INSTALACIÓN Y MANTENIMIENTO
DE REDES INFORMÁTICAS
"ASPECTOS FUNDAMENTALES SOBRE REDES"

Profesor
EDWIN ALBEIRO RAMOS VILLAMIL
Licenciado en Diseño Tecnológico
Universidad Pedagógica Nacional

INSTITUTO TÉCNICO INTEGRAL
Cra. 31 N° 38 – 04. TEL: 6718195
VILLAVICENCIO

CONTENIDO

1. QUÉ ES UNA RED INFORMÁTICA....1
2. PARTES DE UNA RED INFORMÁTICA....2
2.1. PARTE FÍSICA. HARDWARE DE RED....2
2.1.1. TARJETAS O ADAPTADORES DE RED.....2
2.1.1.1. Adaptadores PCMCIA....2
2.1.1.2. Adaptadores PCI....2
2.1.1.3. Adaptadores USB....2
2.1.2. EL MEDIO DE TRANSMISIÓN....2
2.1.2.1. Cables Trenzados....3
2.1.2.2. Cable Coaxial....3
2.1.2.3. Fibra Óptica....3
2.1.2.4. Medios inalámbricos....4
2.1.3. DISPOSITIVOS INTERMEDIARIOS....4
2.1.3.1. Hub....4
2.1.3.2. Switch....6
2.1.3.3. Modem....8
2.1.3.4. Router....11
2.1.4. PERIFÉRICOS COMPARTIDOS.....11
2.2. PARTE LÓGICA. SOFTWARE DE RED....11
2.2.1. SISTEMA OPERATIVO DE RED.....11
2.2.2. CONTROLADORES DE RED.....11
2.2.3. PROGRAMAS DE APLICACIÓN.....12
3. CLASIFICACIÓN DE UNA RED....13
3.1. SEGÚN SU TAMAÑO....13
3.1.1. LAN....13
3.1.2. WAN....13
3.1.3. MAN....13
3.2. SEGÚN SU DISTRIBUCIÓN LÓGICA....13
3.2.1. SERVIDOR.....13
3.2.2. CLIENTE.....13
4. TOPOLOGÍAS....15

4.1. BUS 15
4.2. ESTRELLA 16
4.3. ANILLO 16
4.4. MALLA 17
4.5. ÁRBOL 17
4.6. VARIACIONES SOBRE LAS TOPOLOGÍAS 17
4.6.1. ESTRELLA – BUS 17
4.6.2. ESTRELLA – ANILLO 18
5. COMUNICACIÓN EN UNA RED 19
5.1. CONMUTACIÓN DE CIRCUITOS, DE MENSAJES Y DE PAQUETES 19
5.2. COMUNICACIÓN SIMPLEX, HALF-DUPLEX Y FULL-DUPLEX 19
5.3. MECANISMOS DE DETECCIÓN DE ERRORES 20
5.3.1. Paridad 20
5.3.2. CRC 21
5.4. CONTROL DE FLUJO 21
6. PROTOCOLOS 22
6.1. MODELO DE REFERENCIA OSI 22
6.1.1. CAPA FÍSICA 24
6.1.2. CAPA DE ENLACE DE DATOS 24
6.1.3. CAPA DE RED 24
6.1.4. CAPA DE TRANSPORTE 24
6.1.5. CAPA DE SESIÓN 25
6.1.6. CAPA DE PRESENTACIÓN 25
6.1.7. CAPA DE APLICACIÓN 25
6.2. TCP/IP 25

ASPECTOS FUNDAMENTALES SOBRE REDES

1. QUÉ ES UNA RED INFORMÁTICA

Una red es un sistema de transmisión de datos que permite el intercambio de información entre ordenadores. Si bien esta definición es demasiado general, nos sirve como punto de partida. La información que pueden intercambiar los ordenadores de una red puede ser de lo más variada: correos electrónicos, vídeos, imágenes, música en formato MP3, registros de una base de datos, páginas web, etc. La transmisión de estos datos se produce a través de un medio de transmisión o combinación de distintos medios: cables de fibra óptica, tecnología inalámbrica, enlaces vía satélite.

En la definición anterior hemos indicado el término ordenadores en un intento por simplificar. Sin embargo, los ordenadores son sólo una parte de los distintos dispositivos electrónicos que pueden tener acceso a las redes, en particular a Internet. Otros dispositivos de acceso son los asistentes personales (PDA), algunos celulares como los Blackberry o la televisión (Web TV). Incluso, ya existen frigoríficos capaces de intercambiar información (la lista de la compra) con un supermercado virtual.

Prof. ALBEIRO RAMOS

2. PARTES DE UNA RED INFORMÁTICA

2.1. PARTE FÍSICA. HARDWARE DE RED

2.1.1.TARJETAS O ADAPTADORES DE RED.

Permiten la conexión del hardware al medio de transmisión, y pueden ser: PCMCIA, PCI, USB o Integradas, están basadas en el estándar de Ethernet. Genéricamente a las tarjetas de red se les conoce con las siglas **NIC** (Network Interface Card, Tarjeta de Interface de Red)

2.1.1.1. Adaptadores PCMCIA

Los adaptadores de red PCMCIA, son casi de uso exclusivo de ordenadores portátiles, que son los que normalmente vienen equipados con este tipo de conector. En la figura podemos apreciar la forma de este dispositivo y la "boca" o puerto Ethernet donde conectaremos el cable con terminador RJ45.

2.1.1.2. Adaptadores PCI

Son dispositivos PCI, similares a las tarjetas PCI a las que ya estamos habituados. Su uso está indicado en ordenadores de sobremesa.

2.1.1.3. Adaptadores USB

Este tipo de conexiones de red no son los más habituales, puede ser usado en cualquier ordenador que disponga de puertos USB, sea sobremesa o portátil. Podemos ver en la fotografía un ejemplo de este adaptador. Aquí también se incluyen las memorias pendrive flash.

2.1.2.EL MEDIO DE TRANSMISIÓN

Cumple esencialmente con la transmisión de los datos digitalizados, facilitando nodos o puntos de conexión.

Los medios de transmisión se clasifican en guiados y no guiados. Los primeros son aquellos que utilizan un medio sólido (un cable) para la transmisión, entre ellos están: Los cables trenzados, el cable coaxial y la fibra óptica. Los medios no guiados utilizan el aire para transportar los datos: son los medios de inalámbricos.

Prof. ALBEIRO PINOS

2.1.2.1. Cables Trenzados

El par trenzado es similar al cable telefónico, sin embargo consta de 8 hilos y utiliza unos conectores un poco más anchos. 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.

- Categoría 3, hasta 16 Mbps
- Categoría 4, hasta 20 Mbps
- Categoría 5 y Categoría 5e, hasta 1 Gbps
- Categoría 6, hasta 1 Gbps y más

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

- **UTP** (*Unshielded Twisted Pair*, par trenzado no apantallado)
- **STP** (*Shielded Twisted Pair*, par trenzado apantallado)

Los cables UTP 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 cableado que se utiliza en la actualidad es UTP CAT5. El cableado CAT6 es demasiado nuevo y es difícil encontrarlo en el mercado. Los cables STP se utilizan únicamente para instalaciones muy puntuales que requieran una calidad de transmisión muy alta.

