

Tema 10° : INTERCONEXIÓN DE REDES

1. *Introducción*
2. *Conceptos generales*
3. *Puentes*
4. *Encaminadores*
5. *Diseño e Implementación de una Red Local*

10.1.- Introducción

Construir una red implica interconectar computadoras. De una red de dos computadoras a una red de miles de computadoras, de una red de unos metros a miles de kilómetros, de una red para enviar pequeños archivos esporádicamente a una red para comunicación multimedia en tiempo real, las tecnologías de interconexión, además de las de comunicación, son uno de los elementos fundamentales que van a condicionar un funcionamiento óptimo.

Evidentemente, no es lo mismo disponer de una red con cuatro computadoras en una oficina para compartir archivos, que una red con acceso a información desde varias oficinas, por todo el territorio de un país con garantía de seguridad en el acceso. En el primer caso, la conexión de las computadoras puede ser tan sencilla como un concentrador básico, mientras que en el segundo, puede ser casi tan complejo como las aplicaciones que se requiera utilizar, con el uso de encaminadores avanzados, conmutadores de tráfico, concentradores locales, etc. Los elementos a considerar en el diseño de redes, desde las más sencillas hasta las más complejas se verán con detalle al finalizar este tema, que se inicia con el tratamiento de los componentes de interconexión, la función que desempeñan para la conexión de computadoras su modo de funcionamiento.

10.2.- Conceptos Generales

Los componentes que permiten realizar la interconexión de computadoras y redes son los repetidores, concentradores, puentes, conmutadores, encaminadores y pasarelas.

La principal diferencia entre ellos está en el nivel del modelo de referencia OSI en el que actúan. Si bien existen dispositivos que actúan en casi todos los distintos niveles de comunicación del modelo OSI.

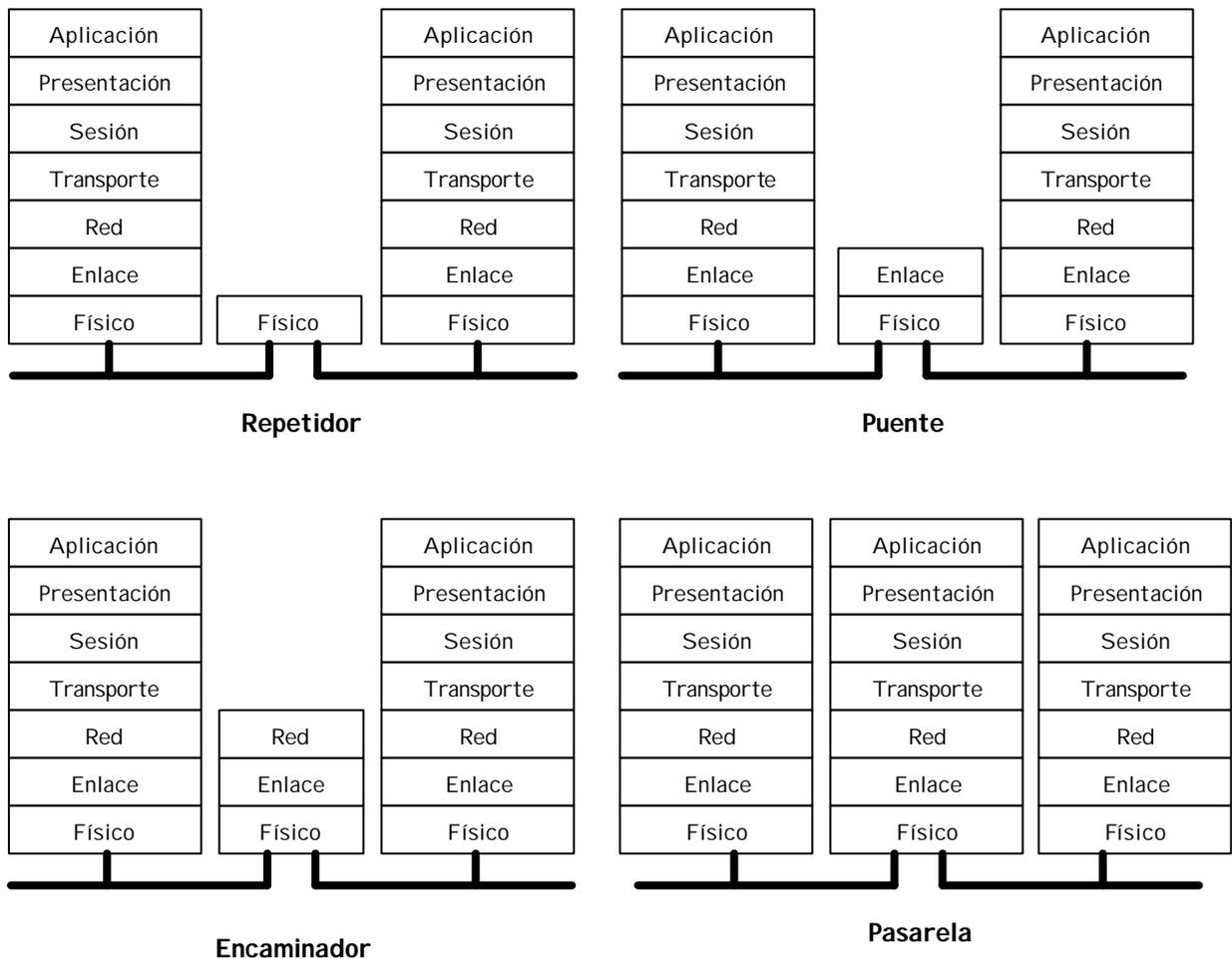
En la Figura adjunta se puede ver el ámbito en el que funcionan los principales componentes.

Los **repetidores** (*repeater*) solamente tienen en cuenta las características físicas de la señal de manera que los protocolos de enlace, red, etc., no se tienen en cuenta. Su función básica es de amplificación de la señal eléctrica.

Los **puentes** (*bridge*) tienen en cuenta el nivel de enlace, de manera que van a tratar de alguna forma las tramas que se crean en este nivel. Se utilizan para la conexión de redes con el mismo protocolo trasladando las tramas de una a otra.

Los **encaminadores** (*router*) llegan al nivel de red, por lo que tendrán en cuenta características propias de este nivel. Sirven para la interconexión de redes, siendo responsables de encontrar un camino para el transporte de la información de un origen a un destino.

Las **pasarelas** (*gateway*), al llegar al nivel de aplicación, son el componente más complejo de adaptación entre dos sistemas. Su uso está dirigido a la interconexión de redes que utilizan diferentes protocolos. A continuación se trata con más detalle cada uno de estos componentes, de manera que se obtenga una visión general del tipo de dispositivos que se pueden emplear para la interconexión de computadoras y redes.



10.2.1. - Repetidor (repeater)

Un repetidor es un dispositivo que permite conectar dos segmentos de red. Esencialmente se trata de considerar dos segmentos de red como si fuese uno solo, salvando de esta forma las restricciones de distancias que establece el protocolo dado. Un repetidor recibe señales desde uno de los segmentos, las amplifica, marca los tiempos y las retransmite al otro segmento. Y ello en ambos sentidos. De esta forma se evita la pérdida que puede sufrir la señal en un cable demasiado largo o en un cable con demasiados dispositivos conectados, regenerando la señal original hacia el otro segmento.

Un repetidor no realiza ninguna acción compleja sobre las señales que recibe. No es capaz de discriminar información, ni acumularla para conectar medios que tengan distintas velocidades. De manera que si recibe señales con errores, las amplifica y retransmite exactamente como él las ha recibido.

Un repetidor sólo se puede utilizar para extender el tamaño de la red. Es como poder utilizar un cable mayor para conectar dispositivos.

Aunque el uso de repetidores puede extender la longitud de la red, hay que tener ciertas precauciones al utilizarlos. Un repetidor simplemente retransmite todo lo que recibe de manera que al extender la red se está añadiendo a la misma todo el tráfico de las dos partes, con lo que resultará más fácil que ésta se sature. Asimismo, el número de repetidores que se pueden colocar es limitado. Suelen ser un elemento primordial en algunos tipos de comunicación como la comunicación inalámbrica o las comunicaciones ópticas, pero con el objetivo de salvar mayores distancias.

10.2.2. - Concentrador (hub)

Un concentrador es un elemento que ha evolucionado mucho con los años. Nace a partir de un elemento de concentración de cableado, principalmente, para redes del tipo CSMA/CD. Los primeros concentradores no eran más que repetidores de señal. Esta primera función de los concentradores ya permitía a los administradores de la red dividirla en segmentos diferenciados mejorando la gestión de la misma, aislando y controlando el tráfico. De ahí se pasa a los concentradores con cierta capacidad de gestión, que pueden informar de incidencias en los equipos que conecta.

