Redes TCP/IP

Luis Gerardo de la Fraga *

Sección de Computación. Departamento de Ingeniería Eléctrica

CINVESTAV-IPN

Av. Instituto Politécnico Nacional 2508. 07300 México, D.F.

Septiembre de 2003

Índice General

*Comentarios a: fraga@cs.cinvestav.mx

1 Introducción

En este capítulo vamos a tratar:

1. Como realizar una red
2. Como interconectar redes
3. El hardware necesario para realizar una red

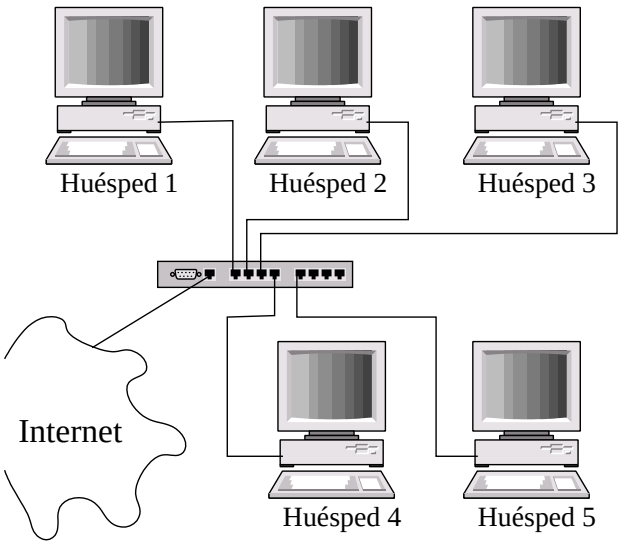

Figura 1: Esquema básico de una red

En la figura 1 vemos la idea básica de este capítulo. En la figura se muestra una red compuesta de cinco huéspedes, en este caso cada huésped es una computadora, interconectada con cable telefónico (conocido técnicamente como *par trenzado*. Vamos a aprender como configurar los huéspedes para permitir la interconexión. La red de la Fig. 1 está directamente conectada a Internet. Generalmente la conexión de intranets como la que se presenta en la Fig. 1 no es directa; es necesario usar un modem para realizar la conexión a través de un proveedor de

Internet. La red de este ejemplo usa un concentrador (aunque podría ser también un etherswitch). En este capítulo también vamos a conocer el hardware necesario para realizar una red.

2 Redes usando TCP/IP

TCP/IP define una *interfaz* abstracta a través de la cual se puede accesar al hardware, esto a su vez es un mecanismo que culta la diversidad de equipo que puede usarse en un ambiente de red [1]. Esta interfaz ofrece un conjunto de operaciones que es el mismo para todos los tipo de hardware y que trata básicamente con el envio y recepción de paquetes.

Por ejemplo, en el sistema GNU/Linux, las interfaces ethernet (las que ofrece una tarjeta de red) tienen nombres como *eth0* y *eth1*. Las interfaces PPP (que se usan para conectarse con un modem) tienen nombres como *ppp0* y *ppp1*.

Antes de usar una interfaz en una red, se debe de asignarle una dirección IP que sirve como su identificación cuando se comunican en el resto del mundo. Esta dirección es diferente del nombre de la interfaz mencionado en el párrafo anterior; si se compara la interfaz con una puerta, la dirección es como la placa de identificación pegada a ella.

Otros parámetros pueden ponerse para el dispositivo, tal como el tamaño máximo de los datagramas que pueden ser procesados por una pieza particular de hardware, el cual es conocido como la Unidad de Transferencia Máxima (Maximum Transfer Unit, MTU). Otros atributos se conocerán posteriormente. Afortunadamente, la mayoría de los atributos tienen valores por defecto funcionales.

2.1 Beneficios de usar una red TCP/IP

TCP/IP permite plataformas-entrelazadas o administración de redes heterogéneas. Por ejemplo una red de Windows NT podría contener una computadora de Unix o Macintosh o hasta redes mixtas. TCP/IP también tiene las siguientes características:

- Buena recuperación de las fallas
- Habilidad de añadir redes sin interrumpir los servicios ya existentes.
- Manejo de alto porcentaje de errores
- Independencia de la plataforma

- Bajos gastos indirectos de información.

Debido a que originalmente TCP/IP fue diseñado por propósitos relacionados al Departamento de Defensa de Estados Unidos, lo que ahora llamamos características fueron de hecho requisitos de diseño. La idea detrás de “Buena recuperación de las fallas” fue que si una parte de red fuera dañada durante un ataque, las piezas de red restantes deben seguir funcionando adecuadamente. Lo mismo aplica para, la capacidad de añadir nuevas redes, sin interrupción a los servicios ya existentes. La habilidad de manejar gran porcentaje de errores fue implantado para que si un paquete de información se pierde al recorrer una ruta, habría un mecanismo que asegurara que éste llegará a su destino mediante otra ruta. Independencia de plataforma significa que las redes y los clientes pueden ser Windows, Unix, Macintosh o cualquier otra plataforma o combinación de ellas. La razón por la cual TCP/IP es tan eficiente son sus gastos indirectos bajos. Desempeño es la clave de cualquier red. TCP/IP no tiene una contraparte en su simplicidad y rapidez.

2.2 Números binarios y decimales [2]

En base dos ó números binarios, el valor representado por “1” es determinado por su posición. No es diferente de la base diez que todos conocemos, en la cual el primer numero desde la derecha enumera unidades, el segundo desde la derecha enumera decenas, el tercero centenas, y así hasta el infinito. Mientras el sistema decimal provee 10 dígitos (de 0 a 9) para representar diferentes valores, el sistema binario solo ofrece dos dígitos validos: 0 y 1. Su posición, al igual que en el sistema decimal, determina el valor que representa. La posición que esta hasta la derecha, en términos decimales, representa 2. La siguiente posición a la izquierda 4, la siguiente 8, etc. Cada posición vale 2 veces más que su vecina derecha. El valor decimal de un numero binario se calcula sumando los valores decimales de los dígitos que tienen 1 en su posición. Matemáticamente, cada octeto de una dirección IPv4 (hay 4 de ellos) puede tener un valor máximo de 225 en el sistema decimal. Un número binario equivalente a 225 consiste de 8 bits, con todos los bits 1. Un ejemplo de la relación entre números decimales y binarios:

Dígito	8	7	6	5	4	3	2	1
Binario	1	1	1	1	1	1	1	1
Valor decimal del dígito	128	64	32	16	8	4	2	1

Como puede observarse, cada bit en la dirección binaria tiene “1” en su posición. Por esto, el valor decimal de este numero binario puede calcularse sumando los

valores de las 8 columnas: $128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 225$.

