

Implantaciones de redes de área local

Javier Fernández Rivera - www.aurea.es

El hardware de las LAN

Las tarjetas de red: también llamados adaptadores de red o tarjeta de interfaz de red (Network Interface Card, NIC), se insertan en el bus de comunicaciones del ordenador. En la mayoría de ordenadores personales la tarjeta de red no viene incorporada.

Las tarjetas de interfaz también pueden utilizarse en minicomputadoras y mainframes.

La tarjeta de interfaz obtiene la información de la PC, la convierte al formato adecuado y la envía a través del cable a otra tarjeta de interfaz de la red local.

Funciones de NIC (tarjeta de red)

1. Comunicaciones de host a tarjeta
2. Buffering
3. Formación de paquetes
4. Conversión serial a paralelo
5. Codificación y decodificación
6. Acceso al cable
7. Saludo
8. Transmisión y recepción

Una tarjeta de red es un dispositivo electrónico que consta de las siguientes partes:

- Interface de conexión al bus del ordenador.
- Interface de conexión al medio de transmisión
- Componentes electrónicos internos, propios de la tarjeta.
- Elementos de configuración de la tarjeta: puentes, conmutadores, etc.

Las tarjetas se deben conectar a un slot de comunicación del ordenador en sí. Por tanto un slot es el conector físico donde se <pincha> una tarjeta.

Los distintos tipos de slots y BUSES internos que se encuentran en el mercado son:

1. EISA: Es un trozo más grande que ISA. Es un BUS de 32 bits y la velocidad es de 33Mps
2. MCA (micro channel arquitectura): Bus de 32bits, alcanza la velocidad de 40Mps.
3. NUBUS: De 32bits, propia de los apple.
4. VESA BUS LOCAL: De 32bits alcanza los 132Mbps. Supuestamente era el mejor pero tiene un problema, que las tarjetas son muy largas.
5. PCI: es el que se usa en la actualidad. Tiene 32bits y 120Mps de velocidad.
6. AGP: No se usa para redes, solo para gráficos de 32bits y se logran 170/180Mps.

Además de tener un conector, hay que saber para que tipo de red se va a comprar la tarjeta. Normalmente no son compatibles las tarjetas Ethernet con las TokenRing.

1. **Tarjetas 10 base 5:** Son tarjetas que usan cable coaxial o gordo.
2. **Tarjetas 10 base 2:** Usan cable coaxial fino, normalmente el R6-58 o R6-59.
3. **Tarjeta 10 Broad 36:** Usan cable coaxial de banda ancha.

4. **Tarjetas 10 base T:** Son tarjetas que aceptan el RJ45 a 10. Cable de 4 pares de hilos
5. **Tarjetas 100 base T:** Tarjetas que alcanza los 100 Mb, usan también el RJ45.
6. **Tarjetas 10 base F:** Fibra óptica. Codificación Manchester.
7. **Tarjetas con varios conectores:** Sirven para varios tipos de cables. En ellas es necesario configurar el parámetro "Tipo de transceptor".

Configuración de las tarjetas de red.

Dependiendo del NOS que usemos tendremos que configurar la tarjeta de red. Para poder instalar una tarjeta de red para un NOS esta debe disponer de un driver específico para dicho NOS. O bien ser compatible con alguno de los drivers existentes.

Cuando conectamos una tarjeta de red a un ordenador para que esta funcione necesitamos instalar un driver en función de estos drivers podemos distinguir las especificaciones:

- NDIS: Son típicamente de windows.
- ODI: Las usa novel y apple.

Estas especificaciones interactúan entre la capa de transporte y de red.

Existen tarjetas de red que llevan incorporada una memoria ROM y dentro de esa memoria lleva un pequeño programa que permite cargar el SO de red remotamente. Últimamente las tarjetas de red usan una tecnología llamada plug and play (Poner y funcionar, con solo instalarlas ya las detecta el SO y pasan a funcionar). No obstante estas tarjetas no siempre funcionan correctamente por lo que a veces es necesario configurarlas manualmente. Esto mismo sucede con las tarjetas que no son plug and play.