Un concentrador recibe conexiones de todos los equipos conectados al mismo, de manera que existe una línea física entre cada equipo y el concentrador. El concentrador tiene un elemento interno, denominado **plano posterior** (*backplane*), al que se conectan todas estas conexiones, formando efectivamente un bus para todos ellos. Es decir, todos los equipos comparten ese bus. Cuando un equipo transmite algo, llega al bus, ya través de él se transmite a todos los equipos conectados al concentrador.

Con su evolución aparecieron concentradores que tenían dentro varios buses que permitían gestionar por separado varios segmentos de red. Y así han ido añadiendo más funcionalidad para convertirse en un elemento que incorpora funciones que eran típicas de otros más complejos. En la actualidad la tendencia es a convertirse en elementos de interconexión para redes de alta velocidad.

Un concentrador es el dispositivo apropiado para instalar una red local de forma rápida. Basta, básicamente, con conectar todas las computadoras al concentrador y configurar un protocolo y las direcciones de red.

El uso de los concentradores permite crear segmentos de equipos que, a su vez, se conectan con otros segmentos, bien a través de una jerarquía de concentradores, lo que pone a todos a un mismo nivel desde el punto de vista de la red, teniendo tan sólo en cuenta las temporizaciones máximas del protocolo, o bien, mediante puentes, encaminadores, etc.

10.2.3. - Puente (bridge)

Un puente es un componente con una función en el nivel de enlace del modelo de referencia OSI. Un puente opera con las tramas que se crean en el nivel de enlace y, más concretamente, en el nivel de control de acceso al medio (MAC). Su objetivo es la interconexión de dos redes (segmentos de red), siempre que en ambas se utilice el mismo protocolo. Al actuar al nivel MAC, es necesario que el protocolo de enlace en las redes que conecta sea el mismo.

Algunos de los objetivos que se cubren con el uso de un puente frente a una gran red son: una mayor fiabilidad, ya que si falla una de las redes la otra puede seguir funcionando, un mayor aislamiento de la información, manteniendo dentro de cada segmento el tráfico

propio (contabilidad, marketing, proyectos, etc.), un mayor rendimiento, al circular por cada segmento sólo el tráfico de dicho segmento, entre otras.

El funcionamiento básico de un puente es muy sencillo. El puente recoge todos los paquetes que circulan en cada segmento. Cuando en uno de los segmentos hay un paquete para el otro, retransmite dicho paquete hacia el otro segmento de red.

El puente no realiza ningún cambio al contenido o formato de las tramas que recibe. Tiene que tener cierta inteligencia, pues debe ser capaz de conocer que direcciones de red existen en cada uno de los segmentos, de manera que pueda decidir si una trama debe retransmitirla al otro segmento o no. Incluso si existen más de dos redes o segmentos de red interconectadas por puentes, un puente debe conocer a qué direcciones se puede llegar, no sólo desde el otro segmento, sino atravesando otros puentes. Es en este punto donde surgen los distintos tipos de puentes y sus estrategias de funcionamiento, que se verán más adelante.

Un puente sirve para segmentar una red. Es decir, para dividir una red en redes de menor dimensión conectadas entre sí.

Un puente ofrece mayor funcionalidad que un repetidor y también mayor retardo en la retransmisión de las tramas entre las redes que separa. Se utiliza principalmente en entornos de redes locales para dar soporte a la segmentación de la red, aunque también se utilizan, en ocasiones, para la interconexión de redes de área local mediante circuitos de comunicaciones de área extensa.

10.2.4. - Conmutador (switch)

Los conmutadores son componentes con una función en el nivel de enlace, como los puentes, y surgen como una evolución de los mismos. En muchos casos, incluso, van ocupando el lugar en que antes se utilizaban puentes para la interconexión. Además de las funciones de los puentes, aportan un mayor rendimiento, un mayor número de puertos, menor coste por puerto, mayor flexibilidad y funciones adicionales como el filtrado.

10.2.5. - Encaminador (router)

Un encaminador actúa hasta el nivel de red. Cuando un encaminador recibe un mensaje de una red dirigida a otra red, el encaminador es el responsable de encontrar un camino, el mejor posible en cierto sentido, para dirigir ese mensaje. Un encaminador difiere de un puente, que también dirige mensajes a otras redes, en varios aspectos:

- ❖ El encaminador tiene en cuenta la información del nivel de red de los mensajes. La información del nivel de enlace se modifica, descartando la información del nivel de enlace que hubiese llegado con el paquete.
- ❖ Entienden el esquema de direcciones jerárquico con que tienen asignadas direcciones las redes, de manera que almacenan información sobre redes y rutas entre las mismas.
- ❖ Utilizan algún tipo de algoritmo de enrutamiento para encontrar la mejor ruta, en algún sentido, hacia el destino.

- ❖ Un mensaje puede seguir varias rutas posibles, a través de varios encaminadores. De esta forma se consigue aumentar la fiabilidad de las comunicaciones, pues si una ruta falla, se puede utilizar otra.
- ❖ Suelen tratar con redes de distinta naturaleza, con distintos protocolos. En este caso se denominan encaminadores multiprotocolo. Un uso típico podría ser conectar un conjunto de redes de área local a través de un anillo FDDI, donde cada red se conecta al anillo a través de un encaminador.
- ❖ Al tratar con protocolos diferentes pueden tener que dividir el mensaje en trozos, porque el tamaño máximo de mensajes de una red sea menor que en la otra. A este proceso se llama segmentado. El proceso contrario es el de reensamblado.

Un encaminador dispone, en general, de muchas más funciones y capacidades que un concentrador, pero también resulta más complejo de configurar apropiadamente.

Un encaminador incrementa el retardo de transmisión de los mensajes más que los componentes anteriores, pero son de mayor utilidad pues incorporan funciones adicionales como el filtrado de paquetes, mecanismos de seguridad, etc.

10.2.6. - Pasarela (gateway)

Una pasarela actúa en niveles superiores al de red, pudiendo llegar al nivel de aplicación. Se requiere de una pasarela en aquellos casos en que la adaptación entre las dos redes requiera una conversión de los protocolos superiores al protocolo de red. Proporcionan conectividad entre redes de distinta naturaleza.

Por ejemplo, si desde una red Novell se deseará acceder a computadoras en una red SNA, se necesitaría una pasarela que pudiese hacer la traducción completa de los protocolos Novell a los protocolos propios de la arquitectura SNA. La pasarela estaría conectada a ambas redes como intermediario y tiene que implantar ambos protocolos completos. Sin embargo, esta adaptación a veces no es tan buena como uno desearía pues hay funciones de una arquitectura de red que la otra no es capaz de proporcionar, o viceversa.

Aunque rara vez se necesitará una pasarela. Este tipo de dispositivos de interconexión se utiliza cuando los sistemas que hay que poner a funcionar conjuntamente siguen especificaciones diferentes, incluso desde el punto de vista del usuario.

Al introducir una pasarela incrementa el retardo de transmisión de los mensajes entre ambas redes más que con los anteriores dispositivos de interconexión. A estos dispositivos también se les llama en algunas ocasiones encaminadores (router), por ejemplo, en TCP/IP, como generalización de los mecanismos de interconexión de los encaminadores

10.3. - PUENTES

Como ya se ha comentado, un puente actúa en el nivel de enlace. Su funcionamiento básico es muy sencillo. Un puente conecta dos segmentos de red que utilizan el mismo protocolo. El puente recoge todos los paquetes que circulan en el segmento 1, por ejemplo. Cuando hay un paquete para el segmento 2, retransmite dicho paquete en el segmento 2. Actúa de la misma forma cuando hay un paquete del segmento 2 dirigido al segmento 1.

Además de unir dos segmentos de red, puede haber varios segmentos de red unidos por puentes. Cuando una computadora envía un mensaje a un segmento que no está unido directamente al mismo puente que la computadora que envía el mensaje, el mensaje debe atravesar varios puentes hasta llegar a la computadora de destino. Por ello, un puente debe tener cierto conocimiento de los segmentos de red que existen más allá de aquellos a los que está conectado.

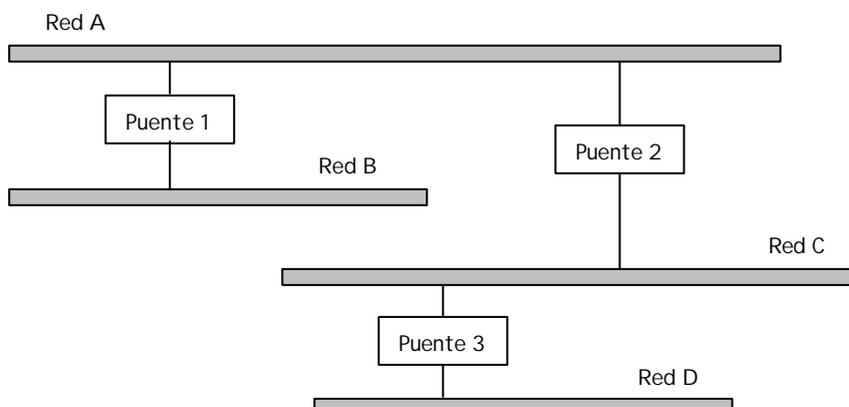
Existen distintas estrategias para redirigir los mensajes por el camino apropiado. En las siguientes secciones se verán distintos tipos de enrutamiento que llevan a cabo los distintos tipos de puente:

- Puentes transparentes, usados principalmente en entornos Ethernet.
- Puentes con enrutamiento fuente, usados principalmente en entornos Token Ring.
- Por último, se tratan los puentes con enrutamiento fuente-transparente, que se utilizan para la interconexión de entornos Ethernet con entornos Token Ring.

