

Comprueba tu aprendizaje

I. Distinguir las funciones de los dispositivos de interconexión de red

1. Confirma la veracidad o falsedad de las siguientes afirmaciones:
 - a) Externamente, un *hub* y un *switch* se distinguen con dificultad.
 - b) Un puente remoto consta de dos dispositivos separados por una línea de conexión.
 - c) Los comutadores operan en el nivel 3 y los puentes en el nivel 2.
 - d) Los repetidores se pueden instalar en cascada indefinidamente.
 - e) Los comutadores saben gestionar el ancho de banda de cada puerto.
 - f) Los repetidores y concentradores copian las tramas entre sus puertos.
2. Relaciona la columna de la izquierda (dispositivos) con su tecnología específica (columna de la derecha). Ten en cuenta que la relación es de uno a varios.

Dispositivos	Tecnología o función específica
1. Repetidor	a. Comutar paquetes
2. Transceiver	b. Regenerar la señal eléctrica
3. Concentrador	c. Doble puerto
4. Puente	d. Múltiple puerto
5. Switch	e. Selecciona tramas

3. ¿Es posible crear VLAN utilizando comutadores? ¿Y si utilizamos concentradores? ¿Y si usamos puentes remotos?

II. Elegir los dispositivos de red de área local en función de las necesidades

4. Busca los errores técnicos en el siguiente comentario:
 «Una empresa acaba de fusionarse con otra y sus directivos proyectan integrar sus dos redes antiguas en una nueva. Cada red está en la sede de su ciudad original. Se ha propuesto la adquisición de un puente remoto para unir las dos sedes, pero una vez comprobado su escaso rendimiento se ha determinado conectarlas mediante un comutador que es mucho más rápido.»
5. Confirma la veracidad o falsedad de las declaraciones siguientes sobre ADSL:
 - a) La tecnología xDSL siempre es simétrica.
 - b) En ADSL el ancho de banda de bajada suele ser superior al de subida porque es una tecnología asimétrica.

c) Un módem ADSL siempre requiere otro dispositivo intermedio para conectarse a la red local.

d) Al igual que el módem, el router ADSL también requiere un dispositivo intermedio para unirse a la red.

6. Busca en las sedes web de los fabricantes de dispositivos de red información técnica y comercial sobre comutadores.

Compara los distintos modelos de varios fabricantes para familiarizarte con las características básicas de este tipo de dispositivos.

Si consigues listas de precios, podrías realizar comparativas de precios.

Ayuda: Las comparativas de precios no se hacen por comutador, sino por puertos, es decir, se divide el precio total del comutador por el número de puertos que posee.

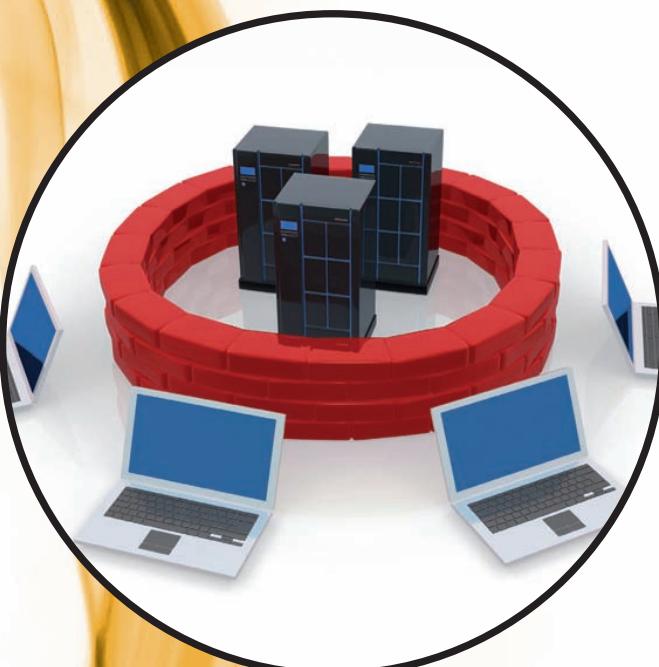
III. Configurar redes locales virtuales

7. ¿Qué tipos de redes de área local virtuales conoces? ¿Cómo se llama el estándar IEEE utilizado en la creación de VLAN?
8. Razona en qué condiciones podrían ser verdad las siguientes afirmaciones:
 - a) Dos puertos que se asocian en la misma VLAN en un comutador pueden comunicarse libremente.
 - b) Dos puertos que pertenecen a dos VLAN distintas solo pueden comunicar los protocolos de gestión.
 - c) Las direcciones MAC de los dos nodos se han asociado a la misma VLAN, pero como están conectados en dos comutadores distintos, nunca podrían comunicarse entre sí.
 - d) Dos nodos que pertenecen a la misma VLAN pero que están conectados a distintos comutadores pueden comunicarse entre sí.
9. Toma tres comutadores que contemplen el protocolo STP o RSTP y prepara en el laboratorio un modelo para la red comutada que aparece en la Fig. 5.24.
 - a) Habilita el protocolo STP en los tres comutadores y comprueba que las tres estaciones pueden comunicarse entre sí.
 - b) Rompe ahora el enlace del camino 1 y comprueba que después de un tiempo sigues teniendo conexión entre las estaciones.
 - c) Repite el proceso anterior deshabilitando los caminos 2 y 3.

6

Unidad

Interconexión de equipos y redes



En esta unidad aprenderemos a:

- Configurar los clientes de una red local para utilizar un sistema de enrutamiento.
- Gestionar un proxy web.
- Diseñar y configurar un sistema de protección para la red local.

Y estudiaremos:

- Los protocolos de acceso desde y hacia la red WAN externa.
- Los parámetros de configuración en enrutadores y servidores proxy.
- La tecnología de una red perimetral.
- Las órdenes que permiten crear y modificar las tablas de rutas de nodos y encaminadores.



CEO

SMR_RL_AAbad_06_TramaPPP.docx

Documento que contiene información sobre el formato de la trama PPP.



A Vocabulario

Encapsulación de protocolo: encapsular un protocolo A dentro de otro B es ponerle cabeceras de protocolo B a cada paquete de datos del protocolo A. Como ejemplo, podríamos decir que el transporte ferroviario de coches consiste en encapsular según las normas ferroviarias el transporte habitual por carretera.

Frecuentemente se utiliza el término «tunelización» como sinónimo de encapsulación de un protocolo.



Investigación

PPPoE (*PPP over Ethernet*) es un protocolo derivado de PPP que se utiliza mucho para utilizar la tecnología PPP cuando la red de transporte es Ethernet. Busca información en Internet sobre el protocolo para descubrir dónde radican sus ventajas.

Puedes empezar tu búsqueda por http://www.adslzone.net/adsl_pppoe.html y por la voz PPPoE en Wikipedia.

De modo análogo también hay un protocolo PPPoA (*PPP over ATM*), que es semejante a PPPoE pero sustituye Ethernet por una red ATM.

Otras direcciones de interés son: <http://es.wikipedia.org/wiki/PPPoA>, <http://es.wikipedia.org/wiki/PPPoE> y <http://www.adslfaqs.com.ar/que-es-el-pppoe-y-ppoa-explicacion-sencilla/>

1. El acceso a las redes WAN

Los ordenadores no son entidades aisladas, y las redes tampoco. De igual modo que los ordenadores se relacionan entre sí utilizando redes de área local, estas pueden interconectarse mediante otras redes de ámbito mayor: las redes de área extensa.

A menudo se segmenta la red de área local corporativa creando varias subredes e interconectándolas entre sí utilizando dispositivos específicos de los que nos ocuparemos en esta unidad.

Las redes WAN no suelen conectar directamente nodos, sino que interconectan redes. Lo específico de ellas es que las líneas que suelen utilizar son públicas y los protocolos de comunicación que requieren tener en cuenta la seguridad de un modo especial.

1.1. Protocolos de acceso remoto

La importancia que tenía el adaptador de red y los protocolos de nivel uno y dos para las redes de área local la tienen ahora los protocolos de acceso remoto para las redes WAN.

A. Protocolo PPP

Bajo la denominación PPP (*Point to Point Protocol*, protocolo punto a punto) se designa a un conjunto de protocolos que permiten el acceso remoto para el intercambio de tramas y autenticaciones en un entorno de red de múltiples fabricantes. Un cliente PPP puede efectuar llamadas y, por tanto, establecer conexiones a cualquier servidor que cumpla las especificaciones PPP. La arquitectura PPP permite que los clientes puedan ejecutar cualquier combinación de los protocolos NetBeui, IPX y TCP/IP, incluyendo las interfaces NetBIOS y sockets de red.

Aunque tradicionalmente PPP ha sido utilizado en conexiones sobre líneas serie, por ejemplo: para marcar por módem y realizar una conexión a Internet, existe una versión en la que se encapsula PPP sobre una capa Ethernet denominada PPPoE (*PPP over Ethernet*), ampliamente utilizada para proveer conexiones de banda ancha añadiendo a Ethernet las ventajas que PPP ofrece como autenticación, cifrado y compresión de datos.

B. Protocolo SLIP

SLIP (*Serial Line Internet Protocol*, protocolo Internet para línea serie) es un protocolo estándar utilizado desde hace tiempo en sistemas UNIX que permite la conexión remota a través de líneas serie utilizando el protocolo IP. Los servidores de acceso remoto siguen contemplando el protocolo SLIP por compatibilidad, aunque está siendo desplazado por PPP.

C. El protocolo de tunelización PPTP

PPTP (*Point to Point Transport Protocol*, protocolo de transporte punto a punto) es un protocolo que encapsula los paquetes procedentes de las redes de área local de modo que se hacen transparentes a los procedimientos de red utilizados en las redes de transporte de datos.

El protocolo PPTP está definido en el RFC 2637. Sus comunicaciones son cifradas y es bastante popular en redes privadas virtuales, que estudiaremos más adelante, ya que Microsoft incorporó un servidor y un cliente PPTP a partir de Windows NT, algo también común en el mundo Linux.

Por ejemplo, dos redes IPX pueden crear un túnel PPTP a través de Internet, de modo que se crea una red virtual utilizando Internet (red IP) como medio de transporte, pero intercambiándose paquetes IPX transparentemente.

1.2. Servicios de acceso remoto

El servicio de acceso remoto (*RAS, Remote Access Service*) conecta equipos remotos, posiblemente móviles, con redes corporativas, es decir, permite las conexiones de equipos distantes de la red de área local, habilitando los mismos servicios para estos usuarios remotos que los que poseen los usuarios presentados localmente. Por tanto, RAS es un encaminador software multiprotocolo con capacidad de autenticación y encriptación de los datos transmitidos.

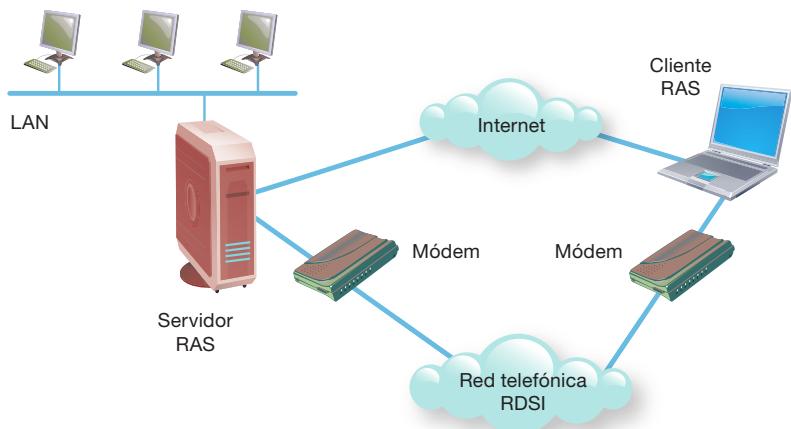


Fig. 6.1. Esquema del acceso de una estación cliente a un servidor RAS y a su red de área local.

A. Escenario de conexión RAS

El servicio de acceso remoto tiene una parte de cliente (quien se conecta) y otra de servidor (lugar al que se conecta el cliente). Son posibles conexiones punto a punto a través de módems analógicos, redes X.25, RDSI, ADSL e incluso RS-232-C. Además, es posible la conexión entre el cliente y el servidor a través de Internet de modo transparente a la red, utilizando el protocolo de túnel PPTP.

RAS es capaz de encaminar tres protocolos de LAN: IPX, TCP/IP y NetBeui, ya que frecuentemente utiliza PPP como transporte y este puede encapsular los tres protocolos de LAN. Por tanto, cualquier cliente que utilice al menos alguno de estos tres protocolos puede realizar una conexión vía RAS hacia una red que ejecute estos mismos protocolos. Es posible configurar el servicio RAS para que el cliente tenga acceso a toda la red o exclusivamente al servidor RAS.

Cuando el cliente se conecta a través de NetBeui, apenas hay nada que configurar, puesto que NetBeui es un protocolo para redes planas cuyo único elemento de configuración es el nombre NetBIOS.

Si un cliente RAS se conecta vía TCP/IP, necesitará una dirección IP compatible con la red a la que intenta conectarse. Lo normal es que el servidor RAS le asigne dinámicamente una dirección que utilizará mientras dure la conexión. Esta es la razón por la que frecuentemente los servidores de acceso remoto incluyen un servidor DHCP o se integran con el DHCP corporativo.

Para el cliente RAS, todo el procedimiento de red es transparente. A través de las interfaces de red apropiadas como NetBIOS o sockets, sus aplicaciones de red funcionarán perfectamente desde su posición remota como si estuvieran en la misma red de área local.