La siguiente tabla muestra de la conversión de un número binario a uno decimal. En este ejemplo el quinto numero desde la derecha es 0. Esta posición representa el valor de 16. De esta manera, el valor de este numero binario es 16 unidades menor que 255: $128 + 64 + 32 + 8 + 4 + 2 + 1 = 239$.

Dígito	8	7	6	5	4	3	2	1
Binario	1	1	1	0	1	1	1	1
Valor decimal del dígito	128	64	32	16	8	4	2	1

Esta relación entre números binarios y decimales es la base de la arquitectura de direcciones IP. Recuerde que hay 4 octetos binarios en cada dirección IPv4, incluyendo subredes enmascaradas. Por eso es necesario entender la relación entre estos sistemas básicos, la conversión del uno al otro, antes de estudiar distintas maneras de implantar dirección de IP.

2.3 Direcciones IP

El protocolo de red IP entiende las direcciones como números de 32 bits. Esta convención es para la versión 4 (IPv4) que será tratada en todo el curso. A cada máquina debe asignársele un número único en el ambiente de la red. Existen algunos intervalos de números IP que se han reservado para usarse en el diseño de intranets (ó redes privadas). Estos intervalos están listados en la tabla 4. Sin embargo, para sitios de Internet, los números eran asignados hace ya algunos años, por una autoridad central, el *Centro de Información de la Red* (NIC, *Network Information Center*). Actualmente los números que se usarán son asignados por el mismo proveedor de Internet al que se le compra la conectividad IP.

Las direcciones IP se dividen por legibilidad en cuatro números de ocho bits, llamados *octetos*. Por ejemplo, luna.computacion.universidad.mx tiene la dirección 0x954C0C04, el cual se escribe como 149.76.12.4. Este formato se refiere frecuentemente como *notación decimal puntuada*. De esta forma cada byte es convertido en un número decimal (0-255), despreciando los ceros a la izquierda a menos que el número en sí sea cero.

Otra razón para esta notación es que una dirección IP se puede dividir en un número de *red*, la cual está contenida en los primeros octetos, y un número de *huésped*, que está en los restantes octetos. Cuando de requieren números IP y se les pide al NIC, este no asigna un número por cada huésped que se planea usar. En vez de ello se asigna un número de red y se permite asignar todas las direcciones IP válidas dentro del intervalo del número de huéspedes sobre su propia red, de

acuerdo al diseño propio que se tenga. Al número de bits que comparten todas las direcciones de una red se le llama máscara de red (netmask), y su papel es determinar qué direcciones pertenecen a la red y cuáles no. Esto puede verse con el ejemplo mostrado en la tabla 1

Dirección IP	192.168.120.21
Máscara de red	255.255.255.0
Número de red	192.168.120.
Número de huésped	.21

Tabla 1: Ejemplo de la división de una dirección IP

Cualquier dirección a la que se aplique una operación AND de bits con su máscara de red, revelará la dirección de la red a la que pertenece. La dirección de red es por tanto siempre el menor número de dirección dentro del intervalo de la red y siempre tiene la porción de huésped codificada toda con ceros.

Por razones administrativas, durante el desarrollo inicial del protocolo IP se formaron, de forma arbitraria, algunos grupos de direcciones como redes, y estas redes se agruparon en las llamadas *clases*. Estas clases proporcionan un cierto número de redes de tamaño estándar que pueden ser reservadas. Los intervalos reservados pueden verse en la tabla 2.

Clase de red	Máscara de red	Direcciones de red
A	255.0.0.0	1.0.0.0 - 126.255.255.255
B	255.255.0.0	128.0.0.0 - 191.255.255.255
C	255.255.255.0	192.0.0.0 - 223.255.255.255
Multicast	240.0.0.0	224.0.0.0 - 239.255.255.255

Tabla 2: Clases de direcciones IP

El número de huéspedes que permite cada clase es:

Clase A . La porción de red está contenida en el primer octeto. Esta clase provee una porción de huésped de 24 bits, permitiendo alrededor de 1.6 millones de huéspedes por red. Esta clase fue diseñada para redes extremadamente grandes.

Clase B . El número de red está en los primeros dos octetos. Esta clase permite 16,320 redes con 65,024 huéspedes cada una. Esta red fue diseñada para redes de tamaño moderado a grandes.

Clase C . El número de red está contenido en los primeros tres octetos. Esta clase permite cerca de dos millones de redes con 254 huéspedes cada una. Esta clase fue diseñada para permitir cientos de redes de tamaño pequeño.

En el ejemplo dado anteriormente, para la dirección IP 149.76.12.4, la dirección de **luna**, se refiere al huésped 12.4 de la red clase B 149.76.0.0.

No todos los números se permiten en la porción del huésped [3]. Los octetos 0 y 255 están reservados para usos especiales. Una dirección donde todos los bits de la porción del huésped son 0 se refiere a la red, y una dirección donde todos los bits de la parte del huésped son 1 se llama una *dirección de difusión* (broadcast). Ejemplo, para la tabla 1:

Dirección IP	192.168.120.21
Máscara de red	255.255.255.0
Número de red	192.168.120.
Número de huésped	.21
Dirección de Red	192.168.120.0
Dirección de Difusión	192.168.120.255

Tabla 3: Tabla 1 con la dirección de red y de difusión

La dirección de difusión es una especial a la que escucha cada máquina en la red además de a la suya propia. Esta dirección es a la que se envían los datagramas si se supone que todas las máquinas de la red lo deben recibir. Ciertos tipos de datos, como la información de encaminamiento y los mensajes de aviso son transmitidos a la dirección de difusión para que cada huésped en la red pueda recibirlo simultáneamente. Hay dos estándares usados comúnmente al respecto de la dirección de difusión. El más ampliamente aceptado es el de usar la dirección más alta posible en la red. En el ejemplo de la Tab. 3 sería 192.168.120.255. Por alguna razón, otras estaciones han adoptado la convención de usar las direcciones de red como direcciones de difusión. En la práctica no importa mucho cual se use, pero hay que asegurarse de que cada máquina en la red está configurada con la misma.

Otras direcciones de red reservados para usos especiales son la 0.0.0.0 y 127.0.0.0. La primera es llamada *ruta por defecto* y la segunda es la *dirección propia* (loopback).

La red 127.0.0.0 esta reservada para el tráfico IP local en el huésped propio. Usualmente la dirección 127.0.0.1 será asignada a una interfaz especial en el

huésped, la *interfaz propia*, la cual actúa como un circuito cerrado. Cualquier paquete IP manejado por esta interfaz será regresado a ella misma tal como si fuese recibido desde alguna otra red. Esto permite desarrollar y probar el software de red aún si no se tiene una red "real". La red propia también permite usar software de red sobre un huésped aislado.

