Reference Guide

WinRoute Pro

Version 4.2

Kerio Technologies

Table of Contents

READ-ME-FIRST

Dear Customer,

Thank you for purchasing WinRoute Pro. Kerio Technologies, a leader in security software for Windows operating systems, is proud to offer this powerful, yet easy to use, secure Internet sharing solution.

WinRoute Pro is a network application that transforms a Windows PC into a substitute for much higher priced hardware based routers and firewalls. As with any network firewall, it is important that the network is properly configured prior to implementing our software. Therefore, a basic understanding of TCP/IP networking principles is necessary.

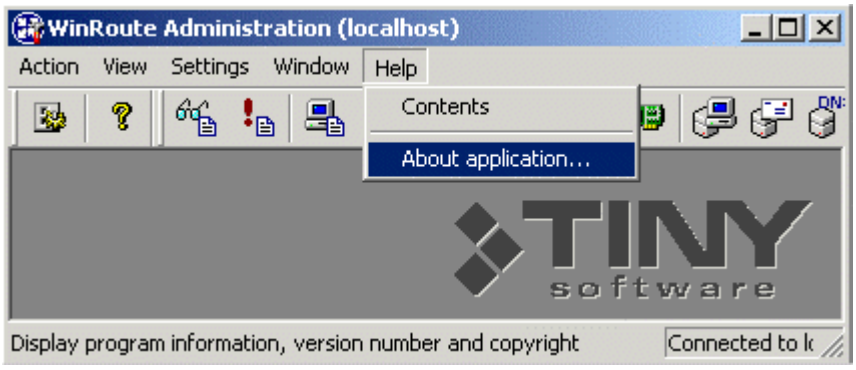
This manual includes several examples of network configurations, as well as a quick checklist to help guide you through your setup. We strongly recommend reviewing this documentation very carefully. Please visit our online support area for additional tips, FAQs and updates.

Kerio Technologies

www.kerio.com

INSERTING THE LICENSE

First make sure that the winroute engine is running so you can access the administration. After you have connected to the administration go to the help menu -> about application as shown below. You should see a set license button, click on it and insert your license key.



WinRoute Maintenance

WinRoute does not include an auto-update feature. New builds are published at www.kerio.com as they become available (typically once every two months). After downloading the latest version you may install it over top of the current WinRoute. All settings and license information will remain. If you have a WinRoute version prior to 4.x refer to www.kerio.com for upgrade information.

CONTACT INFORMATION

Technical Support

Before contacting our technical support team please be sure you have read the 'Quick Checklist and our FAQs' available at www.kerio.com.

Phone support is available at no charge to WinRoute Pro customers and trial users from 8-5 M-F Pacific Standard time. Emails are typically processed within one business day.

Phone: + 1 (408) 496-4500

Email: support@kerio.com

Sales

Phone orders are processed by Element 5.

For pre-sales inquiries please contact Technical Support.

+1 (724) 850-8186 (International)

+49 (0) 221-31088-30 (Europe)

1-800-406-4966 (US)

General

Corporate headquarters

Kerio Technologies Inc.

2855 Kifer Road

Santa Clara, CA 95051

USA

Phone: + 1 (408) 496-4500

Fax: + 1 (408) 496-4506

info@kerio.com

www.kerio.com

European offices

Kerio Technologies France SARL

57, rue d'Amsterdam

75008 Paris

France

Tel : +33(0)1.53.32.17.30

Fax : +33(0)1.53.32.17.32

sales-france@kerio.com

www.kerio.com

Kerio Technologies UK

119 Howard Drive

Letchworth, SG6 2BX

United Kingdom

Tel : +44 1462 670 501

Fax : +44 1462 685 908

info@kerio.co.uk

www.kerio.co.uk

Kerio Technologies CR

Sedlackova 16

301 11 Plzen

Czech Republic

Tel: +420 (19) 733-8901

Fax: +420 (19) 733-8921

info@kerio.cz

www.kerio.cz

CHAPTER 1

WINROUTE DESCRIPTION

In This Chapter

Extensive Protocol Support

WinRoute supports all standard Internet protocols including:

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, ssh, systat, tacacs, uucpover IP, whois, xtacacs and more.

WinRoute Summary

WinRoute Pro is the ultimate **Internet Router - Firewall** software making it virtually effortless to set all of the computers in your network up to share a single Internet connection! Connect through a dial-up line, DSL, Cable, ISDN, LAN, T1, Radio and DirecPC. It's that easy!

Remote Administration

WinRoute Administrator provides the configuration and settings on the WinRoute Engine. WinRoute Administrator is a separate application (wradmin.exe) that may be run from any computer with a connection to the WinRoute Engine computer. Access to the Engine is secured by strong encryption and a password.

Logging

WinRoute Pro provides an administrator with ultimate control over the traffic flowing through the host computer it is running on. The Administrator may benefit from analyzing the flow of TCP, UDP, ICMP, ARP packets, DNS requests, driver information and more. All operations have a Time Stamp.

NAT IP Router

WinRoute includes the (best) implementation of Network Address Translation (NAT) technology available today. It is designed to provide users with the ultimate in routing capability and network protection. The NAT driver written exclusively for WinRoute offers a security solution comparable to more expensive products at substantially less cost.

Advanced NAT Routing

Advanced NAT allows the option to modify the source IP address of outgoing packets based on various criteria. This ensures easy integration of LANs behind WinRoute into the corporate WAN environment with different segments, demilitarized zones, virtual private networks etc.

Hosting Servers behind WinRoute

WinRoute's NAT, when not excluding the host, will prevent all unrequested traffic from entering your entire network, including the computer that WinRoute is installed on. Port Mapping/Forwarding allows users to decide how they want to divert IP packets passing through a NAT'd interface. With WinRoute, users can set packets coming to a specific port to be passed to a specific internal computer. This allows them to run a web server, mail server, FTP server, VPN server or virtually any other type of server securely behind the firewall.

Firewall Security

WinRoute gives users a comparable level of firewall capability found in far more expensive solutions through a combination of its NAT architecture and its ability to operate on a low level. This allows WinRoute to capture both incoming and outgoing packets, which makes it unbreakable. Anti-spoofing is an add-on to WinRoute's packet filtering, for further protection of the LAN against attacks where the intruder falsifies source IP addresses.

Simple Network Configuration

The DHCP server and DNS forwarder included in WinRoute greatly simplify the task of network administration, requiring minimal effort and no client configuration.

Mail Server

WinRoute's mail server, complete with SMTP relay and POP3 server, allows virtually unlimited aliases and automatic mail sorting. It is an ideal solution for small to medium sized businesses that host their own domain and would like to have full control of each user's mailbox. Users can have multiple addresses and receive mail from various accounts. Authentication and anti-spam ensure that your mail server cannot be abused by outside sources.

HTTP Cache

WinRoute's architecture includes an innovative Cache engine. Unlike proxy servers with caching functionality, WinRoute's cache stores passing data in one file of pre-defined length instead of using a single file for each object. This significantly saves the disc space occupied by the cache, especially in FAT16 (most of Windows95) environments.

WinRoute architecture

WinRoute Architecture

For advanced Internetworking, it's helpful to understand how WinRoute works. From the explanation and examples listed below, WinRoute proves to be an excellent solution for almost any network configuration.

Firewalls are typically built on hardened platforms and the software itself is typically difficult to circumvent. However, a major weakness in many network security devices is during the brief window of time between when the hardware is actively capable of routing traffic and when the software takes over control of the network interfaces. Within this critical juncture, security can be completely compromised.

WinRoute’s driver, or Engine, activates as the core files of the Windows operating system (the kernel) load themselves into memory; specifically, the engine loads before the NDIS (Network Device Interface Specification) modules are loaded, so that no network connectivity is supported before WinRoute is active. Thus, protection of all interfaces is active before malicious traffic or other attacks can be mounted on the system. This compares favorably to standalone intrusion-detection-type products that run as a service and are not active until after the system has booted.

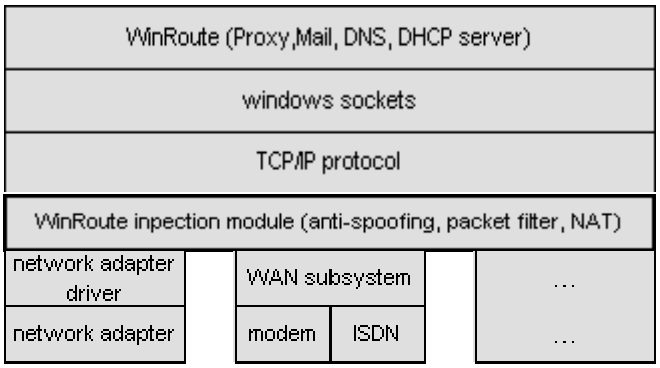
WinRoute "wraps" NDIS in a proprietary fashion such that all TCP/IP traffic is shunted from the network interface card (NIC) driver to the Engine before it proceeds up the network communications stack to the operating system itself.