Los principales parámetros de configuración de una tarjeta son:

1. **IRQ:** (Configura la interrupción). Este parámetro indica el número de línea de interrupción con el que se avisa al NOS y la tarjeta que se va a producir un evento de comunicación entre ellos. Por ejemplo cuando se mandan datos a una tarjeta el IRQ o número de línea procede a una interrupción de esta forma avisa al NOS que hay datos preparados en la tarjeta para ser procesados. Los valores más comunes para IRQ, son: 3, 5, 7, 9 y 11.
2. **DMA:** (Access memory direct) Acceso directo a memoria. Cuando la tarjeta necesita transmitir datos a la memoria central "RAM" un controlador hardware llamado DMA pone de acuerdo a la tarjeta y a la memoria para que se produzca una comunicación ordenada sin intervención del procesador. Se debe definir que canal de DMA va a usar, y que no este usado por otra tarjeta. Este sistema de transferencia se usa poco en las tarjetas modernas.
3. **Dirección de E/S:** Es una dirección de memoria donde escriben y leen el procesador central del sistema y la tarjeta, de modo que les sirve de bloque común de memoria para el intercambio de datos. Es una especie de buffer común para el procesador y la tarjeta. La dirección de entrada y salida se suele expresar en hexadecimal, por ejemplo DC000H.
4. **Dirección del puerto de E/S:** El puerto de entrada y salida es un conjunto de bytes de memoria en los que el procesador central y periféricos intercambian datos de entrada y salida y del estado en el que se efectúan las operaciones.
5. **Tipo de transceptor:** Algunas tarjetas de red incorporan varias salidas con diversos conectores, de modo que se pueden escoger entre ellos en función de las necesidades. Algunas de estas salidas necesitan transceptor externo y hay que indicárselo a la tarjeta cuando se configura.

A la hora de introducir un periférico o tarjeta en un slot. Es bueno seguir el siguiente orden.

- ❖ Primero la tarjeta de video o controladora gráfica.
- ❖ Después la tarjeta de red.
- ❖ Y en tercer lugar la tarjeta de sonido.

Estaciones de trabajo: Una estación de trabajo o workstation. Es cada uno de los nodos que forma parte de la red desde la que trabajan los usuarios.

Cada uno de estos nodos o terminales debe conservar la función de poder trabajar independientemente, realizando sus propios procesos.

Una estación de trabajo no comparte sus propios recursos con otras computadoras.

Su función principal es: Permitir tener acceso a la red.

Las aplicaciones que corren o se ejecutan en las estaciones de trabajo. Suelen funcionar como clientes.

Normalmente una estación de trabajo suele ser una estación normal y dependiendo del tipo de función que valla a realizar debemos evaluar los siguientes parámetros:

- Potencia de proceso: Viene en función del procesador que tengamos.
- Sistema grafico: Sería la controladora o tarjeta grafica.
- Disco duro: Si es en red podemos prescindir de disco duro.
- Tarjeta de red: hay que tener en cuenta el tipo de conexión que se va a usar para acceder a la red

Cluster: Es la unidad mínima de lectura/escriura.

Servidor de red: Es un ordenador que esta conectado a la red y que brinda una serie de servicios al resto de los nodos. Son como ordenadores mas o menos normales, pero con la diferencia de que pueden compartir recursos y dar servicios. Los servers pueden ser de 2 tipos: dedicados o no dedicados, dependiendo del tipo de recursos que ofrezcan. Normalmente los tipos de servidores obtienen su nombre en base a lo que sirvan o compartan, así pues si comparte una impresora, se le llama servidor de impresora, etc.

Un Server dedicado: es aquel que no puede trabajar como estacion de trabajo.

Las características fundamentales que se deben tener en cuenta a la hora de instalar un servidor, deben ser:

1. **Potencia de proceso:** El tipo de procesador que lleva el Server (actualmente los servers suelen ser multiprocesador).
2. **La memoria RAM**
3. **EL disco duro**

Normalmente un Server suele tener los discos duros de tipo SCSI es mucho más rápido y puede manejar muchos más discos.

- ❖ RAID: (sistema de copia de respaldo automático). Hace una copia en otro disco.
- ❖ USB: Conexiones que permiten conectar dispositivos en caliente sin apagar el ordenador.

