Reference Guide

WinRoute Pro 4.1 SP

Para la estructura 22 de la versión 4,1 y más adelante

Tiny Software Inc.

Índice

LÉAME PRIMERO

Estimado cliente:

Le agradecemos la compra/evaluación de WinRoute Pro. Tiny Software, la compañía líder en la tecnología de cortafuegos para PYMES, no ha escatimado esfuerzos ni trabajo de investigación para poner a su disposición un potente enrutador/cortafuegos de fácil uso, diseñado para los sistemas operativos Windows.

WinRoute Pro es una aplicación de red que, junto con un PC, sustituye de forma muy eficiente enrutadores y cortafuegos basados en hardware de costes considerablemente más elevados. Como tal, requiere que la red sea instalada y configurada de la forma adecuada. Por ello, es necesario disponer de cierta experiencia en el ámbito de los entornos de red.

Por favor, tenga en cuenta que (según nuestras estadísticas) alrededor del 90% de los problemas que experimentan nuestros clientes al conectar sus redes a Internet, se deben a una configuración de red incorrecta. En este manual se incluyen varios ejemplos de configuraciones de red. No obstante, cada instalación puede ser diferente a las demás y tener características particulares.

Le recomendamos encarecidamente que lea detenidamente toda la documentación. La misma ha sido concebida presuponiendo que los usuarios cuentan ya con conocimientos básicos sobre redes y son capaces de instalar una red de área local (LAN).

Si después de leer la documentación precisa aún más recomendaciones, listas de control u otro tipo de información, Tiny Software le recomienda también que visite su sección de soporte en línea antes de ponerse en contacto con el departamento de Soporte Técnico.

Permítanos agradecerle una vez más por la compra/evaluación de WinRoute.

TINY SOFTWARE, INC.

CAPÍTULO 1

DESCRIPCIÓN DE WINROUTE

En Este Capítulo

Descripción breve de WinRoute

WinRoute Pro es el más innovador **enrutador - cortafuegos para Internet** que le permite instalar, prácticamente sin esfuerzo, todos los computadores de su red de forma que compartan una sola conexión a Internet. Puede conectarse a través de una línea dedicada, DSL, cable, RDSI, LAN, T1, radio o DirecPC. ¡Es así de fácil!

Administración Remota

WinRoute Administrator permite configurar y ajustar WinRoute Engine, el "motor" de WinRoute. WinRoute Administrator es una aplicación independiente (wradmin.exe) que puede ejecutarse desde cualquier computador con una conexión a WinRoute Engine. El acceso a Engine está protegido por una codificación de alto nivel y por contraseña.

Registro

WinRoute Pro pone a disposición del administrador el máximo control posible sobre el flujo de tráfico, a través del computador host en el que se está ejecutando. El administrador puede beneficiarse del análisis del flujo de paquetes TCP, UDP, ICMP y ARP, solicitudes DNS, información sobre controladores y sobre otros temas. Todas las operaciones tienen un sello de hora.

Enrutador NAT IP

WinRoute incluye la (mejor) implementación de la tecnología de traducción de dirección de red (Network Address Translation, NAT) disponible en la actualidad, y está diseñado para ofrecer a los usuarios la mejor capacidad de encaminamiento y protección de red posibles. El controlador NAT se ha escrito exclusivamente para WinRoute y ofrece una solución de seguridad comparable a la de otros productos más caros, pero a un coste muy inferior.

Encaminamiento NAT Avanzado

La facilidad NAT avanzada pone a disposición la opción de modificar la dirección IP de origen de los paquetes salientes en base a varios criterios. De esta forma se garantiza la integración sencilla de las LAN ubicadas detrás de WinRoute en el entorno WAN corporativo, con diferentes segmentos, zonas desmilitarizadas, redes privadas virtuales, etc.

Servidores host ubicados detrás de WinRoute

Para obtener el máximo nivel de seguridad posible, WinRoute cierra por defecto todos los puertos. Por ello, todas las solicitudes no iniciadas se deniegan, a menos que se cree un mapeo. Mediante la tecnología de mapeo de puerto los usuarios pueden decidir de qué forma desean desviar los paquetes IP que pasan a través de cualquier interfaz operada por WinRoute. Con WinRoute, los usuarios puede definir que los paquetes que entren a un puerto determinado sean transferidos a un computador interno específico. Así, puede operar de forma segura un servidor web, servidor de correo, servidor FTP, servidor VPN o cualquier otro tipo de servidor detrás del cortafuegos.

Seguridad de Cortafuegos

WinRoute pone a disposición de sus usuarios un nivel de capacidad de cortafuegos comparable al ofrecido por otras soluciones mucho más costosas, gracias a la combinación de su arquitectura NAT y su capacidad de operar a un nivel bajo. Por ello, WinRoute puede capturar tanto los paquetes entrantes como los salientes, ofreciendo así un nivel de seguridad prácticamente impenetrable. La facilidad de anti-interferencia es una facilidad adicional del filtro de paquetes de WinRoute, para aumentar la protección de la LAN contra los ataques en los que los intrusos falsifican direcciones IP de origen.

Configuración Sencilla de la Red

El servidor DHCP y el transmisor DNS incluidos en WinRoute Pro simplifican la administración de la configuración de la red. Ambos componentes son tecnologías probadas. El servidor DHCP de WinRoute puede sustituir fácilmente al servidor DHCP incluido en WindowsNT.

Servidor de Correo

El servidor de correo de WinRoute, que abarca compatibilidad SMTP/POP3, creación prácticamente ilimitada de alias y ordenación automática de correo, es extremamente versátil. Los usuarios pueden disponer de una o varias direcciones de correo electrónico y pueden trabajar eficientemente en grupos (por ejemplo, ventas, soporte, etc.), y cada grupo puede asignarse a más usuarios. Todas estas facilidades están disponibles independientemente del tipo de conexión a Internet utilizado.

Memoria Caché HTTP

La arquitectura de WinRoute incluye un innovador motor caché. A diferencia de los servidores proxy con funcionalidad caché, la memoria caché de WinRoute almacena los datos que pasan en un solo fichero de una longitud predefinida, en vez de usar un fichero individual para cada objeto. Esto permite ahorrar una cantidad considerable de espacio del disco que es ocupada por la memoria caché, especialmente en los entornos FAT16 (la mayoría de los entornos Windows95).

Amplio Soporte de Protocolos

WinRoute soporta todos los protocolos Internet estándar, inclusive:

IPSEC, H.323, NetMeeting, Net2Phone, WebPhone, UnixTalk, RealAudio, RealVideo, ICA, Winframe, IRC, FTP, HTTP, Telnet, PPTP, Traceroute, Ping, Year 2000, Aol, chargen, cuseeme, daytime, discard, dns, echo, finger, gopher, https, imap3, imap4, ipr, IPX overIP, netstat, nntp, ntp, ping, pop3, radius, wais, rcp, rlogin, rsh, smtp, snmp, ssl, ssh, systat, tacacs, uucpover IP, whois, xtacacs

Enrutador NAT

En Esta Sección

Introducción a NAT

NAT - Traducción de la Dirección de Red (Network Address Translation)

La traducción de la dirección de red o NAT es una de las facilidades de seguridad más potentes de WinRoute. NAT es un borrador de protocolo estándar de Internet para "ocultar" las direcciones de las redes privadas detrás de una sola dirección o de varias direcciones. Una versión de NAT denominada "IP Masquerading (mascarada IP)" ha gozado durante varios años de mucha popularidad entre los usuarios de Linux. WinRoute es uno de los pocos productos para la plataforma Windows que ofrece funcionalidad NAT al nivel de entrada.

NAT puede implementarse de muchas formas pero, básicamente, crea un rango de direcciones privado casi ilimitado para las redes internas que es "traducido" por WinRoute, de forma que las comunicaciones puedan transferirse a las redes públicas o entrar desde ellas sin revelar ninguna información sobre sistemas internos sensibles. Dado que se desconoce el rango de direcciones privado de la interfaz interna de los cortafuegos WinRoute, es prácticamente imposible atacar directamente a un sistema en la red interna protegida por NAT.

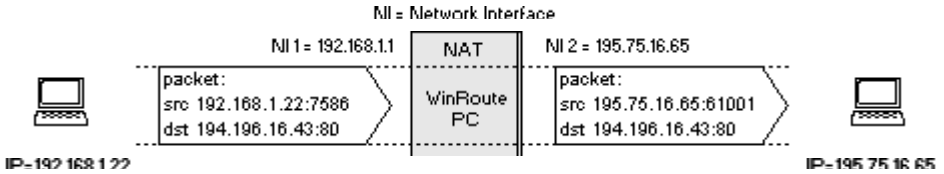
Funcionamiento de NAT

La Traducción de la Dirección de Red (Network Address Translation, NAT) es un proceso que modifica los paquetes transmitidos desde/hacia la red de área local hacia/desde Internet u otras redes basadas en IP.

Paquetes salientes

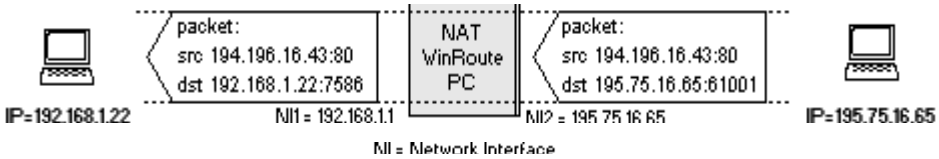
Los paquetes que pasan por el traductor de dirección **saliendo de** la LAN se cambian o traducen para que parezca que proceden del computador en el que se está ejecutando la NAT (ese computador está conectado directamente a Internet). Lo que realmente ocurre es que la dirección IP "origen" es cambiada en el encabezamiento y sustituida por la dirección IP (pública) del computador "NAT".

El motor NAT también crea una tabla de registros que contiene información sobre cada paquete que ha pasado hacia Internet.



Paquetes entrantes
Los paquetes que pasan por NAT **para entrar en** la LAN se comparan con los registros almacenados por el motor NAT. Después, la dirección IP de "destino" se sustituye (en base a los registros de la base de datos) nuevamente por la dirección IP específica de la clase privada interna, para que acceda al computador respectivo en la LAN .

Recuerde que, originalmente, el paquete llegó con la dirección IP pública del computador NAT como su dirección de "destino". El motor NAT tuvo que cambiar esa información para entregar el paquete al receptor correcto dentro de la red local.



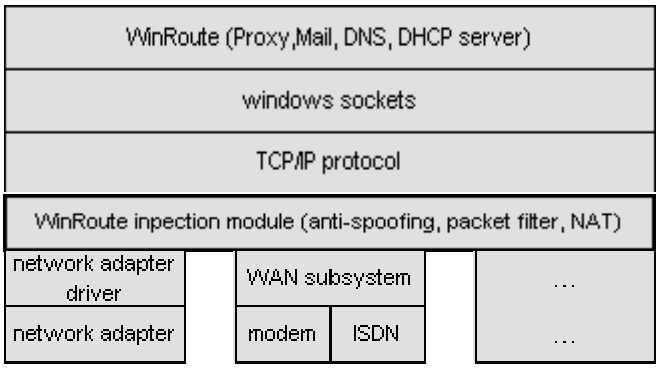
Arquitectura de WinRoute

Arquitectura de WinRoute

Para la interconexión de redes avanzada, es de utilidad comprender cómo funciona WinRoute. De la explicación y los ejemplos siguientes se desprende que WinRoute es una excelente solución para casi cualquier configuración de red.

1. **Seguridad Total**
   WinRoute trabaja **debajo de la pila TCP** al nivel IPSEC. En otras palabras, captura tanto los paquetes **salientes** como los **entrantes ANTES** de que puedan entrar en su computador.

Gracias a este diseño avanzado, el marco de seguridad ofrecido por WinRoute es prácticamente **impenetrable**



2. **Soporte Total de Protocolos**
   WinRoute es un ENRUTADOR de software. Como tal, y a diferencia de servidores Proxy como WinGate o WinProxy, WinRoute puede permitir el paso de casi cualquier protocolo Internet. Al mismo tiempo, WinRoute comprueba cada paquete utilizando la seguridad avanzada y las facilidades de cortafuegos inherentes al diseño del software. En los sistemas que emplean Windows 95 y 98, WinRoute gestiona el encaminamiento de paquetes. En los sistemas que emplean Windows NT, el sistema operativo NT ejecuta el encaminamiento y WinRoute administra la funcionalidad NAT y otros datos más.

3. **Flexibilidad Total**
   WinRoute ejecuta la NAT (traducción de la dirección de red) en las interfaces que usted elija. WinRoute ejecuta también cualquier regla de seguridad preestablecida en las interfaces específicas. De esta manera, el usuario dispone de una gran libertad al diseñar y configurar las opciones de seguridad.

Activar NAT en ambas interfaces

Es posible que sólo desee utilizar WinRoute como el **enrutador de acceso neutral** para el tráfico (paquetes) que llega desde **Internet** hacia una **red local**. En ese caso, ya dispondrá de una solución para el acceso compartido a Internet. Si esa solución no le permite correr en su red privada servidores y aplicaciones a los que se debe poder acceder desde Internet, entonces WinRoute puede ser la solución correcta para esa configuración específica.

Algunos ejemplos de servicios a los que puede desear que se acceda desde Internet son:

- servidor telnet (p. ej., AS400)
- servidor WWW
- servidor de correo
- PC Anywhere
- servidor FTP
- … y cualquier otro servidor (servicio) accesible en un puerto determinado.

WinRoute pondrá a disposición de sus usuarios/clientes un acceso fiable y seguro a esos servicios. La configuración de WinRoute para los servicios indicados arriba se describe en otros capítulos. Debe realizar los siguientes ajustes de formas diferentes:

Facilidad	Recomendado Originalmente	En este escenario
NAT en interfaz Internet	ACTIVADA	ACTIVADA
NAT en interfaz interna (LAN)	DESACTIVADA	ACTIVADA
Dirección IP de interfaz interna de WinRoute como pasarela por defecto para los demás computadores de la red	SI (NECESARIO)	NO (no necesario)

En otras palabras - mediante WinRoute puede disponer que sea posible acceder a determinados servicios desde Internet SIN necesidad de cambiar la configuración de la red.

- ***¡Nota! ¡Si activa NAT en ambas interfaces, NO podrá utilizar WinRoute para el acceso compartido a Internet!***

En el presente ejemplo, los ajustes por defecto de la pasarela le ofrecen muchas posibilidades. Puede mantener todo su entorno existente sin modificarlo. Para mantener en funcionamiento los enrutadores y las rutas ya establecidas en su red, puede agregar nuevos computadores en los que se ejecute WinRoute, de forma que los usuarios externos accedan a los servidores ubicados en su red local.

Esto es de gran utilidad (por ejemplo) cuando dispone de una WAN existente y desea permitir a los usuarios externos el acceso a su AS400 (servidor telnet) o el acceso a su red interna a través de PPTP.

Para ello, debe seguir los siguientes pasos:

1. Conecte a su red un computador con dos interfaces. Una interfaz (externa) funcionará como conexión a Internet, mientras que la otra (interna) funcionará como conexión a su red existente.
2. Asigne a la interfaz externa la dirección IP que se utilizará para acceder a los servicios/servidores que deben ser accesibles desde Internet.

3. Asigne la dirección IP interna o bien manualmente o bien mediante el servidor DHCP
4. Configure WinRoute para que ejecute NAT en ambas interfaces
5. Active el mapeo de puerto para los servicios que desee ejecutar dentro de su red

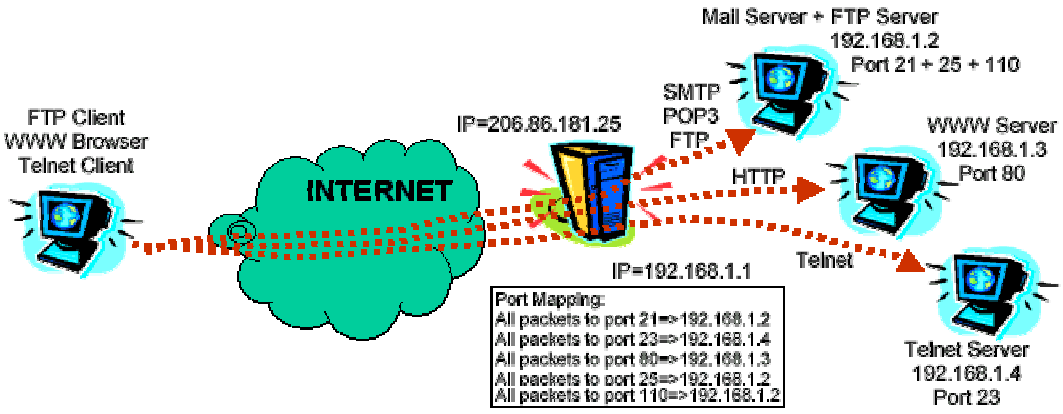
Una vez realizados estos ajustes, los usuarios externos podrán acceder desde Internet a los servicios internos que se están ejecutando en puertos específicos. La seguridad de dichos accesos está garantizada por el cortafuegos de WinRoute.

Mapeo de Puerto - Transmisión de Paquetes

WinRoute ejecuta la facilidad NAT, que impide el acceso externo a la red protegida. Mediante el mapeo de puerto (o traducción de la dirección de puerto, Port Address Translation - PAT) se puede permitir el acceso desde Internet a los servicios públicos como, p. ej., un servidor WWW o un servidor FTP, y a otros servicios más que se ejecuten en su red privada.

Funcionamiento del Mapeo de Puerto

Se comprueba para cada paquete recibido desde fuera de la red (desde Internet), si sus atributos (es decir, protocolo, puerto de destino y dirección IP de destino) coinciden con una entrada en la tabla de mapeo de puerto (protocolo, puerto de escucha, IP de escucha). Cuando el paquete entrante cumple los criterios deseados, es modificado y transmitido a la dirección IP de la red protegida, definida como la "IP de Destino" en la entrada de la tabla, y al puerto definido como "Puerto de Destino".

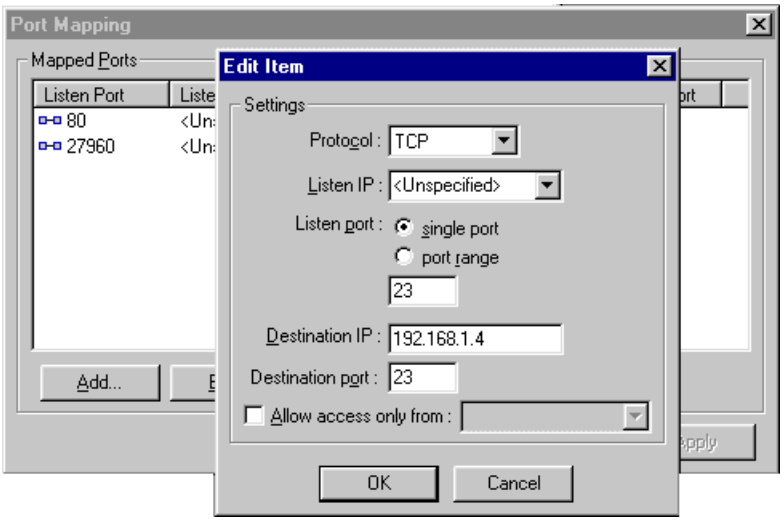


Por ejemplo, supongamos que corre un servidor web con la dirección IP interna 192.168.1.3 y que desea permitir que los usuarios de Internet tengan acceso a él. Las solicitudes de los usuarios de Internet llegarán a su computador WinRoute, que tiene una dirección IP externa equivalente al registro DNS de su servidor web www.sudominio.com. Dado que todas las solicitudes dirigidas al servidor web entran por el puerto 80, usted configurará el mapeo de puerto definiendo que toda la comunicación TCP del puerto 80 sea desviada a la dirección IP interna 192.168.1.3.

Configuración del Mapeo de Puerto

Para establecer el mapeo de puerto

1. Seleccione el menú *Configuración->Avanzada->Mapeo de Puerto*
2. Agregue un nuevo mapeo de puerto:



Protocolo

Seleccione el protocolo utilizado por la aplicación/servicio. Algunas aplicaciones/servicios usan los protocolos TCP y UDP juntos. Por ejemplo, el módulo WinRoute Administrator

IP de Escucha

La dirección IP a la que llegan los paquetes entrantes. Generalmente, es la dirección IP asociada con su interfaz de Internet. Nota: puede haber más de una dirección IP asociada con la interfaz (si dispone de más servidores web, etc.)

Puerto de Escucha

El número de puerto al que llegan los paquetes.

IP de Destino

La dirección IP dentro de su red local en la que funciona el servidor (servicio) que contesta los paquetes entrantes (servidor web, servidor FTP, etc.)

Puerto de Destino

El puerto usado por la aplicación de destino para la escucha. Típicamente, el mismo número que el del puerto de escucha

Sólo Permitir Acceso Desde

Puede especificar la dirección IP desde la cual desea permitir el acceso. Esto es muy importante para aumentar el nivel de seguridad en caso que active el mapeo de puerto para aplicaciones de administración remota, tales como WinRoute Administrator, PC Anywhere, etc. También puede especificar un grupo de direcciones IP. Para ello, debe crear primero un grupo en el cuadro de diálogo "Grupos de Direcciones".

Mapeo de Puerto para Sistemas con Alojamiento Múltiple (más direcciones IP)

Es posible que disponga de más direcciones IP asignadas a la interfaz de Internet, y que dentro de su red funcionen varios servicios a los que se debe poder acceder desde Internet.

Escenario con 5 servidores WWW

A manera de ejemplo, supongamos que desee operar 5 servidores web y que cada uno de ellos tenga un dominio independiente asociado con direcciones IP diferentes.

En un escenario tal, usted podría asignar 5 direcciones IP a su interfaz externa (que conecta a Internet) y operar los servidores web en otros computadores dentro de su red.

Cada servidor web puede correr sobre un computador independiente, o usted puede asignar más direcciones IP a un computador de su red interna y correr todos los servidores web sobre ese computador.

A continuación, debería definir 5 mapeos de puerto en un diálogo de Mapeo de Puerto. Para cada servidor web (dominio) debería definir:

- Dirección IP de escucha (dirección IP pública asociada con el dominio).
- Puerto de escucha: en nuestro escenario, el puerto 80
- Dirección IP de destino: la dirección IP en la que funciona el servidor web
- Puerto de destino: 80 (para www)

Para más ejemplos sobre el Mapeo de Puerto Avanzado, vea el capítulo (Inter)Conexión de Redes Avanzada.

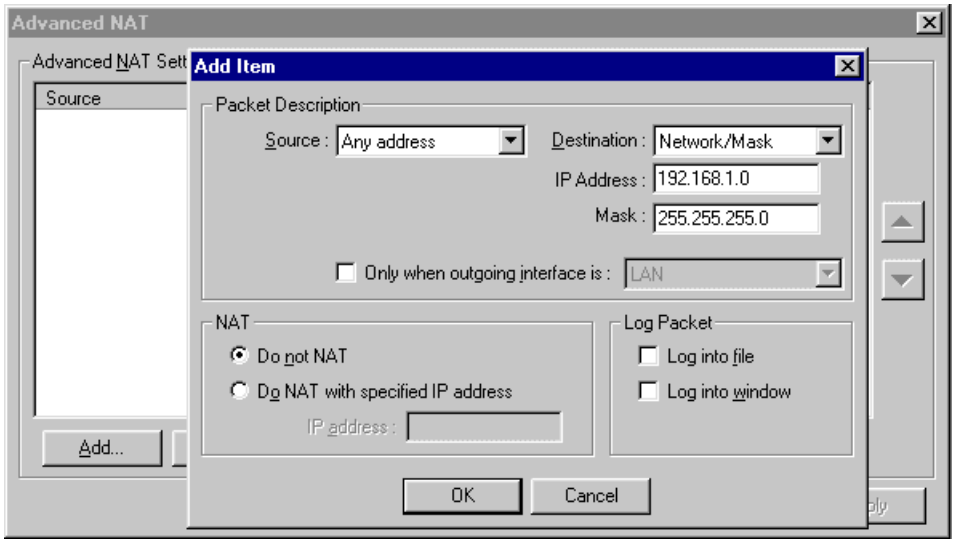
NAT Múltiple

WinRoute permite tanto la **NAT** (traducción de la dirección de red) sencilla, como también otras configuraciones más complejas. Puede especificar, en base a la dirección IP de **origen** o de **destino** del paquete, si NAT debe ejecutarse también para **otras direcciones IP** (es decir, los paquetes aparentan provenir de otra dirección IP) o si **NAT** no debe ejecutarse en absoluto.

Estos ajustes son muy importantes cuando existen configuraciones de redes más complejas, en las cuales:

- determinados computadores deben aparentar que disponen de una dirección IP **diferente a** la dirección IP principal usada por el **resto** de la red
- existen sucursales conectadas a la **WAN** con rangos de direcciones privados, y desea compartir **un** acceso a Internet para todas ellas
- dispone de varios segmentos detrás de WinRoute y uno (o varios) de ellos es una zona DMZ con una dirección IP pública
- desea tener direcciones IP públicas dentro de su red privada (recuerde: póngase en contacto con su ISP (proveedor de servicio) y cerciórese de que esas direcciones IP deben encaminarse a través de su dirección IP principal.)

Encontrará numerosos ejemplos de "Configuración NAT Avanzada" en el capítulo (Inter)Conexión de Redes Avanzada.



Dirección IP de Origen, Dirección IP de Destino

Puede realizar una configuración NAT avanzada basándose en la dirección IP desde la que se transmite (origen) o hacia la que se transmite (destino). Puede introducir como origen la dirección IP Host, la red entera (limitada por la máscara de red) o el grupo de direcciones IP creado previamente en el menú Configuración->Avanzada->Grupos de Direcciones.

No ejecutar NAT

Cuando selecciona esta opción, los paquetes que pasan a través de la interfaz de Internet no se modifican

Ejecutar NAT con Dirección IP Especificada

Cuando selecciona esta opción, los paquetes que pasan se modifican para que parezca que provienen de la dirección IP deseada.

Tabla de Interfaces

La tabla de interfaces es un diálogo en el que WinRoute visualiza todas las interfaces disponibles que ha podido detectar en el computador. Si dispone de más interfaces que los visualizados por WinRoute, es probable que el controlador de dicha(s) interfaz(ces) no haya sido cargado correctamente por el sistema operativo y que, por tanto, WinRoute no haya podido leerlo.

Puede ver lo siguiente:

Nombre de la Interfaz

Puede cambiar el nombre seleccionando “Propiedades” y cambiando el nombre.

Dirección IP

El valor establecido en las propiedades TCP/IP de la interfaz. Si se ha configurado a la interfaz para que reciba la dirección IP del servidor DHCP, verá la dirección IP actual asignada a la interfaz.

NAT “Activada” o “Desactivada”

Cuando NAT se ha configurado para ser ejecutada en la interfaz, se visualizará “Activada” en esta columna

Soporte VPN

Como se mencionó anteriormente, WinRoute dispone de la capacidad completa para pasar el tráfico de los dos protocolos de red privada virtual (VPN) más populares que se utilizan en la actualidad: el protocolo de seguridad IP (IP Security protocol, IPSec) propuesto por IETF, y el protocolo de túnel punto a punto, que se ha popularizado en los últimos años debido a su inclusión en el software del sistema operativo cliente Windows de Microsoft.

Cortafuegos de Filtro de Paquetes

En Esta Sección

Vista de Conjunto del Filtro de Paquetes

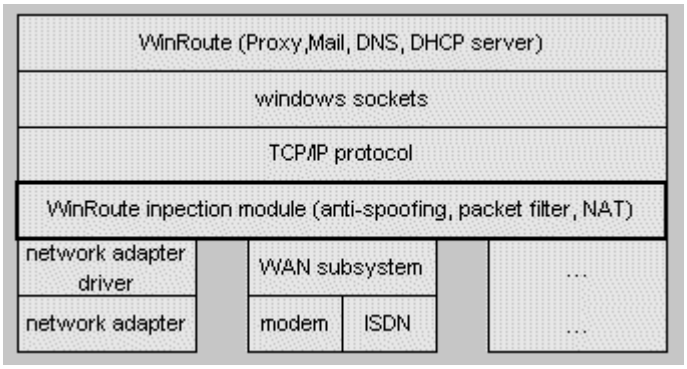
El núcleo de cualquier mecanismo de control de accesos tipo cortafuegos es, naturalmente, la tecnología mediante la cual se permite o se deniega el acceso de los paquetes dirigidos a la red protegida. WinRoute implementa una de las tecnologías más usadas para el control de accesos a la red: el filtro de paquetes. Aunque WinRoute también implementa otros mecanismos de control de accesos, tales como servidor proxy de caching para los protocolos HTTP, FTP y Gopher, esto está concebido, básicamente, como un elemento para aumentar el rendimiento de salida, y no como una facilidad de seguridad.

El filtro de paquetes tiene una larga tradición en el ámbito de la seguridad y todavía está implementado en muchos productos como, p. ej., el sistema operativo de dispositivos de redes IOS de Cisco. Cuando se configuran correctamente, los filtros de paquetes pueden ofrecer un alto nivel de seguridad y son especialmente adecuados para los sitios de Internet con un alto volumen de tráfico, ya que ofrecen el mejor rendimiento.

Arquitectura

Los cortafuegos se construyen, típicamente, sobre plataformas protegidas y, normalmente, es muy difícil burlar este tipo de software. No obstante, un punto débil importante en muchos dispositivos de seguridad de red se produce en el breve intervalo de tiempo que se inicia en el momento en que el hardware es activamente capaz de encaminar el tráfico y termina cuando el software asume el control de las interfaces de la red. Dentro de esta confluencia crítica, la seguridad puede verse seriamente comprometida.

El controlador, o motor, de WinRoute se activa cuando los ficheros núcleo del sistema operativo Windows (el kernel) se cargan a sí mismos en la memoria; más específicamente, antes de que se carguen los módulos NDIS (especificación de interfaz de dispositivo de red, Network Device Interface Specification), de forma que no se soporta ningún tipo de conectividad de red antes de que WinRoute esté activado. Así, la protección de todas las interfaces está activada antes que el tráfico malicioso u otros ataques puedan montarse en el sistema. De esta manera se obtiene una mejor protección que la ofrecida por productos autónomos del tipo detección de intrusión, que se ejecutan como servicio y no están activados sino después de que se ha inicializado el sistema.



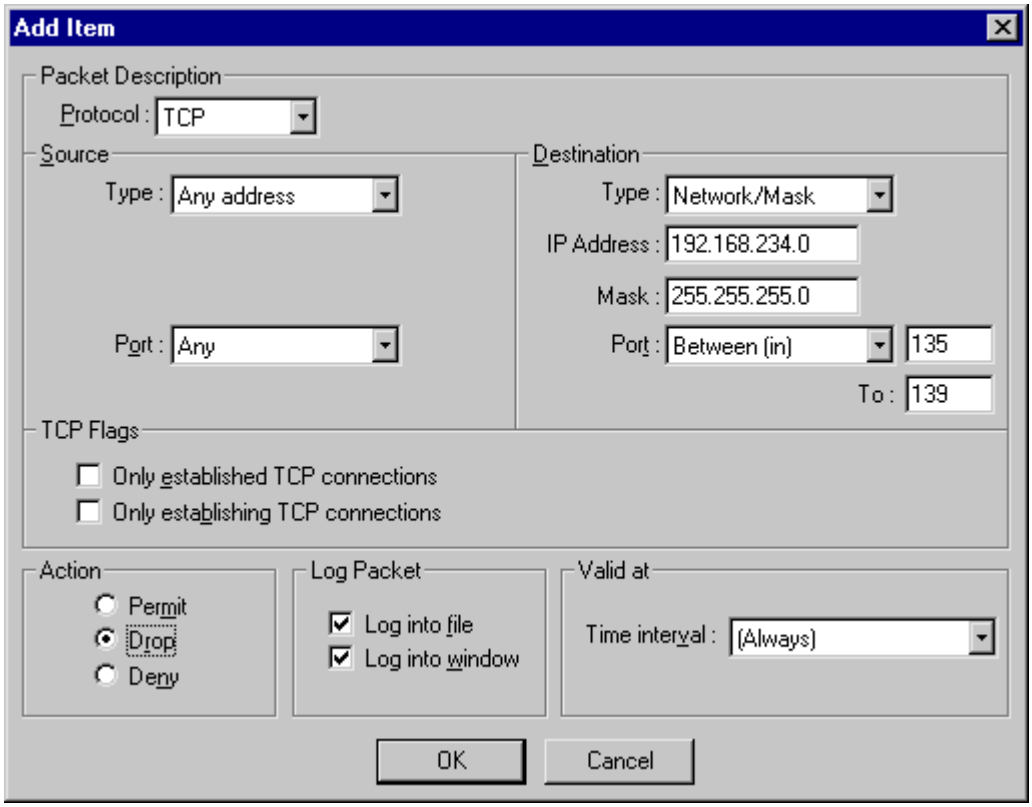
WinRoute "viola" a NDIS de una forma propietaria, de forma que todo el tráfico TCP/IP sea impulsado por el controlador de la tarjeta de interfaz de red (network interface card, NIC) al motor de WinRoute antes de que prosiga a la pila de comunicaciones de la red y al propio sistema operativo.

Mediante esta inserción a bajo nivel en el sistema operativo, WinRoute Engine controla, desde una perspectiva singular, todo el tráfico que llegue a cualquier interfaz (sea éste entrante o saliente). Al igual que muchos productos cortafuegos diseñados para empresas como, p. ej., Firewall-1 de Check Point, WinRoute puede tomar la primera decisión referente a la aceptación o denegación de un paquete determinado. Una vez más, se evitan de esta forma los ataques maliciosos contra otros aspectos del sistema operativo, o los de otro software que pudiera burlar la seguridad ofrecida por un cortafuegos. Esto resulta muy apropiado para las pasarelas de Internet de cara al exterior, pero también puede aportar considerables beneficios a los computadores host autónomos con altos requerimientos de seguridad o que deban ser totalmente anónimos y que dispongan, por ejemplo, de sistemas de detección de intrusión. El software de detección de intrusión, como el Real Secure de Internet Security Systems (ISS), sería prácticamente invisible en un computador host protegido por WinRoute.

Además, el controlador WinRoute Engine asume toda la funcionalidad de encaminamiento de comunicaciones del sistema operativo Windows subyacente (ya sea éste Windows 9x, NT, o 2000). De esta manera se garantiza que si WinRoute Engine fallara por algún motivo, no se encamine ningún tipo de tráfico entre las redes. Esta postura de "cerrado si falla" ha sido el ajuste por defecto tradicional para las configuraciones de cortafuegos durante varios años, y sirve para proteger las redes privadas en los casos de fallas comunes del sistema.

Reglas

A pesar de las discusiones teóricas actuales sobre el filtro de paquetes, el punto principal que hace que los sistemas cortafuegos modernos fallen es la configuración incorrecta, especialmente en el caso de administradores inexpertos. WinRoute convierte la configuración de los filtros en una tarea sencilla y lo suficientemente flexible como para que incluso los administradores de red novatos puedan implementar una configuración segura. Para ello, bastan algunos conocimientos de TCP/IP y unos pocos clic del ratón, como se ilustra en la captura de pantalla siguiente.



Las reglas de filtro pueden aplicarse interfaz por interfaz a todas las siguientes entidades:

- una dirección IP individual
- una lista de direcciones IP definidas por el administrador
- una red o una subred entera

También es importante tener en cuenta aquí que los filtros pueden activarse tanto para el tráfico entrante como para el saliente.

Estas capacidades permiten adaptar minuciosamente las reglas de acceso para que cubran las necesidades de seguridad específicas de casi cualquier organización. Por ejemplo, se podría permitir el acceso de un grupo de desarrolladores web a recursos externos específicos, tales como servidores FTP anónimos de activación, o se puede definir que redes asociadas externas tengan acceso a una lista de direcciones internas específica para depositar ficheros electrónicos. La configuración entrante/saliente hace posible la protección contra ataques maliciosos "de adentro hacia afuera", como Back Orifice (BO), o servlets de denegación de servicio distribuida (distributed denial of service, DDOS), que intentan comunicarse con atacantes externos a través de protocolos no fiables pasando por el cortafuegos.

Las reglas pueden permitir, truncar o denegar el tráfico especificado; la acción "Soltar" proporciona a los potenciales atacantes la menor cantidad de información posible sobre el cortafuegos, ya que no transmite ninguna respuesta ICMP Filtro Prohibido Administrativamente ni TCP Reponer/Confirmar para un paquete de sincronización TCP SYN (el 1er. paso en la secuencia estándar de intercambio de indicativos de control TCP de tres vías).

Las reglas se pueden priorizar para que actúen en un orden específico, definido por el usuario, frente a los paquetes entrantes o salientes. El uso más popular de esta capacidad es agregar así denominadas "reglas de limpieza" a las listas de filtro, que bloquean todo el tráfico no permitido específicamente por las reglas anteriores con una mayor prioridad en la lista (para un ejemplo de una regla de limpieza, vea los conjuntos de Ejemplos de Reglas de Filtro de Paquetes Básicas más adelante en este documento).

Protocolos

Los protocolos soportados por los filtros de paquetes de WinRoute incluyen:

- IP en bruto
- siete tipos ICMP (o Todos)
- TCP
- UDP
- PPTP.

La capacidad de permitir o bloquear tipos ICMP específicos en bruto o protocolos IP en bruto es invalorable para los administradores de red, los mismos que se ven confrontados con una lista de requerimientos de las aplicaciones a soportar que no deja de crecer. En particular, los protocolos VPN relativamente nuevos, tales como el IPSec, viajan a través de protocolos IP en bruto 51 y 52, y sería imposible filtrarlos con algunos cortafuegos más limitados disponibles actualmente en el mercado, que sólo pueden controlar protocolos basados en TCP o UDP.