Algunos intervalos de direcciones para cada clase se han dejado fuera y se han asignado para direcciones "privadas". Estas direcciones se han reservado para ser usadas en redes privadas y no son ruteadas hacia Internet. Estas son usadas por las empresas para construir sus propias intranets, pero se usan aún en redes muy pequeñas. Estas direcciones reservadas se presentan en la tabla 4

Clase	Máscara de red	Direcciones de red
A	255.0.0.0	10.0.0.0
B	255.255.0.0	172.16.0.0 - 172.31.0.0
C	255.255.255.0	192.168.0.0 - 192.168.255.0

Tabla 4: Direcciones reservadas para intranets

De la tabla 4 se desprende que hay una red reservada clase A, 16 redes reservadas clase B y 256 redes reservadas clase C.

Para instalar un nuevo huésped en una red IP existente se debe contactar con los administradores de la red y preguntarles por la siguiente información:

- Dirección IP del huésped
- Dirección IP de la red
- Dirección IP de broadcast
- Máscara de red IP
- Dirección del encaminador (router)
- Dirección del Servidor de Nombre de Dominio (DNS)

Se debería configurar entonces el dispositivo de red del huésped con esos detalles. No pueden inventarse y esperar que la configuración funcione.

Para construir una nueva red propia que nunca conectará con Internet, esto es, si está construyendo una red privada y no tiene intención de conectar nunca esa red a Internet, entonces puede elegir las direcciones que quiera. De todas maneras, por razones de seguridad y consistencia, se deben de usar las direcciones reservadas presentadas en la tabla 4.

3 Subredes

Una subred [4] es un medio para tomar una sola dirección de red IP y localmente particionarla de forma que esta sola dirección IP pueda ser usada realmente en varias redes locales interconectadas. Recuerde que un número de red IP solo puede usarse sobre una sola red.

La palabra importante aquí es *localmente*: para todo el mundo fuera de las máquinas y las redes físicas cubiertas por la red IP puesta como subred, nada ha cambiado – es solo una red IP–. Esto es muy importante: hacer una subred es una configuración local que es invisible al resto del mundo.

3.1 ¿Por qué se usan las subredes?

Las razones detrás de las subredes vienen de las primeras especificaciones de IP, donde solo unos pocos sitios estaban ejecutando números de red clase A. Una red clase A permite millones de huéspedes conectados.

Si todas la computadoras IP en un sitio grande tuviesen que estar conectadas a la misma red, resultaría obviamente tanto en un tráfico enorme como un problema de administración: tratar de manejar tal bestia enorme podría ser una pesadilla y la red podría (casi con certeza) colapsar bajo la carga de su propio tráfico (se saturaría).

Entrando a las subredes: la direcciones de la red IP clase A podrían dividirse para permitir su distribución a través de varias (si no es que muchas) redes separadas. También la administración de cada red separada puede delegarse fácilmente. Esto permite tener redes pequeñas, manejables, que puedan establecerse, quizás usando tecnologías de red diferentes. Hay que recordar que no se pueden mezclar Ethernet, Token Ring, FDDI, ATM, etc., sobre la misma red física. Sin embargo, las diferentes tecnologías si pueden interconectarse.

Otras razones para la realización de subredes son:

- La distribución física del sitio puede crear restricciones (el largo de los cables, por ejemplo) en términos de cómo la infraestructura física puede conectarse, requiriendo múltiples redes. Las subredes permiten realizar esto en un ambiente IP usando un solo número de red IP. Esto es de hecho de realización muy común entre los Proveedores de Internet, los cuales tienen tienen que dar conectividad permanente a clientes con redes locales con números IP estáticos.

- El tráfico de red es lo suficientemente alto para causar caídas significantes. Partiendo la red usando subredes, el tráfico que es local en un segmento de red puede mantenerse local, reduciendo el tráfico total y acelerando la conectividad de la red sin requerir más ancho de banda.
- Los requerimientos de seguridad bien pueden dictar que diferentes clases de usuarios no compartan la misma red, ya que el tráfico sobre una red puede siempre ser interceptado por un usuario experimentado. Las subredes proveen una forma de mantener el departamento de mercadotecnia fuera del fisgoneo de tráfico de red del departamento de Investigación y Desarrollo (o a los estudiantes fuera del fisgoneo sobre la red de administración).
- Se cuenta con equipos que usan tecnologías de red incompatibles y que es necesario interconectar.

3.2 Cómo realizar una subred de un número de red IP

Una vez que se ha decidido poner subredes en el número de red que se tenga, ahora ¿cómo ha de realizarse esto? De forma general tienen que realizarse los siguientes pasos (que luego se explicarán en detalle):

- Poner la conectividad física (cables de red e interconexiones, tales como ruteadores).
- Decidir que tan grande/pequeña se necesita cada subred en términos del número de dispositivos que se conectarán a ellas, esto es, cuantos números IP útiles se requieren para cada segmento individual.
- Calcular la máscara de red y las direcciones de red apropiadas.
- Asignar a cada interfaz sobre la red su propia dirección IP y la máscara de red apropiada.
- Configurar las rutas sobre los ruteadores y las compuertas apropiadas, las rutas y/o rutas por defecto sobre los dispositivos de red.
- Probar el sistema y arreglar los problemas.

Para propósitos de ejemplo, se considerará que se crearán subredes sobre un número de red clase C: 192.168.1.0. Esto provee hasta un máximo de 256 interfaces conectadas, más el número de red obligatorio (192.168.1.0) y la dirección de difusión (192.168.1.255).

3.3 Poniendo la conectividad física

Se debe de instalar la infraestructura correcta de cableado para todos los dispositivos que se deseen interconectar para alcanzar la distribución física.

También será necesario tener un mecanismo para interconectar varios segmentos (ruteadores, convertidores, etc.).

3.4 Tamaño de la subred

Existe un compromiso entre el número de redes que se pueden crear y los números IP "perdidos".

Cada red IP individual tienen dos direcciones que ni pueden usarse como direcciones para una interfaz (ó huésped), el número de red IP en sí mismo y la dirección de difusión. Cada subred tiene estas dos direcciones que no pueden usarse:su propio número de red y dirección de difusión, además de direcciones válidas en el intervalo proveído por la red IP que se quiera dividir en subredes.

De esta forma, haciendo subredes de una dirección IP en dos subredes separadas existen ahora dos direcciones de red y dos direcciones de difusión, incrementando las direcciones "perdidas"; crear cuatro subredes crea ocho direcciones que no pueden usarse; etc.