Ampliación

En las versiones recientes de los servidores Windows, Microsoft ha mejorado aún más el servicio de acceso remoto y lo ha denominado RRAS (*Routing and Remote Access Service, Servicio de enrutamiento y acceso remoto*). Puede conseguirse más información sobre RRAS en <http://technet.microsoft.com/es-es/network/bb545655>

Actividades

1. Confirma la veracidad de las siguientes afirmaciones:
 - El protocolo PPP puede gestionar intercambio de paquetes de cualquier protocolo de red.
 - PPTP es un protocolo que crea túneles sobre los que se encapsula TCP/IP, NetBeui o SPX/IPX.
 - Un protocolo de gestión de la autenticación es el que se encarga de pedir el nombre de usuario y su contraseña.
 - Basta con incorporar a la comunicación cualquier protocolo de autenticación para que la comunicación sea totalmente segura.
2. Descubre el error en el siguiente razonamiento: «El administrador de red de una instalación ha preparado un sistema Linux en el portátil de un comercial que estará de viaje. Desde ese portátil el comercial hará conexiones remotas hacia un servidor RAS Windows localizado en la sede central de las oficinas. El servidor solo tiene configurado el protocolo NetBeui de Microsoft. Cuando el portátil, que tiene Linux, se conecta al servidor RAS emplea el protocolo PPP para transportar paquetes TCP/IP al servidor RAS. Como RAS es compatible con TCP/IP y NetBeui, no importa que cliente y servidor "hablen" protocolos distintos: el sistema hace transparente la comunicación al usuario.»



CEO

S M R _ R L _ A A b a d _ 0 6 _
TecnologíasRedesWAN.docx
Documento que contiene información sobre:

1. Ejemplo de secuencia de conexión con RAS.
2. Gestión multienlace.
3. Canales para redes WAN.



Claves y consejos

La configuración de los enca- minadores puede llegar a ser una de las tareas más difí- ciles del administrador de red, especialmente en redes complejas y en donde los caminos no son únicos. Las compa- ñías fabricantes de routers suelen ofrecer a sus clientes forma- ción específica en cada uno de sus productos. En cualquier caso, constituye un buen hábito laboral tener el manual del fabricante cerca cuando se configuran estos dispositivos.

2. El encaminador

Los encaminadores, enruteadores o routers son dispositivos software o hardware que se pueden configurar para encaminar paquetes entre sus distintos puertos de red utilizando la dirección lógica correspondiente a la Internet (subred), por ejemplo, su dirección IP.

Puesto que la función de encaminamiento se realiza de acuerdo con reglas formadas con las direcciones de red (nivel 3), solo serán enruteables aquellos protocolos que parti- cipen de este nivel. Por ejemplo, puesto que la familia de protocolos que utiliza NetBIOS de modo nativo no tiene la capa 3 (no hay direcciones de red NetBIOS), se puede deducir que NetBIOS no es encaminable: solo funcionará en redes locales y no podrá saltar a otras redes.

2.1. Características generales

El encaminador interconecta redes de área local operando en el nivel 3 de OSI (Fig. 6.2). El rendimiento de los enruteadores es menor que el de los comutadores ya que deben gastar tiempo del proceso en analizar los paquetes del nivel de red que le llegan. Sin embargo, permiten una organización muy flexible de la interconexión de las redes.

Cada enruteador encamina uno o más protocolos. La condición que debe imponerse al protocolo es que sea enruteable, porque no todo protocolo se puede encaminar. Los rou- ters comerciales suelen tener capacidad para encaminar los protocolos más utilizados, todos ellos de nivel 3: IP, IPX, AppleTalk, DECnet, XNS, etc.

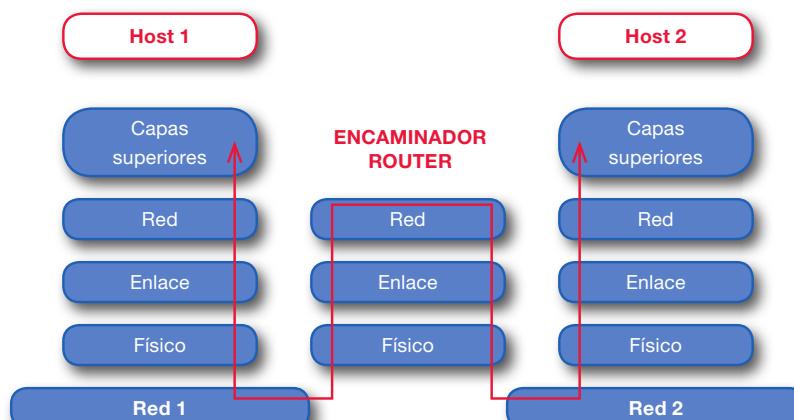


Fig. 6.2. Esquema de operación en la arquitectura de red de un encaminador.

Las características fundamentales de los encaminadores se pueden resumir en que:

- Interpretan las direcciones lógicas de capa 3, en vez de las direcciones MAC de capa de enlace, como hacen los puentes o los comutadores.
- Son capaces de cambiar el formato de la trama, ya que operan en un nivel superior a la misma.
- Poseen un elevado nivel de inteligencia y pueden manejar distintos protocolos previa- mente establecidos.
- Proporcionan seguridad a la red puesto que se pueden configurar para restringir los accesos a esta mediante filtrado.
- Reducen la congestión de la red aislando el tráfico y los dominios de colisión en las distintas subredes que interconectan. Por ejemplo, un router TCP/IP puede filtrar los paquetes que le llegan utilizando las máscaras IP.

O A. Tipos de encaminadores

Pueden establecerse diversas clasificaciones de los encaminadores en función del aspecto que se ponga en estudio, pero los más comunes atienden al lugar en donde se ubican y al protocolo de enrutamiento que utilizan.

A.1. Según su ubicación en la red

Es frecuente que los routers se clasifiquen de acuerdo con el ámbito de la red a la que proporcionan servicio. Según esto, un encaminador puede ser:

- **Router de interior** (*Interior router*). Se trata de un encaminador para ser instalado en una LAN para dar servicio de encaminamiento dentro de la propia red de área local proporcionando a los paquetes de red la posibilidad de saltar de unos segmentos de la red a otros.
- **Router de exterior** (*Exterior router*): en este caso el encaminador comunica nodos y redes en el exterior de la LAN. Estos routers operan típicamente en el núcleo de Internet y son utilizados por los operadores de Internet para comunicarse entre ellos.
- **Router de borde o frontera** (*Gateway router o Border router*). Es un encaminador que se encarga de conectar routers interiores con routers exteriores. Por ejemplo, pueden interconectar una LAN a Internet a través del proveedor de servicios de Internet (ISP, *Internet Service Provider*).

A.2. Según el tipo de algoritmo de encaminamiento

Los routers confeccionan una tabla de encaminamiento en donde registran qué nodos y redes son alcanzables por cada uno de sus puertos. Es decir, la tabla describe la topología de la red. De aquí nace una segunda clasificación de los algoritmos utilizados por los encaminadores para realizar su función:

- Algoritmos de **encaminamiento estático** (*static routing*). Requieren que la tabla de encaminamiento sea programada por el administrador de red. Carecen de capacidad para aprender la topología de la red por sí mismos, cualquier adaptación a cambios topológicos de la red requiere una intervención manual del administrador del router.
- Algoritmos de **encaminamiento adaptativo** (*dynamic routing*). Son capaces de aprender por sí mismos la topología de la red. Por tanto, son mucho más flexibles que los encaminadores estáticos, aunque su rendimiento es menor puesto que tienen que consumir recursos en el intercambio de información con otros enrutadores para, dinámicamente, confeccionar las tablas de encaminamiento que contienen la información con la que tomará las decisiones de enrutamiento de paquetes.

O B. Protocolos de encaminamiento

Un protocolo de encaminamiento es aquel que utiliza un router para calcular el **mejor camino** (*best path*, en la terminología profesional) que le separa de un destino determinado. El mejor camino calculado representa la ruta más eficiente que debe seguir un paquete desde que sale de un nodo origen hasta que llega a su destino pasando por el router.

El mejor camino dependerá de la actividad de la red, de si hay enlaces fuera de servicio, de la velocidad de transmisión de los enlaces, de la topología de la red y de muchos otros factores. Así, un enlace de alta velocidad representará un camino mejor que otro semejante pero de menor velocidad.

El **coste de una ruta** (*route cost*) es un valor numérico que representa cuán bueno es el camino que la representa: a menor coste, mejor camino.

Un protocolo de enrutamiento se caracteriza también por su **tiempo de convergencia**, que es el tiempo que tarda un router en encontrar el mejor camino cuando se produce una alteración topológica en la red que exige que se recalculen las rutas para adaptarse a la nueva situación. Hay que diseñar los protocolos de enrutamiento para que tengan el menor tiempo de convergencia posible.

De modo genérico, a los protocolos de enrutamiento utilizados con routers de interior se les denomina **IGP** (*Interior Gateway Protocol*) mientras que a los utilizados con routers de exterior se les denomina **EGP** (*Exterior Gateway Protocol*).



Fig. 6.3. Algunos modelos de encaminadores. Cisco es una de las compañías líderes en ventas de enrutadores.



Claves y consejos

No hay que confundir protocolo enrutable con protocolo de enrutamiento. Un protocolo enrutable es aquel que proporciona paquetes al router para que este los encamine hacia su destino. Un protocolo de enrutamiento es el protocolo que utiliza el router para comunicarse con otros routers y aprender la topología de la red.

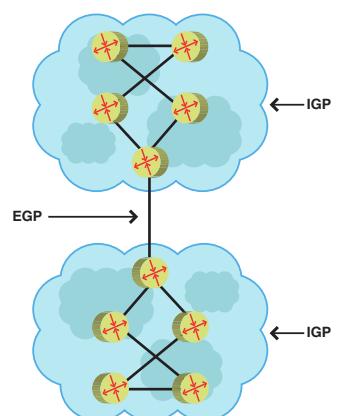


Fig. 6.4. Lugares de la red en donde deben utilizarse protocolos IGP o EGP.

B.1. Protocolos de enrutamiento basados en el vector-distancia

Un protocolo de encaminamiento basado en un vector-distancia es aquel que determina cuál es el mejor camino calculando la **distancia al destino**. La distancia es un número calculado que no necesariamente significa longitud, sino que puede contemplar otros parámetros como el número de saltos que dará para llegar al destino (número de routers por los que pasará el paquete en su viaje hacia su destino), la latencia (tiempo medio en llegar al destino) u otros valores que impliquen costes económicos en la transferencia del paquete que debe enrutararse.

Con vector-distancia, el router debe intercambiar periódicamente su información de enrutamiento con otros routers vecinos para recalcular las nuevas distancias entre ellos.

Los protocolos de enrutamiento basados en vector-distancia más utilizados actualmente son RIP, RIPv2 y BGP.

- **RIP o RIPv1** (*Routing Information Protocol*) es un algoritmo de tipo vector basado en la RFC 1058 apropiado para encaminamiento en redes IP pequeñas. Solo se utiliza en routers interiores y de borde. RIP utiliza cada 30 segundos el puerto UDP número 520 para intercambiar la información de encaminamiento con otros enrutadores, que se calcula como el cómputo de saltos de red necesarios para que un paquete dado alcance su destino. RIP no considera la congestión de la red ni la velocidad del enlace. Si la red es grande, RIP genera excesivo tráfico de red por lo que es muy poco escalable. Además, su convergencia es muy pobre. A cambio, es un protocolo muy estable y está implementado en la mayor parte de los enrutadores. Para que no forme bucles, RIP limita el número de saltos con otros enrutadores para intercambiar información a 15, por lo que si el destino se encuentra más lejos de 15 saltos, RIP considerará el destino como inalcanzable.
- **RIPv2** (*Routing Information Protocol* versión 2) es una actualización de RIPv1 que genera menos tráfico de broadcast, admite subnetting y mejora la seguridad pues en el intercambio de información de enrutamiento se emplean contraseñas. Sin embargo, sigue sin poder exceder los 15 saltos, por lo que sigue siendo poco escalable.
- **BGP** (*Border Gateway Protocol*) es un protocolo de frontera exterior, es decir, se ejecuta en los encaminadores que forman el perímetro de la red y facilitan extraordinariamente el intercambio de rutas con los encaminadores exteriores, típicamente propiedad de los proveedores de Internet. BGP utiliza el puerto TCP número 179 para intercambiar mensajes específicos. El administrador de la red puede configurar BGP para que siga unas políticas que determinen caminos preferentes.

B.2. Protocolos de enrutamiento basados en el estado del enlace

Un protocolo de encaminamiento basado en el estado del enlace (*link-state*) es aquel que le permite a un router crearse un mapa de la red para que él mismo pueda determinar el mejor camino a un destino por sí mismo examinando el mapa que se ha construido. En función de la información de los enlaces que mantiene con sus routers vecinos y la información que estos le proporcionen sobre los segmentos de la red que ellos ven, construirán árboles de caminos que representen el mapa de la red.

Los protocolos de enrutamiento basados en el estado del enlace más utilizados actualmente son OSPF e IS-IS.

- **OSPF** (*Open Shortest Path First*) es un algoritmo caracterizado por que el envío del paquete siempre se realiza por la ruta más corta de todas las disponibles, que siempre es la que requiere un número menor de saltos. Es muy común en las LAN y se utiliza en routers interiores y de borde. Inicialmente se introdujo como una mejora de RIP, por lo que puede convivir con él. Supera la limitación de los 15 saltos como máximo de RIP.
- **IS-IS** (*Intermediate System to Intermediate System*) es un algoritmo propuesto por la ISO para comunicar sistemas intermedios (*intermediate systems*), que es el nombre que emplea la ISO para denominar a los enrutadores. Solo se utiliza en router interiores. Se usa menos que OSPF.



Ampliación

Los protocolos de enrutamiento híbridos son protocolos de encaminamiento que utilizan técnicas tanto de vector-distancia como de estado de enlace para calcular sus tablas de rutas. El protocolo de enrutamiento híbrido más utilizado es EIGRP (*Enhanced Interior Gateway Routing Protocol*).