Clasificación de los servers

Según lo que ofrecen a la red

- Servidor de ficheros
- Servidor de comunicaciones
- Servidor de impresora

En función a la red que se conectan

- LAN
- MAN
- LAN--WAN

Cableado: La LAN debe tener un sistema de cableado que conecte las estaciones de trabajo individuales con los servidores de archivos y otros periféricos. Si sólo hubiera un tipo de cableado disponible, la decisión sería sencilla. Lo cierto es que hay muchos tipos de cableado, cada uno con sus propios defensores y como existe una gran variedad en cuanto al costo y capacidad, la selección no debe ser un asunto trivial. Tipos de cables disponibles:

- a. **Par de cables trenzados:** Es con mucho, el tipo menos caro y más común de medio de red LAN.
 - i. UTP
 - ii. STP
- b. **Cables coaxiales:** Es tan fácil de instalar y mantener como el cable de par trenzado, y es el medio que se prefiere para las LAN grandes.

- i. Coaxial grueso:
 - ii. Coaxial fino
 - iii. Otros cables coaxiales: twinaxial o el dual coax.
- c. **Fibra óptica:** Tiene mayor velocidad de transmisión que los anteriores, es inmune a la interferencia de frecuencias de radio y capaz de enviar señales a distancias considerables sin perder su fuerza. Tiene un costo mayor.
- Para los cables se recomienda que se compre lo mejor, lo mas caro, lo mas bueno.

Conectores: Dependen del tipo de red que se instale, de su topología.

- a. **RJ11, RJ12, RJ45:** Estos son los conectores que se suelen usar con cables UTP o STP.
 - b. **AUI, DB15:** Se usa en la formación de topologías en estrella con cables de pares o para la conexión de transceptores (encargados de adaptar la señal pasándola de un tipo a otro, coge la señal de un cable coaxial a otro de par trenzado).
 - c. **BNC:** Son los conectores que se usan para el cable coaxial fino, típico de ethernet .
 - d. **T (Coaxial):** Es el conector para cable coaxial de una red LAN con topología que sirve de BUS. En los extremos finales se debe poner la llamada resistencia (otro conector).
 - e. **DB25 y DB9:** Son conectores usados para transmisiones en serie.
- Es importante comprar un buen cable, de lo mejor que se pueda.

Otros elementos físicos de una red LAN.

1. **Estaciones de trabajo o terminales:** Cada ordenador conectado a la red.
2. **Servidor:** El equipo principal de la red.
3. **Baluns y transceptores:** Se encargan de pasar la señal de un cable de un tipo a otro de tipo distinto. El uso de estos dispositivos produce una pequeña perdida en la señal.
4. **Rack:** Es un armario que recoge de modo ordenado todas las conexiones y los extremos de cables finales de toda la red LAN.
5. **Latiguillos:** Son cables cortos para prolongar los cables entrantes o salientes del rack o terminal.
6. **Canaleta:** Es una estructura metálica o de plástico, adosada al suelo o pared. Los cables se disponen en su interior. De esta forma evitamos posibles deterioros indeseados o saber con facilidad donde se encuentran los cables.
7. **Placas de conectores y rosetas:** Son conectores que se insertan en las canaletas o se adosan a la pared y que sirve de interface entre el latiguillo que lleva la señal al nodo y el cable de red.
8. **ROUTER:** Es el dispositivo necesario para conectar nuestra red LAN a internet. La palabra ROUTER viene de RUTA. Lo que hace este dispositivo es enrutar los paquetes, encaminarlos para su salida a internet,. Los ROUTERS solo son compatibles con conectores RJ45.
Supongamos que tenemos una red LAN montada en cable coaxial y ponemos un router. Necesitaríamos también un transceptor para cambiar la señal de cable coaxial a par trenzado y que este cable de par trenzado conecte con su conector RJ45 al router.
9. **BackBone:** Este es el cable principal de la red LAN, es el cable del que se ramifican el resto de cables. Vendría a ser como el tronco de un árbol. Si es el cable principal debe ser bueno. Así que es importante comprar lo mejor del mercado, de el dependerá en gran medida la calidad de conexión y transferencia.
10. **HUB o concentradores :** Es el dispositivo controlador que gestiona y comunica las señales de cada ordenador conectado.
11. **Repetidores:** En caso de perdida de señal amplifica y retransmite la señal de red.
12. **Puentes:** Sirven para conectar redes del mismo tipo (LAN con LAN).
13. **Pasarelas:** Comunican redes de distinto tipo (LAN con WAN). Son llamados también routers, en español enrutadores, que enrutan, que encaminan, marcan una ruta.
14. **Compuertas:** Sirve para comunicar redes con tecnologías incompatibles, por ejemplo tenemos una red LAN con ordenadores IBM y otra red LAN con ordenadores MAC. Para poder comunicarlasy necesitaríamos una compuerta para hacer esa comunicación compatible.

