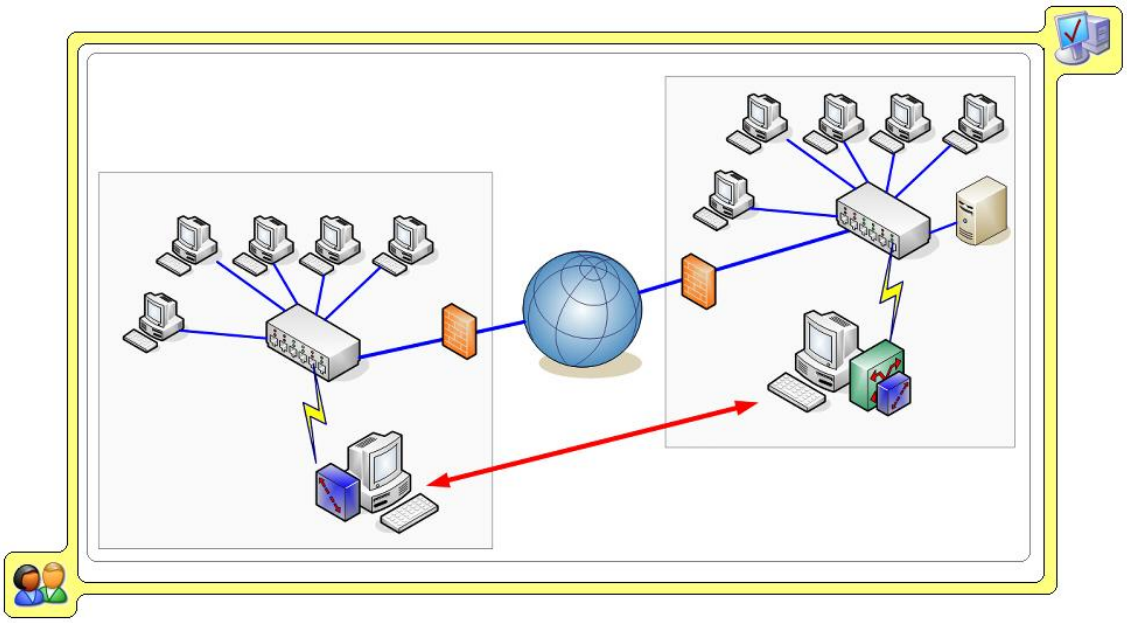
UNIDAD 5. REDES DE ÁREA LOCAL



5.1. ESTÁNDARES DE REDES DE ÁREA LOCAL

En esta sección estudiaremos específicamente los sistemas **LAN** (**L**ocal **A**rea **N**etwork). Como se mencionó en el capítulo anterior, tanto la topología como las técnicas de control de acceso al medio son características fundamentales para la clasificación de las redes LAN y para el desarrollo de normalizaciones. En cuanto a esto último, el comité **IEEE 802** ha desarrollado una serie de estándares. En cada estándar se especifica la técnica de acceso al medio (**MAC**. **M**edium **A**ccess **C**ontrol) , además de diversas opciones de medios de transmisión con distintas velocidades. El protocolo LAN 802 más utilizado es el 802.3, basado en las especificaciones iniciales de Ethernet. El IEEE 802 ha desarrollado además un estándar para LAN inalámbricas, utilizando tecnologías de infrarrojos y de espectro expandido.

A) Ethernet (CSMA/CD)

La técnica de control de acceso al medio más ampliamente utilizada en las topologías en bus y en estrella es la de *acceso múltiple sensible a la portadora con detección de colisiones* **(CSMA/CD C**arrier **S**ense Múltiple **A**ccess with **C**ollision **D**etection). La versión original en banda base de esta técnica fue desarrollada por Xerox para redes LAN Ethernet, este desarrollo fue la base para la posterior especificación del estándar IEEE 802.3. Ver la figura 5.1.

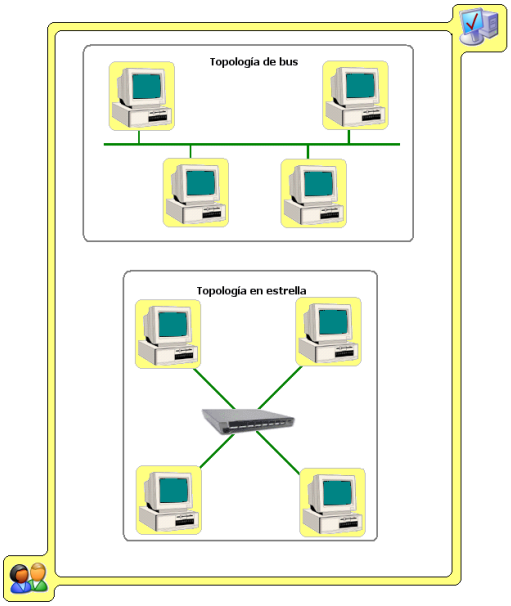


Fig. 5.1. Especificación ETHERNET.

Dependiendo del tipo de cable utilizado y las distancias entre ordenadores, existen diferentes adaptaciones de la norma IEEE 802.3. Dentro de las adaptaciones que vamos a ver a continuación el primer número hace referencia a la velocidad de transmisión en Megabits por segundo. Las adaptaciones de las redes Ethernet son las siguientes:

Especificaciones a 10 Mbps:

- **10BASE-5.** Cable coaxial con una longitud máxima de 500 metros por segmento y capacidad para 100 nodos por segmento.
- **10BASE-2**. Cable coaxial más fino que el anterior con una longitud máxima de 185 metros por segmento y capacidad para 30 nodos por segmento.
- **10BASE-T**. Par trenzado con una longitud máxima de 100 metros por segmento.
- **10BASE-F.** Soporta segmentos de cable de fibra óptica de hasta 2 Km. con una velocidad de transmisión de 10Mb/s.
- **10BROAD-36.** Cable coaxial de tipo RG59 CATV (categoría cinco) con una longitud máxima de segmento de 3600 metros

Especificaciones a 100 Mbps (Fast Ethernet):

- **100BASE-T.** Uso de par trenzado con segmentos de hasta 100 metros. Admite las variantes TX y T4.
- **100BASE-FX.** Uso de par de fibra óptica con segmentos de 100 metros.

Especificaciones a 1000 Mbps (Gigabit Ethernet):

- **1000BASE-SX:** Uso de fibra óptica en enlaces dúplex de hasta 550 metros.
- **1000BASE-LX:** Uso de fibra óptica en enlaces dúplex de hasta 5 Kilómetros.
- **1000BASE-CX:** Enlaces entre dispositivos localizados dentro de una habitación (o armario de conexiones) utilizando latiguillos de cobre.
- **1000BASE-T:** Utiliza cuatro pares no apantallados para conectar dispositivos separados hasta 1000 metros.

Veamos a continuación algunas de las especificaciones que más han sido utilizadas:

10BASE-2 o red fina de Ethernet.

Para montar una red siguiendo estas especificaciones, tendremos que tener en cuenta las siguientes características:

- Utilizar cable coaxial RG58 AU o RG58 CU en todos los segmentos.
- La longitud máxima de cada segmento es de 185 metros.

- Se utilizan conectores en **T** para conectar cada segmento de cable con los adaptadores de red.
- Es necesario utilizar repetidores (amplificadores de la señal de red) entre ordenadores que tengan una distancia superior a la especificada en sus segmentos de cable.
- La longitud máxima de la línea principal no puede exceder de 900 metros.
- Podemos tener un máximo de 30 conexiones sobre la línea principal. Si tenemos más de una línea principal podremos llegar a conectar hasta 1024 segmentos de cable.
- Se tiene que colocar un terminador en cada extremo de la línea principal y uno de ellos es conveniente que esté conectado a tierra.

Este tipo de especificación en la actualidad no se implanta ya que es problemática. Como todos los equipos están unidos por un único cable, cualquier corte o error de conexión en un segmento, en una T, e incluso en los terminadores, provocará que la red deje de funcionar.

Tiene una ventaja muy importante y es su bajo coste, ya que con un poca inversión en cable podemos conectar varios ordenadores sin necesidad de utilizar componentes adicionales. Por el contrario, es una especificación en la que la velocidad no es su principal ventaja, ya que los equipos conectados en los extremos de la misma, serán los más lentos.

También tiene el problema de la ampliación de equipos, ya que al no ser cables independientes los que unen unos ordenadores con otros, tendremos que desconectar la red para integrar otros equipos.

10BASE-T. Este tipo de redes, junto con las 100BASE-T, son las más extendidas en la actualidad. Físicamente son similares a las de tipo 100BASE-T. La diferencia es la velocidad de transferencia.

Para este tipo de redes, es necesario disponer del material que hemos comentado en la unidad anterior: clavijas RJ45, rosetas, segmentos de cable y HUB o SWITCH para interconectar los equipos.