Algunas características de EIGRP son las siguientes:

- Se utiliza en routers interiores y de borde.
- Es un protocolo propietario de Cisco, por lo que solo es compatible con enrutadores de este fabricante. En redes en las que todos los enrutadores son de Cisco es mejor utilizar EIGRP, pero en aquellos en las que haya enrutadores de otros fabricantes hay que utilizar OSPF.
- Su tiempo de convergencia es mínimo.
- Genera muy poco tráfico específico de enrutamiento, por lo que consigue un mejor rendimiento en la transmisión de paquetes de datos de usuario.

Parámetro	RIPv1	RIPv2	IGRP	OSPF	EIGRP
Tipo	Vector-distancia	Vector-distancia	Vector-distancia	Estado enlace	Híbrido
Coste	120	120	100	110	90 (ruta interna) o 170 (ruta externa)
Tipo de red enrutada	De clase	Subnetting	De clase	Subnetting	Subnetting
Métrica	Número de saltos	Número de saltos	Ancho de banda y latencia	Coste y ancho de banda	Ancho de banda y latencia
Mensajes a otros enrutadores	Broadcast (255.255.255.255)	Multicast (224.0.0.0)	Broadcast (255.255.255.255)	Multicast (224.0.0.5 y 224.0.0.6)	Multicast (224.0.0.10)
Tiempo convergencia	Lento	Lento	Lento	Rápido	Rápido
Escalabilidad	Pobre	Baja	Alta	Alta	Alta

Tabla 6.1. Comparativa de las características básicas de distintos protocolos de enrutamiento.

2.2. Configuración del enrutamiento

Cada nodo de una red IP debe tener configurados sus parámetros de red. Desde el punto de vista del enrutamiento, el parámetro más significativo es la puerta por defecto.

A. Rutas de protocolo IP

Cuando el emisor y el receptor de un paquete IP están en la misma red lógica no hay problemas de comunicación porque el emisor sabe que el receptor está en su misma red mediante ARP y, por tanto, todo lo que él escriba en la red será leído por el receptor. Sin embargo, cuando emisor y receptor están en distintas subredes, es muy posible que el emisor no sepa qué tiene que hacer para que el paquete llegue a su destino.

Una **ruta** es la dirección IP de un nodo (router) que tiene suficiente inteligencia electrónica (algoritmos de encaminamiento) para saber qué hacer con un paquete IP que ha recibido de un nodo de la red con objeto de que llegue a su destino, o al menos saber a quién puede enviárselo para que lo resuelva en su nombre, es decir, que una ruta es un apuntador IP a un encaminador. El router decide qué línea de transmisión utilizar para alcanzar su objetivo.

Cuando se utilizan los servicios de una ruta por defecto y la dirección del paquete no puede ser resuelta, se devolverá un mensaje al nodo emisor indicándole que el nodo o la red a la que se destina el paquete IP es inalcanzable.

Las rutas de cualquier nodo, y especialmente las de un encaminador, están recogidas en una o varias tablas de encaminamiento que son utilizadas por el servicio de enrutamiento de red para determinar los caminos que deben seguir los paquetes IP para alcanzar su destino. Las rutas pueden tener atributos; por ejemplo, pueden ser dinámicas, si se crean automáticamente en cuanto varía la estructura de la red mediante apertura de conexiones, y estáticas o persistentes, si se crean en tiempo de arranque del sistema del enrutador.



Vocabulario

Ruta de encaminamiento o simplemente **ruta**: es la dirección IP de un nodo (router) que tiene suficiente inteligencia electrónica (algoritmos de encaminamiento) para saber qué hacer con un paquete IP con objeto de que llegue a su destino, o al menos a quién puede enviárselo para que lo resuelva por él.

Ruta por defecto o **default gateway**: es la ruta a la que se envía un paquete cuando ninguna otra ruta es apropiada para ello, con la confianza de que el router al que apunta sepa cómo distribuir el paquete. En el mundo TCP/IP, especialmente sobre Linux, nos encontraremos que a la ruta por defecto se la denomina *gateway*, aunque el término *gateway* (pasarela) formalmente significa, según la terminología OSI, una máquina de nivel superior al nivel 4.



Ampliación

Modo de nombrar la red IP a la que pertenece un nodo

El modo en que se nombran las redes IP es semejante al que se utiliza para los nodos. Si tenemos una red 10.130.5.10 con máscara 255.255.0.0, la red a la que pertenece ese nodo se nombrará como red 10.130.0.0, aunque algunos sistemas utilizan la nomenclatura 10.130 en la que los ceros se suprimen. La ruta por defecto se representa por la secuencia 0.0.0.0.

Como se ve, la red a la que pertenece un nodo se nombra por la parte de la dirección IP del nodo que se corresponde con la secuencia de «1» en su máscara de red.

Otros ejemplos serían los siguientes:

- 10 es la red del nodo 10.3.23.67/8.
- 192.168 es la red del nodo 192.168.2.55/16.
- 192.168.2 es la red del nodo 192.168.2.55/24.

Cuando las máscaras son distintas de las redes de clase (8, 16 o 24 bits), nombrar la red es algo más complejo, como ya se estudió durante el desarrollo de la tecnología de subnetting.

**Truco**

En Windows la orden utilizada para gestionar la tabla de rutas es **ROUTE**. En Linux suele utilizarse la orden **iptables** e **ip route**. Se puede conseguir información sobre estas órdenes en el calificador de ayuda de la orden. La ejecución de estas órdenes con los calificadores que implican una modificación de la configuración de rutas implica la posesión de permisos de administrador del sistema.

B. Configuración de la tabla de rutas

En la Fig. 6.5 hay un ejemplo de una tabla de rutas sobre un cliente Windows con un acceso a la red de área local, que vamos a analizar detenidamente para hacernos una idea de la información que contiene y cómo se utiliza.

No todas las tablas de rutas son iguales, dependen del sistema operativo en el que operan; sin embargo, la mayoría de las tablas de rutas tienen los siguientes atributos:

- **Destino de red.** Es el nombre de la red que se pretende alcanzar.
- **Máscara de red.** Define la máscara de red de destino. La máscara de red junto con el destino de red definen el conjunto de nodos de red a los que se dirige la ruta.
- **Puerta de acceso o puerta de enlace.** Es la dirección IP del router (*gateway* o puerta de acceso en la terminología de la arquitectura IP), que debe ser capaz de resolver los paquetes que se dirijan a ese destino de red. Cuando la puerta de enlace coincide con la propia red local es señal de que el destino se alcanza inmediatamente por alguna de las interfaces de red local.
- **Interfaz.** Es la dirección IP o, en ciertos casos, el nombre de la interfaz de red que la posee por el que se deben enviar los paquetes de datos para alcanzar la puerta de enlace.
- **Métrica.** Es un parámetro que define una medida del coste telemático que supone enviar el paquete a la red destinataria a través de la puerta de acceso.

En Windows la orden apropiada para gestionar la tabla de rutas es **ROUTE ADD** para añadir rutas y **ROUTE DELETE** para borrarlas. Se puede acompañar de un calificador (**-P**) que hace que la ruta añadida sea permanente, es decir, que cuando se inicie de nuevo el sistema operativo la ruta seguirá estando definida a no ser que antes le hayamos aplicado una orden **ROUTE DELETE** que la elimine.

Además habrá que especificar la dirección de la red de destino junto con su máscara y la puerta de enlace, es decir, la dirección del enrutador que aceptará peticiones hacia esa red. Por ejemplo, si el nodo local tiene una dirección 192.168.1.1/24 y ejecutamos la siguiente orden:

```
ROUTE ADD -P 192.168.201.0 MASK 255.255.255.0 192.168.1.254
```

Entonces el sistema entenderá que cuando se quieran enviar paquetes a la red 192.168.201.0/24 (obsérvese que los nodos de esta red no pueden verse directamente desde el nodo local que es 192.168.1.1) deberá enviarlos al enrutador 192.168.1.254 (que sí es alcanzable por el nodo local), para que este gestione el envío hacia su destino. Además, como hemos proporcionado el calificador **-P**, la ruta será persistente.

Si la especificación de la red de destino hubiera sido 0.0.0.0, entonces la ruta declarada se correspondería con la ruta por defecto.

**Ejemplos**

En la declaración de la orden **ROUTE** se pueden utilizar nombres simbólicos en vez de usar las direcciones numéricas de hosts y redes. En este caso, los nombres simbólicos de redes deben estar declarados en el fichero de Windows C:\WINDOWS\SYSTEM32\DRIVERS\ETC\NETWORKS. De modo semejante, los nombres simbólicos de hosts deben estar declarados en el fichero de Windows C:\WINDOWS\SYSTEM32\DRIVERS\ETC\HOSTS.

Otro calificador que puede ser útil en la orden **ROUTE** es **-f**. Este calificador borra la tabla de enrutamiento en curso para iniciar una nueva configuración limpia de las rutas del sistema. Si el calificador **-f** se usa dentro de un comando cualquiera, se

ejecutaría el comando después del borrado de las rutas en la tabla de rutas.

Por último, la orden **ROUTE CHANGE** se utiliza para hacer cambios en rutas existentes, por ejemplo, si sobre la orden anterior se quiere hacer el cambio de puerta para que tome el nuevo valor 192.168.1.250, ejecutaríamos la orden:

```
ROUTE CHANGE 192.168.201.0 MASK 255.255.255.0  
192.168.1.250
```

en donde ya no sería necesario el calificador de persistencia **-P**, ya que este solo se toma en cuenta junto con el comando **ADD**.



Ejemplos

Reconocer los elementos de una tabla de rutas en un nodo Windows

Fijémonos en la Fig. 6.5, que visualiza la ejecución de la orden **route print** sobre un sistema Windows XP. En primer lugar observamos que hay dos interfaces reales: la de la red de área local inalámbrica (de Intel) y otra denominada *Loopback*. Esta última es el modo en que TCP/IP comunica aplicaciones dentro del mismo nodo, utilizando la dirección de la red 127.0.0.0, que queda reservada para este propósito. De hecho, 127.0.0.1 es el propio nodo local o «local host».

En segundo lugar, observamos la ruta 192.168.1.0 con máscara 255.255.0.0. Define una puerta de acceso que es 192.168.1.137, que es el mismo nodo local. En efecto, cuando el nodo quiere enviar un paquete a otro nodo de su misma red no necesita mandarlo a ningún router y directamente lo pone en su tarjeta de red (192.168.1.137).

La puerta de enlace predeterminada es 192.168.1.1, que sería la dirección del router que resolvería cualquier destino que ninguna otra ruta pueda resolver.

La última línea, que tiene como destino de red 255.255.255.255, es muy especial. Se refiere a los paquetes *broadcast* de la red y, por tanto, tiene un funcionamiento diferente. Al final aparecería una colección de rutas persistentes o estáticas, que en el ejemplo de la figura está vacía.

Cuando un paquete IP alcanza a un nodo, sea o no un router, se compara la dirección de destino con las entradas de la tabla de rutas para averiguar si ese nodo es el destinatario o, en caso contrario, si debe reexpedirlo por alguna de sus interfaces de red. Es posible que un destino se alcance por varias rutas; en ese caso, el software de enrutamiento elige la mejor ruta basándose en las especificaciones de las métricas de cada ruta. Si el destino no se alcanzara por ninguna entrada, entonces se utilizará la ruta por defecto si existe. Si no estuviera definida, se generará un mensaje de error, puesto que el destino sería inalcanzable.

Hay que hacer unas últimas observaciones. La dirección de un nodo y la de su pasarela por defecto deben estar en la misma red; de lo contrario, no podrán verse y el encaminamiento no funcionará. En segundo lugar, hay que tener en cuenta que

```
ca Simbolo del sistema
Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Abbad>route print

ILista de interfaces
0x1 ..... MS TCP Loopback interface
0x2 00 0e 35 0c 43 16 ..... Intel PRO/Wireless 2200BG Network Connection
0x2 PANDA NDIS IM Filter Miniport 5.0.92

Rutas activas:
Destino de red   Máscara de red   Puerta de acceso   Interfaz   Métrica
127.0.0.0       255.0.0.0       192.168.1.137    192.168.1.137  25
127.0.0.0       255.0.0.0       127.0.0.1        127.0.0.1      1
192.168.1.0     255.255.255.0  192.168.1.137    192.168.1.137  25
192.168.1.137  255.255.255.0  192.168.1.137    192.168.1.137  25
192.168.88.0    255.255.255.0  192.168.88.1      192.168.88.1    276
192.168.88.0    255.255.255.0  192.168.88.1      192.168.88.1    276
192.168.88.0    255.255.255.0  192.168.88.1      192.168.88.1    276
192.168.88.0    255.255.255.0  192.168.88.1      192.168.88.1    276
192.168.88.0    255.255.255.0  192.168.88.1      192.168.88.1    276
192.168.200.0   255.255.255.0  192.168.200.1     192.168.200.1    276
192.168.200.0   255.255.255.0  192.168.200.1     192.168.200.1    276
192.168.200.0   255.255.255.0  192.168.200.1     192.168.200.1    276
224.0.0.0        248.0.0.0       192.168.1.137    192.168.1.137  281
224.0.0.0        248.0.0.0       192.168.1.137    192.168.1.137  281
224.0.0.0        248.0.0.0       192.168.1.137    192.168.1.137  281
224.0.0.0        248.0.0.0       192.168.1.137    192.168.1.137  281
Puerta de enlace predeterminada: 192.168.1.1

Rutas persistentes:
ninguno

C:\Documents and Settings\Abbad>
```

Fig. 6.5. Tabla de rutas en un nodo Windows XP.

por cada interfaz de red se puede definir más de una ruta. Y por último, si la tabla de rutas es grande, se ralentizará excesivamente el proceso de análisis: no hay que olvidar que esta comparación con la tabla de rutas debe hacerse con cada paquete IP que llegue al router.