Todos ellos son enrutamientos dinámicos, es decir, se crean durante el funcionamiento del puente. Existe un tipo de enrutamiento más sencillo que es el enrutamiento estático. Antes de poner en funcionamiento el puente se conoce la topología de la red, es decir, las computadoras que existen y sus interconexiones. De esta forma se conoce el camino que deben seguir los mensajes entre dos computadoras cualesquiera. Si existe más de un camino se suele elegir el que menor número de saltos requiere. Se denomina **salto** a cada paso por un puente o encaminador.

En la tabla de enrutamiento viene recogido para cada segmento de red destino de un mensaje a qué red se traslada el mensaje. Si en la tabla no se recoge la transmisión es porque hay otro puente que ya realizará la transmisión a través de un camino con menos saltos.

Por ejemplo, como se puede ver en la Figura adjunta existen cuatro segmentos de red conectados mediante 3 puentes. El enrutamiento estático para esta red puede recogerse en la Tabla de **Selección de puente**. En ella se puede ver cuál es el puente por el que se debe dirigir el tráfico para ir a determinada red de destino. Por ejemplo, para ir de la red B a la red C el puente a elegir es el 1. Las tablas de cada uno de los puentes serán entonces las que se pueden ver en la Tabla **de enrutamiento de cada uno de los puentes**. Como se puede observar, el puente 1 está conectado a la red A y a la red B. Cuando recibe un mensaje de la red A, y el destino del mismo es la red B, debe copiar el mensaje en la red B. Cuando recibe un mensaje de la red B, y el destino del mismo es la red D, debe copiar el mensaje en la red A. Otro puente se encargará entonces de seguir transmitiéndolo.



Como puede verse en la tabla adjunta, no tiene sentido que el puente 1 reciba por la red A un mensaje para la red D, ya que no podría redirigirlo y, por tanto, este puente no hace nada con dichos mensajes.

Tabla de selección de puente

		RED DE DESTINO			
		A	B	C	D
RED DE ORIGEN	A	-	1	2	2
	B	1	-	1	1
	C	2	2	-	3
	D	3	3	3	-

Tabla de enrutamiento en cada uno de los puentes

PUENTE 1			
De la red A		De la red B	
<i>Destino</i>	<i>Siguiente</i>	<i>Destino</i>	<i>Siguiente</i>
B	B	A	A
C	-	C	A
D	-	D	A
PUENTE 2			
De la red A		De la red C	
<i>Destino</i>	<i>Siguiente</i>	<i>Destino</i>	<i>Siguiente</i>
B	-	A	A
C	C	B	A
D	C	D	-
PUENTE 2			
De la red A		De la red C	
<i>Destino</i>	<i>Siguiente</i>	<i>Destino</i>	<i>Siguiente</i>
B	-	A	A
C	C	B	A
D	C	D	-

10.3.1. - Tipos de puentes

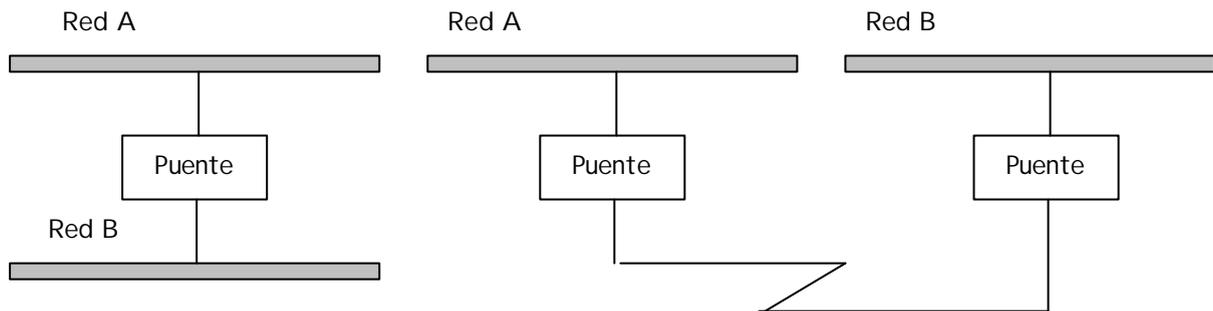
Una clasificación habitual de los puentes distingue entre puentes locales y puentes remotos.

- Un puente local proporciona conectividad entre segmentos de una red dentro de un área local, como puede ser una oficina, una planta de un edificio o un edificio.
- Los puentes remotos conectan segmentos de redes en áreas diferentes, normalmente interconectados mediante líneas de telecomunicaciones, por ejemplo, enlaces dedicados, líneas RDSI, etc.

Un puente también se puede utilizar como dispositivo de conexión a través de una red de área extensa. Sin embargo, se suele preferir un encaminador.

En la figura adjunta se puede ver una representación esquemática de la diferencia entre un puente local y un puente remoto.

Los puentes remotos tienen que solventar algunos problemas derivados de la interconexión a través de redes, normalmente, públicas. El principal de ellos es la diferencia de velocidad entre el medio de comunicación de una LAN y el de una WAN, que conecta los dos segmentos remotos. En este caso, la velocidad de comunicación de una LAN suele ser muy superior a la de una WAN. El uso de los puentes remotos ha de realizar una adaptación de las velocidades entre los tramos de red de la LAN y de la WAN.



La adaptación de velocidades se realiza mediante el uso de buffers intermedios en el puente. De esta forma cuando el puente recibe información para el otro extremo de la red, la recibe a la velocidad de la LAN, por ejemplo, 10 Mbps, y ha de entregarla a través de una línea RDSI a 64 Kbps. Al recibirla la guarda en un buffer propio y desde el buffer la va enviando a la línea RDSI. Este modo de funcionamiento implica que la cantidad de información que se envía al otro extremo debería estar en consonancia con la velocidad a la que el puente puede enviar la información sin que se llene el buffer que está utilizando, ya que tiene una memoria limitada.

Otro problema que se debe resolver es la adaptación del tipo de tramas que se transmiten por el medio de comunicación de la WAN. En este caso se pueden utilizar dos técnicas diferentes:

- **Encapsulamiento:** en este caso, la trama de la LAN se inserta completa como datos de una trama de la WAN. De esta forma es como si se crease una envoltura para la trama original que se desenvuelve al llegar al otro extremo de la WAN.
- **Traducción:** se realiza una traducción de las tramas de la LAN en tramas equivalentes de la WAN, por ejemplo, FDDI. En este caso, la traducción resuelve las limitaciones sobre funciones que pueden estar presentes en una de las redes, pero no en la otra.

La traducción se debe utilizar si existen computadoras conectadas directamente a la red de comunicaciones. Si la red WAN sólo se utiliza para transmitir la información a otra red o segmento de red remoto, es preferible el uso del encapsulamiento, pues se preserva sin modificaciones la trama enviada originalmente.

10.3.2. - Puentes transparentes

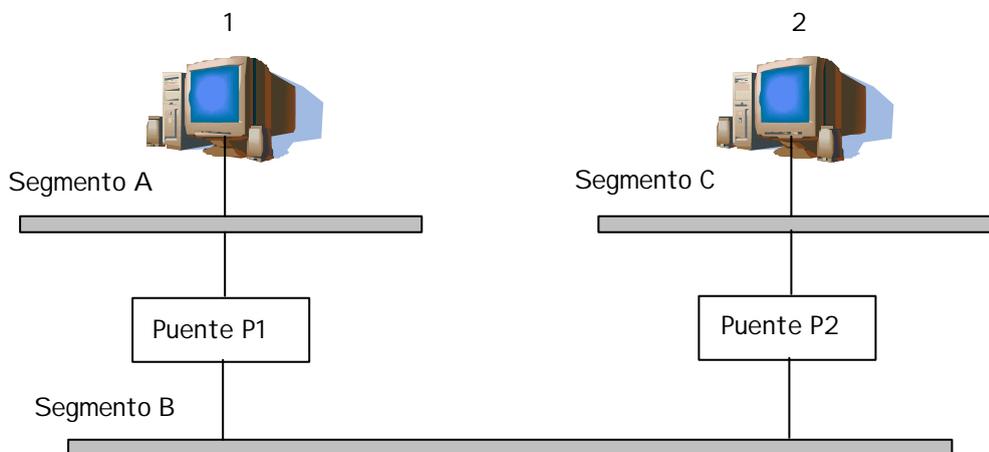
Los puentes transparentes (*Transparent Bridge*), también llamados *Learning bridges*, se denominan de esta forma porque para las computadoras conectadas a la red, es como si no

existiesen. Para ellas es igual si están o si no están. Un puente transparente va aprendiendo la topología de la red, es decir, las direcciones hardware, por observación de los mensajes que se transmiten por ella.