Los segmentos de cable van desde cada una de las estaciones hasta un aparato denominado *hub* o concentrador, formando una topología de estrella.

2.1.2.2. Cable Coaxial

Del tipo RG-58. 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 y separados ambos elementos conductores por un cilindro de plástico. Las redes que utilizan este cable requieren que los adaptadores tengan un conector apropiado: los ordenadores forman una fila y se coloca un segmento de cable entre cada ordenador y el siguiente. En los extremos hay que colocar un terminador, que no es más que una resistencia de 50 ohmios. La velocidad máxima que se puede alcanzar es de 10Mbps.

2.1.2.3. 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 puede emitir luz. Y en el otro extremo se sitúa un detector de luz.

PROF. ALBERTO RAMOS

Curiosamente y a pesar de este sencillo funcionamiento, mediante los cables de fibra óptica se llegan a alcanzar velocidades de varios Gbps. Sin embargo, su instalación y mantenimiento tiene un coste elevado y solamente son utilizados para redes troncales con mucho tráfico. Los cables de fibra óptica son el medio de transmisión elegido para las redes de *cable* que ya están funcionando. Se pretende que este *cable* pueda transmitir televisión, radio, Internet y teléfono.

2.1.2.4. Medios inalámbricos

Denominados también conexión aérea por microondas electromagnéticas de alta frecuencia. Entre los medios inalámbricos (no guiados) se encuentran:

- **Ondas de radio**. Son capaces de recorrer grandes distancias, atravesando edificios incluso. Son ondas omnidireccionales: se propagan en todas las direcciones. Su mayor problema son las interferencias entre usuarios.

- **Microondas o**. Estas ondas viajan en línea recta, por lo que emisor y receptor deben estar alineados cuidadosamente. Tienen dificultades para atravesar edificios. Debido a la propia curvatura de la tierra, la distancia entre dos repetidores no debe exceder de unos 80 Kms. de distancia. Es una forma económica para comunicar dos zonas geográficas mediante dos torres suficientemente altas para que sus extremos sean visibles.

- **Infrarrojos**. Son ondas direccionales incapaces de atravesar objetos sólidos (paredes, por ejemplo) que están indicadas para transmisiones de corta distancia.

- **Ondas de luz**. Las ondas láser son unidireccionales. Se pueden utilizar para comunicar dos edificios próximos instalando en cada uno de ellos un emisor láser y un fotodetector.

2.1.3. DISPOSITIVOS INTERMEDIARIOS

2.1.3.1. Hub

Un *hub* o concentrador es el punto central desde el cual parten los cables de par trenzado hasta las distintos puestos de la red, siguiendo una topología de estrella. Se caracterizan por el número de puertos y las velocidades que soportan. Por ejemplo, son habituales los hubs 10/100 de 8 puertos.

- Los hubs *difunden* la información que reciben desde un puerto por todos los demás (su comportamiento es similar al de un ladrón eléctrico).

PROF. ALBERTO RAMOS

- Todas sus ramas funcionan a la *misma velocidad*. Esto es, si mezclamos tarjetas de red de 10/100 Mbps y 10 Mbps en un mismo hub, todas las ramas del hub funcionarán a la velocidad menor (10 Mbps).

- Es habitual que contengan un *diodo luminoso* para indicar si se ha producido una colisión. Además, los concentradores disponen de tantas lucecitas (LED) como puertos para informar de las ramas que tienen señal.

Interconexión de Hubs

Los concentradores incluyen un puerto diferenciado, etiquetado con el nombre "uplink" o "cascade", para facilitar su interconexión con otros hubs. El puerto "uplink" de un hub se conecta mediante un cable par trenzado directo hasta un puerto cualquiera (que no sea el "uplink") del otro hub. Si ninguno de los dos hubs tuviese el puerto "uplink" libre todavía se podrían interconectar utilizando un cable par trenzado cruzado.

Nota: *Todo lo que se comenta en este apartado referente a hubs (concentradores) es equivalente para los switches (conmutadores).*
¿Dónde se encuentra el puerto "uplink"? Dependiendo de los fabricantes se suele dar una de estas dos situaciones:

- El hub es de *n* puertos pero tiene *n+1* conectores, uno de ellos tiene una marca especial. Por ejemplo, son habituales los hubs que tienen 9 conectores: 7 puertos normales y un puerto mixto con dos conectores contiguos los cuales no se pueden utilizar simultáneamente. El número máximo de cables que podemos conectar es de 8, quedando un conector vacío (el marcado como "uplink" o el que tiene justo a su lado).

- El hub es de *n* puertos y tiene *n* conectores, uno de ellos tiene una marca especial. Mediante un botón conmutamos la función del conector diferenciado entre "uplink" y puerto normal. Las prestaciones son las mismas que en el caso anterior. Este diseño es habitual de los hubs del fabricante 3COM.

¿Cómo enlazar unos hubs con otros?

Los diseños más habituales son los dos siguientes, aunque se suelen combinar:

- ***Hubs encadenados***. Un hub se va conectando con el siguiente formando una cadena. No es conveniente conectar de esta forma más de 3 hubs puesto que el rendimiento de la red disminuirá considerablemente (las señales tardan en pasar desde el primer hub de la cadena hasta el último).

- ***Hubs en estrella***. Se coloca un hub en el centro y de éste se tiran cables hasta el resto de los hubs. Con esta solución se consiguen velocidades más altas en la red aunque el cableado es más costoso.

Prof. AIREJO RIOS

2.1.3.2. Switch

Un *switch* o conmutador es un hub mejorado: tiene las mismas posibilidades de interconexión que un hub (al igual que un hub, no impone ninguna restricción de acceso entre los ordenadores conectados a sus puertos). Sin embargo se comporta de un modo más eficiente reduciendo el tráfico en las redes y el número de colisiones.

- Un switch *no difunde* las tramas Ethernet por todos los puertos, sino que las retransmite sólo por los puertos necesarios. Por ejemplo, si tenemos un ordenador A en el puerto 3, un ordenador B en el puerto 5 y otro ordenador C en el 6, y enviamos un mensaje desde A hasta C, el mensaje lo recibirá el switch por el puerto 3 y sólo lo reenviará por el puerto 6 (un hub lo hubiese reenviado por todos sus puertos).

- Cada puerto tiene un *buffer* o memoria intermedia para almacenar tramas Ethernet.

- Puede trabajar con *velocidades distintas* en sus ramas (*autosensing*): unas ramas pueden ir a 10 Mbps y otras a 100 Mbps.

- Suelen contener 3 *diodos luminosos* para cada puerto: uno indica si hay señal (link), otro la velocidad de la rama (si está encendido es 100 Mbps, apagado es 10 Mbps) y el último se enciende si se ha producido una colisión en esa rama.

¿Cómo sabe un switch los ordenadores que tiene en cada rama?