Anti-Interferencia

Adicionalmente, WinRoute pone a disposición capacidades anti-interferencia, que evitan que los paquetes con direcciones de origen inválidas se originen dentro de la red. La facilidad de anti-interferencia podría haber evitado los ataques ICMP smurf notificados en febrero del 2000, realizados como ataques de denegación de servicio distribuida, que afectaron a sitios web de grandes dimensiones como Yahoo y Buy.com. Los usuarios de WinRoute pueden dormir tranquilos sabiendo que sus redes no serán presa de este tipo de ataques, si implementan esta facilidad.

Registros y análisis de paquetes

En Esta Sección

Acerca de registros y análisis

Una función crítica de cualquier producto de seguridad es su capacidad de registrar eventos en todo momento y de una forma suficientemente detallada. WinRoute graba seis registros diferentes del tráfico que impacta al cortafuegos, inclusive los paquetes que pasan por él, las actividades de los usuarios, acciones de filtro, etc. En la siguiente tabla se ofrece una descripción de cada registro:

Registro HTTP	Sólo muestra los datos HTTP que pasan a través del servidor Proxy de WinRoute; incluye la dirección IP de origen y el nombre del usuario, el sello de hora y las peticiones y respuestas HTTP
Registro de Correo	Registra todas las operaciones del servidor de correo integrado de WinRoute; registra las actividades de transmisión/recepción SMTP y POP3
Registro de Seguridad	Muestra todas las actividades definidas como "Registrar en ventana/fichero" en las reglas de filtro de paquetes (ver abajo para una descripción detallada de los elementos registrados)
Registro de Marcación	Registra información del uso de las interfaces de marcación supervisadas por WinRoute
Registro de Depuración	Configuración personalizada para registrar todos los paquetes ARP, ICMP, UDP, TCP, y/o DNS que pasan físicamente por cualquier interfaz del enrutador WinRoute; se dispone de una configuración minuciosa bajo Configuración | Avanzada | Info Depuración, pestaña Depurar.
Registro de Errores	Muestra todas las operaciones infructuosas que ocurren en cualquier módulo WinRoute en ejecución

Los registros pueden visualizarse en la consola de WinRoute Administrator, escribirse en un fichero, o ambas cosas. Los ficheros de registro se guardan en \%raíz de instalación%\Registros, y sólo se puede acceder a ellos a través de las cuentas NT/2000 de administrador, operador de servidor, SISTEMA y CREADOR PROPIETARIO de la persona que instale WinRoute.

La información del registro grabada por el Registro de Seguridad de WinRoute es fiable, e incluye toda la información necesaria para iniciar una investigación adecuada sobre actividades potencialmente maliciosas:

- Fecha
- Hora
- Regla de filtro de paquetes afectada
- Interfaz
- Acción (Permitir, Soltar, Denegar)
- Protocolo
- Dirección IP de origen y puerto TCP
- Dirección IP de destino y puerto TCP

Las pruebas bajo condiciones de tráfico adversas no afectan la capacidad de registro de WinRoute. Este es un punto crítico para evitar la pérdida de valiosos datos forenses, así como para aliviar una potencial situación de denegación de servicio en la que la funcionalidad de cortafuegos se desactiva cuando el sistema de registro no es capaz de hacer frente al volumen de tráfico.

Registro de Depuración

El **Registro de depuración** es el registro más importante de WinRoute, ya que le permite ver **todos los paquetes IP** (TCP, UDP, ICMP, ARP, DNS) que pasan físicamente por cualquiera de las interfaces del computador WinRoute.

En la ventana **Eventos de depuración** puede ver el conjunto de eventos que puede visualizar.

¿Cómo se lee el registro?

De izquierda a derecha, puede ver lo siguiente:

Sello de hora - se muestran la fecha y la hora exactas en las que ocurrió el evento o en las que el paquete pasó por la interfaz.

El protocolo - el tipo de protocolo del paquete

De/A nombre de la interfaz - el nombre de la interfaz, y si el paquete se dirigió **A** la interfaz o proviene **De** la interfaz (imagínese que WinRoute se esté ejecutando en el PC y las interfaces sean las "pasarelas" entre el computador y la red).

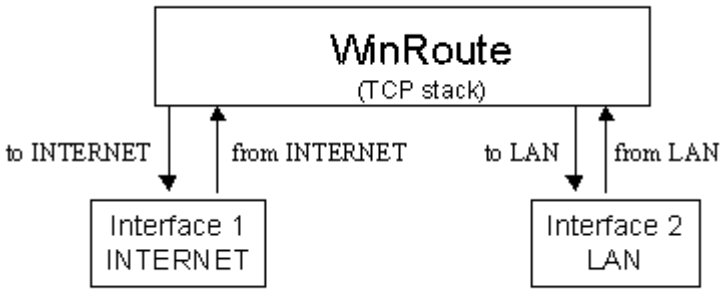
Dirección IP de Origen ->de Destino - las direcciones IP de origen y de destino que se encuentren en el paquete.

Las banderas - identificación adicional sobre la acción.

Ejemplo:

```
[10/Nov/1999 09:32:38] TCP: paquete 511464, de lan,
longitud 1514, 192.168.1.7:2442 -> 192.168.1.1:25,
banderas: ACK

[10/Nov/1999 09:32:38] TCP: paquete 511465, a lan,
longitud 54, 192.168.1.1:25 -> 192.168.1.7:2442,
banderas: ACK
```


WinRoute
(TCP stack)
to INTERNET
from INTERNET
to LAN
from LAN
Interface 1
INTERNET
Interface 2
LAN

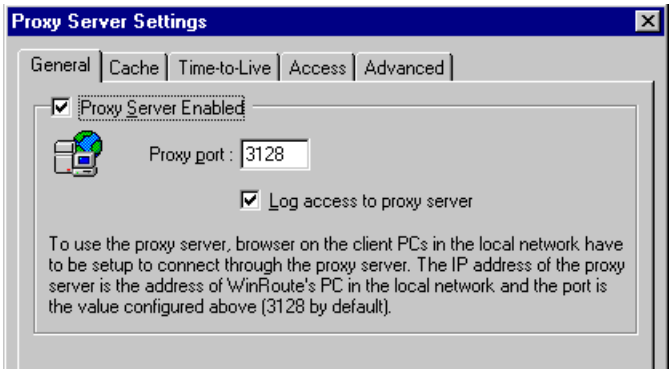
Registro HTTP (Proxy)

El registro HTTP (Proxy) es una potente herramienta que le ayuda a seguir las actividades de los usuarios en Internet. Este registro pone a disposición información menos detallada sobre los usuarios que acceden a la web, que la que se obtiene del registro de Depuración.

¿Cómo funciona este registro?

El registro HTTP (Proxy) sólo visualiza los datos que pasan por el servidor Proxy de WinRoute. Esto significa que si desea obtener datos del servidor Proxy, debería forzar a los usuarios a pasar por ese servidor. Vea los capítulos Ejemplos de Cortafuegos o Servidor Proxy.

Además, debe habilitar el acceso del registro a la configuración del Servidor Proxy.



¿Cómo se lee el registro HTTP (Proxy)?

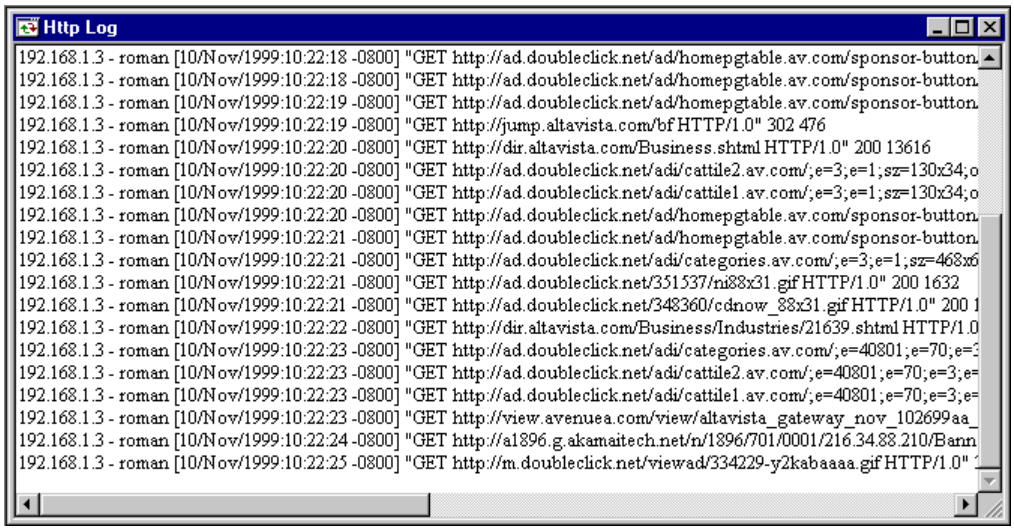
```
192.168.1.3 - roman [10/Nov/1999:10:22:20 -0800] "GET
http://dir.altavista.com/Business.shtml HTTP/1.0" 200
13616
```

De izquierda a derecha:

Dirección IP - nombre - el nombre y la dirección IP actuales del usuario que accede a Internet

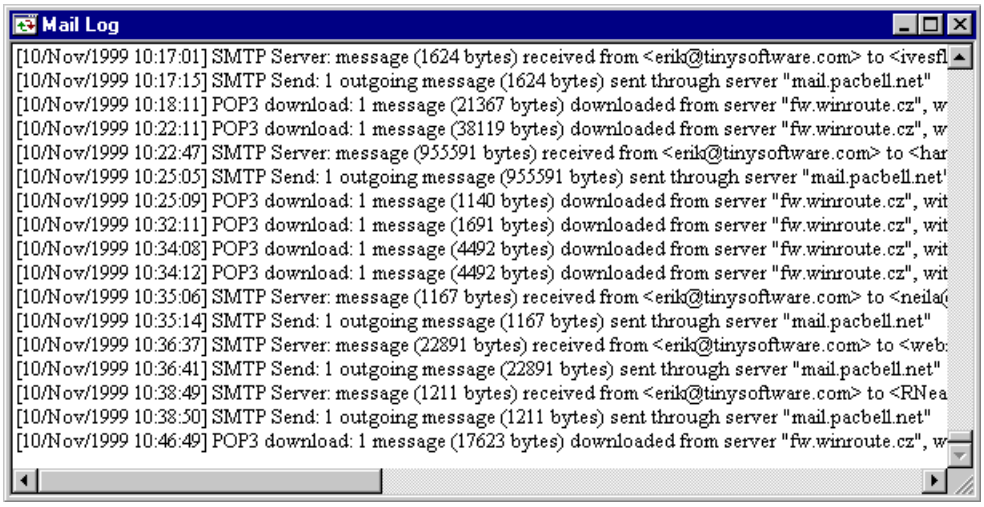
Sello de hora - la fecha y la hora del acceso

GET "http..." - el destino del acceso



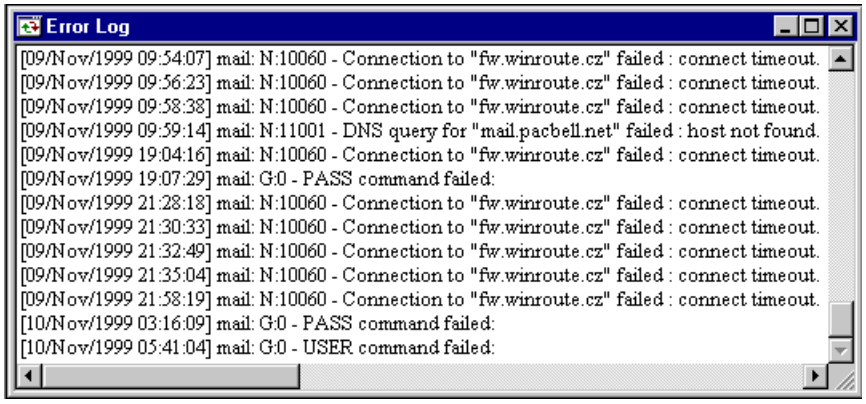
Registro de Correo

En el Registro de Correo se graban todas las operaciones del servidor de correo integrado en WinRoute. Puede ver incluso cuántos mensajes se han transmitido y recibido, a dónde se han transmitido los mensajes, etc. Todas las operaciones tienen un sello de hora.



Registro de Errores

En el Registro de Errores se visualizan todas las operaciones infructuosas realizadas en los módulos activados de WinRoute. Como resultado puede ver los errores en el intercambio de correo, el servidor DNS, etc.



Servidor DHCP

En Esta Sección

Vista de Conjunto DHCP

En una red, cada computador debe tener su propio protocolo TCP/IP debidamente configurado. Esto significa que la dirección IP, la máscara de red, la dirección de la pasarela por defecto, la dirección del servidor DNS, etc., deben configurarse en cada computador. Cuando la persona encargada del mantenimiento debe configurar los parámetros manualmente en numerosas estaciones de trabajo, es difícil evitar que se produzcan errores como, p. ej., utilizar una dirección dos veces - lo que podría provocar colisiones y, por consecuencia, el funcionamiento incorrecto de la red completa.

El protocolo de configuración host dinámica (Dynamic Host Configuration Protocol, DHCP) es una implementación de WinRoute diseñada para simplificar la tarea de administración de la red. DHCP se utiliza para realizar una configuración dinámica del protocolo TCP/IP en los computadores. Durante el arranque, el computador DHCP cliente transmite una petición. Cuando el servidor DHCP recibe la petición, selecciona los parámetros de configuración TCP/IP para el cliente. Los parámetros son la dirección IP, la máscara de red, la pasarela por defecto, la dirección del servidor DNS, el nombre de dominio del cliente, etc. Con esos parámetros, el servidor crea una respuesta y la transmite al cliente.

El servidor puede asignar una configuración al cliente sólo por un periodo de tiempo limitado (el así denominado tiempo de alquiler, lease time). El servidor siempre asigna la dirección IP de forma que no coincida y, por tanto, no colisione con ninguna otra dirección asignada a través de DHCP a otro cliente.

Cuando se dispone de un servidor DHCP, se cumple la premisa para habilitar la opción "Obtener dirección IP del servidor DHCP" y el servidor DHCP asume entonces la responsabilidad por la configuración adecuada de TCP/IP en las estaciones de trabajo. Esto puede contribuir a reducir considerablemente los costes de mantenimiento y gestión de la red.

- ***Cuando algunos de los computadores de su red no sean configurados dinámicamente por DHCP, sino que tengan una configuración fija, debe cerciorarse de que los parámetros utilizados por DHCP no colisionen con los usados en las configuraciones fijas.***

Transmisor DNS

En Esta Sección

Acerca de la Transmisión DNS

Cada computador conectado a Internet es identificado mediante una dirección IP numérica única. Para poder establecer una comunicación con un computador conectado a Internet, es necesario que el computador que establece la conexión conozca la dirección del otro computador. Dado que no es fácil recordar las direcciones IP, se creó el servicio de nombre de dominio (Domain Name Service, DNS).

El DNS es una base de datos que contiene nombres descriptivos, que son más fáciles de recordar. Entonces, el usuario no necesita conocer la dirección IP del servidor con el que desea comunicarse, sino que basta con que introduzca el nombre correspondiente (p. ej., www.yahoo.com) para que DNS se encargue de buscar la dirección IP real.

Transmisor DNS en WinRoute

WinRoute está equipado con un módulo DNS capaz de transmitir peticiones DNS a un servidor DNS elegido en Internet. El módulo DNS almacena los resultados de las peticiones en su memoria caché interna, en la que permanecen durante un periodo de tiempo determinado. Las peticiones subsiguientes que se repiten se contestan entonces utilizando los datos guardados en la memoria caché, sin que sea necesario esperar hasta que llegue una respuesta desde Internet.

El transmisor DNS de WinRoute puede contestar las peticiones DNS basándose en el fichero HOSTS definido por el usuario. Una vez que llega una petición DNS, WinRoute busca primero en el fichero HOSTS antes de transmitir la petición DNS a Internet. Si se encuentra el registro correspondiente, la petición se contesta mediante ese valor. En caso contrario, la petición es transmitida al servidor DNS de Internet.

Servidor Proxy

En Esta Sección

Vista de Conjunto Proxy

La **finalidad principal** de un servidor proxy es **ahorrar ancho de banda** en su conexión a Internet. Cuando los usuarios acceden a Internet a través de un proxy, el servidor proxy **almacena** los diferentes objetos solicitados que pasan por él (como páginas HTML, imágenes y otros tipos de ficheros) en su **memoria caché**.

Cuando las páginas o imágenes son solicitadas nuevamente por el mismo usuario o por otra persona, el servidor proxy pone a disposición, desde su memoria caché, los elementos solicitados . De esta forma se **reduce** la carga de la conexión a Internet y la operación completa es también más rápida que si se descargan nuevamente las imágenes desde Internet.

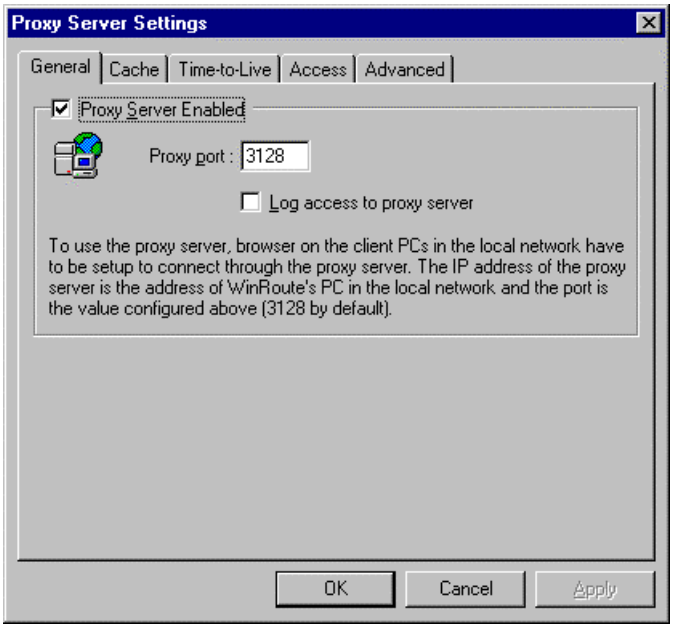
Por otra parte, los objetos guardados en la memoria caché de un servidor proxy no están siempre actualizados. La definición del tiempo de vida (**TTL** ,Time-To-Live) de los documentos guardados es una cuestión muy delicada y debe definirse de forma equilibrada para evitar malentendidos que pueden surgir, por ejemplo, porque el día anterior leyó las noticias del diario.

Configuración rápida

Con WinRoute **no es necesario** que el servidor Proxy acceda a Internet. Su conexión a Internet es mantenida de forma satisfactoria por un **enrutador NAT** incluido en WinRoute. La tecnología NAT es mucho más adecuada para el acceso compartido a Internet que la tecnología Proxy. No obstante, WinRoute incluye también un servidor Proxy para poner a disposición la funcionalidad de memoria caché donde se requiera.

Para empezar a usar el servidor Proxy en WinRoute, siga los siguientes pasos:

En Administración WinRoute seleccione *Configuración -> Configuración Proxy -> General* (pestaña). Marque la opción "Servidor Proxy Habilitado". Mantenga el número original de puerto 3128.



1. En su navegador de Internet (Explorer, Netscape, Opera...) seleccione la configuración proxy, después configuración proxy manual e introduzca la dirección del computador WinRoute como dirección del servidor proxy para los protocolos HTTP, FTP y Gopher. Introduzca 3128 como el número de puerto proxy para todos los protocolos.
2. Pruebe la configuración accediendo a alguna página web desde el navegador.

Pestaña Propiedades Generales

Servidor Proxy Habilitado

Utilice esta opción para activar y desactivar el servidor Proxy.

Número de Puerto

El número de puerto en el que el servidor Proxy escucha las peticiones. Por lo general, no es necesario cambiar el número preestablecido 3128.

Acceso de Registro al servidor Proxy

Cuando esta opción está habilitada, todas las URL solicitadas del proxy por los navegadores se graban en un registro.

Control de Accesos de Usuario

Mediante el servidor Proxy de WinRoute el administrador puede controlar los accesos a las páginas web. El administrador puede disponer que el acceso a determinadas páginas web o dominios sólo le sea permitido a usuarios y/o grupos de usuarios específicos.

Forzar a los usuarios a que utilicen un servidor Proxy

Si decide utilizar el control de accesos del servidor Proxy debe, al mismo tiempo, bloquear el acceso directo a las páginas web para que el acceso a través del proxy sea la única alternativa posible para navegar por Internet. Para bloquear el acceso directo defina una regla de filtro de paquetes. Para más información sobre el filtro de paquetes, vea la sección ***Filtro de Paquetes*** (see "Forzar a los usuarios a utilizar el Servidor Proxy" on page 104) en el manual para el usuario de WinRoute.

Configurar el Control de Accesos Proxy

Para configurar el control de accesos Proxy de WinRoute haga clic en la pestaña "Acceso" de la Configuración del Servidor Proxy

Lista de Accesos

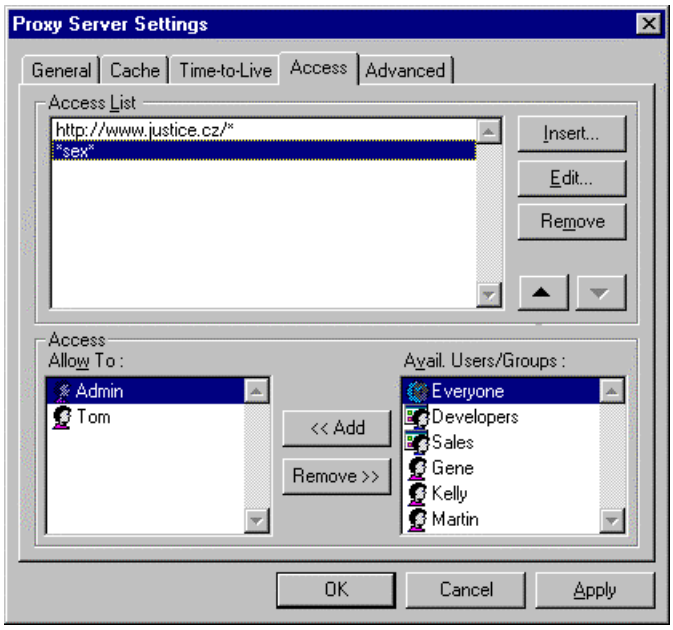
La lista de URL que no están permitidas. Puede utilizar un asterisco como comodín en la URL. Por ejemplo, para incluir a todos los computadores de undominio.com, utilice la cadena "*.undominio.com". WinRoute 4.0 emplea también pruebas de subcadena para incluir las URL. Así, por ejemplo, la cadena "sex" incluye el mismo conjunto de URL que la cadena "*sex*" (sólo que la última variante era soportada en las versiones previas de WinRoute).

Permitir a

La lista de usuarios y/o grupos de usuarios que pueden acceder a la URL en cuestión.

Usuarios/Grupos Dispon.

La lista de usuarios y grupos definidos en WinRoute.



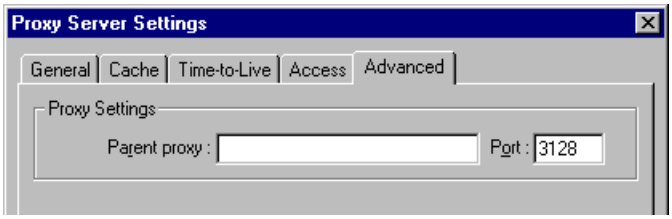
Cuando un usuario intenta acceder a una página web que pertenece a la categoría de páginas con acceso restringido, el navegador del usuario le solicita a éste que se autentifique. WinRoute comprueba entonces si el nombre de usuario y la contraseña son correctos y si el usuario dispone de la autorización para acceder a la página web en cuestión.

El navegador guarda el nombre del usuario y la contraseña en su memoria. Todas las peticiones subsiguientes de autentificación se responden automáticamente, de forma que el usuario no necesita introducir su nombre y su contraseña nuevamente.

Por otra parte, los usuarios deberían estar conscientes de esta facilidad. Si ha introducido su nombre y su contraseña alguna vez durante su navegación por Internet, debería cerrar el navegador cuando deje de utilizar el computador, para que los datos de autentificación se borren de la memoria del computador.

Propiedades Avanzadas

En la pestaña "Avanzada" de la configuración del servidor Proxy, puede especificar que WinRoute debe utilizar un servidor Proxy padre.



En algunos casos, es posible que tenga acceso a un servidor proxy que disponga de una **memoria caché** de un tamaño considerable o de una conexión **rápida** a Internet, y que su conexión a ese servidor sea también razonablemente rápida porque, por ejemplo, utiliza un enlace adicional además del que usa para su propia conexión a Internet.

Para aumentar el flujo de datos, podría definir que el servidor Proxy de WinRoute transmita todas las peticiones a ese servidor Proxy padre. Para hacerlo, simplemente debe introducir el nombre y el número de puerto del **Proxy Padre** en los campos de la pestaña "**Avanzada**".

Acerca de la Memoria Caché

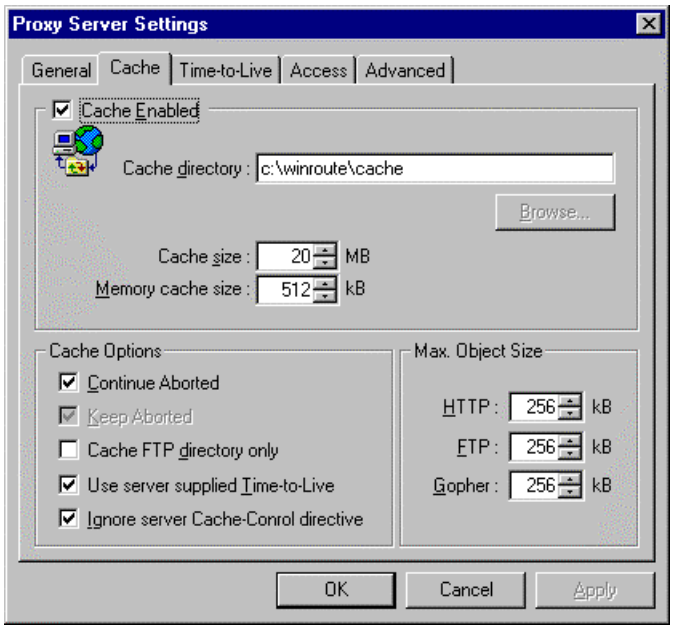
El servidor Proxy de WinRoute utiliza una forma **muy económica** de almacenamiento de datos. Todos los objetos guardados en la memoria caché se almacenan en un **fichero de longitud fija**. En contraposición a esto, muchos servidores proxy guardan cada objeto en un fichero individual.

Cuando el disco utiliza **unidades de asignación grandes** (como FAT16), este último método conlleva un **considerable desperdicio** de espacio del disco, ya que muchos de los componentes de las páginas web son muy pequeños. Por lo general, el 50% de los objetos son de menos de 6 kilobytes, mientras que el tamaño de las unidades de asignación en un disco grande es de 32 KB (con el sistema de ficheros FAT).

El hecho de que la memoria caché de WinRoute almacena los datos en un solo fichero ahorra mucho espacio en el disco - se requiere hasta 10 veces menos espacio en comparación con el método usual. Esto significa que o bien necesitará menos espacio o bien utilizará el espacio de una forma mucho más eficiente.

El archivo único de longitud fija permite también a WinRoute emplear técnicas de indexación muy eficientes, que hacen que la memoria caché de WinRoute sea muy rápida.

Configuración de la Memoria Caché



Caché Habilitada

Activa y desactiva la memoria caché. Cuando está inhabilitada, cada página web se recupera directamente de Internet.

Directorio Caché

El directorio en el que se guardan los objetos.

Tamaño Caché

La cantidad de espacio del disco utilizado por la memoria caché del proxy. Cuando tome una decisión sobre el tamaño, tenga en cuenta el número de usuarios, el tráfico que generan, etc. Si dispone de suficiente espacio libre, configure una memoria caché más grande. El tamaño máximo es de 3072 megabytes (3 GB).

Continuar Abortado

Cuando se marca esta opción, el servidor Proxy siempre finaliza la descarga de un objeto de Internet, incluso cuando el navegador del usuario aborta la petición (el usuario pulsa el botón de cancelación o sigue un enlace a otra página sin esperar que la página actual se descargue por completo). De esta forma, las visitas subsiguientes a la misma página son mucho más rápidas.

Mantener Abortado

Con esta opción, el servidor Proxy de WinRoute guarda en la memoria caché incluso los objetos incompletos (páginas web, imágenes). De esta forma se obtiene una aceleración parcial cuando se visita nuevamente la misma página web. Si se ha marcado "Continuar Abortado", la opción "Mantener Abortado" se pasa por alto.

Caché FTP sólo directorios

Cuando navegue por servidores FTP, use esta opción para guardar en la memoria caché sólo los listados del directorio. Si desea guardar también los ficheros descargados de un servidor FTP, desactive esta opción. La decisión referente a si un fichero específico se guardará en la memoria caché depende también de su tamaño. Vea abajo "Tamaño Máx. Objeto".

Usar Tiempo de Vida suministrado por servidor

El tiempo de vida es el periodo de tiempo tras el cual una página web específica se considera obsoleta y su contenido debe capturarse de nuevo del servidor correspondiente. Cuando se marca esta opción, el servidor Proxy de WinRoute se rige por el Tiempo de Vida (TTL) que viene junto con las diferentes páginas. Cuando una página no dispone de TTL, se utiliza el TTL preestablecido del Proxy.

Ignorar directiva Control de Caché del servidor

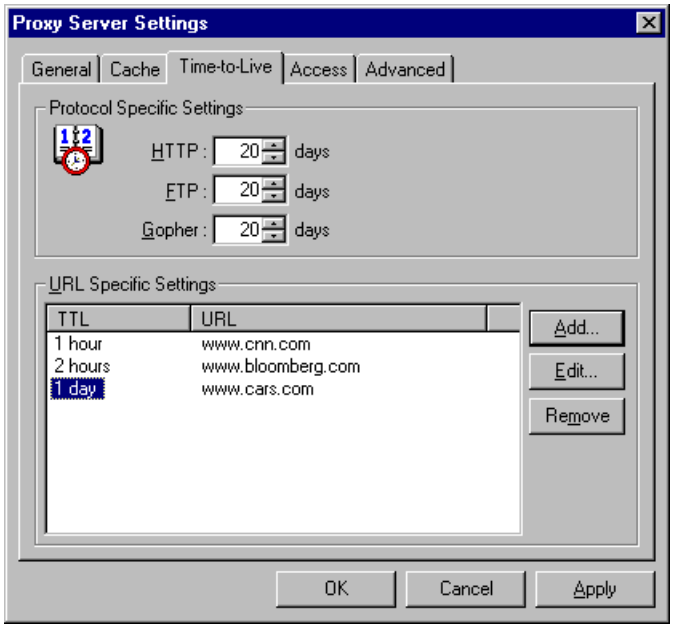
Cuando el contenido de una página web cambia con mucha frecuencia, el autor de la misma puede optar por establecer para ella la directiva "sin-caché". Ésta es una facilidad muy útil, pero algunos sitios web la utilizan demasiado, algunas veces incluso para todas sus páginas, imposibilitando así el objetivo de los servidores proxy. Si desea protegerse contra este procedimiento, habilite esta opción.

Tamaño Máx. Objeto

El tamaño máximo de los diferentes objetos que deben almacenarse en la memoria caché. Los objetos que superan este valor se transfieren al navegador del usuario, pero no se registran en la memoria caché. Por lo general, no es necesario registrar este tipo de objetos (tales como ficheros de archivo de programa), ya que no se descargan repetidamente.

Tiempo de Vida

Puede definir los valores por defecto del Tiempo de Vida (Time-to-Live, TTL) que se usan cuando una página web no dispone de ningún TTL definido para ella, o si decide pasar por alto los valores TTL suministrados por el servidor (vea la opción "Tiempo de Vida suministrado por el Servidor" en la pestaña Caché).



Configuración Específica del Protocolo

Aquí puede configurar el Tiempo de Vida preestablecido en días para los protocolos HTTP, FTP y Gopher.

Configuración Específica de la URL

Si desea configurar tiempos de vida individuales para algunos dominios, servidores web o páginas individuales, introduzca aquí los valores para las diferentes URL. Puede ajustar el TTL en días y/u horas.

Puede utilizar asteriscos como comodines en la URL. Una nueva facilidad de WinRoute 4.0 es una prueba de subcadena, que se utiliza también incluir las URL. Así, basta con introducir "ftp" para incluir a todos los servidores en cuyos nombres aparezca "ftp". (Anteriormente era necesario introducir "*ftp*" para abarcar este caso).

Por favor, tenga en cuenta que si ha habilitado la opción "Usar Tiempo de Vida suministrado por el Servidor" en la pestaña Caché, el TTL suministrado por el servidor tendrá una prioridad superior a la de la opción "Configuración Específica de la URL".

¿Cómo forzar a los usuarios a utilizar Proxy y no NAT?

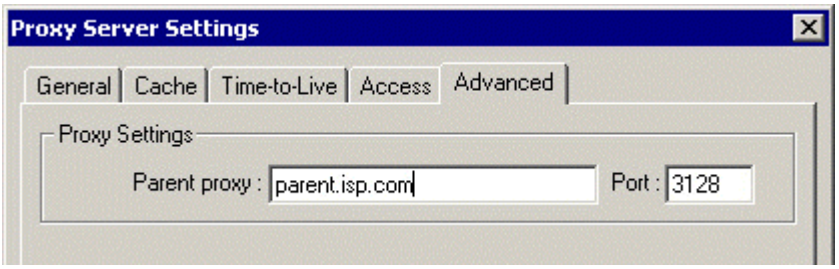
A pesar de que **NAT** le ofrece una capacidad de conexión a Internet excelente, en algunas ocasiones puede resultar más conveniente forzar a los usuarios a utilizar el **Servidor Proxy** para acceder a la **World Wide Web**. Éste es el caso, generalmente, cuando dispone de un acceso de 56K para toda la compañía y la memoria caché es, por tanto, de gran utilidad, o cuando desea **controlar los accesos de los usuarios** a través de un **filtro URL** integrado.

Para utilizar un Proxy para acceder a la WWW debe configurar todos los navegadores para que utilicen el servidor proxy. Recuerde que el puerto de servidor proxy predeterminado en WinRoute es el **3128**. Puede cambiar este puerto en caso necesario. Los usuarios pueden pasar por encima del proxy y acceder directamente a Internet a través de NAT. Para evitar esto, debe configurar el cortafuegos de la forma adecuada. Vea el ejemplo respectivo en el capítulo ***Configurar el Cortafuegos*** (see "Forzar a los usuarios a utilizar el Servidor Proxy" on page 104).

Usar un Servidor Proxy Padre

Servidor Proxy Padre

En algunos casos puede resultar necesario que el servidor Proxy de WinRoute se conecte a un servidor Proxy de una "capa superior", el así denominado **proxy padre**. En el menú *Configuración / Servidor Proxy* seleccione la pestaña *Avanzada* e introduzca allí la dirección IP y el puerto del servidor proxy padre.



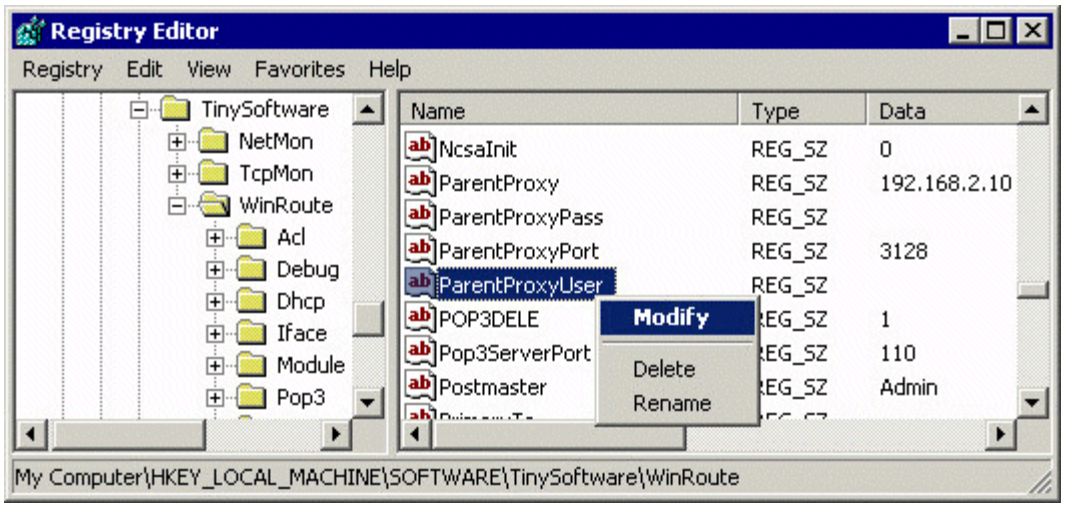
Nombre de usuario y contraseña del Proxy padre

Es posible que el servidor proxy padre le pida al usuario que se identifique para poder acceder a determinados (o a todos) los sitios web, realizando una petición similar a la de WinRoute (para más detalles vea el capítulo *Control de Accesos Proxy*). WinRoute Pro 4.1 incluye este tipo de autentificación desde su revisión 22.