Cuando se conecta un puente transparente, inicialmente no tiene información de qué equipos están conectados a cada segmento de red. Cuando el puente lee un mensaje del segmento A de la red, por ejemplo, proveniente de la computadora 1, ya sabe que la computadora 1 está en el segmento A y añade esta entrada en la tabla. Véase la figura adjunta.

Cuando el puente recibe una trama para un determinado destino examina la tabla, si existe una entrada que indica dónde se encuentra el equipo de destino, lo envía a ese segmento de red. Si no se encuentra, retransmite la trama por todos los puertos de salida, excepto por el que se recibió la trama. De esta forma, en algún momento, el equipo de destino responderá, con lo que el puente recibirá una trama hacia la estación origen, apuntando en la tabla el segmento donde está conectado dicho equipo. La próxima vez que se repita la comunicación ya sabrá dónde localizarle

Por ejemplo, en la figura si se supone que la computadora 1 en el segmento A envía una trama a la computadora 2 en el segmento C. Al recibir la trama el puente P1 apunta en su tabla que la computadora 1 está en el segmento A. Como no tiene información sobre la computadora 2 retransmite la trama al segmento B. Esta trama la lee el puente P2, que apunta en su tabla que la computadora 1 está en el segmento B, y retransmite la trama al segmento C, llegando a la computadora de destino.



Cuando la computadora 2 responde recibe la trama el puente P2, que apunta que la computadora 2 está en el segmento C. En este momento ya sabe que la computadora 1 está en el segmento B, por lo que retransmite en ese segmento la trama. La trama la recibe, entonces, el puente P1 que apunta en su tabla que la computadora 2 está en el segmento B y retransmite la trama en el segmento A, pues era donde la tenía apuntada.

En redes mayores que las del ejemplo es importante el uso de mejores algoritmos de redirección de tráfico.

Para mantener una tabla actualizada, periódicamente se borran de la tabla las entradas que llevan más tiempo sin utilizarse. A esta estrategia se la denomina LRU (Least

Recent Use; Menos uso reciente). Cuando se reciba alguna trama de ellas se volverán a añadir a la tabla.

En una red grande, es normal que existan varios caminos entre dos estaciones. En este caso, el funcionamiento anterior de los puentes transparentes puede hacer que no se retransmitan los mensajes de manera oportuna, perdiéndose, o que se creen bucles de mensajes que pueden colapsar la red. Observe la configuración donde existen dos segmentos de red unidos por dos puentes. Cuando una computadora del lado izquierdo envíe una trama a alguna del lado derecho, ambos puentes reciben la trama y apuntan en sus tablas que dicha computadora está en el lado izquierdo, y retransmiten la trama hacia el lado derecho. Esta trama se transmite por el lado derecho y ambos puentes reciben la trama del otro con lo que ambos apuntan que la computadora inicial está en el lado derecho, cambiando la tabla. Cuando la computadora de destino responda, como ambos puentes han apuntado que la estación inicial está en el lado derecho, nunca retransmitirán la trama hacia el lado izquierdo con lo que la comunicación será imposible.

Sin embargo, las redes con múltiples caminos de comunicación son muy interesantes, pues permiten la comunicación aunque haya problemas en algunos de los puentes que conectan segmentos de red. Para que no ocurran problemas, en redes reales se utiliza otro tipo de algoritmos como el algoritmo de árbol de expansión (STA, Spanning Tree Algorithm). De hecho, los puentes están obligados a implementar este algoritmo de acuerdo con la norma IEE 802.1d.

Los puentes, según la norma IEEE 802.6, han de disponer del algoritmo de árbol de expansión, en su redirección de la información por la red.

El algoritmo de árbol de expansión:

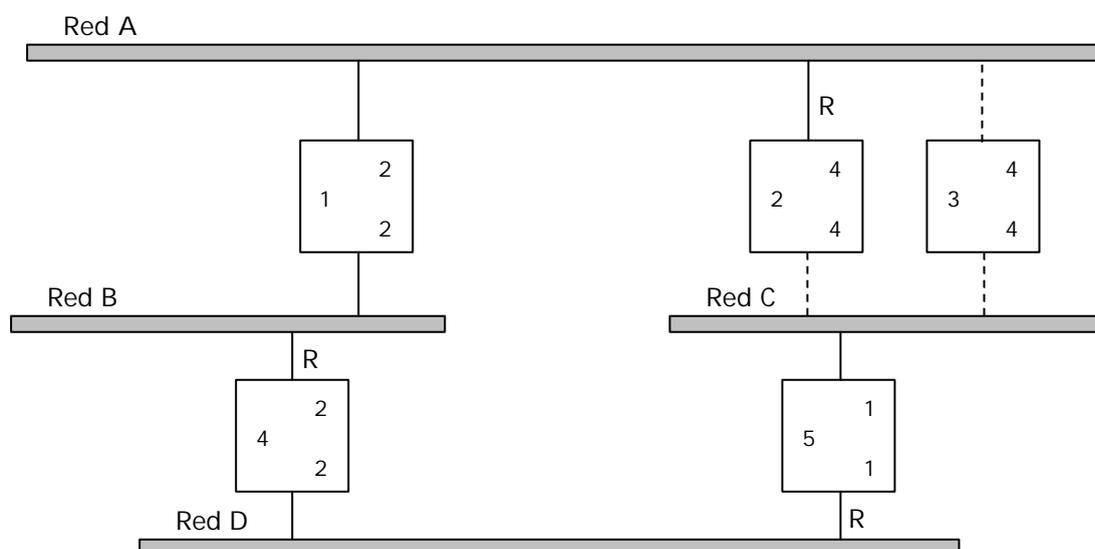
- Da identificadores únicos a los puentes, que puede ser su dirección MAC.
- Cada puerto del puente queda identificado por su identificador de puerto y la dirección MAC del puente.
- Se asigna a cada puerto un coste de trayecto. Al final se elegirá el trayecto cuyo coste sea el menor. Si el coste se asigna a uno, el coste de un trayecto es el número de saltos que hay que realizar.
- Se selecciona el puente con menor identificador como puente raíz. En realidad al principio todos se declaran raíz, estado que van cediendo por observación de los identificadores del resto.
- A continuación el resto de los puentes determinan cuáles de sus puertos que están conectados al puente raíz lo hace con coste mínimo. A estos puertos se les denomina **puertos raíz**. Los puertos raíz son los únicos por los que se puede realizar la retransmisión de tramas. El resto de los puertos no retransmiten las tramas hacia el puente raíz. Si se encuentran dos trayectos con el mismo coste se elige el puente con un menor identificador.
- Los puentes van construyendo de esta forma los caminos hacia el puente raíz. Con ello se consigue que entre cada dos segmentos sólo exista un trayecto, ya que si existiese más de uno, uno de ellos quedaría bloqueado al no ser considerado el de menor coste.

Para llevar a cabo este proceso los puentes intercambian información utilizando un tipo de tramas especiales denominadas Unidades de datos del protocolo de puente (**BPDU**, **Bridge Protocol Data Unit**). Estas tramas contienen información sobre identificadores de puente y puerto, el puente raíz y el coste calculado hasta el puente raíz. Inicialmente todos los puentes consideran que el puente raíz son ellos mismos. Según van conociendo la identidad de otros puentes van indicando que el puente raíz es aquel que menor identificación tenga.

En la próxima figura se puede ver un ejemplo de cómo se construiría un árbol de expansión de la red de la izquierda. En la red se han dibujado con líneas discontinuas los enlaces bloqueados, que no pertenecen al árbol de expansión.

Para calcular el árbol de expansión, se ha seguido el algoritmo expuesto anteriormente. Cada puente tiene su identificador en el centro. Se ha situado el coste del trayecto, a través de cada puerto, en la parte interior al lado de la conexión con el puente. Se selecciona el puente raíz como el puente número 1 que conecta la red A con la red B.

Para la red A, el puente que tiene acceso a la red C con coste mínimo es el puente 2, por lo que el puente 3 bloquea su conexión con la red A. Para la red B, sólo existe el puente 4, que mantiene su conexión. El coste acumulado de llegar al puente raíz para el puente 2 es de 4 y para el puente 4 es de 2. Los puertos raíz se han marcado con la letra R en su parte exterior. Para la red D el coste por el puente 5 es de 5 ($1 + 2 + 2$) que mantiene su conexión. Para la red C el coste por el puente 2 (el puente 3 ya está bloqueado) es de 8 ($4 + 4$). El coste para el puente 5 es de 6 ($1 + 1 + 2 + 2$), por lo que se bloquea el enlace del puente 2 con la red C.



