

CARACTERIZACION DE REDES



Caso práctico



Arquitecto - Anónimo - OpenOffice

CASO: Tomás ha decidido que quiere enterarse de todo lo relacionado con el mundo de las redes de ordenadores, aunque él se dedica a diseñar planos, está cansado de tener que llamar a su cuñado cada vez que deja de funcionar la red que tiene instalada en su oficina, además, siempre ha tenido inquietudes y ha decidido matricularse en un ciclo formativo de enseñanza a distancia. Se ha decidido por el ciclo ASI y aunque consta de varios módulos, por ahora dedicará su tiempo en exclusiva al módulo de Planificación y Administración de Redes. Los profesores le han asegurado que si supera el módulo tendrá los conocimientos suficientes como para poder administrar con garantías su pequeña red. Para empezar, necesita conocer qué tipo de red tiene instalada.

¿Qué tipo de red tendrá instalada en su tienda nuestro personaje?

1. TERMINOLOGIA

En esta unidad tomaremos contacto con el mundo de las redes de ordenadores, conoceremos sus características básicas, así como las diferentes técnicas utilizadas en su estudio.

1.1. CLASIFICACION DE LAS REDES

Las redes de ordenadores se pueden clasificar de acuerdo a varios criterios. Los dos criterios más comunes son la extensión que ocupan todos sus elementos y la tecnología de transmisión.

Atendiendo a la tecnología de transmisión las redes se pueden clasificar en:

- Redes de difusión.
- Redes punto a punto.

Si lo que tenemos en cuenta es la extensión de la red, estas se pueden clasificar en:

- Redes LAN.
- Redes MAN.
- Redes WAN.

1.2. REDES DE DIFUSION

Las redes de difusión son aquellas redes en las que se comparte un mismo canal de comunicación entre todos los nodos. Cuando uno de los nodos envía información, este tipo de redes tiene mecanismos para conseguir que aún compartiendo todos el mismo [canal](#), la información llegue solamente al nodo al que va destinada.

Por ejemplo, cuando nosotros llamamos a una persona que se encuentra entre otras muchas, aunque todas oyen el mensaje, solamente nos contestará la persona requerida. En este caso, hemos compartido todos el mismo canal, pero hemos utilizado el nombre de esa persona para que la información sea solamente válida para ella, aunque todos los demás la han escuchado.

Esta tecnología se utiliza en redes pequeñas.

1.3. REDES PUNTO A PUNTO

Las redes "punto a punto", como su propio nombre nos puede indicar, son redes en las que existen multitud de conexiones entre pares individuales. En este caso no se comparte canal y puede haber muchas rutas. Esta tecnología es la causante del gran éxito de aplicaciones con Emule, aplicaciones que sirven para intercambiar datos entre dos personas. A veces se les asigna el nombre de "p2p" o "pear to pear".

Las redes que soportan esta tecnología son redes grandes.

1.4. REDES LAN

Red de Area Local, es una abreviatura de Local Area Network. Una red LAN es interconexión entre dos o más nodos de red, entendiendo como nodo todo aquel dispositivo que es capaz de ser identificado en la red, cuya extensión puede ir desde los pocos centímetros hasta 1 Km aproximadamente. La visión más sencilla de una red LAN es la de dos ordenadores unidos mediante un cable, pero cuando nos hablan de una red LAN el ejemplo que mejor comprendemos es el de dos ordenadores unidos a un dispositivo (router, switch o hub) mediante cables y que hace posible que se puedan compartir recursos entre ellos. Otro ejemplo de red LAN es la de un conjunto de ordenadores que están situados en un mismo local y tienen una disposición que les permite comunicarse entre sí, por ejemplo, los ordenadores de una oficina que comparten una misma impresora.



RED_LAN – T. Fernández Escudero – Elaboración propia

1.5. REDES MAN

Es una abreviatura de Metropolitan Area Network. Es un conjunto de nodos de red que se hallan distribuidos geográficamente sobre una extensión del tamaño de una ciudad. El objetivo es el mismo que en el caso de las redes LAN, compartir recursos, pero los medios utilizados varían porque la distancia entre nodos es mayor. Si los ordenadores de una ciudad pudieran comunicarse entre sí, utilizando solamente los medios físicos que se encuentran en esa ciudad, diríamos que esos ordenadores formarían una red de tipo MAN. En la actualidad nosotros enviamos un mensaje a un amigo que vive en la calle de al lado a través del ordenador pero lo hacemos utilizando la red de tipo WAN porque utilizamos los servicios que hemos contratado con un determinado ISP. Si en nuestra ciudad hubiera una infraestructura técnica que permitiría conectar todos los ordenadores entre sí sin utilizar servicios de fuera de nuestro área metropolitana, estaríamos en una MAN. Pero esta disposición nos obligaría a almacenar a todos en nuestros equipos muchísima información para poder hacer atractiva nuestra red, y estaríamos renunciando a todos los recursos que navegan en la red WAN (Internet) y también a poder comunicarnos con personas que vivieran fuera de nuestra localidad.



RED_MAN – T. Fernández Escudero – “Elaboración propia”

En la figura anterior, se ve la disposición que tendrían los ordenadores en una red de tipo MAN perteneciente a una ciudad con 5 calles (calle 1, calle 2, calle 3, calle 4, calle 5).

1.5. REDES WAN

Es una abreviatura de Wide Area Network. Es una red que abarca una gran área, este tipo de disposición es la que usa Internet, es un conjunto de redes de tipo LAN y MAN unidas entre sí. Una red WAN puede comunicar distintos puntos de la Tierra. En una red de tipo WAN conviven muchas tecnologías, medios de comunicación y dispositivos, así como clases de usuarios. Así como la red más sencilla es la que está constituida por 2 ordenadores unidos mediante un cable, la más compleja es una red de tipo WAN cuya estructura se asemeja a una gran telaraña que cubre todo un país, continente o planeta.



RED_WAN – T. Fernández Escudero – “Elaboración propia”



Autoevaluación

Las redes se clasifican en LAN, MAN y WAN de acuerdo a:



- ☐ El tipo de interconexiones que utilizan, modem para las LAN y router para las MAN y WAN.
- ☐ La tecnología de transmisión.
- ☐ El número de elementos que forman parte de la red.
- ☐ El área que abarcan todos los elementos que forman la red. (Correcta)

1.6. PROYECTO OPTE

Si representásemos todas las conexiones entre ordenadores servidores que existen y dan vida a Internet nos quedaría algo similar a lo que representa la siguiente figura:



OPTE – OPTE - <http://www.opte.org/maps/>

Cada color representa las redes pertenecientes a los dominios de Internet net, ca, us com, org mil, gov, edu, jp, cn, tw, au, de, uk, it, pl, fr, br, kr, nl.

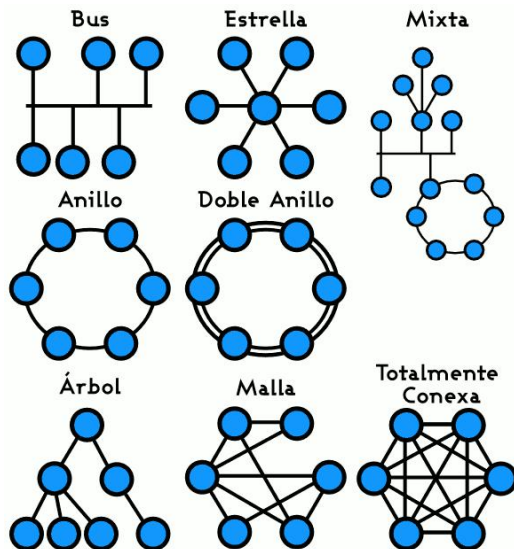
Esto es lo que están haciendo los científicos que están desarrollando el proyecto **OPTE**. Este proyecto tiene como objetivo representar en tiempo real en un mapa todas las conexiones que forman Internet.

net, ca, us com, org mil, gov, edu, jp, cn, tw, au de, uk, it, pl, fr br, kr, nl.

1.7. TOPOLOGIAS

La topología de red se define como la cadena de comunicación usada por los nodos que conforman una red para comunicarse. La topología se puede referir tanto al camino físico como al lógico.

Las principales topologías de red son bus, estrella, anillo y malla. Internet es un claro ejemplo de malla. La topología es uno de los criterios que se pueden tener en cuenta si queremos clasificar una red.



TOPOLOGIAS - [http://commons.wikimedia.org/wiki/GNU - Free_Documentation_License](http://commons.wikimedia.org/wiki/GNU_Free_Documentation_License)

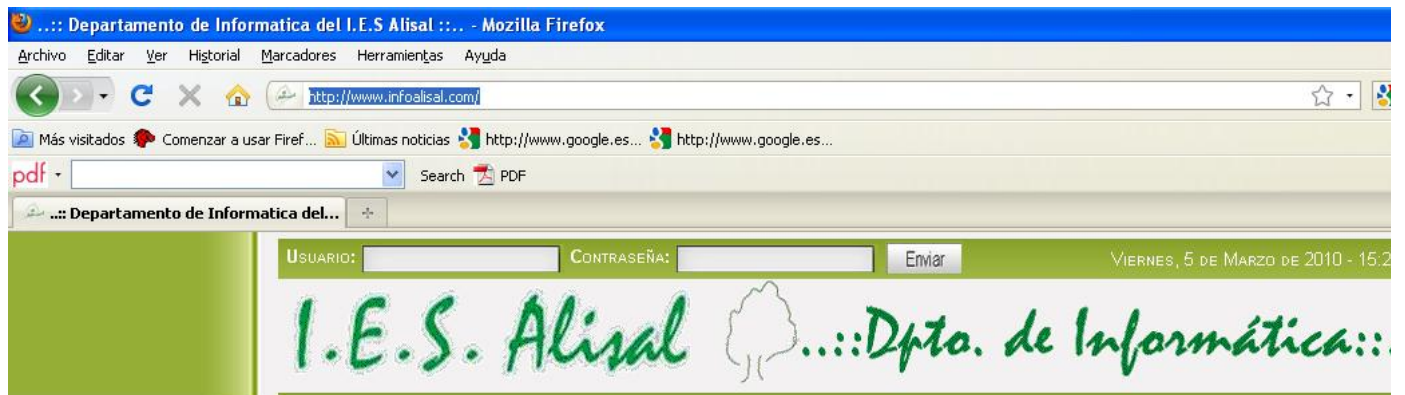
Un tipo de topología muy común es la topología en estrella, un elemento sirve para interconectar los demás nodos de la red, por ejemplo, varios ordenadores unidos entre sí mediante un [switch](#) o un [router](#); En las redes de tipo LAN se suele seguir este tipo de topología.

1.8. ARQUITECTURA

La arquitectura de una red es el conjunto de elementos, normas, protocolos, estándares y todo lo necesario para poder definir un determinado tipo de red. De igual modo que podemos clasificar los edificios por los materiales utilizados, el tamaño, la forma, el color, también lo podemos hacer en las redes informáticas por su arquitectura. Las principales arquitecturas son las arquitecturas de niveles, capas y protocolos OSI y TCP/IP. El principal cometido de una arquitectura es el poder separar las funciones de cada uno de los elementos que intervienen en una red. Por ejemplo, por un lado se gestionan los componentes físicos, por otro lado el software de base y por último las aplicaciones de usuario, esto sería un ejemplo de una arquitectura de red de tres niveles.

1.9. PROTOCOLOS

Los protocolos son las normas que se deben cumplir, tanto a nivel lógico como físico para que una red funcione. Son las reglas necesarias para que la red funcione como tal. Ejemplos de protocolos son, Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, ATM, HDLC, IP, TCP, UDP, FTP, HTTP, Telnet, SSH, POP3, SMTP, IMAP, PPP. Cada protocolo es válido para un determinado nivel; HTTP es el protocolo (entre otros más) que nos permite visualizar una página web en nuestro navegador.



PROTOCOLO HTTP – T. Fernández Escudero - WEB DPTO IES ALISAL

AUTOEVALUACION



Autoevaluación

Cuando todos los elementos que forman parte de una red están unidos entre sí a través de otro nodo central se dice que esa red tiene una topología:

- ☐ En anillo porque si elimino uno de los nodos se rompe la comunicación en toda la red.
- ☐ En estrella.
- ☐ Física en estrella.
- ☐ Lógica en anillo.

2. SISTEMAS DE NUMERACION



Caso práctico



PENSANDO - T. Fernández Escudero - "Elaboración propia"

CASO: Una vez que Tomás tiene claro qué tipo de red tiene instalada y por consejo de su cuñado, ha decidido actualizar uno de los equipos para poder trabajar mejor.

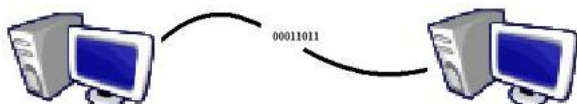
Buscando en los folletos de publicidad del buzón ha encontrado una oferta que le resulta atractiva.

Al leer las prestaciones del equipo se ha sorprendido de que no ha entendido casi nada, a duras penas ha ido traduciendo casi todas las frases pero hay unas cuantas que no consigue entender "nuevo procesador de 64 bits", "memoria RAM 1 GigaByte", "disco duro 300 GigaByte". ¿Qué serán los bits y los Byte?

Información es todo aquello que contiene datos útiles para poder ser tratados por un sistema. Pueden ser datos de entrada, de proceso o de salida.

Los sistemas en los que la información que entra es distinta que la que sale, ya que ha sufrido una transformación, se denominan "sistemas de tratamiento de la información".

Diremos que el computador trabaja con información que se representa mediante códigos. Estos códigos permiten representar en función del alfabeto utilizado, todo tipo de caracteres en general. La labor de asignar un código se conoce con el nombre "codificar" y consiste en traducir un valor real para que el computador pueda interpretarlo.



Sistemas de numeración - T. Fernández Escudero - "Elaboración propia"

Ejemplo: La letra 'A' se representa como 00011011 utilizando el código adecuado.

El ordenador trabaja en alfabeto binario, puesto que los componentes internos solo distinguen entre dos estados. Estos dos estados los representamos como:

0 = Ausencia de información

1 = Información

A los ceros y unos los llamaremos "bits".

El concepto de código se define con la correspondencia que existe entre los caracteres que queramos representar y su representación.

El "código binario" será capaz de representar tantas variables como nos indique el resultado de la fórmula:

$$\text{variables} = 2^n$$

Donde n es el número de bits que tomaremos.

2.1. CODIGOS NUMERICOS

Código decimal:

También llamado sistema en base 10, representa los números en potencias sucesivas de diez.