Software de las LAN

El sistema operativo de red

NOS: Después de cumplir todos los requerimientos de hardware para instalar una LAN, se necesita instalar un sistema operativo de red (Network Operating System, NOS), que administre y coordine todas las operaciones de dicha red. El sistema operativo de red.

Un sistema operativo de red, es el software que hace que un equipo informático tenga la propiedad de comunicarse con otros equipos constituyendo así una red. A veces el software de red viene integrado con el sistema operativo, otros sistemas operativos menos avanzados necesitan una instalación añadida.

Los servicios que el NOS realiza son:

Soporte para archivos: Esto es, crear, compartir, almacenar y recuperar archivos, actividades esenciales en que el NOS se especializa proporcionando un método rápido y seguro.

Comunicaciones: Se refiere a todo lo que se envía a través del cable. La comunicación se realiza cuando por ejemplo, alguien entra a la red, copia un archivo, envía correo electrónico, o imprime.

Servicios de soporte: Aquí se incluyen todos los servicios especiales como impresiones, respaldos en cinta, detección de virus en la red, etc.

Evolución de los NOS.

Los sistemas operativos de red han evolucionado desde las primeras redes de área local.

MSDOS: nació en el año 81 no tiene ningún tipo de posibilidad de comunicación si queríamos intercambiar información con ordenadores equipados con este SO (sistema operativo) se necesitaban adquirir e instalar unos programas que permitían cambiar información entre ordenadores con este SO por los puertos serie RS232, o por los puertos paralelos centronix.

A partir de las últimas versiones de MSDOS se integraron los programas de comunicación en el propio sistema operativo, convirtiéndolo así en un "NOS".

Más adelante y con el paso de los años ya empezaron a surgir otros SO que venían con el software de red integrado, eran ya propiamente dichos NOS, sistemas operativos de red. Hablamos de casos como: LINUX, Windows NT, MacOS.

Conceptos

Grupo de trabajo: Son el total de recursos compartidos por un grupo de usuarios de forma que la información o los recursos de ese grupo de usuarios sea fácilmente accesible para los usuarios pertenecientes al grupo de trabajo.

Dominio: Es una extensión del concepto grupo de trabajo a la cual se le ha añadido una serie de funcionalidades, como son:

- La centralización de la gestión de la red.
- Control de usuarios (logins, IDs) y contraseñas (passwords).
- La jerarquización de los recursos.
- etc.

Sistema de redes Cliente-Servidor: Los servers suelen ser equipos dedicados y normalmente brindan los servicios al resto de equipos que suelen ser estaciones de trabajo.

Redes entren iguales

PEER-TO-PEER en estas redes no existen servidores definidos y cada uno de los equipos puede compartir sus cosas.

Ejemplos de SO

Windows 9X = entre iguales

Windows NT = cliente servidor.

LINUX o UNIX: cliente-servidor

MacOS: entre iguales.

Protocolos de diferentes redes

Protocolos en las redes UNIX o LINUX: Es un sistema operativo que tradicionalmente se ha usado en organizaciones educativas debido a que no es un sistema propietario. Esto quiere decir que lo pueden desarrollar cualquiera. LINUX toolbar licencia el SO como open code (código abierto). Es un sistema multiusuario.

El protocolo de comunicación usado por UNÍS y por tanto también por LINUX es el: TCP/IP

El protocolo TCP/IP: Estamos hablando del protocolo principal de la comunicación de sistemas informáticos. Este protocolo es el más usado para comunicar redes de computadores. Gran prueba de ello es internet. Este protocolo que se esconde bajo el nombre de TCP/IP a menudo es confundido como si fuera un único protocolo. Pero no es así, el protocolo TCP/IP es el conjunto de una serie de protocolos que derivan de los dos protocolos principales, por un lado TCP (transfer control protocol) y por el otro IP (internet protocol).

Historia del TCP/IP: Todo comenzó cuando DARPA inicio un programa de investigación, que trataba de comunicar redes de distintos tipos y características. El proyecto se basaba en transmitir paquetes con información interconectado redes de distintas clases. De este proyecto derivaron dos redes, una dedicada a la investigación, que fue llamada ARPANET, y otra de uso exclusivamente militar, llamada MILNET.