This low-level insertion into the operating system allows the WinRoute Engine a unique perspective on all network traffic arriving on any interface (whether inbound or out). As with many enterprise-class firewall products such as Check Point's Firewall-1, WinRoute is allowed to make the first decision about whether to allow or deny a given packet. Once again, this prevents malicious attacks against other aspects of the operating system or other software that could bypass the security offered by a firewall. This is certainly desirable for externally facing Internet gateways, but can also provide great benefits to standalone hosts with high security or anonymity requirements, such as an intrusion detection system. Intrusion detection software such as Real Secure from Internet Security Systems (ISS) would be practically invisible on a host protected by WinRoute.

Lastly, the WinRoute Engine takes over all communications routing functionality from the underlying Windows operating system (whether it be Windows 9x, NT, or 2000). This ensures that if for some reason the WinRoute Engine were to fail, no traffic would be routed between networks. This "fail-closed" stance has been the traditional default for firewall configurations for many years, and serves to protect private networks in the case of common system failures.

1. **Total Security**
   WinRoute works **below the TCP/IP stack**. In another words - it captures both **outgoing** and **incoming** packets **BEFORE** they have the chance to enter your computer.

This advanced design makes WinRoute's security almost **unbreakable**



2. **Total Protocol Support**
   WinRoute is a software ROUTER. As such, WinRoute can allow almost any Internet protocol to pass through. At the same time, WinRoute checks each packet utilizing the advanced security and firewall features inherent in the software design. On systems running Windows 95 and 98, WinRoute handles the routing of packets. On systems running Windows NT, the NT operating system performs the routing and WinRoute manages the NAT functionality and other data.

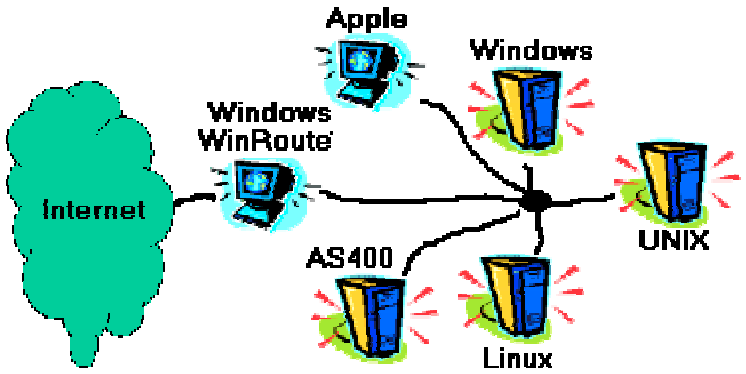
3. **Total Flexibility**
   WinRoute performs NAT (Network Address Translation) on the interfaces of your choice. WinRoute also performs any preset security rules on the specific interfaces. This gives the user a wide range of freedom when designing and configuring security options.

Mixed OS networks (Unix, Mac, AS400)

Connecting multiple operating systems environments (Linux, Unix, AS400, Apple)

WinRoute is suitable for connecting multiple operating system type environments to the Internet. WinRoute acts as a software router. As such, it supports any standard TCP/IP environment.

- ***NOTE: A Windows based operating system must host the WinRoute application.***



VPN support

WinRoute is fully capable of passing traffic from the two most popular VPN protocols in use today: the IP Security protocol (IPSec) proposed by the IETF, and the Point-to-Point Tunneling protocol, made popular in recent years due to its inclusion with Microsoft Windows client operating system software.

Remote Administration

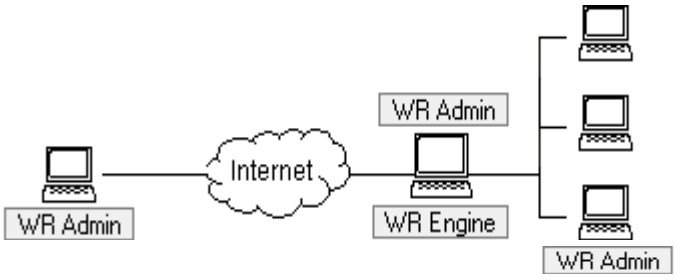
WinRoute Pro provides users with the benefit of remote administration. With proper settings and rights in place, it is possible to securely administer your firewall from any place in the world. Access to the Engine is secured by strong encryption and password.

WinRoute Pro components

WinRoute Pro 4.x consists of three modules:

WinRoute Engine performs all routing and analysis operations (NAT, packet filtering, port mapping etc.). You may Start/Stop the WinRoute Engine from the WinRoute Engine Monitor or if running Windows NT, directly from NT services option. WinRoute Engine runs invisible as a service under Windows2000/NT/98 or 95.

WinRoute Engine Monitor is the monitoring application that shows whether the WinRoute Engine is running or not. It appears as the little blue icon at the right lower corner of your desktop.



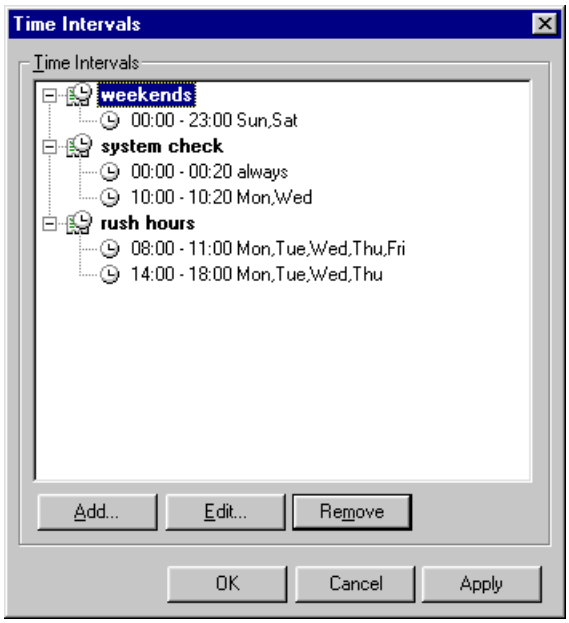
WinRoute Administrator provides the configuration and settings for the WinRoute Engine. The WinRoute Administrator is a separate application (wradmin.exe) that may be run from any computer and connect via a TCP/IP connection to a WinRoute computer.

Time intervals

You may define Time Zones – predefined time intervals – in order to perform certain actions. These actions may be:

- Packet filtering
- Email Exchange (send and receive)
- Connection to the Internet
- Advanced NAT settings

A Time Zone is a group of Time Intervals. As a result you may create non-homogeneous time space consisting of several time intervals.



- ***Example: You may create a time zone called "Holidays and evenings" that will cover: Saturdays, Sundays, Mondays from 4PM to 6PM, Tuesdays from 5PM to 7PM***

To define a time zone:

1 Go to menu *Settings=>Advanced=>Time Intervals*

2 Name the time zone

3 Add the new time interval

Anti-Spoofing

WinRoute provides anti-spoofing capabilities, which prevents packets with invalid source addresses from originating within a network. Anti-spoofing could have prevented the ICMP smurf attacks reported in February 2000 with the distributed denial of service attacks on such major Web sites as Yahoo and Buy.com. WinRoute users can rest comfortably knowing that their networks are unlikely sources of such attacks if they implement this feature.

DHCP overview

In a network, each computer has to have its TCP/IP protocol properly configured. This means that the IP address, network mask, default gateway address, DNS server address, etc. must be configured on each computer. If the maintainer has to set the parameters manually on a large number of workstations, it is difficult to avoid mistakes, e.g. using an address twice - which may cause collisions and consequently also an incorrect function of the entire network.

Dynamic Host Configuration Protocol is a feature of WinRoute designed to simplify the task of network administration. DHCP is used for a dynamic configuration of the TCP/IP protocol on computers. During start-up, the DHCP client computer sends a request. When the DHCP server receives the request, it chooses TCP/IP configuration parameters for the client. The common parameters are IP address, network mask, default gateway, DNS server address, client's domain name, etc.

The server may assign a configuration to the client for a limited time only (the so-called lease time). The server always assigns the IP address so that it does not collide with any other address assigned through DHCP to another client.

With a DHCP server available, it suffices to enable the "Obtain IP address from DHCP server" option and the DHCP server takes over the responsibility for proper configuration of TCP/IP on workstations. This may help to significantly lower the network maintenance and management costs.

- ***If some computers in your network are not configured dynamically by DHCP, but have a fixed configuration instead, you must make sure the parameters used by DHCP do not conflict with the ones used in the fixed configurations.***

About DNS forwarding

Each computer connected to the Internet is identified by a unique numeric IP address. In order to connect to a computer on the Internet, its address must be known to the computer, which is creating the connection. Since IP addresses are difficult to remember, Domain Name Service was created.

The DNS is a database of descriptive names, which are supposed to be easy to remember. Thus the user does not have to know the IP address of the server she/he wants to communicate with. It suffices to enter the appropriate name (e.g. www.yahoo.com) and DNS will find the actual IP address.