De hecho, la subred útil más pequeña conste de solo cuatro números IP:

- Dos números IP para las interfaces, una para la interfaz del ruteador sobre esta red y otro para la interfaz del huésped sobre la red.
- Un numero de red.
- Una dirección de difusión.

Para qué se quería crear una red tan pequeña ya es otra pregunta. Con solamente un huésped sobre la red, cualquier comunicación en red debe ir hacia otra red. Sin embargo, este ejemplo sirve para mostrar las leyes de disminución que se aplican a las subredes.

Por principio, solamente se puede dividir una número de red IP en 2^n (donde n es menor en uno que el número de bits de la parte del huésped del número de red IP que se esté manejando) subredes de igual tamaño (sin embargo, se pueden hacer subredes de una subred ó combinar subredes)

Para ser realistas sobre el diseño de una red propia, se requiere el número mínimo de redes locales separadas que sea consistente con las restricciones de administración, físicas, de equipo y seguridad.

3.5 Cálculo de la máscara de subred y los números de red

La máscara de red es la que realiza toda la magia local de dividir una red IP en varias subredes.

La máscara de red para un número de red IP sin subredes es simplemente un número de red que tiene todos los bits de red puestos a '1' y todos los bits del huésped puestos a '0'. Para las tres clases de redes IP, las máscaras de red estándar son:

- Clase A (8 bits de red) : 255.0.0.0
- Clase B (16 bits de red): 255.255.0.0
- Clase C (24 bits de red): 255.255.255.0

La forma de que una subred opera es tomar prestado uno o más de los bits del huésped disponibles y hacer que las interfaces localmente interpreten estos bits prestados como parte de los bits de red. De manera que para dividir un número de red en dos subredes, podríamos tomar prestado un bit del huésped poniendo a uno el bit apropiado en la máscara de red del primer bit del huésped. Para una red clase C, resultaría una máscara de red de 11111111.11111111.11111111.10000000, ó 255.255.255.128

Para la red de clase C, por ejemplo, 192.168.1.0, estas son algunas de los opciones que tenemos para realizar subredes:

Redes	Huéspedes/red	Máscara de red
2	126	255.255.255.128 (11111111.11111111.11111111.10000000)
4	62	255.255.255.192 (11111111.11111111.11111111.11000000)
8	30	255.255.255.224 (11111111.11111111.11111111.11100000)
16	14	255.255.255.240 (11111111.11111111.11111111.11110000)
32	6	255.255.255.248 (11111111.11111111.11111111.11111000)
64	2	255.255.255.252 (11111111.11111111.11111111.11111100)

En principio, no hay ninguna razón para seguir el camino explicado para realizar la subred, donde los bits de las máscara de red son adicionados en el bit del huésped más significante hacia el bit del huésped menos significante. Sin embargo, si no se realiza de esta manera, los números IP resultantes seguirán una secuencia bastante extraña. Esto lo hace extremadamente difícil, para nosotros los humanos, decidir cual subred pertenece un número IP, ya que nosotros no somos tan buenos para pensar en binario (las computadoras, por otro lado, se manejan igual de bien en cualquier esquema).

Una vez que se ha decidido por la máscara de red apropiada, se tienen que resolver las direcciones de red y de difusión, y el intervalo de números para cada una de las redes. Considerando solamente un número de red clase C, y listando solo la parte final (la porción de huésped) se tiene:

Máscara	Subredes	Red	Difusión	MinIP	MaxIP	Huéspedes	Huéspedes totales
128	2	0	127	1	126	126	
		128	255	129	254	126	252
192	4	0	63	1	62	62	
		64	127	65	126	62	
		128	191	129	190	62	
		192	255	193	254	62	248
224	8	0	31	1	30	30	
		32	63	33	62	30	
		64	95	65	94	30	
		96	127	97	126	30	
		128	159	129	158	30	
		160	191	161	190	30	
		192	223	193	222	30	
		224	255	225	254	30	240

Como puede verse, existe una secuencia muy definida de estos números, lo cual los hace muy fácil de checar. La desventaja de las subredes también puede verse, ya que se reduce el número total de direcciones de huésped disponibles al mismo tiempo que se incrementa el número de subredes.

Con toda esta información, ya se está en la posición de asignar números de huéspedes, números de redes IP y máscaras de red.

4 Hardware necesario

Ya que el TCP/IP está basado en una tecnología convencional de conmutación de paquetes, es independiente de cualquier marca de hardware en particular. La Internet incluye una variedad de tecnologías de red que van de redes diseñadas para operar dentro de un solo edificio a las diseñadas para abarcar grandes distancias. Los protocolos TCP/IP definen la unidad de transmisión de datos, llamada datagrama, y especifican cómo transmitir los datagramas en una red en particular [5]. Sin embargo, al tratarse de redes grandes surge un problema común a todas la redes: el tráfico. Para controlar el trafico de paquetes en la red, ésta se divide en segmentos, ya sea de acuerdo a sus caracteristicas lógicas ó caracteristicas físicas. Para administrar estos segmentos se han diseñado dispositivos como concentradores, ruteadores y etherswitches que trataremos abajo.

4.1 Concentradores (hubs)

Los concentradores (o en inglés, *hubs*) son distribuidores inteligentes de datos y alimentación.

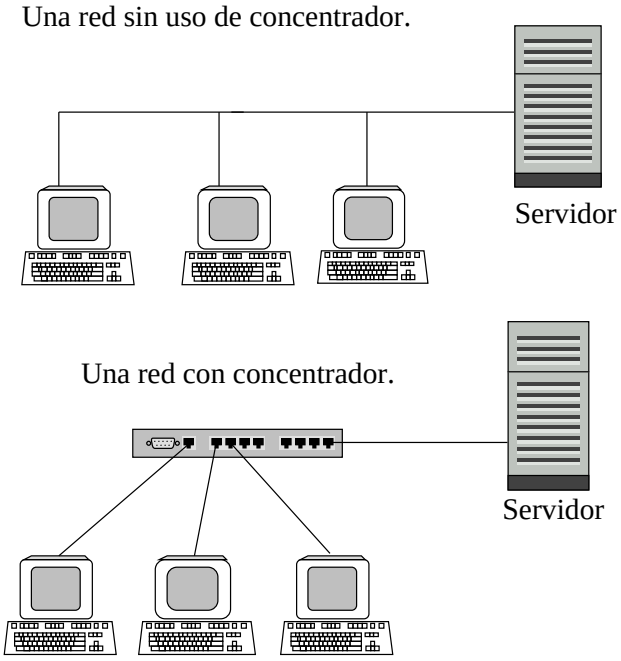

Figura 2: Diferencia entre una red con y sin concentrador.