Ejemplo: 1972 se puede representar como:

$$1 * 10^3 = 1000$$

$$9 * 10^2 = 900$$

$$7 * 10^1 = 70$$

$$2 * 10^0 = 2$$

$$4563$$

De esta representación podemos deducir que para representar un número como suma de potencias sucesivas de la base en la que se está, tenemos que considerar que cada dígito es un número que multiplica de derecha a izquierda a la base en la que queremos representar a dicho número de forma que esta será una potencia que empiece siendo elevada a cero y seguirá incrementando de uno en uno hasta el número más alto representado.

$$a_1 a_2 a_3 \dots a_n_{(10)} = 1972_{(10)}$$

$$Base_{(m)} = Base_{(10)}$$

$$a_1 * 10_{n-1} + a_2 * 10_{n-2} + a_3 * 10_{n-3} + \dots + a_n * 10_{n-n}$$

$$1 * 10^3 + 9 * 10^2 + 7 * 10^1 + 2 * 10^0$$

Código binario:

Es un código que utiliza sólo dos dígitos {0,1}

$$a_1 * 2_{n-1} + a_2 * 2_{n-2} + a_3 * 2_{n-3} + \dots + a_n * 2_{n-n}$$

Ejemplo: 10111_2

$$1 * 2^4 + 0 * 2^3 + 1 * 2^2 + 1 * 2^1 + 1 * 2^0 = 23_{(10)}$$

Código octal:

Es un código que trabaja con ocho dígitos {0, 1, 2, 3, 4, 5, 6, 7}. El método más rápido para pasar a octal desde binario es hacer agrupaciones de tres dígitos del número en binario, calcular el valor decimal de cada grupo, los valores obtenidos formarán el número en octal.

$$a_1 * 8^{n-1} + a_2 * 8^{n-2} + a_3 * 8^{n-3} + \dots + a_n * 8^{n-n}$$

Ejemplo: 675_8

$$6 * 8^2 + 7 * 8^1 + 5 * 8^0 = 445_{(10)}$$

Código hexadecimal:

Es un código que trabaja con diez dígitos y seis letras {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F}. El método más rápido para pasar de binario a hexadecimal es hacer agrupaciones de cuatro dígitos del número en binario, calcular el valor decimal de cada grupo, los valores obtenidos formarán el número en octal. Cuando el equivalente decimal sea superior a 9, se utilizan letras, para el 10 la A, el 11 la B, el 12 la C, el 13 la D, 14 la E y el 15 la F.

$$a_1 * 16^{n-1} + a_2 * 16^{n-2} + a_3 * 16^{n-3} + \dots + a_n * 16^{n-n}$$

$$CFA56_{(16)}$$

$$C * 16^4 + F * 16^3 + A * 16^2 + 5 * 16^1 + 6 * 16^0 = 328198_{(10)}$$

2.2. EQUIVALENCIA ENTRE CODIGOS

La correspondencia entre los sistemas decimal, binario, octal y hexadecimal, es la representada en la siguiente tabla:

DECIMAL	BINARIO	OCTAL	HEXADECIMAL
0	0	000	0000
1	0001	001	0001
2	0010	010	0010
3	0011	011	0011
4	0100	100	0100
5	0101	101	0101
6	0110	110	0110
7	0111	111	0111
8	1000	001000	1000
9	1001	001001	1001
10	1010	001010	A
11	1011	001011	B
12	1100	001100	C
13	1101	001101	D
14	1110	001110	E
15	1111	001111	F

La manera más rápida para pasar de un código a otro es tener el número codificado en binario y a partir de él conseguir el valor en decimal, octal o hexadecimal es una tarea sencilla.

Ejemplo: OCTAL --- BINARIO

$56760_{(8)}$

Si cada uno de los dígitos que forman el número octal lo tomamos como un dígito decimal y le transformamos a su equivalente binario de 3 bits, nos quedaría que:

5 -> 101

6 -> 110

7 -> 111

6 -> 110

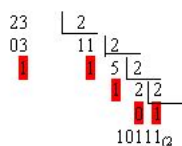
0 -> 000

Con lo que el número en binario que se corresponde con el 56760 octal es $101110111110000_{(2)}$

Conversión decimal a base e:

El paso de base decimal o base 10 a cualquier base se realiza dividiendo sucesivamente el número que queremos transformar utilizando como divisor la base a la que queremos pasar el número hasta que el dividendo sea menor que el divisor. El nuevo número se formará tomando como primer dígito el resultado del último cociente y los restos obtenidos en orden inverso a su obtención.

Ejemplo: $23_{(10)}$



DIVISION - T. Fernández Escudero - "Elaboración propia"

Conversión de base n a base decimal:

El paso de cualquier base a la base diez se realiza multiplicando de derecha a izquierda los dígitos del número que estamos transformando por potencias sucesivas de la base en la que está dicho número empezando por el exponente cero. Cada resultado obtenido se suma y el resultado global es el número en base 10.

Ejemplo: Si tenemos un número en base 16:

$CE72_{(16)}$

Si lo expresamos en función de las potencias de 16, obtendríamos el equivalente en base decimal:

$$C \cdot 16^3 + E \cdot 16^2 + 7 \cdot 16^1 + 2 \cdot 16^0 = 52850_{(10)}$$

Conversión de base m a base n:

El paso correcto sería pasar de la base original a base 10 y después de base 10 a la base destino.

Ejemplo:

Si partimos de un número en base 5 y queremos pasarlo a base 12, primero calculamos su equivalente decimal (base 10)

$$104_{(5)} \\ 1 \cdot 5^2 + 0 \cdot 5^1 + 4 \cdot 5^0 = 29_{(10)}$$

A continuación pasamos el 29 decimal a base 12:

El número en base 12 sería el 25:

$$\begin{array}{r} 29 \div 12 \\ \hline 25_{(12)} \end{array}$$

DIVISION2 - T. Fernández Escudero - "Elaboración propia"



Autoevaluación

La dirección IP 192.168.1.1 está expresada:

- ☐ En código binario y su equivalente decimal es 11000000.10101000.00000001.00000001.
- ☐ En hexadecimal y su equivalente binario es C0.A8.1.1.
- ☐ En binario y su equivalente decimal es 192.168.1.1.
- ☐ En decimal y su equivalente octal es 300.250.1.1.

3. ARQUITECTURA DE REDES



Caso práctico



ARQUITECTO PROTOCOLO - T. Fernández Escudero - "Elaboración propia"

funcionamiento.

Antes de irse, el técnico le ha dicho "Sr. la dirección IP de su router es 192.168.1.1, el usuario es admin y no tiene clave, si necesita acceder al router no tiene más que abrir el explorador y utilizando el protocolo http escribir la dirección del router"

Tomás ha asentido con la cabeza y se han despedido. Tras cerrar la puerta se ha apresurado a apuntar en un papel todo lo que el técnico le ha dicho, pero él no para de preguntarse ¿Qué es eso de IP? ¿Y esos números tan raros? ¿Para qué? ¿Qué es un protocolo?

CASO: Nuestro personaje ya sabe que su red es una red de tipo LAN y que tiene topología física en estrella puesto que todos los ordenadores se unen a un dispositivo común.

Además ya sabe que su ordenador trabaja con 64 bits y que tiene la noción de los que significan los bits.

Ahora Tomás quiere tener más velocidad para navegar por Internet y se lo ha solicitado a la compañía telefónica. Ha venido un técnico y le ha traído un dispositivo nuevo con más luces que el viejo que tenía, le ha conectado todos los cables y lo ha puesto en

La arquitectura de redes viene definida por tres características fundamentales:

- Protocolos de alto nivel: Nos dicen como se comunican las aplicaciones.
- Protocolos de bajo nivel: Definen como se transmiten las señales a nivel físico, por ejemplo por el cable.
- Protocolos de nivel medio: Son protocolos más difíciles de explicar porque rigen el funcionamiento de los niveles intermedios, que son los niveles menos visibles. Un ejemplo serían los protocolos de acceso al medio (CSMA/CD).

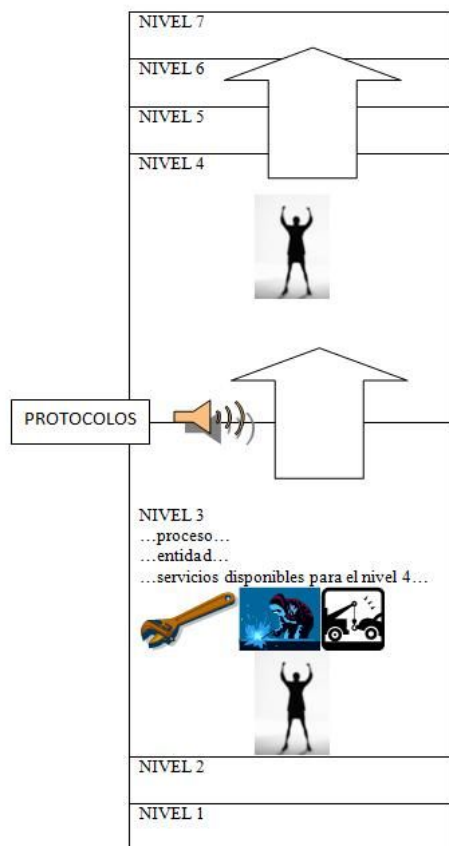
3.1. CAPA, SERVICIO, INTERFAZ, PROTOCOLO

Las redes se organizan en capas o niveles para reducir la complejidad de su diseño ("divide y vencerás").

Cada nivel es responsable de ofrecer servicios a niveles superiores. A la arquitectura por niveles también se la llama JERARQUIA DE PROTOCOLOS.

Cuando se diseña una determinada arquitectura se deben cumplir entre otras, las siguientes reglas:

- Cada nivel dispone de un conjunto de servicios.
- Los servicios están definidos mediante protocolos estándares.
- Cada nivel se comunica solamente con el nivel inmediatamente superior y el inmediatamente inferior.
- Los niveles inferiores proporcionan servicios a los niveles superiores.
- Los niveles de dos equipos diferentes se tienen que poner de acuerdo y utilizar las mismas reglas de transmisión (mismo protocolo).
- A los elementos activos de cada capa se les llama entidades o procesos y son estos los que se comunican mediante el uso del protocolo.
- A las entidades o procesos en máquinas diferentes que están al mismo nivel se les llama entidades pares o procesos pares.



Arquitectura de niveles - T. Fernández Escudero - "Elaboración propia"

"Los servicios utilizan los protocolos para que haya comunicación entre los niveles"

3.1.1. SERVICIOS

Los servicios se pueden clasificar en:

- Orientados a la conexión.
- No orientados a la conexión.
- Confirmados (fiables).
- No confirmados (no fiables).

Los servicios posibles de una capa son:

- Servicios orientados a la conexión y confirmados.
- Servicios orientados a la conexión y no confirmados.
- Servicios no orientados a la conexión y confirmados.
- Servicios no orientados a la conexión y no confirmados.

Los servicios básicos son:

- CONNECT: Para establecer una conexión. Se utiliza en comunicaciones orientadas a la conexión.
- DISCONNECT: Se utiliza para liberar una conexión y terminar la conexión. Servicio orientado a la conexión.
- DATA: Para enviar información, tanto orientado a la conexión como sin conexión.

Cuando una capa cualquiera de la arquitectura desea establecer una conexión con su homónima remota, deberá realizar una llamada al servicio CONNECT de la capa que tienen debajo. Ésta, a su vez, también debe realizar esa llamada, a no ser que se trate de la capa más inferior. Lo mismo ocurre con los servicios DISCONNECT y DATA.

3.1.2. PRIMITIVAS

Un servicio está definido por un conjunto de operaciones más sencillas llamadas primitivas.

PRIMITIVA	SIGNIFICADO
Request (petición)	Solicitud para realizar una acción
Indication (indicación)	Notificación de que ha ocurrido un suceso
Response (respuesta)	Solicitud de respuesta a un suceso
Confirm (confirmación)	Notificación de que ha llegado la respuesta de una acción anterior

Las primitivas no "viajan" entre las estaciones que se comunican. Los mensajes de control o de datos se envían como consecuencia de una llamada a la primitiva correspondiente.

Las primitivas tampoco son recibidas, sino que son utilizadas para notificar a la capa que el mensaje ha sido recibido y está disponible para su inspección o tratamiento.

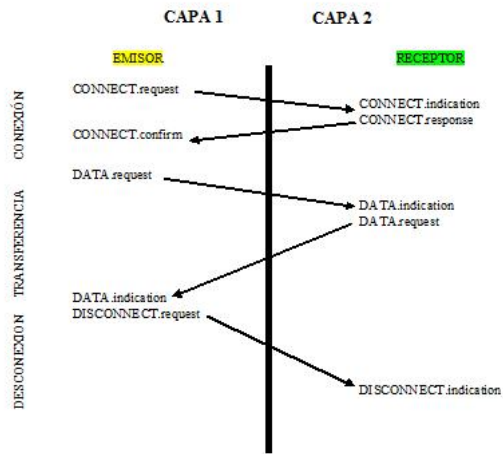
Por lo tanto, las primitivas de solicitud de envío funcionan como "llamadas al sistema", están en cada capa y se activan dependiendo de la tarea a realizar.

SERVICIO.PRIMITIVA	Parámetros
CONNECT.request	Dirección de la estación de destino. Servicio requerido. Tamaño máximo del mensaje.
CONNECT.indication	Dirección de la estación de origen. Servicio que solicita. Tamaño máximo del mensaje.
CONNECT.response	Aceptación de la conexión. Tamaño máximo del mensaje.
CONNECT.confirm	Aceptación de la conexión. Tamaño máximo del mensaje.
DATA.request	Dirección destino. Mensaje a enviar. Tamaño del mensaje. Número de mensaje (para el orden).
DATA.indication	Dirección de origen. Mensaje recibido. Tamaño del mensaje. Número del mensaje.
DATA.response	Número de mensaje recibido. ¿Hay error?
DATA.confirm	Número de mensaje recibido. ¿Hay error?
DISCONNECT.request	
DISCONNECT.indication	

Reglas básicas a la hora de trabajar con primitivas:

- El servicio CONNECT siempre es confirmado, por lo que, si aparece, llevará siempre las primitivas request, indication, response y confirm.
 - Impide la pérdida accidental de datos.
 - Opción al otro extremo de poder negar determinadas solicitudes de conexión.
 - Permite que ambos interlocutores puedan negociar las condiciones de la comunicación.
- El servicio DATA puede ser confirmado o no. Si es no confirmado, sólo llevará las primitivas request e indication.
- El servicio DISCONNECT suele ser no confirmado, aunque a veces hay que asegurar que los dos extremos finalizan la comunicación y así liberan sus recursos reservados.

El siguiente gráfico representa una comunicación entre dos niveles reflejando los servicios y las primitivas que intervienen.



Comunicación entre niveles - T. Fernández Escudero - "Elaboración propia"




Autoevaluación


¿Cuál es la diferencia entre servicios y protocolos?

- ☐ No hay ninguna diferencia.
- ☐ Los servicios se sirven de los protocolos.
- ☐ Los protocolos utilizan los servicios.
- ☐ Los protocolos son los interfaces y los servicios las capas.

4. ENCAPSULAMIENTO DE LA INFORMACION



Caso práctico



CASO: Tomás ya sabe lo que son los protocolos y que protocolo utiliza su ordenador para ser identificado en la red. Como primer experimento ha aprendido a usar el comando ping para verificar la conexión entre dos ordenadores, pero le ha surgido una duda, entre los mensajes que se producen como resultado de esta orden hay uno que dice "paquetes enviados...", ha buscado en Internet información y lejos de aclararse, se ha liado más porque los documentos que ha encontrado hablan de "datos, tramas, paquetes...".

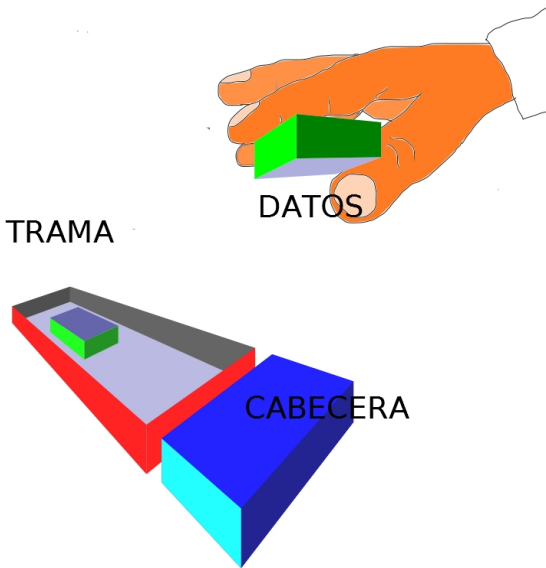
ARQUITECTO TRAMA - T. Fernández Escudero - "Elaboración propia"

Para que los procesos pares puedan comunicarse a un determinado nivel, necesitan información adicional (CABECERA, o información de control, suele ir al principio del mensaje).

Una arquitectura de seis capas añade 5 cabeceras de control para la transmisión. La última capa no suele añadir información adicional ya que se encarga de enviar los dígitos binarios por el cable.

DATOS + CONTROL = TRAMA

Se habla de TRAMA cuando nos referimos al formato y de PAQUETE cuando consideramos los datos. Se dice que los paquetes viajan o se insertan sobre las tramas.



Encapsulamiento de la información - T. Fernández Escudero - "Elaboración propia"

Una trama es la primera estructura en la que se convierten los "1" y "0". Es el primer agrupamiento de información.

A cada nivel se utiliza un "vehículo" diferente para transportar la información, los datos van encapsulados dentro de la trama correspondiente a dicho nivel.

Cada nivel que se atraviesa necesita de una cabecera diferente para que los datos puedan ser transferidos con seguridad y cuando se reciben se van deshaciendo de las cabeceras hasta que llegan al nivel adecuado en el receptor.