Lo averigua de forma automática mediante *aprendizaje*. Los conmutadores contienen una tabla dinámica de direcciones físicas y números de puerto. Nada más enchufar el switch esta tabla se encuentra vacía. Un procesador analiza las tramas Ethernet entrantes y busca la dirección física de destino en su tabla. Si la encuentra, únicamente reenviará la trama por el puerto indicado. Si por el contrario no la encuentra, no le quedará más remedio que actuar como un hub y difundirla por todas sus ramas.

Las tramas Ethernet contienen un campo con la dirección física de origen que puede ser utilizado por el switch para agregar una entrada a su tabla basándose en el número de puerto por el que ha recibido la trama. A medida que el tráfico se incrementa en la red, la tabla se va construyendo de forma dinámica. Para evitar que la información quede desactualizada (si se cambia un ordenador de sitio, por ejemplo) las entradas de la tabla desaparecerán cuando agoten su tiempo de vida (TTL), expresado en segundos.

PROF. ALBERTO RAMOS

Dominios de colisión

Un *dominio de colisión* es un segmento del cableado de la red que comparte las mismas colisiones. Cada vez que se produzca una colisión dentro de un mismo dominio de colisión, afectará a todos los ordenadores conectados a ese segmento pero no a los ordenadores pertenecientes a otros dominios de colisión.

Todas las ramas de un *hub* forman un mismo dominio de colisión (las colisiones se retransmiten por todos los puertos del hub). Cada rama de un *switch* constituye un dominio de colisiones distinto (las colisiones no se retransmiten por los puertos del switch). Este es el motivo por el cual la utilización de conmutadores reduce el número de colisiones y mejora la eficiencia de las redes. El ancho de banda disponible se reparte entre todos los ordenadores conectados a un mismo dominio de colisión.

Nota: *Podemos indicar un número aproximado de 25-30 como medida máxima de ordenadores que se pueden conectar dentro de un mismo dominio de colisión. Sin embargo, este número dependerá en gran medida del tráfico de la red. En redes con mucho tráfico se debe tratar de reducir el número de ordenadores por dominio de colisión lo más posible mediante la creación de distintos dominios de colisión conectados por switches o mediante la creación de distintas subredes conectadas por routers.*

¿Qué instalar hubs o switches?

- Siempre que el presupuesto lo permita *elegiremos un switch antes que un hub*.

- Si nuestra red tiene un elevado número de ordenadores (hay que utilizar varios concentradores enlazados) pero sólo nos podemos permitir un switch, éste lo colocaremos en *el lugar de la red con más tráfico* (habitualmente será el concentrador situado en el centro de la estrella de estrellas o bien, aquél que contenga a los servidores). En el resto de las posiciones colocaremos hubs. El esquema descrito se utiliza a menudo: un hub en cada departamento y un switch para interconectar los departamentos con los servidores. Desde luego, lo ideal sería colocar switches en todas las posiciones.

- Además de la mejora en eficiencia que supone utilizar un switch frente a un hub, debemos considerar también el *aumento de seguridad*: si en un ordenador conectado a un switch se instala, con fines nada éticos, un programa para escuchar el tráfico de la red (*sniffer*), el atacante sólo recibirá las tramas Ethernet que corresponden a ese ordenador pero no las tramas de otros ordenadores que podrían contener contraseñas ajenas.

PROF. ALBEIRO RAMOS

2.1.3.3. Modem

En una red, la conexión a Internet también es importante, siempre se necesitará en cualquier momento sacar información de Internet y el Modem es un medio para conectarse. Hay que tener en cuenta que se usa un Modem para conectarse a Internet a través de la línea telefónica

Módem es un acrónimo de Modulador - DEModulador; es decir, que es un dispositivo que transforma las señales digitales del ordenador en señal telefónica analógica y viceversa, con lo que permite al ordenador transmitir y recibir información por la línea telefónica.

Los chips que realizan estas funciones están casi tan estandarizados como los de las tarjetas de sonido; muchos fabricantes usan los mismos integrados, por ejemplo de la empresa Rockwell, y sólo se diferencian por los demás elementos electrónicos o la carcasa.

Tipos de módems

La distinción principal que se suele hacer es entre módems internos y módems externos, si bien recientemente han aparecido unos módems llamados "módems software" o Winmódems, que han complicado un poco el panorama.

A. Internos: consisten en una tarjeta de expansión sobre la cual están dispuestos los diferentes componentes que forman el módem. Existen para diversos tipos de conector:

- **ISA**: debido a las bajas velocidades que se manejan en estos aparatos, durante muchos años se utilizó en exclusiva este conector, hoy en día en desuso.
- **PCI**: el formato más común en la actualidad.
- **AMR**: sólo en algunas placas muy modernas; baratos pero poco recomendables por su bajo rendimiento. La principal ventaja de estos módems reside en su mayor integración con el ordenador, ya que no ocupan espacio sobre la mesa y toman su alimentación eléctrica del propio ordenador. Además, suelen ser algo más barato debido a carecer de carcasa y transformador, especialmente si son PCI (aunque en este caso son casi todos del tipo “módem software”. Por contra, son algo más complejos de instalar y la información sobre su estado sólo puede obtenerse mediante software.

B. Externos: son similares a los anteriores pero metidos en una carcasa que se coloca sobre la mesa o el ordenador. La conexión con el ordenador se realiza generalmente mediante uno de los puertos serie o "COM", por lo que se usa la

Prof. ALBERO RAMOS

UART del ordenador, que deberá ser capaz de proporcionar la suficiente velocidad de comunicación; actualmente ya existen modelos para puerto USB, de conexión y configuración aún más sencillas.

La ventaja de estos módems reside en su fácil transportabilidad entre ordenadores, además de que podemos saber el estado el módem (marcando, con/sin línea, transmitiendo...) mediante unas luces que suelen tener en el frontal. Por el contrario, son un trasto más, necesitan un enchufe para su transformador y la UART debe ser una 16550 o superior para que el rendimiento de un módem de 28.800 bps o más sea el adecuado.

C. **Módems PC-Card**: son módems que se utilizan en portátiles; su tamaño es similar al de una tarjeta de crédito algo más gruesa, pero sus capacidades pueden ser igual o más avanzadas que en los modelos normales.

D. **Módems software, HSP o Winmódems**: son módems internos (al menos no conozco ninguno externo, y dudo que fuera posible construirlo) en los cuales se han eliminado varias piezas electrónicas, generalmente chips especializados, de manera que el microprocesador del ordenador debe suplir su función mediante software. Lo normal es que utilicen como conexión una ranura PCI (o una AMR), aunque no todos los módems PCI son de este tipo. La ventaja resulta evidente: menos piezas, más baratos. Las desventajas, que necesitan microprocesadores muy potentes (como poco un Pentium 133 MHz), que su rendimiento depende del número de aplicaciones abiertas (nada de multitarea mientras el módem funciona o se volverá una auténtica tortuga) y que el software que los maneja sólo suele estar disponible para Windows 95/98, de ahí el apelativo de Winmódems. Evidentemente, resultan poco recomendables pero son baratos...

E. **Módems completos**: los módems clásicos no HSP, bien sean internos o externos. En ellos el rendimiento depende casi exclusivamente de la velocidad del módem y de la UART, no del microprocesador.