Como se puede observar, en la red resultante, teniendo sólo en cuenta los enlaces sólidos, ya que los enlaces con línea discontinua no permiten el paso de información, no existen bucles.

10.3.3. - Puentes de enrutamiento fuente

Los puentes con enrutamiento fuente (**SRB**, **Source Route Bridge**) se utilizan normalmente en redes Token Ring y, de hecho, la norma que define este tipo de encaminadores se encuentra en el estándar IEEE 802.5. En este tipo de enrutamiento es el equipo transmisor quien decide el trayecto que va a seguir el mensaje que emite. Los puentes

recogen los mensajes de los segmentos de red a los que están conectados y si alguna trama indica que el mensaje debe pasar por él lo retransmiten hacia el siguiente segmento de red indicado en la propia trama.

En el enrutamiento fuente, es el nodo que envía la información quien determina la ruta que sigue la información hasta el nodo de destino, aunque haya de atravesar varias redes

Para poder llevar a cabo este mecanismo es necesario que los equipos sepan el camino que pueden seguir los mensajes hacia su destino. Para ello se utilizan mensajes especiales de descubrimiento de ruta. En el campo de directiva de ruta a seguir se pueden poner cuatro elementos distintos:

- **null:** indica que ningún puente debe retransmitir el mensaje. Por tanto el mensaje debe estar dirigido a una computadora de la misma red que el emisor.
- **Sin difusión:** en este caso, en el mensaje debe ir la ruta completa que debe seguir el mensaje. La ruta completa debe incluir los puentes y direcciones de red por los que debe pasar el mensaje, de manera que defina una ruta completa desde origen a destino.
- **Con difusión:** la trama llegará a toda la red a través de todos los puentes. La computadora de destino recibirá tantos mensajes como posibles caminos pueda seguir el mismo. En cada puente, al retransmitir la trama se añade información del puente que se ha utilizado y la red a la que se transmite. De esta forma, al llegar a la computadora de destino, ésta ya conoce la ruta que debe utilizar para responder a la computadora origen. La computadora de destino envía un mensaje de respuesta por cada mensaje recibido. Cuando la computadora de origen recibe todas las respuestas selecciona uno de los caminos, normalmente, el primero que recibe, pues será el más rápido.
- **Con difusión única:** la trama se envía a la red para que siga el árbol de expansión. Al seguir el árbol de expansión la computadora de destino recibirá una única copia del mensaje. En cada puente se añade a la trama el camino que ha ido siguiendo, al igual que en el caso anterior. Cuando la computadora origen reciba respuesta a su mensaje, en él podrá encontrar la ruta completa para comunicarse con la computadora de destino.

Evidentemente el caso de encontrar la ruta utilizando la difusión única genera muchas menos tramas en la red que el uso de difusión completa. Sin embargo, es necesario conocer con anterioridad el árbol de expansión de la red, que se puede obtener de la forma descrita en la sección anterior.

10.3.4. - Enrutamiento fuente-transparente

El enrutamiento mixto fuente-transparente (**SRT, Source Route Transparent**) es necesario en aquellos entornos donde convivan segmentos de red Ethernet y Token Ring. En este caso, el puente que haga de intermediario entre segmentos de red con estos dos protocolos debe utilizar enrutamiento transparente hacia el segmento con el protocolo Ethernet y enrutamiento fuente hacia el segmento con el protocolo Token Ring.

Como se ha comentado en las secciones anteriores ambos tipos de enrutamiento deben conocer el árbol de expansión, de manera que este árbol se puede utilizar para la comunicación en ambas redes de la siguiente forma: Cuando se transmite un mensaje de la red con enrutamiento transparente hacia la red con enrutamiento fuente, el puente recibe la trama y puede dirigirla a su destino utilizando la directiva de ruta con difusión única, es

decir, siguiendo el árbol de expansión. Cuando una computadora en la red con enrutamiento fuente utiliza una directiva con la ruta completa, al llegar al puente intermediario, convierte el enrutamiento fuente en un enrutamiento transparente a través de la red con enrutamiento transparente.

10.4. - ENCAMINADORES

Un encaminador es un componente de interconexión que crea y mantiene una tabla de trayectos a través de la red y de sus correspondientes condiciones para, junto con un algoritmo, determinar en términos de distancia o coste, el mejor camino que debe seguir un paquete a una computadora de destino. Habitualmente el trayecto de un paquete a través de la red utilizará varios encaminadores antes de llegar a su destino. Los encaminadores suelen emplearse en redes de cierta complejidad, aunque en algunos casos se puede preferir un encaminador a un puente, por las funciones adicionales que ofrece, como filtrado de paquetes, agentes proxy, seguridad, etc.

Un encaminador es un dispositivo que puede llegar a ser complejo de configurar. Un encaminador puede ofrecer funciones de filtrado de paquetes, por multitud de características, seguridad de red, restricciones de acceso, etc.

10.4.1. - Principios básicos de enrutamiento

El enrutamiento es un concepto de nivel de red, un nivel superior al nivel de retransmisión propio de los puentes que actúan en el nivel de enlace. En lugar de hablar de enrutamiento de nivel de red, a partir de ahora sólo se hablará de enrutamiento. Todas las máquinas de la red donde se lleva a cabo el enrutamiento utilizan el mismo formato de direcciones de red, independientemente del protocolo de enlace que se esté utilizando en las distintas subredes, ya sea Ethernet, Token Ring, FDDI, etc.

Las direcciones de nivel de enlace, habitualmente la dirección MAC, son únicas para una determinada interfaz de red, dentro de un determinado nivel de red. Por ejemplo, las direcciones MAC de tarjetas Ethernet siempre son únicas. Las direcciones del nivel de red están compuestas de dos partes: una parte que identifica la red y otra que identifica un equipo o computadora dentro de esa red. Un puente sólo puede conectar redes con el mismo protocolo del nivel de enlace de datos o protocolos relativamente similares (Ethernet y Token Ring, por ejemplo). Un encaminador se suele emplear para la interconexión de redes con protocolos del nivel de enlace diferentes, siempre que compartan el mismo protocolo de nivel de red.

Aparentemente un puente y un encaminador realizan funciones de enrutamiento similares. La diferencia está en que un puente actúa en el nivel de enlace, sólo redirige tráfico, y un encaminador en el nivel de red, indica trayectos para el tráfico, por lo que ambos utilizan información completamente diferente para llevar a cabo su trabajo. Por ello, los métodos y algoritmos de enrutamiento son también diferentes.

10.4.2. -Resolución de direcciones

Para que funcione correctamente el enrutamiento de nivel de red es necesario realizar una correspondencia entre las direcciones de red y las direcciones del nivel de enlace. Las direcciones del nivel de enlace vienen asignadas con la interfaz de red desde fábrica, y son las que se utilizan en último término para la comunicación a través de la red.

Las direcciones del nivel de red las asigna el administrador de la red a su elección, siendo independientes del nivel de enlace.

Las direcciones del nivel de enlace se pueden obtener, a partir de las direcciones del nivel de red, mediante el Protocolo de resolución de direcciones (ARP, Address Resolution Protocol). Supóngase dos computadoras A y B en la misma red. La computadora A difunde un mensaje ARP pidiendo la dirección MAC de B. Este mensaje lo reciben todos los equipos conectados a la LAN, pero sólo responde B con su dirección MAC. En ese momento B ha apuntado en su caché de ARP la dirección MAC de A y A ha apuntado en su caché de ARP la dirección MAC de B. De esta forma cuando A envíe un mensaje a B sólo tiene que consultar en su caché la dirección MAC de B a la que tiene que enviar el mensaje.

El protocolo es un poco diferente cuando la computadora de destino se encuentra en otra red. Suponga dos computadoras A y Z situadas en redes diferentes interconectadas a través de uno o más encaminadores.

- Cuando A intenta obtener la dirección MAC de Z difunde por la red un mensaje ARP. Igual que antes todos los equipos conectados a la LAN reciben el mensaje.
- El encaminador E también recibe el mensaje y observa en su tabla de enrutamiento que es para una computadora que se encuentra en otra red. El encaminador responde a la petición de dirección MAC con su propia dirección MAC haciendo de sustituto de la computadora de destino.
- Cuando A reciba la respuesta apuntará como dirección MAC de la computadora Z la dirección MAC del encaminador E.
- Cuando A envíe un mensaje a Z busca su dirección MAC, encuentra la dirección MAC en su caché de ARP, que en realidad es la del encaminador, y le envía a este último el mensaje.
- El encaminador recibe el mensaje y lo redirige hacia la computadora Z.