Son más caras de montar que las de 10BASE-2, pero son más flexibles, más seguras y más rápidas. Como cada ordenador está conectado a los otros mediante un cable independiente, los problemas de un equipo no afectan a los demás de la red. Por el contrario, tendremos que utilizar mucho más cable, un segmento por cada ordenador, que en las redes de tipo 10BASE-2, que funcionan con un solo cable principal.

Es evidente que este tipo de redes serán más caras de montar, pero insistimos en que se ha demostrado su fiabilidad y flexibilidad. En la actualidad todas las redes se montan siguiendo esta especificación.

Veamos algunas de sus características:

- Utilizan cable par trenzado sin apantallar o apantallado de categoría 3,4,5 o superior.
- Utilizan conectores o clavijas (macho) RJ45 en los extremos de los cables. Los pines 1 y 2 son transmisores de datos y los pines 3 y 6 receptores. Cada par se invierte en el hub o switch para que el transmisor de un extremo se convierta en receptor en el otro.
- A cada estación se puede conectar una roseta o transceptor.
- La distancia desde la roseta o transceptor al hub o switch no puede ser superior a 100 metros.
- Los hub suelen servir para conectar 16 estaciones. Los switch suelen ser para 24.
- Cada hub o switch se puede conectar a otros gracias a la existencia de un puerto específico de interconexión (no cruzado). De no existir este puerto, se podrá realizar la expansión igualmente, pero utilizando un cable de pares cruzado en lugar de directo, tal y como se indicó en la unidad anterior.
- Se pueden tener conectadas hasta 1024 estaciones sin necesidad de utilizar hardware adicional.

100BASE-T. Como ya hemos indicado este estándar denominado Fast Ethernet tiene dos subestándares: TX y T4.

100BASE-T4 está pensado para ofrecer una velocidad de transmisión de datos de 100 Mbps a través de cable de clase 3 de baja calidad: la idea es poder reutilizar las instalaciones existentes de este tipo de cable en edificios de oficinas. La especificación también permite el uso opcional de clase 5.

En 100BASE-T4, al utilizar cable de clase 3 para voz, no es de esperar que los 100 Mbps se obtengan utilizando un único par trenzado. Por el contrario, 100BASE-T4 especifica que la secuencia de datos a transmitir se divida en tres secuencias distintas. Los datos se transmiten haciendo uso de tres pares y se reciben por otros tres. Como disponemos de cuatro pares únicamente, dos de los pares deben configurarse para una transmisión bidireccional.

Sin embargo, con el sistema 100BASE-TX, los 100 Mbps se consiguen en un único enlace, utilizando esquemas de codificación de señal efectivos y eficientes, similares a los que se utilizan en la red FDDI.

B. Token Ring

Queda definido por el estándar 802.5 del IEEE, orientado a redes con topología en anillo. La primera red comercializada de este tipo fue la Token Ring de 4Mb/s. Observar la figura 5.2.

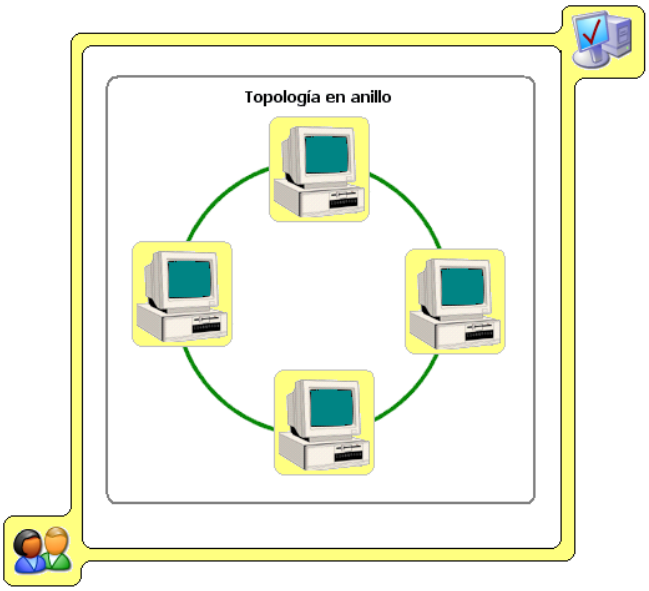


Fig. 5.2. Especificación TOKEN RING

Como se indicó en la unidad anterior, cada ordenador o estación se conectan a equipos de interconexión centrales (MAU) que realizan las funciones de anillo a la hora de repartir la señal. Si conectamos más de un MAU el anillo se hace más grande.

La principal característica de estas redes es que cada ordenador o estación funciona de repetidor de señal. Cuando la señal llega a un ordenador, y éste reconoce que no es para él, la reenvía al siguiente y así sucesivamente. De esta forma se consigue que la señal siempre esté en perfecto estado y sin interferencias, independientemente de la distancia del equipo que envía la señal y el equipo que la recibe.

Las especificaciones de las redes Token Ring son, al igual que en Ethernet, múltiples. Veamos algunas de las más importantes.

- **Tipo1.** Cable apantallado conteniendo dos hilos de par trenzado 22 AWG.
- **Tipo2.** Un cable apantallado para voz y datos con dos hilos de par trenzado 22 AWG para los datos con cuatro hilos añadidos de par trenzado 26AWG fuera de la protección de voz.
- **Tipo3.** Incluye cuatro cables macizos sin apantallar de par trenzado de 22 o 24 AWG.
- **Tipo5.** Cable de fibra óptica de dos fibras.
- **Tipo6.** Cable alargador de par trenzado apantallado y flexible de 26 AWG
- **Tipo8.** Cable par trenzado apantallado de 26 AWG para usar bajo moqueta.
- **Tipo9.** Cable de par trenzado apantallado y antiincendio de 26 AWG.

Con este tipo de redes se pueden conectar hasta 260 estaciones si utilizamos cable apantallado. Si utilizamos cable telefónico de par trenzado sin apantallar, podemos conectar hasta 72. La distancia máxima recomendable en metros de una estación a otra es de 100. Las velocidades que contempla el estándar son 4, 16 y 100 Mbps.

C. FDDI (Fiber Distributed Data Interface)

FDDI es un esquema en anillo con paso de testigo análogo a la especificación IEEE 802.5 diseñada para aplicaciones LAN y MAN. La diferencia fundamental radica en las mayores velocidades de transmisión que alcanza, gracias al uso de un doble anillo de fibra óptica. Permite una mayor longitud entre repetidores que el caso anterior (hasta 2 Km.).

La robustez del estándar radica en la existencia del doble anillo de fibra. Uno de los anillos transmite en el sentido de las manecillas del reloj, y el otro en el sentido contrario. Si alguno de los dos se llega a desactivar, el otro puede emplearse como respaldo; si los dos se desactivaran en el mismo punto, los dos anillos podrán unirse para formar un solo anillo que tendrá una longitud casi del doble, como se muestra en la figura 5.3:

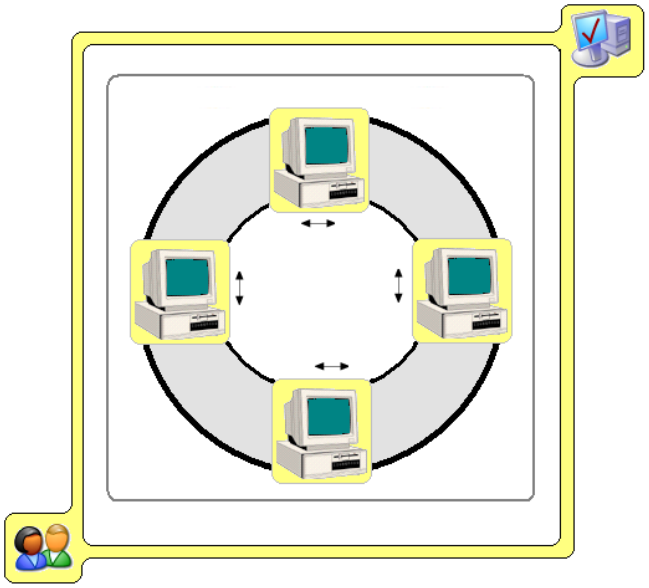


Fig. 5.3. Doble anillo FDDI.

Se definen dos clases de estaciones, A y B. Las estaciones clase A se conectan a los dos anillos, en tanto que las clase B, más económicas, sólo se conectan a uno de ellos. Las estaciones de clase A son las encargadas de conectar ambos anillos en caso de rotura, tal y como se ha explicado. Dependiendo de la importancia que pueda tener la tolerancia a fallos, una instalación puede optar por seleccionar estaciones de clase A, B o mezcla de ellas.

Las redes FDDI normalmente son utilizadas como redes *troncales*, esto es, redes utilizadas para interconectar otras redes de área local.