Cuando un usuario quiere enviar información a otro usuario (por ejemplo un documento de texto), primero utiliza el nivel más externo de la arquitectura donde se encuentran las aplicaciones que permiten confeccionar dicho documento. Una vez creado, dicho documento debe ir atravesando los diferentes niveles hasta llegar al canal físico de transmisión.

Cada vez que atraviesa uno de estos niveles se le van agregando datos para poder ser reconocido por los otros niveles (cabeceras). A medida que la información se aleja del usuario se vuelve más ininteligible y se va pareciendo cada vez más al "código máquina", todo ello gracias a los diferentes protocolos existentes entre los distintos niveles. El último paso será el convertir la información en niveles de tensión (1 y 0) que viajen por el medio de transmisión.

Cuando los impulsos eléctricos llegan al receptor, sufren el proceso contrario, hasta que el documento se libra de todas las cabeceras y se muestra en el nivel más externo del receptor.

Cada nivel es capaz de reconocer su parte si los protocolos que se utilizan son los adecuados. Se habla de "encapsulamiento" porque los datos a medida que atraviesan niveles se van cubriendo de más datos de control que permiten que viajen a través del sistema.

Dependiendo del nivel de la arquitectura que estemos contemplando, los datos que viajan se denominarán de una u otra manera.

DATOS	APLICACIÓN
-------	------------

DATOS	PRESENTACION
DATOS	SESION
SEGMENTOS	TRANSPORTE
PAQUETES	RED
TRAMAS	ENLACE
BITS	FISICO



Autoevaluación

Trama es un concepto que se refiere a:

- ☐ Las aplicaciones que pueden tener los bits
- ☐ La estructura que tiene el agrupamiento de bits a nivel enlace
- ☐ Los datos que se envían.
- ☐ La capa transporte de datos.

5. EL MODELO OSI



Caso práctico



CASO: Visto que hay diferentes formas de llamar a los datos enviados a la red dependiendo del nivel o capa que se esté considerando, la duda para nuestro personaje está en las características de los modelos OSI y TCP/IP. ¿Qué se estudia en cada capa?

ARQUITECTO MODELOS - T. Fernández Escudero - "Elaboración propia"

El modelo OSI de ISO es un modelo que se creó para poder estandarizar todos los protocolos, contempla siete niveles de estudio en la arquitectura de red. Los siete niveles son los que aparecen en la siguiente tabla:

APLICACION
PRESENTACION
SESION
TRANSPORTE
RED
ENLACE
FISICO

En la década de los años 80 hubo un gran desarrollo en el campo de las redes, pero con cierto desorden puesto que cada uno diseñaba programas y protocolos que muchas veces solamente eran válidos para dispositivos específicos de sus marcas. ISO intentó diseñar un método de estudio basado en el concepto de capa o nivel, servicios y protocolos para poder delimitar con coherencia el papel de cada elemento diseñado para que las redes funcionen.

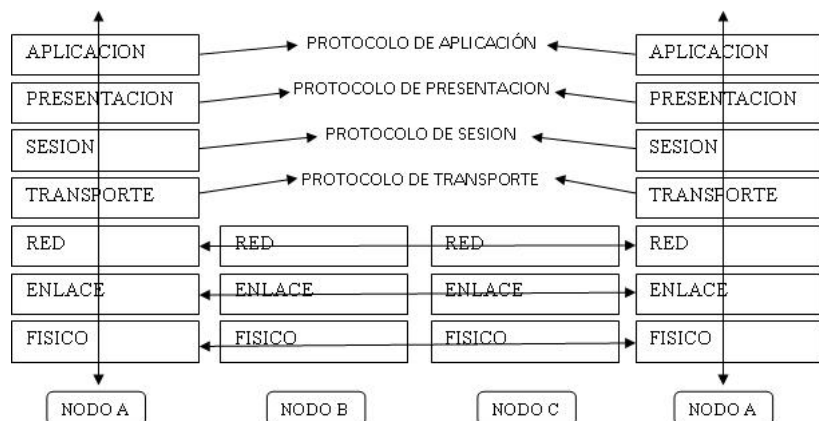
La idea de estandarizar el diseño de las redes hizo que la compatibilidad entre todos los elementos aumentara notablemente y con ello la expansión de las redes de comunicación.

OSI no prosperó como TCP/IP porque cuando se quiso implantar, los protocolos TCP/IP ya eran empleados por la mayoría de los centros de investigación.

OSI es una división más académica que técnica y algunas de las capas que contempla, casi no tienen sentido porque apenas se diferencian entre sí (SESION, PRESENTACION, APLICACION).

El modelo OSI fue un modelo que se creó sobre la teoría y luego se intentó llevar a la práctica; Es, desde el punto de vista académico, muy bueno para estudiar la arquitectura de las redes, aunque menos práctico que el TCP/IP.

La siguiente figura ilustra cómo se lleva a cabo la comunicación entre los diferentes niveles de OSI.



ARQUITECTURA NIVELES - T. Fernández Escudero - "Elaboración propia"

5.1. FISICO

El nivel **FISICO** se encarga de estudiar todo lo relativo al medio de transmisión físico, características técnicas, eléctricas, mecánicas y de composición. En este nivel se definen los estándares que especifican por ejemplo el tipo de cable de debemos utilizar en una determinada red.

5.1.1. ESPECIFICACIONES

-
- Características mecánicas y eléctricas.
- Métodos de transmisión de dígitos binarios por un canal de comunicación.
- Mecanismos que verifiquen que, cuando un lado envíe un "1", se recibe en el otro lado como "1" y no como "0".
- Voltaje que deberá usarse para representar un 1 y un 0.
- Microsegundos que dura un dígito.
- Frecuencia de emisión.
- Puntas que tiene el conector de red y para qué sirve cada una.

5.1.2. OBJETOS DE ESTUDIO EN EL NIVEL FISICO

- Medios de transmisión de señal:
 - Cables de pares
 - Cables coaxiales
 - Fibra óptica
 - Transmisión vía satélite
- Transmisiones y distintas técnicas de modulación.
- Técnicas de multiplexación.
- Técnicas de concentración de canales.
- Técnicas de conmutación:
 - De circuitos.
 - De mensajes.
 - De paquetes.
- Transmisión en serie o en paralelo.
- Transmisión síncrona o asíncrona.
- Normas de conexión en el nivel físico.

5.1.3. FUNCIONES DEL NIVEL FISICO

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados, coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar las señales eléctricas/electromagnéticas.
- Especificar cables, conectores y componentes de interfaz con el medio de transmisión.
- Garantizar la conexión (aunque no la fiabilidad de ésta).

5.2. ENLACE

Se encarga de describir como los niveles superiores utilizan el medio físico para transmitir o recibir información, es el más complicado de comprender puesto que tiene difícil acceso para el usuario. Se estudian protocolos de "acceso al medio" como pueden ser el CSMA/CD.

5.2.1. FUNCIONES

Para conseguir que la comunicación de datos a través de un medio físico se produzca correctamente, se necesita controlar el intercambio de datos. Este control se lleva a cabo por una capa que se coloca por encima del nivel físico y que se denomina nivel de enlace.

El nivel enlace se encarga de controlar los datos del nivel físico y además proporcionar datos fiables al nivel inmediatamente superior (nivel red).

Para que los datos se transmitan correctamente por el enlace, además de un medio físico adecuado son necesarios:

- Sincronización a nivel de trama.
- Control de flujo: La estación emisora y al receptora deben ponerse de acuerdo en el ritmo de transmisión de datos.
- Control de errores.
- Direccionamiento: Si existe más de un posible destino de un mensaje es necesario identificarlo perfectamente.

El nivel enlace se encarga de la creación y el envío de tramas. En la capa física el envío de información se hace en forma de bits; la capa de enlace actúa de manera distinta, construye con los bits paquetes discretos denominados tramas (frames) que son los que envían por la línea. Según el tipo de red la trama puede variar en tamaño. La utilización de las tramas permite simplificar el proceso de detección de errores así como mejorar la capacidad de transmisión del medio mejorando su compartición.

5.2.2. CONTROL DE FLUJO

Otro mecanismo de este nivel es el control de flujo, una técnica que posibilita que el emisor no sature con demasiada información al receptor. El receptor establece una zona de almacenamiento temporal donde va acumulando la información que recibe. El receptor utiliza esta zona para manipular la información y proporcionar los datos correctos al nivel de red (control de errores y ordenación de tramas).

Si no existiese el control de flujo, esta memoria se podría desbordar y se podría llegar a perder información creando colapsos en la red.

5.2.3. DETECCION Y CORRECCION DE ERRORES

En este nivel es donde aparece por primera vez un intento de verificar que la información se transmita correctamente. Se trata de implantar sistemas de detección y/o corrección de errores a nivel binario.

5.2.4. MECANISMOS DE CONTROL DEL CANAL

Las redes locales suelen utilizar la tecnología de difusión (broadcast); en las redes de difusión el canal es compartido por todos los ordenadores de la red. Normalmente, cada mensaje transmitido tiene un único destinatario, cuya dirección aparece en el mensaje, pero para saber si el mensaje es para él, cada ordenador de la red ha de escuchar cada mensaje, analizar la dirección de destino y comprobar si coincide con la propia, descartándolo en caso contrario. Por esta razón, se debe tener un mecanismo que permita a cada ordenador utilizar el canal durante un determinado tiempo para poder enviar la trama a la red. Los protocolos deberán proporcionar los medios para que no haya pérdida de datos ni conflictos.

Debido al problema del reparto del canal en el acceso al medio, en las redes de difusión, la capa de enlace adquiere una configuración más compleja que en las redes punto a punto. Esta es la razón por la cual, para su estudio e implementación, se la suele dividir en dos subcapas:

- MAC: Control de Acceso al Medio (Media Access Control). Controla el acceso al medio de transmisión.
- LLC: Control de Enlace Lógico (Logical Link Control), más superficial que la MAC.

Los protocolos diseñados para gobernar el reparto de canal tienen su origen en los protocolos aloha simple y aloha ranurado.

En 1970, un equipo de la Universidad de Hawai (Norman Abramson) quería conectar terminales de ordenador ubicados en distintas islas del archipiélago con un ordenador situado en Honolulu. El canal que partía de Honolulu no tenía ningún problema pues el emisor era único. Sin embargo el canal de retorno era compartido por varios emisores, por lo que había que establecer algún mecanismo que permitiera solucionar los conflictos que se producirían cuando dos emisores transmitieran simultáneamente (colisión).

La solución fue simple, los emisores transmitían sin esperar a que el canal estuviera libre. Esperaban la confirmación de llegada del mensaje, si no llegaba, suponían que había habido una colisión y volvían a enviar la trama.

Esta técnica se denominó ALOHA (saludo en hawaiano), y fue el primer protocolo de acceso al medio (MAC) que se inventó.

En 1972 fue propuesta una mejora consistente en establecer de antemano unos intervalos de tiempo de duración constante para la emisión de las tramas. De este modo las estaciones estarían sincronizadas y todas sabrían cuando empieza cada intervalo, con lo que disminuiría la probabilidad de colisión. A esta versión se la denominó ALOHA ranurado, en contraste con el anterior método conocido como ALOHA puro.

Hay un conjunto de protocolos, denominados de acceso múltiple con detección de portadora o CSMA (Carrier Sense Multiple Access), que antes de comunicar comprueban si el medio está ocupado. Esta operación permite hacer un uso más eficiente del canal y alcanzar mayores niveles de ocupación. El protocolo de este tipo que goza de mayor popularidad es el CSMA/CD (CSMA Collision Detect)

Las estaciones son capaces de detectar una colisión, lo que las hace terminar sus transmisiones inmediatamente. De este modo se ahorra tiempo y ancho de banda. Después de detectar un choque, una estación termina su transmisión, espera un período aleatorio, y trata de emitir nuevamente.

La única circunstancia en la que puede producirse una colisión es cuando dos ordenadores empiezan a transmitir dentro de lo que se conoce como periodo de contienda (diferencia de tiempo entre el inicio de una transmisión y el momento en que esta transmisión habrá sido detectada por todos los equipos de la red). Para un tiempo de propagación de la señal de un extremo a otro de t , el periodo de contienda será de $2t$. Por este motivo, las redes CSMA/CD se suelen modelar como un sistema ALOHA ranurado con intervalos de tamaño $2t$.

Los protocolos CSMA son probabilísticos (no determinísticos) ya que la posibilidad de colisiones impide conocer cuánto tiempo puede transcurrir hasta que una estación pueda enviar una trama.

Es en este nivel donde mayor contenido presentan los protocolos al ser el desarrollado desde más antiguo. Estudiaremos los protocolos de enlace síncrono de los cuales existen dos tipos, orientados a carácter y orientados a bit.

5.2.5. PROTOCOLOS ORIENTADOS A CARACTER

Los protocolos orientados a carácter basados en código son un tipo de protocolos utilizados en entornos síncronos y en los que la trama consta de un número entero de caracteres pertenecientes al alfabeto de un código determinado. Para efectuar el control de enlace se utilizan algunos de los caracteres del código.

Como ejemplos tenemos el BSC de IBM, el DCMP de Digital o el mismo ASCII, de éste último vamos a ver algunos códigos de control:

- SOH (Start Of Header): Comienzo de secuencia cabecera de mensaje.
- STX/ETX (Start/End of Text): Comienzo y fin de texto.
- EOT (End Of Transmission): Para marcar el final de una comunicación.
- SYN (Synchronous Idle): Dos o más se utilizan como sincronización de comienzo de bloque, es la secuencia 0010110.
- ACK (Affirmative Acknowledgment): Reconocimiento o acuse de recibo positivo.
- NAK (Negative Acknowledgment): Reconocimiento o acuse de recibo negativo.
- DEL (Data Link Escape): Es el carácter que se utiliza para cambiar el significado de los caracteres de control que le siguen.

Una trama básica de un protocolo orientado a carácter tiene el aspecto siguiente:

SYN	SYN	STX	MENSAJE	ETX
"Sincronizando"	"Sincronizando"	"Comienzo mensaje"	"Mensaje"	"Fin de mensaje"

Cada una de las acciones se realizan ("texto entre comillas") viene descrita por una serie de caracteres.

En este tipo de protocolos, el formato de trama es variable. Existen tramas de control y de datos.

5.2.6. PROTOCOLOS ORIENTADOS A BIT

Los protocolos basados en carácter son poco flexibles pues obligan a usar el código en que se basan (ASCII, EBCDIC...). Por este motivo aparecieron los protocolos no basados en código que, además, suelen trabajar a nivel de bit, es decir, en ellos la trama consta de un número variable de bits organizados en un conjunto fijo de campos.

Como ejemplos de protocolos de este tipo están:

- HDLC (High Level Data Link Control). Familia de protocolos definida por la ISO a partir de SDLC (Synchronous Data Link Control).
- LAPB (Link Access Procedure Balanced). Subconjunto de HDLC adoptado por el ITU-T para el nivel de enlace de la norma X.25.
- LAPD (Link Access Procedure D-channel). Subconjunto de HDLC creado para RDSI por ITU-T. Frame Relay también utiliza una variante de LAPD.

A diferencia de los protocolos orientados a carácter, éstos utilizan una trama monoformato lo suficientemente flexible para dar servicio a todos los tipos de transmisión.

Para cubrir todas posibles necesidades de comunicación que surjan, HDLC define:

- Tres tipos de estaciones.
 - Estación primaria: Controla el funcionamiento del enlace. Sus tramas se denominan órdenes.
 - Estación secundaria: Funcionan bajo las órdenes de las estaciones primarias. Las tramas se denominan respuestas.
 - Estación combinada.
- Dos configuraciones de enlace.
 - No balanceada: Una estación primaria y una o varias secundarias con transmisión semidúplex o dúplex.
 - Balanceada: Dos estaciones combinadas con transmisión semidúplex o dúplex.
- Tres modos de operación.
 - NRM (Normal Response Mode): Usado en configuración no balanceada. Sólo la estación primaria puede iniciar una transmisión de datos limitándose la secundaria a responder a las órdenes de aquella. NRM se utiliza en las líneas de múltiples conexiones y, en general, cuando varios terminales se conectan a un ordenador central.
 - ARM (Asynchronous Response Mode): Se utiliza en configuración no balanceada permitiendo a la estación secundaria iniciar un proceso de transmisión. La estación primaria sigue siendo la responsable de la supervisión del sistema.
 - ABM (Asynchronous Balanced Mode): Se utiliza en la configuración balanceada. Permite que cualquier estación combinada inicie la transferencia de datos. ABM es el modo más utilizado. Usado en las redes LAN que usan tramas derivadas de HDLC. Aquí la responsabilidad del control de acceso al medio se retira de cualquier hipotética estación primaria (no existen) y se transfiere a los protocolos de control de acceso al medio (MAC).