Esta segunda parte, cuando la máquina de destino se encuentra en una red diferente, se puede eliminar si se actúa de manera inteligente. Basta con comprobar con la máscara de red que la dirección de red dada está en una red distinta. En este caso se dirige el mensaje al encaminador definido para comunicarse con dicha red.

Hablar de dirección MAC implica el uso de uno de los protocolos definidos bajo los estándares del IEEE. Otros protocolos no necesitan este proceso de obtención de la dirección MAC, pues ésta está incluida dentro de la dirección de nivel de red o se puede utilizar un algoritmo para obtenerla. Estos protocolos son XNS (Xerox Network System), IPX (Novell Internet-work Packet Exchange) y DECnet Phase IV.

10.4.3. - Algoritmos de enrutamiento

Los algoritmos de enrutamiento pueden tener características muy diversas. Dependiendo de sus características pueden afectar al rendimiento de la red, al uso de recursos en el encaminador, cuál es la mejor ruta calculada, etc. Entre los elementos deseables para un algoritmo de enrutamiento estarían:

- **Capacidad de seleccionar la mejor ruta.** Evidentemente la mejor ruta dependerá de la medida que se use para comparar unas con otras, número de saltos, velocidad, ancho de banda, etc.
- **Simplicidad y poca necesidad de recursos,** para que no represente una sobrecarga su cálculo y, por tanto, no ralentice la función de enrutamiento. Cuantos menos recursos se necesiten para calcular la ruta más paquetes por segundo podrán enrutarse.
- **Robustez,** con capacidad de comportarse correctamente ante situaciones no esperadas de la red, como saturación, encaminadores fuera de servicio, etc.
- **Estabilidad,** ofreciendo siempre una respuesta correcta ante variaciones en la topología de la red por eliminación o adición de nuevos encaminadores.
- **Con rápida convergencia,** de manera que se obtenga la mejor ruta en poco tiempo de operación, sobre todo después de un problema serio en la red, la rotura de un enlace, el apagado de un encaminador etc

Según el esquema de funcionamiento se pueden dividir los algoritmos de enrutamiento en:

- ❖ **Estáticos-dinámicos,** si cambian o no en el tiempo sus tablas de enrutamiento.
- ❖ **Unirruta-multirruta,** si pueden dirigir tráfico para un mismo destino por una única ruta o pueden dividirlo entre varias rutas.
- ❖ **Espacio plano-jerárquico,** si manejan una jerarquía de encaminadores o consideran la red de forma plana.
- ❖ **Inteligencia en el host-en el encaminador,** si quien conoce la ruta es quien envía los mensajes o los sistemas intermedios de enrutamiento
- ❖ **Intradominio-interdominio,** si se utiliza dentro de un dominio o para crear rutas entre dominios.
- ❖ **Por vector de distancia-por estado del enlace,** si lo que se cuenta es la distancia hasta el destino en términos de saltos o si se tiene en cuenta parámetros como tráfico, ancho de banda, velocidad de respuesta u otros.

10.4.4. - Enrutamiento en el modelo Internet

Para simplificar el número de algoritmos de enrutamiento y ver sólo algunos de los principales, en esta sección nos vamos a limitar a los algoritmos de enrutamiento utilizados en el modelo Internet. Pero antes hay que aclarar algunos términos.

- **Dominio:** conjunto de nodos que se encuentran bajo una misma administración y control.

Frontera de dominio: aquellas máquinas que sirven para conectar un dominio con su exterior sirviendo de enlace entre la parte interna al dominio y la parte externa.

En Internet se pueden encontrar los siguientes algoritmos de enrutamiento:

- **EGP (*Exterior Gateway Protocol; Protocolo de pasarela exterior*)**. Comunica dos encaminadores en la frontera de los dominios.
- **BGP (*Border Gateway Protocol; Protocolo de pasarela frontera*)**. Sustituto del protocolo EGP. Comunica dos encaminadores interdominios. También puede utilizarse como protocolo dentro de un dominio.
- **IGRP (*Interior Gateway Routing Protocol; Protocolo de enrutamiento de pasarela interior*)**. Comunica dos encaminadores internos, es decir, dos encaminadores dentro de un mismo dominio de administración.
- **EIGRP (*Enhanced Interior Gateway Routing Protocol; Protocolo de enrutamiento de pasarela interior mejorado*)**. Es una mejora del protocolo IGRP para interredes muy grandes.
- **RIP (*Routing Information Protocol; Protocolo de información de enrutamiento*)**. Uno de los primeros protocolos de enrutamiento. Sólo sirve para redes relativamente estables y pequeñas.
- **SPF (*Shortest Path First; Primero el camino más corto*)**. Algoritmo de estado de enlace que mejora el algoritmo RIP.
- **OSPF (*Open Shortest Path First; Primero el camino más corto abierto*)**. Es una mejora del protocolo SPF, con muy buenas características de escalabilidad y respuesta frente a cambios de la red.

Existen muchos tipos de algoritmos de encaminamiento. OSPF es uno de los algoritmos que tienden a utilizarse de manera generalizada.

Una forma de clasificar estos protocolos podría ser atendiendo a su uso dentro de una organización y a la capacidad que tienen para proporcionar conectividad externa. Es lo que se denomina un dominio, es decir, siempre que se encuentre dentro del mismo dominio de administración, o el conjunto de máquinas y encaminadores que administra una única autoridad. Esta clasificación sería:

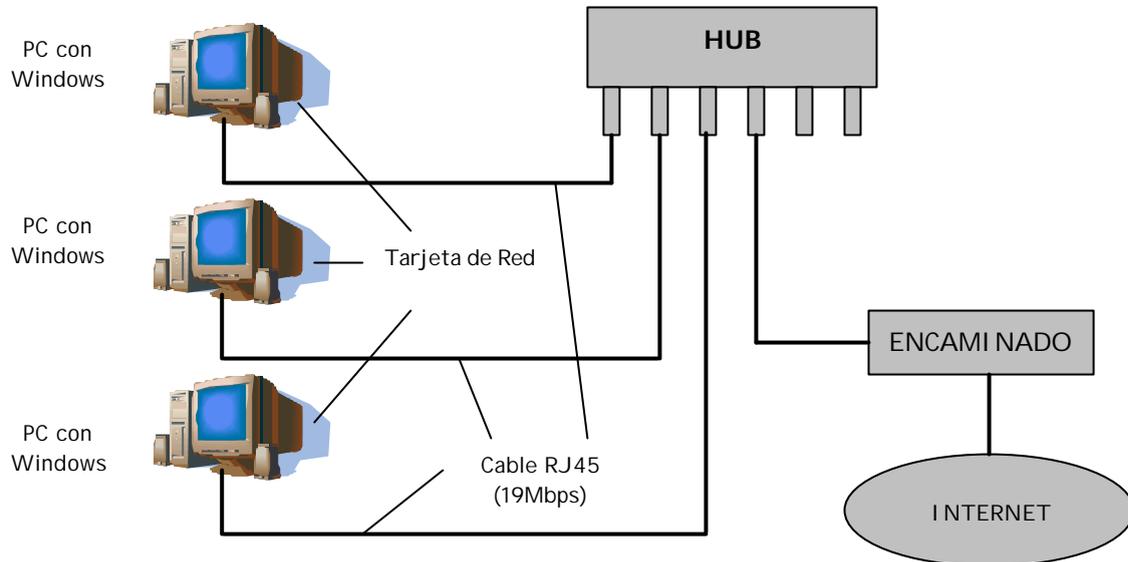
❖ Exteriores

- BGP
- EGP

❖ Interiores

- RIP
- IGRP y EIGRP
- OSPF

10.5.- Diseño e implementación de una Red de Área local



Se va a describir el proceso de diseño, configuración e implantación de una red de área local. Para ello se parte de una situación inicial con unas cuantas computadoras PC con sistema operativo Windows 2000 que se van a interconectar entre sí y que utilizarán un encaminador para conectarse con Internet. La implantación va a seguir una secuencia ordenada. Se consideran inicialmente los siguientes componentes:

- 3 computadoras PC con sistema operativo Windows 2000.
- Un encaminador.
- Tarjetas de red con conectores RJ45.
- Un concentrador con al menos 4 bocas RJ45 (se precisa de uno por cada PC y otro para el encaminador). Cable del tipo par trenzado con metros suficientes como para poder llevar a cabo todas las conexiones.
- Conectores RJ45 para utilizar en los extremos de los cables.
- Un grimpador. El grimpador es un elemento que se utiliza para unir los cables RJ45 a sus respectivos conectores

La construcción de cables mediante un grimpador es una labor tediosa y expuesta a fallos, por lo que muchas veces resulta aconsejable comprarlos hechos directamente con lo que se tienen garantías de que funcionan correctamente, eliminando de esta manera una posible fuente de fallos.