D. Especificaciones ARCNET

Esta especificación permite transferir datos a una velocidad de 2,5 Mbps, soportando longitudes de cable de hasta 675 metros. Las nuevas versiones de Arcnet soportan fibra óptica y par trenzado.

Debido a la flexibilidad de su método de cableado, que permite grandes tramos, es una buena opción, cuando la velocidad no es lo más importante y lo que prevalece es la seguridad en la transmisión de datos. El inconveniente es el precio, ya que este tipo de redes son caras.

En estas redes se utiliza cable coaxial RG62 AU aunque se puede utilizar par trenzado o fibra óptica. Utilizan HUB activos y pasivos. Los activos para distribuir señal y los pasivos como conmutadores entre ordenadores remotos. Puede haber una distancia de hasta 6 Km. entre los dos extremos de la red, pudiéndose conectar hasta 255 estaciones.

E) Redes inalámbricas

En los últimos años las redes de área local inalámbricas (**WLAN**, **W**ireless **L**ocal **A**rea **N**etwork) están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren

nuevas aplicaciones para ellas. Las WLAN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar.

Con las WLAN la red, por sí misma, es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red, y lo más importante incrementa la productividad y eficiencia en las empresas donde está instalada. Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas a velocidades de 11 Mbit/s, o superiores. Observar la figura 5.4:

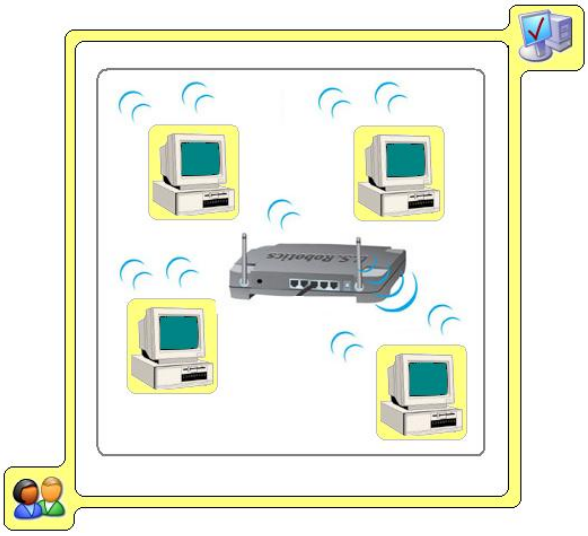


Fig. 5.4. Red inalámbrica.

Pero no solamente encuentran aplicación en las empresas, sino que su extensión a ambientes públicos, en áreas metropolitanas, como medio de acceso a Internet o para cubrir zonas de alta densidad de usuarios en las próximas redes de tercera generación (3G) se ven como las aplicaciones de más interés durante los próximos años

Muchos de los fabricantes de ordenadores y equipos de comunicaciones como son los **PDAs** (**P**ersonal **D**igital **A**ssistants), módems, terminales de punto de venta y otros dispositivos están introduciendo aplicaciones soportadas en las comunicaciones inalámbricas.

Las nuevas posibilidades que ofrecen las WLAN son: permitir una fácil incorporación de nuevos usuarios a la red, ofrecer una alternativa de bajo costo a los sistemas cableados, además de la posibilidad para acceder a cualquier base de datos o cualquier aplicación localizada dentro de la red.

Ventajas de WLAN sobre redes fijas:

- **Movilidad:** las redes inalámbricas proporcionan a los usuarios de una LAN acceso a la información en tiempo real en cualquier lugar dentro de la organización o el entorno público (zona limitada) en el que están desplegadas.
- **Simplicidad y rapidez en la instalación:** la instalación de una WLAN es rápida y fácil y elimina la necesidad de tirar cables a través de paredes y techos.
- **Flexibilidad en la instalación:** La tecnología inalámbrica permite a la red llegar a puntos de difícil acceso para una LAN cableada.
- **Costo de propiedad reducido:** mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN, la inversión de toda la instalación y el costo durante el ciclo de vida puede ser significativamente inferior. Los beneficios a largo plazo son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes.
- **Escalabilidad:** los sistemas de WLAN pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además resulta muy fácil la incorporación de nuevos usuarios a la red.

Entre los principales estándares se encuentran:

- **IEEE 802.11**: El estándar original de WLAN que soporta velocidades entre 1 y 2 Mbps.
- **IEEE 802.11a**: El estándar de alta velocidad que soporta velocidades de hasta 54 Mbps en la banda de 5 Ghz.
- **IEEE 802.11b**: El estándar dominante de WLAN (conocido también como Wi-Fi) que soporta velocidades de hasta 11 Mbps en la banda de 2.4 Ghz.
- **HIPERLAN2**: Estándar que compite con IEEE 802.11a al soportar velocidades de hasta 54 Mbps en la banda de 5 Ghz.
- **HomeRF**: Estándar que compite con el IEEE 802.11b que soporta velocidades de hasta 10 Mbps en la banda de 2.4 Ghz.

Principales estándares WLAN

Estándar	Velocidad máxima	Interface de aire	Ancho de banda de canal	Frecuencia
802.11b	11 Mbps	DSSS	25 MHz	2.4 GHz
802.11a	54 Mbps	OFDM	25 MHz	5.0 GHz
802.11g	54 Mbps	OFDM/DSSS	25 MHz	2.4 GHz
HomeRF2	10 Mbps	FHSS	5 MHz	2.4 GHz
HiperLAN2	54 Mbps	OFDM	25 MHz	5.0 GHz
5-UP	108 Mbps	OFDM	50 MHz	5.0 GHz

Veamos con mas detalle el tipo de interfaces:

- **DSSS:** Direct Sequence Spread Spectrum.
- **OFDM**: Orthogonal Frequency Division Multiplexing
- **FHSS:** Frequency Hopping Spread Spectrum

5.2. PROTOCOLOS DE RED

Definimos protocolo como el software necesario para que dos o más equipos puedan comunicarse entre sí. El protocolo es, por tanto, el lenguaje que utilizan los ordenadores para comunicarse. En particular, los protocolos de red son los necesarios para que dos equipos puedan encontrarse en una red e intercambiar información. Recordemos que éste era el objetivo del nivel de red de la arquitectura de comunicaciones, y por tanto, los protocolos utilizados para conseguirlo se llaman protocolos de red.

En la figura 5.5 puedes observar en que nivel de la arquitectura OSI trabaja cada protocolo:

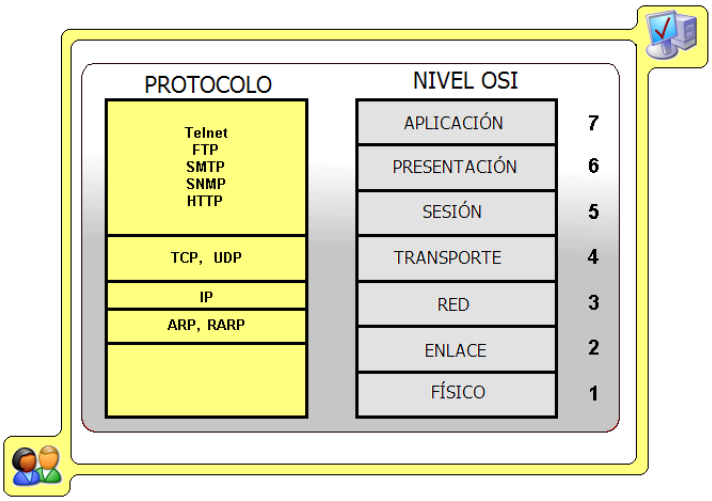


Fig.5.5. Protocolos por niveles en arquitectura OSI.

Los protocolos de red pueden ser de varios tipos, dependiendo de la plataforma con la que nos encontremos. Cada fabricante de sistema operativo incorpora en el núcleo del mismo las herramientas necesarias para que el ordenador pueda enviar y recibir señal a través de la tarjeta de red mediante los protocolos de red.

Entre los protocolos de red podemos destacar fundamentalmente TCP/IP, NetBEUI e IPX/SPX, pero es TCP/IP el protocolo por excelencia. Esto es debido a que ha sido el protocolo adoptado en Internet, y cualquier equipo que quiera navegar por la red tiene que tener instalado este protocolo. Sin embargo, los protocolos NetBEUI y IPX/SPX se utilizan respectivamente por redes Microsoft o por redes Novell y en ámbitos privados.

A continuación nos centraremos el protocolo TCP/IP (**T**ransmisión **C**ontrol **P**rotocol/**I**nternet **P**rotocol), ya que es internacional y se puede utilizar en todo tipo de redes, y es el estándar para trabajar en Internet.

A. Direccionamiento IP 

Los equipos que utilizan TCP/IP como protocolo tienen que estar configurados de acuerdo a unas normas estándar establecidas. Todos los dispositivos hardware, ordenadores, impresoras, enrutadores, etc, que utilicen el protocolo TCP/IP, independientemente del sistema operativo con el que estemos trabajando, estarán identificados con una **dirección IP única** dentro de la red que será su identificación.