Una trama HDLC tiene la forma siguiente:

INDICADOR	DIRECCION	CONTROL	DATOS	SCT	INDICADOR
01111110	8 bits	8 bits	N bits	16 bits	01111110

Donde:

- Tipo 0: RECEIVE READY (ACK).
- Tipo 1: REJECT (NAK).
- Tipo 2: RECEIVE NOT READY. Indica un acuse de recibo pero solicita suspensión del envío para evitar saturar al receptor (control de flujo), cosa que puede ser necesaria si el receptor tiene saturadas sus memorias temporales. Para que la retransmisión se reanude debe ser enviado un Tipo 0, Tipo 1 o ciertas tramas de control.
- Tipo 3: SELECTIVE REJECT. Se utiliza para solicitar retransmisión de una trama determinada cuando se emplea retransmisión selectiva.



Autoevaluación

La dirección física o dirección MAC es una dirección que:

- ☐ Se estudia a nivel de red.
- ☐ Está formada por 4 números.
- ☐ Se estudia a nivel enlace de datos.
- ☐ Se expresa en código octal.

5.3. RED

El nivel de red es el encargado de identificar a cada uno de los nodos que forman parte de la red. En este nivel se describen todas las herramientas necesarias para poder identificar de manera única a cada uno de los nodos. En él se habla de direcciones de red.

El objetivo principal en este nivel es poder encaminar los paquetes desde el origen hasta el destino.

La gran decisión en el nivel de red es si el servicio debiera ser no orientado a la conexión u orientado a la conexión.

- Datagramas.
- Circuitos virtuales.

Ejemplos de ambos enfoques son Internet (no orientado a la conexión) y ATM (orientado a la conexión). Cuando los servicios son "no orientados" a la conexión, el nivel de red solamente garantiza que han llegado todos los datos, pero no garantiza que lleguen en el orden correcto. Cada datagrama (parte del mensaje) debe escoger su camino en cada nodo encaminador sin importarle la ruta que ha tomado otro datagrama que forma parte de un mismo paquete.

En cada nodo encaminador (router) debe existir una tabla que indique las posibles rutas que tienen que tomar los datagramas (tablas de enrutamiento).

En tecnologías que ofrecen servicios "orientados" a la conexión, primero se establece la ruta de la comunicación (circuito virtual) y después se emite. Esto permite que el emisor y el receptor se conozcan a la perfección antes de emitir y puedan negociar los parámetros de la transmisión (control de la congestión). Aquí, el orden de entrega está garantizado y por lo tanto también una "calidad en el servicio" (QoS).

Los servicios del nivel de red fueron diseñados para cumplir los siguientes objetivos:

- Independencia de la tecnología empleada por debajo del nivel de red. Sea cual sea la tecnología empleada en los niveles inferiores, a nivel de red se deben entender los nodos entre sí.
- El nivel de transporte no tiene por qué preocuparse de las características de las subredes. A nivel superior al de red tampoco nos debe importar lo que haya por debajo.
- Las direcciones de red disponibles para el nivel de transporte han de usar un sistema uniforme. Las direcciones que se asignen a los nodos deberán seguir unos estándares que posibiliten un manejo óptimo de ellas, para poder encaminar bien los paquetes.

Uno de los protocolos más usados a nivel de red en el modelo OSI es NetBEUI, aunque este protocolo no funciona con los routers y es válido solamente en redes pequeñas (LAN), además debe actuar junto al protocolo NetBIOS.

5.3.1. CONTROL DE ENCAMINAMIENTO

El encaminamiento es el proceso mediante el cual tratamos de encontrar un camino entre dos puntos de la red: origen y destino. El objetivo consiste en tratar de encontrar la mejor ruta en la red o la ruta que tenga una métrica que más nos favorezca.

Posibles métricas son:

- Número de saltos necesarios para ir de un nodo a otro.
- Retardo de tránsito entre nodos vecinos.
- Coste económico que supone enviar un paquete de nodo a nodo.

El problema de encaminamiento diferirá según la subred sea en modo datagrama o en modo circuito virtual. En las primeras, el encaminamiento puede variar para cada paquete transmitido mientras que en las CV el encaminamiento se decide por sesión y no se cambia a menos que sea imprescindible.

El camino óptimo también dependerá del instante en que se observa la red. Los protocolos serán los encargados de ocultar la red a sus usuarios y comprobar que las condiciones impuestas se verifican siempre. Por esta razón, el encaminamiento debe proveer a la red de mecanismos para que ésta sepa reaccionar ante variaciones del tráfico (evitar la congestión) o de topología (altas y bajas de nodos, ruptura de enlaces) y, en su caso, contribuir al mantenimiento de la [QoS](#).

5.3.2. ALGORITMOS DE CONTROL DE ENCAMINAMIENTO

Para encontrar la mejor ruta entre dos puntos de la comunicación, hay que emplear técnicas y métodos que denominamos algoritmos, los principales tipos son:

- Encaminamiento salto a salto.
- Encaminamiento en origen.

Si consideramos la posibilidad de que el algoritmo reconozca en cada momento la situación de la red y pueda variar su comportamiento, la clasificación sería:

- Algoritmos adaptativos.
 - De ruta más corta (DIKJSTRA, FLOYD-WARSHALL, BELLMAN-FORD).
 - De aprendizaje hacia atrás.
 - Centralizados.
 - Distribuidos.

§ Basados en el "vector distancia" (ARPANET).

§ Basados en el estado del enlace (OSPF).

- Algoritmos no adaptativos.
 - Estáticos.
 - Inundación.
 - Cuasiestáticos.

Para que todos estos algoritmos puedan llevarse a cabo, es necesario que cada nodo encaminador de la red posea una estructura con los siguientes elementos:

- Entorno local: Información de lo que el nodo ve (memoria disponible, enlaces locales, etc.).
- FIB (Forward Information Base): Tabla de encaminamiento que se consulta para hacer el reenvío de los PDU.
- R-PDU (Routing-PDU): Paquete de control remitido por otro nodo. Contiene información de tipo variado sobre la red (nodo sigue activo, distancias a otros nodos).
- RIB (Routing Information Base): Es la base de información de encaminamiento que se consulta para decidir y formar la FIB. El nodo va acumulando en la RIB la información que obtiene a partir de la observación del entorno local y mediante la recepción de R-PDUs. A su vez, con la información almacenada en la RIB, el nodo envía R-PDUs para informar de su conocimiento del estado de la red a los demás nodos.

Es decir, cada nodo encaminador debe examinar en cada momento la situación que le rodea y en base a ello tomar una decisión de la ruta óptima.

5.3.3. CONTROL DE LA CONGESTION

La congestión se produce cuando en alguna parte de la red se da una situación en la que es imposible enviar todo lo que se se recibe.

Existen varias situaciones potencialmente generadoras de congestión:

- Nodos con capacidad de proceso insuficiente.
- Velocidad insuficiente de las líneas.
- Memoria [buffer](#) insuficiente en los conmutadores.

Es distinto el control de flujo (nivel enlace) que el control de la congestión. El control de congestión es un concepto más amplio que el control de flujo. Comprende todo un conjunto de técnicas para detectar y corregir los problemas que surgen cuando no todo el tráfico ofrecido a una red puede ser cursado. Es un concepto global que involucra a toda la red, y no sólo a un remitente y un destinatario de información, como es el caso del control de flujo. El control de flujo es una de las técnicas para combatir la congestión.

5.3.4. ALGORITMOS DE CONTROL DE LA CONGESTION

Existen varios algoritmos que ayudan a reducir la congestión, las dos técnicas principales se basan en vigilar el tráfico e intentar reconducirlo y controlarlo para que no se sature ningún nodo o directamente, descartar aquellos paquetes que saturan el sistema (más radical).

La clasificación sería la siguiente:

- Conformación y vigilancia del tráfico.
 - Algoritmo del cubo agujereado.
 - Algoritmo del cubo con cupones.
 - Control de subredes virtuales.
 - Paquetes reguladores.
- Descarte de paquetes.

5.4. TRANSPORTE

El objetivo principal de este nivel es proporcionar un transporte de datos confiable de la máquina origen a la máquina destino, independientemente del medio físico utilizado; se pretende que para establecer una sesión de comunicación a este nivel no debe importarnos nada más que la dirección origen y la dirección destino.

A nivel de red, los usuarios de a pie no tienen control sobre el funcionamiento del servicio ya que toda la gestión se lleva en los puntos de conexión y enrutamiento, por lo que el nivel transporte pretende añadir mejoras que resuelvan posibles problemas en el servicio. Todo el software a nivel de transporte se ejecuta en las máquinas de los usuarios.

Este nivel es el límite entre el proveedor de servicios y el usuario, en el se habla de términos como **puertos** y **sockets**.

Cuando un proceso de aplicación quiere establecer comunicación con otro proceso de aplicación remoto, debe especificar a cuál se conectará. El método que normalmente se emplea es el de definir direcciones de transporte en las que los procesos pueden estar a la escucha de solicitudes de conexión. Estos puntos terminales se llaman PUERTOS (En ATM se llaman AAL-SAPs). También se pueden denominar TSAP (Punto de Acceso al Servicio de Transporte).

Para el caso del nivel de red, NSAP (Punto de Acceso al Servicio de Red) es lo mismo que decir dirección IP.

A veces los servicios tienen TSAP estables que se listan en archivos en lugares bien conocidos (etc/services de Unix que lista cuáles servidores están enlazados de manera permanente a cuáles puertos).

No es rentable tener TSAP estables porque puede haber puertos que se utilicen muy pocas veces, lo ideal sería que todas las aplicaciones pudieran usar todos los puertos posibles. Por otra parte, hay determinadas aplicaciones que necesitan tener un puerto identificado con un número que no varíe (puertos bien conocidos).

En lugar de que cada servidor concebible escuche en un TSAP bien conocido, cada máquina que desee ofrecer servicio a usuarios remotos tiene un SERVIDOR DE PROCESOS especial que actúa como proxy de los servidores de menos uso.

Este servidor escucha en un grupo de puertos al mismo tiempo, esperando una solicitud de conexión.

Los usuarios potenciales de un servicio comienzan por emitir una solicitud CONNECT, especificando la dirección TSAP del servicio que desean. Si no hay ningún servidor esperándolos, consiguen una conexión al servidor de procesos. El servidor de procesos les asigna un TSAP y vuelve a la escucha.

5.5. SESION

El nivel sesión es el encargado de controlar la comunicación entre las aplicaciones, se dice que controla el diálogo entre aplicaciones de diferentes máquinas para que el transporte de datos sea óptimo. A este nivel se intercambian "datos".

A nivel sesión se establecen comunicaciones proceso a proceso en red entre los distintos hosts. Para que haya comunicación entre dos host de la red es necesario que se establezca una "sesión" entre ellos, antes de empezar a transmitir.

La capa sesión es un concepto que aparece por primera vez con OSI. La capa sesión tiene como misión permitir a sus usuarios (que pueden ser entidades de la capa de presentación o de la capa de aplicación) establecer conexiones, denominadas sesiones, para la transferencia de datos ordenada. Por ejemplo, una sesión podría utilizarse para un acceso desde un ordenador personal a una base de datos remota.

Usualmente, cuando se solicita que la capa de sesión establezca una sesión, con carácter previo se deberá haber establecido una conexión de transporte sobre la que fluirá la sesión. Esta conexión de transporte puede ser monosesión o utilizarse consecutivamente, para más de una sesión.

5.5.1. FUNCIONES

Sus funciones son bastante reducidas consistiendo fundamentalmente en permitir la transferencia de datos, controlar el orden de intervención de los interlocutores en ciertos diálogos (provocar un funcionamiento consulta-respuesta en los accesos a una base de datos), facilitar la vuelta a un estado anterior tras un problema (sincronizar un proceso) y en resumen permitir al usuario el establecimiento de sesiones de comunicación en las cuales puede transmitir datos a través del sistema.

- Actuar de interfaz entre el usuario y la red, gestionando el establecimiento de la conexión entre procesos de hosts remotos.
- Negociar la forma en que se intercambian los datos dos equipos remotos.
- Identificar los usuarios de los host remotos.
- Restablecer las comunicaciones rotas a nivel transporte.

5.6. PRESENTACION

Este nivel es el responsable de codificar los datos para que la comunicación entre los host sea homogénea. Recibe los datos de la capa aplicación en forma de texto, imagen, sonido, instrucción y los transforma para poder generar datos con estructuras similares que se puedan transformar mejor. Por ejemplo, cuando hacemos una mudanza, se pueden transportar mejor las cosas si van metidas en cajas de tamaño homogéneo (se pueden colocar mejor en el medio de transporte) que si las llevamos sueltas, se aprovecha mejor el espacio, se optimiza el medio de transporte y su manejo es más fácil.

Entre los códigos que nos podemos encontrar en este nivel se encuentran EBCDIC, ASCII y UNICODE. A este nivel también aparecen los mecanismos de seguridad y encriptación (firma electrónica) de datos.

Dos tareas complementarias de este proceso de traducción son la compresión y el cifrado de los datos. Con ellos se pretende, por un lado, eliminar de los mensajes por transmitir aquellos componentes superfluos que luego pueden ser añadidos directamente en el extremo receptor y, por otro, enmascarar la información transmitida de modo que un hipotético escucha del sistema de comunicación no pueda recuperar el mensaje original sin conocer el código de descifrado.

No hay ningún impedimento a la existencia de un cifrado de nivel de presentación por un lado, y de un cifrado de nivel aplicación por otro.

5.7. APLICACION

La capa aplicación contiene los programas de usuario (aplicaciones) que hacen el trabajo real para el que fueron adquiridos los ordenadores. Esta capa es la que hace de nuestro ordenador un aparato útil para nosotros (crear textos, chatear, leer correo, visitar webs).

Es el que entra en contacto con los usuarios finales. Tiene la particularidad de que incluye cualquier función o servicio que se use en la red y que no se suministre en los niveles anteriores. Es posible escribir un libro con miles de páginas con la multitud de cosas útiles que hace el nivel de aplicación.

5.7.1. FUNCIONES

Entre los cometidos más importantes de este nivel figuran:

- **Compresión de la información transmitida.**

El coste de utilización de una red de comunicaciones suele ser fuertemente dependiente, en sentido directamente proporcional, de la cantidad de datos transmitidos. Así pues, una forma de reducir dicho coste sería conseguir que la información que se envía por la red ocupase el menor volumen posible. Para ello y manteniendo constantes el resto de parámetros, no hay nada mejor que utilizar las técnicas de compresión.

La compresión de la información se utiliza intensivamente para ahorrar recursos, sean estos, espacio de memoria secundaria, o ancho de banda en comunicaciones. Esta técnica requiere dos algoritmos paralelos pero no necesariamente simétricos, el de compresión y el de descompresión. Respecto a ellos es importante diferenciar entre compresión de datos y compresión multimedia.

En la compresión de datos se exige que lo que se comprimió, sea exactamente lo que se descomprime (sin pérdidas).

En la compresión multimedia no suele ser necesario que al descomprimir se obtenga una imagen perfecta de lo que se codificó (con pérdidas). Se admite una degradación que hace que el proceso sea más rápido.

Ejemplo de compresión de datos es el formato conocido como **mp3**.

- **Seguridad y confidencialidad.**

La seguridad no era algo que preocupara excesivamente a los primeros usuarios de las redes de comunicaciones, usando éstas para poco más que enviarse correo electrónico y compartir alguna impresora dentro de una universidad u organización cerrada, pocos problemas de este tipo podían producirse.

Hoy en día, el panorama ha cambiado, las organizaciones que desean utilizar el correo electrónico y los demás servicios de Internet, bien internamente, bien para relacionarse con el exterior, deben tomar medidas que permitan garantizar la confidencialidad, la integridad y la disponibilidad de la información.