La velocidad del módem

Resulta sin duda el parámetro que mejor define a un módem, hasta el punto de que en muchas ocasiones se habla simplemente de "un módem 33.600", o "un 14.400", sin especificar más. Estas cifras son bits por segundo, bps.

Se debe tener en cuenta que son bits, no bytes. En este contexto, un byte está compuesto de 8 bits; por tanto, un módem de 33.600 bps transmitirá (en las mejores condiciones) un máximo de 4.200 bytes por segundo, o lo que es lo mismo: necesitará como poco 6 minutos para transmitir el contenido de un disquete de 1,44 MB.

PROF. ALBERTO RAMOS

Por cierto: sólo en las mejores condiciones. La saturación de las líneas, la baja capacidad que proporcione el proveedor de acceso a Internet, la mala calidad del módem o de la línea (ruidos, interferencias, cruces...) suelen hacer que la velocidad media efectiva sea mucho menor, de 3.000 bytes/s o menos. Saber cuál de éstos es el factor limitante resulta vital para mejorar nuestro acceso a Internet.

Así mismo, no se debe confundir esta velocidad nominal (la que se supone que podría alcanzar el módem, por ejemplo 33.600 bps) con la velocidad de negociado, que es aquella que se nos indica al comienzo de una conexión a Internet; esta última es aquella que en principio, y en ese momento, ha identificado el módem del otro lado de la línea como válida, y tiene poco que ver con el rendimiento que obtendremos.

Así, una conexión en la que la velocidad de negociado ha sido de 31.200 bps podría acabar siendo mucho más rápida que otra en que se han alcanzado los 33.600. Sólo debe tenerse en cuenta este valor cuando es anormalmente bajo (como 14.400 con un módem de 33.600) o cuando nunca alcanzamos la velocidad máxima (lo que puede indicar que el módem, la línea o el proveedor son de mala calidad).

Las normas de comunicaciones

Las transmisiones de datos por vía telefónica se basan en una serie de estándares internacionales que deben cumplir los dispositivos implicados en la comunicación. Cada norma define una serie de parámetros tales que permiten la correcta comunicación a una cierta velocidad.

Así, cuando se dice que un módem cumple con la norma "V.34", quiere decir que es un módem que cumple una serie de especificaciones tal que le permite comunicarse con módems de esa velocidad (y usualmente de cualquier velocidad inferior a ésa). Las normas más importantes son:

Norma	Explicación	Velocidad máxima (bps)
V.22bis	Comunicaciones módem-módem	2.400
V.32		9.600
V.32bis		14.400
V.34		28.800
V.34+		33.600
V.90 y V.92		55.600
V.29	Comunicaciones módem-fax	14.400
V.42 y MNP2-4	Control de errores	No aplicable
V.42bis y MNP5-10	Compresión de datos	No aplicable

PROF. ALBERTO RAMOS

Además de estos estándares, existen dos pseudo-estándares (no son oficiales) para las transmisiones a 55.600 bps: el "K56flex" y el "x2". Son incompatibles entre sí; el de más éxito en España fue el K56flex de Rockwell, aunque el x2 se usaba mucho en Estados Unidos; estos pseudo-estándares se resistieron mucho a ser sustituidos por la norma oficial V.90 debido al excesivo tiempo que tardó en aparecer ésta.

2.1.3.4. Router

Un router (encaminador) es un dispositivo o componente de una red que tiene por objeto interconectar todas las redes y que tras analizar la información solicitada, selecciona de entre todos los caminos posibles aquel, a través del cual, la información llegará en el menor tiempo posible a su destino

Un router pertenece a la capa de red. Trabaja con direcciones IP. Se utiliza para interconectar redes y requiere una configuración. Podemos averiguar los routers que atraviesan nuestros datagramas IP mediante el comando **Tracert**.

2.1.4. PERIFÉRICOS COMPARTIDOS.

Éstos pueden ser de dos tipos:

A. Directos: Son los que se conectan a la red directamente, a través de su propia tarjeta de red.

B. Indirectos: Son los que se conectan a la red a través de algún equipo Servidor

2.2. PARTE LÓGICA. SOFTWARE DE RED

2.2.1.SISTEMA OPERATIVO DE RED.

Administra y gestiona las comunicaciones y recurso de la red, así como los datos, programas y aplicaciones. Ejemplo: Windows, Ubuntu, MAC, entre otros.

2.2.2.CONTROLADORES DE RED.

Así como cualquier dispositivo del computador necesita tener instalados sus correspondientes controladores, el hardware de red también tiene sus propios controladores. Un controlador es un programa que tiene implícita la forma de comunicación del dispositivo con el resto del sistema informático.

Prof. ALBEIRO RAMOS

2.2.3.PROGRAMAS DE APLICACIÓN.

Pueden ser de todo tipo, desde programas de aplicación general, hasta programas de comunicación tales como correo electrónico, navegador de páginas Web, etc.; hasta programas de terminal tal como el Telnet.

¿Cómo pueden entenderse entre sí, los diferentes componentes de una red informática, compuesta por equipos con distintas Arquitecturas?

La solución está en el estándar de red Ethernet, que se encarga de garantizar la compatibilidad física de los equipos de la red. Las tarjetas de Red Ethernet utilizan un método de control de acceso al medio denominado CSMA/CD, que consiste en que todos los equipos de una red, respetan rigurosamente el turno de palabra; de manera que cuando un ordenador quiere transmitir "escucha" la red hasta que nadie transmita.

Cuando ningún equipo transmite el equipo que quiere transmitir comienza a enviar sus datos. Si al transmitir se produce una colisión con otra transmisión, deja de enviar datos y espera un tiempo hasta continuar transmitiendo.

¡Qué bueno sería que los humanos cuando entablamos una conversación nos comportáramos como los equipos de una red que saben callar cuando el interlocutor está en el turno de palabra!

Prof. ALBERTO RAMOS

3. CLASIFICACIÓN DE UNA RED

3.1. SEGÚN SU TAMAÑO

3.1.1.LAN

(Local Area Network, redes de área local): Son las redes que todos conocemos, es decir, aquellas que se utilizan en nuestra empresa. Son redes pequeñas, entendiendo como pequeñas las redes de una oficina, de un edificio… Debido a sus limitadas dimensiones, son redes muy rápidas en las cuales cada estación se puede comunicar con el resto.

3.1.2.WAN

(Wide Area Network, redes de área extensa): Son redes punto a punto que interconectan países y continentes. Por ejemplo, un cable submarino entre Europa y América, o bien una red troncal de fibra óptica para interconectar dos países. Al tener que recorrer una gran distancia sus velocidades son menores que en las LAN aunque son capaces de transportar una mayor cantidad de datos.

3.1.3.MAN

(Metropolitan Area Network, redes de área metropolitana): Como vemos, las redes LAN son pequeñas y las redes WAN, muy grandes: debe existir algún término para describir unas redes de tamaño intermedio. Esto es, las redes MAN. Un ejemplo es la red utilizada en una pequeña población de la Comunidad Valenciana, Villena, para interconectar todos sus comercios, hogares y administraciones públicas (proyecto InfoVille).