Esta dirección consiste en un valor binario de 32 bits (aunque IP v6. ya considera direcciones de 128 bits), que por claridad suele agruparse en 4 bytes identificados cada uno por el valor decimal correspondiente.

Supongamos la siguiente dirección IP: ***255.255.255.27***

El correspondiente valor binario es: ***11111111.11111111.11111111.00011011***

Insistimos en que cada ordenador de una red tiene que tener una dirección IP única. Si montamos una LAN, cada uno de los ordenadores integrados en la red, tendrán su dirección IP diferente. Lo mismo ocurre en Internet. Cada ordenador o servidor de Internet tiene asignada una dirección única (denominadas direcciones públicas) diferente de cualquier dirección IP del mundo. Estas direcciones de Internet son suministradas por un organismo oficial que tiene la función de regular esta unicidad a nivel mundial.

En redes LAN podremos poner las direcciones IP que queramos, pero debemos tener en cuenta que ninguna de ellas será igual, y por supuesto, si alguno de nuestros equipos estuviera conectado a Internet tendría que tener una dirección IP pública única. Esta dirección de red la podemos conseguir (previo pago) de INTERNIC o Internet Network Information Center o centro de información de red de Internet.

Cada dirección IP consta de dos partes claramente diferenciadas:

- **Identificador de subred.** Identifica los equipos conectados en la misma subred física. Este identificador será idéntico para todos los equipos conectados a una misma subred (es decir, conectados directamente entre sí a través de una única LAN). Las subredes se diferencian entre sí precisamente a través de este identificador.
- **Identificador de Host.** Identifica unívocamente cada equipo conectado dentro de la subred.

La cantidad de bits destinados a cada uno de los identificadores es variable y será elegido en función de las características de la subred que estemos configurando. La **máscara de subred** indicará la cantidad de bits destinados a cada identificador y acompañará siempre a la dirección IP de un equipo. La máscara de subred está formada por 32 bits, al igual que la dirección IP. Sirve como plantilla para la dirección IP, de tal modo que las posiciones de la dirección IP correspondientes con *1's* en la máscara formarán parte del identificador de subred, mientras que las posiciones de la dirección IP correspondientes con *0's* en la máscara formarán parte del identificador de Host.

EJEMPLO:

El equipo de dirección IP siguiente:

00011100.11000000.00110000.11000011 ⇔ 28.192.48.195

con máscara de subred:

11111111.11111111.11111111.00000000 ⇔ 255.255.255.0

tiene como identificador de subred los tres primeros bytes, y como identificador de Host el último byte. Esto es lo mismo que decir que el equipo pertenece a la subred 28.192.48.0, ya que la dirección IP con la parte de identificador de Host con todo ceros tiene un uso especial: identificar a la subred. Esta dirección está reservada para este uso y **nunca** podrá ser utilizada para identificar a un equipo.
Una forma alternativa de indicar la máscara de subred es indicando la cantidad de bits que son unos. Para el ejemplo anterior, la dirección IP quedaría completamente especificada del siguiente modo: **28.192.48.195/24**.

En general, para redes privadas, suele utilizarse un margen de direcciones IP establecido para ello y que no produce conflictos en Internet por no utilizarse como direcciones públicas. Los identificadores de subred típicos en estos casos son 192.168.1.x o bien 192.168.0.x. Cada equipo tendrá un identificador de equipo entre 1 y 254 en el lugar donde aparece la x (el 255 no se utiliza por tener un uso especial: la difusión a toda la subred)

De esta forma podemos tener direcciones IP en nuestra red que sean del tipo: 192.168.1.25, 192.168.1.1, 192.168.1.254, etc.

La comunidad de Internet ha definido **clases de direcciones IP** para dar cabida a redes de distintos tamaños. Cada clase de dirección se distingue por el primer conjunto de dígitos de su dirección.

Estas clases son:

- **CLASE A.** Redes cuyo identificador de subred son los 8 primeros bits. El primer dígito decimal tendrá un rango de 1 a 126 incluido.
- **CLASE B:** Redes cuyo identificador de subred son los 16 primeros bits. El primer dígito decimal tendrá un rango de 128 a 191 incluido.
- **CLASE C.** Redes cuyo identificador de subred son los 24 primeros bits. El primer dígito decimal tendrá un rango que va desde 192 hasta 223.

Veámoslas un poco más en detalle, analizando la figura 5.6:

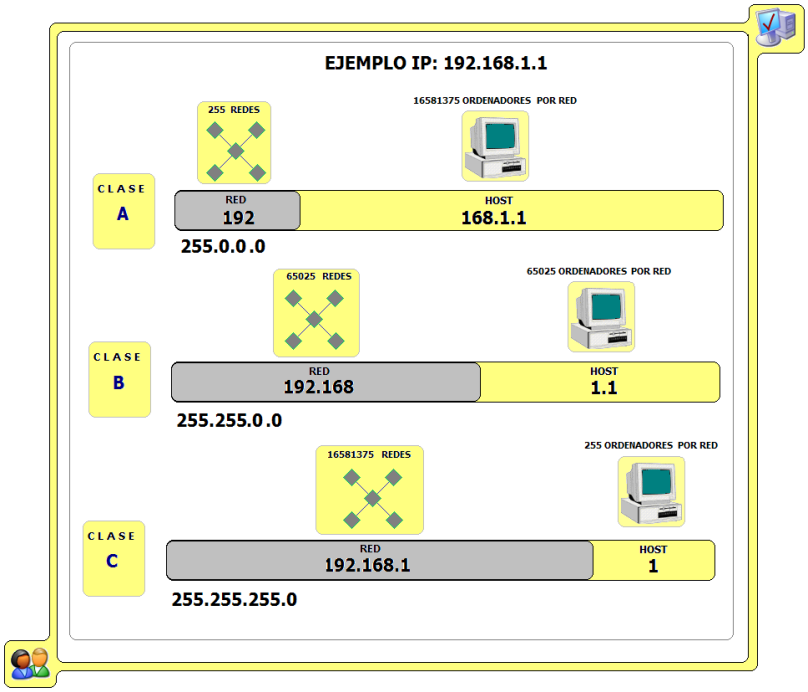


Fig. 5.6. Clases de redes TCP/IP.

CLASE A. Con este identificador de subred podremos montar 126 redes diferentes con un total de 16.777.214 hosts en cada una de ellas. Supongamos la siguiente dirección IP: 125.1.1.1

Se puede ver que es de tipo A debido al identificador de red. El resto de cifras corresponderán a los ordenadores de la red, es decir, a los identificadores de los hosts.

En esta caso, podríamos poner direcciones IP del tipo 125.x.x.x, siendo las tres X la identificación de cada puesto de trabajo o Host.

CLASE B. Las redes de tipo B tienen direcciones IP en las que las dos últimas cifras decimales se utilizan para poder identificar los hosts, en total 65.534, siendo el número de redes posibles de 16.384.

CLASE C. Utilizada normalmente para LAN. Permite definir 2.097.151 redes con un máximo de 254 puestos o hosts por red.

B. Protocolo de resolución de direcciones (ARP) 

Vamos a centrarnos ahora en cómo se realiza físicamente la comunicación entre dos equipos conectados a la misma LAN o subred. Cada uno de estos equipos tendrá, por tanto, una dirección IP, coincidiendo ambas en la parte correspondiente al identificador de subred.

El equipo que origina la comunicación generará un paquete de datos que entregará a la entidad de red, junto con la dirección IP del equipo destinatario. La entidad de red del equipo se encargará de localizar, a partir de la dirección IP destino, en qué subred se encuentra el equipo destinatario. En nuestro caso, esta subred será la misma que el equipo de origen, cosa que será fácilmente averiguada por la entidad de red al ver el identificador de subred.

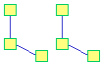
Una vez hecho esto, se trata de entregar el paquete de datos a la tarjeta de red para que ésta lo envíe a la tarjeta de red del equipo destinatario. Pero aquí surge el problema: las tarjetas de red sólo entienden de direcciones físicas, luego es necesario averiguar previamente cuál es la dirección física del equipo destinatario. De esto se encarga el protocolo de resolución de direcciones **ARP** (Address Resolution Protocol), cuyo funcionamiento es como sigue. El equipo origen manda un mensaje de difusión pidiendo que el equipo cuya dirección IP corresponda a la dirección IP de destino se identifique y envíe su dirección física (dirección MAC). De esta forma, una vez conseguida por el equipo origen la dirección física del equipo destinatario, ambas tarjetas de red se comunicarán entre sí para transmitirse la información.