Existen cuatro conceptos básicos en seguridad que son:

o Control de integridad: ausencia de modificación o destrucción no autorizadas de la información.

o Disponibilidad/no repudio: consiste en impedir la denegación no autorizada de acceso a la información.

o Secreto/confidencialidad: supone evitar la divulgación no autorizada de la información.

o Validación de identificación/autenticación: busca la seguridad en el proceso de dar y reconocer la autenticidad de la información y/o la identidad de los actores y/o el permiso por parte de los autorizadores.

Es en este apartado donde se deben abordar los temas relacionados con la criptología, que se divide en dos ciencias antagonistas: la criptografía y el criptoanálisis. Estas ciencias son las encargadas de diseñar todas las técnicas utilizadas para encriptar los datos enviados de un usuario a otro a través de la red.

- **Gestión de red: SNMP.**

El objetivo genérico de un sistema de gestión de red es proporcionar una plataforma de gestión distribuida para todo tipo de entornos de red.

El estándar de gestión más utilizado actualmente es el denominado SNMP, que incluye un protocolo de gestión (RFC 1157), una especificación de estructura de base de datos de información de gestión (MIB) y un conjunto de definiciones de objetos de datos permitidos (RFC 1155). La versión SNMP v2, soporta TCP/IP y OSI. SNMP no proporciona gestión de red sino un marco de trabajo sobre el que se pueden construir aplicaciones de gestión de red.

- **Gestión y conversión de nombres de dominio: DNS.**

Conjunto de protocolos y servicios sobre una red TCP/IP, que permite a sus usuarios utilizar nombres jerárquicos sencillos, en lugar de sus direcciones IP, para comunicarse con otros equipos.

Si no existiera la funcionalidad DNS, tendríamos que sabernos cada una de las direcciones únicas de cada elemento de la red, para poder visualizar la página www.openoffice.org tendríamos que poner en el explorador <http://204.16.104.2>. Sería imposible recordar todas y cada una de las direcciones de todos los portales que quisiéramos visitar.

Antes de la implantación de DNS, la traducción de direcciones IP a nombres de computadoras se efectuaba mediante listas de nombres y sus direcciones IP asociadas, almacenados en archivos hosts.txt.

Estos archivos contenían el nombre y la dirección asociada a ese nombre, de manera que cuando yo quiero conectarme con un host no necesito recordar su dirección, recorro al fichero y en es fichero busco la dirección que corresponde a ese nombre; es más fácil recordar un nombre que 4 números.

DNS está compuesto de una base de datos distribuida de nombres que se organiza según una estructura lógica arborescente conocida como espacio de nombres de dominio.

- Cada nodo o dominio en el DNS tiene un nombre y puede, a su vez, contener subdominios.
- Los dominios y subdominios se agrupan en zonas que permiten la administración distribuida del espacio de nombres.
- Cada dominio se nombra por la trayectoria desde él hasta la raíz (que no tiene nombre) separando cada nivel jerárquico con un punto.
- La raíz de la base de datos de DNS en Internet es administrada por el InterNIC. Los nombres de dominios siguen el estándar internacional ISO 3166.

Cuando un usuario desea crear un portal y asignarle un determinado nombre, por ejemplo hola.adios, debe "pedir permiso" a InterNIC para saber si ese nombre está o no permitido y disponible. Hay muchas empresas que se dedican a proporcionar el servicio de alojamiento ("hosting") a cambio de dinero, pero también hay posibilidad de tener un nombre en Internet de manera gratuita (www.gratisweb.com).

Esta mecánica de asignar nombres para poder identificar ciertos host en Internet hizo que en su día, usuarios demasiado avispados registraran nombres asociados a marcas de bebidas, ropa o aparatos electrónicos impidiendo que esas compañías pudieran utilizarlos, provocando que tuvieran que desembolsar grandes cantidades de dinero para poder utilizar los nombres asociados a sus marcas.



Para saber más

Si quieres saber más sobre **mp3**

6. EL MODELO TCP/IP

El modelo TCP/IP contempla cinco niveles y debe su nombre a los dos protocolos más importantes que estudia. Los niveles son:

APLICACION
TRANSPORTE
INTERNET
SUBRED

Este modelo es uno de los artífices del éxito de Internet como red global. Al contrario que OSI, los diseñadores de TCP/IP fueron creando aplicaciones, programas, estándares, protocolos, etc..., que funcionaban y después las trataban de englobar en un determinado nivel, es por ello que hay niveles que contienen cosas que no tienen demasiados puntos en común. Por ejemplo, mientras en el modelo OSI existen tres capas (SESION, PRESENTACION, APLICACIÓN) para tratar de describir todo lo que está más cerca del usuario, en el TCP/IP solamente se utiliza una (APLICACIÓN).

La diferencia con OSI, es que OSI siempre ha sido más académico pero menos práctico. TCP/IP desde el principio trabajó con estándares que funcionaban correctamente y después trataban de darles un enfoque más académico.

6.1. SUBRED

En el nivel subred se estudia todo lo relativo a los parámetros físicos de la red, lo que en el modelo OSI engloba en el nivel FÍSICO. Se estudiarán todas las características físicas de los medios de transmisión.

Como quiera que el modelo TCP/IP no contempla un nivel intermedio que le separe del nivel Internet, en este nivel se estudiarán los protocolos de acceso al medio entre otros que el modelo OSI trata en el nivel enlace.

Lo más cercano a un protocolo de nivel enlace en TCP/IP es el protocolo de subred. Consiste en dos capas (IMP). Su objetivo consiste en proporcionar una capa fiable para la transmisión de tramas de un IMP a sus vecinos inmediatos.

Un caso particular de nivel enlace en Internet es el que atañe al transporte de tramas IP sobre líneas serie. Su importancia es cada vez mayor ya que se aplica a las conexiones temporales de Internet entre PC de usuarios y los proveedores de servicios de Internet.

Los dos protocolos más característicos son SLIP y PPP.

SLIP - SERIAL LINE IP

Este es el más antiguo de los protocolos y data de 1984. Se trata de un protocolo muy sencillo que utiliza un carácter como indicador, y caracteres de relleno en caso de que dicho carácter aparezca en la trama. Solo se utiliza en comunicaciones conmutadas.

SLIP no es capaz de detectar tramas erróneas. Su uso ha decaído a favor de PPP.

PPP (POINT TO POINT PROTOCOL)

PPP se ha diseñado para ser muy flexible, para lo cual incluye un protocolo especial, denominado LCP (Link Control Protocol), que se ocupa de negociar (handshaking) una serie de parámetros en el momento de establecer la conexión con el sistema remoto.

La estructura de la trama PPP se basa en la de HDLC, aunque se trata de un protocolo orientado a carácter. La trama tiene la siguiente estructura:

Indicador	Dirección	Control	Protocolo	Datos	SCT	Indicador
01111110	11111111	00000011	Protocolo	Variable	CRC	01111110

El campo dirección no se utiliza, siempre vale todo 1. Ello se debe a que las conexiones son siempre punto a punto y, por lo tanto, no tiene sentido utilizar dirección alguna.

El campo control contiene siempre el valor 00000011, que indica una trama no numerada. Por defecto PPP no suministra transmisión fiable (con números de secuencia y acuse de recibo como HDLC).

LCP negocia siempre la supresión de los bytes dirección y control de la trama al inicio de la sesión cuando no se pide transmisión fiable.

El campo protocolo establece a que tipo de protocolo pertenece el paquete recibido de la capa de red. PPP permite establecer una comunicación multiprotocolo, puede utilizarse para transmitir paquetes pertenecientes a diferentes protocolos del nivel de red entre dos ordenadores.

LCP también suministra mecanismos que permiten validar al ordenador que llama (claves usuario/password).

PPP es un mecanismo de transporte de tramas multiprotocolo que puede utilizarse sobre medios físicos muy diversos, por ejemplo, conexiones módem y RTC, RDSI, líneas dedicadas, o incluso por conexiones SONET/SDH de alta velocidad.

6.2. INTERNET

El nivel de red en el modelo TCP/IP está determinado por las características del protocolo IP, definido en un documento público RFC 791.

6.2.1. FORMATO DE TRAMA

Toda la información en una red IP ha de viajar en datagramas IP.

El tamaño máximo de un datagrama IP es de 65535 bytes, a repartir entre encabezado y texto. Se trata de un valor teórico que no se utiliza en la práctica. Normalmente, el nivel de red adapta el tamaño de cada paquete para que viaje en una trama de enlace de la red utilizada.

Una trama IP tiene el siguiente aspecto:

VERSION	IHL	TIPO SERVICIO			LONGITUD TOTAL
IDENTIFICACION		F	DF	MF	DESPLAZAMIENTO DEL FRAGMENTO
TIEMPO DE VIDA		PROTOCOLO			SUMA VERIFICACION DEL ENCABEZADO
DIRECCION ORIGEN					
DIRECCION DESTINO					
OPCIONES					

- Versión: Ipv4, Ipv6. Permite que coexistan tramas de diferentes versiones.
- IHL: Longitud en palabras de 32 bits del encabezamiento.
- Tipo de servicio.
- Longitud total del datagrama.
- Identificación: Determina a que datagrama pertenece el fragmento. Todos los fragmentos de un datagrama incluyen la misma identificación.
- DF: Orden a todos los routers de que no fragmenten el datagrama, ya que el destino no puede montarlo de nuevo.
- MF: Todos los fragmentos, salvo el último de un datagrama tienen este bit activado.
- Desplazamiento del fragmento: A que parte del datagrama pertenece este fragmento. El tamaño del fragmento elemental es de 8 bytes. Todos los fragmentos excepto el último han de tener un tamaño múltiplo del tamaño elemental.
- Tiempo de vida: Cada vez que llega a un router es minorado. Se utiliza para ir descontando saltos. Cuando llega a cero, el paquete se descarta y se envía al host origen un aviso.
- Protocolo: Protocolo de transporte al que debe entregar el datagrama.
- Suma de comprobación: Aritmética de complemento a 1 para controlar la producción de errores en la cabecera.
- Direcciones origen y destino.
- Opciones: Incluyen el encaminamiento en origen estricto, el encaminamiento libre desde el origen, la grabación de la ruta, la marca de tiempo y la seguridad.

6.2.2. DIRECCIONES IPv4

La versión más extendida hasta ahora, ha sido IPv4, en la que las direcciones de los nodos tienen la forma 195.235.113.3, cuatro números con valores entre 0 y 255 separados por puntos.

Las direcciones IP que identifican los dispositivos y estaciones de la red tienen un tamaño fijo de 32 bits.

Las direcciones IP pueden ser:

- Públicas (válidas y únicas en Internet).
- Privadas (válidas a nivel local, son únicas a nivel local).
- Estáticas (no cambian con el tiempo).
- Dinámicas (cambian su valor cuando ha pasado un intervalo de tiempo determinado).

Ejemplo:

Convertir la siguiente dirección IP a decimal: 10001111010101100011110101100001

Solución: 143.86.61.97

Con este método se pueden identificar 2^{32} (4.294.967.296) direcciones, aunque no se puedan utilizar todas para identificar equipos.

Una dirección IP consta de los siguientes campos:

IDENTIFICADOR (TIPO) + NUMERO DE RED + NUMERO DE ESTACION

CLASE	IDENTIFICADOR	Nº DE RED	Nº ESTACION
A	0	7 bits	24 bits
B	10	14 bits	16 bits
C	110	21 bits	8 bits
D	1110	28 bits	-
E	11110	27 bits	-

Las direcciones IP se configuran manualmente en las estaciones.

El NIC (Network Information Center/Centro de Información de la Red) es la institución encargada de asignar direcciones de Internet, para impedir duplicados. Esta institución solo asigna la clase de red y el número de red, y cada administrador de red deberá asignar los sufijos de identificador de estación.

CLASE	RANGO	Nº DE REDES	Nº DE ESTACIONES
A	1.0.0.0 - 127.255.255.255	127	16777216
B	128.0.0.0 - 191.255.255.255	16384	65536
C	192.0.0.0 - 223.255.255.255	2097152	256
D	224.0.0.0 - 239.255.255.255	-	-
E	240.0.0.0 - 247.255.255.255	-	-

De las direcciones de la tabla anterior, hay algunas que no se pueden utilizar porque están reservadas para el uso del protocolo.

- 0.0.0.0: Se utiliza cuando se están arrancando las estaciones, hasta la carga del sistema operativo, luego no se usa.
- 127.0.0.1: Para especificar la estación actual, cuando se desea especificar el ordenador local (al igual que podría utilizar la IP asignada).
- Nº estación todo 0: Red actual.
- Nº estación todo 1: Difusión (broadcast). Para enviar mensajes a todas las estaciones dentro de la misma subred (todas las estaciones con el mismo número de red).

No hay que confundir las direcciones de difusión de las subredes (para enviar mensajes a las estaciones de la misma subred) con las direcciones de la clase D, que más bien, se utilizan para agrupar estaciones y enviarlas mensajes de difusión (pueden pertenecer a redes o subredes distintas).

Además de las direcciones reservadas anteriores, se han establecido otros rangos de direcciones IP para ser asignados a redes locales que se conectan a Internet a través de un proxy o mediante un encaminador que sigue un protocolo NAT.

CLASE	RANGO RESERVADO
A	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.0.0
C	192.168.0.0 - 192.168.255.0



Ejercicio resuelto

Convertir la siguiente dirección IP a decimal: 10001111010101100011110101100001
Separamos los dígitos binarios en grupos de 8, empezamos de derecha a izquierda.

10001111010101100011110101100001

Calculamos el equivalente decimal de cada grupo.

01100001 $\rightarrow 0 \cdot 2^7 + 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 97$

00111101 $\rightarrow 0 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 61$

01010110 $\rightarrow 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 86$

10001111 $\rightarrow 1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 143$

Solucion: 143.86.61.97

6.2.3. PROTOCOLOS RELACIONADOS CON IP

Existen una serie de protocolos que están estrechamente relacionados con el protocolo IP, entre otros, los más conocidos son:

- ARP: Es un protocolo capaz de encontrar la dirección física (MAC) si se le proporciona la dirección IP correspondiente.
- RARP: Es capaz de realizar el camino inverso a ARP, encontrar la IP a partir de la dirección física.
- ICMP: Es el responsable de enviar al usuario los errores que proporciona una determinada aplicación sobre el sistema operativo.
- IGMP: Protocolo responsable de los mensajes a los miembros de un grupo en una red de tipo LAN.

6.3. TRANSPORTE

El nivel transporte, tal como se ilustra en la figura que representa la comunicación entre los niveles OSI, es el primer nivel en el que dejamos de preocuparnos por las características de los nodos intermedios entre el emisor y el receptor. El nivel transporte en el modelo TCP/IP viene determinado por las características de los dos protocolos más importantes TCP y UDP.

La capa de transporte añade la noción de puerto para distinguir entre los muchos destinos dentro de un mismo host. No es suficiente con indicar la dirección IP del destino, además hay que especificar la aplicación que recogerá el mensaje. Cada aplicación que esté esperando un mensaje utiliza un número de puerto distinto; más concretamente, la aplicación está a la espera de un mensaje en un puerto determinado (escuchando un puerto).

Pero no sólo se utilizan los puertos para la recepción de mensajes, también para el envío: todos los mensajes que envíe un ordenador debe hacerlo a través de uno de sus puertos.

Cuando se habla de "abrir puertos", a lo que realmente nos referimos es a ejecutar aplicaciones que usan un determinado puerto, con lo que conseguimos tener ese puerto activo y listo para para enviar o recibir datos.

Un puerto es un número de 16 bits, por lo que existen 65536 puertos en cada ordenador. Las aplicaciones utilizan estos puertos para recibir y transmitir mensajes.

Los números de puerto de las aplicaciones cliente son asignados dinámicamente y generalmente son superiores al 1024. Cuando una aplicación cliente quiere comunicarse con un servidor, busca un número de puerto libre y lo utiliza. En cambio, las aplicaciones servidoras utilizan unos números de puerto prefijados: son los llamados puertos well-known ("bien conocidos"). Puertos conocidos son 80 (http), 21 (ftp), 23 (telnet).

Los puertos tienen una memoria intermedia (buffer) situada entre los programas de aplicación y la red. De tal forma que las aplicaciones transmiten la información a los puertos. Aquí se va almacenando hasta que pueda enviarse por la red. Una vez que pueda transmitirse, la información irá llegando al puerto destino donde se irá guardando hasta que la aplicación esté preparada para recibirla.