DNS Forwarder in WinRoute

WinRoute is equipped with a DNS module that is able to forward DNS queries to a chosen DNS server on the Internet. The DNS module stores the results of the queries in its internal cache where they are kept for a certain time. Subsequent repeated queries are then answered using the cached data without the need to wait until an answer from the Internet arrives.

The DNS forwarder in WinRoute is also equipped with a user-defined HOSTS file. After a DNS query arrives, WinRoute looks at the HOSTS file prior to forwarding the DNS query to the Internet. If the corresponding record is found, the query is answered by its value, if not it is forwarded to another DNS server.

POP3/SMTP Services

WinRoute includes a relay SMTP server and **POP3** server. You may use these services the same way you would use the mail server of your ISP.

POP3 service: WinRoute can download email from remote POP3 servers and deliver mail to each WinRoute user account. Each WinRoute user may have several different remote POP3 accounts through WinRoute. This allows users to gather all mail from one central location, even when they are outside the WinRoute network. You can also deliver mail to a group of users.

Sorting: An advanced feature of WinRoute's remote POP3 is the ability to filter gathered email by recipient. WinRoute checks the 'to' and 'cc' fields and can deliver to a WinRoute user or group based on the content in those fields.

SMTP Relay: WinRoute's SMTP service functions as a mail forwarder so all email can be collected from and sent through the same location.

Email scheduling: Email can be sent immediately or during intervals. Mail must be gathered during user-defined intervals. For dial-up connections the connection can be automatically opened then closed for sending/receiving email.

Anti-Spam: If you host your own domain it is smart to restrict SMTP access so that WinRoute will not be treated as a spam server. Anti-Spam requires users who are sending email to any address outside of your domain to first authenticate into WinRoute. You can allow anonymous relaying to user-defined domains, or only users from specific IP addresses may relay to any domain through WinRoute.

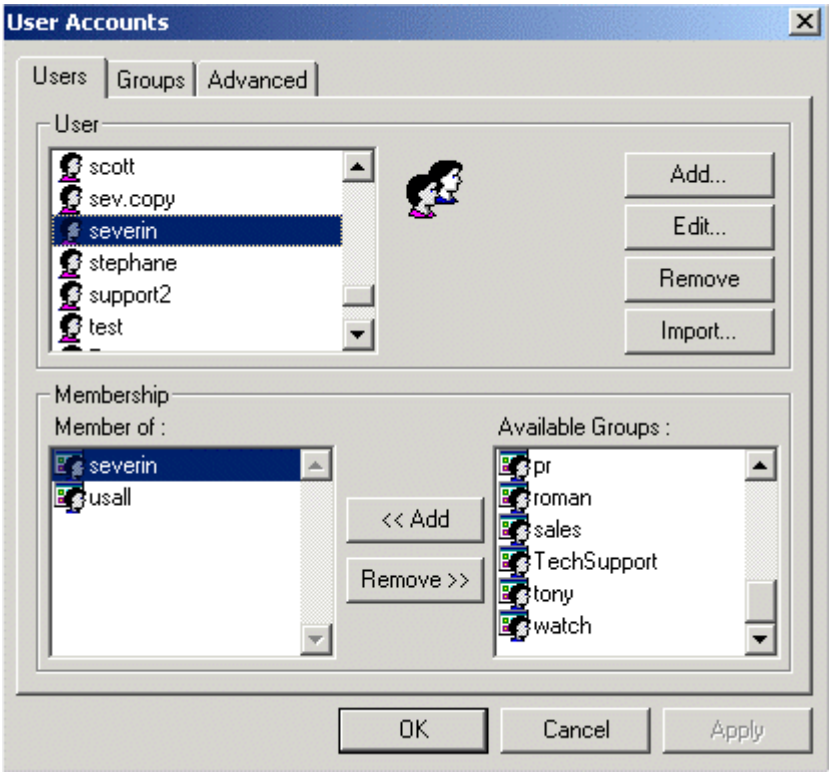
Aliasing: If you host your own domain, mail will be delivered to the WinRoute computer and dropped in the appropriate user's mailbox. Aliases can be configured so that each WinRoute user can have multiple email accounts within your domain.

Logging: For diagnostic and regulatory reasons the WinRoute administrator can trace all email processing through the Mail and Debug logs.

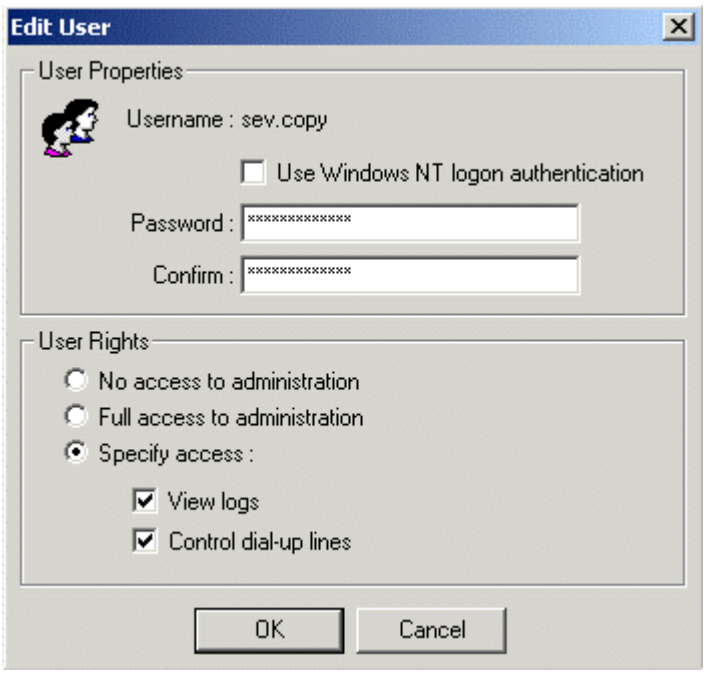
If you do not use the mail server

It is not necessary to use WinRoute's mail server. You may still use the mail server of your ISP or another third party mail server. In which case, WinRoute will act as the router/firewall that will allow your email client software to communicate with the email server of your ISP by using Network Address Translation.

WinRoute requires specific user accounts for use with the built-in Mail Server, Proxy Server, and Administration component.



Each user has its own rights for Administering WinRoute.



Users can be added manually or imported from a domain for easier administration.

NAT (Network Address Translation)

Intro to NAT

NAT - Network Address Translation

Network Address Translation, or NAT, is one of WinRoute's most powerful security features. NAT is an Internet draft standard protocol for hiding private network addresses behind a single address or multiple addresses. A version of NAT called IP Masquerading has been popular for many years with the Linux community and WinRoute is one of few products for the Windows platform to actually provide entry-level NAT functionality. NAT works by translating the source information of each packet leaving the NAT'd interface. When incoming traffic arrives at the NAT'd interface, its destination information is compared to the NAT table providing the functionality of stateful packet inspection. If there is no entry in the table the packet is rejected. Otherwise, it is retranslated to the proper destination information and routed back to the client.

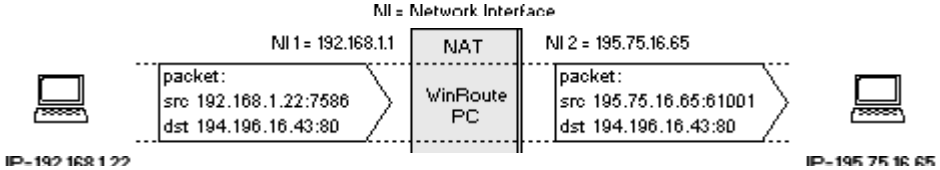
How NAT works

Network Address Translation (NAT) is a process that modifies packets sent from/to the local area network to/from the Internet or other IP based networks.

On the way out

Packets passing through the address translator engine on the way **from** the LAN are changed or translated to look as if they came from the computer running NAT (this computer is directly connected to the Internet). What actually happens is the "source" IP address is changed in the header and replaced by the (public) IP address of the "NAT'd" interface.

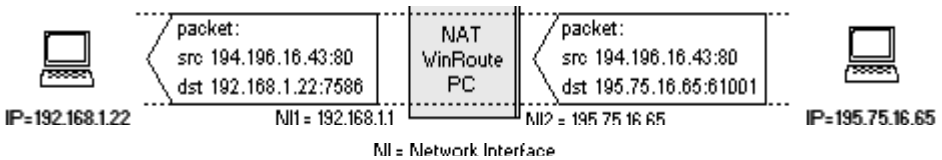
The NAT engine also creates a record table of information for each packet that passed through to the Internet or other public network.



On the way back

Packets passing through the NAT on the way **TO** the LAN are checked against the records kept by the NAT engine. There, the "destination" IP address is changed (based on the records in the table) back to the specific internal private class IP address in order to reach the computer on the LAN .