C. Protocolo de configuración dinámica de Host (DHCP) 

Hemos visto cómo resulta imprescindible que cada equipo que quiera comunicarse utilizando el protocolo TCP/IP reciba una dirección IP única dentro de la red. La asignación de direcciones IP a los equipos por parte del administrador puede realizarse de dos formas: *estática* o *dinámicamente*.

Direccionamiento estático: de esta forma, se realiza una planificación previa de direcciones IP por parte del administrador, y una vez realizada se configura manualmente cada equipo con su dirección. Esta dirección IP será fija para cada equipo, al menos hasta que el administrador decida modificarlas.

Direccionamiento dinámico: cada equipo que se inicia en la red solicita una dirección IP de un servidor de direcciones IP, denominado *servidor DHCP*. Este servidor DHCP puede ser cualquier equipo de la red, aunque se recomienda seleccionar un equipo que cumpla funciones exclusivamente de servidor y no de estación de trabajo. Esta variante tiene la ventaja de que el administrador no tiene que configurar cada equipo individualmente, si no que basta con que configure correctamente el servidor, indicándole el *ámbito* de direcciones IP que puede entregar cuando le sea requerido, así como la máscara de subred asociada y eventualmente otros parámetros de configuración, como puertas de enlace.

D. División en subredes 

En muchas situaciones puede ser necesario que las direcciones IP de nuestras subredes privadas no pertenezcan a ninguna de las clases específicas anteriormente explicadas. Es decir, puede que la máscara de subred que nos interese sea diferente de las tres posibilidades vistas: 8, 16 ó 24 bits.

EJEMPLO:

Tenemos la subred de clase C de dirección 192.168.1.0/24, que puede albergar direcciones en el margen 192.168.1.1 – 192.168.1.254 (recordemos que las direcciones IP con valores de identificador de Host todo ceros o todo unos tienen un uso especial y nunca se asignan a equipos).

Sin embargo, nos interesa que estas direcciones IP se repartan entre dos subredes diferentes, por ejemplo, por cuestiones de seguridad. Para ello, procederemos a la división de la subred anterior en dos subredes diferentes. El proceso a seguir será el siguiente:

1. Ampliaremos la máscara en tantos bits como sea necesario para distinguir entre la cantidad de subredes que queremos obtener. En nuestro ejemplo, al querer obtener dos subredes, necesitaremos ampliar un único bit. En general, para obtener **m** subredes ampliaremos **n** bits, de tal forma que $\mathbf{2^n=m}$.

Dirección de subred original:

192.168.1.0 ⇔ 11000000.10101000.00000001.00000000

Máscara original:

255.255.255.0 ⇔ 11111111.11111111.11111111.00000000

Nueva máscara:

255.255.255.128 ⇔ 11111111.11111111.11111111.**1**0000000 (25 bits)
^
|
bit ampliado

2. Obtendremos los identificadores de las dos subredes resultantes de la división, combinando los bits que se han incorporado al identificador de subred. En nuestro caso se ha incorporado un único bit, luego tenemos dos combinaciones posibles: **0** y **1**.

Subred 1:

11000000.10101000.00000001.**0**0000000 ⇔ **192.168.1.0/25**

Subred 2:

11000000.10101000.00000001.**1**0000000 ⇔ **192.168.1.128/25**

3. Obtendremos el margen de direcciones IP asignables a cada subred combinando los bits correspondientes al nuevo identificador de Host:

Subred 1: 192.168.1.1/25 - 192.168.1.126/25
Subred 2: 192.168.1.129/25 – 192.168.1.254/25

Siguiendo el proceso de ejemplo, hemos obtenido dos subredes. Estas dos subredes, por supuesto, estarán incomunicadas entre sí, a menos que coloquemos un *enrutador* entre ambas, como veremos a continuación.

E. Encaminamiento IP

Las diferentes subredes TCP/IP se enlazan o conectan mediante dispositivos denominados **encaminadores, enrutadores** o **routers.** Estos dispositivos son los encargados de pasar la información de una subred a otra, en función de la dirección IP de destino de la misma. Veremos a continuación en detalle cómo se realiza el enrutamiento IP a través de los enrutadores.

Cada equipo (estación de trabajo o enrutador) en una subred TCP/IP tiene configurada lo que conocemos como una **tabla de encaminamiento**, que indica el siguiente equipo intermedio en la comunicación, en función de la dirección IP de destino de la información. Estas tablas de enrutamiento tienen el aspecto siguiente:

Subred destino	Máscara	Puerta de enlace	Interfaz	Métrica
192.168.2.0	255.255.255.0	192.168.1.2	192.168.1.1	1
192.168.1.1	255.255.255.0	192.168.1.1	192.168.1.1	1
0.0.0.0	0.0.0.0	192.168.1.200	192.168.1.1	1

La primera de las rutas de la tabla anterior se interpretaría de la siguiente forma: si la dirección de destino final del paquete de datos pertenece a la subred 192.168.2.0/24, entonces el paquete se enviará al equipo intermedio (enrutador) de dirección IP 192.168.1.2, y se hará a través de la interfaz del equipo local de dirección IP 192.168.1.1. Obviamente, los campos puerta de enlace e interfaz de cada ruta deben pertenecer siempre a la misma subred, en caso contrario no podría realizarse el envío directo del paquete de datos. El enrutador de dirección IP 192.168.1.2, a su vez, tendrá una tabla de enrutamiento que indicará a dónde reenviar la información en función de la dirección IP final, y así sucesivamente hasta que la información alcance el equipo destinatario final.

Las dos rutas siguientes que aparecen en la tabla ejemplo tienen un significado especial. En la segunda de ellas comprobamos que el campo puerta de enlace y el campo interfaz tienen el mismo valor. Esto indica que la subred de destino es la misma a la que pertenece el equipo que tiene dicha tabla configurada. Eso significa que la información ya ha llegado a la subred en la que se encuentra el equipo destino, luego se procede al envío directo a través de la subred.

La tercera ruta indica cuál es el siguiente equipo intermedio en caso de que la subred de destino (a la que pertenece la dirección IP final) no esté contemplada en ninguna de las rutas anteriores. Es lo que se llama la ***ruta por defecto***, y el equipo que aparece en el campo puerta de enlace es el que en general se conoce como **puerta de enlace predeterminada de la subred**.

En resumen, cualquier equipo que tenga que enviar información TCP/IP consultará en su tabla de encaminamiento hasta que encuentre la ruta a la que se adapta la dirección final de dicha información, y enviará los datos tal y como indique la ruta. La diferencia entre enrutadores y equipos finales es que estos últimos sólo envían información generada por ellos mismos y sólo aceptan información destinada a ellos mismos, mientras que los enrutadores son capaces de actuar como verdaderos equipos intermedios reenviando la información.

Vamos a entender esto un poco más a través de un ejemplo.

EJEMPLO:

Asumiendo la situación indicada en el siguiente esquema, la tabla de enrutamiento del enrutador A será la siguiente:

Subred destino	Máscara	Puerta de enlace	Interfaz	Métrica
192.168.3.0	255.255.255.0	192.168.1.2	192.168.1.1	1
192.168.1.0	255.255.255.0	192.168.1.1	192.168.1.1	1
192.168.2.0	255.255.255.0	192.168.2.1	192.168.2.1	1
0.0.0.0	0.0.0.0	192.168.2.100	192.168.2.1	1

El campo métrica indica el coste que tiene para el paquete ser reenviado. El objetivo es que a cada salto la información pierda tiempo de vida, de modo que se pueda descartar información que por algún motivo lleva demasiado tiempo en la red y pueda entorpecer su funcionamiento.

Los enrutadores de Internet configuran sus tablas de forma *dinámica*, es decir, a medida que se incorporan nuevos servidores y nodos, los enrutadores propagan esta información entre sí para adaptar sus tablas de enrutamiento, de manera que el funcionamiento global sea óptimo.

Sin embargo, los enrutadores que se configuran en entornos de subredes pequeñas y privadas suelen ser configurados de manera estática por el administrador, que tendrá la labor de actualizar las tablas

manualmente en caso de que cambie la configuración de la red. En particular, el comando ROUTE nos permite trabajar con las tablas de enrutamiento. El comando TRACERT nos permite averiguar los enrutadores intermedios para alcanzar un destino.

5.3. APLICACIONES SOBRE TCP/IP 

El protocolo de red TCP/IP ofrece a las aplicaciones instaladas en el equipo un acceso a la red a través de lo que se conoce como **puertos TCP**. Para que una aplicación pueda trabajar en un entorno de red necesita acceder a un puerto TCP. TCP asegura que las comunicaciones que se soliciten a través de estos puertos serán fiables y sin errores. Existen hasta 65536 puertos TCP, estando los 1024 primeros reservados a aplicaciones específicas. Son los que se conocen como puertos "bien conocidos". Por ejemplo, el puerto habitual para el servicio http es el puerto 80.

