección IP está formada por 32 bits, que se agrupan en octetos:

01000001 00001010 00000010 00000011

Para entendernos mejor utilizamos las direcciones IP en formato decimal, representando el valor decimal de cada octeto y separando con puntos:

129.10.2.3

Las dirección de una máquina se compone de dos partes cuya longitud puede variar:

- **Bits de red:** son los bits que definen la red a la que pertenece el equipo.
- **Bits de host:** son los bits que distinguen a un equipo de otro dentro de una red.

Los bits de red siempre están a la izquierda y los de host a la derecha, veamos un ejemplo sencillo:

Bits de Red	Bits de Host
10010110 11010110 10001101	11000101
150.214.141.	197

Para ir entrando en calor diremos también que esta máquina pertenece a la red 150.214.141.0 y que su máscara de red es 255.255.255.0. Si queréis ir reflexionando sobre algo os mostramos de nuevo en formato binario la máscara de red llevando a caballitos a la dirección de la máquina:

10010110	11010110	10001101	11000101
11111111	11111111	11111111	00000000

La máscara de red es un número con el formato de una dirección IP que nos sirve para distinguir cuando una máquina determinada pertenece a una subred dada, con lo que podemos averiguar si dos máquinas están o no en la misma subred IP. En formato binario todas las máscaras de red tienen los “1” agrupados a la izquierda y los “0” a la derecha.

Para llegar a comprender como funciona todo esto podríamos hacer un ejercicio práctico.

Ejercicio 1

Sea la dirección de una subred 150.214.141.0, con una máscara de red 255.255.255.0

Comprobar cuales de estas direcciones pertenecen a dicha red:

150.214.141.32

150.214.141.138

150.214.142.23

Paso 1: para ver si son o no direcciones validas de dicha subred clase C tenemos que descomponerlas a nivel binario:

150.214.141.32 10010110.1101010.10001101.10000000
150.214.141.138 10010110.1101010.10001101.10001010
150.214.142.23 10010110.1101010.10001110.00010111
255.255.255.0 11111111.1111111.11111111.00000000
150.214.141.0 10010110.1101010.10001101.00000000

Paso 2: una vez tenemos todos los datos a binario pasamos a recordar el operador lógico AND o multiplicación:

Valor A	Valor B	Resultado
0	0	0
0	1	0
1	0	0
1	1	1

Vamos a explicar como hace la comprobación el equipo conectado a una red local.

Primero comprueba la dirección IP con su máscara de red, para ello hace un AND bit a bit de todos los dígitos:

150.214.141.32 10010110.1101010.10001101.10000000
255.255.255.0 11111111.1111111.11111111.00000000

150.214.**141**.0 10010110.1101010.10001101.00000000

Luego hace la misma operación con la dirección IP destino.

150.214.141.138 10010110.1101010.10001101.10001010
255.255.255.0 11111111.1111111.11111111.00000000

150.214.**141**.0 10010110.1101010.10001101.00000000

El resultado que obtenemos ambas veces es la dirección de red, esto no indica que los dos equipos están dentro de la misma red.

Paso3: vamos ha hacerlo con la otra dirección IP.

150.214.142.23 10010110.1101010.10001110.00010111
255.255.255.0 11111111.1111111.11111111.00000000

150.214.142.0 10010110.1101010.10001110.00000000

Como vemos este resultado nos indica que dicho equipo no pertenece a la red sino que es de otra red en este caso la red sería 150.214.142.0.

Ejercicio 2

Pasamos ahora a complicar un poco más la cosa. Como hemos leído antes la dirección IP se compone de dos partes la dirección de red y la dirección de host(máquina o PC). Imaginemos que en nuestra red solo hace falta 128 equipos y no 254 la solución sería dividir la red en dos partes iguales de 128 equipos cada una.

Primero cogemos la máscara de red.

	Dirección de red	Dirección de host.
	_____._____._____._____	
255.255.255.0	11111111.11111111.11111111.00000000	

Si lo que queremos es crear dos subredes de 128 en este caso tenemos que coger un bit de la parte de identificativa del host.