Veamos la ejecución de una orden **route print** en Windows 7 (Fig. 6.6). En primer lugar se observa que hay una interfaz de red real (Adaptador de red Broadcom 802.11n). El resto de las tarjetas de red que aparecen son virtuales y tienen funciones especiales. A la izquierda de estas tarjetas de red se pueden ver las direcciones físicas asociadas a cada interfaz (C4:46:19:1B:45:B1 para la interfaz física considerada anteriormente).

También se puede ver un adaptador especial denominado *Software Loopback Interface*, que es el utilizado por el sistema operativo para comunicar aplicaciones dentro del mismo nodo utilizando TCP/IP. Se corresponde con la dirección de red 127.0.0.0. De hecho, el propio nodo se direcciona localmente como 127.0.0.1, que es una dirección reservada y que se puede nombrar como «local host». Su dirección equivalente en IPv6 es «::1».

El mapa de rutas es semejante al visto para Windows XP, pero al final del mismo aparece una extensión para el sistema de enruteamiento para IPv6, que viene instalado por defecto en Windows 7 y no en Windows XP.

```
ca Simbolo del sistema
C:\Users\Abbad>route print

ILista de interfaces
1\.....c4 46 19 45 b1 .....Adaptador de red Broadcom 802.11n
2\.....00 56 c0 00 00 00 .....Unidad Virtual Ethernet Adapter for VMnet1
3\.....00 56 c0 00 00 00 .....Unidad Virtual Ethernet Adapter for VMnet8
4\.....00 00 00 00 00 00 .....Software Loopback Interface 1
27\....00 00 00 00 00 00 .....Adaptador ISATAP de Microsoft #2
22\....00 00 00 00 00 00 .....e0 Adaptador ISATAP de Microsoft #2
11\....00 00 00 00 00 00 .....e0 Adaptador Gto4 de Microsoft
23\....00 00 00 00 00 00 .....e0 Adaptador ISATAP de Microsoft #3
15\....00 00 00 00 00 00 .....e0 Teredo Tunneling Pseudo-Interface

IPv4 Tabla de enruteamiento
=====
Rutas activas:
Destino de red   Máscara de red   Puerta de enlace   Interfaz   Métrica
0.0.0.0          0.0.0.0          192.168.1.129    192.168.1.129  25
127.0.0.1        255.0.0.0       En vinculo        127.0.0.1      306
127.0.0.1        255.255.255.255 En vinculo        127.0.0.1      306
127.255.255.255 255.255.255.255 En vinculo        127.0.0.1      306
192.168.1.0      255.255.255.0  En vinculo        192.168.1.129  281
192.168.1.129   255.255.255.0  En vinculo        192.168.1.129  281
192.168.255.255 255.255.255.255 En vinculo        192.168.1.129  281
192.168.88.0     255.255.255.0  En vinculo        192.168.88.1    276
192.168.200.0   255.255.255.0  En vinculo        192.168.200.1    276
192.168.200.0   255.255.255.0  En vinculo        192.168.200.1    276
192.168.200.0   255.255.255.0  En vinculo        192.168.200.1    276
224.0.0.0        248.0.0.0       En vinculo        127.0.0.1      306
224.0.0.0        248.0.0.0       En vinculo        192.168.200.1    276
224.0.0.0        248.0.0.0       En vinculo        192.168.88.1    276
224.0.0.0        248.0.0.0       En vinculo        192.168.1.129  281
255.255.255.255 255.255.255.255 En vinculo        192.168.200.1    276
255.255.255.255 255.255.255.255 En vinculo        192.168.1.129  281
255.255.255.255 255.255.255.255 En vinculo        192.168.1.129  281

Rutas persistentes:
ninguno

IPv6 Tabla de enruteamiento
=====
Rutas activas:
Cuando destino de red métrica   Puerta de enlace
1 306 ::1/128                  En vinculo
1 306 ff00::/8                 En vinculo

Rutas persistentes:
ninguno
```

Fig. 6.6. Tabla de rutas en un nodo Windows 7.



Ejemplos

Reconocer los elementos de una tabla de rutas en un nodo Linux

En la Fig. 6.7 podemos observar el resultado de la orden **ip route show** sobre un sistema Linux, que sirve para pedir información relacionada con las rutas del nodo sobre el que se ejecuta.

El resultado en este caso es de tres líneas, de las que nosotros nos fijaremos en la primera y en la tercera. En la primera línea se especifica el nombre de la red IP, que es 192.168.1.0/24, la interfaz de red asociada (eth1) y la dirección IP en esta interfaz

que corresponde al nodo local (192.168.1.34), que obviamente deberá estar en el ámbito de la red (192.168.1.0/24).

En la tercera línea se especifica la ruta por defecto (*default*). Esta línea se interpreta como que el *default gateway* del sistema se puede conseguir por la interfaz eth1 (dev eth1), siendo la dirección IP del enrutador (*default Gateway*) 192.168.1.1.

Obsérvese que la dirección del enrutador de la red local está en la misma red local que la dirección IP local, de lo contrario el nodo local no podría comunicar con su enrutador más próximo y el nodo quedaría aislado.

```

Archivo Editar Ver Terminal Solapas Ayuda
aabab@ptx:~$ ip route show
192.168.1.0/24 dev eth1 proto kernel scope link src 192.168.1.34
169.254.0.0/16 dev eth1 scope link metric 1000
default via 192.168.1.1 dev eth1
aabab@ptx:~$
```

Fig. 6.7. Tabla de rutas en un nodo Linux.

En Linux, el sistema de creación de nuevas rutas es semejante al visto anteriormente para Windows. En este caso se utiliza la orden **ip route add**, que también admite muchos calificadores. Como siempre, la recomendación habitual cuando se usa Linux es consultar la ayuda del distribuidor de software o la ayuda de la orden para conocer con precisión los parámetros que admite y su forma de uso.

Si el nodo local tuviera, como antes, la dirección 192.168.1.1/24, y ejecutamos en Linux la orden:

ip route add -net 192.168.201.0/24 gw 192.168.1.254 dev eth0

Entonces tendríamos declarada la misma ruta que hemos creado antes sobre Windows. En este caso hemos declarado que la interfaz por donde se alcanza el router es eth0 (en Windows también se podría especificar, aunque, si se omite, Windows selecciona automáticamente la interfaz compatible con la dirección del encaminador).

2.3. Interconexión de encaminadores

Un encaminador resuelve las rutas de los paquetes cuyo destino se encuentra en alguna de las interfaces de red que posee o bien delega esta función en otro encaminador próximo.

Es evidente que el enrutador corporativo no puede tener una interfaz de red por cada posible red de destino, por lo que no sería capaz de resolver el destino de la mayor parte de los paquetes.

Para solucionar esto, los enrutadores se configuran estableciendo relaciones de unos con otros. El nexo lógico de unión entre dos encaminadores son las entradas de la tabla de rutas en que se hacen referencia entre sí. De este modo, cuando un router recibe un paquete, consulta su tabla de rutas para averiguar si es capaz de resolver el destino. Si no encuentra la dirección en su tabla de rutas, entonces encamina el paquete hacia un encaminador de orden superior confiando en que él sepa resolverlo.



Ejemplos

Configuración de red con dos encaminadores

Vamos a estudiar un ejemplo de configuración en el que dos nodos se sitúan en segmentos de red distintos e interconectados a través de un encaminador. Este encaminador se conecta a un segundo enrutador para su salida al exterior de la red (Fig. 6.8).

En el diagrama de red se pueden ver tres redes distintas configuradas con dos nodos, uno en la red1 y otro en la red2, y dos routers, uno llamado Router1, que conecta las redes de los dos nodos, y otro Router2, que se utilizará como *gateway* por defecto. En la parte inferior aparece una tabla simplificada de las rutas más específicas que tendrán que crearse en el Router1. El gráfico nos va a servir para explicar los dos casos siguientes.

Comunicación de dos nodos con rutas conocidas

Supongamos que el nodo1 de la red1 quiere enviar un paquete IP al nodo2 situado en la red2. Puesto que el nodo2 no está en la misma red lógica que el nodo1, este le enviará el paquete IP al Router1, al que descubrirá por estar escrito en su tabla de rutas como pasarela por defecto, para que cumpla con su función de encaminamiento.

Una vez que el paquete llega al Router1, este comparará la dirección de destino (209.85.15.20) con las entradas de su tabla de encaminamientos y observará que hay una ruta (la número 1) que alcanza la red2, y ello lo consigue si reexpide el paquete a través de su interfaz de red NICr2. Una vez escrito el paquete IP en la red2, ya habrá acabado su función logrando su objetivo porque no hay que dar un salto posterior (la red se alcanza como vínculo local).

Comunicación a través de la ruta por defecto

Imaginemos ahora el caso de que el nodo1 quiere enviar un paquete IP a una dirección cualquiera que no se encuentra ni en la red1 ni en la red2. En ese caso, cuando el paquete llegue al Router1, configurado como ruta por defecto del nodo1, se examinará la tabla de rutas para ver si existe alguna entrada capaz de alcanzar el destino. Como el Router1 no tiene ninguna entrada con ese destino, utilizará la ruta por defecto, que en este caso apunta al router externo cuya dirección es 65.23.4.1, que será previsiblemente capaz de resolver el destino. Para alcanzar su objetivo, el Router1 sabe que con ese salto no se alcanza el destino ya que su siguiente salto es el Router2.

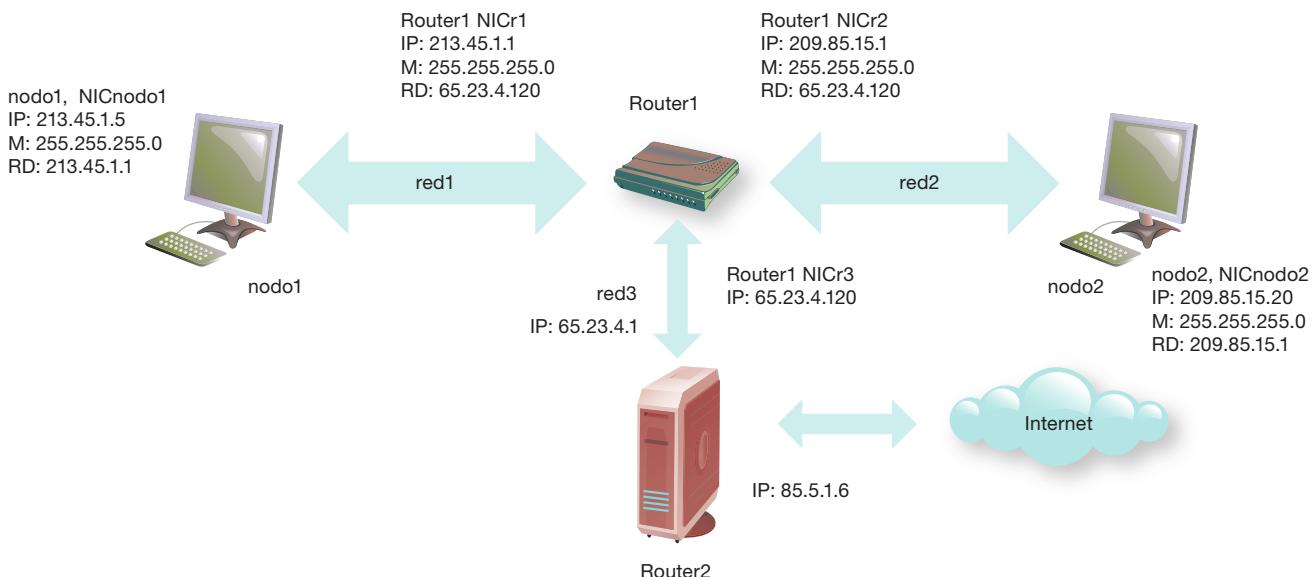


Fig. 6.8. Ejemplo gráfico de enrutamiento IP.

Número ruta	Red destino	Máscara	Puerta acceso	Interfaz	Siguiente salto
1	209.85.15.0	255.255.255.0	209.85.15.1	NICr2	Vínculo local
2	213.45.1.0	255.255.255.0	213.45.1.1	NICr1	Vínculo local
3	0.0.0.0	255.255.255.255	65.23.4.1	NICr3	Router2



Investigación

En la página web [http://www.wikilearning.com/tutorial/manual_practico_de_ipables-que_es_un_firewall/9755-1](http://www.wikilearning.com/tutorial/manual_practico_de_iptables-que_es_un_firewall/9755-1) puedes encontrar un completo manual de **iptables** junto con una descripción de lo que es un cortafuegos. Tiene mucho interés que te familiarices con la estructura de calificadores de esta orden porque es ampliamente utilizada en el mundo Linux. Te puede ser de gran utilidad confeccionarte una tabla con los calificadores más importantes. Puedes ayudarte también de la información que hay en la página web https://www.ac.usc.es/docencia/ASRII/Tema_4html/node6.html



Ampliación

Entre las ventajas que aporta la tecnología NAT se encuentran:

- Ahorro de direcciones IPv4 públicas, que están prácticamente agotadas.
- Mejoras en la seguridad de la LAN al hacer ocultas las direcciones IP privadas al exterior.
- Permite a los administradores de red desarrollar su propio sistema de direccionamiento IP interno.

Cuando NAT sustituye una dirección privada con otra pública elegida arbitrariamente entre todas las IP públicas contratadas disponibles, se habla de **DNAT** (*Dynamic Network Address Translation*) o formalmente *IP Masquerading*. En cambio, cuando la asignación de la IP pública se define específicamente sin dejar capacidad de elección al sistema, entonces se habla de **SNAT** (*Static Network Address Translation*).

Cuando se desarrolle la teoría sobre cortafuegos se ampliará la información sobre los protocolos de traducción, entre otros **PAT** (*Port Address Translation*) para la traducción de puertos.