6.3.1. UDP

Es un protocolo de la capa transporte cuya principal característica es la de que no es orientado a la conexión.

Este protocolo proporciona una comunicación muy sencilla entre las aplicaciones de dos ordenadores. Al igual que el protocolo IP de la capa de red, este protocolo es "no confiable", es decir, los datos pueden llegar dañados. Utiliza a IP para transportar sus mensajes, la trama es parecida a la de IP pero incorpora el puerto origen y el puerto destino. Este protocolo solo sirve para aplicaciones que no necesiten garantías en la comunicación. Esto es muy práctico en aplicaciones en que es más importante la velocidad de transmisión (como comunicación de audio y vídeo: IPTV, VoIP, juegos en línea) o en aplicaciones servidoras sin estado que deben responder pequeñas consultas de un gran número de clientes (como DNS). A diferencia de TCP, UDP permite paquetes de difusión (broadcast y multicast).

Esto es muy práctico en aplicaciones en que es más importante la velocidad de transmisión (comunicación de audio y vídeo, VoIP, juegos en línea) o en aplicaciones servidoras sin estado que deben responder pequeñas consultas de un gran número de clientes (DNS). A diferencia de TCP, UDP permite paquetes de difusión (broadcast y multicast).

6.3.2. TCP

Es un protocolo de la capa transporte cuya principal característica es la de que es orientado a la conexión. Se diseñó precisamente para proporcionar un servicio confiable sobre una red no confiable. Es decir, es necesario establecer una comunicación previa entre emisor y receptor antes de transmitir los datos. Además el uso de este protocolo nos asegura que los datos recibidos son exactamente los datos enviados.

El flujo de datos entre una aplicación y otra viajan por un circuito virtual. Sabemos que los datagramas IP pueden seguir rutas distintas, dependiendo del estado de los encaminadores intermedios, para llegar a un mismo sitio. Esto significa que los datagramas IP que transportan los mensajes siguen rutas diferentes aunque el protocolo TCP logró la ilusión de que existe un único circuito por el que viajan todos los bytes uno detrás de otro.

Para que esta comunicación pueda ser posible es necesario abrir previamente una conexión. Esta conexión garantiza que los todos los datos lleguen correctamente de forma ordenada y sin duplicados.

Cada byte no se envía inmediatamente después de ser generado por la aplicación, sino que se espera a que haya una cierta cantidad de bytes, se agrupan en un segmento y se envía el segmento completo. Para ello son necesarias unas memorias intermedias o buffers.

Cada uno de estos segmentos viaja en el campo de datos de un datagrama IP. Si el segmento es muy grande será necesario fragmentar el datagrama, con la consiguiente pérdida de rendimiento; y si es muy pequeño, se estarán enviando más cabeceras que datos. Por consiguiente, es importante elegir el mayor tamaño de segmento posible que no provoque fragmentación.

La carga útil de IP es de 65515 bytes, el segmento TCP debería tener ese tamaño, pero en la práctica sucede que cada red tiene una unidad máxima de transferencia (**MTU**), en redes Ethernet el tamaño de la carga útil es de 1500 bytes.

El formato de la trama TCP sería de la siguiente forma:

PUERTO TCP ORIGEN		PUERTO TCP DESTINO	
NUMERO DE SECUENCIA			
NUMERO DE ACUSE DE RECIBO			
HLEN	RESERVADO	BITS CODIGO	VENTANA
SUMA DE VERIFICACION		PUNTERO	
OPCIONES		RELLENO	
DATOS			
...			
...			

6.3.3. CONEXIONES

Una conexión está formada por el par **dirección IP + puerto**. No puede haber dos conexiones iguales en un mismo instante pero sin embargo un mismo ordenador si puede tener dos conexiones distintas utilizando un mismo puerto. A estas conexiones se las llama **SOCKET**.

6.4. APLICACION

Este nivel engloba a todos aquellos protocolos que están más cerca del usuario final. Los protocolos pertenecientes a esta capa son los más conocidos por todos los usuarios (http, ftp, smtp, dns).

La diferencia con el nivel aplicación de OSI, es que aquí las capas sesión, presentación y aplicación se funden todas en una. Esto provoca que haya protocolos y servicios que según el modelo TCP/IP se sitúan en al mismo nivel y que tienen pocas cosas en común. Por otra parte, se consigue que no haya niveles que como en el caso del modelo OSI aparezcan casi vacíos.



Autoevaluación

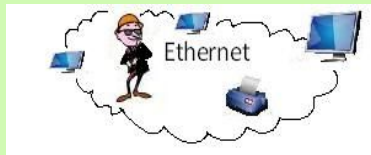
El modelo TCP/IP triunfó sobre el OSI porque:

- ☐ Se implantó antes.
- ☐ Por las IP.
- ☐ Se crearon protocolos que se utilizaban de inmediato.
- ☐ Era más académico.

7. REDES TOKEN RING, FDDI Y ETHERNET



Caso práctico

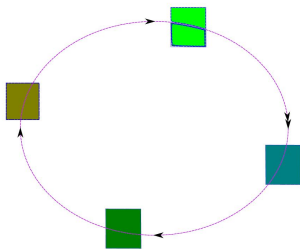


ARQUITECTO ETHERNET - T. Fernández Escudero - "Elaboración propia"

CASO: Nuestro personaje va conociendo más y más cosas sobre su red y a medida que más conoce se da cuenta que son muchas más cosas las que desconoce. Está ahora contemplando los ordenadores, unidos a través de un dispositivo (que el técnico ha llamado router) y de repente se ha preguntado como emiten y reciben datos, que mecanismos utilizan para saber que los datos van dirigidos a uno u otro equipo y como funciona realmente el dispositivo de interconexión. Su cuñado, que sabe de informática, le ha contado que "eso es gracias a que es una red Ethernet" ¿Qué es una red Ethernet?

Estas tres tecnologías son las más utilizadas en redes de tipo LAN. Todas ellas son redes de "enlace directo", en todas ellas, las estaciones comparten un mismo medio para transmitir con lo que aumenta el peligro de colisión en los mensajes transmitidos. Para solucionar esto, todas tienen definido un protocolo de acceso al medio que minimiza la probabilidad de colisiones.

7.1. TOKEN RING



TOKEN RING – T. Fernández Escudero – "Elaboración propia"

Definidas en el estándar IEEE 802.5, las redes de este tipo se presentan con una topología física de tipo estrella y topología lógica tipo anillo. Utilizan un dispositivo de interconexión que se denomina MAU. A simple vista no podremos distinguirlas de las otras redes. El gráfico representa el funcionamiento del dispositivo de interconexión (MAU). Las LAN que utilizan esta tecnología pasan un testigo de un nodo a otro denominado "testigo" o "token".

Esta tecnología la diseñó IBM en los años 70 y fue muy popular en bancos y grandes empresas.

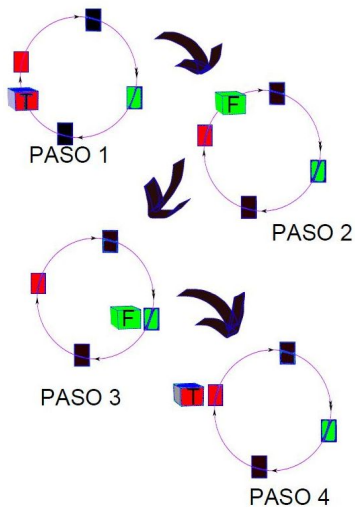
Un token es una secuencia especial de bits que circula por el anillo. Cada nodo recibe y luego despacha el testigo. Solamente puede utilizar el medio de transmisión, aquella estación que posee el testigo, es como "dar la palabra" en un debate entre personas.

Como todas las redes en las que las estaciones comparten un medio de transmisión, en esta existe un protocolo de acceso al medio denominado "Token Passing".

Si nos fijamos en el gráfico, están representados los pasos que se dan desde que una estación (color rojo) quiere enviar datos a otra estación (color verde). En el primer paso, la estación que quiere transmitir, debe capturar un "token" (T) para poder hacer uso del canal.

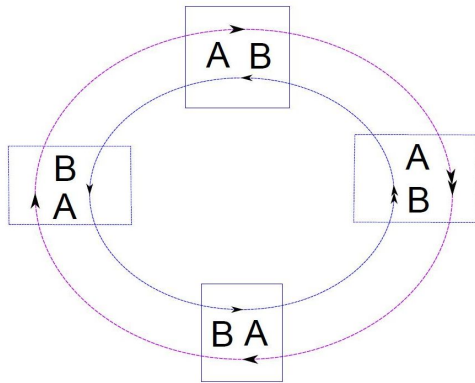
Una vez capturado el "token", en el segundo paso, se envía una trama (F) destinada a la estación verde. El paso 3 es en el que la estación destinataria de los datos recoge la trama de datos.

Cuando se ha producido la comunicación, la trama vuelve a la estación emisora (roja) en el paso 4. Ahora, la estación que inició la comunicación retira de la circulación dicha trama y deja libre el testigo para que pueda usar el canal otra estación de la red.



TOKEN PASSING – T. Fernández Escudero – "Elaboración propia"

7.2. FDDI



FDDI - T. Fernández Escudero - "Elaboración propia"
que la emitió, la hace desaparecer.

Este tipo de red utiliza una arquitectura similar a la TOKEN RING pero con doble anillo, una de ellas en apoyo en caso de que la principal falle. Se utiliza en redes de fibra óptica, aunque acepta líneas de transmisión coaxial y de par trenzado.

La evolución de FDDI ha dado como resultado la tecnología CDDI, esta tecnología ha sido una pieza clave en el desarrollo de Internet porque la alta tasa de transferencia que tiene es imprescindible para el tráfico de vídeo, audio, voz y datos que existe hoy en día.

Cada estación principal, conocidas con el nombre de DUAL ATTACHED STATION (DAS), está conectada a los dos anillos primario (exterior) y secundario (interior). Estas estaciones tienen al menos dos puertos. Uno de los puertos sirve de entrada al anillo primario y salida al secundario y el otro realiza la función inversa, salida para el primario y entrada para el secundario.

La manera de transmitir es similar a las redes Token Ring, hay una señal (token) que indica el derecho a transmitir para una estación. Este token es enviado continuamente de una estación a otra por la red. Cuando una estación tiene algo que enviar, captura el token, envía la información en tramas tipo FDDI y después libera el token.

Las cabeceras de estas tramas contienen la dirección de la estación destinataria, todos los nodos leen la trama cuando pasa por el anillo para poder saber si son los receptores adecuados o no.

Cuando una estación descubre que es la destinataria de esa trama, coge los datos que le interesan y retransmite la trama a la siguiente estación. Cuando se ha completado la vuelta y la trama vuelve a la estación

7.3. ETHERNET

Conocemos a Ethernet como la tecnología que está definida en el estándar IEEE 802.3. Hoy en día es la tecnología que proporciona conectividad en las redes LAN a casi el 98% de los equipos del mundo.

Si bien IEEE 802.3 y Ethernet son similares, no son idénticos. Las diferencias entre ellos son lo suficientemente significantes como para hacerlos incompatibles entre sí.

Las variantes de Ethernet tienen la misma arquitectura de acceso al medio múltiple con detección de errores, CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

Sin embargo, el estándar IEEE 802.3 ha evolucionado de forma que ahora soporta múltiples medios en la capa física, incluyendo cable coaxial, cable par trenzado sin blindaje (Unshielded Twisted Pair o UTP), cable par trenzado con blindaje (Shielded Twisted Pair o STP) y fibra óptica.

Su nombre se debe a "Luminiferous ether". En un tiempo se pensó que la radiación electromagnética se propagaba a través de él. En el siglo XIX Maxwell descubrió que la radiación electromagnética se podría describir mediante una ecuación de onda, los científicos supusieron que el espacio debía estar lleno de algún medio etéreo en el cual se propagaba la radiación, después se descubrió que la radiación electromagnética se podía propagar en el vacío.

En 1972 en PARC (Centro de Investigación de Xerox en Palo Alto) se diseñaba lo que se consideraba la 'oficina del futuro', se estaban probando unos ordenadores denominados Alto, que disponían de capacidades gráficas y ratón y son considerados los primeros ordenadores personales, también se estaban fabricando las primeras impresoras láser.

Se quería conectar los ordenadores entre sí para compartir ficheros y las impresoras. La comunicación tenía que ser de muy alta velocidad, del orden de megabits por segundo, ya que la cantidad de información a enviar a las impresoras era enorme (tenían una resolución y velocidad comparables a una impresora láser actual). Estas ideas que hoy parecen obvias eran completamente revolucionarias en 1973.

A Metcalfe, el especialista en comunicaciones del equipo con 27 años de edad, se le encomendó la tarea de diseñar y construir la red que uniera todo aquello. Contaba para ello con la ayuda de un estudiante de doctorado de Stanford llamado David Boggs. Las primeras experiencias de la red, que denominaron 'Alto Aloha Network', las llevaron a cabo en 1972. Fueron mejorando gradualmente el prototipo hasta que el 22 de mayo de 1973 Metcalfe escribió un memorándum interno en el que informaba de la nueva red. Para evitar que se pudiera pensar que sólo servía para conectar ordenadores Alto cambió el nombre inicial por el de Ethernet, que hacía referencia a la teoría de la física hoy ya abandonada según la cual las ondas electromagnéticas viajaban por un fluido denominado éter que se suponía llenaba todo el espacio.

(Metcalfe llamaba éter al cable coaxial por el que iba la portadora).

La red de 1973 ya tenía todas las características esenciales de la Ethernet actual. Empleaba CSMA/CD para minimizar la probabilidad de colisión, y en caso de que ésta se produjera ponía en marcha el mecanismo de retroceso exponencial binario para reducir gradualmente la 'agresividad' del emisor, con lo que éste se autoadaptaba a situaciones de muy diverso nivel de tráfico. Tenía topología de bus y funcionaba a 2,94 Mbps sobre un segmento de cable coaxial de 1,6 Km de longitud.

Las direcciones eran de 8 bits y el CRC de las tramas de 16 bits. El protocolo utilizado a nivel de red era el PUP (Parc Universal Packet) que luego evolucionaría hasta convertirse en el actual XNS (Xerox Network System).

En 1977 Metcalfe, Boggs y otros dos ingenieros de Xerox recibieron una patente por la tecnología básica de Ethernet, y en 1978 Metcalfe y Boggs recibieron otra por el repetidor. En esta época todo el sistema Ethernet era propietario de Xerox.

Ethernet usaba topología en bus con cable coaxial en sus inicios, hoy en día lo más normal es encontrarse una topología física en estrella con cable de par trenzado.



Xerox Alto - Wikimedia Commons - Creative Commons



Autoevaluación

Ethernet, FDDI y Token Ring tienen en común que:

- ☐ Las tres utilizan un testigo para que las estaciones puedan transmitir.
- ☐ Las tres tienen topología en anillo.
- ☐ Las tres se empezaron a utilizar en redes locales.
- ☐ Las tres tienen topología física en anillo y lógica en estrella.

8. LAS TECNOLOGIAS ETHERNET

Ethernet es una tecnología con múltiples variantes, como otro tipo de tecnologías se pueden clasificar atendiendo al medio de transmisión que utilizan, en este caso al tipo de cable.