Para transmitir la información entre las redes o en una misma red, se diseñó el protocolo de internet y distintos tipos de protocolos para el control de transmisión. Mas adelante estos protocolos fueron englobados en los dos principales que dan nombre al protocolo referido (TCP/IP).

El NOS UNÍS incluyo este protocolo en su versión 4.2 de Berkeley. A partir de entonces ARPANET desapareció oficialmente y INTERNET se popularizó.

El modelo básico de internet usa los llamados programas cliente-servidor. Esto es que un programa (cliente) requiere de los servicios de un servidor y este se los proporcionan. Un ejemplo de programas cliente-servidor sería el archifamoso mIRC cliente de IRC. En este caso el cliente es el programa mIRC y el servidor es de IRC (chat).

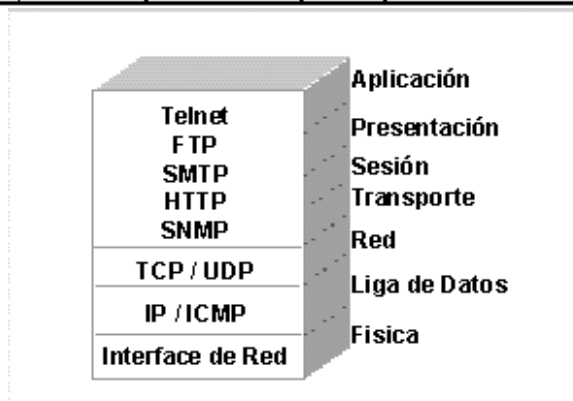
El protocolo TCP/IP trabaja sobre este tipo de aplicaciones. De ahí parte de su importancia.

Este protocolo no sigue la arquitectura OSI y dispone de 4 capas:

- Interface de red.
- Internet
- Transporte
- Aplicaciones

Representación gráfica de la estructuración del protocolo TCP/IP, creadas por: Juan Salvador Miravet Bonet

Aplicación						
Presentación	TELNET	FTP	SNMP	SMTP	DNS	HTTP
Sesión						
Transporte	TCP					
Red	IP					
Liga de Datos	802.2				X.25	LLC/SNAP
	802.3	802.5		LAPB		ATM
Física	Ethernet	Token Ring	FDDI	Línea Síncrona WAN		SONET



El protocolo TCP/IP está compuesto por 2 protocolos. El IP (internet protocolo) que se corresponde con la capa de red del sistema OSI.

El protocolo IP tiene un problema que es que carece de seguridad en la entrega de paquetes, lo que quiere decir que necesita otro protocolo para poder establecer una comunicación. Cuando se diseñó este protocolo se hizo con la idea de enviar paquetes que pudiesen circular por diferentes tipos de redes pero para poder enviar información necesitan un protocolo de transporte, y es aquí donde aparece el protocolo TCP ("transfer control protocol" protocolo de control de transferencia).

Un datagrama o un paquete IP está compuesto por dos partes: una cabecera y un campo de datos.

La cabecera está formada por una parte fija de 20 bytes y el resto variable y entrecabecera y cuerpo no puede superar los 64kB. Las partes de las que consta la cabecera del protocolo IP son:

1. **Versión:** Es la versión del protocolo IP usado en la transmisión. Su función es, hacer compatibles y que funcionen las distintas versiones de este protocolo.
2. **Campo IHL (internet header long):** Nos indica la longitud que tiene la cabecera.
3. **Tipo de servicio:** Define el tipo de servicios que se requiere para la transmisión. Decide si es más importante la seguridad o la rapidez.
4. **Longitud total del mensaje (datagrama):** Menos siempre de 64kB
5. **Identificación:** Es un número que indica el fragmento del datagrama que se está enviando. Este número indica que fragmento se está enviando.
6. **BIT DF:** Este bit si tiene valor 1 indica que el datagrama no puede ser fragmentado
7. **BIT MF:** Este bit tiene un valor 1 en todos los fragmentos de un datagrama dividido, excepto en el último.
8. **Desplazamiento de fragmento:** Indica la posición real en la que debe ser insertado un fragmento de mensaje pero que al final quede compuesto correctamente.
9. **Tiempo de vida:** Este campo indica un valor que es el tiempo de vida de un paquete. Que si se pierde se auto destruye a un tiempo determinado. El tiempo máximo que se le puede aplicar para su destrucción es de 255 segundos.
10. **Protocolo:** Es el protocolo que se usa para el transporte. Normalmente el TCP.
11. **Código de redundancia cíclica o checksum:** Para controlar errores dentro de la cabecera.