Remember that the packet originally returns with the public IP address of the NAT'd computer as its "destination". The NAT engine had to change this information in order to deliver the packet to the correct recipient within the local network.

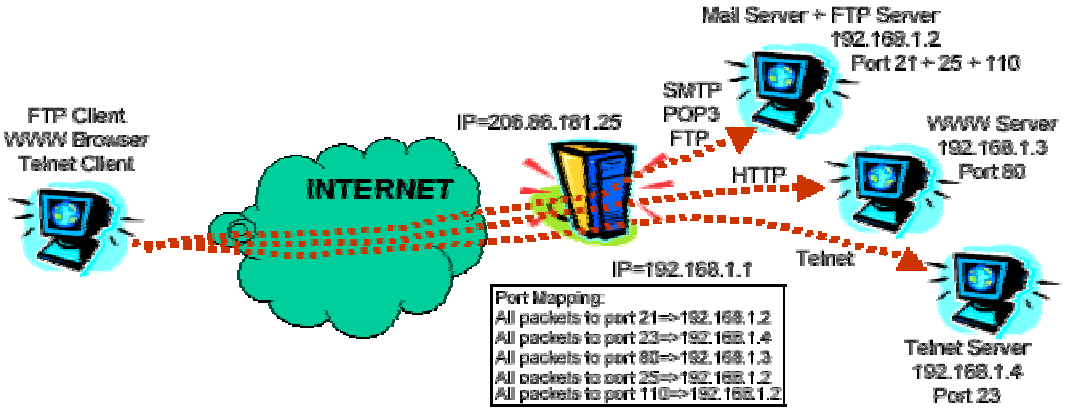


Port Mapping

WinRoute performs NAT, which makes the protected network inaccessible from outside. Using port mapping, public services like a WWW server or an FTP server, and others running on your private network may become accessible from the Internet.

How Port Mapping Works

Each packet received from the outside network (from the Internet) is checked whether its attributes (that is the protocol, destination port, and destination IP address) comply with an entry in the port mapping table (Protocol, Listen Port, Listen IP). If the arriving packet meets the desired criteria, the packet is modified and routed to the IP address within the protected network defined as the "Destination IP" in the table's entry and to the port defined as "Destination port".



For example if you run a telnet server at internal IP 192.168.1.4 and you want to allow users from the Internet to access it. There will be requests from Internet users coming to your WinRoute computer on the external IP address that is equal to the DNS record for your web server www.yourdomain.com. As all requests to the telnet server are coming on port 23 you will set up port mapping saying that all TCP communication on port 23 will be diverted to the internal IP address 192.168.1.4.

Setting NAT on both interfaces

If you have a subnet of **ONLY** servers and you would like the maximum amount of security, you may want to consider the following multi-NAT configuration.

Important Notes:

- Servers such as FTP (passive mode only) open a new connection to the client. Servers of this nature will not work under this specific scenario.
- The NAT table is limited in its capacity; therefore this configuration is not suggested for services that may receive more than one hundred simultaneous connections. To configure security for traffic intensive servers refer to the chapter on setting up security.
- Setting up NAT on both interfaces will NOT allow you to use WinRoute for Internet sharing.
- The WinRoute computer must be assigned an IP address within the same subnet as your local servers.

	Originally recommended	In this scenario
NAT on Internet interface	ON	ON
NAT on internal (LAN) interface	OFF	ON
WinRoute's internal interface IP address as the default gateway for the other computers within the network	YES (a MUST)	NO (not necessary)

In other words, using WinRoute will allow you to make certain services accessible from the Internet WITHOUT a need to change the network configuration. The following example services (and many others) may be handled under the multi-NAT'd environment.

- Telnet
- SSH
- HTTP/HTTPS
- POP/SMTP
- PC Anywhere/VNC
- FTP (active mode only)

For this configuration follow the steps below:

1. Add a computer with two interfaces to your network. One Interface (external) will link to the Internet or other public network, while the other (internal) will link to your existing network.
2. Configure the necessary TCP/IP properties for the (external) interface connected to Internet or other public network.
3. Configure the necessary TCP/IP properties for the (internal) interface connected to the local network.

4. In the interface table enable NAT for both interfaces.
5. In the port mappings settings, add a mapping for each protocol hosted by each server so that these services may pass through NAT. Refer to the port mapping section of this chapter for further explanation.

The default gateway setting in this example gives you great freedom. You may keep all your existing environments unchanged, keeping the routers and routes already established within your network.

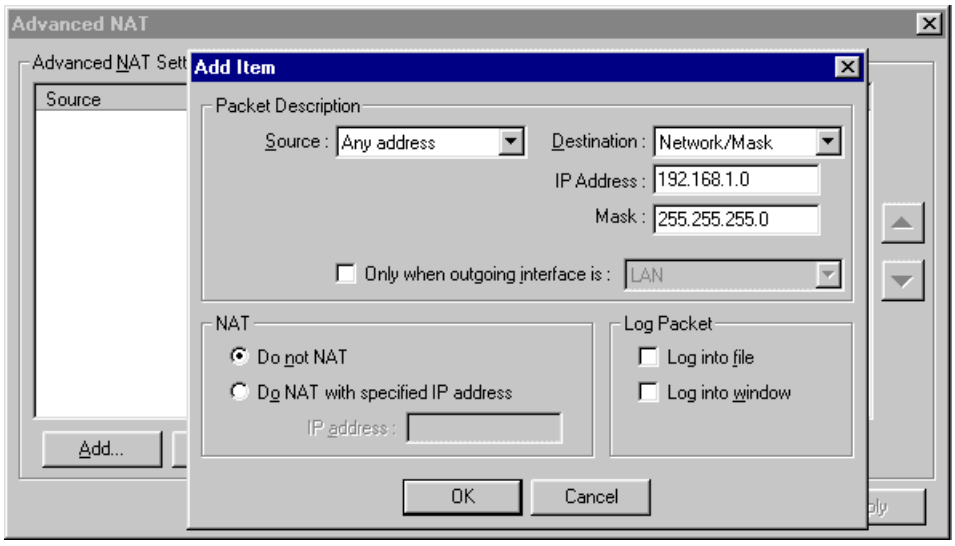
Advanced NAT

WinRoute allows simple **NAT** (Network Address Translation) and also more complicated settings. You may specify, based on **source** or **destination** IP address of the packet, that NAT would be provided with some **other IP address** (i.e. packets would look as if they originate from another IP address) or that **NAT** won't be performed at all.

Such settings are of great importance, with settings of more complicated networks where:

- Certain computers should look like **another** IP address other than the main one used by the **rest** of the network.
- You have branch offices connected to the **WAN** with private address space, and, assuming these private addresses can be properly routed to WinRoute, you want to allow them to pass through NAT as if the internal subnet was a DMZ.

- You have multiple segments behind WinRoute where one (ore more) segment is DMZ zone with publicly routable IP addresses.



Source IP address, Destination IP address

You may perform advanced NAT settings based on the IP address from which they are sent (source) or where they are sent (destination). As a source you may enter Host IP, the whole network (limited by network mask) or the group of IP addresses previously created in menu Settings->Advanced->Address Groups.

Do not NAT

If selected, packets passing through the selected NAT'd interface that match the src/dest'n criteria will not be NAT'd.

Do NAT with specified IP address

If selected, packets passing through the selected NAT'd interface will be translated to reflect the source address of the one specified by this setting. Note that the interface performing the address translation must occupy the address you have specified in this option. This can only be accomplished on NT/2000 systems where more than one IP address may be assigned to a single interface.

Notes:

- Advanced NAT rules are only valid on Interfaces for which NAT is enabled.
- When applying a rule for a DMZ you will specify that outbound traffic having a source IP address from that of the DMZ must not be NAT'd. WinRoute will automatically route incoming traffic to those IP addresses through NAT. In other words, WinRoute becomes a neutral router for those addresses.
- It is important that when defining the DMZ segment either in the address groups or elsewhere that you do not include WinRoute as part of the DMZ unless you plan to use packet filters to restrict access to the WinRoute computer through that IP address.

Packet Filter

Packet filtering overview

The heart of any firewall access control mechanism is, of course, the technology by which it permits or denies packets destined for protected networks. WinRoute implements one of the most commonly used technologies for network access control: packet filtering. Although WinRoute does implement other access control mechanisms, such as an integrated caching proxy server for HTTP, FTP, and Gopher protocols, this is primarily intended as an outbound performance enhancing element and not a security feature.

Packet filtering has a long tradition in the security community, and is still implemented widely in products such as Cisco's IOS network device operating system. Configured properly, packet filters can be made quite secure, and are particularly appropriate for high-volume Internet sites as they provide the best performance benefits.

Rules

Despite theoretical issues surrounding packet filtering, the primary point of failure for modern firewall systems is misconfiguration, especially by inexperienced administrative staff. WinRoute makes configuration of filters simple and yet flexible enough so that even novice network administrators can implement a secure configuration with little knowledge of TCP/IP.