Para configurar una autentificación:

- Pare el controlador WinRoute Engine (desde Servicios Windows o mediante el programa WinRoute Engine Monitor)
- Inicie el editor del registro Windows (regedit.exe)
- Busque la clave *HKEY_LOCAL_MACHINE\Software\TinySoftware\WinRoute*
- En el campo derecho, busque los elementos de texto **ParentProxyUser** y **ParentProxyPass** y cambie sus contenidos, introduciendo el nombre de usuario y la contraseña adecuados.
- Cierre el editor del registro e inicie WinRoute Engine.

Después de este procedimiento, el servidor proxy de WinRoute se autentificará a sí mismo como el servidor proxy padre.



Servidor de Correo

En Esta Sección

Acerca del servidor de correo de WR

WinRoute incluye un servidor de correo SMTP/POP3 con funcionalidad completa. Puede usarlo de la misma forma que usaría el servidor de correo de su proveedor de servicios de Internet (ISP). Mediante el servidor de correo de WinRoute puede enviar mensajes de correo electrónico a Internet y a los usuarios locales de su LAN, y también recibir correo electrónico y guardarlo en los buzones de los usuarios de WinRoute. WinRoute incluye también un planificador que le permite programar el intercambio de correo electrónico.

Si no utiliza el servidor de correo

No es necesario que utilice el servidor de correo de WinRoute. Puede continuar utilizando el servidor de correo de su proveedor u otro servidor de correo de terceros. En ese caso, WinRoute actuará como enrutador/cortafuegos que permitirá que su software cliente de correo se comunique con el servidor de correo de su proveedor de servicios.

- ***Nota: ¡No configure su software cliente de correo para que utilice el Proxy! Debe emplear la facilidad NAT de WinRoute para acceder a Internet y configurar su software cliente para que acceda directamente a Internet. Si no puede establecer el intercambio de correo electrónico, esto significa que NAT no está configurada correctamente. Vea la siguiente*** Lista de Control ***para configurarla de la forma adecuada.***

Cuentas de Usuario

En Esta Sección

Acerca de las cuentas de usuario

WinRoute - Cuentas de Usuario

WinRoute puede programarse con cuentas de usuario individuales que pueden juntarse en grupos (configuradas bajo Configuración | Cuentas… | Usuarios (pestaña). Los usuarios existentes de Windows NT/2000 pueden importarse a través de la pestaña Avanzada en el menú Configuración | Cuentas…

¿Qué es un usuario?

Como usuario de WinRoute puede participar en la administración de WinRoute y con un buzón, participar en las directrices de restricción de acceso del servidor Proxy de WinRoute.

Los usuarios pueden crear grupos y aplicarles los privilegios o restricciones mencionados arriba.

Agregar un usuario

Para agregar un usuario:

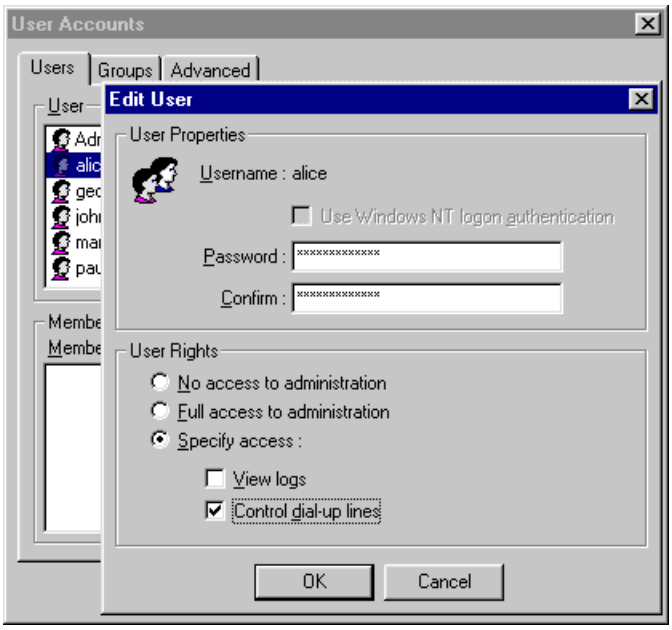
1. En el menú **Configuración->Cuentas**
2. Pulse el botón **Agregar**
3. Defina un **nombre de usuario** y una **contraseña**
4. Asigne **derechos** al usuario:

   El usuario no tiene autorización para administrar WinRoute.

   El usuario tiene acceso completo a la administración

   - **Ver registros:** El usuario tiene el derecho de iniciar la sesión en WinRoute Administrator y ver, solamente, las ventanas de los registros (información de depuración, registro proxy, registro de correo, etc.). El usuario no dispone de ningún acceso más para modificar los demás parámetros de la configuración.

- **Controlar líneas de marcación:** El usuario tiene el derecho de iniciar la sesión en WinRoute Administrator y establecer – desconectar la conexión a Internet. El usuario no dispone de ningún acceso más para modificar los demás parámetros de la configuración.



Grupos de usuarios

En WinRoute puede reunir a numerosos usuarios en diferentes grupos. Un usuario puede ser miembro de varios grupos a la vez.

Puede asignar **derechos** al grupo.

- ***Nota: los derechos asignados al grupo "sobrescriben" los derechos asignados a un usuario.***

Los miembros de los grupos pueden disponer de los siguientes **derechos**:

El usuario no dispone de acceso para administrar WinRoute.

El usuario dispone de acceso completo a la administración.

- **Ver registros:** El usuario tiene el derecho de iniciar la sesión de WinRoute Administrator y ver, solamente, las ventanas de los registros (información de depuración, registro proxy, registro de correo, etc.). El usuario no dispone de ningún acceso más para cambiar los demás parámetros de la configuración.
- **Controlar las líneas de marcación:** El usuario tiene el derecho de iniciar la sesión de WinRoute Administrator y establecer – desconectar la conexión a Internet. El usuario no dispone de ningún acceso más para cambiar los demás parámetros de la configuración.

Administración Remota

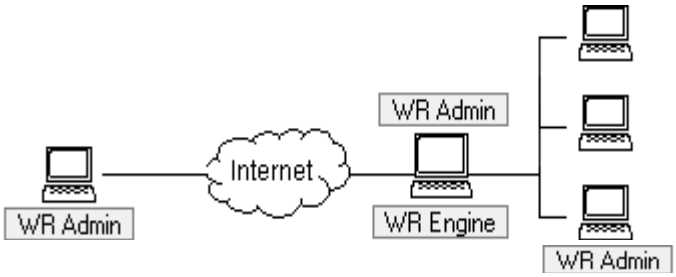
WinRoute Pro pone a disposición de los usuarios las ventajas de la administración remota. Con la configuración y los derechos adecuados, puede administrar su cortafuegos de forma segura desde cualquier parte del mundo. El acceso al motor (WinRoute Engine) está protegido por una codificación de alto nivel y por contraseña.

Componentes de WinRoute Pro

WinRoute Pro 4.x consta de tres módulos:

WinRoute Engine, el "motor" de WinRoute, ejecuta todas las operaciones de encaminamiento y análisis (NAT, filtro de paquetes, mapeo de puerto, etc.). Puede Arrancar/Parar WinRoute Engine desde la aplicación WinRoute Engine Monitor o, si está utilizando Windows NT, directamente desde la opción Servicios NT. WinRoute Engine se ejecuta de forma invisible como un servicio bajo Windows2000/NT/98 ó 95.

WinRoute Engine Monitor es la aplicación de supervisión que indica si WinRoute Engine se está ejecutando o no. Aparece como un pequeño icono azul en la esquina inferior derecha de su pantalla.



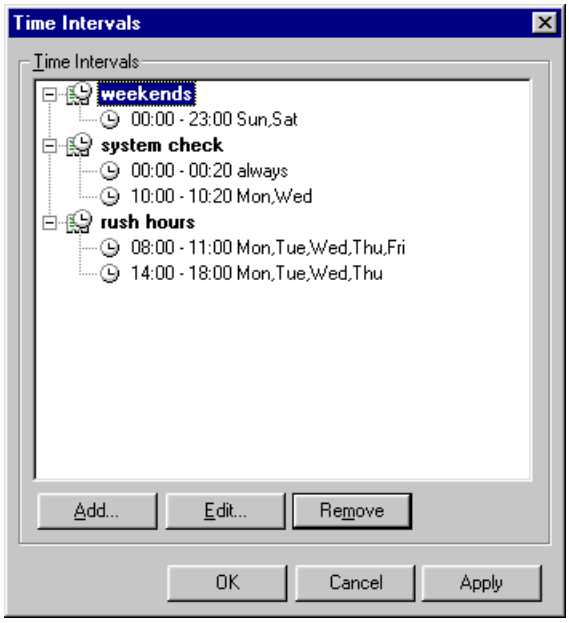
WinRoute Administrator permite realizar la configuración y los ajustes de WinRoute Engine. WinRoute Administrator es una aplicación individual (wradmin.exe) que puede funcionar en cualquier computador conectado con el computador WinRoute Engine a través de una conexión TCP/IP. Para más información sobre los ajustes necesarios en WinRoute Engine para permitir una conexión remota, vea los otros capítulos en esta sección.

Intervalos de tiempo

Puede definir zonas de tiempo – intervalos de tiempo preestablecidos – para ejecutar determinadas acciones. Dichas acciones pueden ser:

- Filtro de Paquetes
- Intercambio de correo electrónico (transmitir y recibir)
- Conexión a Internet
- Configuración NAT avanzada

Una zona de tiempo es un grupo de intervalos de tiempo. Por lo tanto, puede crear un espacio de tiempo heterogéneo que conste de varios intervalos de tiempo.



- ***Ejemplo: Puede crear una zona de tiempo denominada "Días festivos y tardes" que cubra: sábados, domingos, lunes de 4PM a 6PM, martes de 5PM a 7PM***

Para definir una zona de tiempo:

1 En el menú *Configuración=>Avanzada=>Intervalos de Tiempo*

2 Otorgue un nombre a la zona de tiempo

3 Agregue el nuevo intervalo de tiempo

CAPÍTULO 2

EMPEZAR A USAR WINROUTE

En Este Capítulo

Requisitos del sistema

Para instalar y ejecutar WinRoute Pro 4.1 se recomienda un sistema con, como mínimo:

- PC clase Pentium (procesador individual o dual)
- Windows 95/98/NT4.0/2000 OS
- 32MB de memoria aleatoria
- 1MB de espacio en el disco duro
- como mínimo, 2 interfaces disponibles. Éstas pueden ser Ethernet, RAS, TokenRing o DirecPC

Lista de Control Rápido

Para todos los usuarios de WinRoute existe un listado básico de ajustes y reglas que, cuando se aplican, garantizan una conexión exitosa de sus redes a Internet. Naturalmente, es indispensable disponer de una conexión a Internet que funcione correctamente.

Debe realizar los ajustes que se describen abajo para sacar el máximo provecho de NAT al compartir el acceso a Internet. Si desea utilizar un servidor Proxy (integrado en WinRoute), no es necesario que realice estos ajustes. En ese caso deberá dirigir sus navegadores y aplicaciones hacia el servidor Proxy de WinRoute. No obstante, recomendamos encarecidamente utilizar NAT (traducción de la dirección de red, Network Address Translation) siempre que sea posible, pues es más rápida, segura y fiable.

Ajustes y reglas

1 **En el computador WinRoute - Dos Interfaces (NIC)**
Compruebe que el computador WinRoute disponga (como mínimo) de dos interfaces. Una está destinada a la conexión a Internet y la otra, a la conexión local /cliente. Pueden haber adaptadores de red o líneas RAS. Una interfaz (Ethernet o RAS/conmutada) se usa para la conexión a Internet, mientras que la(s) otra(s) interfaz(ces) (Ethernet, token ring…) se usa para la conexión a su red(es).

2 **¡Cerciórese de que todas las direcciones IP se encuentren activas!**
Para que WinRoute funcione correctamente, la máquina host de WinRoute debe responder a los ping enviados tanto a su dirección IP pública como privada por las máquinas clientes.

3 **En el PC WinRoute - ¡Habilite NAT en la interfaz de Internet!**
Cerciórese de que NAT esté marcada como ACTIVADA para la interfaz que conecta a Internet (Ethernet, línea RAS). Esto se puede ajustar en el menú **Configuración=>Tabla de Interfaces** seleccionando las propiedades de la interfaz deseada.

4 En el PC WinRoute - ¡Inhabilite NAT en la interfaz interna!
Cerciórese de que NAT **NO ESTÉ MARCADA** en la interfaz o interfaces que conectan a la red interna.
Nota: En configuraciones muy especiales, NAT se puede marcar como "ACTIVADA" incluso en la interfaz interna. Puede ver un ejemplo aquí (si está disponible).

5 En el PC WinRoute - ¡Ninguna pasarela en la interfaz interna!
Compruebe que no haya NINGUNA pasarela por defecto en las propiedades de red de la interfaz (tarjeta de red) que conecta a la red interna. Naturalmente, la pasarela por defecto de la interfaz que conecta a Internet debe ajustarse de conformidad con los detalles especificados por su proveedor de servicios de Internet (ISP).

6 En el PC WinRoute - ¡Introduzca las opciones en la configuración DHCP!
En la mayoría de los casos, utilizará el servidor DHCP de WinRoute para automatizar la configuración de la red. Cerciórese de que realmente ha definido el rango(s) de direcciones IP que desea que el servidor DHCP asigne junto con las opciones. Bajo Opciones se especifica otra información que se suministra a sus estaciones de trabajo como, por ejemplo, servidor DNS, pasarela por defecto, etc.

7 En el PC cliente - ¡La dirección IP interna del PC WinRoute es la pasarela por defecto!
El PC WinRoute actúa como PASARELA POR DEFECTO para todos los computadores de la LAN. Por ello, utilice la dirección IP de la tarjeta de interfaz de red interna del host WinRoute (p. ej., 192.168.1.1) como la pasarela para cada computador interno/cliente. Ajuste este valor en cada computador "cliente" O ajuste el valor una sola vez en el servidor DHCP de WinRoute para que éste asigne el valor automáticamente a todas las estaciones de trabajo.
Si necesita utilizar una pasarela por defecto diferente, vea los Ejemplos de (Inter)Conexión de Redes Avanzada.

8 En el PC cliente - ¡Compruebe el DNS!
En la mayoría de los casos utilizará el transmisor DNS integrado de WinRoute, como servidor DNS para los computadores conectados a la red. Cerciórese de que el transmisor DNS integrado de WinRoute está ACTIVADO y configurado. Puede utilizar la dirección del servidor DNS de su proveedor de servicios, introduciéndola en los campos correspondientes de la configuración TCP/IP de cada computador conectado a la red.

- ***En los casos en los que WinRoute se use sólo como cortafuegos o como servidor de correo (es decir, sin petición de acceso compartido a Internet), NO es necesario ACTIVAR NAT en ninguna interfaz.***

- ***Las interfaces del computador WinRoute deben tener direcciones IP distintas de redes diferentes. No se puede asignar a la interfaz una dirección IP de la misma red (es decir, una 207.181.216.23 y la otra 207.181.216.24). Típicamente, dispondrá de una interfaz local (LAN) y de una interfaz de Internet. Es este caso no tendrá ningún problema. Si dispone de tres interfaces (2 locales y una de Internet) debería asignar a las interfaces locales direcciones IP de redes diferentes (una 192.168.1.1 y la otra 192.168.2.1).***

Software conflictivo

Se conocen diversos aspectos relacionados con software incompatible:

Norton Antivirus

Inhabilite el puerto 110 en la configuración de Norton Antivirus si desea ejecutar el servidor de correo WinRoute. Si mantiene el puerto 110 en Norton, el computador no podrá arrancarse.

WinGate

Desinstale WinGate antes de instalar WinRoute. Desinstale tanto el software de servidor como el de cliente.

SyGate

Desinstale SyGate antes de instalar WinRoute. Desinstale tanto el software de servidor como el de cliente.

Servidor Proxy MS

Desinstale el servidor Proxy MS antes de instalar WinRoute. Desinstale tanto el software de servidor como el de cliente. Quite el TCP/IP, rearranque el sistema y agréguelo de nuevo.

Conexión a Internet Compartida (Internet Connection Sharing) de Microsoft

Desinstale MS ICS antes de la instalación, quite el protocolo TCP/IP, rearranque el sistema y agregue TCP/IP de nuevo.

WinProxy de Ositis

Desinstale WinProxy antes de la instalación, quite el protocolo TCP/IP, rearranque el sistema y agregue TCP/IP de nuevo.

Todo el software mencionado arriba utiliza controladores que no funcionan correctamente con las porciones más bajas del protocolo de conexión en red empleado por WinRoute.

Tablas de encaminamiento

Es posible que instale y configure todos los componentes con éxito, pero aun así no disponga de la funcionalidad completa. Lamentablemente, los sistemas operativos Windows 95/98/NT no están diseñados para funcionar óptimamente en las conexiones en red. Incluso después de configurar correctamente WinRoute y su red, es posible que la configuración no funcione. En ese caso, vea la tabla de encaminamiento y elija una de las siguientes opciones:

- reparar las rutas borrándolas y agregándolas de nuevo - sólo para usuarios experimentados

o

- quitar por completo el protocolo TCP/IP, reinicializar el computador y agregarlo de nuevo. El rendimiento está garantizado.

Software de Cliente Proxy

Algunos servidores proxy requieren que el software se instale en todas las máquinas clientes. Este software cliente hace que todas las aplicaciones soliciten un servidor proxy. Si no se quita el software proxy cliente, es posible que la máquina en cuestión no se conecte a Internet porque WinRoute no está configurado como servidor proxy. Si después de quitar el software el cliente aún no puede conectarse a Internet, reinstale TCP/IP y sus ajustes y reinicialice el sistema.

Controladores de Tarjetas de Red

Intente utilizar las tarjetas de interfaz de red con los estándares más usuales. Si su computador está equipado con una tarjeta especial, anticuada o apenas salida al mercado, es posible que sus controladores incluyan instrucciones específicas que impidan que WinRoute se comunique con ella. Busque la tarjeta Ethernet más usual utilizada en su red y simplemente cambie su posición con la de la otra tarjeta. Muchos de los clientes inicialmente "descontentos" han quedado totalmente satisfechos tras cambiar la tarjeta o actualizar el controlador.

WinRoute es un enrutador/cortafuegos basado en software completamente neutral, que no requiere ningún software cliente ejecutándose en ninguno de los computadores clientes a menos que se use la administración remota, en cuyo caso debe instalarse WinRoute Administration "wradmin.exe" en una máquina cliente o externa.

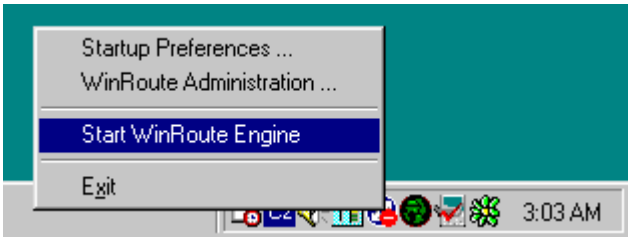
Administración en WinRoute

En Esta Sección

Administración desde la red local

Para administrar WinRoute desde la red local o desde el computador en el que se ejecuta WinRoute, debe hacer lo siguiente:

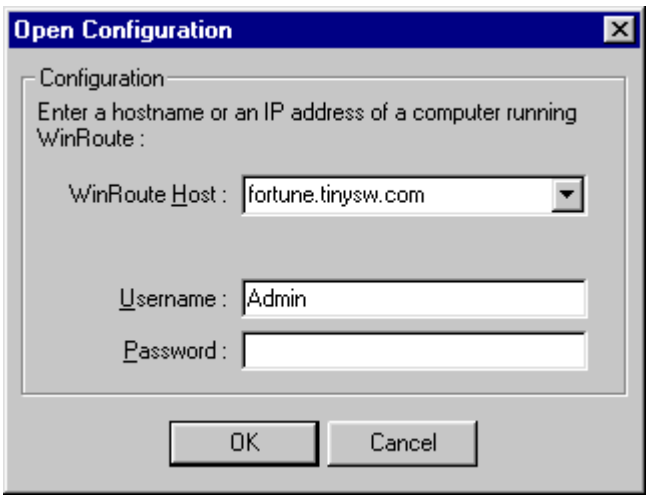
1. **Verifique que WinRoute Engine está activado y ejecutándose**
   Para comprobar que WinRoute se ha arrancado, inicie la aplicación de supervisión WinRoute Engine Monitor en el grupo de programas WinRoute 4.0. A continuación debería aparecer un icono pequeño azul y blanco en la bandeja del sistema de la barra de tareas (esquina inferior derecha del escritorio). Esto indica que la aplicación se está ejecutando. Una cruz roja sobre el icono indica que WinRoute se ha parado. Para iniciar WinRoute Engine basta con **hacer clic con el botón derecho del ratón** sobre el icono, y seleccionar Iniciar WinRoute Engine en el menú emergente que aparece.



2. Iniciar WinRoute Administrator

Para iniciar el módulo de administración de WinRoute, arranque la aplicación desde el menú Inicio=>Programas=>WinRoute 4.0, o haciendo clic con el botón derecho del ratón en el icono de WinRoute Engine Monitor y seleccionando *Administración WinRoute* en el menú emergente. También puede copiar el fichero *WRAdmin.exe* a cualquier otro computador en su red y ejecutarlo desde allí.

Cuando emerge la ventana Admin puede mantener el host local predeterminado o introducir la dirección IP del computador en el que se está ejecutando WinRoute. Introduzca el nombre de usuario y la contraseña que se emplean para la administración.



Nota: Cuando se conecta por primera vez, puede usar "Admin" como nombre de usuario y dejar la contraseña en blanco. Ver Configuración del Usuario para más detalles sobre las directrices referentes al nombre de usuario y a la contraseña para la administración.

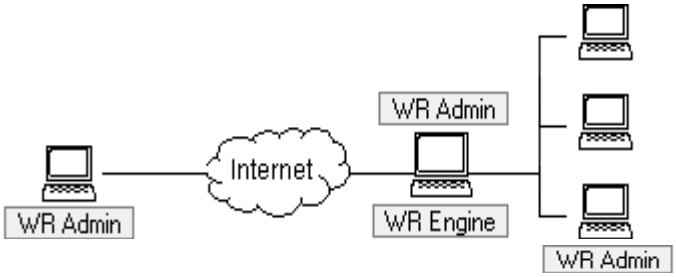
Debe iniciar la sesión con éxito como administrador de WinRoute Engine para poder llevar a cabo la configuración.

Posibles motivos para un inicio de sesión infructuoso desde una red local:

- WinRoute Engine no está activado ni ejecutándose
- Nombre de usuario y contraseña incorrectos
- Dirección IP incorrecta introducida al conectarse a WinRoute Engine
- No dispone de los derechos para administrar WinRoute
- Se ha activado NAT en la interfaz que conecta a su red – vea el capítulo Lista de Control y Configuración de la Red para obtener ayuda a este respecto

Administración desde Internet

Puede administrar WinRoute Pro Engine desde cualquier computador en cualquier parte del mundo, siempre que disponga de una conexión TCP/IP en el lugar en que se encuentre. La administración es segura (codificada) y se controla mediante el nombre de usuario y la contraseña.



Para administrar el computador WinRoute desde fuera de la LAN (desde Internet), debe establecer el mapeo de puerto en el computador WinRoute. Tenga en cuenta que cuando NAT está activada en la interfaz que conecta a Internet (es necesario para compartir el acceso a Internet), su red completa, inclusive el computador WinRoute, está totalmente protegida y, por ello, nadie puede acceder a ella.

Para establecer el mapeo de puerto para la administración remota seleccione el menú *Configuración=>Avanzada=>Mapeo de Puerto*, pulse agregar y establezca:

Protocolo: TCP/UDP

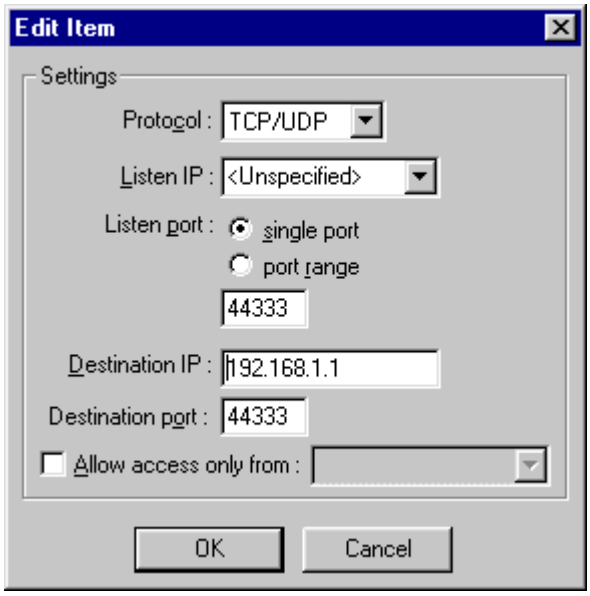
IP de escucha: <no especificada> (recomendada) o la dirección IP de la interfaz.

Puerto de escucha: 44333

IP de destino: La dirección IP de la interfaz que conecta el computador WinRoute con la red local (dirección IP de clase privada)

Puerto de destino: 44333

Sólo permitir acceso desde: Cuando se marca esta opción, puede restringir el acceso a WinRoute Engine. Debe predeterminar las direcciones IP a las que se les permitirá el acceso a WinRoute Engine desde Internet. Seleccione para ello *Configuración=>Avanzada=>Grupos de Direcciones*. Puede agrupar direcciones IP individuales, rangos de direcciones IP y redes.



Vea los ejemplos para más detalles sobre el mapeo de puerto. Una vez que haya configurado todo correctamente, simplemente ejecute el programa de administración de WinRoute desde cualquier computador e introduzca la dirección IP (registrada - p. ej., 206.86.181.25) del computador en el que se ejecuta WinRoute, así como el nombre del usuario y la contraseña para la administración de ese computador. Para más detalles sobre las directrices referentes al nombre del usuario y la contraseña, vea la Configuración del Usuario.

Posibles motivos para un inicio de sesión infructuoso desde Internet:

- WinRoute Engine no está activado ni ejecutándose
- Nombre de usuario y contraseña incorrectos
- Dirección IP incorrecta introducida al conectarse a WinRoute Engine
- No dispone de los derechos necesarios para administrar WinRoute

- No se ha establecido ningún mapeo de puerto o se ha establecido un mapeo de puerto incorrecto en el computador en el que se ejecuta WinRoute Engine

Contraseña Admin extraviada

Si pierde su contraseña de administración, por favor, envíe un mensaje electrónico a support@tinysoftware.com para recibir más instrucciones a este respecto. Por motivos de seguridad no podemos publicar aquí la solución de este problema.

Configuración de la red

En Esta Sección

Acerca de DHCP

El servidor DHCP puede simplificar considerablemente la configuración de las estaciones de trabajo dentro de su LAN. Cuando utiliza el servidor DHCP, el único ajuste que debe realizar en las estaciones de trabajo clientes es configurarlas para que obtengan una dirección IP dinámicamente del servidor DHCP. (Este es un ajuste por defecto cuando se agrega el protocolo TCP/IP en las propiedades de la red.)

- ***Puede utilizar el servidor DHCP integrado en WinRoute o cualquier otro servidor DHCP del mercado. ¡Cerciórese de que sólo haya un servidor DHCP habilitado a la vez en su red!***

Vista de conjunto de pasarelas por defecto

WinRoute actúa como un enrutador. Como tal, requiere dos ajustes TCP/IP básicos en cada computador de su red:

- Asignación de la dirección IP – o bien manualmente o bien mediante el servidor DHCP (p. ej., el servidor DHCP de WinRoute)

- Definir la pasarela (gateway) por defecto

La pasarela por defecto de cada computador que acceda a Internet a través del computador WinRoute, debe ajustarse en la **dirección IP** de la interfaz Ethernet del computador WinRoute que conecta a la LAN.

Ejemplo:

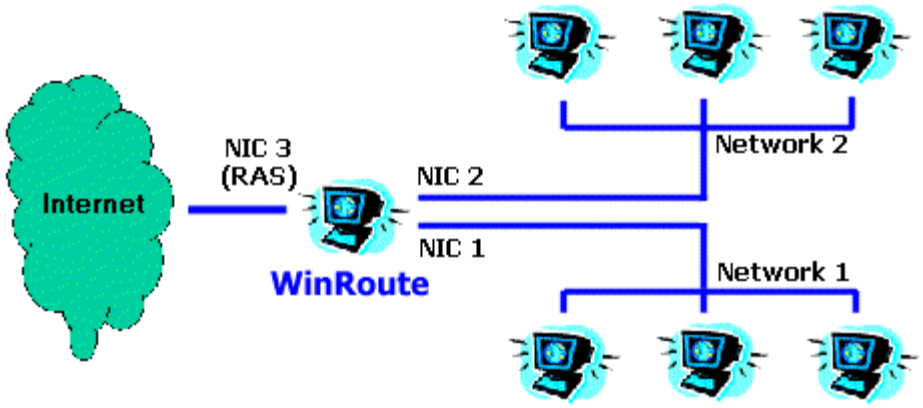
El computador cliente tiene la dirección IP 10.10.10.23, mientras que el PC WinRoute tiene dos interfaces: una de ellas está conectada con el modem de cable con la dirección IP del proveedor de servicios (p. ej., 203.23.14.232), y la otra conecta con la red privada (10.10.10.1). La pasarela por defecto en el computador 10.10.10.23 debe ajustarse en 10.10.10.1.

- ***Nota 1: Cuando crea un rango de direcciones IP dentro de su red local, debe usar la dirección IP de la misma subred, es decir que si emplea la máscara de subred 255.255.255.0, todas las direcciones deben encontrarse entre 10.10.10.1 y 10.10.10.255.***
- ***Nota 2: Es posible que hayan más redes conectadas a Internet a través de WinRoute. En ese caso, puede disponer de más interfaces en el computador WinRoute, una para cada red. Entonces, cada una de esas interfaces (sus direcciones IP) representa la pasarela por defecto para el resto de la red conectado a ella.***

Elegir el computador WinRoute adecuado

WinRoute **SIEMPRE DEBE FUNCIONAR** en un computador conectado a Internet - a través de la tarjeta de red, cable, modem DSL, enlace conmutado o enrutador.

WinRoute siempre actúa como pasarela entre dos (o más) redes, siendo cada red representada por una interfaz. Dichas interfaces pueden ser tarjetas Ethernet, adaptadores RAS, adaptadores USB a Ethernet, adaptadores PPPoE, etc.


Internet
NIC 3
(RAS)
NIC 2
NIC 1
WinRoute
Network 2
Network 1

Configuración IP con el servidor DHCP

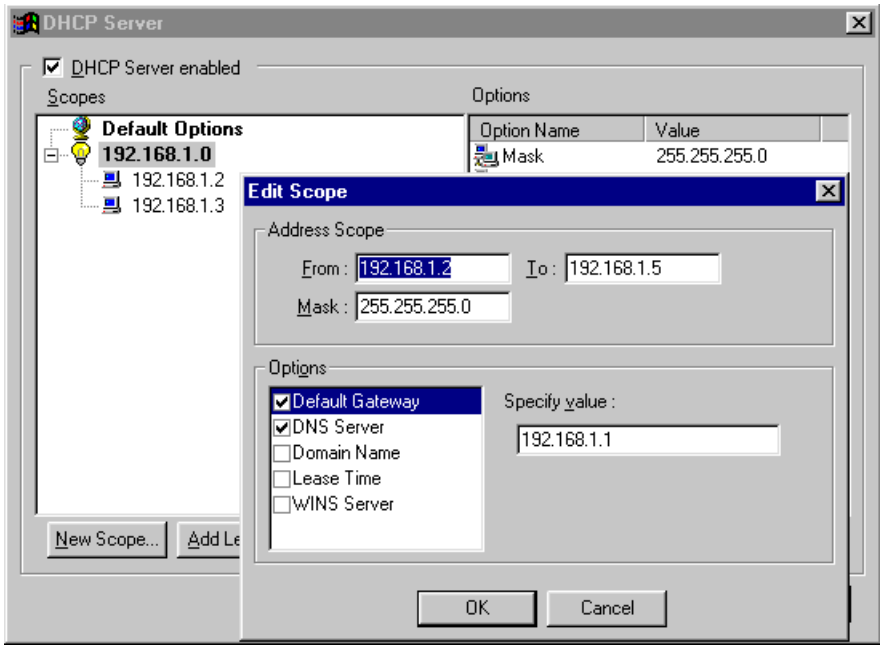
Compruebe que sus estaciones de trabajo estén configuradas para obtener una dirección IP del servidor DHCP (vea *TCP/IP->interfaz de red* propiedades en cada computador) y que todas las demás propiedades TCP/IP estén en blanco, inclusive la información sobre el servidor DNS.

A continuación, inicie el programa Administración WinRoute:

1. Seleccione el menú *Configuración=>servidor DHCP*.
2. ACTIVE el servidor DHCP (marque la casilla) y pulse el botón Agregar **Nuevo Rango**.

3. Agregar Rango
Especifique aquí el rango de direcciones IP utilizadas por el servidor DHCP que serán asignadas a las estaciones de trabajo. Recuerde que una dirección IP ya está siendo utilizada por el computador WinRoute, por lo que no debe usarla. El rango de direcciones IP debe pertenecer a la misma subred. Vea la figura en el ejemplo.

4. Especifique las opciones (¡importante!)
Bajo Opciones puede especificar qué otra información se suministrará a las estaciones de trabajo (p. ej., pasarela por defecto, servidor DNS, etc.). Marque la casilla junto a cada componente en el cuadro de diálogo e introduzca la información adecuada. Introduzca la información para la pasarela por defecto y el servidor DNS (típicamente, usará WinRoute como servidor DNS) y utilice la dirección IP del computador WinRoute (p. ej., 192.168.1.1). Puede dejar las demás opciones en blanco.


DHCP Server
DHCP Server enabled
Scopes
Options
Default Options
192.168.1.0
192.168.1.2
192.168.1.3
Option Name
Value
Mask
255.255.255.0
Edit Scope
Address Scope
From :
192.168.1.2
To :
192.168.1.5
Mask :
255.255.255.0
Options
Default Gateway
DNS Server
Domain Name
Lease Time
WINS Server
Specify value :
192.168.1.1
New Scope...
OK
Cancel

- ***Nota: Debe asignarse la dirección IP de la interfaz Ethernet (que conecta con la LAN) en el computador WinRoute y debe usar esa dirección IP en los otros computadores como la pasarela por defecto y, opcionalmente, como servidor DNS. No obstante, la pasarela por defecto de esa interfaz quedará en blanco.***

Configuración IP con el 3er. servidor DHCP

Cuando utiliza un tercer servidor DHCP para configurar su red, debe comprobar detenidamente los valores que dicho servidor DHCP asigna a las estaciones de trabajo clientes en su red.

Cerciórese de que el servidor DHCP esté suministrando la información correcta a sus estaciones de trabajo clientes. En otras palabras, debe configurar el servidor DHCP de forma que asigne a los otros computadores las direcciones IP de la tarjeta LAN del computador WinRoute como la pasarela por defecto y (opcionalmente) como servidor DNS.

Asimismo, las direcciones IP asignadas a las estaciones de trabajo clientes deben pertenecer a la misma subred que el computador WinRoute.

CERCIÓRESE de que se haya asignado realmente una dirección IP fija a la tarjeta de red interna del computador WinRoute (p. ej., 192.168.1.1) y que el DHCP asigne dicha dirección como la pasarela por defecto al resto de la red. El servidor DHCP no puede asignar ninguna dirección IP al host WinRoute.

Ejemplo:

El servidor NT con DHCP está funcionando en 192.168.1.1, mientras que WinRoute está funcionando en 192.168.1.5. La pasarela por defecto (y DNS si utiliza el DNS de WinRoute) a la que se dará salida hacia las estaciones de trabajo será 192.168.1.5.

Configuración IP - asignación manual

En algunos casos es necesario asignar direcciones IP manualmente a las estaciones de trabajo. Cuando esto resulte necesario, tenga en cuenta las siguientes reglas:

Asignación de dirección IP

Asigne a cada computador una dirección IP de "tipo interno", generalmente, 192.168.x.x o 10.x.x.x. Asigne a cada sistema una dirección IP de la misma subred. Por ejemplo, una vez que una dirección IP para el host WinRoute se establece en 192.168.1.1, debe continuar con el mismo esquema de numeración (p. ej., 192.168.1.2., 192.168.1.3, etc.)

Establezca la pasarela por defecto

Utilice la dirección IP del computador host WinRoute como la pasarela por defecto para todos los computadores clientes. En otras palabras, cada computador cliente debe usar la dirección IP del host WinRoute (dirección IP interna) como pasarela por defecto. Esta información se introduce en TCP/IP=>adaptador_Ethernet en las Propiedades de Red del computador.

Establezca el DNS

Finalmente, utilice la dirección IP del computador WinRoute como transmisor DNS para todos los computadores (la dirección IP interna, si está empleando el servidor DHCP de WinRoute). La única excepción posible es cuando utiliza la dirección DNS de su proveedor de servicios (ISP) u otro servidor DNS. En ese caso, debe introducir los datos DNS que le han sido suministrados por su ISP (en TCP/IP->NIC propiedades de cada estación de trabajo).

¡Importante! Vea el capítulo de este manual referente a la configuración DNS.

Configurar el transmisor DNS

El servidor DNS se configura mediante el menú *Configuración => Servidor DNS*.

"Habilitar la transmisión DNS"

Mediante esta opción se activa o desactiva el servidor DNS.

"Transmitir peticiones DNS automáticamente al servidor seleccionado entre los servidores DNS conocidos por el sistema operativo."

Cuando se selecciona esta opción, todas las peticiones DNS se transmiten al servidor DNS elegido en la configuración TCP/IP de la interfaz Internet o de la conexión en red conmutada.