3.2. SEGÚN SU DISTRIBUCIÓN LÓGICA

Todos los ordenadores tienen un lado cliente y otro servidor: una máquina puede ser servidora de un determinado servicio pero cliente de otro servicio.

3.2.1.SERVIDOR.

Máquina que ofrece información o servicios al resto de los puestos de la red. La clase de información o servicios que ofrezca determina el tipo de servidor que es: servidor de impresión, de archivos, de páginas web, de correo, de usuarios, de IRC (charlas en Internet), de base de datos…

3.2.2.CLIENTE.

Máquina que accede a la información de los servidores o utiliza sus servicios. Ejemplos: Cada vez que estamos viendo una página web (almacenada en un servidor

PROF. ALBEIRO RAMOS

remoto) nos estamos comportando como clientes. También seremos clientes si utilizamos el servicio de impresión de un ordenador remoto en la red (el servidor que tiene la impresora conectada).

Dependiendo de si existe una función predominante o no para cada puesto de la red, las redes se clasifican en:

- **REDES CLIENTE/SERVIDOR**. Los papeles de cada puesto están bien definidos: uno o más ordenadores actúan como servidores y el resto como clientes. Los servidores suelen coincidir con las máquinas más potentes de la red. No se utilizan como puestos de trabajo. En ocasiones, ni siquiera tienen monitor puesto que se administran de forma remota: toda su potencia está destinada a ofrecer algún servicio a los ordenadores de la red. Internet es una red basada en la arquitectura cliente/servidor.

- **REDES ENTRE IGUALES**. No existe una jerarquía en la red: todos los ordenadores pueden actuar como clientes (accediendo a los recursos de otros puestos) o como servidores (ofreciendo recursos). Son las redes que utilizan las pequeñas oficinas, de no más de 10 ordenadores.

Prof. ALBEIRO RAMOS

4. TOPOLOGÍAS

Es la forma como se conectan físicamente los equipos dentro de una red. Existen las siguientes topologías: Bus, Estrella, Anillo, Malla, Arbol y variaciones.

- La topología física de una red es el propio cable.
- La topología lógica es la forma en que se transmiten las señales por el cable.

4.1. BUS

Un enlace por cada nodo y estos se conectan a un enlace que une todas las estaciones. Único cable llamado backbone o trunk.

Comunicación en el bus

- Los datos en forma de señales se envían a todos los equipos
- Información aceptada por el equipo cuya dirección coincida
- Solo puede haber un equipo enviando señales
- El número de equipos conectados afectará el rendimiento de la red.

Factores que afectan el rendimiento

- Número de equipos conectados a la red
- Número total de ordenes emitidas esperando a ser ejecutadas
- Tipo de aplicación (cliente –servidor)
- Tipo de cable usado en la red
- Distancia entre los equipos en la red

Funcionamiento de señal

- La señal viaja de un lado a otro evitando que otros equipos envíen señales
- La señal debe ser detenida una vez haya encontrado la dirección
- Se detiene la señal usando un terminador.

Interrupción

- Si se desconecta uno de los extremos donde esta el terminador la señal rebotara y la red se detiene.
- Equipos funcionan como equipos aislados.

Expansión de la Red

Se deben utilizar los siguientes métodos:

Prof. ALBEIRO RAMOS

- Usar un acoplador (unión entre dos segmentos). Varios conectores debilitan la señal.
- Usar un dispositivo llamado repetidor para conectar dos cables.

Repetidor

- Amplifica la señal antes de reenviarla por el cable.
- Permite que una señal viaje más lejos y siga siendo recibida correctamente.

4.2. ESTRELLA

El nodo central, para N estaciones tiene N-1 enlaces, mientras que las otras estaciones tan solo tendrían uno que es el que les vendría de la estación central.

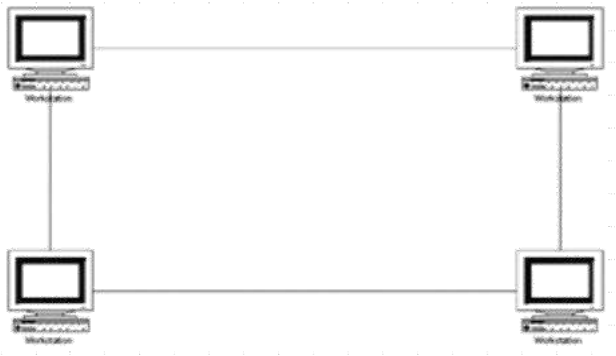
Funcionamiento

- Las señales son transmitidas desde el equipo emisor a través del hub o switch a todos los equipos de la red.
- Centraliza los recursos y la gestión.
- Cada equipo está conectado a un punto central

Interrupción

- Si el punto central falla, cae toda la red
- Si falla el cable que conecta el hub cae toda la red
- Si falla un solo equipo, este será el único que no podrá enviar o recibir datos de la red.

4.3. ANILLO



Cada nodo tiene dos enlaces, puesto que la información siempre le vendrá de un lado y la enviará hacia el otro.

Funcionamiento

- No existen finales con terminadores.
- La señal viaja en una dirección y pasa por cada equipo
- Cada equipo actúa como repetidor amplificando la señal, luego la envía a el otro equipo.
- El fallo de un equipo puede tener impacto sobre toda la red.

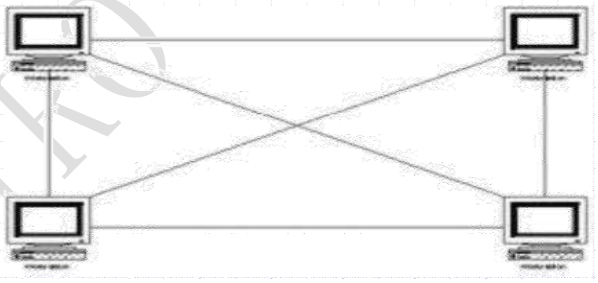
PROF. ALBEIRO RAMOS

Funcionamiento de señal

- Pase de testigo (método para transmitir en anillo)
- **Testigo**: secuencia especial de bits que viajan alrededor de una red token ring
- Cada red tiene únicamente un testigo
- El testigo pasa de equipo en equipo hasta que llega a un equipo con datos para enviar
- El equipo emisor modifica el testigo y coloca una dirección electrónica y lo envía por el anillo
- Los datos pasan por cada equipo hasta llegar al que tiene la dirección que coincide con la dirección de los datos.
- El receptor devuelve al emisor un mensaje verificando los datos.
- El testigo puede circular por un anillo de 2000 metros de diametro alrededor de unas 477.376 veces por segundo.

4.4. MALLA

Se caracterizan por encontrar caminos entre estaciones muy rápidamente Teniendo en cuenta (N(N-1))/2 enlaces.