Para hacerse una idea con la mayor exactitud posible de cómo realizar la implantación, en la figura anterior se presenta la topología de interconexión de los elementos.

En la dicha figura se observa la disposición de los PC con una tarjeta de red en cada uno de ellos, que se unen mediante el cable RJ45 al hub. El encaminador que proporciona salida a Internet también estaría unido al hub.

En este caso, y dado que se trata de una red pequeña, se considera que el encaminador se encuentra unido a Internet mediante una línea RDSI que llega al proveedor

de Internet que le presta el servicio. En la sección dedicada a la instalación del encaminador se precisarán los datos necesarios para configurar correctamente este tipo de líneas.

A continuación se explica el detalle de cada uno de los pasos que hay que realizar para conectar los PC dentro de una red de área local con conexión a Internet:

1.- Instalación de los componentes y de los cables.

2.- Instalación del software en los PC. En este caso hemos utilizado el sistema operativo Windows 2000, aunque dadas las características de los sistemas operativos Windows, el ejemplo es aplicable, sin pérdida de generalidad, a cualquiera de los sistemas operativos Windows con mínimos cambios en la configuración del software que se describe aquí. Cuando las diferencias en la configuración han sido significativas con respecto a otros sistemas operativos Windows, se especifica el procedimiento alternativo.

3.- Configuración del encaminador.

4.- Pruebas de interconectividad.

Seguidamente se presentan cada uno de los pasos por separado:

10.5.1.- Instalación de los componentes y de los cables

Para la instalación de los componentes se puede seguir el gráfico de la figura anterior. En primer lugar hay que instalar las tarjetas en los PC y realizar los cables. Para estas dos operaciones conviene considerar los siguientes puntos:

- Para la instalación de tarjetas es suficiente abrir el PC insertar la tarjeta en una ranura vacía y reiniciar el PC. En condiciones normales el sistema operativo reconocerá la instalación de un nuevo hardware, y pedirá los datos para proceder a su instalación. El sistema de configuración de Windows 2000 hace que dicha instalación se realice evitando problemas de interrupciones con otros dispositivos. Si la tarjeta no es detectada en el momento de insertarla se puede utilizar el procedimiento de detectar hardware de manera automática y elegir el tipo de tarjeta y los controladores a utilizar.
- Para la realización de los cables hay que considerar la colocación de los pequeños cables (8 en total) que van de un conector hasta otro. Se trata de cables planos, por tanto, se debe establecer una configuración inicial y respetarla en todos los demás conectores. No son cables cruzados, como en un principio se podría pensar, son cables planos y, por tanto, la conexión de origen y destino debe estar directamente comunicada. En la figura siguiente se proporciona un ejemplo de cómo podrían disponerse los cables para la implementación de un cable plano con los conectores a ambos lados, de las características descritas con anterioridad.

Una vez que se hayan realizado todos estos pasos se deben unir los dispositivos, tal como se especifica en la figura de la página anterior de descripción de la topología de la red. Con respecto al concentrador, hay que destacar que es un dispositivo del tipo conectar y listo (plug & play).



Una vez los RJ-45 conectados a las bocas del hub, éste no precisa de ninguna configuración adicional. Si un hub produce problemas, se trata de un defecto de fábrica y, en este caso, se debería cambiar por otro.

A partir de este momento, los pasos consistirán en configurar los PC y el encaminador para la conexión a Internet

10.5.2. - Instalación del software en los PC

Para la instalación del software en los PC se supone que el Sistema Operativo ha sido instalado previamente y que la tarjeta de red ya ha sido identificada e instalada por el sistema, según el método pug & play comentado anteriormente. (Windows 2000 no es un entorno pensado para usuarios domésticos. Para estos casos es más conveniente utilizar Windows 98, o Windows XP, entornos más gratos al usuario).

A continuación se verifica para cada PC la configuración TCP/IP. Para ello se utiliza el menú *Propiedades de Mis sitios de red* en el escritorio. Una vez seleccionado esto, se seleccionan las propiedades de *Conexión de área local* y sobre la pantalla que se obtenga, las propiedades del *protocolo TCP/IP*.

Si se va a utilizar DHCP (común en la configuración de Windows2000), se configura el PC para obtener **la dirección IP de forma automática**. Posteriormente se explicarán los pasos a realizar en caso de no utilizar DHCP.

DHCP es un protocolo que asigna dinámicamente la dirección IP y la de DNS a los clientes de una red de computadores.

A continuación se verifica que la configuración es correcta. Para realizar esto, se utiliza el comando **winipcfg** para sistemas operativos *Windows 95/98* o comando **IPconfig** para sistemas operativos *Windows NT* o *Windows 2000*. De una forma u otra, a partir de aquí se obtiene la configuración del PC.

En redes con PC, la compartición de archivos se puede realizar utilizando el protocolo de compartición de archivos de Microsoft (**NetBEUI**), sin necesidad de recurrir a aplicaciones TCP/IP como NFS que añaden mayor carga a los clientes.

En el caso de NT o Windows 2000 se selecciona el comando **IPconfig** a partir del menú «Programas-Accesorios-símbolo del sistema» y se escribe IPconfig en la pantalla que se obtiene (pantalla de comandos de MS-DOS).

En este caso, el PC tratará de encontrar un servidor DHCP en la red. En este caso, tal vez no existiera ese servidor en la red (alguno de los PC presentes podría actuar como

servidor). En ese caso utilizaría la opción de autoconfiguración para asignarse automáticamente una dirección IP y una máscara de red.

Es posible que se quiera asignar una dirección IP fija con una máscara de red predeterminada sin dejar opción a que el sistema le asigne una de manera automática. En tal caso se sigue el mismo procedimiento al descrito inicialmente, pero al llegar a la ventana de propiedades de TCP/IP se selecciona la opción «**Usar la siguiente dirección IP**» y se especifica tanto la dirección IP como la máscara de red y, si procede, la puerta de enlace.

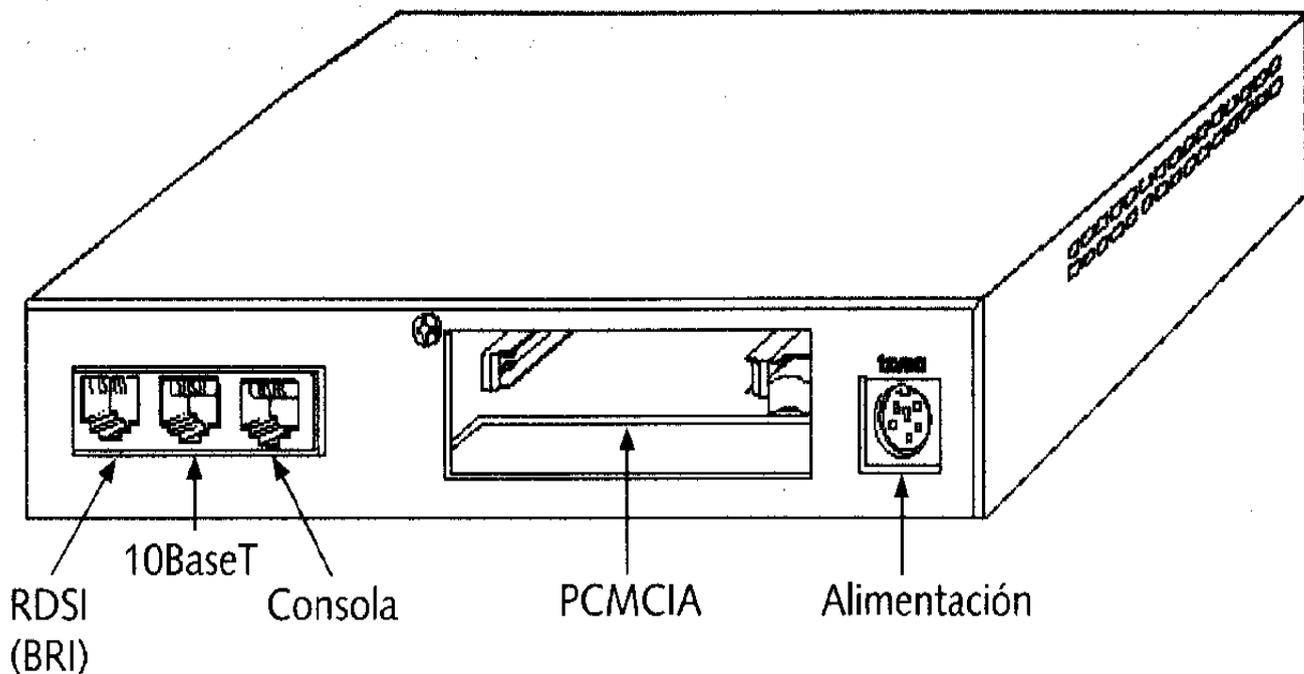
Se pueden utilizar submáscaras de red para seccionar redes C en dominios más pequeños.