12. **Dirección de origen:** Este campo contiene 2 identificadores, correspondientes al emisor, el identificador de red (NetID) y el identificador de host (HostID).
13. **Dirección de destino:** Igual que el anterior pero los identificadores son los del destinatario.
14. **Opción:** Esta capa esta vacía para futuras ampliaciones.

Las direcciones de IP asignadas a los usuarios del protocolo TCP/IP: Las direcciones IP hacen que el envío de datos entre ordenadores se haga de forma eficaz, de un modo similar al que se utilizan los números de teléfono.

Las direcciones IP tienen 32 bits, formados por cuatro campos de 8 bits separados por puntos. Cada campo puede tener un valor comprendido entre 0 y 255. Esta compuesta por una dirección de red, seguida de una dirección de subred y de una dirección de host.

Para incorporar el protocolo TCP/IP en un ordenador debemos configurar 3 cosas

- La dirección del ordenador. Normalmente esta dirección la asigna el administrador de red.
- La máscara de red o subred: sirve para indicar cual es la red y cuales son los host o ordenadores de la red.
- La puerta de enlace: O el gateway, es la dirección predeterminada como nodo encaminadoro router. Este nodo sirve para poder acceder a un ordenador que no esta dentro de nuestra LAN.

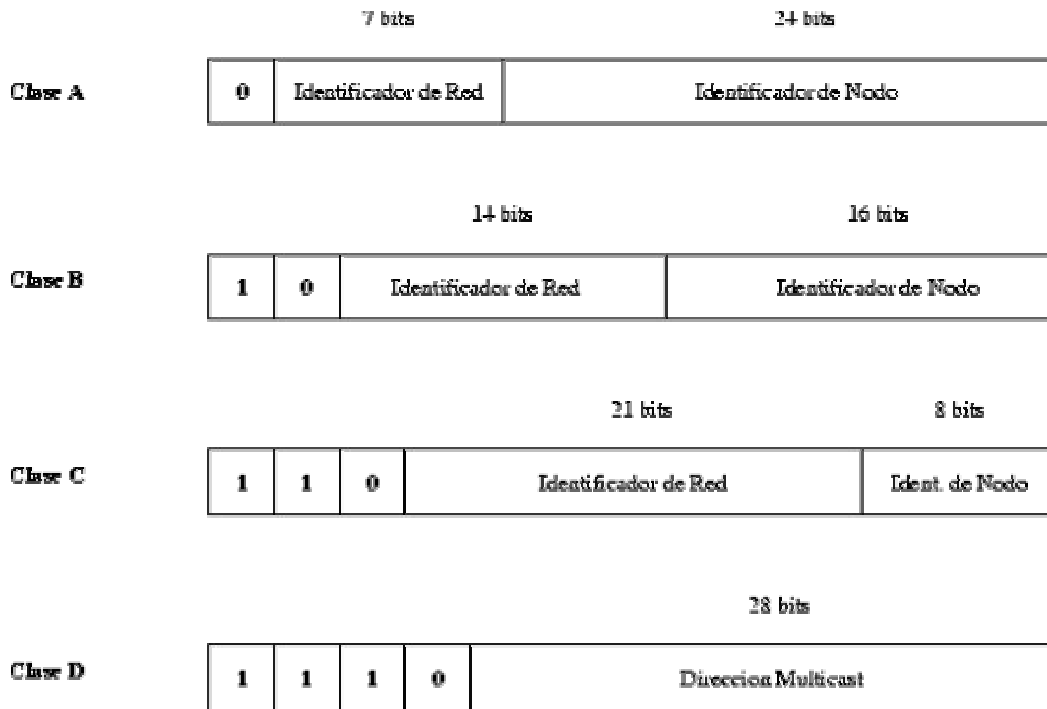
Mascaras de subred: Una máscara es una secuencia de 32bits que sirve para identificar que parte de la red es dinámica y que parte es fija o que parte indica la identificación de la red local y que parte indica cada uno de los ordenadores que la componen.

Para las redes locales se suelen poner ips tales como: 192.168.xxx.xxx o 127.168.xxx.xxx

Una máscara es una secuencia de 32 bits que viene para identificar que parte de la red es dinámica y que parte es física o lo que es lo mismo; que parte indica la identificación de la red local y cual indica cada uno de los ordenadores que la componen.