2.4. Enmascaramiento IP

El enmascaramiento IP (*IP Masquerading*) es una función de red de algunos sistemas operativos actuales que permiten la conexión de otros miembros de la red a Internet a través de la conexión que ya posee la máquina que soporta el enmascaramiento. Para el correcto funcionamiento del *IP Masquerading* no es necesario que todas las estaciones de la red tengan una dirección IP única y pública de Internet; basta con que tengan la pila de protocolos IP y correctamente configurado su sistema de rutas. Analicemos con un ejemplo cómo funciona esta técnica. La función de *IP Masquerading* también la realiza el protocolo **NAT** (*Network Address Translation*).

Supongamos que tenemos un host, que llamaremos **CLIENTE** y que tiene por dirección IP 10.1.1.5 y máscara de toda la red 255.0.0.0, que quiere acceder a Internet solicitando páginas a través de su navegador. La conexión a Internet se ha realizado en otro host de la red al que llamaremos **SERVIDOR** con dirección IP 10.1.1.1 y que está en la misma subred que **CLIENTE**.

Cuando **SERVIDOR** realiza una conexión a Internet, su proveedor le proporciona una dirección IP a la interfaz de red WAN por la que se conecta remotamente que es 213.97.2.12.

Debemos tener en cuenta que los pasos 1 y 4 se producen dentro de una LAN, mientras que los números 2 y 3 proceden de una WAN.

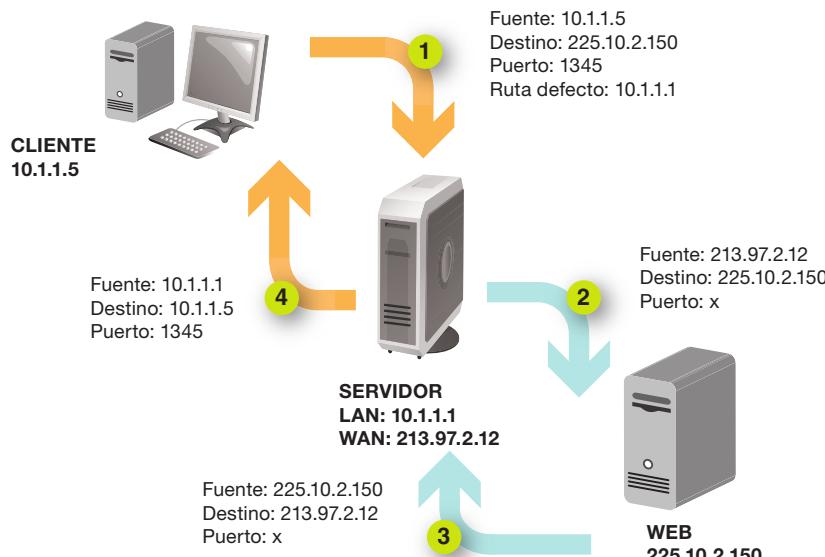


Fig. 6.9. Esquema de un ejemplo de utilización de enmascaramiento IP.

En **CLIENTE**, configuramos TCP/IP para que la ruta por defecto apunte a **SERVIDOR**. Por otra parte, por ejemplo, el navegador pediría datos utilizando un puerto que el servidor que le brinde las páginas aprovechará para enviárselas con la seguridad de que el navegador se quedó escuchando por ese puerto.

Si el navegador en **CLIENTE** solicita una página al servidor 225.10.2.150 por el puerto 1345, como **CLIENTE** no tiene acceso por red al host 225.10.2.150, mandará el mensaje por la ruta de defecto a **SERVIDOR**. Si **SERVIDOR** tiene habilitado el servicio de enmascaramiento, sustituirá la dirección IP de **CLIENTE** por la suya propia en la interfaz WAN (213.97.2.12) y el número de puerto por otro que tenga libre, haciéndole la petición al servidor web de dirección 225.10.2.150. Cuando el servidor web le conteste, **SERVIDOR** sustituirá la dirección IP WAN suya (213.97.2.12) por la dirección IP propia en su red de área local (10.1.1.1) y se lo mandará a **CLIENTE** por el puerto por el que este se quedó esperando, en nuestro ejemplo, el 1345. De este modo, **CLIENTE** ha recibido sus datos transparentemente.

3. El cortafuegos

Abrir la propia red de área local al mundo exterior de Internet, que es absolutamente público y mayoritariamente incontrolado, puede ser peligroso para la organización, ya que pueden producirse accesos indebidos desde el exterior, desde los simples curiosos hasta los procedentes del espionaje de la competencia.

3.1. Características generales

Es conveniente que las organizaciones restrinjan los accesos a su red desde el exterior. Para ello se instala en el perímetro de la red un nodo especial denominado cortafuegos o *firewall* que se encarga de limitar los accesos en ambas direcciones, haciendo invisible la red de área local desde el exterior o restringiendo los accesos desde dentro hacia afuera.

En general, un cortafuegos tiene que proporcionar tanto seguridad en los accesos como transparencia en los envíos de datos.



Actividades

3. Confirma la veracidad de las siguientes afirmaciones:
 - a) El encaminador opera siempre en el nivel 3 de OSI.
 - b) Algunos encaminadores toman funciones de niveles superiores al 3.
 - c) Un router solo puede encaminar paquetes IP.
 - d) Todos los protocolos de red son encaminables con el router adecuado.
 - e) Los routers no pueden encadenarse en cascada.

4. Escribe en la columna de la derecha el nombre de la red del nodo que aparece en la de la izquierda. La primera línea te servirá como ejemplo:

Nodo	Red
10.0.1.88/24	10.0.1
192.168.1.1/16	
192.168.1.1/8	
192.168.1.1./32	

5. Preséntate en una máquina Windows como administrador del sistema para que puedas modificar los parámetros de red.
 - a) Crea una ruta para alcanzar la red 192.168.30 por el enrutador 192.168.30.254.
 - b) Crea una ruta que alcance la red 192.168 por el enrutador 192.168.101.254.
 - c) Visualiza las rutas para comprobar que están creadas correctamente.
 - d) Borra las dos rutas.

6. Repite el ejercicio anterior sobre una estación Linux.
7. Confirma la veracidad de las siguientes afirmaciones:
 - a) Los encaminadores pueden ser abiertos, cerrados o de frontera.
 - b) Los algoritmos de encaminamiento estático son aquellos que impiden que se cambien las tablas de rutas del encaminador en el que se ejecutan.
 - c) Un algoritmo de encaminamiento adaptativo habilita al router para aprender por sí mismo la topología de la red.
 - d) El coste de una ruta es el precio económico que se ha de pagar por transmitir un paquete.
 - e) El tiempo de convergencia es el tiempo que tarda un router en arrancar desde que se enciende hasta que queda operativo.

8. Relaciona los elementos de la columna de la izquierda con los de la derecha:

Tipo de protocolo de enrutamiento	Protocolo de enrutamiento
IGP	RIPv1 o RIPv2
EGP	BGP
	OSPF
	IS-IS
	EIGRP



CEO

S M R _ R L _ A A b a d _ 0 6 _
Cortafuegos.docx

Documento que contiene información sobre cortafuegos personales y corporativos.

Hay cortafuegos que operan en muy distintos niveles de la arquitectura OSI. Así, un cortafuegos que opere en niveles bajos será más fácilmente configurable pero menos flexible. Por ejemplo, una vez que se ha establecido la conexión lícitamente, la misión del cortafuegos se extingue. Otros firewalls, sin embargo, operan en los niveles superiores e investigan en el interior de cada paquete de datos, lo que los hace lentos pero extraordinariamente flexibles.

Los cortafuegos suelen configurarse mediante políticas o reglas que se establecen en función del origen, del destino y del protocolo utilizado. Por defecto, un cortafuegos cierra toda comunicación. Es el administrador de red quien tiene que abrir los diferentes puertos de comunicación y habilitar los flujos de transporte permitidos.

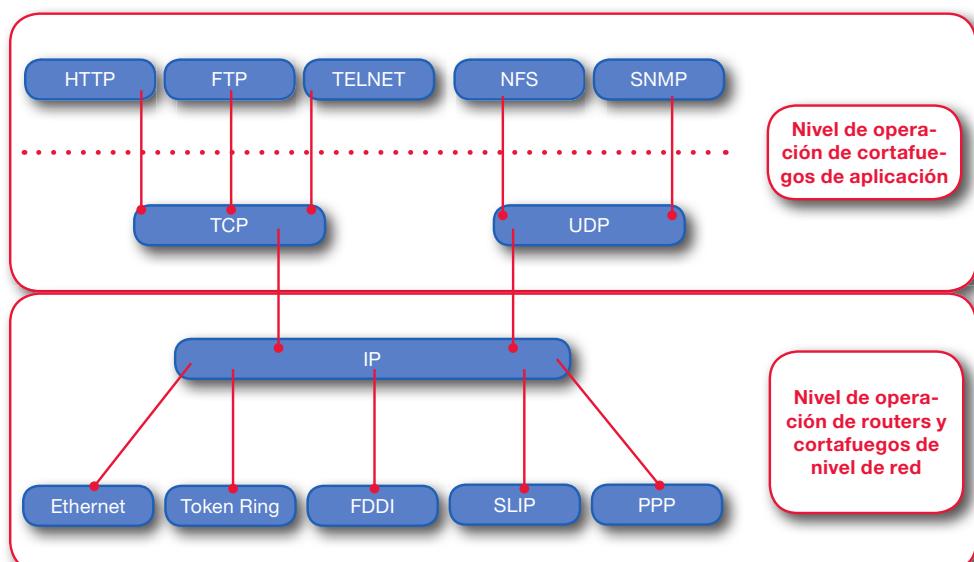


Fig. 6.10. Niveles de operación de los cortafuegos de nivel de red y de aplicación.

Además, si el cortafuegos opera en un nivel elevado, puede incluir nuevas funcionalidades, por ejemplo, en la admisión de correo electrónico a través del puerto 25 puede analizarse el contenido para explorar si el mensaje incorpora algún virus.

Cuando un equipo conectado a la red pierde su conexión, lo primero que hay que hacer es comprobar el sistema de cableado pero, inmediatamente después, debemos sospechar del cortafuegos del equipo, que puede estar impidiendo las conexiones desde o hacia el exterior del equipo por un error en la configuración de las políticas de acceso a la red.



Ampliación

En la actualidad los cortafuegos operan en las capas superiores y pueden incorporar nuevos valores añadidos que mejoran la seguridad (Fig. 6.10). Algunos de estos valores se citan a continuación:

Traducción de direcciones NAT. Consiste en que las direcciones IP utilizadas por los hosts de la Intranet solo tienen validez dentro de la propia red de área local. El cortafuegos se encarga de sustituir cada dirección IP de la Intranet en los paquetes que entran y salen a su través por otras direcciones IP virtuales, protegiendo de este modo contra accesos indeseados a través de direcciones Internet que realmente no existen en la Intranet. NAT es un caso particular de *IP Masquerading*.

Traducción de direcciones y puertos NAPT (*Network Address Port Translation*). Es una variación de NAT en donde no solo se sustituyen las direcciones IP sino también los números de puertos. En ocasiones a este protocolo también se le llama **PAT** (*Port Address Translation*), que es una nomenclatura propia de Cisco.

Se trata de sustituir el puerto de escucha del segmento de salida por otro que queda abierto en la interfaz de salida del gateway (o cortafuegos) y que enmascara al original. PAT ofrece una mejora de la seguridad de las aplicaciones locales ocultando su puerto de escucha y además asigna automáticamente puertos a las aplicaciones que se lo solicitan.

Protección frente a virus. Al operar en las capas altas, estos cortafuegos son capaces de analizar la información que fluye hacia la Intranet, y pueden detectar anomalías en los datos y programas.

Auditoría. El cortafuegos puede auditar recursos concretos de la Intranet y avisar a través de un sistema de mensajería electrónica del intento de violación de algún recurso o de accesos indebidos.

Gestión de actividad. A través de agentes SNMP o DMI, propios de gestión de red, se puede monitorizar el cortafuegos con el fin de realizar informes sobre la actividad de la red.

3.2. Zonas desmilitarizadas

Una red desmilitarizada o **DMZ** (*Demilitarized Zone*) es una red compuesta por uno o más ordenadores que, en la instalación de red, se sitúan lógicamente entre la red corporativa, que se supone segura, e Internet, que es insegura. Los servicios típicos que se ubican en una DMZ son servidores web, ftp, de correo y DNS.

Existen muchas posibilidades para la construcción de una DMZ. Aquí nos fijaremos en algunas de ellas, pero todas tienen que cumplir su principal misión, que consiste en que se proporcionen servicios públicos a Internet sin comprometer la seguridad de los datos alojados en la red corporativa.

En el primer modelo de DMZ expuesto (Fig. 6.11-A), tanto la red corporativa como la DMZ se conectan a Internet a través de un router. La protección de la DMZ reside en la protección de cada uno de los servidores más el filtrado que pueda realizar el encaminador.

Sin embargo, la red corporativa queda protegida por un cortafuegos. Ninguna conexión procedente de Internet debe alcanzar a la red corporativa, pues toda la información disponible para Internet debe residir en la DMZ.



Vocabulario

En la documentación técnica es frecuente referirse a las zonas desmilitarizadas como redes perimetrales o, de modo más simple, referirse al perímetro. Así, para expresar que un servidor está situado en una **DMZ** podremos decir que es un servidor del perímetro.