A partir de aquí se verifica que la dirección y la máscara se encuentran reconocidas (en el caso de Windows 95/98/NT habría que reiniciar el PC, en el caso de Windows 2000 esto ya no es necesario). Para ello se recurre a IPconfig o a winipcfg según el sistema operativo.

Repetiendo estos pasos en cada uno de los PC todos estarán preparados para entrar en funcionamiento. De momento se deja la configuración tal cual, para verificar durante el paso 4 que todo funciona correctamente.

Ahora se configura el encaminador que da salida a Internet.

10.5.3. - Configuración del Encaminador



La configuración del encaminador es un aspecto muy dependiente de la marca del fabricante. En este ejemplo se utiliza un encaminador Cisco 1004 con conexión externa RDSI. Aunque las notas y los pasos que se exponen, están centrados en ese modelo, el proceso de instalación es muy similar para otros modelos o marcas y resulta más didáctico puntualizar en un modelo para que la comprensión sea más adecuada. El aspecto del encaminador es el que

muestra la figura adjunta, con la indicación sobre cada uno de los puertos que se van a utilizar.

En la figura anterior se puede ver un puerto para la conexión a RDSI, otro 10BaseT para la conexión RJ45 al concentrador y un puerto de consola que se utiliza para parametrizar directamente al propio encaminador. Adicionalmente existe una ranura PCMCIA que se utiliza para la memoria flash y una conexión para toma de corriente.

Los encaminadores permiten emular funcionalidades parecidas a la de los cortafuegos mediante las listas de acceso. Con estas listas se puede filtrar en función de las direcciones IP y de los puertos de acceso.

Toda la configuración se realiza según las indicaciones del fabricante de una manera bastante directa, aunque aquí se destacan los pasos más importantes para comprender las fases de implantación de una arquitectura de red.

En primer lugar, si la conexión se quiere realizar mediante una línea RDSI hay que entrar en contacto con la compañía local para que nos proporcionen el acceso a la línea. Una vez que contrate la línea será suficiente conectarla directamente al encaminador en la conexión indicada como RDSI (o ISDN).

Es necesario estar en posesión de la siguiente información generada por la empresa con la que se contrata la línea RDSI:

- *Tipo de conmutación RDSI.*
- *Identificador de servicio RDSI. (SPID).*
- *Números de teléfono RDSI locales. (LDN).*

A continuación se configura el encaminador. Para ello se coloca una consola de computadora (monitor y teclado) directamente conectada a la entrada de consola que se encuentra en el encaminador. Este paso se puede evitar si se dispone de una memoria flash configurada con toda la información e insertada en la entrada PCMCIA del encaminador.

La mayoría de los encaminadores proporcionan ayuda en línea, de gran utilidad, para su configuración a través de las webs de los fabricantes

Una vez conectada la consola se observa al poco tiempo un mensaje del encaminador para proceder a su configuración. Tras una presentación sobre la empresa y sobre las características del encaminador, se nos muestra el estado de las interfaces del encaminador. En este caso el encaminador tiene dos interfaces, una para RDSI y otra Ethernet de conexión con nuestra red de área local. El mensaje que nos aparece inicialmente es el que se muestra en la tabla adjunta:

Interface	IP-address	OK?	Method	Status	Protocol
Ethernet()	unassigned	NO	not set	up	up
BRIO	unassigned	NO	not set	up	up

En la tabla se presentan las dos interfaces sin dirección IP y sin configuración, ya que el campo OK? que indica su configuración tiene el valor NO. Será necesario configurar cada una de las dos interfaces siguiendo la línea de comandos del encaminador. El menú de línea de comandos es particular para cada encaminador, en nuestro caso, se asignan las

direcciones correspondientes a cada una de las interfaces. En el caso de la interfaz Ethernet, y a modo de resumen, se obtiene la siguiente configuración:

```
Configuring interface parameters
Configuring interface Ethernet():
  is this interface in use? [yes]:
  IP address for this interface 192.168.1.1
  Number of bits in subnet field [()]:
  Class B network in 192.168.0.0, 8 subnet bits, mask is
255.255.255.0
```

En dicha configuración se observa cómo se ha asignado a la interfaz Ethernet del encaminador la dirección IP 192.168.1.1 que estaba inicialmente planificada para asignar a esa interfaz del encaminador. La máscara de red está configurada como 255.255.255.0. Por tanto, se tiene la posibilidad de albergar a una red completa del tipo "C". Para el caso de la interfaz RDSI, se obtiene la siguiente configuración:

Configuring interface BRIO.

```
Is this interface in use? [yes]
Configuring IP on this interface? [yes]:
  IP address for this interface: 130.2205.22
  Number of bits in subnet field [()]:
  Class B network in 130 22.0.0, 8 subnet bits, mask is 255.255.255.0
```

En este caso se ha asignado la dirección IP a la interfaz BRIO, que, en este caso, llegaría a la línea telefónica RDSI. Se conserva la misma máscara de red en este caso, aunque ésta es una circunstancia que nos debería asegurar nuestro proveedor de red.

Una vez realizado esto, el encaminador nos mostrará los datos de configuración y se ratifica la corrección de los mismos o se rectifican aquellos introducidos de manera indebida.

A partir de aquí sólo queda configurar el enlace físico de la RDSI, ya que ésta presenta características diferentes en función del sitio donde se encuentra.

Para ello se utiliza el menú de configuración de la RDSI y se especifican los siguientes datos:

- Tipo de conmutación RDSI (isdn switch-type).
- Interfaz BRI.
- Método de encapsulación (por ejemplo, PPP).
- Dirección IP del encaminador destino.
- Número de teléfono al que hay que llamar.
- Grupo al que pertenece el número de teléfono.

Estos datos se tienen que obtener previamente de la entidad con la que se contrate el acceso RDSI. A partir de aquí existe la posibilidad de configurar algunos parámetros opcionales como las listas de acceso, para finalmente introducir el tipo de ruta que se utilice para llegar al encaminador remoto. En la mayoría de los casos se trata de una ruta estática.

Con todo esto el encaminador queda configurado. Se puede desconectar la consola y poner el encaminador en funcionamiento.

A continuación nos resta verificar si el funcionamiento de toda la instalación es correcta. De eso se ocupa el siguiente paso.

10.5.4. - Pruebas de interconectividad

Una vez que se ha completado la instalación llega el momento de comprobar si todo funciona correctamente, y en caso de que no funcione como es debido hay que aislar el problema, estudiarlo detenidamente y tratar de darle una solución.

Es relativamente normal, que las primeras veces que se realiza una instalación se produzcan problemas o existan detalles olvidados y que son suficientes para que el conjunto deje de funcionar.

Ante todo resulta imprescindible la paciencia para ir solucionando los problemas mediante el aislamiento de los mismos. Hay que considerar que se trata de entornos complejos, con muchas piezas, y programas software funcionando de modo conjunto. Resulta imprescindible localizar el componente o programa causante del fallo para que se pueda estudiar con detenimiento.

La mejor prueba para verificar que todo funciona es sencillamente tratar de conectar con algún lugar de Internet. Si se escribe en un navegador (es posible que utilice agente proxy para la conexión a Internet. En ese caso debe obtener previamente la dirección IP del agente proxy e introducirla en el menú de opciones del navegador que vaya a utilizar. Para averiguar la dirección de su proxy tendrá que ponerse en contacto con su proveedor de Internet), que habitualmente se encuentra incluido en el paquete software estándar de instalación de los sistemas operativos, un lugar de Internet tal como Yahoo! (<http://www.yahoo.com>) y nos aparece directamente el lugar, todo va bien y se puede pensar que la instalación ha finalizado correctamente.

Restaría en ese caso configurar alguna aplicación de Internet que se quiera utilizar, como podría ser la aplicación de correo electrónico a partir del lector del propio navegador o de programas particulares como Eudora o Outlook. Para ello bastará seguir las instrucciones que proporcionan este tipo de programas.

Es posible que se intente la comunicación con el lugar y no se obtenga ninguna respuesta durante un período prolongado (30 segundos), para obtener finalmente algún tipo de mensaje relativo a que no es posible realizar la comunicación con el lugar deseado. Llega el momento de aislar el problema y tratar de corregirlo. Aunque hay miles de problemas posibles y sería interminable abarcarlos todos, se van a proporcionar algunas pistas para poder aislar convenientemente los problemas más frecuentes que se puedan tener.

En primer lugar, si no es posible la comunicación con el lugar de Internet hay que verificar si el problema viene de un PC o de todos los PC que están en la red de área local. Para ello es conveniente probar la misma dirección con otro PC conectado. En función de esto se procederá de una u otra manera.

También hay que verificar si el problema es relativo a la configuración del encaminador o a los cables que se han realizado en la primera fase.

En el cuadro de la siguiente página, se proporcionan algunas pistas sobre la forma de actuar en cada una de las posibles situaciones y sobre las acciones a emprender.