"Habilitar búsqueda en fichero HOST"

Cuando se marca esta opción, se le permite al servidor DNS que use los datos del fichero HOSTS al contestar las peticiones.

"Editar fichero HOSTS..."

Mediante este botón se inicia un editor de texto externo en el cual puede editar el fichero HOSTS.

"Dominio DNS"

Introduzca aquí su nombre de dominio (p. ej., "acme.com"). Cuando se contestan las peticiones DNS, el nombre de dominio se adjunta al nombre host obtenido del fichero HOSTS o de la tabla de alquiler (lease) DHCP.

"Transmitir peticiones DNS a"

Introduzca la dirección IP numérica del servidor DNS al que desee transmitir las peticiones DNS. Seleccione una dirección del servidor DNS de su ISP o de un servidor al que tenga acceso rápido.

"Habilitar caché DNS"

Esta opción permite que las contestaciones de las peticiones DNS se guarden en la memoria caché interna. Las peticiones subsiguientes se procesan entonces utilizando el contenido de la memoria caché, sin necesidad de esperar hasta que responda el servidor DNS ubicado fuera de la red.

"Al devolver nombre del fichero HOSTS o de la tabla de alquiler, combinarlo con dominio DNS"

Esta facilidad se puede entender más fácilmente mediante un ejemplo - es posible que desee contestar una petición DNS del computador JOHN. En el fichero HOSTS introdujo que su dominio OFFICE debe asociarse con una dirección IP específica. Entonces, la petición JOHN.OFFICE puede resolverse correctamente.

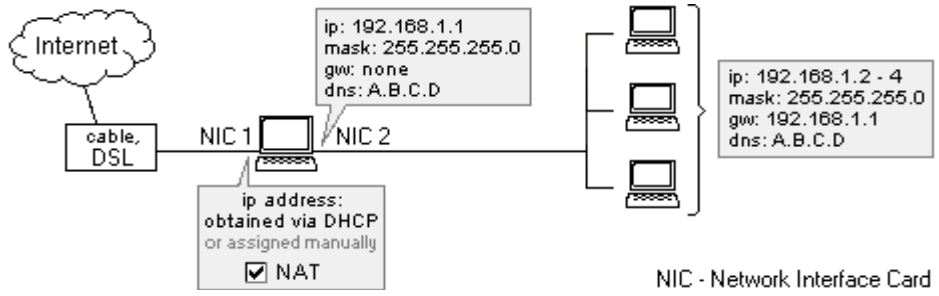
- ***Tenga en cuenta que en la memoria caché sólo se guardan las respuestas del tipo "Nombre => dirección IP". Las respuestas se almacenan hasta que expiren. El tiempo de expiración es suministrado por el servidor DNS junto con cada respuesta.***

Conectar la red a Internet

En Esta Sección

Conexión DSL

Para las conexiones DSL (ADSL, SDSL) se requieren dos tarjetas de interfaz de red (Network Interface Card, NIC) instaladas en el computador WinRoute. Una NIC funcionará como enlace a Internet (modem DSL), mientras que la otra NIC funcionará como enlace hacia la red interna.



Configuración de WinRoute

Para conectarse a Internet

1. Seleccione el menú Configuración->Tabla de interfaces
2. Seleccione Enlace NIC a Internet, haga clic en Propiedades y marque ACTIVADA en "Ejecutar NAT con dirección IP de la interfaz en todas las comunicaciones que pasen". Cuando se abra el cuadro de diálogo de la tabla de interfaces, verá NAT ACTIVADA junto a esta línea externa.
3. Compruebe que NAT NO ESTÉ ACTIVADA para la interfaz que conecta con la red interna (seleccione las propiedades de esta interfaz en la tabla de interfaces)
4. Compruebe que NO se haya configurado ninguna pasarela en las propiedades TCP/IP de la NIC interna (bajo Configuración de la red) y que se haya asignado una dirección IP interna a la NIC.

5 Compruebe que la NIC que conecta con Internet se haya configurado con los datos correctos suministrados por su ISP. En caso de que disponga de direcciones IP asignadas dinámicamente, deje los ajustes de la dirección IP en blanco.

Para más detalles sobre otras configuraciones de red, vea los capítulos correspondientes, especialmente la ***Lista de control*** .

Conexión DSL PPPoE

PPPoE es una tecnología desplegada recientemente para muchos abonados DSL. A pesar de que está siendo desplegada a gran escala por varios ISP, ofrece a sus usuarios sólo un rendimiento insuficiente y no es (en la actualidad) la mejor solución disponible para conectar su red a Internet. Los clientes deberían optar, siempre que sea posible, por la solución DSL estándar.

El despliegue de PPPoE con WinRoute es similar al de DSL estándar en lo referente a la configuración TCP/IP. WinRoute Pro debería instalarse en el mismo computador que el adaptador PPPoE. WinRoute Pro reconocerá el adaptador PPPoE como una interfaz de red. Debería habilitar NAT en esa interfaz. El adaptador ethernet (conectado en el modem de cable) aparecerá también como interfaz en la tabla de interfaces de WinRoute Pro. No debe habilitar NAT en esa interfaz.

WinRoute Pro funciona correctamente con todos los adaptadores PPPoE disponibles en el mercado. No obstante, los clientes pueden experimentar, de vez en cuando, pérdidas de rendimiento cuando utilizan ciertos adaptadores PPPoE:

Cliente Enternet 100, 300, 500 PPPoE

WinRoute Pro 4.1 funciona correctamente con el cliente Enternet PPPoE de NTS si activa el controlador de protocolo, en vez del controlador de filtro por defecto. Para ello, ejecute el cliente Enternet PPPoE, seleccione el menú Configuración->Avanzada y modifique los valores deseados.

Si se produce una pérdida de rendimiento, es posible que también deba reducir la MTU a 800 en las máquinas clientes.

WinPoet de Ivasion

WinRoute Pro 4.1 funciona correctamente con WinPoet bajo las siguientes condiciones: la compresión de encabezamiento IP (configuración RAS/conexión en red conmutada) está desactivada.

Reducir la MTU:

El adaptador PPPoE agrega información adicional al encabezamiento de cada paquete saliente. Windows utiliza por defecto el tamaño máximo permitido de paquete. El adaptador PPPoE compensa esto garantizando que la MTU de la máquina se reduzca ligeramente, compensando así la información adicional agregada a cada paquete. Lamentablemente, todas las demás máquinas continúan usando el tamaño máximo para la transmisión. Esto conlleva la pérdida de paquetes. En los siguientes enlaces encontrará información sobre la forma de reducir la MTU para todos los clientes.

Para usuarios de Windows 95/98:

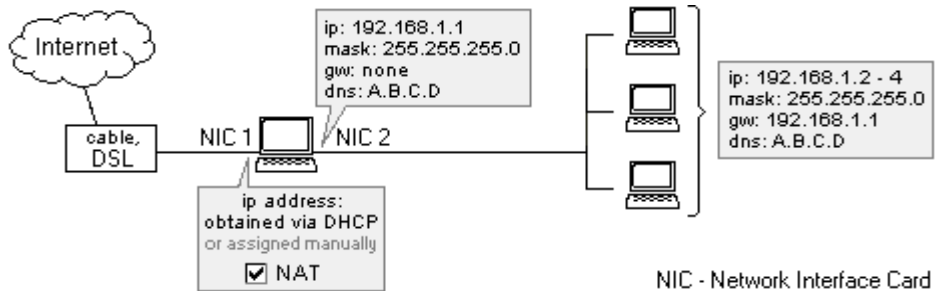
http://www.microsoft.com/support/kb/articles/Q158/4/74.asp

Para usuarios de Windows NT4/2000:

http://www.microsoft.com/WINDOWS2000/library/resources/reskit/samplechapters/cnbd/cnbd_trb_vcfx.asp

Conexión de modem de cable (bidireccional)

Para la conexión de modem de cable se requieren dos tarjetas de interfaz de red (Network Interface Card, NIC) instaladas en el computador de WinRoute. Una de ellas funcionará como conexión hacia Internet (modem de cable), mientras que la otra NIC conectará con la red interna. Para más información sobre los modem de cable unidireccionales (modem ascendente, cable descendente), véase el capítulo respectivo.



Configuración de WinRoute

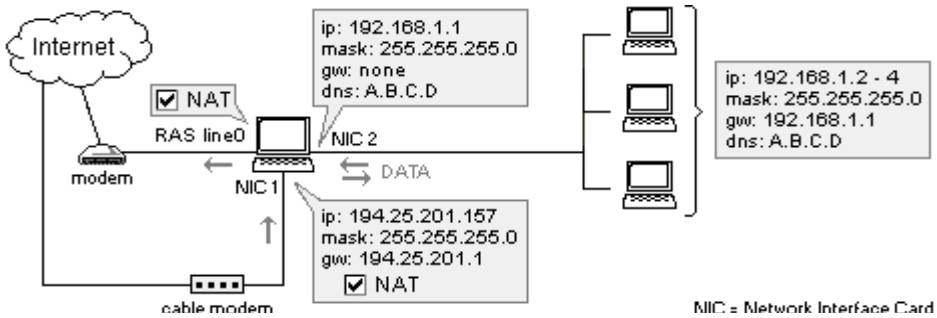
1. Seleccione Configuración->Tabla de Interfaces
2. Elija Enlace NIC a Internet, haga clic en Propiedades y marque ACTIVADA en "Ejecutar NAT con dirección IP de la interfaz para todas las comunicaciones que pasan". Cuando se abra el cuadro de diálogo de la tabla de interfaces, verá NAT ACTIVADA junto a esta línea externa.
3. Compruebe que NAT NO ESTÉ ACTIVADA para la interfaz de conexión a la red interna (seleccione las propiedades de esa interfaz en la tabla de interfaces)
4. Compruebe que NO se haya configurado NINGUNA pasarela en las propiedades TCP/IP de la NIC interna (bajo Configuración de la red) y que se haya asignado una dirección IP interna a la NIC.
5. Compruebe que el enlace NIC hacia Internet se haya configurado correctamente con los datos de su ISP. Si dispone de una dirección IP asignada dinámicamente, deje en blanco los ajustes de la dirección IP.

Para más detalles sobre otras configuraciones de red, vea los capítulos correspondientes (p. ej., ***lista de control*** , ***configuración IP*** , etc.)

Modem de cable unidireccional (modem ascendente, cable descendente)

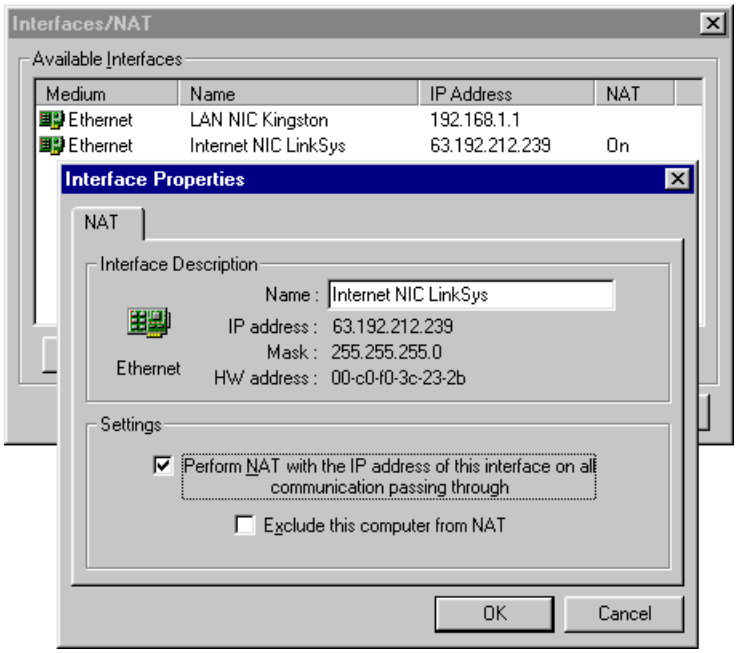
NOTA: Este tipo de conexión a Internet **no es una "configuración soportada oficialmente"** ya que los ajustes **pueden variar** de un ISP a otro. No obstante, intentamos ofrecer soluciones de acceso para la mayor cantidad de escenarios posible. Muchos de nuestros usuarios han tenido éxito al establecer la comunicación con la siguiente configuración.

En general, el flujo de datos es **similar al de Direc PC**. Los paquetes salientes fluyen a través de su interfaz **de conexión por marcación**. Cuando los paquetes regresan, se encaminan **a través de un cable**. En realidad, su proveedor de servicios de Internet (ISP) debe asociar sus dos interfaces para que trabajen juntas. Esto suena a truco, pero es la única forma de establecer una conexión con éxito. Por tanto, le recomendamos que aclare este punto con su ISP antes de decidirse a comprar el software WinRoute.



1. Seleccione *Configuración->Tabla de Interfaces*. A continuación verá una interfaz de **línea RAS** (su modem) y dos interfaces de **tarjeta de red** - una que conecta a Internet y otra que conecta a su red local

2. Haga clic en la interfaz de tarjeta de red que conecta a Internet y seleccione *"Propiedades."* Marque la opción ACTIVADA en *"Ejecutar NAT con dirección IP de la interfaz en todas las comunicaciones que pasen."*



3. Haga clic en la **interfaz RAS** y seleccione *"Propiedades."* Marque la opción ACTIVADA en *"Ejecutar NAT con la dirección IP de la interfaz en todas las comunicaciones que pasen"*. En la **pestaña RAS** seleccione la conexión que usará para conectarse con su ISP, e introduzca su nombre de usuario y contraseña.

4. Compruebe que NAT **NO ESTÉ ACTIVADA** para la interfaz que conecta a la red interna (seleccione las propiedades de esta interfaz)

5. Compruebe que no se haya establecido **NINGUNA pasarela** en las propiedades TCP/IP de la NIC interna (en la configuración de la red) y que se haya asignado a la NIC una **dirección IP** de clase privada (p. ej., 10.10.1.1).

6. Compruebe que la NIC que conecta a Internet se haya configurado correctamente con los datos de su ISP (propiedades TCP/IP.) Nota: si dispone de una dirección IP asignada dinámicamente, deje en blanco los ajustes de la dirección IP.

- ***Por regla general, la NAT debería estar "ACTIVADA" en las dos interfaces que conectan a Internet - RAS y conexión por marcación.***

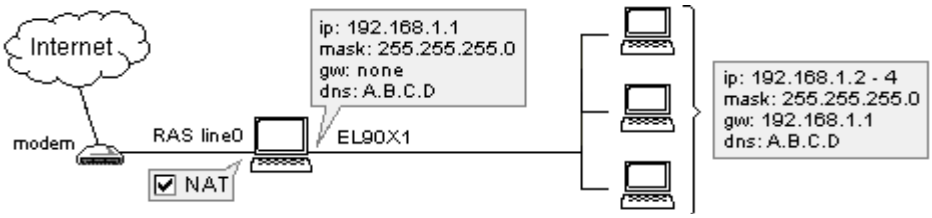
Conexión por marcación o RDSI

Conexión por marcación o RDSI

Si dispone de un acceso de conexión por marcación a Internet (regular de 56K o RDSI) en un PC con el sistema operativo Win95, Win98 o NT4.0 , cumple todos los requisitos para ejecutar WinRoute. WinRoute debe funcionar en un computador que disponga de:

- un modem conectado a la línea telefónica o RDSI

- una tarjeta de interfaz de red (Network Interface Card, NIC) que conduzca a la red interna.



En caso de que disponga de un modem RDSI conectado a su computador mediante una tarjeta Ethernet, vea el capítulo Conexión mediante DSL . En ese caso debe configurar a WinRoute para que trabaje con dos tarjetas Ethernet.

Antes de la conexión

Antes de conectarse a Internet, compruebe lo siguiente:

- · el protocolo TCP/IP está instalado y configurado correctamente (ver la lista de control o el capítulo Configuración de la red)
- · el servicio de Acceso telefónico a redes (Windows 95/98) o el servicio RAS (WindowsNT) está instalado y configurado
- · el modem está enchufado en el computador host WinRoute.

WinRoute utiliza los servicios Acceso telefónico a redes o RAS de su sistema operativo para la conexión a Internet.

Le recomendamos que conecte a Internet el computador en el que instalará WinRoute ANTES de instalar y ejecutar WinRoute, para que quede garantizado que la conexión esté configurada correctamente y que el Acceso telefónico a redes o el servicio de acceso remoto RAS funcionen sin problemas.

Configuración de WinRoute

Una vez que haya realizado la configuración descrita arriba:

1. Seleccione el menú Configuración->Tabla de interfaces -debería ver todas las interfaces de red disponibles en su computador. En WinRoute, las interfaces de conexión por marcación se denominan RAS (tanto para los sistemas operativos 95/98 como NT).
2. Seleccione las Propiedades de la interfaz RAS seleccionada
3. Marque la casilla "Ejecutar NAT con la dirección IP de esta interfaz en todas las comunicaciones que pasen"
4. Seleccione la tabla RAS en el diálogo Propiedades, elija o cree su conexión y configure las opciones según sus requerimientos. Vea la tabla RAS para más detalles.

- ***¡Recuerde! NAT debe marcarse como "ACTIVADA" en la interfaz RAS, pero permanecer "SIN SER MARCADA" en la interfaz(ces) que conecta a la red interna.***

Configuración de la interfaz Ethernet

1. A la tarjeta de interfaz de red que conduce a la red interna se le ha asignado una dirección IP (de clase privada), pero NO se le ha asignado NINGUNA pasarela.
2. Las entradas DNS usadas para esta interfaz se basan en los datos de su ISP. Si su proveedor de servicios no le ha suministrado estos datos, diríjase a él y solicítelos.

Puede configurar a WinRoute para que ponga a disposición la facilidad de marcación a petición, mediante la cual la conexión se establece automáticamente en base al tráfico (datos) saliente de la red local. Para más detalles, haga clic aquí.

Conexión AOL

Mediante WinRoute Pro puede conectar su red a Internet a través de una sola cuenta de conexión por marcación de AOL. Nota: AOL soporta solamente computadores Win95/98. Para conectarse a través de AOL, siga los siguientes pasos:

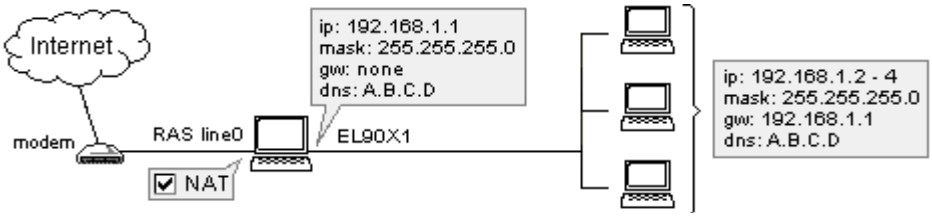
1. Instale un cliente AOL (preferiblemente AOL 5.0 o superior)
2. Conéctese a Internet para garantizar que la conexión funcione correctamente
3. Instale WinRoute Pro
4. En la Administración WinRoute seleccione el menú *Configuración->Tabla de Interfaces*
5. Debería ver el adaptador de AOL entre las interfaces disponibles. Haga clic en las propiedades de esa interfaz y elija "Ejecutar NAT" en esa interfaz.

Configure su computador WinRoute y los clientes de conformidad con la lista de control (ver el capítulo respectivo).

- ***Nota: No funcionará la facilidad de marcación a petición. Debe iniciar la conexión a AOL manualmente.***

Conexión T1 o LAN

Para las conexiones T1 o LAN se requieren dos tarjetas de interfaz de red (Network Interface Card, NIC) instaladas en el computador WinRoute. Una NIC es el enlace hacia Internet (p. ej., enrutador), y la otra el enlace hacia la red interna.



Para conectarse a Internet:

1. Seleccione el menú Configuración->Tabla de Interfaces
2. Seleccione la NIC que conecta a Internet, haga clic en Propiedades y marque la opción ACTIVADA en "Ejecutar NAT con la dirección IP de la interfaz en todas las comunicaciones que pasen". Cuando se abra el cuadro de diálogo de la tabla de interfaces, verá NAT ACTIVADA junto a esa línea externa.
3. Compruebe que NAT NO ESTÉ ACTIVADA en la interfaz que conecta a la red interna (seleccione las propiedades de esa interfaz en la tabla de interfaces)
4. Compruebe que no se haya establecido NINGUNA pasarela en las propiedades TCP/IP de la NIC interna (en la configuración de la red) y que se haya asignado a la NIC una dirección IP interna.

5 Compruebe que la NIC que conecta a Internet se haya configurado correctamente con los datos de su ISP. En caso de que disponga de una dirección IP asignada dinámicamente, deje los ajustes de la dirección IP en blanco.

Para más detalles sobre otras configuraciones de red, vea los capítulos respectivos, especialmente la ***Lista de control*** .

Conexión DirecPC

DirecPC utiliza un modem (analógico, RDSI, ...) o una NIC (Ethernet, Token Ring) para el enlace ascendente, y una antena parabólica para descargar datos. Puede elegir entre una conexión a Internet puesta a disposición por la compañía DirecPC, o seguir usando una conexión por marcación existente de su proveedor.

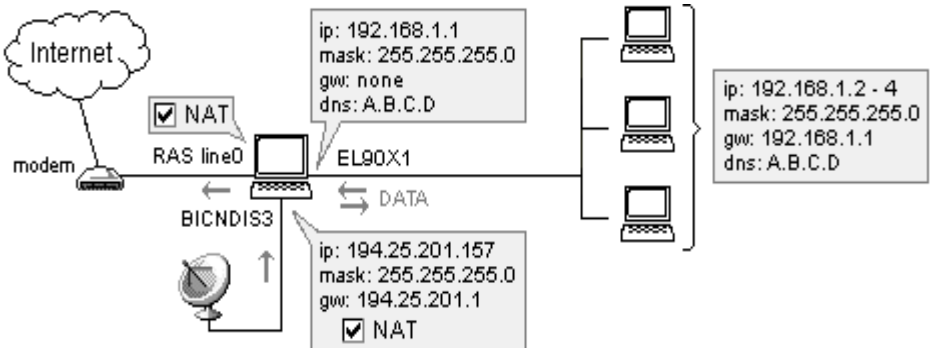
Los datos se dirigen, a través de modem, desde su computador hasta el servicio Internet de DirecPC, desde donde son encaminados hacia su destino final. En la otra dirección, DirecPC asocia los paquetes (datos) dirigidos a su computador con otros datos, para encaminarlos a través de una antena parabólica.

Configuración de WinRoute

En primer lugar, debe instalar correctamente todo el software y los componentes de DirecPC. Después puede configurar a WinRoute según sus requerimientos específicos.

A continuación puede elegir entre el dialer de DirecPC o WinRoute RAS para el enlace ascendente. Si utiliza WinRoute se beneficiará de la facilidad de marcación a petición y ahorrará dinero durante sus conexiones.

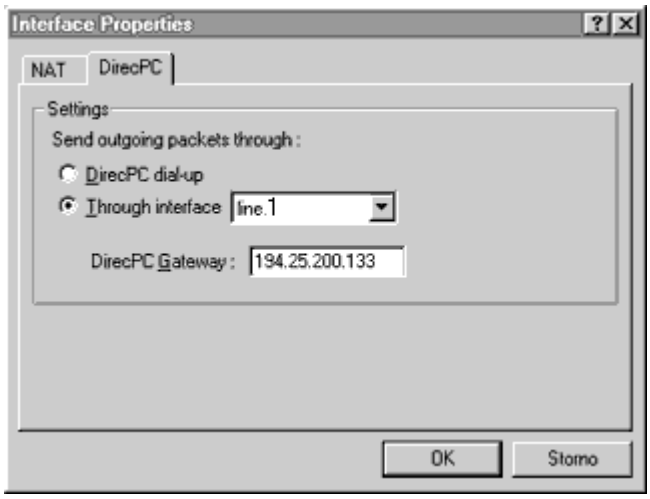
1. Utilizar la línea RAS para el enlace ascendente



Seleccione el menú *Configuración->Tabla de Interfaces*. Podrá ver la interfaz de línea RAS (su modem) y la tarjeta de interfaz de DirecPC.

Haga clic en la tarjeta de interfaz de DirecPC y seleccione "Propiedades". Verá dos pestañas - **NAT** y **DirecPC**.

- En la pestaña NAT marque la opción ACTIVADA en *"Ejecutar NAT con la dirección IP de la interfaz en todas las comunicaciones que pasen"*.
- En la pestaña DirecPC seleccione que utilizará *line0* como enlace ascendente. Introduzca la *dirección IP de la pasarela (gateway)* que le haya sido suministrada por DirecPC.

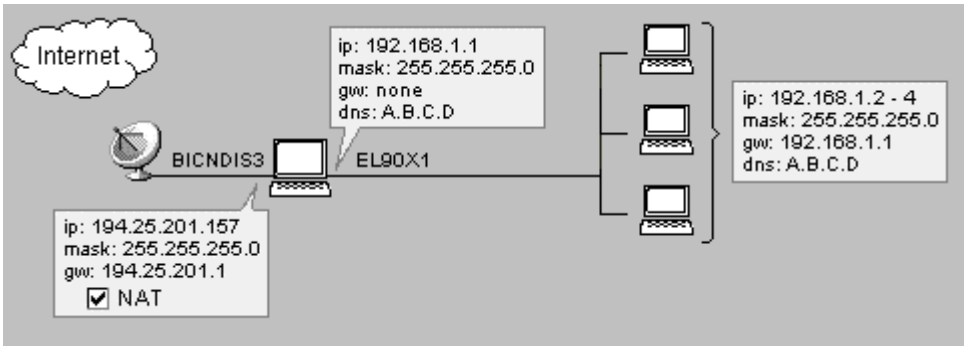


3.Haga clic en la interfaz RAS y seleccione "Propiedades". Marque la opción ACTIVADA en "Ejecutar NAT con la dirección IP de la interfaz en todas las comunicaciones que pasen". En la pestaña RAS seleccione la conexión que usará para conectarse a su proveedor y, a continuación, introduzca su nombre de usuario y su contraseña.

- ***Nota: Debe DESMARCAR la opción "Usar la pasarela por defecto en la red remota" en las propiedades de la cuenta creada para conectarse a su ISP. Configure esta opción en las propiedades TCP/IP de su interfaz de conexión por marcación.***

2. Usar el dialer de DirecPC para el enlace ascendente

Puede utilizar el dialer integrado de DirecPC, si está disponible. No obstante, le recomendamos que emplee la línea RAS de WinRoute siempre que sea posible.



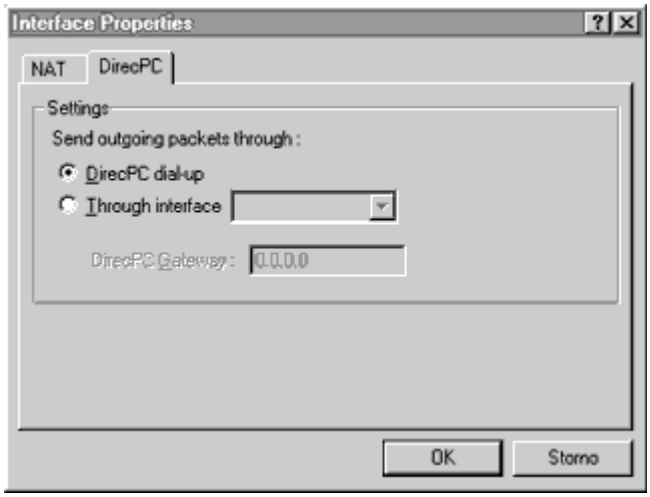
Para usar el dialer de DirecPC:

Seleccione el menú *Configuración->Tabla de Interfaces*. Podrá ver la interfaz de la línea RAS (su modem) y la tarjeta de interfaz de DirecPC

Haga clic en la tarjeta de interfaz de DirecPC y seleccione "*Propiedades*". Allí verá dos pestañas - NAT y DirecPC.

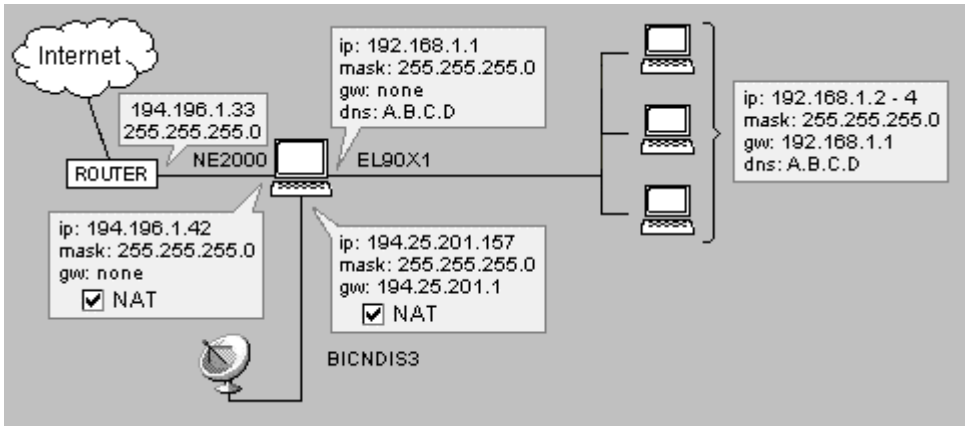
- En la pestaña NAT marque la opción ACTIVADA en "*Ejecutar NAT con la dirección IP de la interfaz en todas las comunicaciones que pasen*".

- En la pestaña DirecPC seleccione "*Usar el dialer DirecPC para el enlace ascendente*".

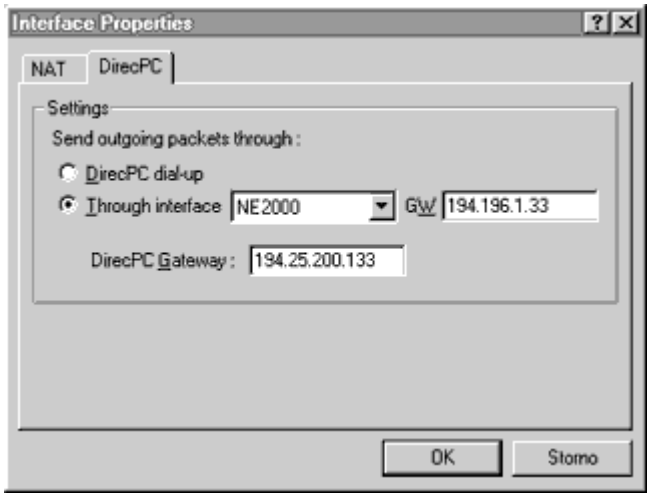


3. Utilizar la interfaz Ethernet para el enlace ascendente

Es posible que en algunos casos desee emplear la interfaz Ethernet para el enlace ascendente. Esto ocurre, típicamente, cuando el enlace ascendente se realiza sobre la conexión RDSI (y se dispone de un enrutador o modem RDSI) o sobre una conexión V-SAT (antena parabólica con adaptador Ethernet).



Seleccione el diálogo de las propiedades de la tarjeta de interfaz de DirecPC.



- En la pestaña NAT marque la opción ACTIVADA en "*Ejecutar NAT con la dirección IP de la interfaz en todas las comunicaciones que pasen*".
- En la pestaña DirecPC seleccione "*A través de interfaz*" y seleccione la interfaz que conecta a Internet. A continuación, introduzca la pasarela por defecto de su ISP en el campo "GW" (p. ej., 194.196.1.33).

Incrementar el flujo de datos

Para obtener el mayor flujo de datos posible mientras esté conectado a Internet a través de DirecPC, reduzca el tamaño de la **ventana de recepción TCP** en todos los computadores que usarán DirecPC:

En Windows NT:

1. Seleccione el registro HKEY_LOCAL_MACHINE\SYSEM\CurrentControlSet\Services\Tcpip\Parameters
2. Agregue (si ya existe, edítela) una entrada denominada "TcpWindowSize" (es del tipo DWORD) al registro. Ajuste su valor en 0xBB80.

En Windows 95:

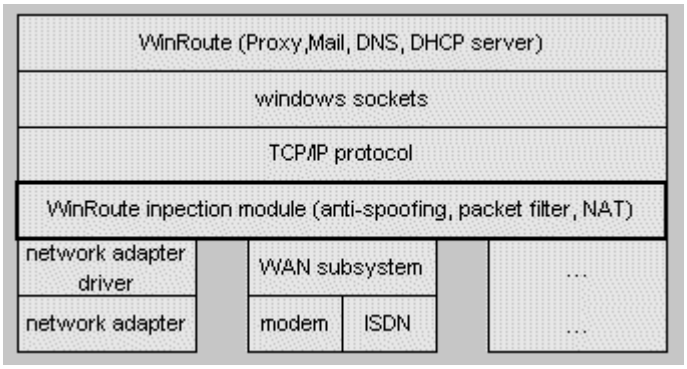
1. Seleccione el registro HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\MSTCP.
2. Agregue (si ya existe, edítela) una entrada denominada "DefaultRcvWindow" (es del tipo cadena) al registro. Ajuste su valor en "0xBB80".

Configurar la Seguridad

En Esta Sección

Seguridad NAT

WinRoute ejecuta las operaciones NAT en la capa de protocolo de conexión en red más baja posible. WinRoute controla el tráfico entre el controlador de la NIC (tarjeta de interfaz de red) y la pila TCP. WinRoute dispone de un control total sobre el tráfico de Internet y captura tanto los paquetes salientes como los entrantes, minimizando así las posibilidades de ser burlado. Ésta es una facilidad especial de la implementación NAT de WinRoute. Adicionalmente, ofrece ampliaciones de seguridad, tales como un cortafuegos basado en el filtro de paquetes o una facilidad anti-interferencia. Con la función NAT de WinRoute, la red completa está totalmente protegida, inclusive el computador en el que funciona WinRoute.



Opciones de Seguridad NAT

En la configuración avanzada de WinRoute a partir del build 20, se ofrece un menú de opciones de seguridad NAT que incorpora un **modo silencioso**. **Modo silencioso** significa que WinRoute puede "soltar" paquetes para tipos especiales de peticiones, de forma que su red sea invisible hacia el exterior.

Petición de eco ICMP entrante:

El protocolo de mensaje de control de Internet (Internet Control Message Protocol, ICMP) es el protocolo utilizado para transmitir una petición de información (transmitir ping, por ejemplo, ping206.86.211.32). Cuando cualquier computador transmite un **ping** al host WinRoute, las **Opciones de Seguridad NAT** ofrecen dos posibilidades:

- Si selecciona *"transmitir respuesta de eco ICMP"*, el computador solicitante recibirá una respuesta.
- Si selecciona *"soltar petición (modo silencioso)"*, el datagrama se suelta y simplemente se pierde en el tránsito. El computador solicitante recibe entonces el mensaje *"no se puede acceder al host de destino."*

Paquetes entrantes sin ninguna entrada en la tabla NAT:

WinRoute examina todo el tráfico que entra y que sale de la LAN. Independientemente de si WinRoute debe ejecutar NAT o no para un paquete específico, primero examina el paquete y registra determinada información, como el número de puerto y la dirección IP, en una tabla NAT. Así, cuando el paquete regresa, WinRoute puede compararlo con la tabla NAT para determinar hacia dónde debe encaminarse dicho paquete. Si el paquete no se ha iniciado en la red, es decir, no es un paquete que regresa, WinRoute lo compara con la tabla NAT y determina que es un paquete no iniciado. Si no se crea ningún mapeo de puerto, WinRoute no puede transmitir el paquete a ningún computador que esté dentro de la LAN.

- La opción "enviar paquete denegación" simplemente devuelve el paquete al emisor, indicándole que no se pudo establecer la conexión.

- La opción “soltar paquete (modo silencioso)" elimina el paquete y no transmite ningún paquete de retorno. De esta forma, se da la impresión de que ni el host WinRoute ni la LAN detrás de él existen.

Paquetes UDP entrantes:

Algunas aplicaciones que usan el protocolo de datagrama de usuario (**User Datagram Protocol**, UDP) le piden que transmita paquetes UDP a un servidor central. WinRoute registra el origen y el destino de todos los paquetes UDP que salen hacia el servidor asignado por la aplicación que envía el paquete. En algunos casos, el servidor transfiere su dirección IP y su puerto a otro computador, el mismo que envía entonces un paquete UDP con la información que usted haya solicitado. Aun cuando ese computador aleatorio tenga una dirección IP diferente a la del servidor, puede transmitir paquetes UDP a su red, ya que conoce la dirección IP y el puerto que usted está utilizando.

- Si en el ejemplo de arriba usted selecciona “*puede pasar por NAT con cualquier dirección IP de origen*”, el paquete UDP pasará a través de WinRoute.
- Para aumentar la seguridad, puede seleccionar “*puede pasar por NAT sólo si proviene de la dirección IP de origen que se registró al enviarse el primer paquete saliente de LAN.*” De esta forma, sólo los paquetes UDP provenientes del servidor central podrán pasar por WinRoute.

Opciones de registro NAT:

En el marco de las opciones de seguridad avanzada, se puede registrar información de paquetes que entran en la LAN y que no fueron originalmente pedidos por nadie desde dentro de la LAN. Esto atañe, principalmente, a las redes en las que funcionan servidores Web, FTP, DNS u otro tipo de servidores detrás de WinRoute, y es una facilidad útil para determinar la causa de un problema.