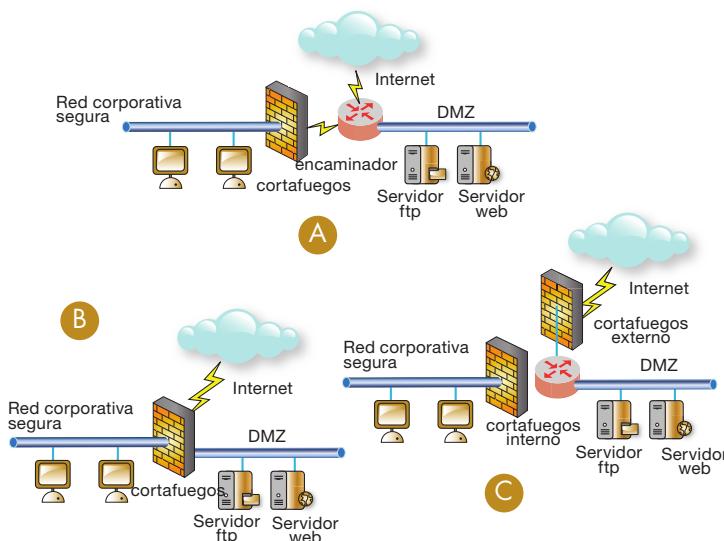


Fig. 6.11. Tres modelos para una DMZ.

En el segundo modelo (véase Fig. 6.11-B), tanto la red corporativa como la DMZ quedan protegidas por el cortafuegos. Esta configuración, que es la más común, requiere que el cortafuegos tenga definida una tercera red para la construcción de la DMZ. El filtrado de las conexiones será mucho más restrictivo en la red corporativa que en la DMZ.

En el tercer modelo que estudiaremos, la arquitectura de la red se complica (Fig. 6.11-C). En este caso, la DMZ queda encerrada entre dos cortafuegos. Obviamente es la configuración más segura, pero también la más costosa.

La configuración de la DMZ dependerá de la arquitectura de ella y de su relación con la red interna (protegida) y la externa. Según esto, el cortafuegos que hace de frontera entre la DMZ, la LAN e Internet debe establecer tres tipos de políticas de comunicación diferenciadas entre ellas:

a) **Políticas de relación LAN con Internet.** Estas directivas configuran el acceso de los usuarios de la LAN a Internet, por ejemplo, con servicios como navegación.

b) **Políticas de relación LAN con la DMZ.** Aquí se configurará cómo los usuarios de la LAN pueden acceder a los servicios provistos por los servidores ubicados en la DMZ, por ejemplo, para actualizar la información de las páginas web de un servidor web que se ubique en la DMZ.

También aquí debe configurarse cómo los servidores de la DMZ pueden acceder a los servicios ofrecidos desde la LAN. Cuanto menos restrictivos sea aquí, menor grado de protección se tendrá.



Investigación

En <http://bookalexa.blogspot.com/2008/02/perimetro-de-seguridad.html> tienes información sobre qué elementos en una red perimetral pueden ayudar a fortalecer la seguridad de una DMZ. Léela atentamente para hacerte una idea de los riesgos a que están expuestos los hosts que tienen un contacto perimetral con Internet y la forma en que se previenen.

Para instalaciones en entornos colaborativos, también puedes consultar la dirección <http://www.microsoft.com/spain/exchange/securomessaging/seguridad.mspx>

c) **Políticas de relación DMZ con Internet.** Aquí se configura cómo los usuarios de Internet (supuestamente anónimos) acceden a los servicios publicados por los servidores de la DMZ.

Para clarificar cómo puede cooperar una DMZ con la seguridad de la instalación de red, tomemos como ejemplo la instalación de una sede de comercio electrónico.

El comprador accede a la página web del vendedor a través de Internet y selecciona el artículo que desea comprar. Al servidor web, que estará situado en la DMZ del vendedor, se accede con una dirección IP pública, que puede ser propia del servidor web o la del encaminador o cortafuegos externo del vendedor, dependiendo de la configuración DMZ elegida. En cualquiera de los casos, la petición http del comprador debe llegar al servidor web situado en la DMZ.

La página web recoge información del cliente y la escribe en una base de datos. Es muy peligroso que esta base de datos resida en Internet o en una DMZ, puesto que los equipos situados en estas zonas de la red están expuestos a ataques. El diseñador de la aplicación ha resuelto que la base de datos debe residir en un servidor dentro de la red corporativa mucho más segura.

Por tanto, el administrador de la red tiene que definir unas políticas de acceso de modo que:

- Ninguna conexión procedente de Internet pueda acceder al servidor de bases de datos de la red corporativa.
- A esa base de datos solo puede acceder el servidor web situado en la DMZ y además exclusivamente a los puertos específicos para el acceso a la base de datos y no a otros.

De este modo, si un intruso quiere acceder a la red corporativa, el cortafuegos se lo impedirá; solo puede acceder al servidor web de la DMZ.

Si este servidor tuviera un agujero de seguridad y se hiciera con su control, solo podría acceder al servidor de bases de datos de un modo restringido.



Actividades

9. Comprueba si son ciertas o falsas las siguientes afirmaciones:

- Un cortafuegos siempre impide el paso de paquetes de red.
- El *firewall* siempre impide el paso a los paquetes entrantes, pero permite el paso de paquetes de red salientes.
- El cortafuegos opera siempre en los niveles más altos de OSI.
- El protocolo PAT de Cisco equivale exactamente al protocolo NAT.
- El cortafuegos por antonomasia en Linux es iptables.

10. Busca los errores técnicos en el siguiente comentario:

«Para proteger una red de área local de los accesos indebidos desde la red externa se ha instalado un cortafuegos al que se conectan la red local, Internet y una red perimetral. Para que un paquete de red procedente de Internet llegue a la red desmilitarizada, previamente debe pasar por la red local protegida. Sin embargo,

los paquetes con destino en Internet que proceden de la red local no es necesario que pasen por el cortafuegos ya que los riesgos siempre están en la red externa.»

11. Para realizar este ejercicio necesitas tener acceso a un router con capacidades de cortafuegos y gestión de una DMZ. Muchos de los enruteadores que suministran los proveedores de Internet de banda ancha tienen esta capacidad y te pueden servir.

- Accede a la página web de gestión del router por su dirección IP y comprueba que tienes activada la función de cortafuegos o que tienes habilitado el protocolo NAT.
- Ahora crea una zona DMZ (en estos encaminadores sencillos, la DMZ suele corresponderse con una red de un único nodo en donde se supone que se instalará el bastión de la DMZ que publicará servicios hacia Internet).
- Crea alguna regla en la DMZ para publicar algún servicio en la DMZ y que sea accesible desde Internet por la dirección pública del router.

● 4. Servidores proxy

Es evidente que no todos los ordenadores de una red pueden estar directamente en Internet. Cada host en Internet consume al menos una dirección IP, y ya hemos visto que con el sistema de direccionamiento IPv4 esto no es posible, ya que hay menos direcciones IP disponibles que nodos en Internet.

Por otra parte, no podemos poner un módem u otro acceso a cada estación de la red que tenga acceso a Internet. Lo ideal sería que las conexiones remotas pudieran ser compartidas por varios equipos.

● 4.1. Características generales

Una aplicación de red especializada para el acceso a Internet desde una red de área local es el **servidor proxy**, que se encarga, entre otras funciones, de compartir las conexiones a Internet y de habilitar una memoria caché con las páginas solicitadas por los usuarios de la LAN de modo que los accesos repetidos a la misma página sean mucho más rápidos, salvaguardando elpreciado ancho de banda.

Un servidor proxy de un servicio es un intermediario de red entre el cliente que solicita el servicio y el servidor que lo brinda. El cliente solicita el servicio al proxy, quien a su vez gestiona la petición en su propio nombre al servidor de destino.

Aunque el servicio proxy es muy especializado, algunos sistemas operativos de red, incluso de escritorio, incorporan funcionalidades tecnológicamente cercanas al proxy para compartir accesos remotos a Internet en pequeñas redes locales, típicamente domésticas. Es el caso de la tecnología **ICS** (*Internet Connection Sharing*, compartición de conexión a Internet) que Microsoft incorpora en sus sistemas a partir de Windows 98 para redes domésticas, o las tecnologías **NAT** (*Network Address Translation*, traducción de direcciones de red) comentadas en el RFC 1631.

El servidor proxy más común es webproxy (servidor proxy web o simplemente proxy), que permite a una red interna navegar por Internet mediante una única conexión a Internet.

Un servidor proxy enmascara las direcciones IP internas de la red de área local, sustituyéndolas al poner los paquetes en Internet por la suya propia, dirección real y única en el ámbito de Internet. De este modo, el cliente, típicamente un navegador, negocia la petición a Internet con el proxy y este gestiona el acceso a las páginas solicitadas. Cuando el servidor web remoto envía información al proxy, este hace la sustitución inversa en las direcciones IP y envía los datos a la estación que los solicitó. Por tanto, un servidor proxy también cumple con algunas de las funciones de cortafuegos.

● 4.2. Configuración del proxy

El navegador debe ser configurado correctamente para informarle de que cada vez que quiera realizar un acceso a Internet, no debe hacerlo directamente, sino a través del proxy. Los parámetros de configuración son básicamente dos: la dirección o nombre del proxy que atenderá nuestras peticiones y los puertos que atenderán nuestras peticiones en función de las aplicaciones. En las Figs. 6.12, 6.13 y 6.14 se pueden ver las fichas de configuración de tres navegadores para la utilización de un servidor proxy.

Ampliación

Aunque aquí se ha hablado siempre del servidor proxy como un intermediario entre el explorador de Internet del usuario y el servidor web sobre el que navega, no siempre hay que entender los servicios proxy de este modo, aunque sí es lo habitual. Los servidores proxy lo son de algún servicio en concreto, por ejemplo, existen servidores proxy de DNS que admiten peticiones de resolución de nombres de clientes y las encaminan en su nombre a los auténticos servidores DNS.

En general, cuando se habla de servidor proxy se referirán al servidor proxy web si no se especifica nada más, pero hay que fijarse bien porque a veces los servidores proxy llevan apellido.

CEO

S M R _ R L _ A A b a d _ 0 6 _ EjemploIPCOP.docx

Documento que contiene información sobre un ejemplo de cortafuegos corporativo IPCOP.

CEO

S M R _ R L _ A A b a d _ 0 6 _ EjemploNetBoz.docx

Documento que contiene información sobre un ejemplo de cortafuegos corporativo NetBoz.



Investigación

Un proxy transparente es aquel que proporciona servicios a sus clientes sin necesidad de una configuración especial, pero a cambio requiere que la red esté configurada de una manera específica. Por ejemplo, como el navegador no tendrá configurada su ficha de proxy, las peticiones se harán siempre a la puerta por defecto, que debe coincidir siempre con el servidor proxy «transparente» que admite peticiones directas del navegador.

Investiga en Wikipedia por la voz «proxy»: qué se entiende por proxy transparente y para qué se utiliza.

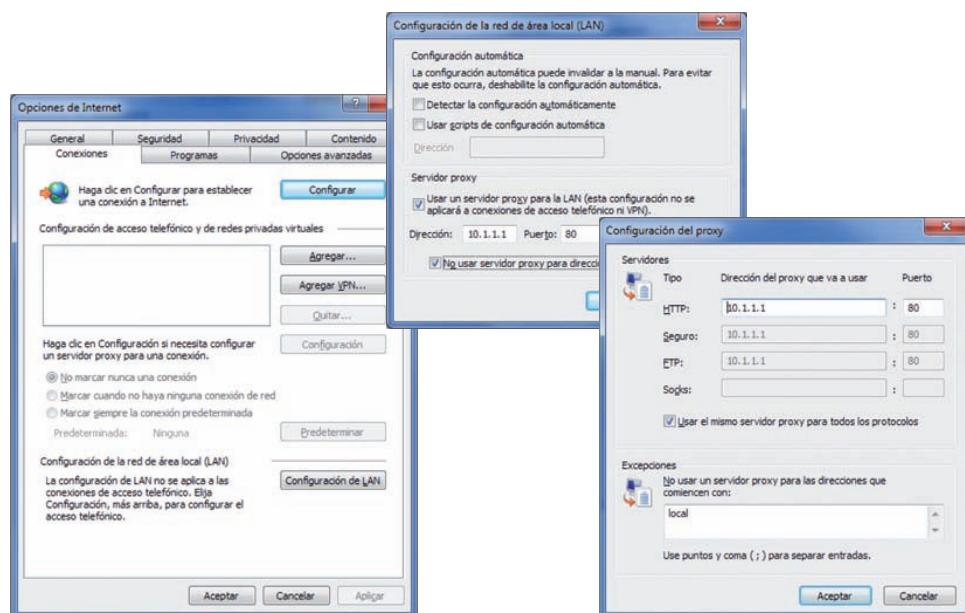
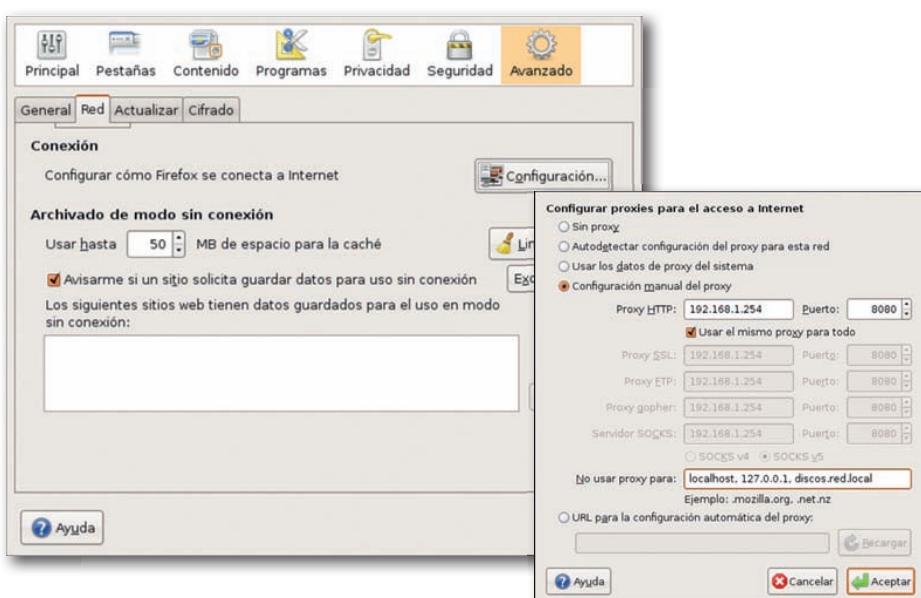


Fig. 6.12. Fichas de configuración del navegador Internet Explorer para el acceso a través de servidor proxy.