Existen cinco clases de subredes:

Clases de Direcciones IP



- **La clase A** contiene 7 bits para direcciones de red, con lo que permite tener hasta 128 redes, con 16.777.216 ordenadores cada una. Las direcciones estarán comprendidas entre 0.0.0.0. y 127.255.255.255., y la mascara de subred será 255.0.0.0.
- **La clase B** contiene 14 bits para direcciones de red y 16 bits para direcciones de hosts. El numero máximo de redes es 16.536 redes, con 65.536 ordenadores por red. Las direcciones estarán comprendidas entre 128.0.0.0. y 191.255.255.255., y la mascara de subred será 255.255.0.0.
- **La clase C** contiene 21 bits para direcciones de red y 8 para hosts, lo que permite tener un total de 2.097.142 redes, cada una de ellas con 256 ordenadores. Las direcciones estarán comprendidas entre 192.0.0.0. y 223.255.255.255., y la mascara de subred será 255.255.255.0.
- **La clase D** se reserva todas las direcciones para multidestino (multicast), es decir, un ordenador transmite un mensaje a un grupo específico de ordenadores de esta clase. Las direcciones estarán comprendidas entre 224.0.0.0. y 239.255.255.255.
- **La clase E** se utiliza exclusivamente para fines experimentales. Las direcciones están comprendidas entre 240.0.0.0. y 247.255.255.255.

Protocolos derivados y usados en el TCP/IP

Protocolo TCP (Transmission Control Protocol)

Es un protocolo de transmisión que fue diseñado para realizar conexión en redes inseguras.

Es un protocolo que afecta a las capas de transporte y que acepta cualquier paquete de una capa superior tenga el tamaño que tenga y lo convierte en bloques de un numero de K prefijadas y se lo pasa a la capa IP para su envío. La arquitectura TCP es idónea para transmitir datos por sesiones lo cual esta especialmente indicado para aplicaciones cliente-servidor. Es un protocolo que crea una especie de circuito de datos virtual entre el cliente y el servidor, es el protocolo contrario al UDP.

Así pues este protocolo es el que se encarga de la comunicación directa entre las aplicaciones cliente-servidor pero para esto usa una interface (TCB).

El TCP tiene varios estados, algunos son:

1. **CLOSED:** No existe, solo para referencia.
2. **LISTEN:** Esperando solicitud de conexión de un TCP remoto.
3. **ESTABLISHED:** Representa un a conexión abierta. Los datos recibidos pueden ser enviados a un protocolo de una capa superior. Este es el estado normal de la fase de transferencia de la conexión.
4. **CLOSING:** Esperando el conocimiento de una solicitud de final de conexión de un TCP remoto.

IE (Internet Protocol)

El protocolo IE es el que se encarga de rutear los paquetes de información. Este es el encargado de transmitir la información de una red a otro haciendo una comunicación compatible entre redes de distintos tipos. Es capaz de mandar una información de una red LAN a una red WAN. Pero presenta un problema y es que es un protocolo muy inseguro, poco fiable, de hay que dependa necesariamente del protocolo de transmisión TCP que asegura y garantiza una transmisión segura.

Protocolo UDP (User Datagram Protocol)

Es un protocolo que se puede usar en la capa de transporte. Este protocolo es un protocolo de transporte pero no necesita acuse de recibo para seguir enviando. Este protocolo se transmite y no verifica ni da respuesta de que la información ha llegado, no hace un chequeo de errores ni controla el flujo.

Protocolo ICMP

Es un protocolo que se usa como protocolo de supervisión, normalmente nos indica, cuando ha excedido el tiempo de envío, cuando el host de destino esta inaccesible.

Protocolo ARP

El protocolo ARP se encarga de averiguar donde esta localizado el ordenador al que se le quiere enviar un paquete.

Protocolo NFS (network file system)

Sirve para el intercambio de ficheros entre un ordenador y un disco duro de uns servidor.

Servicios Potocolo DHCP

En una LAN donde hay muchos ordenadores o muchos portátiles es bastante complicado asignar direcciones a todos los equipos de la red.

El protocolo DHCP lo que permite es realizar una configuración dinámica de host, esto es asignar automáticamente la dirección IP cuando un ordenador se conecta.