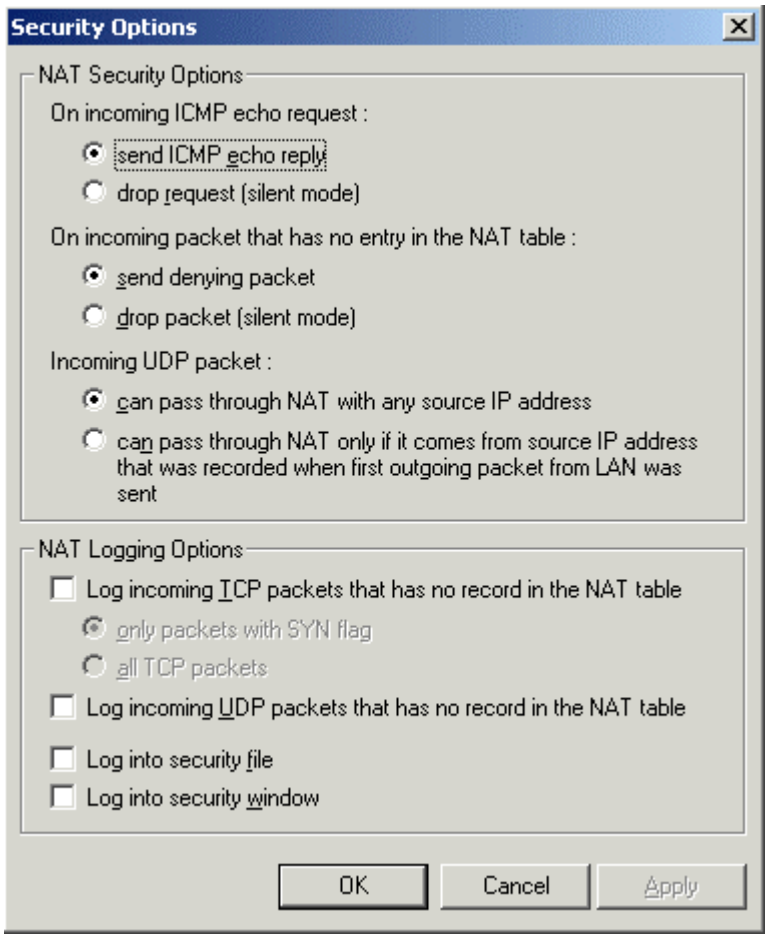
Resgistrar paquetes entrantes sin ninguna entrada en la tabla NAT:

WinRoute le ofrece dos opciones para registrar paquetes TCP que no se encuentran en la tabla NAT.

- Si decide registrar "*sólo paquetes con bandera SYN*" (de sincronización), el paquete TCP sólo se registra si se establece previamente una conexión entre el transmisor y el receptor.
- Mediante la opción "*todos los paquetes TCP*" se registran todos los paquetes TCP entrantes, independientemente de si se establece o no una conexión. Dado que los paquetes UDP no utilizan banderas, se registran todos los paquetes UDP no iniciados cuando selecciona el registro de paquetes UDP.

Registrar en un fichero o en una ventana:

- Si selecciona "*registrar en ventana de seguridad*" puede ver la información de registro desde la aplicación Administración WinRoute, especificando ver-registros-registro seguridad.
- Si selecciona "*registrar en fichero*", WinRoute guarda la información de registro en el registro de seguridad ubicado en la carpeta registros de WinRoute Pro (típicamente c:/Archivos de programa/WinRoute Pro/Registros)


Security Options
NAT Security Options
On incoming ICMP echo request :
send ICMP echo reply
drop request (silent mode)
On incoming packet that has no entry in the NAT table :
send denying packet
drop packet (silent mode)
Incoming UDP packet :
can pass through NAT with any source IP address
can pass through NAT only if it comes from source IP address that was recorded when first outgoing packet from LAN was sent
NAT Logging Options
Log incoming TCP packets that has no record in the NAT table
only packets with SYN flag
all TCP packets
Log incoming UDP packets that has no record in the NAT table
Log into security file
Log into security window
OK
Cancel
Apply

Configuración del Filtro de Paquetes

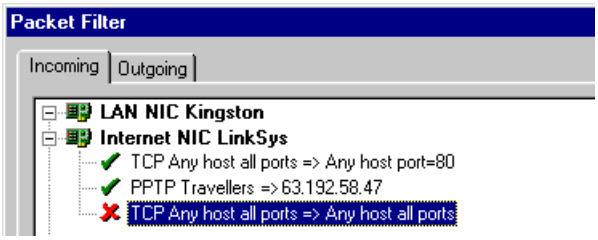
La configuración de la porción de filtro de paquetes del cortafuegos de WinRoute Pro es muy sencilla. No obstante, es necesario entender cabalmente la lógica en la que se basa la funcionalidad de filtro de paquete que se aplica en WinRoute.

Reglas establecidas para la interfaz

Los usuarios pueden definir reglas de seguridad individuales para las diferentes interfaces de computador de sus ordenadores. Esta es una facilidad muy importante cuando se administran redes de segmentos múltiples.

Ejemplo: en la siguiente figura se muestra el ejemplo de una red que:

- *permite cualquier acceso desde Internet al servidor web ubicado dentro de la red*
- *sólo permite que algunos miembros del grupo de direcciones predefinido, denominado Travellers, accedan al servidor PPTP ubicado dentro de la red, para acceder así a la red*



Reglas diferentes para los paquetes salientes y los paquetes entrantes

WinRoute aplica reglas específicas a los paquetes salientes y a los paquetes entrantes. Se crea una tabla para cada interfaz dentro de WinRoute. En esa tabla se registran tanto los paquetes entrantes como los salientes. En otras palabras, cada paquete dispone de dos entradas: una para la salida y una para la entrada.

¿Qué son paquetes SALIENTES/ENTRANTES?

WinRoute siempre considera a su motor como la pieza básica de todo el sistema. Esto significa que todos los paquetes que salen de WinRoute son SALIENTES, sin importar si se dirigen a Internet o a la LAN. De forma similar, todos los paquetes que LLEGAN al PC WinRoute son ENTRANTES, independientemente de su origen. Por favor, tenga en cuenta este punto al crear reglas de seguridad.

APLICAR LAS REGLAS:

De INICIO a FIN

Las reglas se definen en una lista y se aplican desde el principio hasta el final. Una vez que el paquete llega a la interfaz, se controla según la lista de criterios definidos. La comprobación empieza por el primer criterio de la lista y va bajando hasta el último criterio de la misma. Cuando el paquete coincide con los criterios, la regla en cuestión se aplica y las demás reglas se omiten.

Las reglas pueden aplicarse a:

- usuarios individuales
- un rango de direcciones IP
- un grupo de direcciones IP definido por el usuario (para más informaciones sobre cómo definir un grupo de usuarios, vea la parte respectiva de este manual)

- la subred o red completa

Las reglas pueden aplicarse en zonas de tiempo predefinidas

En algunos casos, puede resultar útil aplicar reglas específicas durante horas de oficina, y criterios diferentes para los accesos fuera de esas horas. O talvez desee permitir que algunos usuarios accedan a la red durante la hora de almuerzo o durante el horario de trabajo, o sólo permitir el acceso a recursos específicos durante horas determinadas.

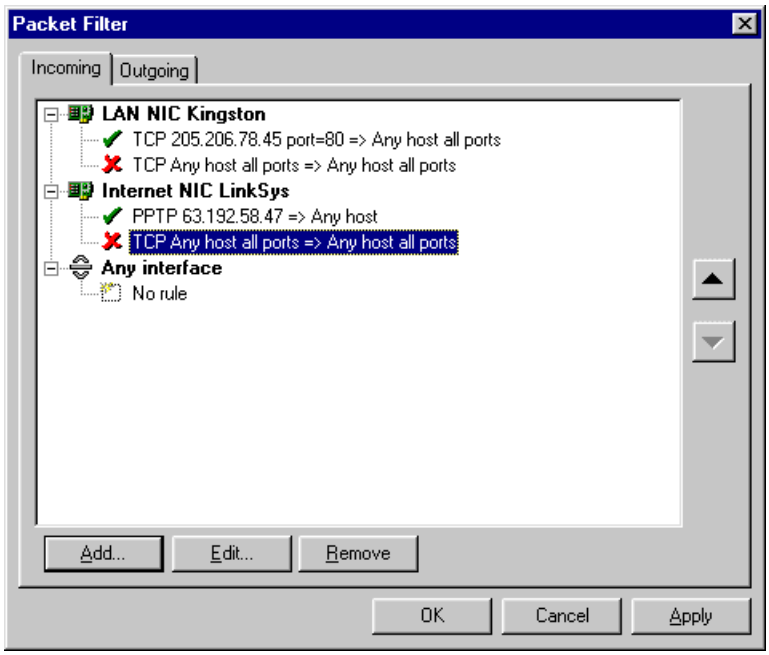
Ejemplo:

Control total de los accesos de los usuarios: el administrador de la red desea que sólo los usuarios a los que se les ha concedido acceso tengan los derechos correspondientes. No obstante, muchas configuraciones de red tienen servidores Web o FTP detrás del sistema WinRoute, que requieren acceso público.

En el ejemplo de arriba, las reglas se establecerían en el siguiente orden para los paquetes entrantes.

1. Permitir el acceso de los paquetes de cualquier host dirigidos al puerto 80
2. Permitir el acceso de los paquetes de cualquier host dirigidos al puerto 21
3. Denegar el acceso de todos los paquetes

Cuando el paquete entrante cumple con la regla 1. ó 2., se le permite pasar y no se aplica la regla 3. Si no cumple con 1 ó 2, se le deniega el acceso.



Ejemplo de Conjunto de Reglas Básicas de Filtro de Paquete

Reglas entrantes (cerciórese de que estén ordenadas de esta forma)

Protocolo	Origen	Destino	Tipos ICMP	Acción	Registro	
UDP	Cualquier dirección, puerto = 53	Cualquier dirección, puerto > 1023		Permitir		
TCP	Cualquier dirección, cualquier puerto	Cualquier dirección, puerto > 1023		Permitir TCP establecido		
ICMP	Cualquier dirección	Cualquier dirección	Respuesta eco	Permitir		
IP	Cualquier dirección	Cualquier dirección		Soltar	En ventana	

Nota: Esta última regla interferirá con cualquier herramienta de captura de paquetes que se use en ese host.

Ejemplo de Conjunto de Reglas Básicas de Filtro de Paquete para HTTP y FTP entrante

Protocolo	Origen	Destino	Tipos ICMP	Acción	Registro	De
TCP	Cualquier dirección, cualquier puerto	[este host], puerto = 80		Permitir	(opcional)	Per ent hos
TCP	Cualquier dirección, cualquier puerto	[este host], puerto = 21		Permitir	(opcional)	Per ent
TCP	Cualquier dirección, cualquier puerto	[este host], puerto = 20		Permitir	(opcional)	Per ent FT req pue rec

Permitir la comunicación en determinados puertos

Desea aplicar las siguientes reglas:

- máxima seguridad
- permitir el acceso a su servidor web
- permitir la comunicación hacia su servidor SMTP

- permitir que su correo electrónico de Internet se recoja en su Servidor de Correo
- permitir el acceso a su servidor FTP

Máxima seguridad:

Pestaña Entrante

Protocolo: TCP, Denegar el acceso de todos los paquetes entrantes

IP de origen - Cualquiera	IP de destino - Cualquiera
Puerto de origen - Cualquiera	Puerto de destino - Cualquiera

Esta regla será siempre la más baja de las disponibles en la interfaz.

Permitir el acceso a su servidor web desde Internet:

Pestaña Entrante

Protocolo: TCP

IP de origen - Cualquiera	IP de destino - dirección IP del servidor web
Puerto de origen - Cualquiera	Puerto de destino - 80

Permitir el acceso de determinadas direcciones a su servidor FTP desde Internet.

Pestaña Entrante

Protocolo: TCP

IP de origen - Cualquiera	IP de destino - dirección IP del servidor FTP
Puerto de origen - Cualquiera	Puerto de destino - 21

IP de origen - Cualquiera	IP de destino - dirección IP del servidor FTP
Puerto de origen - Cualquiera	Puerto de destino - 20

Permitir que su servidor SMTP se comunique sólo a través del servidor SMTP de retransmisión (del proveedor de servicios):

Pestaña Entrante

Protocolo: TCP

IP de origen - servidor SMTP de retransmisión del ISP	IP de destino - dirección IP del servidor SMTP de su LAN
Puerto de origen - Cualquiera	Puerto de destino - 25

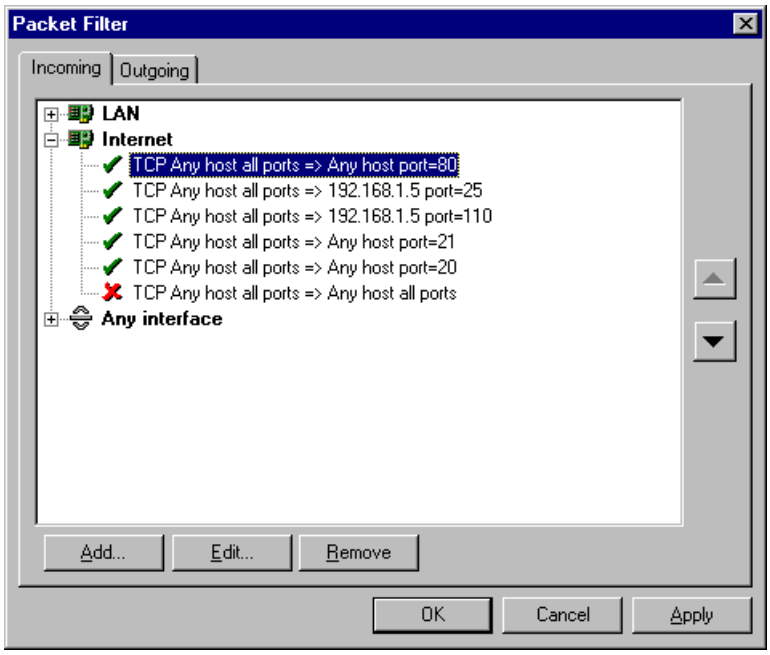
Pestaña Saliente

IP de origen - su servidor SMTP	IP de destino - dirección IP del servidor SMTP del ISP
Puerto de origen - Cualquiera	Puerto de destino - 25

Permite recoger correo electrónico proveniente de Internet en su Servidor de Correo

Pestaña entrante

IP de origen - su servidor SMTP	IP de destino - dirección IP del servidor SMTP de su LAN
Puerto de origen - Cualquiera	Puerto de destino - 110


Packet Filter
Incoming
Outgoing
LAN
Internet
TCP Any host all ports => Any host port=80
TCP Any host all ports => 192.168.1.5 port=25
TCP Any host all ports => 192.168.1.5 port=110
TCP Any host all ports => Any host port=21
TCP Any host all ports => Any host port=20
TCP Any host all ports => Any host all ports
Any interface
Add...
Edit...
Remove
OK
Cancel
Apply

Forzar a los usuarios a utilizar el Servidor Proxy

En algunas ocasiones puede resultar conveniente utilizar el **Servidor Proxy integrado** de WinRoute. Esto es útil si desea **supervisar** la actividad de los usuarios cuando éstos acceden a sitios web o si desea **aplicar restricciones** a clientes que acceden a determinados sitios web, o si desea que los clientes usen la **memoria caché**.

- ***Nota: Puede utilizar el** filtro de paquetes **para controlar el tráfico web; no obstante, es más fácil emplear el** filtro URL proxy integrado**, ya que resuelve los nombres de dominio, es decir, basta con introducir las URL en vez de las direcciones IP asociadas.***

Configuración:

Debe crear dos reglas de seguridad para paquetes **salientes**:

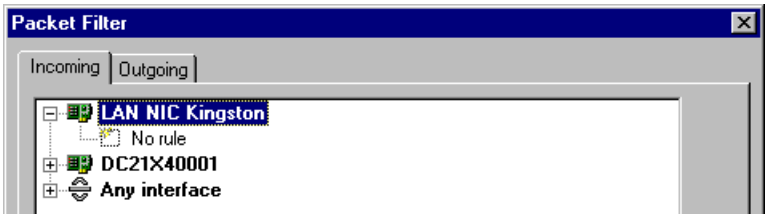
1. **Permitir** los paquetes salientes con el *puerto de destino 80 y la IP de origen* del host WinRoute
2. **Denegar** todos los paquetes salientes con el *puerto de destino 80*

Las reglas deben aplicarse en el orden exacto indicado arriba. WinRoute aplica las reglas de **arriba hacia abajo**. Las reglas se aplican según el principio de "se sirve primero al que llega primero", es decir, el paquete entrante se compara con las reglas en el orden en que aparecen en la lista, de arriba hacia abajo. Se aplica la primera regla que coincide con la descripción del paquete y se omite el resto de reglas.

Para configurar reglas:

1. En WinRoute Administrator seleccione el menú *Configuración=>Avanzada=>Filtro Paquetes*, y después, la pestaña *Saliente*.

2. Haga doble clic en su interfaz externa (Internet). Se presenta la lista de reglas o el mensaje "Ninguna regla".



3. Pulse el botón *Agregar* para agregar una nueva regla que permitirá al host WinRoute establecer conexiones con servidores web en el puerto 80.

Seleccione Protocolo: TCP

Tipo de Origen: Host

Dirección IP: la dirección externa de su cortafuegos WinRoute (p. ej., 204.23.43.26)

Puerto de Destino: Igual a (=) 80, bajo Acción: seleccione Permitir.

4. Pulse nuevamente el botón *Agregar* para agregar una segunda regla que denegará todas las demás conexiones TCP dirigidas al puerto 80.

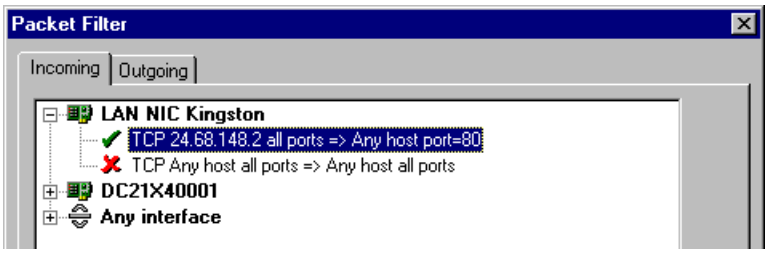
Seleccione Protocolo: TCP

Tipo de Origen: Cualquiera

Puerto de Destino: Igual a (=) 80

Acción: Denegar.

Si desea registrar los intentos de conexión, marque la casilla de verificación Registrar en fichero.



- ***NOTA: Cuando configure reglas adicionales, no olvide crear las reglas de ARRIBA hacia ABAJO (prioridad).***

Configurar el Servidor de Correo

En Esta Sección

Usuarios del correo

En WinRoute existen varias reglas básicas referentes a los usuarios, a las direcciones de correo electrónico y a los buzones.

Un usuario = Un buzón...

Para cada usuario de WinRoute se crea un **buzón**. El buzón asume el nombre del usuario. En caso de que disponga de un dominio de Internet registrado y lo haya introducido en WinRoute, la dirección de correo electrónico del usuario será, automáticamente, usuario@dominio.com.

Un usuario = Más direcciones

Para utilizar diferentes direcciones de correo electrónico y crear buzones generales, tales como ventas@..., soporte@...., info@... puede definir alias. Las combinaciones son, prácticamente, ilimitadas.

Para agregar usuarios:

1. Seleccione el menú **Configuración=>Cuentas**
2. Agregue **Usuarios**
3. En caso necesario, reúnalos en **Grupos**

Ejemplo:

La compañía dispone del dominio brutus.com. El usuario Juan tendrá la dirección de correo electrónico juan@brutus.com. Para más opciones de direcciones, vea Alias.

- ***Nota: Los buzones se encuentran en un directorio separado. Generalmente, en c:/Archivos de Programa/WinRoute/Correo. Los buzones se crean físicamente DESPUÉS de que llega el primer email.***

Enviar email a otros usuarios de WinRoute en su red

Para enviar mensajes de correo electrónico a otros usuarios **dentro** de su LAN, debe usar el **nombre de usuario de WinRoute** del destinatario, en vez de su **dirección de correo electrónico** completa.

Ejemplo: El nombre de usuario del destinatario es Juan y su dirección email completa es juan@company.com. Sólo debe introducir *juan* en el campo *Para:* del mensaje de correo electrónico.

Alias

Cuando utiliza la **dirección de correo electrónico completa** de un usuario local, el mensaje pasará **a través de** Internet, es decir, al servidor SMTP de retransmisión de WinRoute, y después de vuelta a WinRoute. Para evitar esto, debe especificar alias.

- ***Recuerde: Debe configurar su PC WinRoute como su servidor de correo saliente (SMTP).***

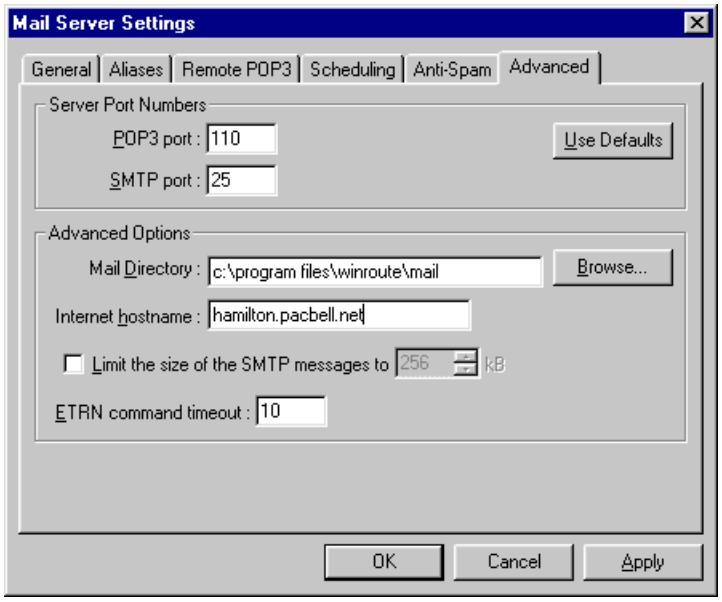
Autentificación

Autentificación

Algunos ISP realizan una autentificación de los mensajes de correo electrónico entrantes para evitar el spamming. Para ello, debe suministrar la información necesaria a su ISP.

1. Vaya a la ventana *Servidor de Correo->Avanzado*

2. Introduzca el **nombre host** que desee en el campo Nombre de host Internet. Por lo general, es el nombre del computador conectado a Internet, p. ej., *host.isp.com*.



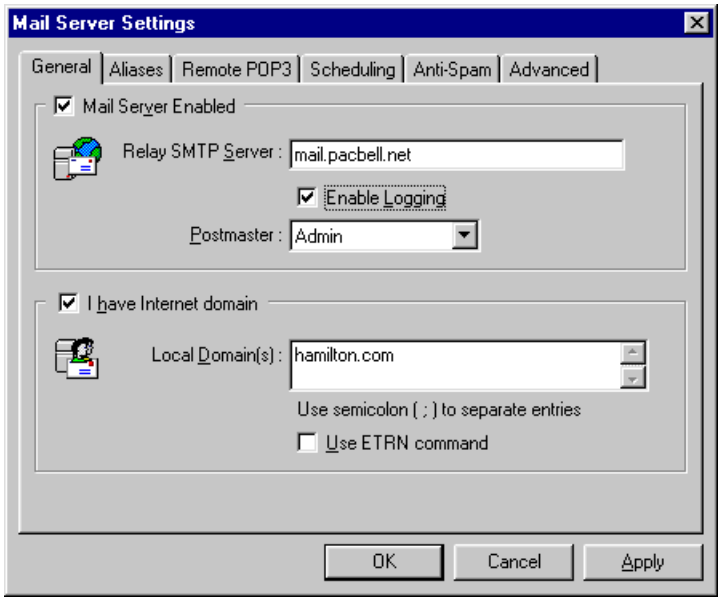
Enviar mensajes Email a Internet

Puede utilizar a WinRoute como su **servidor SMTP** para el correo saliente. WinRoute usa el **servidor SMTP de retransmisión** de su ISP para transmitir mensajes de email hacia el exterior de la red, en vez de usar registros MX. En otras palabras, todo el correo electrónico saliente se transmite mediante el otro servidor de correo que introduzca (por lo general, el servidor de correo de su proveedor de servicios). Las mismas reglas pueden aplicarse a sus clientes de correo electrónico - el servidor de correo de WinRoute puede ser su servidor SMTP de retransmisión.

Para configurar el servidor SMTP de retransmisión para el correo saliente:

1 Seleccione el menú *Configuración=>Servidor de Correo*

2 Introduzca el servidor de correo saliente de su ISP en el campo *Servidor SMTP de retransmisión*

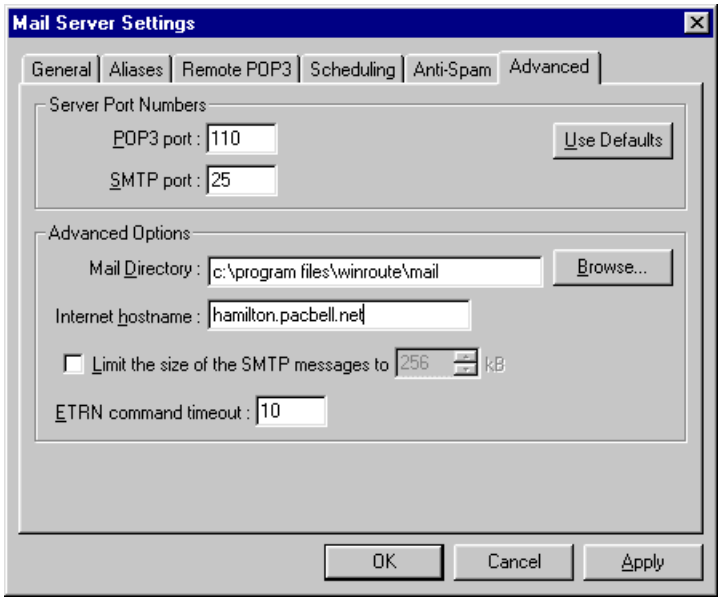


Autentificación

Algunos ISP llevan a cabo una autentificación de los mensajes de email que entran para evitar el spamming. Para ello, debe suministrar la información requerida a su ISP.

1. Vaya a la ventana *Servidor de Correo->Avanzado*

2. Introduzca el **nombre del host** que desee en el campo Nombre de host Internet. Por lo general, es el nombre del computador conectado a Internet, p. ej., *host.isp.com*.



Alias

En WinRout los **Alias** o nombres alternativos se usan para proporcionar direcciones **adicionales** a los usuarios de WinRoute, y también para **sustituir** direcciones de correo electrónico.

Mediante los **alias** puede:

- asignar más direcciones a un usuario
- asignar una dirección de correo electrónico a varios usuarios
- asignar una dirección de correo electrónico a un grupo de usuarios
- asignar varias direcciones a un grupo

Ejemplo:

Este ejemplo muestra que las posibilidades son, prácticamente, ilimitadas.

Supongamos que una compañía tiene 2 dominios:

- compañía.com
- compañía2.com

El usuario *Juan* debe recibir los mensajes de email dirigidos a:

juan_perez@compañía.com

juan@compañía2.com

ventas@compañía.com

soporte@compañía.com

Los mensajes de email dirigidos a *ventas@compañía.com* deben enviarse también al grupo *[Ventas]*.

Solución:

1. Seleccione el menú *Configuración=>Servidor de Correo=>Alias (pestaña)*.

2. Agregue los siguientes alias:

*juan** entregar a *Juan* -

de esta forma, todos los mensajes de email que llegan desde Internet en los que aparezca juan en el nombre del destinatario, es decir, tanto *juan_perez@compañía.com* tomo también *juan@compañía2.com*, se entregarán al usuario *Juan.* De esta manera, se evitará también que el correo electrónico enviado por usuarios locales al destinatario *juan@compañía.com* pase a través de Internet. El correo electrónico se enviará directamente al buzón de Juan en WinRoute.

ventas entregar a *Juan* -

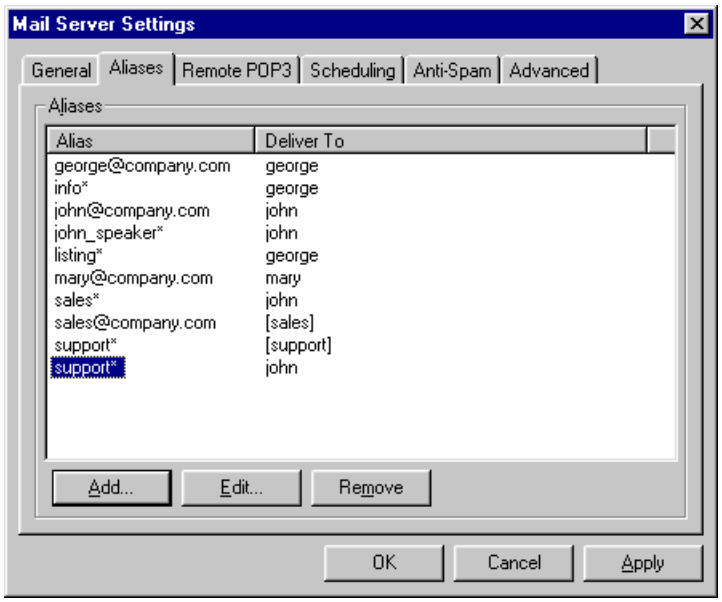
todo el correo electrónico dirigido a *ventas@…….* se entregará al usuario *Juan*

Soporte entregar a *Juan* -

todo el correo electrónico dirigido a *soporte@……* se entregará a *Juan*

Ventas entregar a *[Ventas]* -

el correo electrónico dirigido a *ventas@….* se entregará a todos los miembros del grupo *[Ventas]*



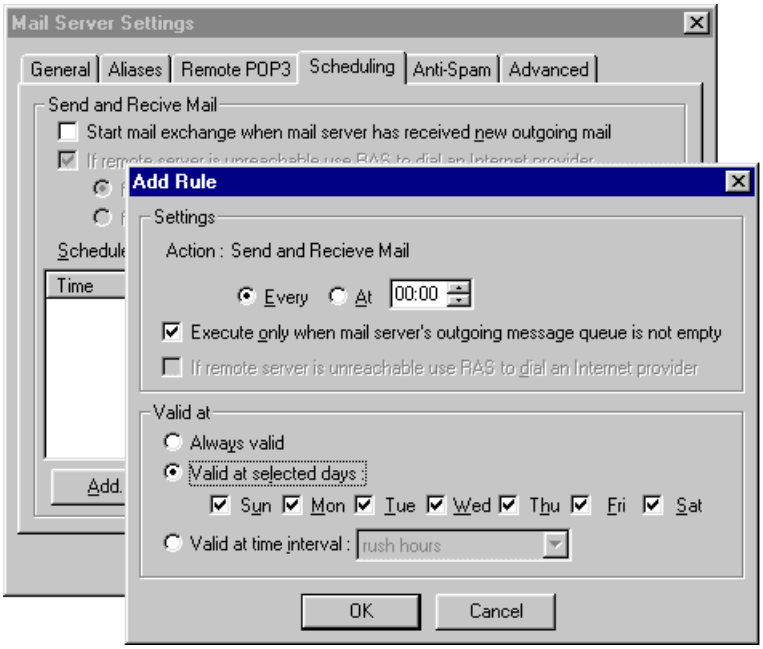
Programar el Intercambio de Correo Electrónico

La opción Programación en los ajustes del servidor de correo le permite configurar:

- intervalos regulares para controlar si hay correo electrónico en el servidor de su ISP (POP3 o SMTP, usando ETRN)
- reglas para enviar correo electrónico fuera de la red
- los intervalos de tiempo en los cuales son válidas las reglas. Puede predefinir los intervalos de tiempo en el menú *Configuración->Avanzada->Intervalos de Tiempo*

Puede elegir si desea transmitir los nuevos mensajes de email salientes tan pronto lleguen al servidor de correo, o si desea transmitirlos en periodos de tiempo predefinidos.

También puede decidir si el servidor de correo debe establecer o no una comunicación cuando existen nuevos mensajes de email salientes. Cuando selecciona esta opción, el servidor de correo de WinRoute establece una conexión cada vez que sus usuarios envían nuevos mensajes de correo electrónico.



Para recibir correo electrónico puede especificar el calendario completo, indicando exactamente cuándo desea recoger su correo. Puede combinar diferentes reglas para garantizar que la recuperación de su correo sea lo más eficiente posible.

1. Seleccione el menú *Configuración->Servidor de Correo->Programación*
2. Especifique las opciones que desee y agregue nuevas reglas para controlar el correo electrónico.

- ***Nota: Las reglas para los "Intervalos de Tiempo" deben configurarse en el menú Configuración->Avanzada->Intervalos de Tiempo***

Recibir correo electrónico

En Esta Sección

Si dispone de un dominio propio (SMTP)

El Servidor de Correo de WinRoute es totalmente compatible con ***SMTP***[1] y ***POP3***[2]. Es posible que haya registrado su propio **dominio Internet** y que reciba correo electrónico a través de SMTP, y/o que WinRoute recoja automáticamente su correo de la cuenta POP3 de su ISP.

---

[1] **SMTP** (Simple Mail Transfer Protocol) se usa para la comunicación directa entre servidores de correo (como, por ejemplo, el servidor de correo de WinRoute y el servidor de correo de su ISP) y para transmitir correo electrónico saliente desde su software cliente de correo electrónico. SMTP es un protocolo de "una vía" - es decir, el servidor de correo puede transmitir o recibir correo, pero no puede recoger el correo electrónico en otro servidor mediante este protocolo.

El protocolo SMTP es un protocolo TCP que funciona en el **puerto 25**. Si desea acceder a este protocolo con el servidor de correo que corre detrás de o sobre el computador WinRoute (para permitir que otro servidor de correo le envíe correo electrónico o para usar este servidor de correo para su email saliente cuando está en su LAN), debe configurar un **mapeo de puerto** para el protocolo TCP, puerto 25 hacia una dirección de **clase privada** del PC sobre el que corre el servidor de correo.

[2] El protocolo **POP3** es usado, en la mayoría de los casos, por el software cliente de correo electrónico para recoger el correo de los buzones, en los servidores de correo compatibles con POP3. El servidor de correo de WinRoute también dispone de esta capacidad, es decir, puede recoger el correo electrónico automáticamente en cualquier servidor de correo compatible con POP3, y distribuirlo a los buzones de los destinatarios locales.

El protocolo POP3 es un protocolo **TCP** que funciona en el **puerto 110**. Si desea acceder al servidor de correo POP3 que funciona detrás del computador WinRoute (para recoger su correo electrónico PROVENIENTE de Internet), debe configurar un **mapeo de puerto** para el protocolo TCP, puerto 110 hacia la dirección IP de **clase privada** del PC sobre el que corre el servidor de correo.

Si dispone de un dominio Internet registrado con su dirección IP externa (pública), WinRoute puede recibir el correo electrónico mediante el protocolo SMTP. Introduzca el nombre del dominio que haya registrado en la pestaña General del cuadro de diálogo del Servidor de Correo.

- ***¡No olvide mapear el protocolo TCP puerto 25 a la dirección IP de clase privada de su cuadro WinRoute! En caso contrario, el protocolo SMTP no podrá pasar por la NAT de WinRoute.***

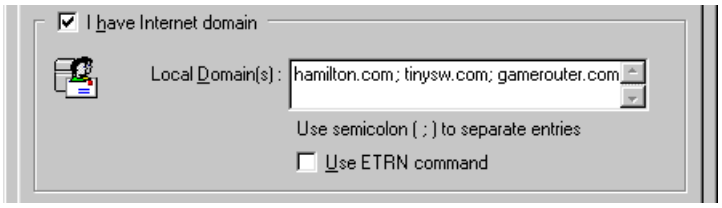
Según el tipo de conexión a Internet del que disponga, tenga en cuenta lo siguiente:

1 Si dispone de una conexión permanente

No se requiere ningún ajuste específico. Sólo debe introducir el dominio(s).

2 Si dispone de una conexión por marcación o RDSI (comando ETRN)

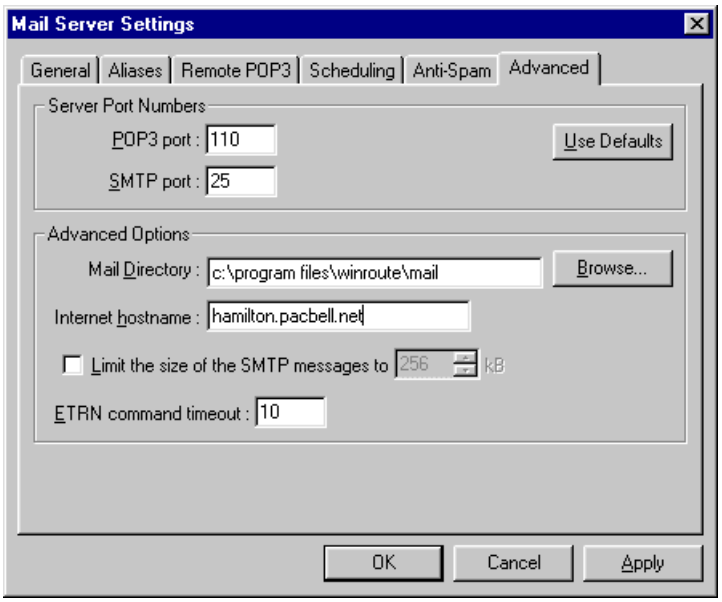
Si no está conectado de forma permanente, su correo electrónico se almacena temporalmente en el servidor del ISP. El correo se transfiere mientras está conectado. Para algunos proveedores de servicios se requiere el comando ***ETRN***[3] para pedir el correo electrónico. El Servidor de Correo de WinRoute soporta el comando ETRN. Puede activar esta opción marcando la casilla de verificación correspondiente en la pestaña *General* del cuadro de diálogo **Servidor de Correo**.



[3] ETRN es un comando usado por los servidores SMTP para negociar un periodo de tiempo más largo. Tras establecer una conexión, el servidor SMTP debe pedir el correo SMTP.