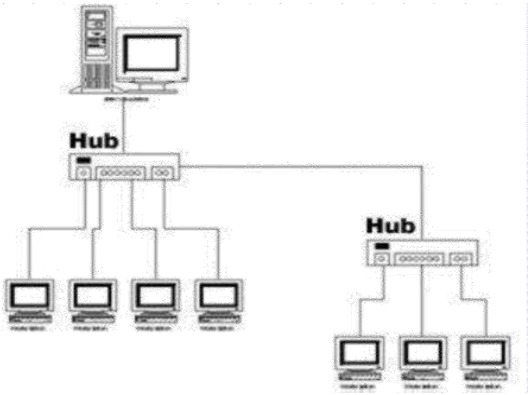
Funcionamiento

- Cada equipo está conectado a todos los demás equipos mediante cables separados.
- Si falla un cable otro se hará cargo del tráfico.
- Son costosas de instalar, ya que se utiliza mucho cableado.

4.5. ÁRBOL

Todas las estaciones cuelgan de un ordenador central y se conectan entre ellas a través de los hubs o switch ya instalados.

En cambio, un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos.



4.6. VARIACIONES SOBRE LAS TOPOLOGÍAS

4.6.1. ESTRELLA – BUS

- Varias redes con topología en estrella están conectadas entre sí con segmentos de bus.
- Si un equipo cae esto no afectara al resto de la red.

PROF. ALBEIRO RAMOS

- Si un hub o switch deja de funcionar, todos los equipos conectados a dicho hub no podrán comunicarse.
- Si un hub o switch está conectado a otros hubs o switch, estas conexiones también se interrumpirán.

4.6.2.ESTRELLA – ANILLO

- También llamado anillo cableado en estrella.
- Centradas en un hub que contiene el anillo o bus real
- Los hubs estan conectados en forma de estrella al hub principal

Prof. ALBEIRO RAMOS

5. COMUNICACIÓN EN UNA RED

5.1. CONMUTACIÓN DE CIRCUITOS, DE MENSAJES Y DE PAQUETES

La comunicación entre un origen y un destino habitualmente pasa por nodos intermedios que se encargan de encauzar el tráfico. Por ejemplo, en las llamadas telefónicas los nodos intermedios son las centralitas telefónicas y en las conexiones a Internet, los *routers* o encaminadores. Dependiendo de la utilización de estos nodos intermedios, se distingue entre conmutación de circuitos, de mensajes y de paquetes.

- En la **conmutación de circuitos** se establece un camino físico entre el origen y el destino durante el tiempo que dure la transmisión de datos. Este camino es exclusivo para los dos extremos de la comunicación: no se comparte con otros usuarios (ancho de banda fijo). Si no se transmiten datos o se transmiten pocos se estará infrautilizando el canal. Las comunicaciones a través de líneas telefónicas analógicas (RTB) o digitales (RDSI) funcionan mediante conmutación de circuitos.

- Un mensaje que se transmite por **conmutación de mensajes** va pasando desde un nodo al siguiente, liberando el tramo anterior en cada paso para que otros puedan utilizarlo y esperando a que el siguiente tramo esté libre para transmitirlo. Esto implica que el camino origen-destino es utilizado de forma simultánea por distintos mensajes. Sin embargo, éste método no es muy útil en la práctica ya que los nodos intermedios necesitarían una elevada memoria temporal para almacenar los mensajes completos. En la vida real podemos compararlo con el correo postal.

- Finalmente, la **conmutación de paquetes** es la que realmente se utiliza cuando hablamos de *redes*. Los mensajes se fragmentan en paquetes y cada uno de ellos se envía de forma independiente desde el origen al destino. De esta manera, los nodos (*routers*) no necesitan una gran memoria temporal y el tráfico por la red es más fluido. Nos encontramos aquí con una serie de problemas añadidos: la pérdida de un paquete provocará que se descarte el mensaje completo; además, como los paquetes pueden seguir rutas distintas puede darse el caso de que lleguen desordenados al destino. Esta es la forma de transmisión que se utiliza en Internet: los fragmentos de un mensaje van pasando a través de distintas redes hasta llegar al destino.

5.2. COMUNICACIÓN SIMPLEX, HALF-DUPLEX Y FULL-DUPLEX

- En una comunicación **simplex** existe un solo canal unidireccional: el origen puede transmitir al destino pero el destino no puede comunicarse con el origen. Por ejemplo, la radio y la televisión.

PROF. ALBERTO RAMOS

- En una comunicación **half-duplex** existe un solo canal que puede transmitir en los dos sentidos pero no simultáneamente: las estaciones se tienen que turnar. Esto es lo que ocurre con las emisoras de radioaficionados.

- Por último, en una comunicación **full-duplex** existen dos canales, uno para cada sentido: ambas estaciones pueden transmitir y recibir a la vez. Por ejemplo, el teléfono.

5.3. MECANISMOS DE DETECCIÓN DE ERRORES

¿Cómo puede saber el receptor que ha recibido el mismo mensaje que envió el emisor? ¿Cómo puede saber que no se ha producido ningún error que haya alterado los datos durante la transmisión? Estas cuestiones son las que vamos a plantear en este apartado: se necesitan mecanismos de detección de errores para garantizar transmisiones libres de errores. Si el receptor detecta algún error, puede actuar de diversas maneras según los protocolos que esté utilizando. La solución más sencilla es enviarle un mensaje al emisor pidiéndole que le reenvíe de nuevo la información que llegó defectuosa.

Los mecanismos de detección se basan en añadir a las transmisiones una serie de *bits* adicionales, denominados *bits de redundancia*. La redundancia es aquella parte del mensaje que sería innecesaria en ausencia de errores (es decir, no aporta información nueva: sólo permite detectar errores). Algunos métodos incorporan una redundancia capaz de corregir errores. Estos son los *mecanismos de detección y corrección de errores*. Como ejemplos de mecanismos de detección de errores vamos a estudiar a continuación la paridad y los códigos CRC.

5.3.1.Paridad

Las transmisiones se dividen en palabras de cierto número de bits (por ejemplo, 8 bits) y se envían secuencialmente. A cada una de estas palabras se le añade un único bit de redundancia (*bit de paridad*) de tal forma que la suma de todos los bits de la palabra sea siempre un número par (*paridad par*) o impar (*paridad impar*).

El emisor envía las palabras añadiendo los correspondientes bits de paridad. El receptor comprobará a su llegada que la suma de los bits de la palabra incluyendo la redundancia es un número par (si la codificación convenida entre emisor-receptor es de paridad par) o un número impar (paridad impar). Si el receptor encuentra alguna palabra que no se ajuste a la codificación establecida, le solicitará al emisor que le reenvíe de nuevo la información. La paridad únicamente permite detectar errores simples, esto es, que varíe un único bit en cada palabra. Si varían 2 bits, este mecanismo no es capaz de detectar el error.

Veamos un ejemplo de paridad par:

PROF. ALBERTO RAMOS

Datos *(8 bits)*	**Datos + redundacia** *(9 bits)*	**Suma de bits**
10110110	101101101	6
00101001	001010011	4
11001001	110010010	4
11111010	111110100	6
00010000	000100001	2

El receptor realizará la suma de bits a la llegada del mensaje. Si alguna palabra no suma un número par, significará que se ha producido un error durante la transmisión.