Por otra parte, el servidor proxy debe estar correctamente configurado. La información típica de configuración de un servidor proxy consiste en el conocimiento de las líneas de comunicación que puede habilitar en caso de necesidad (por ejemplo, a través del marcado automático), los usuarios que tendrán derecho de acceso a Internet, posibles filtros de contenidos, configuración de la memoria caché de páginas, etc.

En Firefox se puede configurar el proxy accediendo al menú *Editar* en la opción *Preferencias*. Desde allí podemos elegir la pestaña *Red* (figura de la izquierda). El botón de *Configuración* permitirá abrir la ventana de *Configurar proxies para el acceso a Internet* (figura de la derecha).



Hemos configurado que el proxy http esté en 192.168.1.254 y atenderá peticiones por el puerto 8080. Este proxy http también puede resolver las peticiones del resto de los protocolos: ssl, ftp, etc.

Por último, le indicamos al navegador que no utilice proxy cuando tenga que acceder a algunas direcciones, que se supone que se alcanzarán en local o a través de alguna de las rutas de red: localhost (el propio nodo), 127.0.0.1 (también el propio nodo, alcanzable por la dirección de loopback) y el servidor discos.red.local.

Fig. 6.13. Fichas de configuración del navegador Firefox sobre Linux para el acceso a través de servidor proxy.

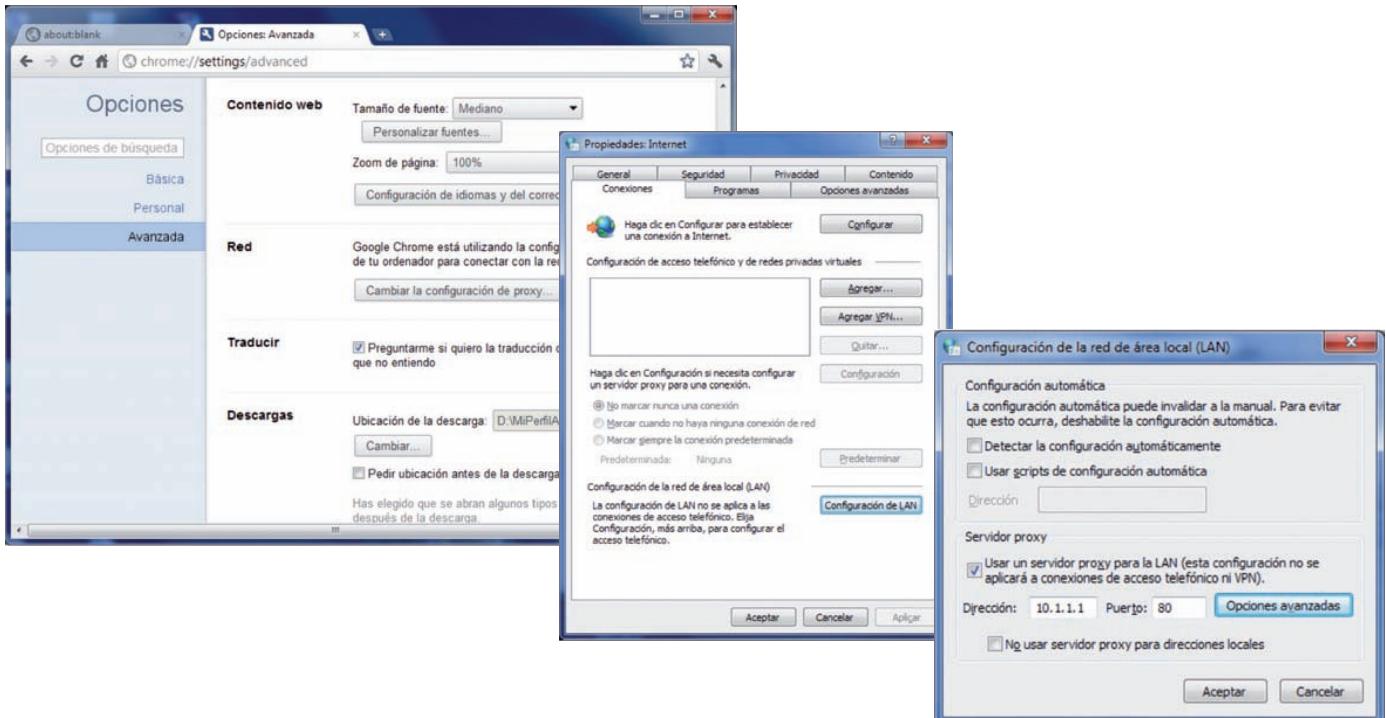


Fig. 6.14. Fichas de configuración del navegador Google Chrome sobre Windows para el acceso a través de servidor proxy.



Actividades

12. ¿Cuáles de las afirmaciones siguientes son erróneas?

- a) El protocolo NAT traduce los números de puertos entre la red externa y la interna.
- b) Cuando se utiliza NAT las direcciones privadas quedan ocultas a la red externa.
- c) Hay que elegir entre traducir direcciones o traducir puertos, pero no se pueden traducir ambos simultáneamente.
- d) Dos proxies web pueden encadenarse siempre y cuando no utilicen NAT.
- e) Todos los enruteadores que tienen acceso a Internet deben configurar NAT en la red externa.

13. Descubre dónde están los errores en el siguiente razonamiento:

«Un servidor proxy atiende peticiones web por la dirección 10.1.20.15 y el puerto 80. Este proxy web está encadenado a otro, utilizando NAT, con dirección 10.1.30.1 por el puerto 8080, que ya no usa NAT para salir a Internet. Un cliente de la red tiene por dirección IP 10.1.20.100 con máscara 255.255.255.0 y sin puerta por defecto. Como el segundo proxy no uti-

liza NAT el usuario ha decidido configurar su ficha de proxy en el navegador apuntando a 10.1.30.1 por el puerto 8080, que es por el que escucha el segundo web proxy. Después el usuario prueba la navegación, pero no le funciona».

14. Presentate en una máquina Windows y modifica los parámetros de configuración del proxy en Internet Explorer.

- a) Configura el navegador para utilizar el proxy 192.168.201.254 por el puerto 8080 para todos los protocolos que admite el navegador.
- b) Configura ahora el navegador para utilizar el proxy anterior, pero solo para los protocolos http y ftp.

15. Repite el ejercicio anterior sobre una estación Linux con navegador Firefox. Si no dispones de esta estación, puedes descargar una versión de Firefox sobre Windows desde <http://www.mozilla-europe.org/es/firefox/>

16. Vuelve a repetir la operación del ejercicio anterior con Google Chrome, que se puede descargar desde <http://www.google.es/chrome>



Caso práctico 1

Configuración de red de un equipo portátil para utilizar varios proxies

Supongamos que una empresa contrata un servicio de auditoría y el auditor se incorpora temporalmente a la empresa para llevar a cabo su función en donde conectará su portátil. La instalación de red de la empresa, por seguridad, tiene prohibida la navegación web, sin embargo, los trabajadores necesitan ftp para cargar y descargar ficheros de un servidor en Internet. Para ello, el administrador ha contratado los servicios de un proxy ftp en la dirección 192.168.120.55 por el puerto 8008. Los clientes habituales no pueden modificar ni la configuración de sus navegadores ni sus direcciones IP, de modo que la seguridad está relativamente garantizada.

El auditor, en cambio, sí necesita acceder a la web mediante protocolo http y el administrador de red ha resuelto instalar temporalmente un servidor proxy local en 192.168.1.101 por el puerto 8080. Cuando el auditor acabe su tarea, el administrador dará de baja el web proxy y todo volverá a ser como antes, puesto que nada más en la red se ha modificado para habilitar temporalmente este servicio.

La red local tiene un servidor DHCP que le ha dado al portátil del auditor la dirección 192.168.1.20/24 con puerta por defecto 192.168.1.254, que es el enrutador hacia Internet.

Vamos a estudiar cómo el administrador de red tiene que configurar el navegador del auditor y qué ruta siguen los paquetes cuando se utiliza el protocolo http y el ftp.

Para configurar correctamente el servidor proxy del portátil del auditor, deberemos tener en cuenta que el servidor proxy ftp debe apuntar al servidor ftp de la empresa (utilizará para ftp los mismos servicios de red que el resto de los empleados: 192.168.120.55 por el puerto 8008), mientras

que para el resto de los protocolos se hace apuntar el navegador al nuevo proxy (192.168.1.20 por el puerto 8080).

Ahora vamos a estudiar qué ruta siguen los paquetes http y ftp fijándonos en el diagrama de la Fig. 6.15.

Protocolo http

Cuando el auditor quiere acceder a una página web (accesible mediante el protocolo http), la configuración de su navegador le indica que debe recurrir al servidor web proxy 192.168.1.101 por el puerto 8080. Como 192.168.1.101 está en la misma red IP que el portátil del auditor (cuya dirección es 192.168.1.20/24), el proxy se alcanza sin necesidad de ningún enrutamiento y la conexión es directa (paso A).

Una vez que la petición esté en el proxy web este mandará la petición al encaminador corporativo (paso B) que es quien sabe salir a Internet, en donde estará situado el servidor web solicitado (paso C).

Protocolo ftp

En este caso la configuración del proxy dice que hay que acudir al proxy ftp situado en 192.168.120.55 por el puerto 8008, pero esta dirección no está en la red local, que es la red 192.168.1 (en donde están el portátil del auditor y el puerto LAN del enrutador corporativo). Entonces, para enviar este paquete hay que pasar antes por el encaminador (paso D), que sabrá llegar a la dirección 192.168.120.55 que es donde está el proxy ftp (paso E) y este a su vez reencañará la petición al servidor ftp solicitado, utilizando los mecanismos de enrutamiento disponibles para su salida hacia Internet, lo que dependerá de la dirección IP del destino, posiblemente pasando de nuevo por el enrutador corporativo.

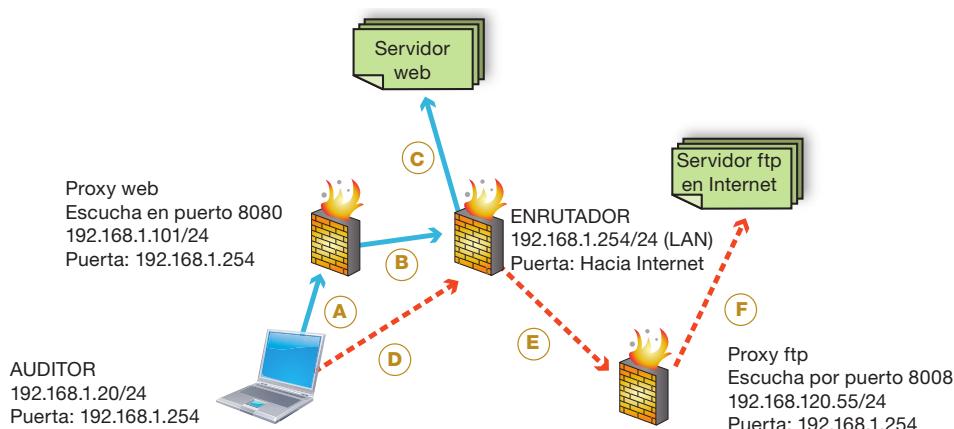


Fig. 6.15. Ruta de los paquetes http (línea continua) y ftp (línea discontinua) desde el portátil del auditor.



Caso práctico 2

Configuración de un equipo para mejorar el servicio utilizando un webproxy

Los servicios webproxy pueden proporcionar cierto valor añadido. Esto se consigue si en el proceso de convertir sus entradas desde Internet hacia las salidas en la LAN se introduce un nuevo paso que aporte valor al proceso.

Por ejemplo, si estamos descargando un fichero, el webproxy podría encargarse de hacer un test al fichero y comprobar si está infectado por algún virus.

Esto quiere decir que los servicios de descarga, típicamente http y ftp, deberían modificar su trayectoria de comunicación hacia Internet haciendo que los navegadores tengan configurado un servidor proxy con esta capacidad antivirus con estos dos servicios. La mayor parte de los antivirus comerciales analizan el tráfico de navegación de los clientes en donde se instalan por este procedimiento.

En este caso la configuración del proxy en el navegador de un usuario de la red tendría que tener el aspecto de la Fig. 6.16.

Algunos otros ejemplos de procesos proxy con valor añadido son:

- Chequeo de spam en correo electrónico para servidores proxy SMTP y POP.
- Chequeo de antivirus para correo electrónico para servidores proxy de correo.
- Filtrado de direcciones web sobre servidor proxy.



CEO

SMR_RL_AAbad_06_ConfiguracionProxies.pptx

Documento que contiene información sobre figuras de configuración de diversos servicios proxy con valor añadido como filtrado de spam o antivirus.

Se puede ver que el proxy lleva configurados exclusivamente los dos servicios que serán tratados por el antivirus: http y ftp, que apuntarán a la dirección 192.168.15.2 por el puerto 8080 que es donde supuestamente debe recoger las entradas en proxy que incorpora la aplicación antivirus.

El resto de protocolos saldrán por la ruta normal de salida: habitualmente la puerta por defecto del equipo.