Filter rules may be applied on a per-interface basis to all of the following:

- A single IP address
- An administrator-defined list of IP addresses
- An entire network or subnet

It is also important to note here that filters can be set for both incoming and outgoing traffic.

These capabilities allow granular tailoring of access rules to the security needs of almost any organization. For example, a group of Web developers could be granted access to specific external resources such as anonymous FTP staging servers, or a specified list of internal addresses can be designated accessible to external partner networks for drop-off of electronic files. The inbound/outbound configuration allows protection from malicious "inside-out" attacks such as Back Orifice (BO) or distributed denial of service (DDOS) servlets that attempt to communicate over unreliable protocols back out through the firewall with external attackers.

Rules can either Permit, Drop, or Deny the specified traffic; the "Drop" action gives away the least information about the firewall to potential attackers, as it does not send an ICMP Administrative Prohibited Filter or a TCP Reset/Acknowledge response to a TCP SYN packet (the 1st step in the standard three-way TCP handshake sequence).

Rules may be prioritized to act in a specific, user-defined order upon incoming or outgoing packets. The most popular use of this capability is to add so-called "cleanup rules" to filter lists that block all traffic not specifically allowed by previous rules that have higher priority in the list (for an example of a clean-up rule, see the Sample Basic packet Filter Rule sets, later in this document).

Protocols

Protocols supported by WinRoute packet filters include:

- Raw IP
- Seven ICMP types (or All)
- TCP
- UDP
- PPTP
- Other/Protocol number

The ability to permit or block raw specific ICMP types or raw IP protocols is invaluable to network administrators faced with an ever-growing list of application requirements to support. In particular, relatively new VPN protocols such as IPSec travel over raw IP protocols 50 and 51, which would be impossible to filter using some of the more limited firewall products on the market today that are only capable of controlling TCP or UDP-based protocols.

Logs and packet analyses

About logs and analysis

A critical function of any security product is the ability to record events at all times in a sufficiently detailed fashion. WinRoute offers six different logs that encompass error reporting, debugging, user defined, status, mail transactions, web browsing and so on. A description of each log is shown in the following table:

HTTP Log	Displays only HTTP data passing through the WinRoute Proxy server; includes source IP address and username, time stamp, and HTTP queries and responses
Mail Log	Records all operations of the WinRoute's built-in mail server; records SMTP an POP3 send/receive activities
Security Log	Shows all activities defined as "Log to window/file" in packet filter rules (see below for detailed description of items recorded)
Dial Log	Records usage information for dial-up interfaces monitored by WinRoute
Debug Log	A la carte settings to record all ARP, ICMP, UDP, TCP, and/or DNS packets that physically cross any interface of the WinRoute router; granular configuration available under Settings | Advanced | Debug Info, Debug tab.
Error Log	Displays all unsuccessful operations occurring in any running WinRoute module

Logging can be displayed to the console of the WinRoute Administrator, or written to a file, or both. The log files are stored in \%installroot%\Logs, which is only accessible to the NT/2000 accounts within Administrators, Server Operators, SYSTEM, and the CREATOR OWNER who installed WinRoute.

The log information recorded by WinRoute's Security Log is robust, including all necessary information to initiate a proper investigation into potentially malicious activities:

- Date
- Time
- Packet Filter rule impacted
- Interface
- Action (Permit, Drop, Deny)
- Protocol
- Source IP address and TCP port
- Destination IP address and TCP port

Testing under adverse high-traffic conditions does not affect the WinRoute logging capability. This is critical to avoid loss of valuable forensic data as well as to alleviate potential denial-of-service situation where firewall functionality shuts down if the logging system is overwhelmed.

Debug log

Debug log is the most important log in WinRoute. It allows you to see **all IP packets** (TCP, UDP, ICMP, ARP, DNS) that physically cross any of the interfaces present in the WinRoute computer.

In the **Debug Events** window you can see the set of events you might want to have displayed.

How to read the log?

From the left you may see following:

Time stamp - the date and time displaying exactly when the event happened or packet crossed the interface.

The protocol - the type of protocol of the packet

From/To Interface name - the name of the interface and whether the packet went **To** or came **From** the interface (imagine that WinRoute is running on the PC and interfaces are meant to be the "gates" between the computer and the network).

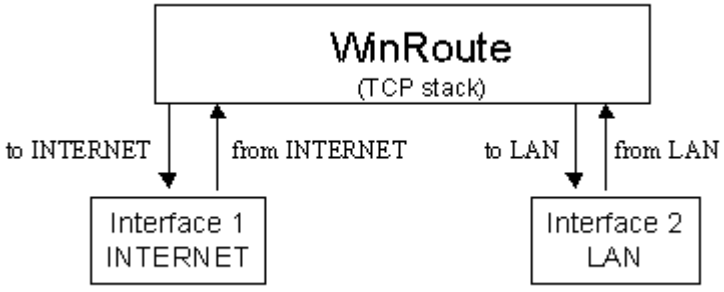
Source IP -> Destination IP address - the source and destination IP addresses present in the packet.

The flags - further identification about the action.

Example:

```
[10/Nov/1999 09:32:38] TCP: packet 511464, from lan, length
1514, 192.168.1.7:2442 -> 192.168.1.1:25, flags: ACK

[10/Nov/1999 09:32:38] TCP: packet 511465, to lan, length
54, 192.168.1.1:25 -> 192.168.1.7:2442, flags: ACK
```


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

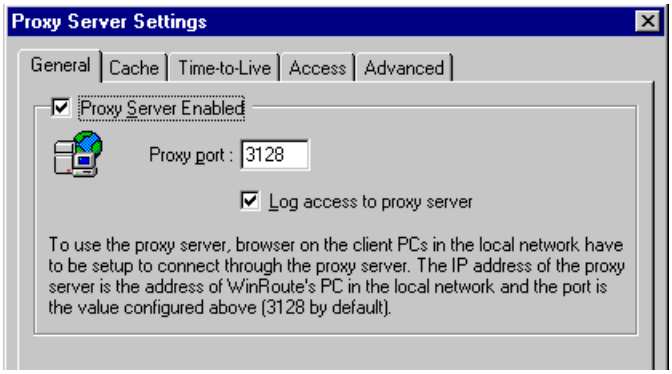
HTTP (Proxy) log

HTTP (Proxy) log is a powerful tool that helps you keep track of the users activities on the Internet. It provides more user-friendly information about users accessing the web than you would get from the Debug log.

When does the log work?

HTTP (Proxy) log displays only data going through the Proxy Server of WinRoute. It means, if you want to get data from the Proxy server you should force your users to go through the Proxy server. See the Firewall Examples or Proxy Server chapters.

Also - you have to enable the log access to the Proxy Server configuration.



How to read the HTTP (Proxy) log?

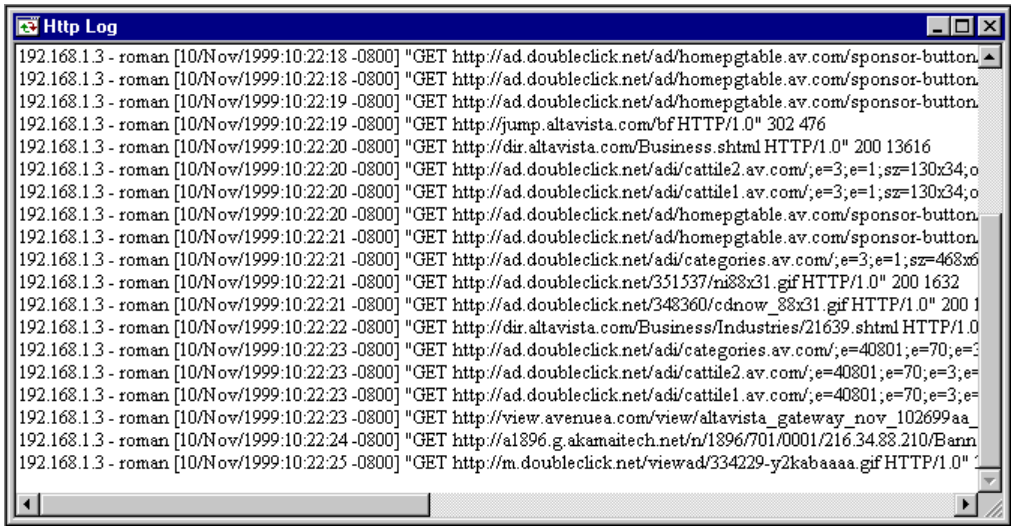
```
192.168.1.3 - roman [10/Nov/1999:10:22:20 -0800] "GET
http://dir.altavista.com/Business.shtml HTTP/1.0" 200 13616
```

From the left to right:

IP address - name - the name and current IP address of the user accessing the Internet