El comando ETRN se usa siempre que un servidor SMTP no está "en línea" 24 horas y el correo electrónico para dicho servidor SMTP debe guardarse en una memoria temporal en otro servidor SMTP.

En caso necesario, puede establecer un límite de tiempo para ETRN (en la pestaña *Avanzada*).



Límite de tiempo para el comando ETRN

En esta entrada se especifica el tiempo que debe transcurrir después del establecimiento de la conexión hasta que el servidor SMTP de WinRoute pida el correo SMTP.

Varios dominios

Varios dominios

Es posible que disponga de varios dominios asignados a su conexión a Internet. Si dispone de varios dominios, seleccione el menú *Configuración=>Servidor de Correo=>General* (pestaña), e introduzca todos los dominios separándolos mediante punto y coma.

Cuestiones específicas de varios dominios

Existen dos formas para configurar varios dominios asignados a su red:

1. Cada dominio está asociado con su propia dirección IP

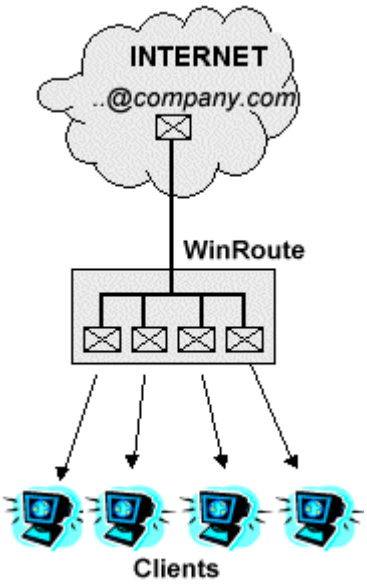
   En este escenario deben haber más direcciones IP públicas mapeadas hacia la interfaz utilizada por WinRoute para las conexiones a Internet. Entonces, se usarán más ajustes de mapeo de puerto - uno para cada dirección IP - con la misma dirección IP de destino del computador WR.

2. Todos los dominios están asociados con una sola dirección IP

   En este caso no se requieren ajustes especiales, excepto establecer el mapeo de puerto para el protocolo TCP en el puerto 25 hacia la dirección IP local de su computador WinRoute.

Si dispone de un dominio asignado a una cuenta POP3

Puede acordar con su ISP que todo el correo electrónico dirigido a su dominio llegue a una sola cuenta. Entonces, WinRoute puede controlar esa cuenta, recoger los mensajes y distribuir automáticamente el correo a los buzones de los usuarios locales.

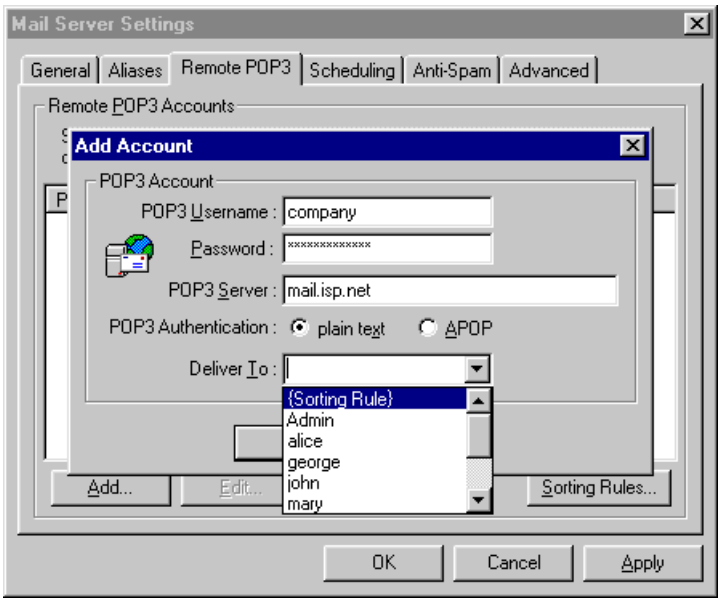


Ejemplo

Su ISP le ha puesto a disposición el buzón compañía@mail.isp.net. Su dominio puede ser compañía.com, pero todo el correo electrónico para su dominio (ventas@compañía.com, juan@compañía.com) llegará al buzón compañía@mail.isp.net del proveedor de servicios.

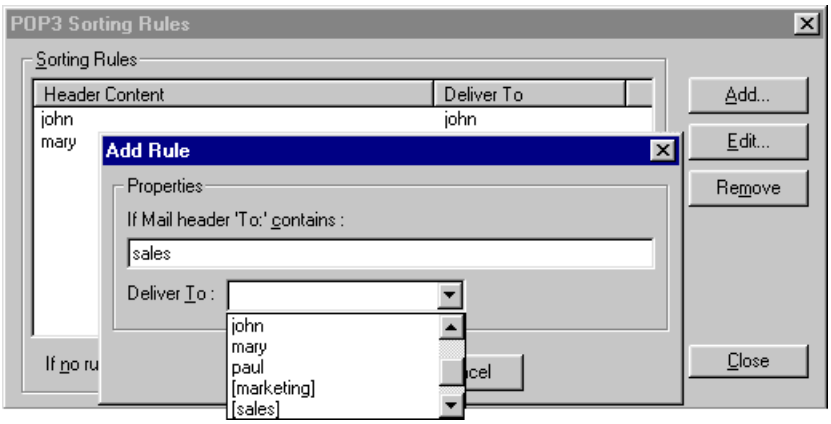
1 Seleccione el menú *Configuración=>Servidor de Correo=>POP3 Remoto*, agregue una nueva cuenta e introduzca sus detalles

2 En el campo "Entregar a:" seleccione "Reglas de Ordenamiento"



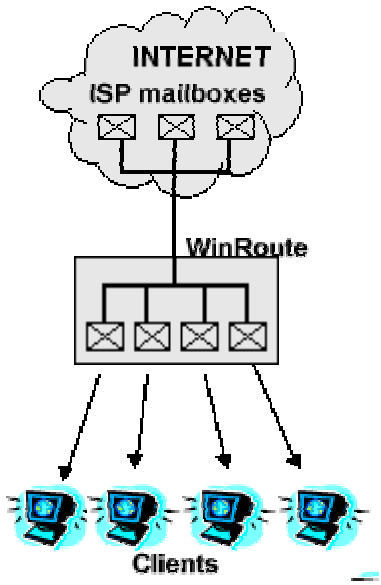
3 Pulse el botón Reglas de Ordenamiento y agregue nuevos criterios. WinRoute entregará el correo electrónico basándose en la dirección de correo electrónico del destinatario, del remitente o en el tema.

4 En el mismo diálogo, seleccione un usuario o un grupo de usuarios al que deba enviársele el correo electrónico.

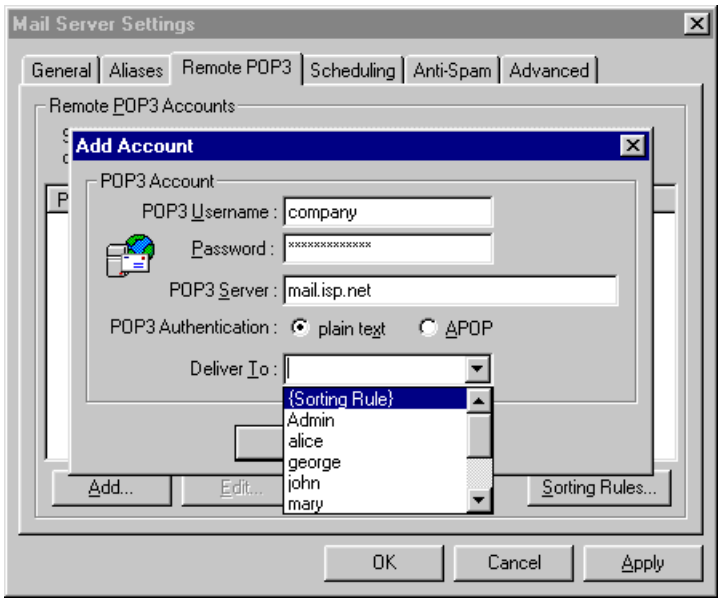


Recibir email - Si dispone de varios buzones del ISP

WinRoute puede controlar diferentes cuentas en varios ISP y distribuir automáticamente el correo recibido a los buzones de los destinatarios locales.



1. Seleccione el menú *Configuración=>Servidor de Correo=>POP3 Remoto*, agregue una nueva cuenta e introduzca sus detalles.
2. En el campo "Entregar a:" seleccione el destinatario o el grupo de destinatarios



Configuración del software cliente de Email

En Esta Sección

Para que pase por el Servidor de Correo de WinRoute

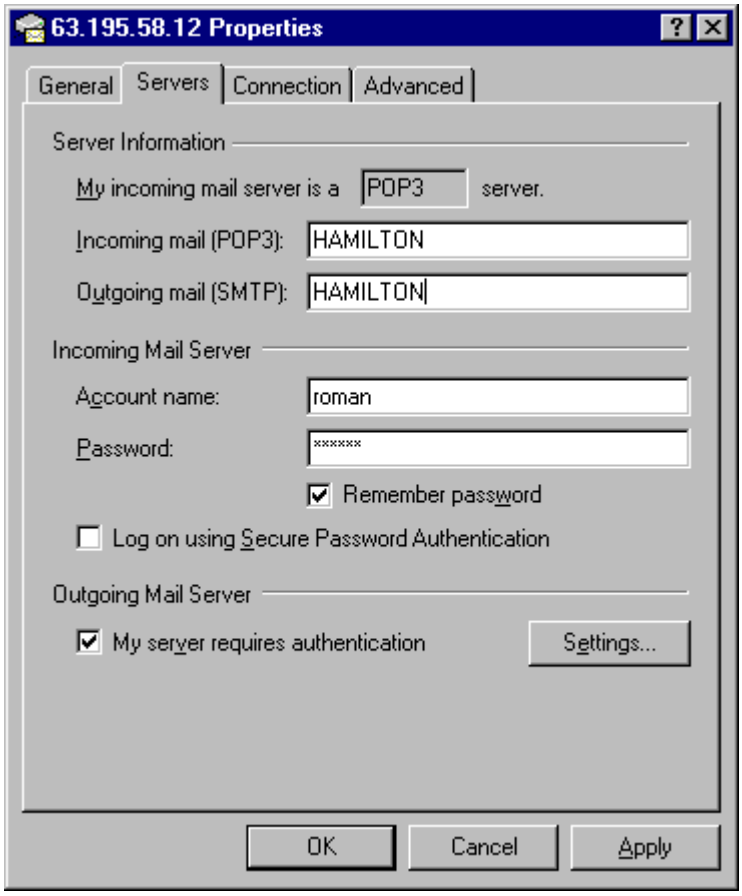
Para que el correo electrónico pase por el Servidor de Correo de WinRoute

Para utilizar el servidor de correo de WinRoute debe configurar su **software cliente de email**. El computador actuará como servidor de correo **Entrante** y **Saliente**. Por tanto, debe introducir el nombre del computador WinRoute en el campo correspondiente de su software de email. Si se presentan problemas al transmitir y recibir correo, le recomendamos que introduzca la dirección IP en vez del nombre del computador, antes de tomar otras medidas. En algunos casos los problemas pueden deberse a la resolución DNS en su red local, y puede parecer como si no estuviera usando el servidor DNS de WinRoute.

Ejemplo:

El Servidor de Correo de WinRoute funciona en un computador con una dirección IP pública asignada dinámicamente y la dirección IP privada 192.168.1.1. El nombre del computador es Hamilton (ver Red en el Panel de Control).

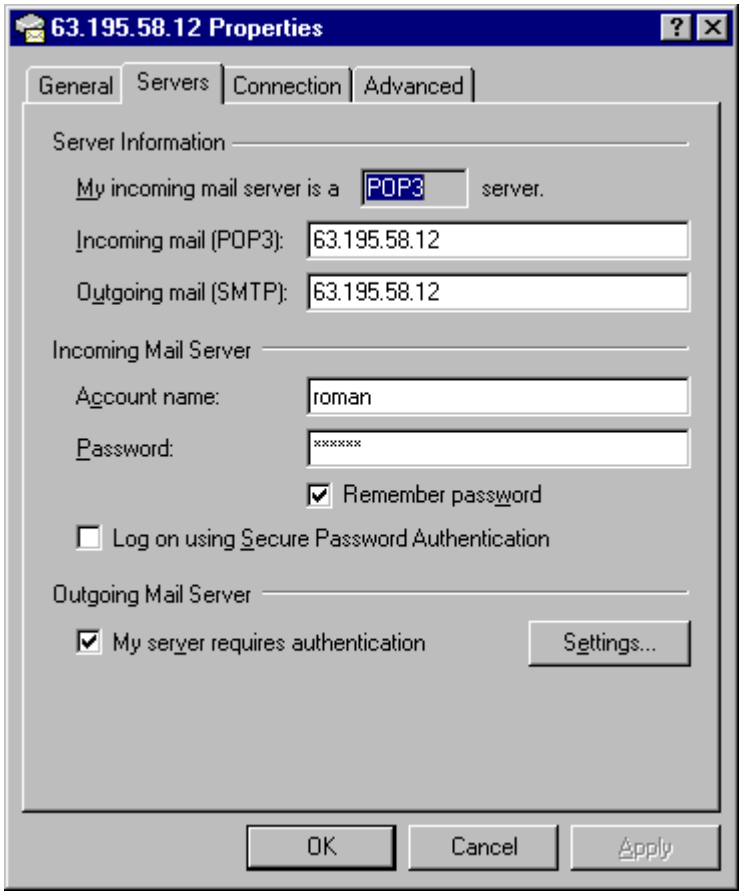
Puede introducir HAMILTON o 192.168.1.1 en los campos Entrante (POP3) y Saliente (SMTP) del servidor de correo de su software de email.


63.195.58.12 Properties
General
Servers
Connection
Advanced
Server Information
My incoming mail server is a
POP3
server.
Incoming mail (POP3):
HAMILTON
Outgoing mail (SMTP):
HAMILTON
Incoming Mail Server
Account name:
roman
Password:
******
Remember password
Log on using Secure Password Authentication
Outgoing Mail Server
My server requires authentication
Settings...
OK
Cancel
Apply

Pasar por alto el servidor de correo de WinRoute

Es posible que desee pasar por alto el servidor de correo de WinRoute y recibir o transmitir mensajes de correo electrónico directamente desde un cliente de correo, a través del servidor de correo de su ISP.

En ese caso, introduzca la configuración entrante y saliente del servidor de correo y el nombre del servidor de correo de su ISP.



- ***Nota: ¡No configure su software cliente de email para usar Proxy! Debe usar NAT de WinRoute para acceder a Internet y configurar su software cliente para que tenga***

acceso directo a Internet. Si no puede intercambiar mensajes de email, eso significa que NAT no se ha configurado correctamente. Configure NAT correctamente basándose en la Lista de control ***.***

CAPÍTULO 3

EJEMPLOS DE DESPLIEGUE

En Este Capítulo

Soluciones IPSEC, NOVELL y PPTP VPN

En Esta Sección

IPSEC VPN

WinRoute Pro 4.1 soporta IPSEC y el así denominado "**Modo túnel**". El "**Modo túnel**" debería soportar a cualquier cliente IPSEC que permita que se cambie la dirección IP de transporte.

Nota: WinRoute no soporta el software cliente de red privada virtual Checkpoint Secure Remote VPN.

Configuración de WinRoute:

Cree un puerto mapeado para ESP:

Protocolo: Otro 50

IP de escucha: <no especificada>

IP de destino: la dirección IP privada del PC cliente

También recomendamos que se cree un puerto mapeado para IKE. Esto no es necesario en los casos en los que la comunicación se inicia desde DETRÁS de WinRoute hacia Internet. No obstante, algunas implementaciones de IPSEC pueden requerir esta configuración:

Mapeado de puerto IKE:

Protocolo: UDP

IP de escucha: <no especificada>

Puerto de escucha: 500

IP de destino: la dirección IP privada del PC cliente

Puerto de destino: 500

Ejecutar varias sesiones IPSEC simultáneamente

Si existen más clientes IPSEC, debe usar una dirección IP individual para cada cliente. Nota - la NAT de WinRoute permitirá el paso simultáneo de todos los clientes que desee, siempre que la conexión se inicie DESDE la red local y cada cliente "utilice" una dirección IP asignada a la interfaz externa de WinRoute.

Información general sobre IPSEC

IPSec es un protocolo de cifrado de seguridad que se usa para las comunicaciones seguras entre dos computadores.

IPSec emplea o bien AH (Authentification Header, encabezamiento de autentificación) o bien ESP (Encapsulating Security Payload, campos de información de seguridad encapsulados). AH sólo verifica la identidad del transmisor y el contenido del paquete. Los datos no se codifican.

ESP codifica los datos. ESP permite utilizar el así denominado "Modo Túnel", que es similar al protocolo PPTP. El paquete incluye, entonces, el encabezamiento IP (necesario para el transporte) que no está codificado, y la porción de datos que incluye el paquete original completo codificado.

El protocolo IKE (algunas veces denominado ISAKMP) se usa para la autentificación (intercambio de claves de seguridad). IKE funciona sobre el protocolo UDP en el puerto 500. Este puerto se usa como origen y como destino.

AH usa el protocolo 51, ESP el protocolo 50. IPSec puede comunicarse también con la autoridad de certificación completa, empleando los demás protocolos que no interfieren con NAT.

El protocolo 50 se incorporará en WinRoute automáticamente, de forma que no será necesario ya realizar ningún mapeo de puerto. La única condición para establecer la conexión automáticamente es que la conexión se inicie DESDE la red local.

La mayoría de los productos IPSec emplean los algoritmos MD5 y SHA1 para la autentificación, y DES, 3DES y Blowfish para el cifrado. IPSec no está relacionado estrechamente con ningún algoritmo específico, de manera que las soluciones de diferentes fabricantes pueden ser incompatibles entre sí.

Novell Border Manager VPN

Utilizar WinRoute Pro con Novell BorderManager VPN (IPSEC)

En este documento se describe la configuración que hace posible conectar una red local que utiliza NAT para compartir una sola dirección IP suministrada por un ISP, a una red remota que utiliza el servidor Novell BorderManager Enterprise Server para la conectividad VPN.

Según el fichero README.TXT suministrado en el disquete de instalación del cliente VPN de Novell BorderManager,

"No puede utilizar NAT en la ruta entre un cliente VPN y un servidor VPN. Esto se debe a que cuando los paquetes IP e IPX se encapsulan y codifican en el cliente VPN, la dirección IP origen empleada para la encapsulación es la dirección del cliente VPN. El cálculo del encabezamiento de autentificación (AH) IPSEC del paquete se basa en esta dirección y en la dirección del servidor VPN de destino. Por ello, si una de las direcciones (del cliente VPN o del servidor VPN) es modificada por NAT, el cálculo falla cuando llega al servidor VPN de destino y el paquete se descarta. Es más probable, sin embargo, que NAT suelte los paquetes IPSEC porque sólo trata paquetes TCP, UDP e ICMP (Internet Control Message Protocol, protocolo de mensaje de control de Internet).

Cuando dispone de estaciones de trabajo en una intranet que deben comunicarse de forma segura, a través de Internet, con redes protegidas por un servidor VPN, le recomendamos que utilice la facilidad VPN sitio-a-sitio Novell BorderManager Enterprise Edition (en vez de la VPN cliente-a-sitio)."

Sin embargo, el coste del servidor Novell BorderManager Enterprise Server es muy elevado. Adicionalmente, requiere amplias medidas de configuración para las rutas estáticas de la red remota a la que se accede. Por tanto, la solución recomendada arriba por Novell no es factible para una persona que desee conectar su red local que utiliza NAT, a una red remota a través de la red privada virtual Novell BorderManager.

Sorprendentemente, es posible conectar una red local que usa NAT a una red remota que usa WinRoute Pro y el cliente VPN Novell BorderManager. Mediante esta configuración, cualquier computador en la red local puede acceder a los recursos de la red remota una vez que el túnel VPN se haya establecido en el computador enrutador. No es necesario realizar ningún tipo de configuración en la red remota.

A continuación se indican los pasos de configuración a seguir para la red local.

Paso 1: Instale y configure el software cliente VPN Novell BorderManager en el computador que se utilizará como enrutador. Cerciórese de que la conexión VPN a la red remota pueda establecerse con éxito y que se disponga de acceso a los recursos de la red remota.

Paso 2: Instale WinRoute Pro en el computador enrutador. Siga las instrucciones de la Guía del Administrador para configurar WinRoute Pro y para configurar los computadores de la red local de forma que trabajen con WinRoute Pro. Use la configuración regular para compartir una sola dirección IP. Cerciórese de que se pueda acceder a los recursos de Internet desde cualquier computador de la red local.

Paso 3: Cuando necesite acceder a los recursos de la red remota, ejecute el cliente VPN Novell BorderManager en el computador enrutador y dese de alta en la red remota.

Esto es posible gracias a la arquitectura de WinRoute Pro. Dado que trabaja al nivel IPSEC, la traducción de la dirección se realiza antes de que el paquete se encamine al adaptador de la red virtual. Por ello, los paquetes transmitidos al servidor VPN disponen de la dirección IP de origen real. A su regreso, los paquetes recibidos del adaptador de la red virtual pasan por la capa de traducción de dirección y se encaminan al computador correcto de la red local.

Las limitaciones de esta configuración son que el inicio de sesión VPN debe realizarse manualmente en el computador enrutador, y que la conexión VPN expira después de un periodo de inactividad determinado, que se define en el servidor VPN. Además, los paquetes IPX no se encaminan ni aunque el protocolo IPX esté habilitado en el túnel VPN. Por tanto, el túnel IPX sólo estará disponible en el computador enrutador.

En términos generales, mediante esta configuración es posible conectar, de forma económica y sencilla, una red local que usa NAT a una red remota que usa la red privada virtual Novell BorderManager VPN.

Un servidor PPTP detrás de NAT

Para hacer funcionar un servidor PPTP en la red detrás de WinRoute (inclusive el computador en el que se ejecuta WinRoute), debe configurar el mapeo de puerto.

Importante: Si el servidor VPN está ubicado en la máquina host WinRoute, debe mapear la IP de destino a la **dirección pública***, y no a la privada. La IP de escucha debe permanecer no especificada.*

Para la conexión de control:

- Protocolo: TCP
- IP de escucha:
- Puerto de escucha: 1723
- IP de destino: dirección IP de su servidor PPTP (p. ej., 192.168.1.12)

- Puerto de destino: 1723

Para los paquetes GRE (PPTP):

- Protocolo: PPTP
- IP de escucha:
- IP de destino: dirección IP de su servidor PPTP (p. ej., 192.168.1.12)

Una vez que haya configurado el mapeo de puerto como se muestra arriba, puede ubicar su servidor PPTP en cualquier posición detrás de WinRoute, INCLUSIVE el computador CON WinRoute. Los usuarios accederán a su servidor PPTP "marcando" la dirección IP externa (pública) de su red. Cuando los paquetes lleguen al computador WinRoute se transmitirán automáticamente al computador adecuado detrás del cortafuegos.

Ejemplo de una solución PPTP

WinRoute pone a su disposición una forma muy económica de crear su propia WAN entre las sucursales de su compañía conectadas a Internet. Partimos de la premisa de que las personas que leen este documento tienen conocimientos básicos sobre las conexiones en red y sobre WindowsNT.

Puede crear una WAN como la mencionada arriba llevando a cabo varios pasos sencillos:

1. Controle el entorno:

   Servidor NT en ambos extremos

   WinRoute Pro instalado en ambos extremos

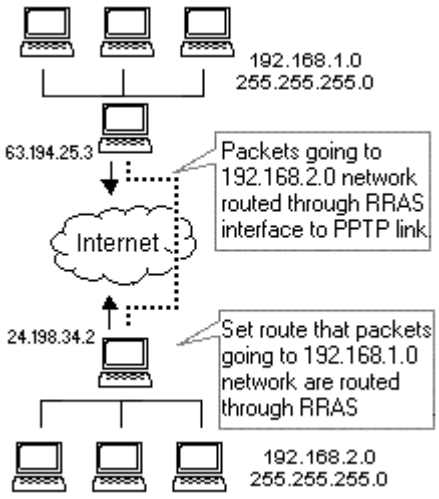
   RRAS (Stealhead) instalado en ambos servidores NT

2. Cree una ruta estática en ambos servidores NT, especificando que los paquetes dirigidos a la red colateral deben pasar por la interfaz RRAS. A continuación, al visualizar las propiedades TCP en el registro de depuración de WinRoute Administrator, debería ver una interfaz de marcación entrante listada entre otras interfaces disponibles.

3 En la Administración de WinRoute seleccione la Tabla de interfaces y visualice las propiedades de la interfaz RAS usada para el enlace PPTP. Cerciórese de que no se ejecutará NAT en esa interfaz.

4 En la pestaña RAS de las propiedades de la interfaz RAS, seleccione la conexión PPTP entre las entradas RAS. Si no ve la conexión RAS entre las entradas RAS, cerciórese de que ha configurado el listín telefónico correcto. Seleccione el menú *Configuración->Avanzada->Varias Opciones* y elija el listín telefónico RAS correcto a utilizar.

5 Pruebe la conexión - debería poder transmitir un ping a la red colateral y, al mismo tiempo, debería poder acceder a Internet.



Clientes PPTP detrás de NAT

No se requiere ningún ajuste especial para los clientes PPTP ubicados detrás de WinRoute (NAT), que accedan al servidor PPTP en Internet. Puede establecer la cantidad de conexiones simultáneas que desee.

Solución DNS

En Esta Sección

Servidor DNS sobre el PC WinRoute

Cuando el servidor DNS funciona en el PC WinRoute, esto no debería provocar ningún tipo de dificultades. Todas las peticiones DNS provenientes de su servidor DNS se contestarán mediante la dirección IP Internet regular asociada con el dominio. Este tipo de dirección IP debe asociarse con la interfaz de red enlazándola desde el PC WinRoute a la Internet, y los servidores WWW escuchan tanto en las interfaces públicas como en las privadas.

Cuando el PC local transmite una petición DNS para resolver www.midominio.com, recibe una dirección IP pública asociada con ese dominio y se conecta al servidor web con una dirección IP (asignada a la interfaz de Internet).

- ***¡Cerciórese de que se haya configurado el mapeo de puerto para las peticiones DNS, incluso aunque el servidor DNS funcione sobre el PC WinRoute! Debe mapear el protocolo UDP y el puerto 53 a la dirección IP de la interfaz de Internet.***

Servidor DNS detrás del PC WinRoute

Puede correr un servidor DNS real sobre cualquier PC de su red local. Para ello, debe configurar el mapeo de puerto:

Protocolo: UDP

IP de escucha: no especificada o la dirección IP asociada con el servidor DNS (mapeada como segunda dirección IP)

Puerto de escucha: 53

IP de destino: la dirección IP privada del PC con el servidor DNS

Puerto de destino: 53

Servidor DNS y WWW detrás de NAT

Si su propio servidor DNS y su servidor WWW funcionan en la misma red privada, es posible que se haga las siguientes preguntas:

¿Cómo puedo gestionar las consultas DNS para www.midominio.com provenientes de mi LAN? ¿Cómo serán contestadas mediante la dirección IP de la red privada del servidor web, mientras que las consultas DNS provenientes de Internet recibirán una dirección IP regular asociada con www.midominio.com?

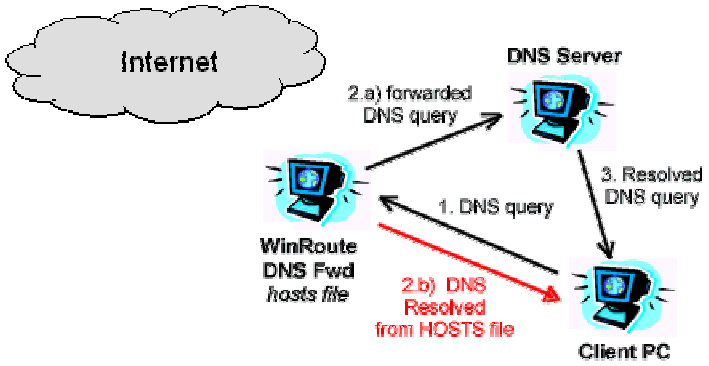
La solución es bastante sencilla y utilizará el **Transmisor DNS** integrado en WinRoute para resolver el problema. Debe configurar el Transmisor DNS de WinRoute como el servidor DNS en todos los PC clientes. En el PC WinRoute debe realizar los siguientes ajustes:

- ACTIVE el Transmisor DNS de WinRoute
- Edite el fichero HOSTS:

  En el fichero HOSTS, agregue un registro especificando que www.midominio.com se encuentra en una dirección IP privada específica (la dirección en la que funciona su servidor web - p. ej., 10.10.10.8). El fichero HOSTS se encuentra en el directorio raíz de su directorio windows (donde está instalado windows - c:\Windows o c:\win98, etc.). También puede acceder al fichero HOSTS desde el diálogo del Transmisor DNS de WinRoute, haciendo clic en el botón "Editar fichero HOSTS".

¿Cómo funciona esto?

Todas las peticiones DNS transmitidas por los computadores clientes de LAN serán resueltas primero por el Transmisor DNS de WinRoute. En primer lugar, se controlarán todas las peticiones en base a los registros del fichero HOSTS. Cuando el registro correspondiente coincide con la petición, ésta se contesta mediante los detalles de ese registro (en nuestro escenario, dirección IP privada).



Si en el fichero HOSTS no hay ningún registro que coincida con la petición, ésta se compara con los registros de la memoria caché DNS de WinRoute (incluida en el Transmisor DNS de WinRoute). Si la memoria caché DNS no contiene ningún registro que coincida, la petición se transmite al servidor DNS especificado en el Transmisor DNS de WinRoute como el DNS al que deben enviarse las peticiones.

Todas las consultas DNS provenientes de Internet se transfieren, en base a los ajustes del mapeo de puerto, directamente al servidor DNS y se resuelven de conformidad con sus registros.

- ***Nota: En este escenario el servidor DNS no puede funcionar en el mismo computador en el que se ejecuta WinRoute. Esto se debe a que ambos servicios - el Transmisor DNS de WinRoute y su servidor DNS, se ejecutarían en el mismo puerto - UDP 53. Esto provocaría errores fatales.***

Asuntos específicos de DNS

Un servidor Web (o FTP, etc.) y un servidor DNS en la misma red privada, detrás de NAT de WinRoute

Es posible que desee correr un servidor web con el dominio www.midominio.com detrás de NAT, y utilizar su servidor DNS en la misma red para la resolución de nombres.

Un servidor Web (o FTP, etc.) sobre el PC WinRoute

Si corre un servidor web sobre el PC WinRoute, no tendrá ningún problema con las consultas locales. Todas las consultas DNS para www.cualquierdominio.com que lleguen a su servidor DNS serán contestadas mediante la dirección IP regular de Internet asociada con ese dominio. Esa dirección IP debe estar asociada con la interfaz de red que conecta el PC WinRoute con la Internet, y los servidores WWW pueden escuchar tanto en las interfaces públicas como en las privadas.

Cuando un PC local transmite una consulta DNS para resolver www.cualquierdominio.com, recibe una dirección IP pública asociada con ese dominio. Como resultado, conecta al servidor web con la dirección IP (asignada a la interfaz de Internet como se describe arriba).

Un servidor Web (o FTP, etc.) sobre un PC ubicado detrás de WinRoute

Puede desear correr su servidor sobre un PC ubicado detrás de WinRoute (con una dirección IP privada, p. ej. 10.10.10.8). El servidor web con www.midominio.com está ubicado físicamente en una dirección IP privada 10.10.10.8, pero su consulta DNS será resuelta con una dirección IP regular (como, p. ej., 206.86.181.25) asociada con ese dominio.

Entonces, su navegador o cliente ftp se dirigirá a la dirección pública, en la que no funciona ningún servidor web, ya que éste se encuentra dentro de su red.

Solución

Para resolver este asunto debe utilizar el **Transmisor DNS** integrado en WinRoute, como el servidor DNS de sus computadores.

En el fichero **HOSTS** debe agregar una nueva entrada especificando que **www.midominio.com** está operando en la dirección IP **interna** correcta (de clase privada). De esta manera, el Transmisor DNS buscará primero en su fichero HOSTS antes de transmitir la consulta DNS a un servidor regular.

Entonces, cada vez que un usuario envíe una consulta para **www.midominio.com**, dicha consulta será contestada mediante la dirección local correcta.

Servidores WWW, FTP, DNS y Telnet detrás de WinRoute

En Esta Sección

Un servidor WWW detrás de NAT

Para que el servidor web funcione detrás de NAT:

1. Seleccione el menú *Configuración ->Avanzada ->Mapeo de Puerto*
2. Agregue un nuevo mapeo de puerto:

   Protocolo: TCP

   IP de escucha: no especificada o la dirección IP asociada con el dominio. Esa dirección IP debe estar asociada con la interfaz

   Puerto de escucha: 80

   IP de destino: introduzca la dirección IP del servidor WEB (p. ej., 192.168.1.10)

   Puerto de destino: 80

Los usuarios que accedan a estos servicios accederán a ellos utilizando o bien el nombre de dominio o bien la dirección IP pública de su red. Una vez que los paquetes llegan a WinRoute, se desvían automáticamente hacia los computadores internos con la dirección IP interna correspondiente.

Un servidor DNS detrás de NAT

El Transmisor DNS integrado en WinRoute le permite transferir consultas DNS a un servidor DNS regular para resolver los nombres de dominio. Ese transmisor puede resolver las consultas DNS locales (cuando se usa el nombre del computador local). No obstante, las consultas DNS como *www.cualquierdominio.com* deben ser resueltas por un servidor DNS regular. El **Transmisor DNS** de WinRoute se encarga de **transferir** las consultas DNS al **servidor DNS**.

Un servidor DNS detrás de NAT (WinRoute)

Para que el servidor DNS funcione detrás de NAT/WinRoute, debe configurar el mapeo de puerto como se describe abajo. Los servidores DNS se comunican entre sí mediante el protocolo **UDP** en el **puerto 53**. Sin este ajuste, su servidor DNS no podrá funcionar. Es necesario que realice este ajuste. Cuando corre el servidor DNS en el mismo computador que WinRoute, el módulo de inspección de WinRoute ejecuta la NAT **ANTES** de que los paquetes lleguen a cualquier aplicación, inclusive el servidor DNS.

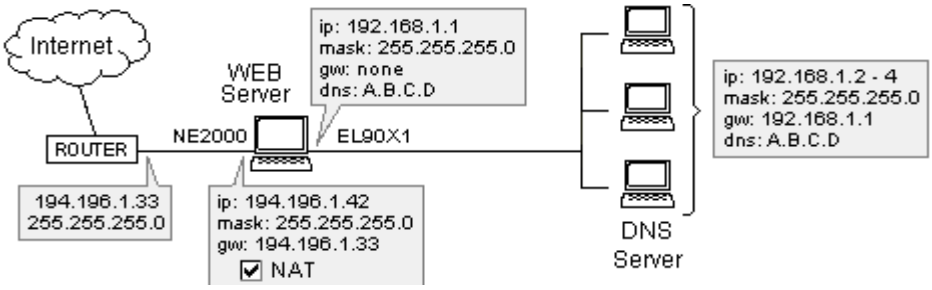
Protocolo: UDP

IP de escucha: no especificada o dirección IP pública del servidor DNS que desee operar

Puerto de escucha: 53

IP de destino: dirección pública o privada del servidor de nombres de dominio

Puerto de destino: 53



- ***Nota: Es** imposible **que un servidor DNS regular funcione en el mismo computador en el que se ejecuta el Transmisor DNS de WinRoute. Ambos servicios utilizan el protocolo UDP y el puerto 53. Si ambos servicios DNS funcionan en el mismo PC, esto provocará errores fatales en el encaminamiento IP. No obstante, puede DESACTIVAR el Transmisor DNS de WinRoute si desea hacer funcionar el servidor DNS en el PC WinRoute.***

Un servidor FTP detrás de NAT

Para que un servidor FTP funcione detrás de NAT:

1. Seleccione el menú *Configuración ->Avanzada ->Mapeo de Puerto*
2. Agregue un nuevo **mapeo de puerto**:

   Protocolo: TCP

   IP de escucha: no especificada o la dirección IP asociada con el dominio. Esa dirección IP debe asociarse con la interfaz de Internet

   Puerto de escucha: 21

   IP de destino: introduzca la dirección IP del servidor FTP (p. ej., 192.168.1.10)

   Puerto de destino: 21

Para que un servidor FTP funcione en un puerto no estándar:

Ajuste el mapeo de puerto de forma que coincida con el puerto usado por el servidor FTP.

Un servidor de correo detrás de NAT

Para que un servidor de correo funcione detrás de WinRoute, le recomendamos crear dos entradas de mapeo de puerto - una para el protocolo SMTP (que funciona sobre el puerto 25) y una para el protocolo POP3 (que funciona sobre el puerto 110). De esta forma, otros servidores SMTP podrán acceder a su servidor SMTP y, además, podrá recoger su correo electrónico de Internet mediante POP3.

Es necesario que configure un mapeo de puerto en caso de que el servidor de correo corra sobre el computador WinRoute. Esto se debe a la posición del módulo de inspección de WinRoute, que funciona debajo de la pila TCP, de forma que los paquetes se cambian/deniegan antes de que lleguen al sistema operativo.