Además de TCP, sobre IP puede trabajar otro protocolo, el protocolo **UDP** (User Datagram Protocol). Este protocolo ofrece también puertos para que las aplicaciones puedan acceder a la red. Se diferencia con TCP en que es menos fiable y no corrige errores en la comunicación, pero tiene como ventaja ofrecer mayor rapidez. Un ejemplo de aplicación que utiliza UDP es el servicio de resolución de nombres DNS.

Algunas de las aplicaciones más conocidas que se han diseñado para trabajar sobre el protocolo TCP/IP son las siguientes:

- **FTP (File Transfer Protocol):** Nos permite intercambiar ficheros desde nuestra máquina con un servidor de ficheros.
- **HTTP (Hypertext Transfer Protocol):** Permite descargar páginas Web en nuestro navegador desde un servidor Web.
- **TELNET (Terminal Virtual):** Con esta aplicación podemos trabajar en nuestro terminal como si estuviéramos en un equipo remoto, que será el servidor telnet.
- **SMTP (Simple Mail Transfer Protocol):** Esta aplicación intercambia correo entre servidores de correo electrónico.
- **SNMP** (Simple Network Management Protocol): Gestiona de forma sencilla la red.
- **IGMP (Internet Group Message Protocol):** Gestiona grupos de difusión en Internet.
- **ICMP (Internet Control Message Protocol):** Este protocolo trabaja directamente sobre IP, y sirve para intercambiar información de control, por ejemplo, para actualizar tablas de encaminamiento.

5.4. SERVICIOS DE NOMBRES 

Hemos visto que cuando un equipo necesita intercambiar información a través del protocolo TCP/IP necesita conocer la dirección IP del equipo destino. Verdaderamente, sería muy complejo si los equipos tuvieran que recordar las direcciones IP de sus interlocutores. El proceso de comunicación se facilitaría enormemente para el usuario si este pudiera acceder a otros equipos en la red (por ejemplo, servidores Web, ficheros, etc) conociendo únicamente el nombre de los mismos. Esto se puede hacer gracias a la existencia de los servicios de nombres. El servicio de nombres más utilizado en redes TCP/IP, y en particular en Internet, es el servicio DNS.

A. DNS (Domain Name Server) 

B.

El servicio DNS asigna nombres jerárquicos del tipo *campo1.campo2.campo3.etc*, por ejemplo, **www.mcgraw-hill.es**. Cuando un equipo intenta acceder a otro a través de su nombre DNS, automáticamente se lanza en el equipo local la aplicación llamada **solucionador DNS**. Este solucionador consulta al servidor DNS, cuya dirección IP habremos configurado en nuestro equipo, para que le indique cuál es la dirección IP del equipo al que estamos tratando de acceder. Si este servidor no la conociera,

propagaría la consulta de forma jerárquica a otros servidores de Internet hasta encontrar la respuesta. Una vez que nuestra máquina tiene la dirección IP destino, puede acceder al puerto TCP que corresponda para lanzar la comunicación.

Los servidores DNS están configurados mediante registros DNS, que almacenan las correspondencias entre direcciones IP y nombres DNS. En resumen, es lo mismo conectar con un nombre concreto que con una dirección IP particular. Evidentemente es más fácil recordar un nombre que un número de 4 cifras, pero el resultado sería exactamente el mismo. Esto es lo que se denomina *resolución de nombres* de ordenadores, en los que cada ordenador está identificado con un nombre y una dirección IP. Da lo mismo comunicarse con otro ordenador a través de su dirección IP que a través de su nombre.

En algunos casos, si no tenemos instalado un servicio de nombres en la red, podemos resolver igualmente los nombres en direcciones IP mediante archivos almacenados en los equipos. Si no disponemos de un servidor DNS dentro de nuestra red, tendremos un fichero HOSTS grabado en cada ordenador con el aspecto siguiente (por ejemplo, en Windows):

192.168.1.1	**principal**
192.168.1.2	**contabilidad**
192.168.1.3	**compras**
192.168.1.25	**ventas**
192.168.1.200	**encaminador**

Si este fichero lo tenemos en cada ordenador en el lugar que le corresponde automáticamente cada ordenador que realice una petición a otro quedará identificado, ya que el ordenador que envía información se identifica y el que recibe sabe la dirección IP del que la ha enviado, ya que asocia al nombre de máquina la dirección IP correspondiente.

Este archivo tiene que estar situado en el mismo sitio que se encuentre TCP/IP. Concretamente en Windows está en el directorio **C:\WINDOWS**. En UNIX/LINUX se encuentra en **/etc**.

EJEMPLO:

Supongamos que contratamos con un proveedor de Internet un acceso. Este nos suministrará varios datos como nombre de usuario, clave de acceso, etc. Uno de los más importantes que nos suministra son las direcciones de servidores DNS. Esta información hace referencia concretamente a la dirección IP del propio servidor de Internet. Cuando configuramos el acceso a Internet, tendremos que configurar el servidor DNS que utilizará TCP/IP.

De esta forma cuando realicemos la conexión con el proveedor, lo que se hará será buscar un ordenador con la dirección IP especificada como DNS.

Una vez establecida físicamente la conexión con el proveedor, podemos querer ir a otro ordenador, es decir, visitar una página diferente a la que nos suministra nuestro proveedor por defecto. De esta forma cuando nosotros introducimos una dirección cualquiera: www.macgraw-hill.es, automáticamente se produce una búsqueda de la dirección IP equivalente al nombre especificado. Supongamos que la transformación resultante es 137.25.37.7.

¿Quién realiza esta transformación? La realizan precisamente los Servidores de Nombres de Dominio o servidores DNS que nos proporciona nuestro proveedor de Internet.

C. Servicio WINS D.

En redes que trabajan exclusivamente con sistema operativo Windows se puede utilizar un servicio de nombres conocido como WINS. Se diferencia con el servicio DNS en que no es jerárquico, sino plano. Utiliza también servidores, con la diferencia fundamental respecto a DNS de no necesitar una configuración manual por parte de un administrador. El servidor WINS va registrando los equipos a medida que éstos van enviando mensajes de difusión identificándose.

Conviene recalcar que este servicio de nombres sólo puede ser utilizado en entornos únicamente Windows, y nunca en Internet, ya que DNS es el servicio de nombres exclusivo en este caso.

5.5. ACCESO A INTERNET CON TCP/IP 

Cuando queremos acceder desde nuestro equipo o red particular a Internet necesitamos contratar un acceso a una red pública que nos permita acceder a cualquier equipo con dirección IP pública. Los accesos más habituales son mediante conexión telefónica o líneas ADSL y RDSI.

Cuando accedemos a través de redes telefónicas hay que utilizar un protocolo que enmascare los datagramas, dado que TCP/IP no está preparado para trabajar con redes telefónicas. En la actualidad el más difundido es **PPP** (Point to Point Protocol). Con este tipo de acceso necesitaremos un **módem** en nuestro ordenador que conectará con el número de teléfono de un **ISP** (Internet Service Provider). Este proveedor nos suministrará una dirección IP pública temporal para todo el tiempo que dure la comunicación, así como otros parámetros necesarios para la navegación (servidores DNS, etc).

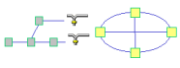
Si preferimos una conexión vía línea ADSL (Asymetrical Digital Suscriber Line), el suministrador nos instalará un enrutador al que conectar nuestro equipo o red local. Este **router ADSL** tendrá dos interfaces de red: la interna que se conecta con nuestra red local y la externa que tendrá una dirección IP pública fijada por el suministrador del servicio. Esta interfaz externa es la que se conecta a la línea ADSL. Este enrutador ADSL sustituirá las dirección IP del equipo privado que solicite comunicación por la suya propia, pública, es decir, hará la función de **PROXY**.

5.6. INSTALACIÓN DE UNA RED TCP/IP 

Vamos a recapitular los pasos necesarios para montar una red LAN utilizando el protocolo TCP/IP, en topología de estrella con par trenzado 10BASE-T/100BASE-T categoría 5 y con acceso a Internet:

- Realizar los segmentos de cables y conectar las clavijas.
- Conectar y cablear rosetas.
- Conectar segmentos de cable al HUB/SWITCH.
- Conectar el router como un equipo más al HUB/SWITCH.
- Configurar las direcciones IP de cada ordenador con su nombre correspondiente.
- Configurar el router con su dirección IP y su nombre correspondiente. Configurar también los datos de acceso a Internet (puerta de enlace predeterminada, servidores DNS, etc).
- Asignar la máscara de subred adecuada a cada equipo de la red.
- Configurar como puerta de enlace en cada ordenador la dirección IP del router.
- Configurar el fichero HOSTS con los datos de los ordenadores de la RED.
- Introducir en cada equipo las DNS suministradas por el proveedor de Internet.
- Introducir como dominio dentro de cada ordenador, el de nuestro servidor DNS si lo tenemos, y si no disponemos de él las DNS del proveedor de Internet.