Un concentrador es el punto común de la conexión para los dispositivos en una red y fue diseñado en 1989. Cuando un paquete de información llega a un puerto, se copia a todos los puertos de salida de modo que todos los segmentos de la LAN puedan recibir todos los paquetes [6]. La desventaja de este dispositivo es que todos los miembros de la red obtienen el total de ancho de banda, lo que disminuye la eficiencia total de red [7]. Todas las terminales de una red estarán físicamente conectados (por medio de cables específicos) a este dispositivo y cada concentrador estará conectado a la linea principal de comunicación (*backbone*). Por eso un concentrador necesariamente trabaja en una red con topología de estrella. Un concentrador contiene puertos múltiples y probablemente varios tipos de puertos, facilitando la conexión de otros dispositivos a éste. También es posible conectar varios concentradores entre si. Si este es el caso, su linea principal de comunicación debe ser de alta velocidad y muy eficiente, posiblemente de fibra óptica, para optimizar el funcionamiento de los concentradores. Por eso, como se ve en la Figura 2 un concentrador cambia considerablemente la topología de una red y aumenta la eficiencia de ésta. Al desempeñar los concentradores un papel tan vital en una red con topología de estrella, existen varios tipos de éstos:

- *Concentradores pasivos.* Este tipo de concentradores es el más sencillo. No ayuda a encontrar fallas en hardware ó “embotellamientos” de información, sino que solo se limita a remitir los paquetes de información que le llegan a los demás puertos. Este tipo de concentrador de 8 puertos cuesta menos de unos 200 dólares, aunque el precio puede variar dependiendo de la LAN [8].

- *Concentradores activos.* Este tipo de concentrador tiene más utilidades que el concentrador pasivo. A parte de remitir los paquetes que le llegan, este concentrador se fija en la información de lo paquetes. Esto no significa que dé prioridades a unos paquetes, sino que repara los paquetes ”dañados”. Si una señal débil, pero aún legible llega a este concentrador éste la aumenta, como si fuera un micrófono, antes de remitirlo. Adicionalmente, algunos de estos concentradores reportarán las fallas existentes en la red. A veces un cable experimenta disturbios electromagnéticos, causando pérdidas de datos transmitidos por ese cable. Es este caso, los concentradores activos recompensan los paquetes perdidos, retransmitiéndolos a puertos individuales y resincronizan la entrega de los paquetes en una conexión más lenta. Por eso, la conexión de todos los dispositivos conectados a ese concentrador se vuelve más lenta, sin embargo a veces eso es preferible a la pérdida total de

datos. Así, este tipo de concentradores tienen la ventaja de diagnosticar el funcionamiento de la red y reportar errores existentes [8].

- *Concentradores inteligentes.* Este tipo de concentrador es el más reciente y el más eficiente en el funcionamiento de una red. Este concentrador tiene las caracteristicas de un concentrador activo, pero además proporciona la posibilidad de manejar la red entera desde una sola localización central. Si algún dispositivo incorporado a la red presenta problemas, este concentrador hace posible identificar, diagnosticar, y reparar la falla usando la información proporcionada por el concentrador. Además este concentrador maneja los recursos de la red y distribuye la rapidez de transmisión. Así un administrador puede dar más capacidad de transmisión (10 kbps, 100kbps, etc) a los dispositivos que lo necesiten [8].

4.2 Ruteadores

Manejar una red simple de unas pocas terminales es muy sencillo, pero al añadirle más terminales se vuelve más complejo y menos práctico. Una solución fácil a esta situación es rompiendo la red en segmentos clasificados por alguna característica en especial. Sin embargo estas sub-redes necesitan comunicarse entre si por que todos son parte de una una sola red. Aquí es donde entran en juego los ruteadores. Por ejemplo un ruteador de TCP/IP puede dividir la red en segmentos de acuerdo a su IP. Un ruteador es dispositivo usado para encaminar los paquetes desde de una red a otra. Los ruteadores también se utilizan en el Internet para transportar los paquetes de los datos una su máquina a otra. Éstos saben qué trayectoria entre las redes deben tomar los paquetes de información y los remiten al siguiente ruteador. Cada paso de un ruteador se llama salto, o en ingles *hop* [9].

Un ruteador trabaja a nivel de protocolo y en una forma similar a la de un etherswitch, filtrando y removiendo el tráfico innecesario en la red o en los segmentos de ésta. Pero a diferencia de un etherswitch, un ruteador clasifica los paquetes por su protocolo específico. De esta manera, un ruteador divide la red en segmentos *lógicos*. Así, los paquetes de información solo entran al segmento de la red al cual están destinados. Al trabajar a nivel de protocolo los ruteadores tienen una característica muy importante: funcionan como cortafuego (en inglés, *firewall*). Un cortafuego es una barrera (como un filtro) que no permite que determinados paquetes entren o salgan de la red. Por eso algunas empresas que guardan datos personales, ponen un ruteador entre su propia red y el mundo, por ejemplo, Internet. Configurando las listas de acceso en un ruteador se puede permitir o prohibir

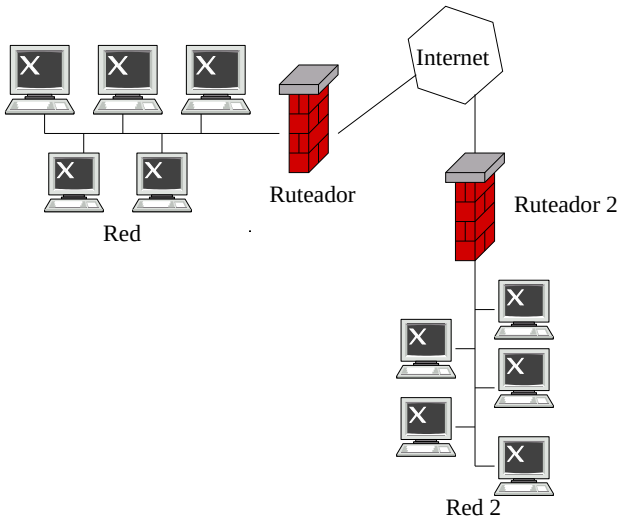

Figura 3: Como funciona un ruteador

el acceso de un huésped y así fortalecer la seguridad de la red. La ventaja de un ruteador es que éste puede filtrar los paquetes que llegan de una red externa (por ejemplo Internet) o desde una sub-red [7].