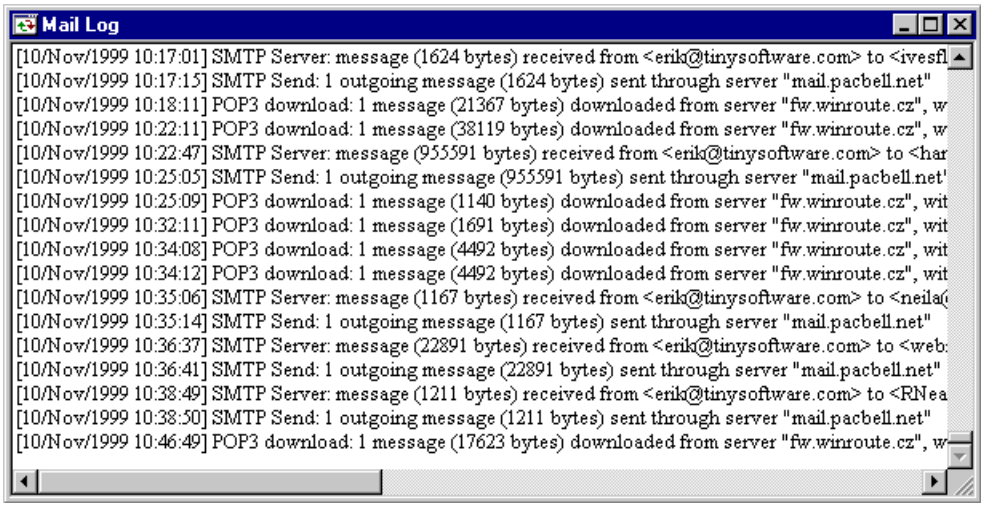
Time Stamp - the date and time of the access

GET "http..." - the target of the access



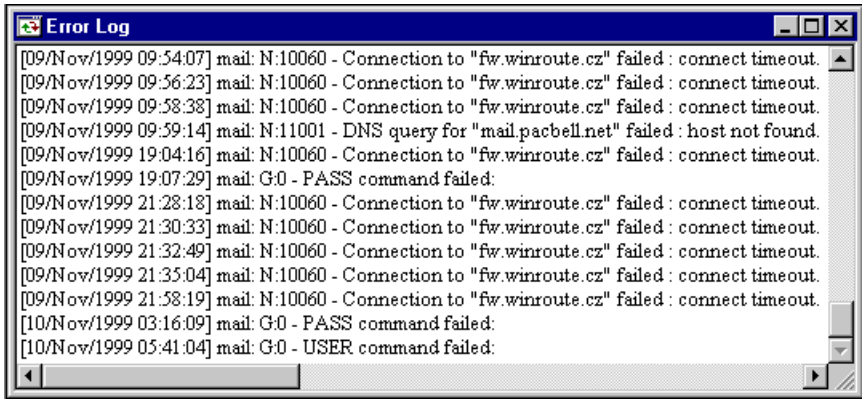
Mail log

Mail log records all operations of WinRoute's built-in Mail Server. You can see how many messages were sent, received, where the messages were sent etc. All operations are time stamped.



Error log

Error log displays all unsuccessful operations in the modules of WinRoute that are turned on. As a result you may see the errors in the mail exchange, DNS server etc.



CHAPTER 2

WINROUTE CONFIGURATION

In This Chapter

System requirements

To install and run WinRoute Pro 4.2 we recommend at least:

- Pentium class PC (single or dual processor)
- Windows 98/ME/NT4.0/2000/XP
- 32 MB memory
- 10 MB of free disk space
- At least 2 interfaces available. These may include: Ethernet, RAS, TokenRing, DirecPC

Quick Checklist

For all WinRoute users, there is a basic list of settings and rules that, if performed, ensure a successful connection of their network to the Internet. Of course that functional Internet connection is a must.

You will perform the settings described below if you want to benefit from using NAT to share Internet access. If you want to use the Proxy Server built into WinRoute you do not have to perform these settings. In that case you would need to point your browsers and applications to WinRoute's Proxy Server. We strongly recommend using NAT (Network Address Translation) wherever possible. It is faster, more secure and reliable.

Settings and rules

1. **At WinRoute PC - Two Interfaces (at minimum)!**
2. **Ensure that all IP addresses are pingable!** Before installing WinRoute, make sure that each client is able to communicate with the machine WinRoute will be installed on.
3. **At WinRoute PC - Enable NAT on the Internet interface!** For simplified firewall administration and internet sharing you must enable Network Address Translation (NAT) on the interface connected to the internet or any other non-trusted network. You enable NAT on devices from the interface table, not advanced NAT! In cases where WinRoute is used only as a Packet Filter Firewall, Proxy server or Mail Server, it is not necessary to turn NAT "ON" for any interface.
4. **At WinRoute PC - No Gateway on internal interface!**
   Check that there is NO default gateway in the network properties of the interface (network device) linking to the internal network. Of course the default gateway on the Interface linking to the Internet will be set according to the details from your ISP.

5 **At client PC - WinRoute PC internal IP address is the default gateway!**
The WinRoute PC acts as the DEFAULT GATEWAY for all computers in the LAN. Therefore, use the IP address of the internal Network Interface Card on the WinRoute host (e.g.192.168.1.1) as the Gateway on every internal/client computer. Set this value at each "client" computer OR set this value once in WinRoute's DHCP server settings and it will assign this value to your workstations automatically! See Advanced (Inter) networking Examples if you would like to use a different default gateway!

6 **At client PC - Check DNS!**
In most cases you will use WinRoute's built in DNS forwarder as the primary DNS server for your networked computers. Make sure that WinRoute's built in DNS forwarder is enabled and configured. You may alternatively use the DNS server address of your ISP by entering it directly to the appropriate fields in the TCP/IP configuration of each networked computer.

7 **Each interface on the WinRoute computer must be part of a different subnet!** The subnet mask defines all IP addresses included in a subnet. For local area networking it is easiest to use class C subnets where the mask is 255.255.255.0. With this mask the third octet will differentiate a subnet (i.e. 192.168.1.1 and 192.168.2.1 are in separate subnets if you are using a class C mask)

Conflicting software

Microsoft Internet Connection Sharing

Uninstall MS ICS before the installation, remove TCP/IP protocol, restart and bring it back.

Active Directory

WinRoute may co-exist on a system configured as a domain controller, however Active Directory requires DNS service. This means that the DNS forwarder in WinRoute must be disabled. Functionality such as DNS cache, local DNS using the host file, and demand dial for DNS queries will not work.

Anti-Virus

Some Anti-Virus programs act as a mail server by binding to common mail ports such as 25 for simple mail transfer or 110 for POP. If you would like to run anti-virus software on the WinRoute computer you must change the ports that WinRoute uses. This is done in the advanced settings of the mail server.

Proxy Client software issues

Some proxy servers require software to be installed on all client machines. This client software makes all applications query a proxy server. If the client proxy software is not removed, that machine may not be connected to the internet because WinRoute is not setup as a proxy server.

Network Card driver issues

Try to use the most standard network interface cards. If you have a special, old or brand new card in your computer, its driver may include specific instructions that will prevent WinRoute from communication with it. Try to find the most standard Ethernet card in your network and simply exchange their position. Quite a few originally "unhappy" customers turned to "happy " customers just by changing the card or updating the driver.

WinRoute is a fully neutral software router/firewall that does not require any client software running on client computers unless remote administration is used in which case a client or external machine must install WinRoute Administration "wradmin.exe".

IP configuration - manual assignment

In some cases it is necessary to assign workstations with IP addresses manually. When doing so, take into consideration the following rules:

Assign IP Address

Assign each computer with an "internal type" IP address. Usually 192.168.x.x or 10.x.x.x. Assign each system IP addresses from the same subnet. For example, once an IP address for WinRoute host is set at 192.168.1.1, you must continue with the same numbering scheme. (e.g.192.168.1.2., 192.168.1.3 etc.)

Set default gateway

Use the WinRoute host computer IP address as the default gateway for all your client computers. In other words, each client computer will use the IP address of the WinRoute host (internal IP address) as the default gateway. This is entered in the TCP/IP=>Ethernet_adapter in the Network Properties of the computer.

Set DNS

Finally, use the WinRoute computer's IP address (the internal IP address) as the DNS server for all of your computers. The only exception might be when using the DNS address of your ISP or another DNS server. Then you will enter DNS details given to you by your ISP (in TCP/IP->NIC properties of each workstation).

Important! See recommended chapter of this manual regarding further DNS settings!

Interface table

The Interface table is a dialog where WinRoute displays all interfaces available in the computer that it could recognize. If you should have more interfaces than WinRoute displays it is likely that the driver for such interface(s) were not properly loaded by the operating system and WinRoute could not read it.

You can see:

Name of the Interface

You can change the name by selecting “properties” and changing the name.

IP address

The value set in TCP/IP properties of the Interface. If the interface is set to get IP address from DHCP server you would see the actual IP address assigned to the Interface.