Una clasificación posible sería:

- **1Base5:** Cable de par trenzado, [banda base](#) a 1Mb/s, distancia máxima de 250m.
- **10Base2:** Cable coaxial delgado (Thin Ethernet). Banda base a 10MB/s, distancia máxima de 185m.
- **10Base5:** Cable coaxial grueso (Thick Ethernet). Banda base a 10Mb/s, distancia máxima de 500m.
- **10Broad-36:** Cable coaxial de banda ancha a 10Mb/s, distancia máxima de 3600m.
- **10Base-T:** Cable de par trenzado sin blindaje UTP (Unshielded Twisted Pair), velocidad de 10 Mbps. topología de cableado horizontal en forma de estrella, con una distancia máxima de 100m desde una estación a un hub.
- **10Base-F:** Fibra óptica, banda base a 10Mb/s, distancia máxima de 2.000 metros.
- **100Base-FX (Fast Ethernet):** Fibra óptica multimodo (Fiber), velocidad de 100Mbps. Banda base a 100Mb/s sobre un sistema de cableado de dos fibras ópticas de 62.5/125 μ m.
- **100Base-TX (Fast Ethernet):** Cable de par trenzado, velocidad de 100 Mbps. Banda base a 100Mb/s sobre dos pares (cada uno de los pares de categoría 5 o superior) de cable UTP o dos pares de cable STP.
- **1000Base-T (Gigabit Ethernet):** Dos pares de cables trenzados de categoría 5, velocidad de 1 Gbps.
- **100BASE-T2:** Banda base a 100 Mb/s sobre 2 pares de categoría 3 (o superior) de cable UTP.
- **100Base-T4:** Cable UTP de categoría 3 (o superior) en banda base a 100Mb/s sobre 4 pares.
- **1000Base-SX (Gigabit Ethernet):** Fibra óptica multimodo y utiliza una longitud de onda corta (Short). Banda base a 1000Mb/s (1Gb/s) sobre 2 fibras multimodo (50/125 μ m o 62.5/125 μ m) de cableado de fibra óptica.
- **1000Base-LX (Gigabit Ethernet):** Fibra óptica multimodo y utiliza una longitud de onda larga (Long). Banda base a 1000Mb/s (1Gb/s) sobre 2 fibras monomodo o multimodo (50/125 μ m or 62.5/125 μ m) de cableado de fibra óptica.
- **1000Base-CX:** Banda base a 1000Mb/s (1Gb/s) sobre cableado de cobre blindado balanceado de 150 Ω . Este es un cable especial con una longitud máxima de 25m.

9. EL MODELO OSI Y ETHERNET

Ethernet opera en dos áreas del modelo OSI, la mitad inferior de la capa de enlace de datos, conocida como subcapa MAC y la capa física. Cuando una estación emite un mensaje a otra, la información pasa por todo el "dominio de colisión".

Los estándares garantizan un mínimo ancho de banda y operatividad especificando el máximo número de estaciones por segmento, la longitud máxima del mismo, el máximo número de repetidores entre estaciones, etc. Las estaciones separadas por repetidores se encuentran dentro del mismo dominio de colisión. Las estaciones separadas por puentes o routers se encuentran en dominios de colisión diferentes.

La capa física tiene un papel clave en la comunicación que se produce entre los dispositivos, pero cada una de estas funciones tiene limitaciones solucionadas por la capa enlace.

La capa física transforma los impulsos eléctricos en bits que se envían a través de los medios físicos. La capa enlace determina los métodos de acceso al medio y además es la responsable del direccionamiento a este nivel (direcciones MAC).

10. TIPOS DE CABLEADO ETHERNET

En sus orígenes Ethernet utilizaba cable coaxial grueso y topología en bus, hoy en día el tipo de cable más utilizado en estas redes es el cable de par trenzado que incluye varios tipos. De hecho, si nos referimos a un cable como "cable Ethernet", la mayoría de la gente piensa en un cable de par trenzado y casi nunca en un cable coaxial.

10.1. CABLEADO COAXIAL

Las primeras redes de tipo Ethernet tenían un cableado coaxial con topología en bus. Este tipo de red está formada por varios equipos unidos entre sí mediante un cable coaxial. Para unir cada equipo al cable se utilizan las conexiones tipo "T".

Además, en los extremos del cable se utilizan "terminadores" que se unen a un extremo de la "T" de los ordenadores de los extremos de la red. Si por alguna causa el cable se rompe, la red deja de funcionar.

10.2. CABLEADO DE PAR TRENZADO

Las redes Ethernet actuales utilizan un cable de par trenzado y suelen tener una topología en estrella. El cable utilizado es un cable de 8 hilos, con conectores tipo RJ45. Este tipo de cableado ha ganado terreno respecto al cableado coaxial por su instalación y coste.

11. CABLEADO ESTRUCTURADO

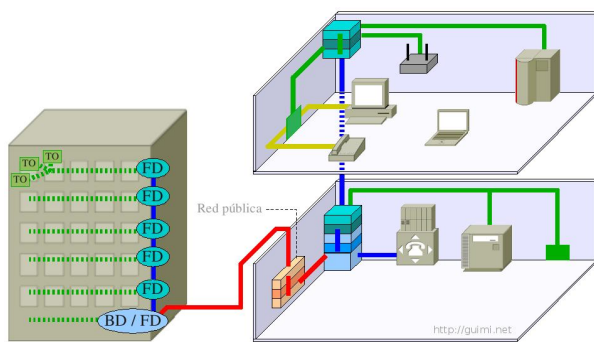


Caso práctico



ARQUITECTO Q - T. Fernández Escudero - "Elaboración propia"

CASO: Recientemente, Tomás ha recibido una visita de unos técnicos de calidad. Por su trabajo, sabe que la calidad en las construcciones es algo importantísimo. Mientras tomaban un café en un descanso, uno de ellos le ha sugerido que "certificase" la instalación de su oficina, que era algo que le iba a facilitar mucho la administración y que desde el punto de vista comercial le iba a aportar muchos enteros. Tomás le ha preguntado por los requisitos que debería cumplir la instalación para poder certificarse y le han respondido que todos están recogidos en el documento relativo al "cableado estructurado". ¿Qué es el cableado estructurado?



CABLEADO ESTRUCTURADO - guimi.net - Creative Commons

El concepto de "cableado estructurado" se entiende como el sistema de cables, conexiones, canalizaciones, espacios y demás dispositivos que deben ser instalados para establecer una infraestructura de telecomunicaciones genérica en un edificio.

La instalación de todos los elementos debe seguir un estándar para que se califique de cableado estructurado.

El que la instalación siga un estándar implicará un beneficio en su administración y gestión. Básicamente, el cableado estructurado consiste en el tendido de cables en el interior de un edificio con el propósito de implantar una red de área local. Suele tratarse de cable de par trenzado de cobre, para redes de tipo IEEE 802.3. No obstante, también puede tratarse de fibra óptica o cable coaxial.

11.1. TIPOS DE CABLES

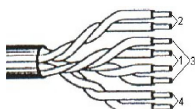
Las principales diferencias de rendimiento entre los distintos tipos de cables radican en:

- La anchura de banda permitida (y consecuentemente en el rendimiento máximo de transmisión).
- Inmunidad frente a interferencias electromagnéticas.
- Relación entre la pérdida de la señal y la distancia recorrida (atenuación).

Existen básicamente tres tipos de cables para el cableado en el interior de edificios o entre edificios:

- Cable de par trenzado.
- Cable coaxial.
- Fibra óptica.

11.2. CABLE DE PAR TRENZADO

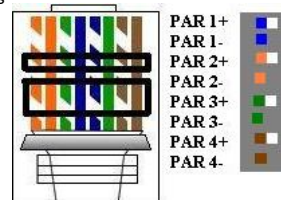


PAR TRENZADO - Anónimo - CC

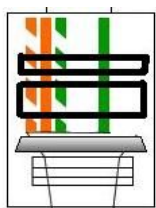
Este tipo de cable es el más usado en las redes LAN, es un cable similar al cable telefónico original, con la diferencia de que consta de 8 hilos en lugar de 2 o 4 que utiliza RTC. Otra diferencia está en que este cable tiene los hilos trenzados para evitar las interferencias (crosstalk), el propio cable sirve de pantalla por sí mismo.

Los cables de par trenzado pueden contener varios pares, dependiendo del uso o de la situación, son los llamados multipares (20 a 500 pares).

Aunque este tipo de cable dispone de 8 hilos, en la mayoría de las comunicaciones solamente son necesarios 4 hilos.



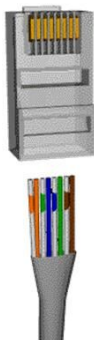
T568B - T. Fernández Escudero - "Elaboración propia"



T568B-4 - T. Fernández Escudero - "Elaboración propia"

La función de cada hilo viene determinada en el documento de los estándares EIA/TIA 568A - 568B, el cable de la figura pertenece al estándar 568B. Se diferencian por el orden de los colores de los pares a seguir en el armado de los conectores RJ45. El uso de cualquiera de las dos normas es indiferente, generalmente se utiliza la T568B para el cableado recto.

Según el estándar T568B, para transmitir y recibir se utilizan los pares 2 y 3, el para 1 sería para telefonía y el par 4 de respaldo. Es decir, una conexión Ethernet nos funcionaría con los pares 2 y 3 (4 hilos).



PAR TRENZADO RJ - Anónimo - CC

Los hilos siguen una normativa de nomenclatura (colores) que les identifican con la función que deben cumplir (datos o alimentación). Hay situaciones en las que no seguir la nomenclatura estandarizada desemboca en mala comunicación (distancias cortas), pero en instalaciones con muchos metros de longitud puede dar lugar a errores, la razón estriba en que no todos los hilos tienen la misma longitud porque no todos soportan el mismo trenzado. Es importante, por lo tanto seguir los estándares en los cables.

Por otra parte, dependiendo del conector que utilicemos y de la función del cable, los hilos seguirán una disposición u otra.

Para diseñar un cable de conexión "directo" (el cable más común que podemos encontrar y que nos puede servir para unir un PC con un router por ejemplo), con conector RJ45 (parecido al del teléfono pero más ancho) los hilos deberán situarse en el conector RJ45 en ambos extremos como se muestra en la figura.

En el peor de los casos, si no recordamos cual es la secuencia de colores que debemos seguir, tendremos que utilizar la misma secuencia en ambos extremos. En este último caso, si la longitud del cable es demasiado larga (varios), tendremos muchas probabilidades de que haya problemas en la conexión.

Los comités de la Asociación de la Industria de Telecomunicaciones (TIA) y de la Organización Internacional para la Normalización (ISO) son los líderes en el desarrollo de normas de cableado estructurado.

En los cables de pares hay que distinguir dos clasificaciones:

- Categorías:

Cada categoría especifica unas características eléctricas para el cable, atenuación, capacidad de la línea e impedancia.

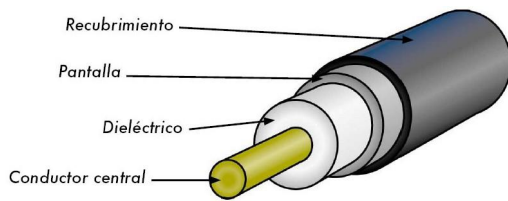
- Clases:

Cada clase especifica las distancias permitidas, el ancho de banda conseguido y las aplicaciones para las que es útil en función de estas características.

11.3. CABLE COAXIAL

El cable coaxial está formado por un núcleo de cobre (llamado "vivo") rodeado de un material aislante (dieléctrico); el aislante está cubierto por una pantalla de material conductor, que según el tipo de cable y su calidad puede estar formada por una o dos mallas de cobre, un papel de aluminio, o ambos. Este material de pantalla está recubierto a su vez por otra capa de material aislante.

Por su construcción el cable coaxial tiene una alta inmunidad electromagnética frente al ruido, poca atenuación de la señal y puede llegar a tener unos anchos de banda considerables; siendo adecuado para grandes distancias y/o capacidades.



COAXIAL - <http://guimi.net> - CC

El cable coaxial más utilizado en la actualidad es el de 75 Ω de impedancia también llamado cable coaxial de banda ancha, que no es ni más ni menos que el cable coaxial utilizado para televisión y redes de cable (CATV).

Originalmente fue el cable más utilizado en las redes locales debido a su alta capacidad y resistencia a las interferencias, pero en la actualidad su uso está en declive.

Su mayor defecto es su grosor, el cual limita su utilización en pequeños conductos eléctricos y en ángulos muy agudos, además de que debe manipularse con cuidado.

Para redes de datos se han utilizado dos tipos de cable coaxial:

- Grueso (Coaxial amarillo de 50 Ω). Su capacidad en términos de velocidad y distancia es grande, pero el coste del cableado es alto y su grosor no permite su utilización en canalizaciones con demasiados cables. Utilizado en la norma Ethernet 10Base-5.
- Fino (Coaxial RG58 de 50 Ω) con terminaciones BNC. Es más barato y fino y, por tanto, solventa algunas de las desventajas del cable grueso; aunque obtiene peores rendimientos que el cable amarillo. Utilizado en la norma Ethernet 10Base-2.

11.4. FIBRA OPTICA

La fibra óptica permite la transmisión de señales luminosas y es insensible a interferencias electromagnéticas externas.

Cuando la señal supera frecuencias de 10^{10} Hz hablamos de frecuencias ópticas. Los medios conductores metálicos son incapaces de soportar estas frecuencias tan elevadas y son necesarios medios de transmisión ópticos.

Para poder transmitir utilizando la fibra óptica son necesarias fuentes especializadas generadoras de señal:

- Fuentes láser: Son las fuentes capaces de producir una señal de más calidad.
- Diodos láser: Es una fuente semiconductor de emisión de láser de bajo precio.
- Diodos LED: Son semiconductores que producen luz cuando son excitados eléctricamente.

Un cable de fibra óptica consta de:

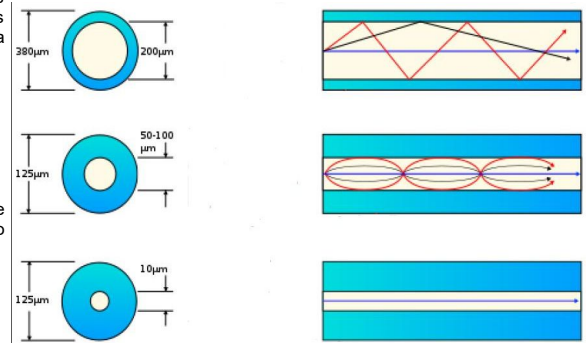
- Núcleo.
- Revestimiento.
- Cubierta externa protectora.

El núcleo, es el conductor de la señal luminosa y su atenuación es despreciable. La señal es conducida por el interior de éste núcleo fibroso, sin poder escapar de él debido a las reflexiones internas y totales que se producen, impidiendo tanto el escape de energía hacia el exterior como la adicción de nuevas señales externas.

Actualmente se utilizan tres tipos de fibras ópticas para la transmisión de datos:

- Fibra multimodo de índice escalonado.
- Fibra multimodo de índice gradual.
- Fibra monomodo.

En cuanto a calidad en la señal, capacidad y fiabilidad, la fibra óptica no tiene comparación posible con los demás medios de transmisión. Por el contrario, es más costosa de instalar, tiene un precio más alto y además es mucho más difícil de unir entre sí que los cables de pares o coaxiales.



FIBRA OPTICA - Wikimedia - CC

11.5. SELECCION DEL TIPO DE CABLEADO

Es recomendable que los cables de cobre y fibra óptica dentro de un edificio sean resistentes al fuego, generen poco humo y cero halógenos y sean retardantes de la llama.

Cuando se instalen cables de cobre o de fibra óptica en canalizaciones subterráneas, éstos deben tener protección adicional contra roedores, humedad y agua, radiación ultravioleta, campos magnéticos y tensión de instalación.

Si la distancia o el ancho de banda demandado lo exige será necesario utilizar fibra óptica. además se recomienda utilizar fibra cuando se da alguna de las siguientes circunstancias:

- El cableado une edificios diferentes; en este caso el uso de cable de cobre podría causar problemas debido a posibles diferencias de potencial entre las tierras de los edificios que podrían provocar corrientes inducidas en el cable. Además se podría ver muy afectado por fenómenos atmosféricos.
- Se desea máxima seguridad en la red (el cobre es más fácil de interceptar que la fibra).
- Se atraviesan atmósferas que pueden resultar corrosivas para los metales.
- Se sospecha que puede haber problemas de interferencia eléctrica por proximidad de motores, luces fluorescentes, equipos de alta tensión, etc.

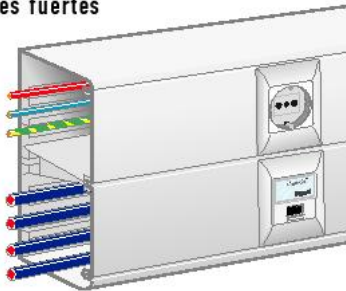
Cuando no se dé alguna de las razones que aconsejan utilizar fibra es recomendable utilizar cobre, ya que es más barato el material, la instalación y las interfaces de conexión de los equipos; además es más fácil realizar modificaciones en los paneles de conexión, empalmes, etc.