4.3 Etherswitches

Los etherswitches aumentan la eficiencia de la red disminuyendo el tráfico extraño que pasa a través de ésta ó a través de segmentos individuales de la red. También pueden filtrar los paquetes de información en una forma similar a la de un ruteador. La diferencia con el ruteador es que un ruteador filtra los paquetes por protocolos específicos , mientras que un etherswitch los filtra por dirección de paquetes. Así un etherswitch divide la red en segmentos *físicos* [10]. Cuando un paquete llega, etherswitch lee su encabezado para determinar a que segmento de la red esta destinando y se transmite a ese segmento. Esto previene que los paquetes sean retransmitidos a todos los segmentos de la red, disminuyendo considerablemente el tráfico [7]. Esto se puede observar en más detalle en la figura 4

Existen dos tipos de “Etherswitches”:

- Cut-Through: Cuando un paquete ingresa a este tipo de “Etherswitch”, éste lee su encabezado y lo transmite de inmediato al segmento de la red co-

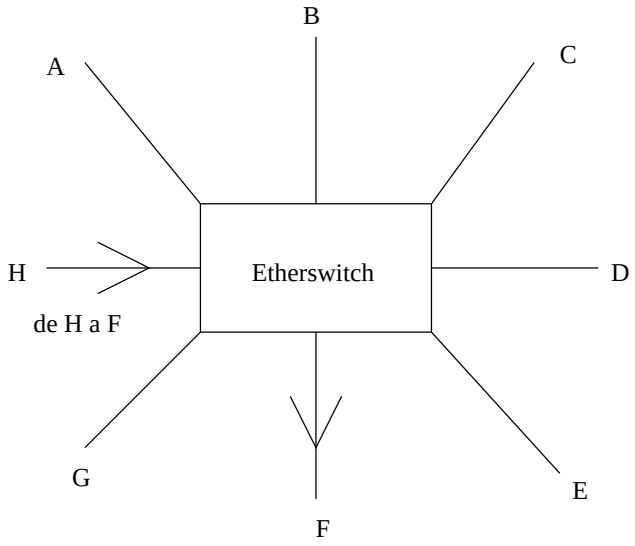

Figura 4: Esquema de un etherswitch mandando un paquete del puerto H al puerto F

rrespondiente, antes de recibir el paquete completo. Este dispositivo es más veloz que el "store&forward" (*almacena y transmite*).

- Store&Forward: A diferencia de "Cut-Trough" este tipo de "Etherswitch" analiza el paquete entero antes de transmitirlo al segmento correspondiente. Este tipo de switch busca errores en el paquete, y si los encuentra detiene su propagación por la red.

Los "Etherswitches" son más eficientes que los ruteadores [10].

4.4 Tarjetas de Red

Una tarjeta de red se usa para conectar una computadora a una red Ethernet. La tarjeta en si, provee una interfaz a los medios. Esto puede realizarse usando un transmisor-receptor externo(como se ve el la Figura 5) ó a través de un transmisor-receptor interno integrado a la computadora y montado en la tarjeta de red PCB. Habitualmente la tarjeta también contiene un respaldo lógico e inalterable del protocolo (o en ingles *Protocol Control firmware*) y un Controlador de Acceso del Medio (o en inglés, *MAC- Medium Control Access*) que es el protocolo de transmisión de datos usado en Ethernet. El fabricante de tarjetas de red les asigna una

dirección única que dentro de ésta se almacena en PROM. Globalmente, estas direcciones son únicas y se almacenan en bloques de 16(u ocho) millones. Esto asegura que no haya dos tarjetas de red con la misma dirección de remitente.

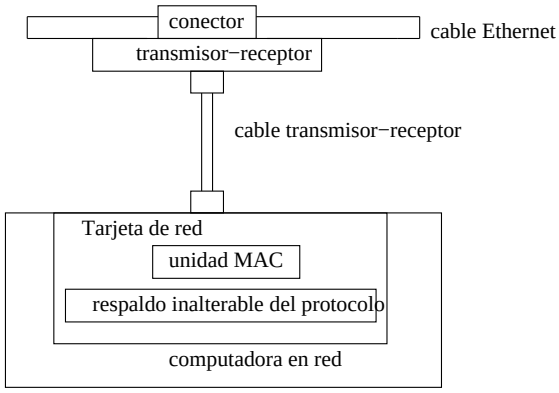

Figura 5: Una tarjeta de red

El protocolo MAC se usa para que la capa de transmision de datos de Ethernet funcione. Este protocolo encapsula los datos de carga útil, añadiéndole un encabezado de 14 bytes y un apéndice de 4 bytes. Este proceso es precedido por una pequeña pausa (de unos 9.6 microsegundos) y una preámbulo de 8 bytes. El propósito de esta pausa antes de comenzar el proceso, es permitir que la electrónica de cada nodo se readapte después del proceso anterior. AL transmisión comienza cuando el nodo manda una secuencia de 8 bytes (64 bits) que consiste en 62 “1” y “0” alternados y luego un patrón “11”. Esta secuencia de 64 bits produce una onda de 5 MHz. Cuando el primer bit de esta preámbulo se recibe, cada receptor puede estar en un estado arbitrario (o sea tener una fase arbitraria para su reloj local). Al llegar los demás bits los receptores se sincronizan en la fase correcta y al llegar el “11” se termina la secuencia. Cuando esta secuencia se termina, la información que se quiere mandar se encapsula. Las partes principales de esta cápsula son: el encabezado, el cuerpo y el apéndice [11].

- El encabezado consiste de tres partes. La dirección del destinatario (6 bytes) que especifica a donde quiere llegar el paquete de información. La segunda parte es la dirección del remitente (6 bytes) que especifica de donde proviene el paquete. Y por último la parte (2 bytes) donde se especifica que tipo de protocolo se usa, por ejemplo el protocolo de redes IP. El tamaño total es de 14 bytes.

- El cuerpo es la información en sí que lleva el paquete
- El apéndice de 32 bits detecta errores en el paquete ó colisiones en la red.

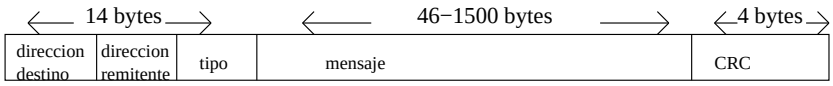

Figura 6: Encapsulación Mac de un paquete de información

Otra parte importante de tarjeta de red es el transmisor-receptor de MAC que también se conoce como Unidad de Acceso de Medio (en inglés, *Medium Acces Unit*). Este dispositivo contiene los circuitos electrónicos que unen la tarjeta de red y el cable Ethernet. Esta unidad contiene transmisor de linea (el transmisor), un receptor de línea (el receptor), un circuito de detección de actividad (para determinar si el cable esta en uso) y control electrónico (para asegurarse que el dispositivo trabaja correctamente) [11]. El control electrónico de transmisor-receptor contiene circuitos necesarios para:

- Recibir los paquetes de un cable o mandar paquetes hacia el cable.
- Detectar colisiones de paquetes en el cable.
- Proveer el aislamiento eléctrico entre el cable coaxial y la electrónica de interfaz de cable.
- Proteger el cable de malfuncionamientos del transmisor-receptor ó la tarjeta de red en sí.