NAT “On” or “Off”

If NAT is to be performed on an interface then “On” is displayed in this column.

Setting up the network (DHCP)

About DHCP

Using the DHCP server you can significantly simplify configuration of the workstations within your LAN. When using the DHCP server the only setting you have to perform on the client workstations is to set them to get an IP address dynamically from the DHCP server. (This setting comes as the default when adding the TCP/IP protocol in network properties.)

➢ ***You may use either WinRoute's built-in DHCP server or any third party DHCP server within your network. Make sure that only one DHCP server is running on your network at a time!***

Default gateway overview

WinRoute acts as a router. As such it requires two basic TCP/IP settings on each computer in your network. Note that the following only applies to clients. The WinRoute host should have a static IP assigned to the private interface.

- Assign IP address – either manually or from DHCP server (e.g. WinRoute's DHCP server)
- Set default gateway

The Default Gateway on each computer accessing the Internet through the WinRoute computer; must be set to the **IP address** of the Ethernet interface of the WinRoute computer that links to the LAN.

Example:

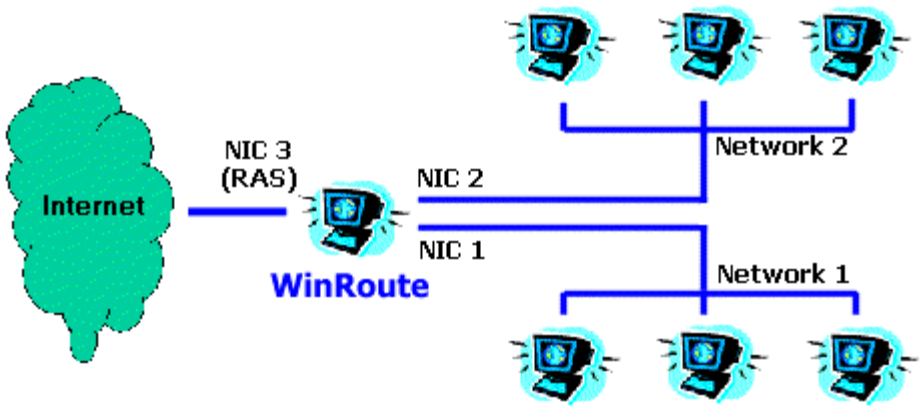
Client computer has IP address 10.10.10.23 while WinRoute PC has two interfaces, one linking to the cable modem with an IP from the ISP and another one linking to the private network (10.10.10.1). The default gateway for the computer at 10.10.10.23 will be set as 10.10.10.1.

- ***Note 1: When creating IP address space within your local network you must use the IP address from the same subnet. i.e. if the subnet mask you use is 255.255.255.0 then all addresses must be from 10.10.10.1 to 10.10.10.254.***
- ***Note 2: You may have more networks connected to the Internet through WinRoute. You may have more Interfaces in the WinRoute computer, one for each network. Then each of these interfaces (their IP address) represents the default gateway for the rest of the network connected to it.***

Choosing the right WinRoute computer

WinRoute **MUST ALWAYS** run on the computer that is connected to the Internet - through the network card, cable, DSL modem, dial-up link or a router.

WinRoute always acts as the gateway between two (or more) networks where each network is represented by one interface. These interfaces may be Ethernet cards, RAS adapters, USB-to-Ethernet Adapters, PPPoE adapters etc.



IP configuration with DHCP server

Double check that your workstations are set to get an IP address from the DHCP server (see *TCP/IP->network interface* properties on each computer) and that all other TCP/IP properties are blank including DNS server information.

Then run WinRoute Administration program:

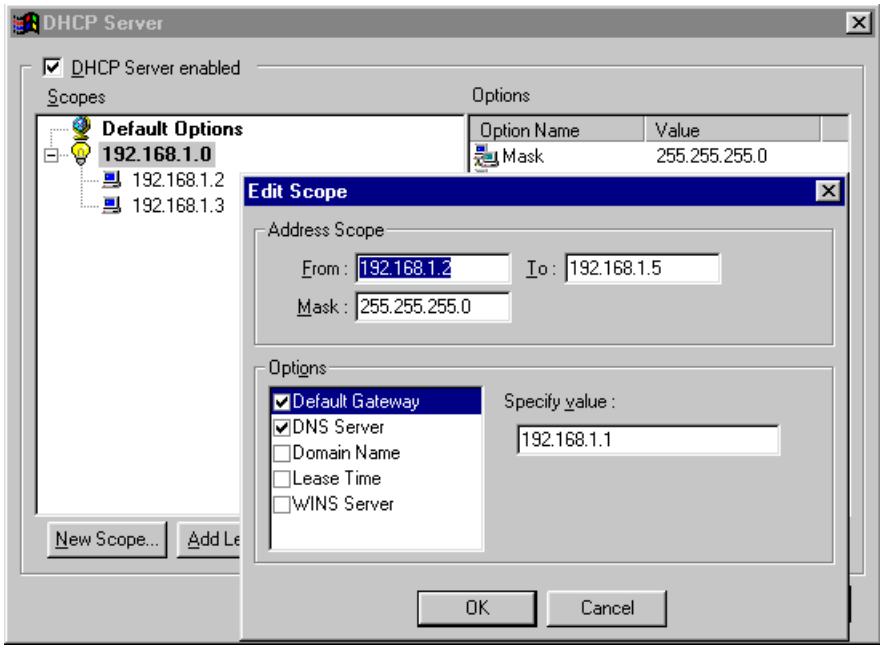
1. Go to menu *Settings=>DHCP server*.
2. Switch DHCP server ON (check the button) and press Add **New Scope** button.

3. Add Scope

Here you will specify the scope of IP addresses used by the DHCP server which are given out to workstations. Remember one IP address is already used by the WinRoute computer so avoid using it. The IP address range must be of the same subnet. See the picture as the example.

4. Specify Options (important!)

In Options you specify what other information will be given to workstations (e.g. default gateway, DNS server etc.). Check the button beside each component in the dialog box and enter the appropriate information. Enter the information for default gateway and DNS server (typically you would use WinRoute as the DNS server) and use the IP address of the WinRoute computer (e.g. 192.168.1.1). You may leave other options blank.


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

IP configuration with 3rd DHCP server

Using a third party DHCP server for your network configuration requires that special attention be paid to the values issued by such a DHCP server to the client workstations within your network.

Double check that your DHCP server is issuing the correct information to your client workstations! i.e. You must set the DHCP server to assign other computers with the IP address of the LAN card of WinRoute's computer as the default gateway and (optionally) DNS server and, of course, the IP address issued to the client workstation must be in the same subnet as the WinRoute computer.

DOUBLE CHECK (!!!) that the internal network card on the WinRoute computer **has assigned** a fixed IP address (e.g. 192.168.1.1) and this address is issued by DHCP as the Default Gateway to the rest of the network. The DHCP server may not assign an IP address to the WinRoute host!

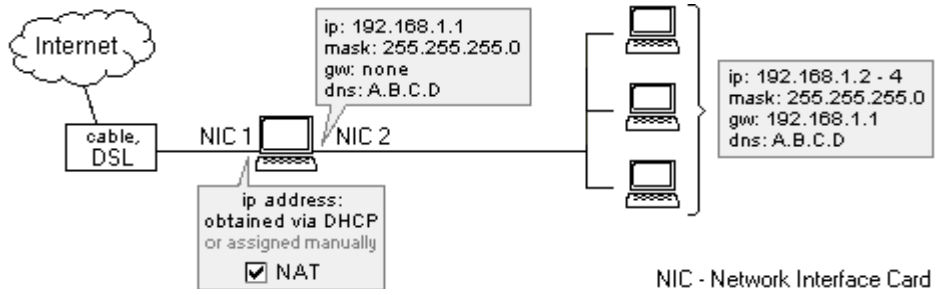
Example:

NT server with DHCP is running on 192.168.1.1 while WinRoute is running on 192.168.1.5. The default gateway (and DNS if you would use WinRoute DNS) information issued to workstations will be 192.168.1.5.

Connecting the network to the Internet

DSL connection

DSL (ADSL, SDSL) connections require at least two Network Interface Cards (NICs) installed in the WinRoute computer. One NIC will link to the Internet (DSL modem) while another NIC will link to the internal network.



WinRoute Configuration

To connect to the Internet

1. Go to menu Settings->Interface Table
2. Choose NIC linking to the Internet, click on Properties and check ON "Perform NAT with IP address of the interface on all communication passing through". When opening the interface table dialog box you will see NAT ON beside this external line.
3. Check than NAT is NOT ON for the Interface linking to the internal network (go to the properties of this interface in Interface Table)

4. Check that there is NO gateway set in TCP/IP properties of the internal NIC (go to network settings) and NIC has assigned an internal IP address.
5. Check that the NIC linking to the Internet was properly assigned with data from your ISP. In case you have a dynamically assigned IP addresses leave the IP address settings blank.