Protocolo SMTP:

Protocolo: TCP

IP de escucha:

Puerto de escucha: 25

IP de destino: introduzca la dirección IP del servidor de correo SMTP (p. ej.,192.168.1.10)

Puerto de destino: 25

Protocolo POP3:

Protocolo: TCP

IP de escucha:

Puerto de escucha: 110

IP de destino: introduzca la dirección IP del servidor de correo POP3 (p. ej.,192.168.1.10)

Puerto de destino: 110

Un servidor Telnet detrás de NAT

Telnet es utilizado por muchas compañías para operar datos de forma remota. Este protocolo es usado, sobre todo, por los servidores AS400.

Para que un servidor Telnet funcione detrás de WinRoute, es necesario que configure un mapeo de puerto para el protocolo TCP en el puerto 23. En cambio, no se requiere ningún ajuste especial para un cliente Telnet que acceda a un servidor Telnet ubicado en Internet.

Protocolo: TCP

IP de escucha: no especificada o la IP del servidor Telnet

Puerto de escucha: 23

IP de destino: introduzca la dirección IP del servidor Telnet (p. ej. 192.168.1.10)

Puerto de destino: 23

Asuntos específicos de FTP cuando se usan puertos no estándar

En Esta Sección

Acceder a servidores FTP con puertos no estándar

Si se encuentra detrás de WinRoute e intenta acceder a un servidor FTP con un número de puerto que no sea el 21, no recibirá ningún listado de directorios. Para realizar esta acción con éxito, debe seguir los siguientes pasos:

1. Vaya a la máquina en la que funciona WinRoute
2. Desactive el motor WinRoute
3. Seleccione el menú Inicio->Ejecutar en el escritorio
4. Introduzca "regedit" para acceder al Editor del Registro;
5. Busque HKEY_LOCAL_MACHINE/SOFTWARE/TinySoftware/WinRoute/Module/0
6. Modifique SpecParams de forma que el valor sea igual al número de puerto del servidor FTP al que desee acceder

7 Active nuevamente el motor WinRoute.

Mediante este ajuste, cualquier computador detrás de WinRoute debería poder acceder al servidor FTP en Internet con un puerto no estándar.

➢ ***Nota: Puede especificar varios puertos, dejando un espacio en blanco entre cada valor.***

Un servidor FTP detrás de WinRoute que utiliza un puerto no estándar

Es posible que, bajo ciertas circunstancias (por ejemplo, un cliente corporativo detrás de un cortafuegos), se restrinja el acceso de un usuario para que sólo pueda acceder a FTP en el modo **pasivo**. Cuando un servidor FTP ubicado detrás de WinRoute utiliza un puerto no estándar, no se puede establecer ningún acceso en el modo **pasivo**. Esto se debe a que WinRoute considera el puerto 21 como el puerto FTP por defecto, de manera que si los usuarios desean usar un puerto diferente, deben realizar primero los ajustes correspondientes en WinRoute. Mediante el siguiente procedimiento se corrige este problema y se permite el acceso en el modo **pasivo**.

1 Vaya a la máquina sobre la que se corre WinRoute

2 Desactive el motor WinRoute

3 Seleccione el menú Inicio->Ejecutar en el escritorio

4 Introduzca "regedit" para acceder al Editor del Registro;

5 Busque HKEY_LOCAL_MACHINE/SOFTWARE/TinySoftware/WinRoute/Mport. Es probable que vea allí subcarpetas que incluyen información sobre el mapeo de puerto. Si no hay ninguna subcarpeta, no hay ningún mapeo de puerto.

6 Busque la carpeta con el mapeo de puerto basado en el puerto utilizado por el servidor FTP

7 Modifique la clave *"flags"* a ‘1’

8 Modifique la clave *"NatApp"* a ‘FTP’

9 Active nuevamente el motor de WinRoute.

Estos ajustes le "indicarán" a WinRoute que los paquetes provenientes del puerto que ha definido corresponderán al protocolo FTP y, por tanto, WinRoute realizará las acciones necesarias para que pasen.

Redes Especiales

En Esta Sección

Redes Token Ring

Conectar redes Token Ring

Token Ring es un tipo muy especial de red. Por tanto, partimos de la premisa de que sólo profesionales en materia de redes se ocuparán de Token Ring, y no ofreceremos aquí ninguna explicación detallada.

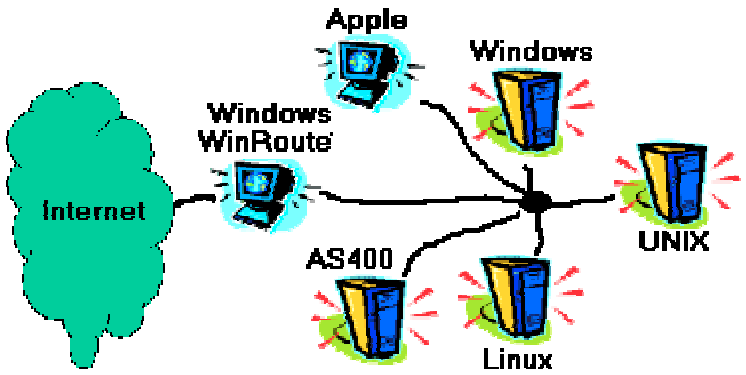
- Para todos los computadores dentro de Token Ring, la MTU (maximum transmission unit, unidad máxima de transmisión) debe ajustarse en 1500
- En el computador WinRoute seleccione Configuración->Avanzada->Varias Opciones y marque la casilla "Soporte para redes Token Ring"
- Siga las instrucciones de configuración adicionales específicas de cada tipo de conexión a Internet

Entornos con varios sistemas operativos (Linux, AS400, Apple)

Conectar entornos con varios sistemas operativos (Linux, Unix, AS400, Apple)

WinRoute permite conectar a Internet entornos con varios sistemas operativos. WinRoute actúa como un enrutador de software y, como tal, soporta cualquier entorno TCP/IP estándar.

- ***NOTA: Se requiere un sistema operativo basado en Windows que sirva de host a la aplicación WinRoute. Por tanto, debe existir, como mínimo, un computador basado en Windows 95/98/NT en la red WinRoute. El host no puede ser un sistema UNIX. No obstante, UNIX puede operar como sistema cliente.***



Conectar varias redes

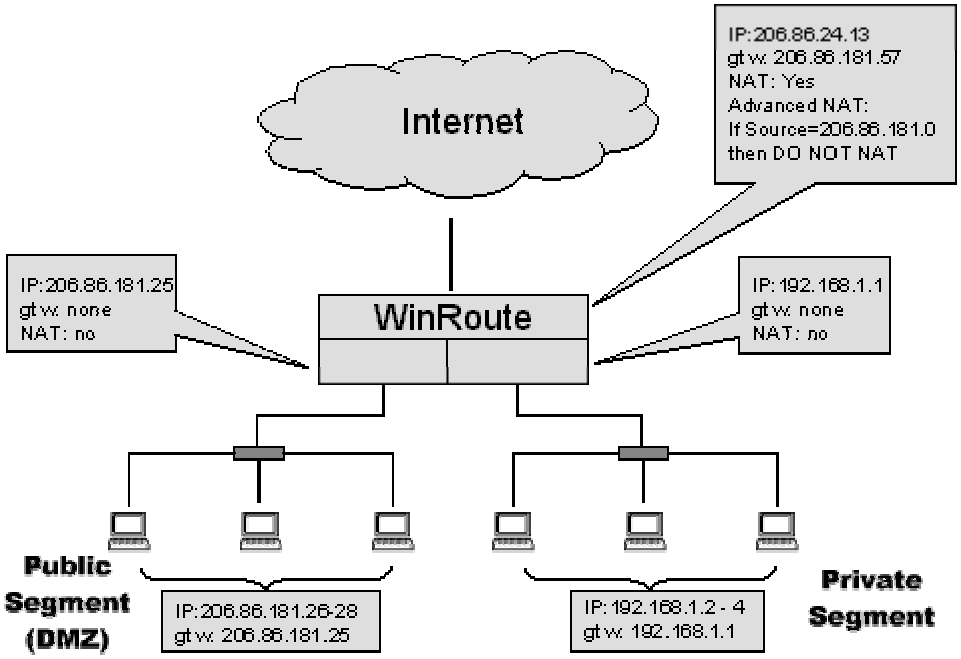
En Esta Sección

Conectar Segmentos Públicos y Privados (DMZ)

Un segmento privado consta de computadores que utilizan direcciones Internet de tipo privado. Esas direcciones están dedicadas a las redes privadas y no pueden ser usadas en Internet. Es por eso que WinRoute debe traducirlas primero a direcciones públicas, permitiendo así la conexión a Internet. No es posible acceder directamente desde fuera de la red (desde Internet) a los computadores con direcciones privadas.

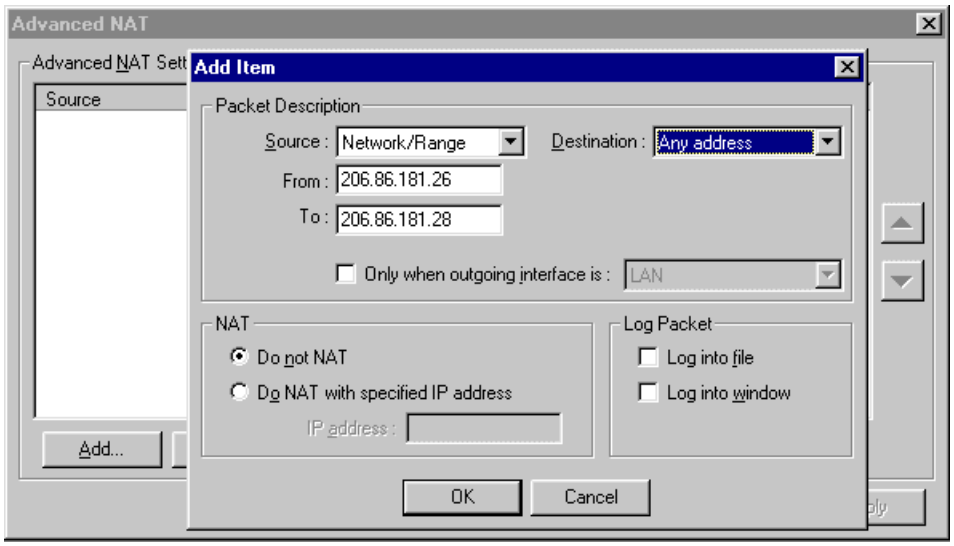
Un segmento público consta de computadores que disponen de una dirección IP pública cada uno. Es posible acceder a esos sistemas directamente desde Internet, si las reglas de seguridad lo permiten.

Cada segmento debe disponer de su propia interfaz de red en el computador WinRoute. Entonces, el motor de WinRoute permite que sus segmentos públicos y privados compartan una conexión a Internet.



Configuración de WinRoute

Es necesario realizar ajustes en la configuración NAT avanzada, de forma que WinRoute no ejecute la NAT para los paquetes provenientes del segmento público. Para ello, seleccione el menú Configuración=>Avanzada=>NAT.



Configuración de la red pública y de la red privada

Estas redes deben configurarse de la misma forma, como se describe en otras secciones de este manual. La única diferencia en los segmentos públicos es que debe utilizar direcciones públicas en ellos. Debe guiarse, básicamente, por las siguientes reglas:

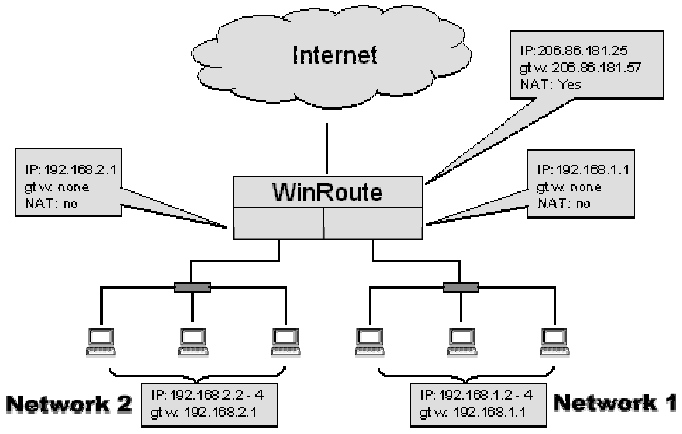
- NINGUNA pasarela por defecto en las interfaces en WinRoute
- La dirección IP de esas interfaces debe usarse como pasarela por defecto para el resto de sus respectivas redes.
- NINGUNA NAT en las interfaces en WinRoute

…para más detalles, vea la ***Lista de control***

La conexión es compartida por dos redes con 1 dirección IP

Si dispone de dos redes conectadas a Internet a través de un computador sobre el que corre WinRoute, no es necesario realizar ningún ajuste específico. Básicamente, existen varios segmentos que conducen al computador WinRoute, y cada uno de ellos tiene una interfaz de red separada. En nuestro ejemplo existen tres interfaces de red en el computador WinRoute:

- Interfaz de Internet
- Interfaz de red 1
- Interfaz de red 2



Los únicos ajustes necesarios que debe tener presentes son:

Interfaz de Internet

NAT está habilitada
La dirección IP se especifica según los datos suministrados por su ISP
La pasarela se configura según los datos suministrados por su ISP

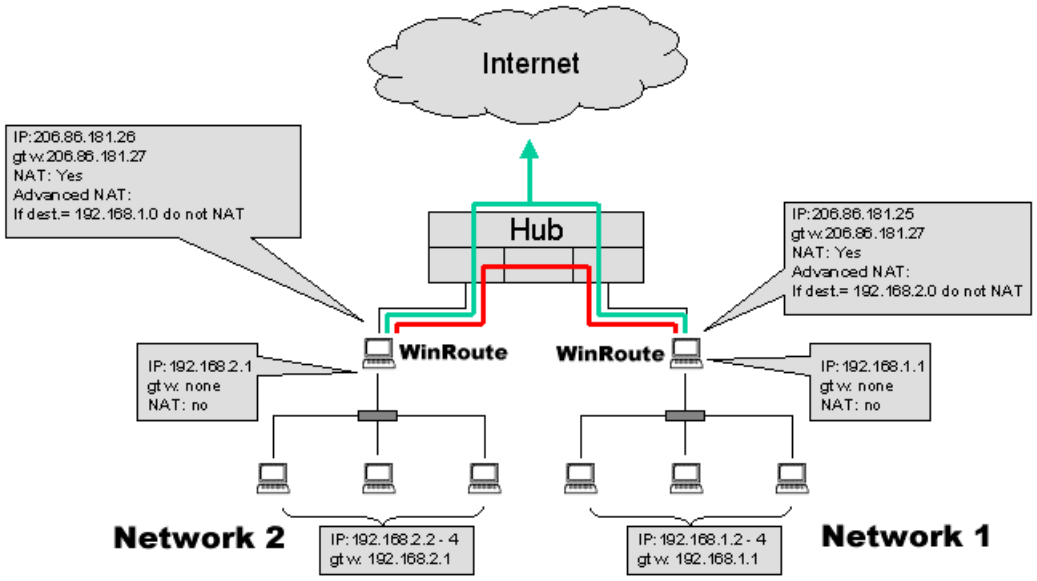
Interfaces internas

NAT NO está habilitada
NINGUNA pasarela configurada en ambas interfaces
La dirección IP debe ser de tipo interno (p. ej.,192.168.1.1)

Los demás ajustes son los mismos que se describen en otras secciones de este manual. El tráfico proveniente de cada subred se encamina a la otra subred o a Internet, y viceversa.

La conexión es compartida por dos redes con 2 direcciones IP

Es posible que desee compartir el acceso a Internet entre dos redes, y que cada red disponga de una dirección IP pública propia y que, al mismo tiempo, desee acceder a los computadores de ambas redes privadas.



En un escenario de encaminamiento como este, es MUY IMPORTANTE que tenga presente lo siguiente:

- NO EJECUTE NAT con ninguno de los paquetes dirigidos a la otra red.
- EJECUTE NAT con todos los paquetes dirigidos a Internet

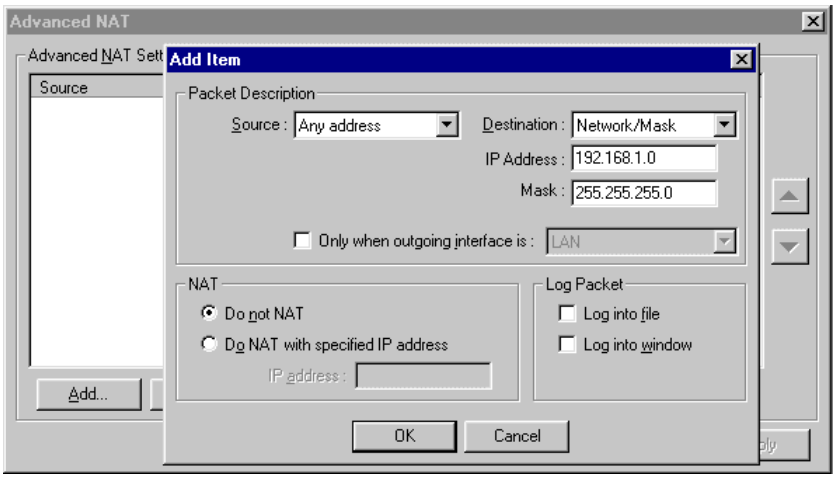
En otras palabras, WinRoute ejecutará NAT en base al destino de los paquetes IP que pasen. Los paquetes que van a la red remota no se modifican, mientras que los paquetes que van a Internet se someten por completo a NAT.

¿Enrutador o hub?

Según sus requerimientos, debe decidir si desea disponer de un enrutador entre sus redes, o si basta un concentrador (hub). En nuestro escenario existe un concentrador que pone a disposición la funcionalidad necesaria para compartir una conexión (de alta velocidad) a Internet.

Configurar a WinRoute para que no ejecute NAT en base al destino del paquete:

1. Seleccione el menú Configuración->Avanzada->NAT.
2. Introduzca los criterios de destino - generalmente, la subred o el rango de direcciones IP
3. Seleccione la opción "No ejecutar NAT"



Consejo: En la configuración NAT avanzada encontrará otra opción que especifica que no se debe ejecutar NAT en base a la dirección IP de origen. Este ajuste puede resultar útil cuando usted sabe qué estaciones de trabajo no necesitan acceder a Internet. En ese caso, en vez de establecer los criterios del cortafuegos puede encontrar otra solución en la configuración NAT avanzada.

Si especifica que no se ejecute NAT con paquetes específicos, es decir, la dirección de origen se mantiene como la dirección IP interna, nunca se obtendrá una respuesta. En otras palabras, el usuario en cuestión puede intentar conectarse a Internet cuantas veces desee, pero nunca lo conseguirá.

Servidor de Acceso Remoto (marcación entrante y acceso a Internet)

Solución de Servidor de Acceso Remoto

En algunas ocasiones, puede resultar necesario acceder a su red corporativa desde el exterior a través de una línea telefónica y utilizar ese acceso a Internet. WinRoute pone a disposición esta funcionalidad en WindowsNT cuando el servicio RAS está instalado y configurado.

En este caso, deben aplicarse reglas específicas:

- Su red corporativa debe disponer de una subred (p. ej., 192.168.1.0)
- El servidor DHCP de WindowsNT debe asignar direcciones IP de una subred diferente (p. ej., 192.168.2.0) a los usuarios que lleguen a través de RAS
- NAT se ejecutará solamente en las interfaces que conducen a Internet

En otras palabras, la tarjeta de red (NIC) que conduce a su red local debe tener la dirección IP de una subred (p. ej., 192.168.1.1), mientras que el usuario que se conecta a su servidor a través de RAS debe recibir una dirección IP de una red diferente (p. ej., 192.168.2.1). WinRoute actúa como un enrutador, es decir, puede encaminar los paquetes entre dos o más interfaces de redes distintas - pero no de la misma red.

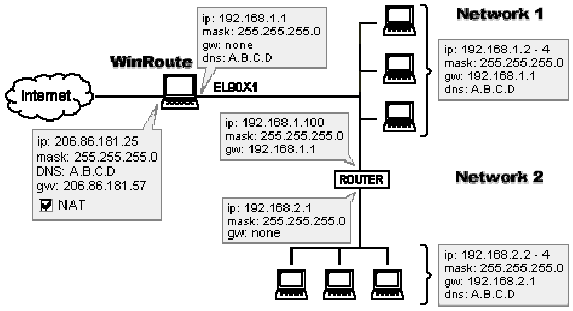
Este tipo de configuración podría reflejar la configuración de un proveedor de servicios pequeño. WinRoute no limita la cantidad de usuarios que acceden simultáneamente a su servidor NT. Siempre que el servidor NT otorgue a los usuarios remotos direcciones IP de subredes diferentes (que no sean la red principal), la cantidad de usuarios sólo quedará limitada por la cantidad de interfaces RAS que usted haya instalado.

Conectar Segmentos en Cascada a través de 1 Dirección IP

Las configuraciones de red en las que las redes a conectar no conducen directamente al computador WinRoute sino que son conectadas a través de un enrutador, se denominan Segmentos en Cascada.

El enrutador entre las dos redes puede ser cualquier enrutador de hardware, un computador WindowsNT o un computador Windows 95/98 con WinRoute. WinRoute actúa como enrutador o bien ejecutando NAT o sin ejecutarla.

Figure 1: Connecting cascaded segments to the Internet



Por lo general, es necesario "indicarle" al computador WinRoute hacia dónde deben enviarse los paquetes entrantes para las otras redes. En cambio, para los paquetes salientes deben existir enlaces similares en el enrutador (dividiendo las dos redes), que especifican hacia dónde deben enviarse los paquetes que salen de la segunda red. Esto se logra agregando nuevas rutas - una en el computador WinRoute (para los paquetes entrantes) y una en el enrutador (para los paquetes salientes).

- La RUTA en el computador WinRoute (miembro de la red1) encaminará los paquetes IP dirigidos a la otra red (red2) a la dirección IP específica de la red1 del enrutador. El enrutador se encarga entonces de hacer llegar los paquetes a su destino final.
- La RUTA POR DEFECTO en el enrutador (que conecta ambas redes) encaminará todos los paquetes provenientes de la red2 a la dirección IP de la red1 del computador WinRoute. A continuación, WinRoute traducirá la dirección de red de esos paquetes (NAT) y los enviará a Internet.

Ejemplo

En nuestro ejemplo hay dos redes 192.168.1.x y 192.168.2.x.; el enrutador se encuentra en 192.168.1.100.

Nota: Puede utilizar como enrutador cualquier enrutador de hardware o cualquier computador Win95/98 con WinRoute o un computador con WindowsNT.

Configuración de la red1 (red primaria)

- Debe indicarle al computador WinRoute: "Todos los paquetes dirigidos a la red 192.168.2.0 deben pasar por el enrutador 192.168.1.100":
- 1. Llame la ventana de entrada de MS-DOS
- 2. Introduzca el siguiente comando:

```
Route -p add 192.168.2.0 mask 255.255.255.0
192.168.1.100
```

- En el enrutador 192.168.1.100, la ruta por defecto debe conducir al computador con WinRoute, p. ej., 192.168.1.1. En otras palabras, debe indicarle al enrutador que encamine todos los paquetes salientes hacia Internet a través del PC WinRoute.
- Todos los demás ajustes de la red deben llevarse a cabo como se describe en los otros capítulos (Configuración de la red).

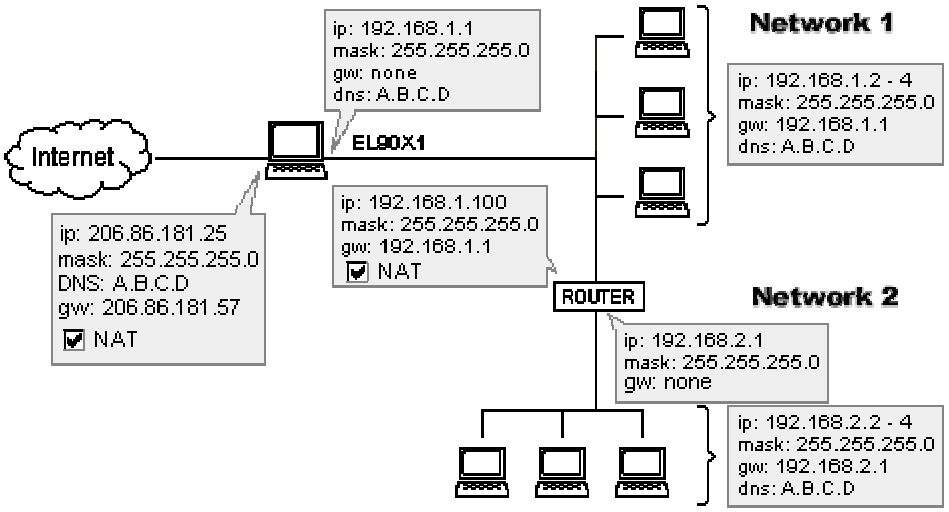
Configuración de la red2 (red secundaria)

Todos los ajustes son ajustes regulares, y la red2 será la red autónoma. La pasarela por defecto en todos los computadores de la red2 será la dirección IP de la red2 del enrutador (en nuestro ejemplo, 192.168.2.1).

NAT entre la red1 y la red2

Figure 2: Connecting cascaded segments to the Internet

Puede utilizar WinRoute con NAT “ACTIVADA” para conectar la red primaria y la secundaria. La red secundaria parecerá un computador individual, de forma que gozará de las ventajas de una administración más sencilla y una mayor seguridad en la red secundaria. Debe realizar los ajustes pertinentes en la configuración NAT avanzada, ya que no deseará modificar el tráfico entre estas dos redes.



Configuración NAT avanzada en el PC WinRoute que divide la red1 y la red2

Basándose en la dirección IP de destino, debe decidir si se ejecutará o no se ejecutará NAT. En nuestro ejemplo, si el destino de los paquetes se encuentra en la red 192.168.1.0, no se traducirá la dirección de red de los paquetes (NAT). De esta forma se permitirá la comunicación entre las dos redes como si no se ejecutara NAT.

Para configurar la red, guíese por las reglas descritas en los demás capítulos de este manual.

Adaptadores Ethernet Multipuerto

Entre las más de 170.000 redes que emplean actualmente WinRoute Pro como su solución de enrutador/cortafuegos, la configuración más común es la de dos tarjetas de interfaz de red (NIC), una conectada a Internet y la otra a la red de área local (LAN). En esta configuración básica se filtran los paquetes que salen hacia Internet y los que entran desde allí. Sin embargo, no se pueden filtrar los paquetes que viajan entre segmentos locales, ya que en ese caso no pasa tráfico a través de WinRoute. En la figura 1 se ofrece un ejemplo de esta configuración.

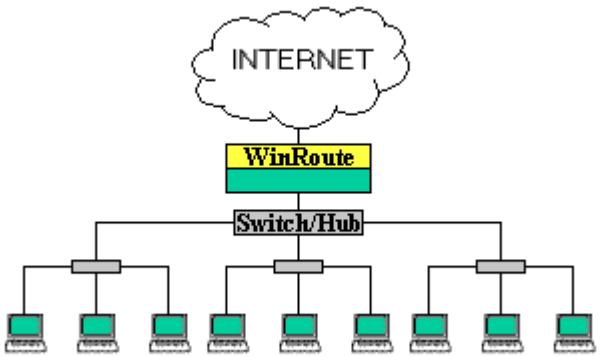


Figura 1. La configuración más común de WinRoute Pro.

En algunos casos se agrega una tercera NIC a la máquina WinRoute para crear un segmento separado seguro. En este escenario, WinRoute filtra tanto los paquetes que salen de ese segmento seguro hacia Internet y hacia los otros segmentos, como también los que entran desde Internet y los otros segmentos, ofreciendo así un nivel adicional de seguridad.

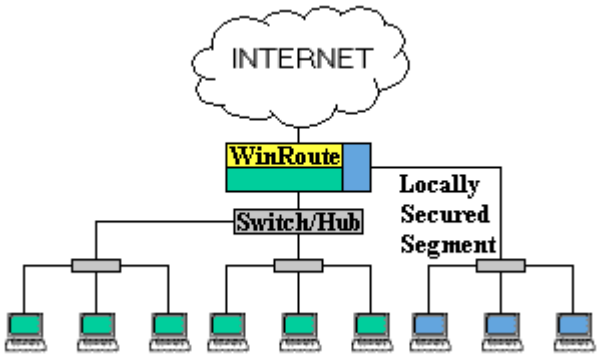


Figura 2. Se puede agregar un segmento separado a la LAN mediante una tercera NIC.

En las redes más grandes que pueden tener varios segmentos separados, cada uno de ellos con sus propias directrices de seguridad, se presenta el problema de que la cantidad de segmentos está limitada por la cantidad de puertos de la máquina WinRoute. Debido a ello, se requiere hardware adicional para el encaminamiento/conmutación posterior y para las directrices de seguridad. Con la reciente introducción en el mercado de las NIC Ethernet multipuerto, WinRoute puede convertirse en el único controlador del tráfico de la red. Dado que las tarjetas multipuerto permiten que la máquina WinRoute disponga de más de 24 puertos, dependiendo de la cantidad de ranuras de tarjeta en la placa madre, la máquina WinRoute puede funcionar también como servidor, enrutador, conmutador, controlador de dominio, etc. De esta forma, la administración de la red puede centralizarse y controlarse en un solo punto. En la figura 3 se muestra una configuración en la que WinRoute Pro utiliza una NIC Ethernet multipuerto para controlar tres redes distintas.

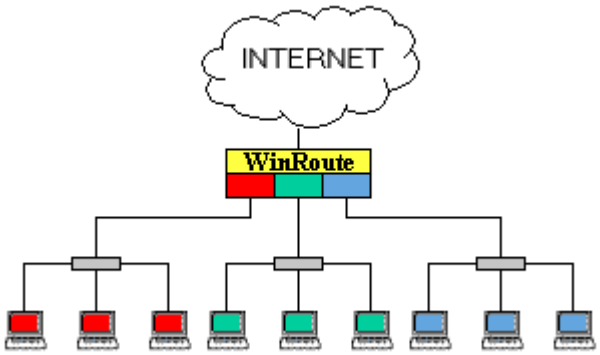


Figura 3. WinRoute Pro equipado con una NIC Ethernet multipuerto.

Además de la seguridad ampliada y la administración centralizada puestas a disposición por las NIC Ethernet multipuerto, existen otras ventajas adicionales como el balance de la carga y la protección contra fallos. Tenga en cuenta la asignación de los tres puertos en el segmento medio en la figura 4.

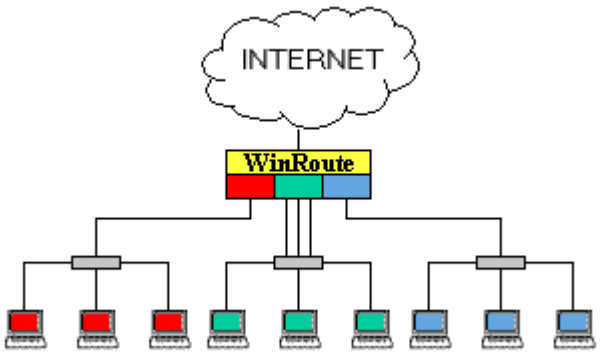


Figura 4. Se han asignado tres puertos al segmento medio para la agregación de puertos.

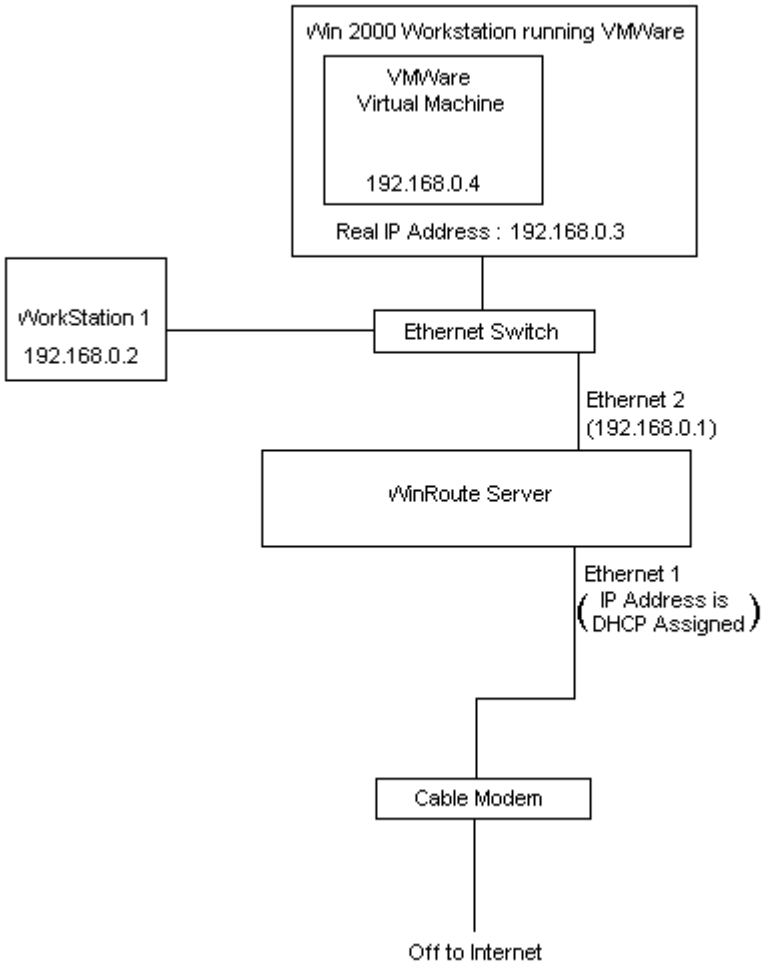
El balance de la carga puede realizarse agregando puertos. Por ejemplo, en la figura de arriba, se han asignado tres puertos al segmento medio de la red. Si el segmento utiliza un conmutador para conectarse a la máquina WinRoute, cada uno de los tres computadores puede recuperar datos a 100 Mbps cada uno. Los otros dos segmentos sólo pueden recuperar datos a una velocidad total de 100Mbps cada uno, debido a que sólo un puerto de ese segmento está conectado a la máquina WinRoute. La protección contra los fallos de los puertos se obtiene mediante una funcionalidad adicional de agregación de puertos. Si una línea se desconecta, el tráfico se reencamina entonces a través del siguiente puerto disponible.

Mediante la combinación de NICs multipuerto con WinRoute, se puede realizar un sistema de multiencaminamiento muy eficiente, a un precio sumamente económico y concentrado las tareas administrativas en un solo punto. WinRoute se ha probado con éxito con **D-Link 4 port DFE 570 TX** y **Adaptec 2 port Duralan ANA-62022**. No se ha probado ninguna tarjeta más.

Cabe mencionar que este tipo de diseño de red requiere diferentes subredes para cada segmento de red conectado a la máquina WinRoute.

VMWare

VMWare es una aplicación que puede emular el PC en el que está instalada hasta el nivel de hardware. Desde la perspectiva de la red, ese computador virtual es una entidad totalmente independiente. Dado que el computador virtual tiene sus propiedades de red propias, WinRoute considera a la máquina virtual como un computador adicional.