Esta Unidad de Acceso de Medio se conecta al puerto de Interfaz de Unidad de Accesorios (o en inglés *AUI-Attachment Unit Interface*) de la tarjeta de red. Este puerto es un conector de tipo D de 15 pernos (*pin*). Para conectarlos se usa un cable especial que consiste de 5 cables trenzados de cobre cada uno cubierto con su propia capa. Este cable tiene un conector AUI en cada extremo y su longitud puede ser de hasta 50 metros. Esto se puede ver en la Figura 7.

4.5 Modems

Modem (*mo*dulador-*dem*ulador) es un dispositivo que convierte señales digitales a señales análogas y viceversa. La mayor parte de las lineas telefónicas están

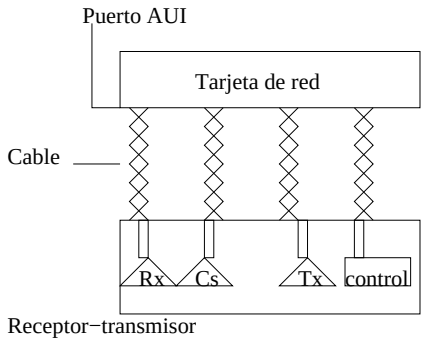

Figura 7: Transmisor–receptor conectado a la tarjeta de red.

diseñadas para transmitir datos análogos (voces), mientras que las computadoras generan datos digitales (pulsos). Un modem recibe pulsos digitales de una computadora, modula algunas propiedades (frecuencia, amplitud, etc) de un medio análogo y transmite estos datos (ya análogos) por líneas telefónicas. Al recibir un dato análogo, el modem revierte el proceso [12]. Existen cuatro tipos básicos de modem para PC: interno, externo, incorporado y UBS. El modem externo, así como USB se encuentran fuera de PC, mientras que los otros dos tipos están dentro de éste. Los modems exteriores se enchufan a la computadora mediante un conector conocido como el "puerto serial". Este puerto es diseñado solo para modems exteriores y no se pueden usar con ningún otro dispositivo como printer u otro tipo de modem. En Linux este puerto usualmente se llama ttyS0 y/o ttyS1. El modem interno es una tarjeta insertada en la computador, mientras que el modem incorporado es parte de la tarjeta madre, y por eso se considera parte de la computadora. Es similar al modem interno, con la diferencia de que el modem incorporado no puede ser reemplazado o removido. Este tipo de modems generalmente son para laptops. Los modems internos son más baratos, y es más probable que no pierdan información si el búfer (en inglés, *buffer*) se sobrecarga. Además usan menos electricidad y no usan espacio del disco. Por otro lado los modems externos son más fáciles de instalar y requieren de menos configuración. Además, tienen luces indicadoras que te pueden dar una pistas sobre qué ocurre si hay problemas y ayudar a resolverlos. El hecho de que el puerto serial y el modem pueden separarse físicamente, también ayuda a resolver algunos problemas. Se pueden mover más fácilmente a otra computadora. Si se quiere reiniciar un modem externo, no se tiene que apagar todo el equipo. Desafortunadamente, la mayoría de los modems externos no tienen un interruptor para apagarse si no esta en uso, y por eso consume más electricidad. Otra posible desventaja de un modem externo es que se

estará forzado a usar el puerto serial ya existente que tal vez solo permite la velocidad de 115,200 bps. Los modems internos son especialmente problemáticos cuando se usan con Linux. Configurarlos puede ser muy fácil (automáticamente) o extremadamente difícil, dependiendo del modem, tus habilidades y qué tan fácil es encontrar información sobre el modem. Algunos modems solo trabajan con MS Windows debido a la escasez de drivers para Linux.. Sin embargo los modems no se limitan a esto sino que también pueden mandar fax y los modems de voz pueden usarse como contestadora [13].

4.6 Cables

Existen diversos tipos de cables:

- *Par Trenzado.(STP/UTP)*
    1. Su nombre oficial es 10BasebandT.
    2. Puede conectar segmentos de 0.6 a 100m de distancia.
    3. Es barato.
    4. Algunos edificios ya tienen instalado par trenzado.
    5. Fácil de interferir.
    6. Capacidad de media a baja.
    7. Tiene 2 categorías: Categoría 3 (10 MBps) y Categoría 5 (100 MBps)
- *Cable Coaxial.*
    1. Capacidad media.
    2. Se usa comúnmente en sistemas Ethernet y Arcnet.
    3. No es tan fácil de interferir como el cable de par trenzado.
    4. Es más difícil de instalar que el par trenzado.
- *Fibra Óptica.(10BasebandF)* Comúnmente se usa para cubrir distancias muy largas. Por ejemplo, puede usarse para conectar dos concentradores, que en otras condiciones no podrían conectarse debido a limitaciones de distancia.
    1. Es caro.
    2. Se usa en línea central de comunicación (backbone).

3. Puede conectar segmentos que están a 2 km de distancia.
4. Alta capacidad.
5. Inmune a interferencias.
6. Los conectores para fibra óptica son caros.
7. Cubre distancias largas.
8. Es difícil de instalar.

Si se quiere empezar una red, se tiene que decidir si usar Ethernet delgado (cable coaxial RG58 con conectores de BNC) o usar 10baseT (cables de par trenzado con conectores RJ-45). Los Ethernet delgados, cables RG-5 con conectores N son obsoletos y raramente vistos.

Los cables de Ethernet delgados son baratos, así como los cables de par trenzado. Es esencial finalizar cada cable con un terminador de 50 Ohm. También es vital que los cables no tengan “cabos” sueltos – los conectores “T” deben ser adjuntados directamente a tarjetas de Ether [14]. Hay dos desventajas principales de usar un cable Ethernet delgado. La primera es que esta limitado a 10Mb/seg - las redes de 100Mb/seg requieren cables de par trenzado. La segunda desventaja es que si se tiene un numero grande de computadoras interconectadas en círculo, y alguien interrumpe el círculo desconectando un solo cable, la red entera se desmorona por que el circuito esta abierto, en lugar de una terminación de 50 ohms [14]. Este tipo de cable es conveniente para segmentos entre 0.5m y 185 m y para conectar no más de 30 nodos. Este tipo de cables también se conoce como 10Base2.