De esta forma todos los equipos quedarán conectados en red y además tendrán acceso al exterior a través del router.

5.7. INTERCONEXIÓN DE LAN 

Hemos visto cómo es posible interconectar subredes TCP/IP a través de enrutadores o encaminadores convenientemente configurados. Conviene señalar ahora que también es posible interconectar diferentes LAN's a través de otros dispositivos, como los puentes.

Los **puentes** (**brigdes**) se utilizan para comunicar redes de área local con tecnologías diferentes (por ejemplo, una red Ethernet con una Token Ring). Los puentes son capaces de encaminar en función de direcciones físicas o direcciones MAC. Es importante que quede claro que el puente es completamente transparente para el protocolo TCP/IP: dos LAN conectadas a través de un puente pueden constituir una única subred TCP/IP.

Si lo que queremos es interconectar LAN's que siguiendo la misma tecnología MAC se diferencian en el medio físico (por ejemplo, una 10BASE-T con una red 10BASE-2) podremos utilizar un **transceptor**. De nuevo, el transceptor es completamente transparente para el protocolo TCP/IP: dos LAN conectadas a través de un transceptor pueden constituir una única subred TCP/IP.

En la figura siguiente pueden verse ejemplos de estos dispositivos.

Fig. 5.7. Transceptores de RED.

5.8. TIPOS DE SISTEMAS OPERATIVOS EN RED.

Teniendo en cuenta las necesidades de la empresa o de la organización en la que vamos a montar la red de ordenadores, los sistemas operativos, como software de red, pueden clasificarse en los siguientes:

Punto a punto (peer to peer). En este caso el sistema operativo de red se ejecuta en cada ordenador de los usuarios conectados. Cada usuario conectado a la red, puede compartir libremente los recursos que quiera de su ordenador para que el resto de los usuarios tenga acceso a ellos.

Lo que es evidente es que cada usuario solamente tendrá acceso a los recursos que el resto de usuarios dé a compartir a la red, además de los locales, es decir de todos los recursos de su ordenador. Este tipo de redes se denominan **de igual a igual** ya que todos los ordenadores son clientes y servidores a la vez.

En estos sistemas operativos la figura del administrador de red no es relevante, ya que es cada usuario el que se encarga de gestionar su máquina. En Windows, esta gestión recibe el nombre de **grupos de trabajo**.

Estos grupos de trabajo son eficaces, siempre y cuando el número de usuarios conectados no supere un número determinado (10 a 15), ya que a partir de este número, la gestión de los recursos de la red puede verse alterada por la mala gestión de los propios usuarios.

Supongamos que un usuario es el que tiene en su máquina todo el software de aplicaciones OFFICE. Si este usuario no va un día a su trabajo y no conecta su máquina, el resto de usuarios de la red, o del grupo de trabajo, no podrán hacer nada con este software. Es por lo que decimos que, hasta un número reducido de ordenadores, puede ser efectivo.

Con servidor. En este punto tendríamos que matizar si el sistema operativo es con servidor dedicado o no dedicado.

Un servidor dedicado, es aquel que suministra el software, archivos, y al que generalmente están conectados los recursos hardware para que sean utilizados por los usuarios de la red, con la particularidad, que este equipo, no se puede utilizar como puesto de trabajo independiente.
Un servidor no dedicado, es aquel que además de suministrar todos los recursos a los usuarios de la red, permite ser utilizado como puesto de trabajo independiente.

Lo normal en la actualidad es que todos los sistemas operativos en red estén diseñados para instalarlos en servidores que sean dedicados. Este tipo de sistemas operativos, se ejecuta en un ordenador específico, que se utiliza exclusivamente para tareas de red, como compartir archivos, comunicaciones y administración. La información está centralizada en el servidor, y es gestionada por un administrador, que establece las diversas políticas de acceso de los usuarios, la seguridad, la protección de datos y otros requerimientos.

Hoy en día la mayoría de los sistemas operativos son sistemas diseñados para poder trabajar en RED. Ocurre que unos son realmente sistemas operativos en RED como UNIX, NOVELL, Windows NT Server, Windows 2000/2003 Server, etc., pero otros aunque sirven para trabajar en red, no están diseñados específicamente para estas labores.

Los sistemas operativos en red son los que tienen la configuración de todas los usuarios de la red; nombre y tipos de usuarios conectados; privilegios de conexión al ordenador central; horarios de conexión; etc.

Hablaremos de varios tipos de sistemas operativos de RED. Concretamente hablaremos de NT Server, 2000/2003 Server y UNIX/LINUX. De los sistemas operativos Punto a Punto, hablaremos en la siguiente unidad, en los denominados grupos de trabajo en Windows.

5.9.. CONSIDERACIONES FINALES 

En esta unidad acabamos de ver como trabajan las redes, especialmente las de área local. Hemos dato especial importancia a las especificaciones, ya que a la hora de decidir el tipo de red que queremos montar, tendremos que tener en cuenta circunstancias de este tipo.

En particular, hemos hablado del protocolo TCP/IP y de los protocolos que lo componen, funciones específicas de cada uno de ellos y configuración, especialmente centrada, en redes de área local.

Por último indicar que los servicios WINS, DHCP y DNS son servicios que en la actualidad se utilizan mucho, tanto, que sin darnos cuenta, nuestras redes no serian capaces de funcionar de forma efectiva sin alguno de estos servicios.

5.10. CUESTIONES

CUESTIONES

CUESTIONES OBJETIVAS

CONTROL SEGUNDA EVALUACIÓN: REDES

1.- El cable utilizado en las especificaciones 10BROAD-36 es del tipo…..
a) UTP
b) AGP
c) BNC
d) RJ45
e) RG59 CATV

2.- Una de las especificaciones que más han sido utilizadas es:
a) 10BASE-2 o red fina de Ethernet.
b) 10BASE-5.
c) 10BASE-T.
d) 100BASE-FX.
e) 1000BASE-T.

3.- ¿Cuales de las siguientes son especificaciones de redes Token Ring?
a) Tipo1. Cable apantallado conteniendo dos hilos de par trenzado 22 AWG.
b) Tipo3. Incluye cuatro cables macizos sin apantallar de par trenzado de 22 o 24 AWG.
c) Tipo5. Cable de fibra óptica de dos fibras.
d) Tipo8. Cable par trenzado apantallado de 26 AWG para usar bajo moqueta.
e) Todas son ciertas.

4.- Las especificaciones ARCNET tienen características tales como…..
a) Poder transferir datos a una velocidad de 2,5 Mbps
b) Soportar longitudes de cable de hasta 675 metros.
c) Soportar fibra óptica y par trenzado
d) Son ciertas a,b y c.
e) Son ciertas a y b.

5.-Una de las características principales una red con especificación Arcnet es que:
a) Que utilizan HUB pasivos como conmutadores entre ordenadores remotos.
b) Que utilizan HUB activos para distribuir señal.
c) Que utilizan cable Coaxial RG62 AU.
d) Son correctas a y b
e) Son correctas a, b y c.

6.- ¿Cuantos equipos puedo integrar en una misma red que tiene una máscara de subred de 31 bits?
a) 255 ordenadores.
b) 31.
c) 9.
d) 1.
e) Ninguno, ya que esa máscara de subred no existe.

7.-Cuantos ordenadores puedo integrar en una misma red si la máscara de subred utilizada es la siguiente: 11111111.11111111.11111100.00000000 ?
a) 1024

b) 255
c) 65536
d) 16777216
e) Tantos como quiera.

8.- ¿Puedo tener dos redes (Windows/Linux con TCP/IP) diferentes de tipo C (máscara de 24 Bits) conectadas entre ellas?
a) Si, siempre que quiera.
b) Si, pero necesitare un Router.
c) No, ya que las redes de tipo C no "pueden verse" entre sí.
d) Si, pero necesitare un Bridge.
e) Si, pero necesitaré una Pasarela.

9- ¿Para que se utiliza el servicio DHCP?
a) Para asignar en forma estática direcciones IP
b) Para asignar de forma dinámica direcciones IP.
c) Para conectar varios ordenadores de dos redes diferentes.
d) Son correctas 1 y 3
e) Son correctas 2 y 3

10.- ¿Cuantos protocolos puedo tener instalados en mi ordenador?
a) Tantos como quiera, siempre y cuando el sistema operativo los identifique.
b) Solamente TCP/IP, NetBEUI y IPX/SPX.
c) Solamente uno, ya que Windows no reconoce más de una tarjeta de red.
d) Uno por cada tarjeta de red instalada.
e) Todas son falsas.