CAPÍTULO 4

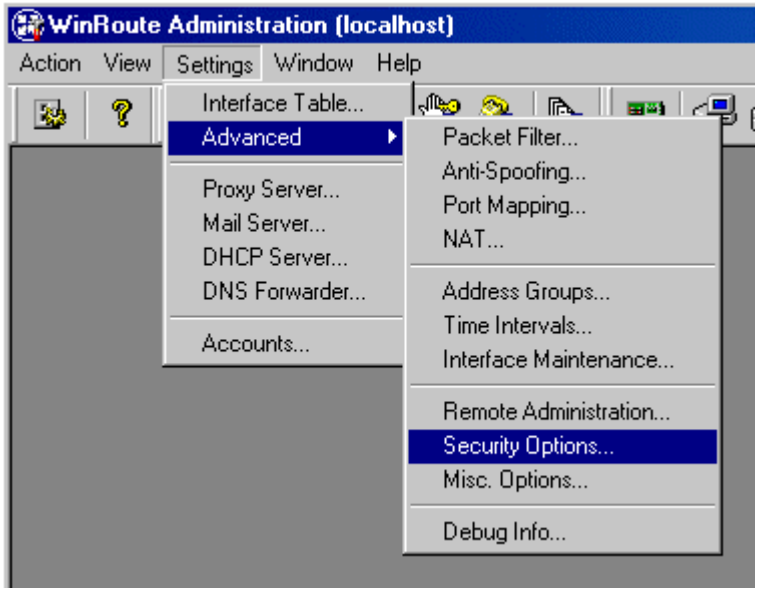
CONFIGURACIÓN DEL CORTAFUEGOS

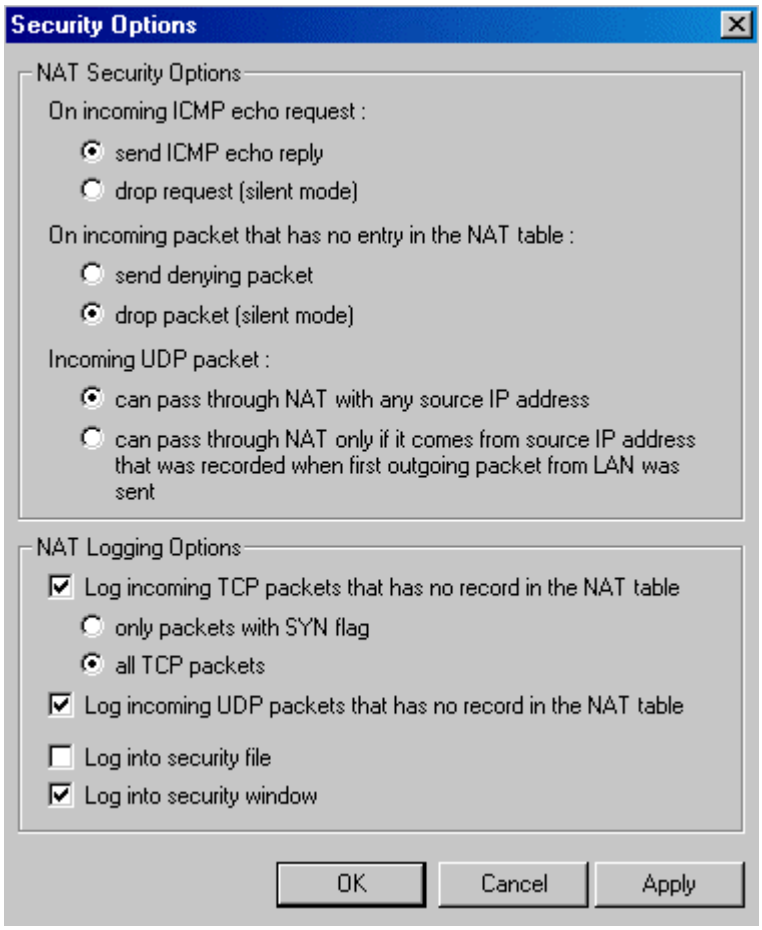
En Este Capítulo

Buscar la asignación de puerto correcta

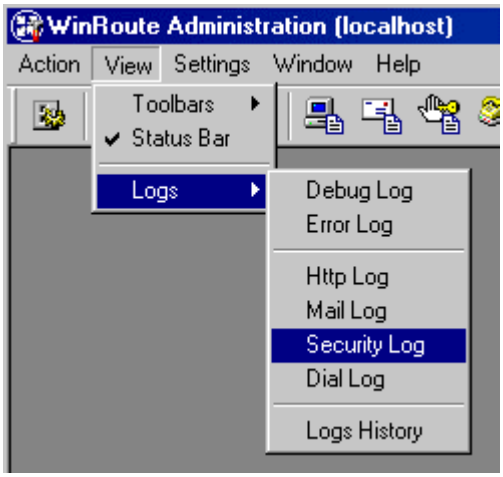
➢ ***Si dispone de build 19 o superior>***

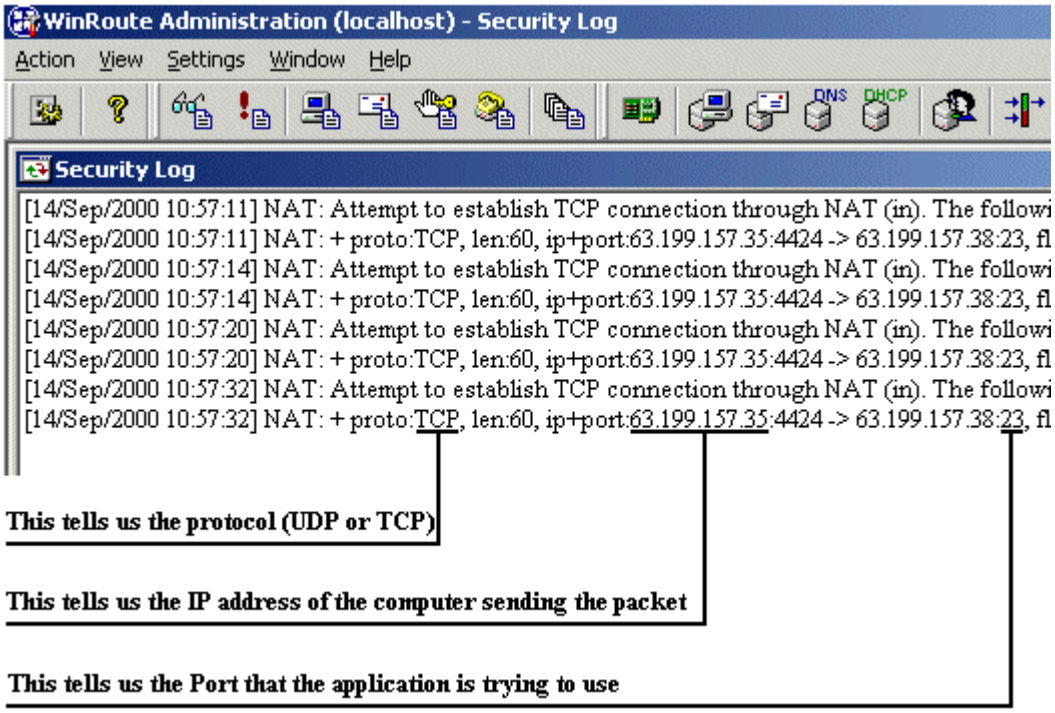
En la ventana de Administración, seleccione Configuración-> Avanzada-> Opciones de Seguridad




Security Options
NAT Security Options
On incoming ICMP echo request :
send ICMP echo reply
drop request (silent mode)
On incoming packet that has no entry in the NAT table :
send denying packet
drop packet (silent mode)
Incoming UDP packet :
can pass through NAT with any source IP address
can pass through NAT only if it comes from source IP address that was recorded when first outgoing packet from LAN was sent
NAT Logging Options
Log incoming TCP packets that has no record in the NAT table
only packets with SYN flag
all TCP packets
Log incoming UDP packets that has no record in the NAT table
Log into security file
Log into security window
OK
Cancel
Apply

En la parte inferior de la ventana de las opciones de seguridad encontrará algunas opciones de registro. Habilite en la ventana de seguridad el registro de los paquetes TCP y UDP que no se encuentren en la tabla NAT. De esta forma sólo se registran los paquetes iniciados desde fuera de WinRoute. WinRoute soltará esos paquetes, a menos que se haya configurado un mapeo de puerto. Dado que ésta es una forma limitada de registro, sólo nos ocuparemos de una cantidad selecta de paquetes para que nos sea más fácil encontrar la descripción del paquete que buscamos. El siguiente paso es abrir el registro de seguridad desde el menú ver-> registros.





En este caso, un computador en 63.199.157.35 transmite un paquete desde el puerto 4424 al puerto 23 de un computador en 63.199.157.38. El puerto 23 es el puerto estándar para telnet. Si dispone de un servidor telnet que funciona en una dirección privada como, p. ej., 192.168.1.3 el servidor estaría en estado de escucha en el puerto 23. Por tanto, debería mapear los paquetes TCP en el puerto 23 hacia 192.168.1.3.

Servicios de Mensajería y Telefonía

En la actualidad existen varios servicios de mensajería instantánea que soportan la transferencia de ficheros, así como las charlas de pc a pc o de pc a teléfono. WinRoute Pro ha sido probado con éxito con las siguientes configuraciones de **AOL instant messenger**, **Yahoo instant messenger**, **MSN Messenger** e **ICQ**.

Para **AIM** no se requiere ningún ajuste específico. Utilice los ajustes de la conexión por defecto y cerciórese de no especificar que está utilizando un servidor proxy.

Los usuarios de **Yahoo IM** deben cambiar las preferencias de inicio de sesión -> conexión a "Sin detección de red". Todos los servicios IM de Yahoo deberían funcionar correctamente detrás de NAT con este ajuste.

MSN Messenger funciona de la mejor forma posible cuando se utiliza un proxy HTTP. Habilite el servidor proxy de WinRoute en el puerto por defecto 3128 (además de la traducción de la dirección de red). Las charlas de PC a PC no funcionan actualmente detrás de WinRoute; no obstante, las charlas PC a teléfono sí funcionan.

ICQ funciona en la mayoría de los casos con los ajustes por defecto de la **última** versión. Si se presentan complicaciones al utilizar la transferencia de ficheros, le recomendamos usar el proxy HTTPS que encontrará bajo preferencias -> conexiones -> servidor y cortafuegos. Habilite el servidor proxy de WinRoute en el puerto por defecto 3128 (además de la traducción de la dirección de red).

Nota: No debería resultar necesario mapear ningún puerto para las aplicaciones mencionadas arriba.

H.323 - NetMeeting 3.0

WinRoute incluye el soporte del protocolo H.323. Esto significa que todas las aplicaciones de voz sobre IP pueden comunicarse a través de WinRoute. Algunas aplicaciones de este tipo son Microsoft NetMeeting, CuSeeMee, telefonía a través de Internet (por ejemplo, puede utilizar el Siemens IP phone a través de WinRoute), etc.

Cuando la comunicación se inicia detrás de WinRoute

En este caso no se requiere ningún ajuste. Winroute soportará una cantidad virtualmente ilimitada de conexiones simultáneas.

Cuando la comunicación se establece desde Internet hacia el PC detrás de WinRoute

En este caso es necesario crear un mapeo de puerto. En otras palabras, debe indicarle a Winroute hacia dónde debe encaminar los paquetes H.323 entrantes. Debe configurar el siguiente mapeo de puerto:

Protocolo:	TCP
IP de escucha:	No especificada o la dirección IP usada para la comunicación H.323 en caso de un sistema multihome
Puerto de escucha:	1720
IP de destino:	La dirección IP LAN de la aplicación H.323

Puerto de destino:	1720

El protocolo H.323 no corre sólo sobre el puerto 1720 - WInRoute agregará las demás conexiones automáticamente. Debido a las limitaciones del protocolo H.323, sólo una estación de trabajo puede usar una comunicación de este tipo a la vez.

IRC - Internet Relay Chat

No se requiere ningún ajuste especial para que funcione un cliente IRC . Incluso DCC (Direct Chat/Send(Receive) Files) funcionará automáticamente si usa el puerto estándar 6667 en su IRC.

Para que el servidor IRC funcione detrás de NAT mapee, por favor, los siguientes puertos:

Protocolo: TCP

IP de escucha: no especificada o la dirección IP que desee utilizar para el servidor IRC

Puerto de escucha: 6667

IP de destino: la dirección IP del PC con su servidor IRC

Puerto de destino: 6667

Si utiliza cualquier puerto que no sea el estándar, DCC no funcionará.

CITRIX Metaframe

WinRoute soporta totalmente el protocolo **CITRIX Metaframe**. Para acceder desde Internet al servidor CITRIX Metaframe que funciona dentro de la red WinRoute, debe realizar el siguiente mapeo de puerto:

Para CITRIX Metaframe:

Protocolo: TCP

IP de escucha: no especificada o la dirección IP que desee asignar al servidor

Puerto de escucha: 1494

IP de destino: la dirección IP de clase privada del servidor ubicado dentro de la red

Puerto de destino: 1494

Puede crear más puertos mapeados y acceder a más servidores simultáneamente. Para ello, debe predeterminar en los computadores clientes el puerto que deben utilizar para acceder al servidor. Puede especificar esto en el fichero .ini del cliente al crear el icono de la conexión.

MS Terminal Server

WinRoute soporta totalmente el protocolo **MS Terminal Server**. Para acceder desde Internet al servidor MS Terminal Server que funciona dentro de la red de WinRoute, debe configurar el siguiente mapeo de puerto:

Para MS Terminal Server:

Protocolo: TCP

IP de escucha: no especificada o la dirección IP pública que desee asignar al servidor

Puerto de escucha: 3389

IP de destino: dirección IP de clase privada del servidor dentro de la red

Puerto de destino: 3389

Puede crear más puertos mapeados y acceder a más servidores simultáneamente. Para ello, debe predeterminar en los computadores clientes el puerto que utilizarán para acceder al servidor. Puede especificar esto en el fichero .ini del cliente, al crear el icono de la conexión.

Telefonía a través de Internet - BuddyPhone

WinRoute es el primer enrutador/cortafuegos de la industria que toma en serio la telefonía a través de Internet. BuddyPhone le permite establecer llamadas a través de Internet de una red a otra.

El soporte para BuddyPhone funciona de la mejor manera posible con ICQ. Registre este software de mensajes instantáneos y podrá disfrutar de operaciones en las que basta con "pulsar un botón" para llamar a sus amigos.

Todos los usuarios activos en la lista de ICQ aparecerán en el listín telefónico de BuddyPhone, y para establecer una llamada sólo debe seleccionar un usuario en la lista.

No se requiere ningún tipo de ajuste siempre que utilice BuddyPhone e ICQ juntos.

Utilizar BuddyPhone sin ICQ

WinRoute puede desviar las llamadas provenientes de Internet hacia el destinatario adecuado en la red local, basándose en el puerto.

Use los puertos 710 y superiores para asignar las propiedades de puerto a los usuarios locales.

Ejemplo:

En su LAN hay tres usuarios que utilizan BuddyPhone.

Nombre del usuario	Dirección IP interna del usuario	Puerto asignado al usuario

John	192.168.1.2	710
Guido	192.168.1.3	711
Bob	192.168.1.4	712

Entonces, configurará el mapeo de puerto:

Puerto de escucha	IP de destino	Puerto de destino
710	192.168.1.2	700
711	192.168.1.3	700
712	192.168.1.4	700

Para establecer una llamada telefónica hacia el usuario sólo tiene que introducir compañía.com:núm. puerto en el diálogo de marcación directa de BuddyPhone. Por ejemplo, ventas.gamerouter.com:711.

- ***Nota: ¡No se trata de un error en nuestra documentación! El puerto de destino es realmente 700. Éste es el número de puerto usado por BuddyPhone durante su funcionamiento. WinRoute ejecutará el encaminamiento en base al puerto de escucha.***

CU-YouSeeMe

Se requiere el siguiente mapeo de puerto para recibir llamadas **CU-SeeMe** a través de NAT:

Protocolo: UDP

IP de escucha: <no especificada>

Puerto de escucha: 7648

IP de destino: la dirección IP de la estación de trabajo en la que funciona el cliente CU-SeeMe

Puerto de destino: 7648

Protocolo: UDP

IP de escucha: <no especificada>

Puerto de escucha: 7649

IP de destino: la dirección IP de la estación de trabajo en la que funciona el cliente CU-SeeMe

Puerto de destino: 7649

Limitaciones:

- En la actualidad no se puede correr más de un cliente CU-SeeMe en una red de área local
- No se puede conectar un "reflector" protegido mediante contraseña.

Acceso Remoto - PC Anywhere

En Esta Sección

PC Anywhere

WinRoute incluye el mejor soporte para PC AnyWhere de Symantec de todos los enrutadores de software del mercado. PC AnyWhere permite a los usuarios acceder y gestionar computadores dentro de una red. Para ello, debe existir el siguiente escenario:

1. PC Anywhere Host debe correr sobre el computador administrado.
2. PC Anywhere Remote debe correr sobre el computador remoto.
3. El mapeo remoto en el computador WinRoute debe configurarse de la siguiente forma:

   Protocolo: TCP/UDP

   IP de escucha: no especificada

   Puerto de escucha (rango): 5631-5632

   IP de destino: la dirección IP del PC Anywhere Host en su red (p. ej., 192.168.1.12)

   Puerto de destino: 5631-5632

Seguridad

Para aumentar la seguridad y evitar que su red se abra hacia el exterior, WinRoute permite a los usuarios elegir una dirección IP específica desde la cual se permite el acceso a través de puertos específicos. Esta configuración sólo permite que determinados computadores o redes accedan a su sistema desde Internet.

Para configurar computadores que puedan acceder a su red debe, en primer lugar, definir un grupo de direcciones (incluso si introduce un solo computador). Para ello, seleccione el menú Configuración=>Avanzada=>Grupos de direcciones.

Cambiar el acceso a diferentes computadores

Puede definir derechos de Administrador en WinRoute para habilitar una conexión directa hacia el host WinRoute. En el host, puede cambiar la IP de destino en el mapeo de puerto y acceder directamente al PC que desee. ¡Sorprendente!

PC Anywhere gateway

Cuando PC Anywhere funciona en el modo gateway (pasarela), el cortafuegos de WinRoute le permitirá al cliente remoto recuperar una lista de host PC Anywhere disponibles que funcionan detrás del cortafuegos. Desde esa lista puede gestionar cualquiera de los host PC Anywhere ubicados detrás del cortafuegos de WinRoute.

En la siguiente descripción se presupone que está utilizando pcAnywhere 9.0 y que no se filtra ningún paquete entrante ni saliente en el cortafuegos de WinRoute.

- En los computadores gestionados detrás del cortafuegos WinRoute se ejecuta PC Anywhere Host con TCP/IP
- En el computador remoto se ejecuta PC Anywhere Remote con TCP/IP
- pcAnywhere está instalado en el cortafuegos de WinRoute usando el modo Gateway. Cuando se configura el dispositivo Gateway, tanto los dispositivos entrantes como los salientes deben ajustarse en TCP/IP

- En el cortafuegos de WinRoute, PC Anywhere debe estar configurado para escuchar en la NIC interna (p. ej., 192.168.1.1). En el sitio web de Symantec encontrará instrucciones para configurar la aplicación PC Anywhere de forma que escuche en una dirección IP/NIC específica.
- Agregue la dirección(es) IP específica(s) de los computadores a gestionar en las opciones de red de PC Anywhere. Para explorar la subred completa, utilice 255 como el último octeto (192.168.1.255).
- Configure el mapeo de puerto en WinRoute de la siguiente forma:

  Protocolo: TCP/UDP

  IP de escucha: NIC externa (206.86.181.25)

  Puerto de escucha: RANGO (5631-5632)

  IP de destino: NIC interna (192.168.1.1)

  Puerto de destino: 5631-5632

Sección de juegos

En Esta Sección

Juegos detrás de NAT

Juegos

Muchos de los juegos actuales soportan un entorno multiusuario. Los usuarios pueden combatir uno contra otro a través de Internet o LAN, o pueden conectarse con uno de los servidores de juegos existentes actualmente en Internet. Los usuarios también pueden operar sus propios servidores de juegos y permitir a sus amigos, familiares o a terceros participar activamente en los juegos.

Para muchos juegos no se requiere ningún ajuste especial en WinRoute. Antes de intentar configurar WinRoute para un juego específico, le recomendamos que use primero una versión de demostración. A diferencia de los servidores Proxy, la arquitectura básica de WinRoute soporta muchos juegos directamente.

Para que algunos juegos funcionen correctamente, es necesario configurar un puerto específico en WinRoute. Los puertos se usan para volver a identificar al jugador en el servidor de juegos (de forma general).

Cuando un juego está asociado con un puerto específico, esto no representa ningún problema para WinRoute. Basta con configurar el mapeo de puerto de WinRoute para que los demás paquetes que lleguen a su red se encaminen al computador del jugador ubicado detrás del cortafuegos.

Los puertos utilizados varían de un juego a otro. Para más información, por favor vea la documentación adjunta de cada juego o llame al servicio técnico del vendedor del mismo. Este manual contiene sólo algunos ejemplos de configuración para los juegos más populares.

Aasheron's call

Asheron's call es un popular juego en la Microsoft Gaming Zone. Para poder jugarlo desde un computador ubicado detrás de GameRouter, debe configurar el siguiente mapeo de puerto:

1 Seleccione el menú *Configuración->Avanzada->Mapeo de Puerto*

2 Realice los siguientes ajustes:

Nombre:	S1	S2	S3	S4	S
Número de puerto:	2300-2400	9000-9013	6667	28800 - 29000	
IP de destino:	IP del PC con el juego	IP del PC con el juego	IP del PC con el juego	IP del PC con el juego	I c j
Protocolo:	TCP/UDP	UDP	TCP	TCP	

Battle.net (Blizzard)

Debe configurar el siguiente mapeo de puerto para poder participar en los juegos en battle.net. Sólo puede participar un jugador a la vez.

Protocolo: TCP/UDP

IP de escucha: no especificada

Puerto de escucha: 6112

IP de destino: dirección IP del computador del jugador (p. ej., 192.168.1.6)

Puerto de destino: 6112

Half-Life

Half-Life

Protocolo: TCP/UDP

IP de escucha: no especificada

Puerto de escucha: 27015

IP de destino: dirección IP del computador del jugador (p. ej., 192.168.1.6)

Puerto de destino: 27015

MSN Gaming zone

La siguiente configuración se ha probado exhaustivamente con MechWarior3 en la **MSN Gaming Zone**. Sólo una máquina puede acceder a la MSN a la vez.

1. Seleccione el menú *Configuración->Mapeo de Puerto*
2. Agregue un nuevo mapeo de puerto

   Protocolo: TCP

   IP de escucha: "no especificada"

   Puerto de escucha: rango 2300 a 2400

   IP de destino: la dirección IP local de la máquina que desee conectar a la MSN

   Puerto de destino: rango 2300 a 2400
3. Agregue otro mapeo de puerto

   Protocolo: UDP

   IP de escucha: "no especificada"

   Puerto de escucha: rango 28800 a 28912

IP de destino: la dirección IP local de la máquina que desee conectar a la MSN

Puerto de destino: rango 28800 a 28912

Quake

Quake 3

Clientes Quake 2/3

No se requiere ningún ajuste especial

Servidor Quake 2/3

Para servidor Maestro:

Protocolo: UDP

IP de escucha: no especificada

Puerto de escucha: 8002 individual

IP de destino: x.x.x.x

Puerto de destino: 8002

Para los clientes que se conecten al servidor Quake3 Arena:

Protocolo: UDP

IP de escucha: no especificada

Puerto de escucha: 27960 individual

IP de destino: x.x.x.x

Puerto de destino: 27960

StarCraft

Jugar con StarCraft

WinRoute Pro incluye un singular soporte para todos los jugadores de StarCraft (Blizzard Entertainment). Varios jugadores de la red conectada a Internet a través de WinRoute Pro pueden divertirse jugando con sus "enemigos" virtuales en Internet.

En la actualidad, el soporte totalmente automático sólo funciona cuando todos los jugadores que participan desde una red utilizan computadores que se encuentran detrás de WinRoute Pro, y no la máquina host.

Para más detalles, visite nuestro sitio en www.tinysoftware.com

Mapeos adicionales para juegos/aplicaciones comunes

Puertos necesarios para varias aplicaciones

Age of Empires II - se requiere mapeo de 2 puertos

Protocolo: TCP

IP de origen: no especificada

Puerto de origen: 47624

IP de destino: dirección IP de la máquina sobre la que corre la aplicación

Puerto de destino: 47624

Protocolo: TCP/UDP

IP de origen: no especificada

Puerto de origen: rango 2300 - 2400

IP de destino: dirección IP de la máquina sobre la que corre la aplicación

Puerto de destino: rango 2300 - 2400

Delta Force

Protocolo: TCP

IP de origen: no especificada

Puerto de origen: rango 3568 - 3569

IP de destino: dirección IP de la máquina sobre la que corre la aplicación

Puerto de destino: rango 3568 - 3569

Dial Pad

Protocolo: UDP

IP de origen: no especificada

Puerto de origen: rango 51200 - 51201

IP de destino: dirección IP de la máquina sobre la que corre la aplicación

Puerto de destino: rango 51200 - 51201

Gamespy

Registro

Protocolo: UDP

IP de origen: no especificada

Puerto de origen: 25635

IP de destino: dirección IP de la máquina sobre la que corre la aplicación

Puerto de destino: 25665

Para los juegos propiamente dichos

Protocolo: UDP

IP de origen: no especificada

Puerto de origen: rango 25000 - 30000

IP de destino: dirección IP de la máquina sobre la que corre la aplicación

Puerto de destino: rango 25000 - 30000

Kali - se requiere un mapeo de 3 puertos

Protocolo: UDP

IP de origen: no especificada

Puerto de origen: 2213

IP de destino: dirección IP de la máquina sobre la que corre la aplicación

Puerto de destino: 2213

Protocolo: UDP

IP de origen: no especificada

Puerto de origen: 6666

IP de destino: dirección IP de la máquina sobre la que corre la aplicación

Puerto de destino: 6666

Protocolo: UDP

IP de origen: no especificada

Puerto de origen: 57

IP de destino: dirección IP de la máquina sobre la que corre la aplicación

Puerto de destino: 57

Mplayer

Protocolo: TCP/UDP

IP de origen: no especificada

Puerto de origen: 8000 - 9000

IP de destino: dirección IP de la máquina sobre la que corre la aplicación

Puerto de destino: 8000 - 9000

PCanywhere versiones 2.0 - 7.51 - se requiere un mapeo de 2 puertos

Protocolo: TCP

IP de origen: no especificada

Puerto de origen: 65301

IP de destino: dirección IP de la máquina sobre la que corre la aplicación

Puerto de destino: 65301

Protocolo: UDP

IP de origen: no especificada

Puerto de origen: 22

IP de destino: dirección IP de la máquina sobre la que corre la aplicación

Puerto de destino: 22

Quicktime - se requiere un mapeo de 2 puertos

Protocolo: TCP

IP de origen: no especificada

Puerto de origen: 554

IP de destino: dirección IP de la máquina sobre la que corre la aplicación

Puerto de destino: 554

Protocolo: UDP

IP de origen: no especificada

Puerto de origen: rango 6970 - 6999

IP de destino: dirección IP de la máquina sobre la que corre la aplicación

Puerto de destino: rango 6970 - 6999

RTSP

Protocolo: UDP

IP de origen: no especificada

Puerto de origen: rango 6970 - 7170

IP de destino: dirección IP de la máquina sobre la que corre la aplicación

Puerto de destino rango 6970 - 7170

VNC

Protocolo: TCP

IP de origen: no especificada

Puerto de origen: 59xx (según el número de display)

IP de destino: dirección IP de la máquina sobre la que corre la aplicación

Puerto de destino 59xx

Protocolo: TCP

IP de origen: no especificada

Puerto de origen: 58xx

IP de destino: dirección IP de la máquina sobre la que corre la aplicación

Puerto de destino 58xx

GLOSARIO DE TÉRMINOS

A

ARP

El protocolo de resolución de dirección (Address Resolution Protocol) asocia una dirección IP con una dirección de hardware, pidiendo a la máquina transmisora una información adicional denominada dirección MAC. WinRoute sólo utiliza ARP para fines de registro, con la finalidad de aumentar la seguridad.

B

Banderas (Flags)

Las banderas son una parte del paquete que contiene información. Ellas contienen información adicional sobre el paquete usado por los enrutadores. A continuación una lista de las banderas indicadas por WinRoute:

SYNC - Synchronize - sincronizar; el paquete que establece una conexión TCP

ACK - Acknowledge - confirmar; confirmación sobre el intercambio de datos

RST - Reset - reponer; petición para reestablecer la conexión

URG - Urgent - urgente; paquete urgente

PSH - Push - impulsar; solicitud para la entrega inmediata del paquete a las capas superiores

FIN - Finalize - finalizar; finalizar la conexión

BOOTP

Protocolo de carga inicial (Bootstrap Protocol), que simplemente se refiere a aquéllos computadores dentro de una red de área local diseñados para aceptar una dirección IP dinámicamente de un servidor DHCP.

Buzones en WinRoute

Los buzones se encuentran en un directorio separado en donde se ha instalado WinRoute. Generalmente en c:/Archivos de Programa/WinRoute/Mail.

No se crea ningún buzón más después de la instalación, incluso si se crean usuarios. Los buzones se crean físicamente DESPUÉS de que llega el primer mensaje de correo electrónico para un usuario.

C

Caché

Se refiere a la memoria en la que los datos se almacenan temporalmente. WinRoute utiliza la memoria caché para el almacenamiento temporal de páginas web, con el fin de mantener el ancho de banda.

Cortafuegos (Firewall)

Un módulo de filtro ubicado en una máquina que funciona como pasarela (gateway), encargado de examinar todo el tráfico entrante y saliente, para determinar si debe ser encaminado a su destino. WinRoute pone a disposición un cortafuegos muy eficiente de la siguiente forma: funcionalidad NAT, la asignación de reglas para direcciones IP específicas y la capacidad de registrar determinadas informaciones que van en una dirección, para que puedan ser autorizadas al regreso.

D

DHCP

El protocolo de configuración host dinámica (Dynamic Host Configuration Protocol) es un protocolo para organizar y simplificar la administración de direcciones IP para las máquinas locales. En muchos casos (como en el caso de WinRoute) hay un servidor DNS integrado en el servidor DHCP, para una simplificación aún mayor. Cuando se especifica la dirección IP de un dispositivo de red determinado, generalmente el dispositivo conectado a Internet, DHCP usará los valores DNS asociados con el dispositivo en cuestión.

Dirección IP

La dirección IP es un número único de 32 bits que identifica a un computador en una red IP. En Internet, se asigna una dirección IP única a cada computador. Cada paquete que viaja por Internet contiene la información que indica desde qué dirección fue enviado (dirección IP de origen) y a qué dirección debe ser entregado (dirección IP de destino).

Dirección MAC

La dirección MAC (Media Access Control) es más específica que la dirección IP y no puede ser cambiada, ya que es específica de cada dispositivo de hardware de red.

DNS

El sistema de nombres de dominio (Domain Name System) es un esquema de asignación de nombres a las direcciones IP. Por ejemplo, www.tinysoftware.com es un nombre de dominio y está asociado con una dirección IP. Un servidor DNS devuelve las direcciones IP correspondientes a los nombres de dominio. Utilizamos el sistema de nombres de dominio porque es más fácil recordar un nombre de dominio que una cadena de números.

E

ETRN

ETRN es un comando usado por los servidores SMTP para negociar un periodo de tiempo más largo. Tras establecer una conexión, el servidor SMTP debe pedir el correo SMTP.

El comando ETRN se usa siempre que un servidor SMTP no está "en línea" 24 horas y el correo electrónico para dicho servidor SMTP debe guardarse en una memoria temporal en otro servidor SMTP.

F

FTP

El protocolo de transferencia de ficheros (File Transfer Protocol) es un protocolo de aplicación usado para transferir, actualizar, borrar, desplazar, cambiar el nombre o copiar datos en Internet.

I

ICMP

El protocolo de mensaje de control de Internet (Internet Control Message Protocol) utiliza datagramas para notificar errores en la transmisión entre el host y la pasarela.

Interfaz de red

La interfaz de red es el dispositivo que conecta al computador con otros computadores a través de un medio de comunicación. Una interfaz de red puede ser una tarjeta Ethernet, un modem, una tarjeta RDSI, etc. El computador transmite y recibe paquetes mediante la interfaz de red.

IPSEC

En pocas palabras, mediante la seguridad del protocolo de Internet (Internet Protocol Security) se puede realizar una conexión en red privada empleando facilidades de autentificación y codificación del transmisor. WinRoute soporta las variantes IPSEC de Novel y Cisco.

L

LAN

Una red de área local (Local Area Network, LAN) es un grupo de computadores interconectados con la capacidad de compartir recursos.

M

Mapeo de puerto

El mapeo de puerto (o traducción de la dirección de puerto, Port Address Translation - PAT) es el proceso en el cual los paquetes que llegan a la interfaz se controlan según su número de puerto y la dirección IP a la que desean acceder. En base al número de puerto, la dirección IP encuentra a estos paquetes, que son transmitidos a la dirección IP de clase privada predefinida de la red local.

Máscara de red

La máscara de red se usa para agrupar direcciones IP. Existe un grupo de direcciones asignado a cada segmento de la red. Por ejemplo, la máscara 255.255.255.0 agrupa 254 direcciones IP. Si tenemos, por ejemplo, una subred 194.196.16.0 con la máscara 255.255.255.0, las direcciones que podremos asignarles a los computadores en la subred irán de 194.196.16.1 hasta 194.196.16.254.

N

NAT

Mediante NAT - la facilidad de traducción de la dirección de red (Network Address Translator) - se puede conectar a Internet mediante una sola dirección IP y los computadores dentro de la red utilizarán la Internet como si estuvieran conectados directamente a ella (con algunas limitaciones).

Es posible conectar una red completa utilizando una sola dirección IP registrada, dado que el módulo NAT sobrescribe las direcciones de origen en los paquetes transmitidos desde los computadores ubicados en la red de área local, con la dirección del computador sobre el que corre WinRoute.

NAT difiere considerablemente de muchos servidores proxy y de pasarelas a nivel de aplicación, ya que éstos no son capaces la cantidad de protocolos que soporta NAT.

P

Paquete

Un paquete es una unidad de datos de comunicación básica usada durante la transmisión de datos de un computador a otro. Cada paquete contiene una cantidad determinada de datos. La longitud máxima de un paquete depende del medio de comunicación. Por ejemplo, en las redes Ethernet la longitud máxima es de 1500 bytes. En cada capa, el contenido de un paquete se puede dividir en dos partes: la parte de encabezamiento y la parte de datos. El encabezamiento contiene información de control de la capa específica, y la parte de datos contiene los datos que pertenecen a la capa superior. En la sección referente al filtro de paquetes encontrará informaciones más detalladas sobre la estructura de los paquetes.

Pasarela (Gateway)

El punto de entrada de una red a otra. Las pasarelas se encargan de distribuir correctamente los datos que entran y salen de una red de área local. WinRoute debe instalarse en la máquina que funciona como pasarela, denominada también computador host.

POP3

El protocolo **POP3** es usado, en la mayoría de los casos, por el software cliente de correo electrónico para recoger el correo de los buzones, en los servidores de correo compatibles con POP3. El servidor de correo de WinRoute también dispone de esta capacidad, es decir, puede recoger el correo electrónico automáticamente en cualquier servidor de correo compatible con POP3, y distribuirlo a los buzones de los destinatarios locales.

El protocolo POP3 es un protocolo **TCP** que funciona en el **puerto 110**. Si desea acceder al servidor de correo POP3 que funciona detrás del computador WinRoute (para recoger su correo electrónico PROVENIENTE de Internet), debe configurar un **mapeo de puerto** para el protocolo TCP, puerto 110 hacia la dirección IP de **clase privada** del PC sobre el que corre el servidor de correo.

PPTP

PPTP - el protocolo de túnel de punto a punto (Point To Point Tunnelling Protocol) - es un protocolo VPN utilizado por los sistemas operativos de Microsoft para crear conexiones codificadas entre dos computadores.

Protocolo

Define reglas para la transmisión de datos.

Proxy

Proxy es otro método para compartir un acceso a Internet. Proxy opera con los datos en un nivel de protocolo más alto, por lo que compartir el acceso a Internet mediante servidores Proxy nunca ha sido fiable. Además, se requiere una pasarela de aplicación especial para el protocolo de conexión en red.

Puerto

Un puerto es un número de 16 bits (el rango permitido es de 1 hasta 65535) usado por los protocolos de la capa de transporte - a saber, el protocolo TCP y el UDP. Los puertos se utilizan para direccionar aplicaciones (servicios) que corren sobre un computador. Si hubiera una sola aplicación de red ejecutándose en un computador, no se necesitarían números de puerto y la dirección IP bastaría para direccionar los servicios.

Sin embargo, es posible que se ejecuten muchas aplicaciones simultáneamente en un computador determinado, y que sea necesario diferenciarlas. Para este fin se emplean los números de puerto. Por tanto, un número de puerto puede considerarse como la dirección de una aplicación dentro de un computador.

R

RAS

El servicio de acceso remoto (Remote Access Service) se refiere a la capacidad de establecer una comunicación por marcación con otro computador o con otra red de forma remota. En el contexto de WinRoute, RAS simplemente se refiere a una comunicación por marcación.

Registros MX

Los registros MX contienen información sobre otros servidores de correo en Internet. Mediante los registros MX puede pasar por alto al servidor de correo de su ISP y entregar correo electrónico directamente al servidor de correo de destino.

Esto presenta ventajas si el servidor de su proveedor de servicios *no es fiable*. Por otro lado, si intenta enviar correo electrónico *directamente al destino*, eso puede repercutir en el periodo de tiempo de entrega del correo. En caso de que no se pueda acceder al *servidor de correo de destino*, el correo electrónico *no se transmite* y permanece en la cola de espera de correo saliente de su servidor de correo WinRoute.

S

SMTP

SMTP (Simple Mail Transfer Protocol) se usa para la comunicación directa entre servidores de correo (como, por ejemplo, el servidor de correo de WinRoute y el servidor de correo de su ISP) y para transmitir correo electrónico saliente desde su software cliente de correo electrónico. SMTP es un protocolo de "una vía" - es decir, el servidor de correo puede transmitir o recibir correo, pero no puede recoger el correo electrónico en otro servidor mediante este protocolo.

El protocolo SMTP es un protocolo TCP que funciona en el **puerto 25**. Si desea acceder a este protocolo con el servidor de correo que corre detrás de o sobre el computador WinRoute (para permitir que otro servidor de correo le envíe correo electrónico o para usar este servidor de correo para su email saliente cuando está en su LAN), debe configurar un **mapeo de puerto** para el protocolo TCP, puerto 25 hacia una dirección de **clase privada** del PC sobre el que corre el servidor de correo.

T

Tabla de encaminamiento

Las tablas de encaminamiento son el conjunto de reglas generadas por los sistemas operativos de Microsoft, en base a los ajustes que realice en la configuración del protocolo TCP/IP. Las tablas de encaminamiento se usan en WinRoute como el conjunto de reglas para encaminar los paquetes. Para ver la tabla de encaminamiento llame la ventana de MS-DOS e introduzca el comando `route print`.

TCP/IP

TCP/IP es una suma de protocolos de conexión en red, usados para la comunicación entre computadores. Todos los protocolos se basan en paquetes, es decir que los datos transmitidos se dividen en partes pequeñas y se transmiten a lo largo de la red. Los protocolos TCP/IP son: IP, TCP, UDP, ICMP y otros protocolos basados en IP.

U

UDP

El protocolo de datagrama de usuario (User Datagram Protocol) utiliza un tipo especial de paquete denominado datagrama. Los datagramas no requieren una respuesta, ya que son de una sola vía. Por lo general, los datagramas se usan en medios continuos, porque la pérdida ocasional de un paquete no afecta al producto final de la transmisión.

V

VPN

Una red privada virtual (Virtual Private Network) abarca varias redes de área local con la capacidad de compartir recursos a lo largo de Internet mediante la creación de un túnel directo, que ejecuta la codificación y la descodificación en ambos extremos. WinRoute soporta las redes privadas virtuales a través de PPTP.

INDEX

D

E

F

G

H

I

S

T

U

V