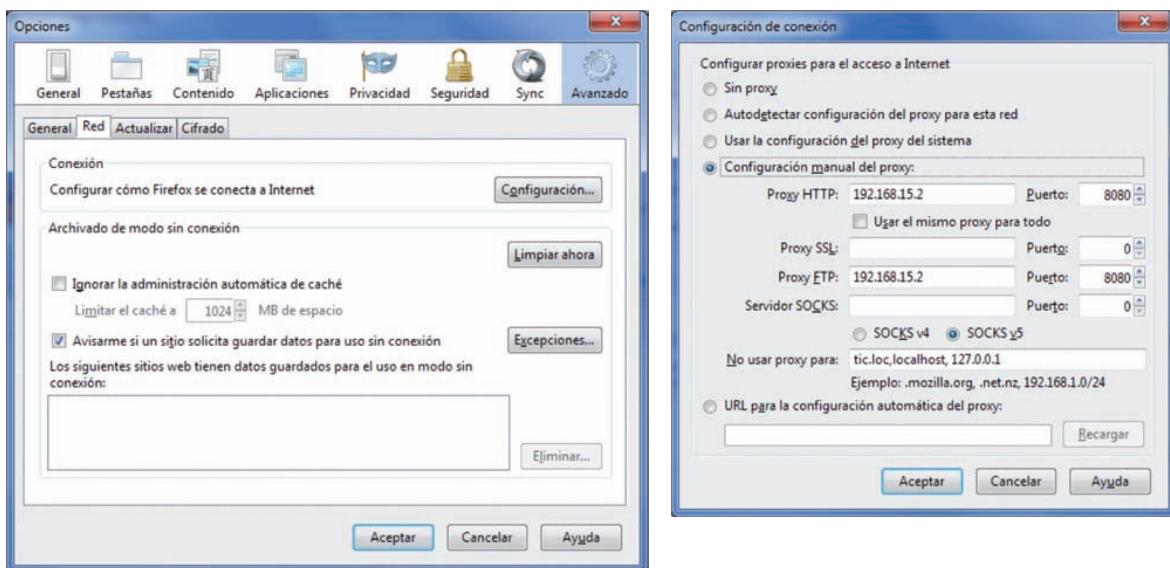
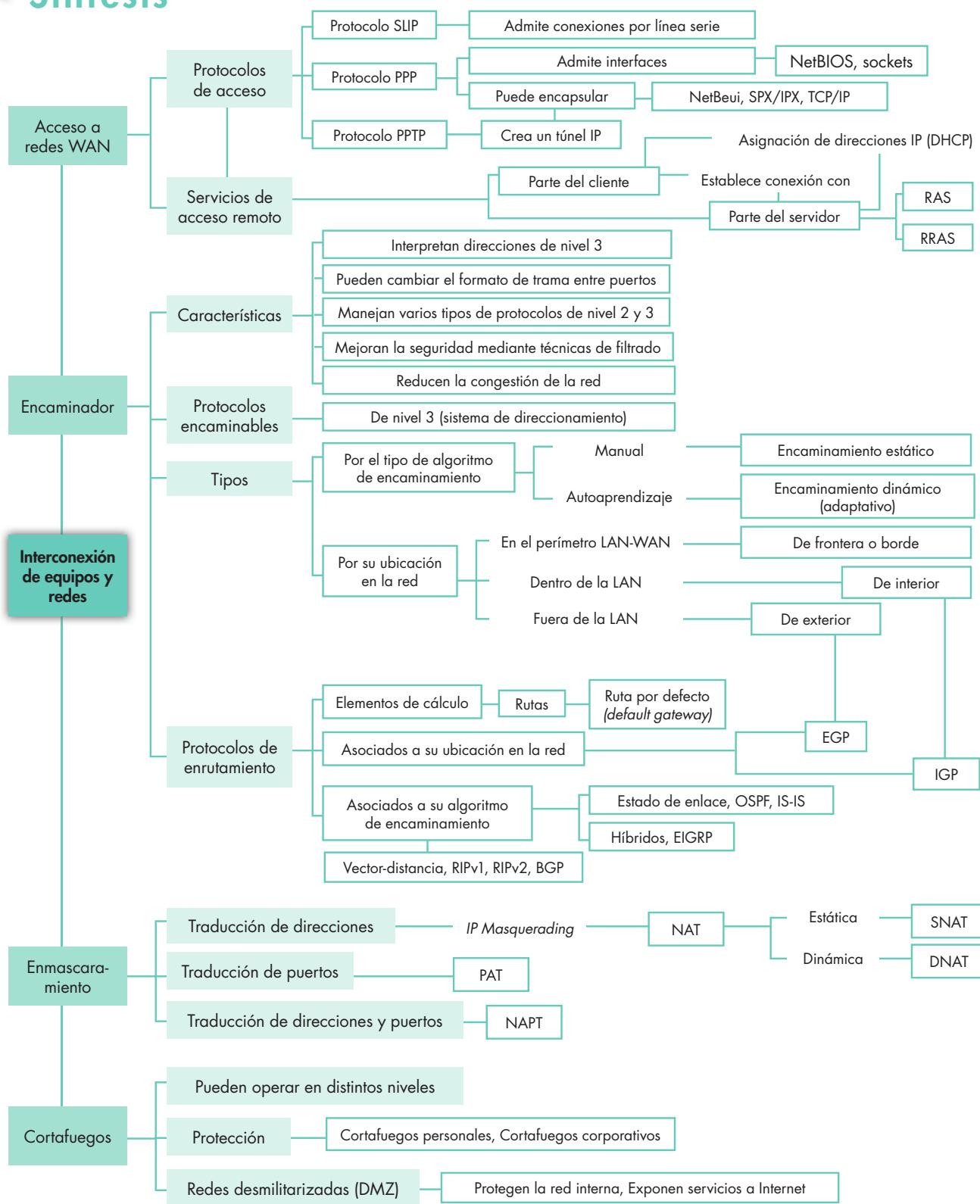


Fig. 6.16. Configuración del navegador Firefox para una redirección de servicios http y ftp.

Síntesis





Test de repaso

1. Enlaza los siguientes elementos característicos de algunas de las tecnologías de acceso a redes:

a) PPTP/SLIP	1) Servidor de acceso
b) RAS/RRAS	2) Acceso sobre ATM
c) PPPoE	3) Acceso sobre Ethernet
d) PPPoA	4) Protocolo de acceso remoto

2. El encaminador...

- a) Opera en el nivel 3 de OSI.
- b) Enruta paquetes NetBIOS.
- c) Enruta paquetes IP.
- d) Enruta segmentos TCP.
- e) Enruta tramas Ethernet.

3. Asocia los siguientes protocolos de enrutamiento con el tipo de tecnología que usan en su algoritmo de enrutamiento:

a) RIPv1	1) Híbrido
b) RIPv2	2) Estado de enlace
c) IGRP	3) Vector distancia
d) OSPF	
e) EIGRP	

4. Cuáles de las siguientes afirmaciones son verdaderas:

- a) Un router de exterior solo puede ejecutar algoritmos de encaminamiento estático.
- b) Un router de interior solo puede ejecutar algoritmos de encaminamiento estático.
- c) Un router de interior puede ejecutar cualquier tipo de algoritmo de encaminamiento, tanto estático como dinámico.
- d) Los routers de frontera no pueden ejecutar algoritmos de encaminamiento.

5. Asocia las características de los protocolos de traducción siguientes:

a) NAT	1) Asignación estática de direcciones públicas
b) PAT	2) Traducción de puertos
c) DNAT	3) Asignación dinámica de direcciones públicas
d) SNAT	4) Traducción de puertos y direcciones
e) NAPT	5) Traducción de direcciones

6. La orden **ROUTE ADD -P 192.168.201.0 MASK 255.0.255.0 192.168.1.254**

- a) Es incorrecta porque hay un problema en la máscara.

b) Es válida en Windows, pero no en Linux.

c) Es totalmente correcta en Windows.

d) Si fuera correcta, añadiría una ruta permanente.

7. Una red DMZ...

- a) Proporciona un segmento de red desmilitarizado que no puede sufrir ataques.
- b) Expone algunos servidores hacia Internet protegiendo la red interna.
- c) No tiene comunicación con la red interna.
- d) Impide la comunicación de sus nodos con Internet.

8. Relaciona las órdenes que aparecen en la columna de la izquierda con los sistemas operativos que se indican en la columna de la derecha.

a) ip route add	1) Windows
b) route add	2) Linux
c) route delete	
d) iptables	
e) ip route	
f) route print	

9. El cliente que accede a Internet a través de un webproxy no transparente:

- a) Basta con que configure en el navegador la dirección IP del webproxy.
- b) Basta con que configure en el navegador el puerto de escucha del webproxy.
- c) Necesita configurar en el navegador tanto la dirección IP como el puerto de escucha del webproxy.
- d) No requiere de ninguna configuración especial.

10. Un servidor proxy web está configurado como transparente. Según esto, analiza la veracidad de las siguientes afirmaciones para que pueda navegar por Internet:

- a) La puerta por defecto del cliente debe apuntar al servidor proxy.
- b) La puerta por defecto del cliente tiene que ser lógicamente compatible (estar en la misma subred) con la IP del servidor proxy.
- c) Basta con que cliente y servidor sean visibles recíprocamente en el segmento de red local.
- d) Necesita configurar en el navegador tanto la dirección IP como el puerto de escucha del webproxy.

Solución: 1: a-4, b-1, c-3, d-2, 2: a y c; 3: a-3, b-3, c-3, d-2, e-1, 4: c; 5: a-5, b-2, c-3, d-1, e-4; 6: a, b y d; 7: b; 8: a-2, b-1, c-1, d-2, e-2, f-1, g: c; 10: a.

Comprueba tu aprendizaje

I. Configurar los clientes de una red local para utilizar un sistema de enrutamiento

- Los protocolos PAP y CHAP, entre otros, son protocolos utilizados por RAS para la autenticación de usuarios. Busca información para comprender mejor cómo funcionan. Fíjate de modo especial en si las contraseñas viajan o no encriptadas por redes inseguras. Puedes empezar tu búsqueda por:
 - <http://es.tldp.org/Manuales-LuCAS/GARL2/garl2-x-087-2-ppp.authentication.html>
 - <http://www.tech-faq.com/lang/es/ppp-authentication.shtml>

- Utiliza la orden de Windows ROUTE PRINT para identificar todas las rutas IP de un nodo conectado a una red TCP/IP. Observa cuál es el destino de la ruta por defecto. Identifica las direcciones IP de las redes y sus máscaras.

Ahora repite el mismo procedimiento en otras estaciones de la misma red y establece comparaciones entre los resultados obtenidos en cada estación, razonándolas.

Puedes repetir esta actividad sobre un nodo Linux utilizando la orden **ip route show**.

- En la dirección web <http://es.wikipedia.org/wiki/Enrutador> puedes encontrar una información detallada de las características técnicas, protocolos y procedimientos de routers para acceso de banda ancha. Lee el documento para darte cuenta de cómo se integran todos estos elementos en las propuestas comerciales de los fabricantes de hardware de comunicaciones. Acude después a la sede web de algún fabricante de routers para contrastar el documento que has leído con las especificaciones técnicas concretas de algún modelo de router. Te pueden servir las páginas <http://www.juniper.net/es/> o <http://www.cisco.com/web/ES/index.html>

- ¿Cuáles de las siguientes afirmaciones son verdaderas?
 - La distancia telemática al destino se mide con un parámetro que se denomina coste de la ruta.
 - RIPv1 está limitado a 15 saltos, sin embargo la versión RIPv2 supera esta limitación.
 - OSPF siempre envía el paquete por la ruta más corta según el número de saltos.
 - EIGRP es un protocolo de enrutamiento híbrido.

II. Gestionar un proxy web

- Ayudándote de Internet, responde:
 - ¿Cómo se debe configurar un cliente para que pueda utilizar un proxy transparente?
 - ¿Para qué utilizan los proveedores de Internet los proxies transparentes?

c) ¿Sabrías averiguar si tu proveedor de Internet te proporciona el servicio de acceso a través de un proxy transparente?

- Si resumimos los datos planteados en el Caso práctico 1, tenemos que un cliente de red tiene dirección IP 192.168.1.20/24 y su puerta por defecto es 192.168.1.254. El usuario presentado en ese cliente necesita navegar, pero 192.168.1.254 no tiene un proxy transparente y, por tanto, necesita configurar un servidor web proxy. La red tiene dos servidores proxy, uno para el protocolo ftp en la dirección 192.168.120.55 por el puerto 8008 y otro proxy para el resto de los protocolos en la dirección 192.168.1.101 en el puerto 8080.
 - Si habilitamos en 192.168.1.254 un proxy transparente de tipo web (solo http), ¿cómo sería la ficha de configuración del navegador?
 - Ahora en 192.168.201.254 habilitamos también la transparencia para el protocolo https, ¿cómo habría que configurar el proxy?
 - En el caso c), ¿qué puertos tendría que poner a la escucha el servidor proxy transparente en 192.168.1.254?

III. Diseñar y configurar un sistema de protección para la red local

- Imaginemos un nodo de la red local que no necesita conectarse a Internet más que para navegar por la web.
 - Si no puede acceder a un servidor proxy, ¿debe tener configurada al menos la puerta por defecto para poder navegar por la web?
 - ¿Y si tiene acceso a un servidor proxy que está en la red de área local?
 - ¿Y si tiene acceso a un servidor proxy que está en otra red?
- Conecta dos estaciones de trabajo en una misma red de modo que sus parámetros de red hagan sus comunicaciones totalmente compatibles.
 - Comprueba que desde cada estación puedes acceder a todos los servicios de la otra sin ninguna restricción. Por ejemplo, puedes habilitar servidores web y ftp locales para realizar estas pruebas.
 - Ahora cierra todas las comunicaciones en una de las estaciones y habilita el cortafuegos personal. Comprueba que ahora no puedes acceder a los servicios a los que antes tenías acceso.
- En <http://m0n0.ch> puedes encontrar el software y documentación técnica de m0n0wall, un *firewall* sobre Linux FreeBSD con muchas prestaciones. Lee la documentación técnica para instalar sobre una máquina un cortafuegos m0n0wall, configúralo para que sea útil en tu red y prueba su funcionamiento. Una alternativa muy interesante a m0n0wall es IPFire, que se puede descargar de <http://www.ipfire.org/>