Por lo que la máscara de re quedaría de esta manera.

	Dirección de red	Dirección de host.
	_____._____._____.x._____	
255.255.255.128	11111111.11111111.11111111.10000000	

Donde X es el bit que hemos cogido para dicha construcción. Por lo que el último octeto tendría el valor 10000000 que es 128 en decimal.

Si la dirección de red que hemos utilizado es la 150.214.141.0 al poner esta máscara de red tendríamos dos subredes.

La 150.214.141.0 y la 150.214.141.128 que tendrían los siguientes rangos IP:

La 150.214.141.0 cogería desde la 150.214.141.1 hasta la 150.214.141.127

La 150.214.141.128 sería pues desde la 150.214.141.128 hasta la 150.214.141.254.

La máscara de red para las dos subredes sería la 255.255.255.128.

Comprobar.

Sea la máscara de red 255.255.255.128

La dirección de red 150.214.141.128

Comprobar si las siguientes direcciones pertenecen a dicha subred.

150.214.141.134

150.214.141.192

150.214.141.38

150.214.141.94

Si hemos realizado el ejercicio se tiene que comprobar que:

150.214.141.134 150.214.141.192 pertenecen a la subred 150.214.141.128

150.214.141.38 150.214.141.94 pertenecen a la subred 150.214.141.0

Clases de red

Para una mejor organización en el reparto de rangos las redes se han agrupado en cuatro clases, de manera que según el tamaño de la red se optará por un tipo u otro.

Las direcciones de clase A

Corresponden a redes que pueden direccionar hasta 16.777.214 máquinas cada una.

Las direcciones de red de clase A tienen siempre el primer bit a 0.

0 + Red (7 bits) + Máquina (24 bits)

Solo existen 124 direcciones de red de clase A.

Ejemplo:

	Red	Máquina		
Binario	0 0001010	00001111	00010000	00001011
Decimal	10	15	16	11

Rangos (notación decimal):

1.xxx.xxx.xxx - 126.xxx.xxx.xxx

Las direcciones de clase B

Las direcciones de red de clase B permiten direccionar 65.534 máquinas cada una.

Los dos primeros bits de una dirección de red de clase B son siempre 01.

01 + Red (14 bits) + Máquina (16 bits)

Existen 16.382 direcciones de red de clase B.

Ejemplo:

	Red		Máquina	
Binario	01 000001	00001010	00000010	00000011
Decimal	129	10	2	3

Rangos (notación decimal) :

128.001.xxx.xxx - 191.254.xxx.xxx

Las direcciones de clase C

Las direcciones de clase C permiten direccionar 254 máquinas.

Las direcciones de clase C empiezan con los bits 110

110 + Red (21 bits) + Máquina (8 bits)

Existen 2.097.152 direcciones de red de clase C.

Ejemplo:

	Red			Máquina
Binario	110 01010	00001111	00010111	00001011
Decimal	202	15	23	11

Rangos (notación decimal):

192.000.001.xxx - 223.255.254..xxx

Las direcciones de clase D

Las direcciones de clase D son un grupo especial que se utiliza para dirigirse a grupos de máquinas. Estas direcciones son muy poco utilizadas. Los cuatro primeros bits de una dirección de clase D son 1110.

Direcciones de red reservadas

Existen una serie de direcciones IP con significados especiales.

- Direcciones de subredes reservadas:

  000.xxx.xxx.xxx (1)

  127.xxx.xxx.xxx (reservada como la propia máquina)

  128.000.xxx.xxx (1)

  191.255.xxx.xxx (2)

  192.168.xxx.xxx (reservada para intranets)

  223.255.255.xxx (2)

- Direcciones de máquinas reservadas:

  xxx.000.000.000 (1)

  xxx.255.255.255 (2)

  xxx.xxx.000.000 (1)

  xxx.xxx.255.255 (2)

  xxx.xxx.xxx.000 (1)

xxx.xxx.xxx.255 (2)

(1) Se utilizan para identificar a la red.

(2) Se usa para enmascarar.