También existen sistemas de cable que se ven como un solo cable entrando a la tarjeta, pero de hecho ese cable son dos cables que se pegan juntos y se cubren por una capa exterior, dando al cable una forma oval. Al girar el cable, un conector BNC que se conecta a la tarjeta es empalmado. Así se tienen equivalente de dos cables y un conector de BNC, pero en este caso es imposible para el usuario quitar el cable del conector y destruir la red [14].

En el caso de redes a base de par trenzado, se requieren concentradores activos y cables un poco más caros que los de Ethernet delgado. Cabe aclarar, que no se pueden usar los cables telefónicos para este tipo de red. Todas las sistemas de Ethernet de 100Mb/seg se basan en el par trenzado, así como la mayoría de instalaciones de negocios. Se recomienda usar el par trenzado de categoría 5. Si solo se conectan dos computadoras se puede evitar el uso de un concentrador, interconectando los pares Rx y Tx (1-2, 3-6). Si se coloca el conector RJ-45 de

frente (como si se lo quisiera conectar en la boca) entonces los pernos (o en inglés *pins* se enumeran de derecha a la izquierda, como se muestra en la Figura 8. Los usos de estos pernos se muestran en la tabla 5.

Perno	Para que se usa
1	Salida de datos (+)
2	Salida de datos (-)
3	Entrada de datos (+)
4	Reservado para uso telefónico
5	Reservado para uso telefónico
6	Entrada de datos (-)
7	Reservado para uso telefónico
8	Reservado para uso telefónico

Tabla 5: Descripción de los pernos para un conector RJ-45

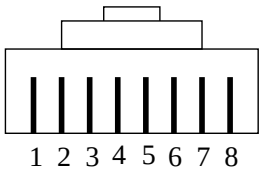

Figura 8: Un conector RJ-45

Si se quiere hacer un cable lo anterior lo explica claramente. Los pares diferenciados de la señal deben estar en el mismo par trenzado para obtener la pérdida mínima para un cable UTP. Si se examina la tabla, verá que 1 y 2, 3 y 6 son dos conjuntos de pares diferenciados de la señal . No 1 y 3, 2 y 6 !!! Usando 10 MHz y en distancias cortas aun con esos errores el cable posiblemente funcione, pero no en 100MHz [14].

Para un cable normal, que termina con “A” y “B”, se debe mapear directamente perno a perno (*pin-to-pin*), con la entrada y la salida cada uno usando cables de par trenzado. Eso significa que 1A va con 1B, 2A va con 2B, 3A va con 3B, 6A va con 6B. Los cables que unen 1A-1B y 2A-2B deben ser un par trenzado. De la misma manera los cables que unen 3A-3B y 6A-6B deben ser otro par trenzado. Como se muestra en la Figura 9 .

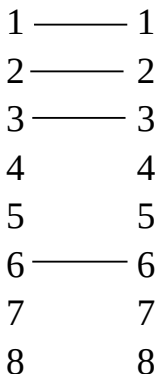

Figura 9: Un cable normal

Si no se tiene un concentrador y se quiere hacer un cable nulo, se debe conectar de tal manera que la entrada de “A” sea la salida de “B” y la salida de “A”- la entrada de “B” sin cambiar la polaridad. Esto significa que se debe conectar 1A con 3B (salida positiva de A con entrada positiva de B) y 2A con 6B (salida negativa de A con entrada negativa de B). Estos cables deben ser un par trenzado. Éstos llevan lo que tarjeta/enchufe “A” considera salida y lo que tarjeta/enchufe “B” considera salida. Luego se conecta 3A a 1B (entrada positiva de A con la salida positiva de B) y también 6A con 2B (entrada negativa A con salida negativa B). Estos dos también deben ser un par trenzado y llevan lo que tarjeta/enchufe A considera una entrada y la tarjeta/enchufe B considera una salida. Como se muestra en la Figura 10

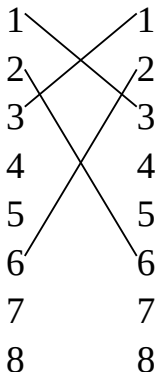

Figura 10: Un cable nulo

Así, si se tiene un cable normal se puede cortar uno de sus extremos, interconectar las posiciones de pares trenzados Rx y Tx en el enchufe nuevo y se obtendrá un cable nulo. No es complicado, solo se necesita encaminar la señal de Tx de una tarjeta a la señal RX de la otra y viceversa.

Cabe destacar que antes de que 10BaseT fuera estandarizado, existían otros formatos de redes que usaban el conector RJ-45 y el mismo esquema de cableado que describimos arriba. Los ejemplos son: LattisNet de SynOptics y StarLAN de AT&T. En algunos casos se podía configurar los puentes para que la tarjeta "hablara" con los concentradores de varios tipos, pero en la mayoría de los casos las tarjetas diseñadas para estas redes obsoletas no trabajarían con redes 10BaseT ó concentradores [14].

Referencias

[1] O. Kirch and T. Dawson. *Linux Network Administrators Guide*. O'Reilly, 2000.

[2] T. Parker and M.A. Sportack. *TCP/IP Unleashed*. SAMS, 1999.

[3] Redes-en-linux-como. Disponible en www.tldp.org.

[4] R. Hart. Ip sub-networking mini-howto, 2001. Disponible en www.tldp.org.

[5] Julio Cesar Chavez Urrea. Protocolos de red: Tcp/ip. Disponible en http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml.

[6] Vocabulary. http://www.tronlink.co.jp/e/vocabulary.html.

[7] Network components. http://www.d-m.com/documents/network/networks.html#routers.

[8] *High-Performance Networking Unleashed*. Macmilian Computer. http://docs.rinet.ru/NeHi/ch06/ch06.htm.

[9] What is a router? http://howto.lycos.com/lycos/step/1,,1+13+26124+24910+394,00.html.

[10] Introducción a redes ethernet. http://www.exert.com.ar/Intel/redes.htm.

[11] Dr. Fairhust. Course. http://www.erg.abdn.ac.uk/users/gorry/course/.

[12] D. Korin. Introduction to computer communication, 1994. http://www2.rad.com/networks/1994/modems/modem.htm.

[13] David S. Lawyer. Modem-howto. Julio 2003. http://www.tldp.org/HOWTO/Modem-HOWTO.html.

[14] Paul Gortmaker. Linux ethernet-howto. Octubre 2000. http://www.tldp.org/HOWTO/Ethernet-HOWTO.html.