11.- ¿Quién determina el tipo de red (A, B o C) con el que se integra un equipo en red?
a) El protocolo.
b) La dirección IP.
c) La máscara de subred.
d) EL adaptador de red.
e) Todas son falsas.

12.- La dirección IP 192.168.1.200 siempre será una dirección para una red de tipo:
a) A
b) B
c) C
d) Cualquiera de ellas, dependiendo de la máscara de subred.
e) Puede ser de tipo A o B, dependiendo si tenemos instalado Router y acceso a Internet.

13.- El servicio WINS se utiliza para la resolución de nombres de dominio en….
a) Redes mixtas.
b) Redes LINUX.
c) Redes Windows.
d) Internet.
e) Todas son falsas.

14.- El tipo de red (peer to peer) referencia a una red….
a) Con servidor.
b) Con terminales con emulación.
c) Con servidor y terminales puros.
d) Punto a punto.
e) Todas son ciertas.

15.- ¿Cuando utilizamos el fichero HOST para resolver los nombres de equipo en una LAN?
a) Cuando no tenemos instalado el servicio DHCP.
b) Cuando no tenemos instalado el servicio DNS.
c) Cuando tenemos instalado el servicio DHCP y DNS.
d) Solamente cuando trabajamos en redes con servidor, que es el que contendrá este fichero.
e) Todas son falsas.

16.- El protocolo utilizado para visualizar páginas WEB en nuestro equipo a través del navegador es….

a) FTP
b) SMTP
c) TELNET
d) HTTP
e) Cualquiera de los anteriores, siempre y cuando estén configurados para esta función

CUESTIONES A DESARROLLAR

1. Comparar las diferentes topologías de red: estrella, física y bus.
2. Dibujar el esquema de colores necesario para realizar latiguillos de cable UTP con conector RJ-45 directos y cruzados en 100BASE-T.
3. Diferencias entre enrutador, puente y transceptor.
4. Disponemos de 90000€ para montar una red en un edificio con las siguientes características:

- un despacho de director
- cinco aulas de informática
- diez despachos de servicios

Queremos informatizar la empresa sabiendo que los ordenadores a montar y las necesidades a cubrir son las siguientes:

- el despacho del director tendrá un ordenador servidor de red. En él estará ubicado todo el software que se utiliza en la empresa, se validarán los usuarios y tendrá siempre conectada una impresora láser de altas prestaciones compartida por todos los usuarios de la red. Este ordenador tendrá acceso a Internet.

- cada aula informática tendrá
  - un ordenador para el profesor conectado al ordenador principal
  - una impresora de color conectada al ordenador del profesor
  - diez ordenadores de alumnos conectados en red entre sí y con el ordenador del profesor. Todos tendrán acceso a Internet pero no a los demás recursos de la red
  - sólo el ordenador del profesor tiene acceso a los recursos hardware y software del ordenador principal

- los ordenadores de los despachos tendrán acceso al ordenador principal, a la impresora principal y a Internet. Estarán en red entre sí, con los ordenadores de profesor y con el ordenador principal.

La distribución física de los ordenadores es la siguiente:

- cada aula tiene 50 m^2 (10x5)
- desde cada aula al ordenador principal hay una media de 100 mts
- desde cada despacho al ordenador principal hay una media de 50 mts

Se trata de analizar los requisitos hardware para realizar la configuración de la red informática, teniendo en cuenta que el software del que dispone la empresa es:

- Windows 2000 Server para el ordenador principal
- Windows XP Prof. para ordenadores de despachos y aulas
- Software proxy
- Resto de software necesario

El análisis consiste en realizar un presupuesto y proyecto de cableado, asumiendo que la empresa no tiene nada (serán necesarios cables, hubs, switchs, contratación de líneas telefónicas, etc).

En este proyecto no se considerará la mano de obra ni material que no sea imprescindible, tales como canaletas, tomas de corriente, etc. Sólo se considerará el material informático hardware (cableado, ordenadores, etc).

Para realizar este ejercicio recurriremos a información de varios proveedores para adaptar de la mejor forma posible el presupuesto de 90000€, cumpliendo la normativa vigente.

PLANTILLAS PARA EL DISEÑO.

Nº	*Nombre de ordenador*	PUERTA ENLACE / PROXY	DIRECCION IP	MASCARA DE SUBRED	GRUPO DE TRABAJO	IMPRESORA LOCAL / CLAVE DE ACCESO	IMPRESORA EN RED / CLAVE DE ACCESO	UNIDADES LÓGICAS	TOMA INFORMATICA	HUB O SWITCH Nº
1										
2										
3										
4										
...										
65										
66										

Plantilla de identificación de impresoras:

IMPRESORA	MODELO	TIPO	NOMBRE DE IMPRESORA EN RED	ORDENADOR EN EL QUE ES INSTALADA
PRINCIPAL				
AULA 1				
AULA 2				
AULA 3				
AULA 4				
AULA 5				

5. Imagina la disposición de subredes físicas independientes que se indica en la figura. Diseña las tablas de enrutamiento necesarias en los enrutadores IP R1, R2, R3, y R4 para que exista interconexión total entre las subredes. Supón que deseas conectar todos los equipos de todas las subredes a Internet. Diseña una posible solución, asumiendo que todas las direcciones IP de las subredes son privadas.

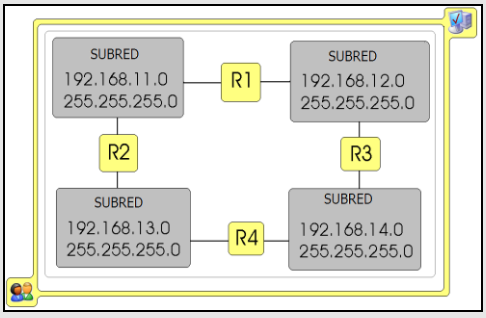


FIGURA 1 CUESTIONES

¿Se te ocurre una configuración física más eficiente en la interconexión de estas cuatro subredes entre sí que la propuesta? Coméntala.

6. Tenemos una única subred física de dirección IP 152.77.0.0 (no procedente de ninguna subdivisión) que queremos dividir en cinco subredes físicas independientes, donde cada subred deberá alojar 5000 equipos como máximo. Determina las direcciones de subred resultantes con sus respectivas máscaras, así como el rango de direcciones IP que pueden asignarse en cada una de las subredes.

7. Imagine la disposición de subredes siguiente:

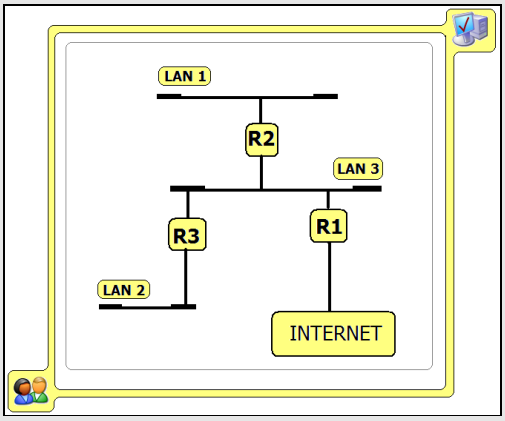


FIGURA 2 CUESTIONES

El enrutador R1 tiene una dirección pública de Internet, mientras que el resto de los equipos tiene direcciones privadas en el rango 192.170.0.0/16. Las subredes LAN 1 y LAN 2 albergarán la mitad de equipos que la red LAN 3, cubriendo entre las tres subredes todo el rango IP propuesto. Diseñar la distribución de direcciones IP por subred y configurar las tablas de enrutamiento para R1, R2 y R3 en los casos siguientes:

a.- R2 y R3 tienen software proxy
b.- R2 tiene software proxy y R3 no
c.- R3 tiene software proxy y R2 no

Supón que quiere que todas las direcciones IP privadas sean asignadas automáticamente. Proponga una planificación de servidores DHCP.

8. Imagina la siguiente distribución:

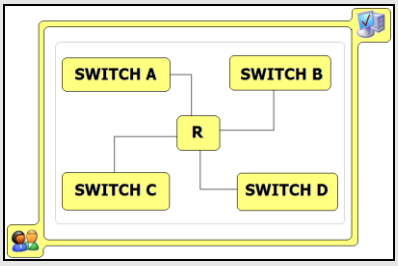


FIGURA 3 CUESTIONES

Disponemos de un rango IP de la forma 192.168.0.0/16 para utilizar en las subredes A, B, y C, y de un conjunto de direcciones públicas de la 60.25.3.4 a la 60.25.3.8, para asignar a la subred D. Las subredes A y B deben tener la mitad de tamaño que la subred C. Haga la distribución de direcciones IP para las subredes, configure la tabla de rutas del router, y proponga un acceso a Internet para el conjunto. En cada subred queremos un equipo que monitorice los accesos a Internet de los equipos, ¿qué solución propone para llevar esto a cabo?