En general en una instalación grande se utiliza fibra para los tendidos principales (uniones entre edificios y cableado vertical para distribución por plantas dentro del edificio) y cobre para el cableado horizontal y quizá también para el cableado vertical (junto con la fibra) si las distancias entre los armarios así lo aconsejan.

11.6. CANALIZACIONES

Las canalizaciones son utilizadas para distribuir y soportar el cable y conectar equipamiento entre la salida del área de trabajo y el cuarto de telecomunicaciones. Los cables deben ir fijados en capas mediante abrazaderas colocadas a intervalos de 4 metros. Para evitar interferencias electromagnéticas la canalización de las corrientes débiles (cables de datos) debe mantenerse separada de corrientes fuertes (cables eléctricos y dispositivos electromagnéticos). Además en caso de cruzarse deben hacerlo perpendicularmente.

Corrientes fuertes



Corrientes débiles

CANALIZACIONES - <http://guimi.net> - CC

11.7. TENDIDO DE CABLE DE PAR TRENZADO



El cable de par trenzado es muy manejable y esto hace que a veces cometamos errores o nos permitamos licencias que van a repercutir en el funcionamiento general de la red. Es conveniente seguir unas pautas generales que se pueden resumir en este gráfico.

Sobre todo hay que tener en cuenta las curvaturas que se le den (esquinas del local), cuanto y como cortemos el cable, no hacer uniones si no es estrictamente necesario, si se deben hacer, emplear los elementos de interconexión que nos proporcionen garantías en el funcionamiento de la red (nunca cinta adhesiva o similar).

TENDIDO CABLE - <http://guimi.net> - CC

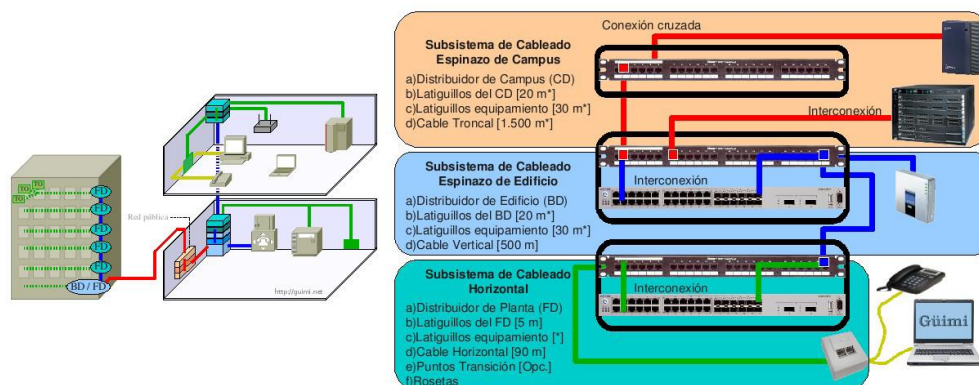
11.8. INSTALACION DE CABLEADO ESTRUCTURADO

Toda instalación que se precie debe seguir unas normas establecidas bajo algún estándar, además ese estándar debe ser seguido por la mayoría de las instalaciones para poder evitar problemas de incompatibilidades. Todo esto nos ahorra tiempo y dinero empleado en la administración de los sistemas de comunicaciones en nuestros edificios de trabajo. Cuando una instalación recibe el nombre de cableado estructurado se dice que sigue las normas TIA/EIA-568B, ISO/IEC 11801 y la EN 50173. La norma europea EN 50173 1 (la versión española es la UNE-EN 50173) se basa en la norma ISO 11801.

EPHOS 2 (European Procurement Handbook for Open Systems - Phase 2) recuerda que desde 1986 se "obliga a todos los responsables de contrataciones públicas (...) a hacer referencia a estándares o prestandares europeos o internacionales". Es decir se obliga a cumplir las normas EN 50173 1, ISO 11801, ISO 802.x... y cumplir una serie de requisitos de Compatibilidad Electromagnética (CEM), protección de incendios, número de zocalos, etc.

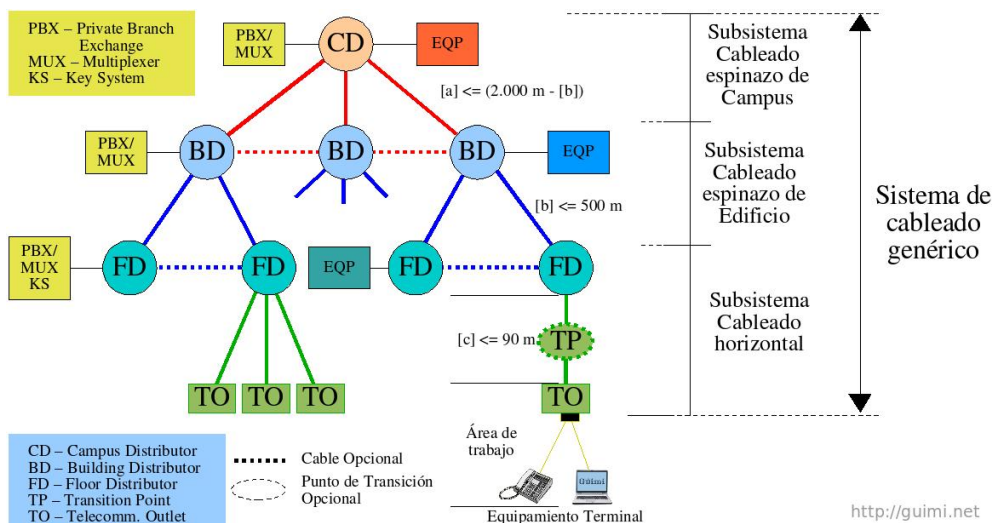
En el cableado estructurado se distinguen tres subsistemas:

- Subsistema de cableado de Campus o entre edificios.
- Subsistema de cableado Vertical (reparto entre plantas de un edificio).
- Subsistema de cableado Horizontal (reparto en cada una de las plantas del edificio).



SUBSISTEMAS CABLEADO ESTRUCTURADO - <http://guimi.net> - CC

El esquema teórico del cableado estructurado sería el siguiente:



ESQUEMA DE CABLEADO ESTRUCTURADO - <http://guimi.net> - CC

• CABLEADO Y EQUIPAMIENTO DEL AREA DE TRABAJO

El cableado y equipamiento del área de trabajo no es parte del sistema de cableado genérico y la norma no impone requisitos al respecto. Incluye:

- Cable del área de trabajo.
- Equipamiento terminal.

Se asume una longitud eléctrica combinada de (a) y (b) equivalente a 7,5 m de cable.

• DISTRIBUIDORES

Debería haber un mínimo de un armario distribuidor de planta (FD) por cada 1.000m² de espacio reservado para oficinas, con un mínimo de un FD por planta. Si una planta se utiliza poco para oficinas (como un vestíbulo) puede atenderse desde un FD de una planta adyacente.

Todo distribuidor (CD, BD, FD) debe estar en un cuarto de telecomunicaciones o en un cuarto de equipamiento.

Todas las interconexiones del cableado genérico se realizan con paneles de conexión.

Cuando los equipos activos (enrutadores, conmutadores...) se cablean directamente a paneles de algun subsistema de cableado, se denomina 'interconexion' (interconnect), y cuando lo hacen a paneles independientes se denomina 'conexión cruzada' (cross connect).

Suele ser más eficiente, por coste inicial y de mantenimiento, disponer de pocos distribuidores grandes que de muchos distribuidores pequeños, teniendo en cuenta que la distancia de los FD a las TO no debe superar los 90 m. Es decir, normalmente, las TO estarán en un radio de 60 m desde el FD, debido a que el cable debe subir, bajar y hacer curvas.

Además los FD deberán situarse, siempre que haya espacio disponible, lo más cerca posible de la(s) vertical(es).

En la instalación de los distribuidores de edificio (BD) y de campus (CD) debe considerarse también su proximidad a los cables de comunicaciones con el exterior.

• CUARTOS DE TELECOMUNICACIONES/CUARTOS DE EQUIPAMIENTO

Un cuarto de telecomunicaciones (TC: Telecommunications Closet) es un espacio cerrado de un edificio utilizado para el uso exclusivo de cableado de telecomunicaciones y

sistemas auxiliares, bastidores (racks), concentradores, aire acondicionado propio...

Cada cuarto debe tener acceso directo al cable espinazo.

Un cuarto de equipamiento (ER: Equipment Room) es un espacio cerrado de uso específico para equipamiento de datos y telecomunicaciones que puede contener o no distribuidores (haciendo la función de TC). Todo espacio que contenga más de un distribuidor se considera un ER.

Los cuartos de telecomunicaciones deben considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable (CATV), alarmas, seguridad o audio. No debe contener otras instalaciones eléctricas que no sean del equipamiento propio del cuarto.

Un cuarto de equipamiento puede incluir espacio de trabajo para el personal correspondiente.

Los armarios (bastidores o racks) deben de contar con al menos 82 cm de espacio libre por delante y detrás, medidos a partir de la superficie más sobresaliente del armario.

Deben disponer de acometida eléctrica diferenciada, apantallamiento frente a interferencias electromagnéticas, sistemas de alimentación interrumpida, sistema de luz de emergencia y ventilación adecuada.

Todo edificio debe contener al menos un cuarto de telecomunicaciones o un cuarto de equipo; no hay un límite máximo.

En los TC la temperatura debe mantenerse permanentemente entre 10 y 35 grados centígrados y la humedad relativa debe mantenerse por debajo del 85%, realizándose un cambio completo de aire por hora.

En los ER la temperatura debe mantenerse permanentemente entre 18 y 24 grados centígrados y la humedad relativa debe mantenerse entre el 30% y el 55%, realizándose un cambio completo de aire por hora.

Por esto a veces los TC y ER son también llamados "salas frías".

• SALIDAS DE TELECOMUNICACIONES Y PUNTOS DE TRANSICION

Una alta densidad de TOs aporta flexibilidad al cableado para permitir cambios. En muchos países se utilizan dos Tos para un máximo de 10m2.

Pueden presentarse individualmente, por parejas o en grupo, pero cada área de trabajo debe cubrirse con al menos dos.

Cada TO debe estar identificado con una etiqueta permanente y visible. Si uno de ellos está conectado con cable de par trenzado y utiliza menos de 4 pares debe ser claramente marcado. La configuración mínima consiste en:

- Un TO con cable balanceado de 100 Ω , preferentemente cable de 4 pares, Categoría 3 o superior.
- Otro(s) TO con dos hilos de fibra óptica multimodo (50/125 o 62,5/125) o cable balanceado categoría 3 o superior).

Se conocen como MUTO (Muti-User TO) las rosetas multiusuario, que pueden dar servicio a 12 aéreas de trabajo como máximo (24 TOs). Deben ser fácilmente accesibles y su instalación debe ser permanente, es decir, no pueden estar localizadas en un techo o piso falso, en un armario... El cable desde el FD hasta un PT o un MUTO debe tener mínimo 15 m.

Un TP sirve para cambiar entre distintas formas del mismo tipo de cable (p.e. de cable plano a cable redondo) o como punto de consolidación. No puede ser utilizado como distribuidor ni se pueden conectar a él equipos activos. Las características de los cables deben ser mantenidas en la entrada y la salida.

Los puntos de consolidación son una interconexión en el cableado horizontal que permite configuraciones más sencillas en oficinas cambiantes y se permiten para un máximo de 12 áreas de trabajo (24 TOs).

La diferencia más visible entre un TP y una MUTO es que el TP requiere una conexión adicional (una TO) para cada cable horizontal. Las TP se utilizan en oficinas cambiantes donde las TO se irán moviendo de un sitio a otro y las MUTO en oficinas que necesitan concentrar sus TO.

• TIPO DE CABLEADO

Los tipos de cable permitidos por la norma vigente son:

- Cable de pares trenzados con o sin blindaje de 100 Ω .
- Cable de fibra óptica multimodo de 62.5/125 μm .
- Cable de fibra óptica multimodo de 50/125 μm .
- Cable de fibra óptica monomodo 8-10/125 μm (para largas distancias).

Se usaran preferentemente los dos primeros tipos de cable.

• ADMINISTRACION

La administración es un aspecto esencial del cableado genérico. La administración incluye la identificación exacta y el registro de todos los componentes del sistema, así como las canalizaciones y los espacios (TC y ER). Un buen registro puede incluir diagramas de cableado, mapas de conectividad y localización de los TO.

Deben registrarse todos los cambios que se realicen y cuando se han realizado, preferentemente por ordenador, y preparar procedimientos adecuados de actualización.

Si se realizan test de aceptación deberían registrarse también sus resultados.

Cada elemento, canalización y espacio debe tener su identificación claramente visible. A cada elemento, canalización y espacio se le asignara una identificación (mediante colores, números o cadenas alfanuméricas) unívoca.

Cada TO debe etiquetarse de modo que referencie la impedancia del cable, su categoría y número de pares o bien el diseño de fibra óptica utilizado.

Los cables deben marcarse en ambos extremos.

12. ALGORITMO DE ACCESO AL MEDIO

El protocolo CSMA surge para solucionar el problema del reparto del canal en las redes Ethernet, se basa en obligar a cada estación a "escuchar el canal" antes de transmitir. Si el canal estuviera ocupado, espera para transmitir, si está libre transmite y si escucha una colisión espera un tiempo y luego transmite.

Hay varios tipos de protocolo CSMA:

- CSMA 1-persistente.
 - o Transmite con probabilidad 1 al estar el canal desocupado.
 - o Una colisión puede ocurrir cuando dos nodos encuentren el canal libre y comiencen a transmitir con una separación en el tiempo menor que la distancia que les separa.
 - o Es sensible a los retardos de línea.
- CSMA no-persistente.
 - o Igual que el anterior, antes de transmitir se escucha al canal.
 - o Si el canal está ocupado espera un tiempo para transmitir, este tiempo está calculado por un algoritmo.
 - o Se diferencia con el 1-persistente en que la estación no está escuchando continuamente a que el canal quede libre para transmitir.
 - o Para poco tráfico se comporta peor que el 1-persistente (es más lento) pero cuando el tráfico es alto reduce el número de colisiones.
- CSMA p-persistente.
 - o Se utiliza en canales en los que el uso se limita a franjas de tiempo.
 - o Si el canal está desocupado transmite con probabilidad p y $q=1-p$, retarda la transmisión hasta el próximo intervalo de tiempo.
 - o En caso de que el intervalo de tiempo estuviera ocupado el canal se comporta como si hubiera una colisión, espera un tiempo aleatorio para poder volver a transmitir.
 - o Es más eficiente, en general, que cualquiera de los dos anteriores.
- CSMA/CD
 - o Cuando una estación detecta una colisión asegura una transmisión de una fracción mínima del frame. esta fracción se denomina JAM y su objetivo es alertar a las demás.
 - o Al detectar una colisión, las estaciones dejan de transmitir, esperan un tiempo aleatorio y vuelven a transmitir.

13. ESTRUCTURA DE LA TRAMA ETHERNET

Los impulsos eléctricos (bits) transmitidos por el medio se ordenan en forma de trama a nivel enlace del modelo OSI, esta trama en el protocolo Ethernet organiza la secuencia de bits como se explica en la siguiente figura.

PREAMBULO (7 BYTES)	INICIO (1)	DIRECCION DESTINO (2 - 6)	DIRECCION ORIGEN (2 - 6)	LONGITUD DATOS (2)	DATOS (0 - 1500)	RELLENO (0 - 46)	CRC (4)

- Preámbulo. Son 7 bytes con el formato 10101010 (negociación de la comunicación).
- Inicio. Es un campo de 1 byte compuesto por los bits 10101011, indica que comienza la transmisión.
- Dirección de destino. Es un campo que puede ocupar de 2 a 6 bytes con la dirección (MAC) del nodo destinatario de la comunicación.
- Dirección de origen. Contiene la dirección MAC de la estación que emitió la trama.
- Longitud. Especifica la longitud de los datos transmitidos
- Datos. Son los datos a transmitir puede tener hasta 1500 bytes.
- Relleno. Se utiliza para conseguir que la trama tenga el tamaño mínimo exigible por la normativa.
- CRC. Es un campo de 4 bytes que sirve para el control de errores (Código de Redundancia Cíclica).