5.3.2.CRC

Los códigos de paridad tienen el inconveniente de que se requiere demasiada redundancia para detectar únicamente errores simples. En el ejemplo que hemos visto, sólo un 8/9 de la información transmitida contenían datos, el resto era redundancia. Los *códigos de redundancia cíclica* (CRC) son muy utilizados en la práctica para la detección de errores en largas secuencias de datos. Se basan en representar las cadenas de datos como polinomios. El emisor realiza ciertas operaciones matemáticas antes de enviar los datos. El receptor realizará, a la llegada de la transmisión, una división entre un polinomio convenido (*polinomio generador*). Si el resto es cero, la transmisión ha sido correcta. Si el resto es distinto significará que se han producido errores y solicitará la retransmisión al emisor.

5.4. CONTROL DE FLUJO

El control de flujo determina cómo enviar la información entre el emisor y el receptor de forma que se vaya recibiendo correctamente sin saturar al receptor. Nótese que puede darse el caso de un emisor rápido y un receptor lento (o un receptor rápido pero que esté realizando otras muchas tareas).

El mecanismo más sencillo de control de flujo se basa en devolver una *confirmación* o *acuse de recibo* (ACK) cada vez que el receptor reciba algún dato correcto o una señal de error (NACK) si el dato ha llegado dañado. Cuando el emisor recibe un ACK pasa a enviar el siguiente dato. Si, en cambio, recibe un NACK reenviará el mismo dato.

El procedimiento anterior tiene el gran inconveniente de que el canal se encuentra infrautilizado: hasta que el emisor no reciba un ACK no enviará ningún dato más, estando el canal desaprovechado todo ese tiempo. Una mejora de este método es el envío de una serie de datos numerados, de tal forma que en un sentido siempre se estén enviando datos (dato1, dato2, dato3…) y en el otro sentido se vayan recibiendo las confirmaciones (ACK1, ACK2, ACK3…). La cantidad de datos pendientes de ACK o NACK se establecerá según la memoria temporal del emisor.

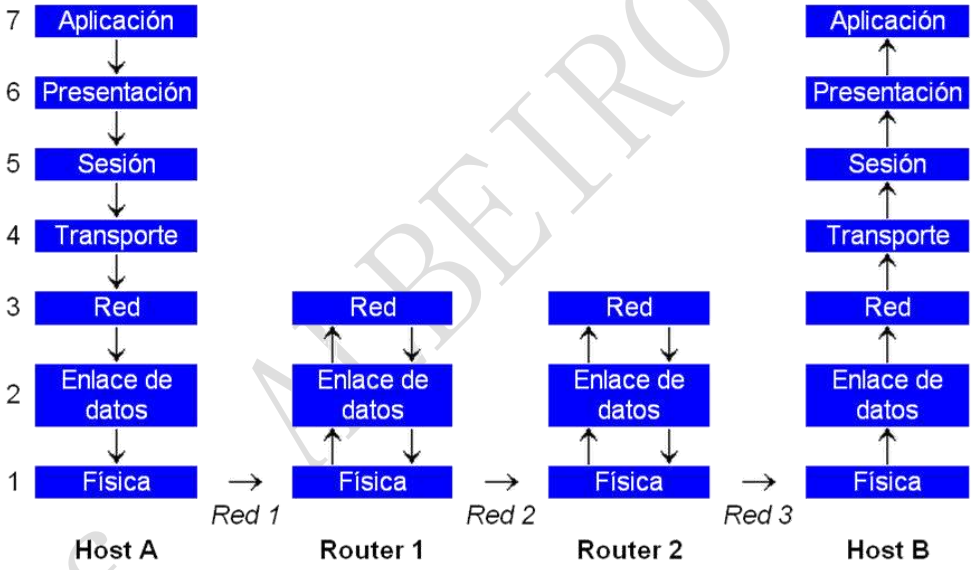
Prof. ALBERTO RAMOS

6. PROTOCOLOS

6.1. MODELO DE REFERENCIA OSI

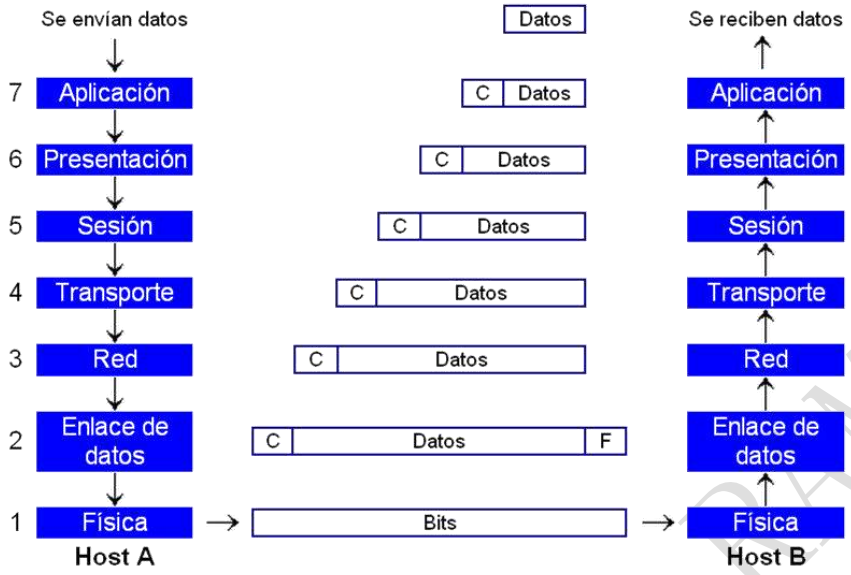
El modelo OSI (*Open Systems Interconnection*, interconexión de sistemas abiertos) fue un intento de la Organización Internacional de Normas (ISO) para la creación de un estándar que siguieran los diseñadores de nuevas redes. Se trata de un modelo teórico de referencia: únicamente explica lo que debe hacer cada componente de la red sin entrar en los detalles de implementación.

El modelo divide las redes en capas. Cada una de estas capas debe tener una función bien definida y relacionarse con sus capas inmediatas mediante unos interfaces también bien definidos. Esto debe permitir la sustitución de una de las capas sin afectar al resto, siempre y cuando no se varíen los interfaces que la relacionan con sus capas superior e inferior. Los creadores del modelo OSI consideraron que era 7 el número de capas que mejor se ajustaba a sus requisitos.



El gráfico anterior muestra las 7 capas del modelo OSI. Las tres primeras capas se utilizan para *enrutar*, esto es, mover la información de unas redes a otras. En cambio, las capas superiores son exclusivas de los nodos origen y destino. La capa física está relacionada con el medio de transmisión (cableado concreto que utiliza cada red). En el extremo opuesto se encuentra la capa de aplicación: un programa de mensajería electrónica, por ejemplo. El usuario se situaría por encima de la capa 7. El siguiente gráfico muestra el flujo de información entre capas.