Servicios Protocolo DNS (domain nameserver)

Es un sistema de articulación de nombres para nodos TCP/IP que intenta organizar de modo jerárquico el nombre de todos los nodos conectados a Internet.

Los DNS son como dos pilas. Todos los servers tienen su servidor DNS. Cuando en el navegador ponemos una URL estamos solicitando una dicción URL que busca un DNS que redirección a una IP.

El servidor DNS es jerárquico cuando no se encuentra en el primer paso al segundo y así sucesivamente, existen 6 niveles.

En algunos sistemas donde existen pocos ordenadores otra forma de comunicación la dirección ip asignada a cada nombre es usando un fichero llamado host que debe ir en cada uno de los ordenadores de la redy que esta compuesto por dos columnas.

En una va el nombre y en la otra la IP.

Servicios Protocolo WINS

Es un servidor de nombres para redes NETBIOS (red propia de microsoft) Usa el protocolo NETBEUI

Redes NETWARE

Fue el sistema de NOS mas usado en la década de los 80 y parte de los 90. La ventaja que aporta este sistema es que puede correr o funcionar bajo ordenadores absolutos de igual forma que en ordenadores modernos.
Usa el protocolo IPX/SPX propiedad de novell. Microsoft implementa el protocolos clónicos del IPX. Estos protocolos son llamados por microsoft NWLINK.

Redes MAC

Usan el protocolo APPLETALK: Este protocolo fue desarrollado por apple para compartir ficheros e impresoras entre ordenadores que estuvieran conectados. Dentro de este tipo de protocolos se pueden distinguir

- LOCALTALK: Red local de MAC (max 32).
- ETHERTALK: Red ethernet, en ordenadores MAC.
- TOKENTALK: Una red de tokenring para MAC.

Redes microsoft

Dispone de diferentes sistemas operativos para redes (NOS). Como pueden ser Windows 95/98/Millennium/2000/NT.
Los protocolos que habitualmente usan las redes microsoft son: NETBEUI, TCP/IP, IPX/SPX, ademas suelen soportar otros protocolos como pueden ser: appletalk, el DLC, etc.

Pasos para instalar una red.

Análisis de las necesidades: Antes de instalar una red en una empresa hay que realizar un seguimiento actual dentro de la empresa, este trabajo aunque parezca innecesario nos va a permitir obtener informacion muy importante, como puede ser:

- Como efectúa el trabajo la empresa, que hace cada uno, que documentos tienen acceso cada uno, quien le pasa información a quien. Que volumen de información gestiona, cuantos usuarios van a trabajar, a cuantos usuarios va a beneficiar. Instalacion existente, en caso de que ya exista una instalación previa se debe evaluar lo que se tenga que aprovechar
- Hay que realizar un diseño de la red y de los servicios.
- Ejecución del diseño: Cuanto tiempo se va a emplear, cuantas personas, a quien tenemos que contratar o no.
- Seguridad, la red tiene que ser segura ante posibles ataques de personas no autorizadas, virus, gusanos, etc.
- Tiempo de testeo: Testear o controlar durante un tiempo el funcionamiento de la red. Seria bueno dejar la instalación antigua por si la nuestra fallase que no tenga la empresa parada.
- Régimen de explotación: Una vez probada la red se procedera a un implantacion definitiva en cuanto que toda red siempre hay que hacer mejoras.
-

Medidas a la hora de instalar un servidor en una empresa.

El emplazamiento de un servidor dentro de una red es una de las tareas mas importantes a la hora de planificar una red.

- Protección contra la electricidad estática y el calor: Tanto la electricidad estatica como el calor afectan altamente al rendimiento de un ordenador y por consiguiente tambien de un servidor. La temperatura a la que debe estar el ambiente que rodea al servidor se debe encontrar entre 18 y 25 grados. Es importante también que este aireado. Que la CPU este en un sitio abierto, con espacio libre.
- Evitar altibajos de tensión: Debemos de evitar los altibajos de tensión o cortes de suministro. Para esto podemos comprar lo que se llama un SAI, actualmente rondan las 18000 pts "el SAI es bueno mantenerlo encendido prácticamente siempre". Para evitar tener que comprar para todos los puestos de una red el SAI, existen también unos enchufes o regletas que protegen las subidas de tensión
- Evitar ruidos eléctricos: Para evitarlos se debe instalar una línea de corriente dedicada para el Server siempre con toma de tierra.
- Evitar tener cerca del Server materiales inflamables.