Prof. ABEIRO RAMOS



El host A es el nodo origen y el host B, el nodo destino. Nótese que estos papeles se intercambian continuamente en cualquier comunicación. Supongamos que mediante este modelo queremos enviar un mensaje al usuario del host B. El mensaje son los "datos" que se han dibujado por encima de la capa 7. Estos datos van descendiendo de capa en capa hasta llegar a la capa física del host A. Cada capa añade un encabezado (C = cabecera) a los datos que recibe de la capa superior antes de enviárselos a su capa inferior. En la capa de enlace de datos se ha añadido también una serie de códigos al final de la secuencia (F = final) para delimitar no sólo el comienzo sino también el final de un paquete de datos. La capa física no entiende de datos ni de códigos: únicamente envía una secuencia de bits por el medio de transmisión (un cable).

Estos bits llegarán, probablemente pasando por varios encaminadores intermedios, hasta la capa física del host destino. A medida que se van recibiendo secuencias de bits, se van pasando a las capas superiores. Cada capa elimina su encabezado antes de pasarlo a una capa superior. Obsérvese que el mensaje que envía cada capa del host A a su capa inferior es idéntico al que recibe la capa equivalente del host B desde una capa inferior. Finalmente los datos llegarán a la capa de aplicación, serán interpretados y mostrados al usuario del host B.
Los paquetes de datos de cada capa suelen recibir nombres distintos. En la capa de enlace de datos se habla de *marcos* o *tramas*; en la capa de red, de *paquetes* o *datagramas*. En la capa de transporte, en ocasiones se utiliza el término *segmento*.

Cada capa se comunica con la capa equivalente de otro host (por ejemplo, la capa de red de un host *se entiende* con la capa de red de otro host). Sin embargo, como hemos visto, la comunicación realmente se realiza descendiendo capas en el host origen, transmitiendo por el medio físico y aumentando capas en el host destino. Cada capa añade algo nuevo a la comunicación, como vamos a ver ahora:

PROF. ALBERTO RAMOS

6.1.1.CAPA FÍSICA

Se encarga de la transmisión de bits por un medio de transmisión, ya sea un medio guiado (un cable) o un medio no guiado (inalámbrico). Esta capa define, entre otros aspectos, lo que transmite cada hilo de un cable, los tipos de conectores, el voltaje que representa un 1 y el que representa un 0. La capa física será diferente dependiendo del medio de transmisión (cable de fibra óptica, cable par trenzado, enlace vía satélite, etc.) No interpreta la información que está enviando: sólo transmite ceros y unos.

6.1.2.CAPA DE ENLACE DE DATOS

Envía tramas de datos entre hosts (o *routers*) de una misma red. Delimita las secuencias de bits que envía a la capa física, escribiendo ciertos códigos al comienzo y al final de cada trama. Esta capa fue diseñada originalmente para *enlaces punto a punto*, en los cuales hay que aplicar un control de flujo para el envío continuo de grandes cantidades de información. Para las *redes de difusión* (redes en las que muchos ordenadores comparten un mismo medio de transmisión) fue necesario diseñar la llamada **subcapa de acceso al medio**. Esta subcapa determina quién puede acceder al medio en cada momento y cómo sabe cada host que un mensaje es para él, por citar dos problemas que se resuelven a este nivel.

6.1.3.CAPA DE RED

Se encarga del encaminamiento de paquetes entre el origen y el destino, atravesando tantas redes intermedias como sean necesarias. Los mensajes se fragmentan en paquetes y cada uno de ellos se envía de forma independiente. Su misión es unificar redes heterogéneas: todos los host tendrán un identificador similar a nivel de la capa de red (en Internet son las direcciones IP) independientemente de las redes que tengan en capas inferiores (Token Ring con cable coaxial, Ethernet con cable de fibra óptica, enlace submarino, enlace por ondas, etc.)

6.1.4.CAPA DE TRANSPORTE

Únicamente se preocupa de la transmisión origen-destino. Podemos ver esta capa como una canalización fiable que une un proceso de un host con otro proceso de otro host. Un host puede tener varios procesos ejecutándose: uno para mensajería y otro para transferir archivos, por ejemplo. No se preocupa del camino intermedio que siguen los fragmentos de los mensajes. Integra control de flujo y control de errores, de forma que los datos lleguen correctamente de un extremo a otro.

PROF. ALBERTO RAMOS

6.1.5.CAPA DE SESIÓN

Se encarga de iniciar y finalizar las comunicaciones. Además proporciona servicios mejorados a la capa de transporte como, por ejemplo, la creación de puntos de sincronismo para recuperar transferencias largas fallidas.

6.1.6.CAPA DE PRESENTACIÓN

Codifica los datos que recibe de la capa de aplicación a un sistema convenido entre emisor y receptor, con el propósito de que tanto textos como números sean interpretados correctamente. Una posibilidad es codificar los textos según la *tabla ASCII* y los números en *complemento a dos*.

6.1.7.CAPA DE APLICACIÓN

Aquí se encuentran los protocolos y programas que utiliza el usuario para sus comunicaciones en red. Esta capa tendrá que ser adaptada para cada tipo de ordenador de forma que sea posible el envío de un correo electrónico (u otros servicios) entre sistemas heterogéneos como Macintosh, Linux o Windows.

El modelo OSI, patrocinado por la Comunidad Europea y, más tarde, por el gobierno de los Estados Unidos, nunca llegó a tener la implantación esperada. Entre otros motivos, porque el modelo TCP/IP ya había sido aceptado por aquella época entre investigadores los cuales se resistieron a un cambio que, para la mayoría, era un cambio a peor. Las bases que sustentan Internet son realmente sencillas y quizás esto ha sido la clave de su éxito; el modelo OSI, en cambio, fue tan ambicioso y complejo que terminó arrinconado en las estanterías de los laboratorios. Sin embargo, la idea de la división por capas del modelo OSI es realmente valiosa. Esta misma idea se aplica a todas las redes actuales, incluyendo Internet.

6.2. TCP/IP

Como hemos comentado al principio, OSI es un modelo teórico general que da preferencia a un buen diseño en papel, antes que a la implementación de los protocolos. El modelo TCP/IP (Transmission Control Protocol/Internet Protocol, Protocolo de Control de Transmisión/Protocolo de Internet) se hizo justamente al revés: primero vinieron los protocolos y, después, se pensó en sus especificaciones. De tal forma, que el modelo TCP/IP únicamente es aplicable para la pila de protocolos TCP/IP pero no es válido para nuevas redes.

El modelo TCP/IP tiene únicamente 3 capas: capa de red, de transporte y de aplicación. No tiene las capas de sesión ni de presentación que, por otro lado, estaban prácticamente vacías en el modelo OSI. Tampoco dice nada de las capas física y de enlace a datos. Sin embargo, nosotros seguiremos un modelo de referencia fruto de combinar los modelos OSI y TCP/IP. Se trata del modelo real que

PROF. ALBERTO RAMOS

se está utilizando actualmente en las redes TCP/IP. El siguiente gráfico refleja las 5 capas de nuestro modelo.

Capa de aplicación (HTTP, SMTP, FTP, TELNET…)
Capa de transporte (UDP, TCP)
Capa de red (IP)
Capa de acceso a la red (Ethernet, Token Ring…)
Capa física (cable coaxial, par trenzado…)

Prof. ALBEIRO RAMOS