For other network settings refer to appropriate chapters, especially the ***CheckList*** .

PPPoE DSL connection

Configuring WinRoute Pro/Lite with ADSL using PPPoE

Many DSL service providers offer a connection method for their service called PPP over Ethernet or PPP over ADSL. PPPoE combines the Point-to-Point Protocol (PPP), commonly used in dialup connections, with the Ethernet protocol. With PPPoE, the user must install special software that is used to announce the computers presence and to obtain an IP configuration. In the process, the software uses a virtual interface to encapsulate each ethernet frame with additional header information. Depending on the type of PPPoE software used, WinRoute may need to be adjusted to fragment data packets, or in some cases, you will need to lower the Maximum Transmission Unit (MTU) on each computer behind WinRoute.

Basic network setup for PPPoE:

IP Configuration: (For basic configuration with only two Ethernet adapters, though more may be used)

Assign an IP address and subnet mask to both ethernet adapters and nothing more, e.g. no gateway/dns etc.

For example NIC1 may have an address like 192.168.10.1 mask 255.255.255.0

NIC2 may have an address like 192.168.20.1 mask 255.255.255.0

It is a common misconception that the interface connected to the ADSL modem should use DHCP. You must assign this adapter an IP address and mask and it must be in a different subnet than any other interface so that proper routing may take place.

NAT Configuration:

The PPPoE software supplied to you should install specific drivers as well as an additional interface. This interface is typically identified in WinRoute as either a virtual ethernet adapter or a RAS connection. You must enable NAT on only this interface. Note that NAT will be enabled by default for all RAS adapters. For WinRoute Lite users, if your PPPoE adapter is a RAS type you must specify dial-up as your connection type and select the corresponding PPPoE RAS connection from the drop down menu. If it is a virtual adapter you will specify a second network adapter and select the PPPoE adapter from the drop down menu.

PPPoE Configuration:

RASPPPOE by Robert Schlabbach and WinPoet from Fine Point Technologies

WinRoute works best with these known PPPoE software providers because they both use RAS interfaces to connect to the internet. Most users choose to set the connection to persistent dial for an "always on" connection. By using RAS, WinRoute may remain running as a system service and initiate the connection at start-up. You may notice an error WRSendPacket() failure in the error log. This can be fixed by allowing WinRoute to fragment incoming packets. Refer to our FAQ page for further explanation and instruction.

Enternet 300 by Efficient Networks

In the advanced connections/settings of the Enternet 300 you must enable protocol driver in place of filter driver. You must also connect to the internet and successfully receive your IP configuration before starting the WinRoute engine. This means that you must disable WinRoute as a service so that it will not launch the engine at startup. NAT must only be enabled on the NTS pppoe adapter. If you have WinRoute Lite this adapter should be specified as your 2nd network adapter.

WRSendPacket() failure

It is likely that you will find this message in the error log of WinRoute. If so, follow these steps:

Stop the WinRoute engine.

Open up the registry editor. In Windows click on the Start button go to “Run” type in “regedit” click OK

Expand “HKEY Local Machine / Software / Kerio / Winroute”

Change the value of the IpFragMode key to “1”

Close the registry editor and restart WinRoute

Setting The MTU

The Maximum Transmission Unit (MTU) is a value that defines the maximum size of each packet leaving your computer. You may need to lower this value on each computer behind WinRoute. To see if this is necessary you can perform a ping test from a client computer as follows.

From a dos window type: ping -f -l 1472 yahoo.com

If you receive the message: Packet needs to be fragmented but DF set. Then you need to lower the MTU. Try the same test again using 1400 in place of 1472. If you get a message like: Reply from 216.115.108.243: bytes=1400 time= 180ms TTL= 246.Then 1400 is a sufficient size. Otherwise you'll need to continue lowering the value until you get a reply. It is possible that you may not get a reply, this is ok. You only need to lower the MTU if you get the specific response "Packet needs to be fragmented but DF set."

Note: If the client is set to obtain its IP information through DHCP, the registry structure may not appear as follows. To make sure you apply the necessary MTU value to the proper location you need to exit the registry editor and proceed to the TCP/IP settings of the adapter for which you are setting the MTU. Disable DHCP and manually input an IP address and subnet mask. Use a random value such as 1.2.3.4 that is easy to remember. Reboot the computer and refer back to the registry editor and follow the steps outlined below. Once you have set the MTU and rebooted you can go back to the TCP/IP properties and reset the adapter to obtain its IP information through DHCP.

Windows 95/98/ME

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Class\NetTrans\{000x}

Beneath NetTrans should be several keys labeled 000x. Select the first key and refer to the window to the right. Look for an IP address setting that will display the IP you inputted in the TCP/IP settings, 1.2.3.4 in our example. If you cannot find the IP then select the next key down and so on until you have located the IP address. When you have located the correct key look for a value called MaxMTU. If it does not exist, add a string value and label it MaxMTU taking into account case sensitivity. Modify its contents to reflect the necessary bit size determined by the ping test. Under most circumstances 1400 is sufficient. You must reboot the machine for the changes to take affect.

Windows NT

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\"ethernet-adapter"\Parameters\Tcpip

When you have located the correct key look for a value called MTU. If it does not exist, add a dword value and label it MTU taking into account case sensitivity. Modify its contents to reflect the necessary bit size determined by the ping test. Under most circumstances 1400 is sufficient. You must reboot the machine for the changes to take affect.

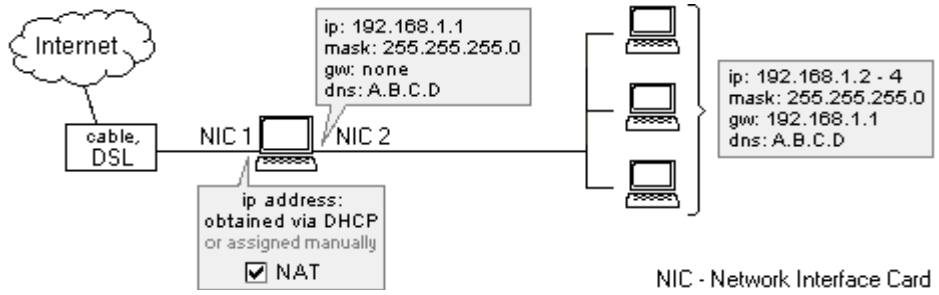
Windows 2000

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{interface}

Beneath Interfaces should be several keys signifying each interface. Select the first key and refer to the window to the right. Look for an IP address setting that will display the IP you inputted in the TCP/IP settings, 1.2.3.4 in our example. If you cannot find the IP then select the next key down and so on until you have located the IP address. When you have located the correct key look for a value called MTU. If it does not exist, add a dword value and label it MTU taking into account case sensitivity. Modify its contents to reflect the necessary bit size determined by the ping test. Under most circumstances a decimal value of 1400 is sufficient. You must reboot the machine for the changes to take affect.

Cable modem (Bi-directional) connection

Cable modem connection requires two Network Card Interfaces (NIC) included in the WinRoute computer. One NIC will link to Internet (cable modem) while another NIC will link to the internal network. For UNI-directional cable modems (modem up, cable down) refer to the next section.



WinRoute Configuration

1. Go to menu Settings->Interface Table
2. Choose NIC linking to the Internet, click on Properties and check ON "Perform NAT with IP address of the interface on all communication passing through". When opening the interface table dialog box you will see NAT ON beside this external line.

3 Check than NAT is NOT ON for the Interface linking to the internal network (go to the properties of this interface in Interface Table)

4 Check that there is NO gateway set in TCP/IP properties of the internal NIC (go to network settings) and NIC has assigned an internal IP address.

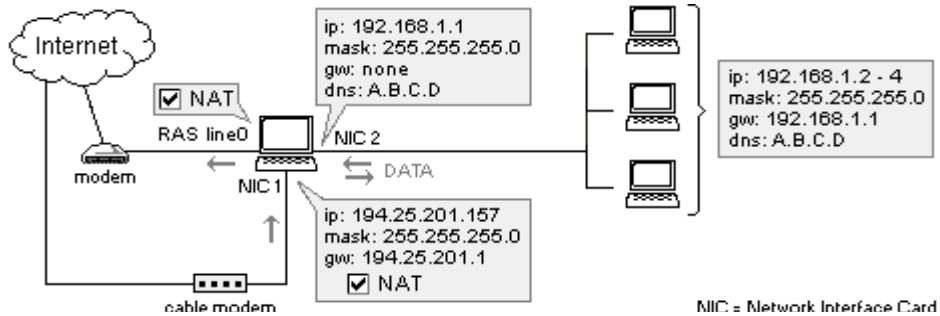
5 Check that the NIC linking to the Internet was properly assigned with data from your ISP. In case you have a dynamically assigned IP addresses leave the IP address settings blank.

For other network settings refer to appropriate chapters (e.g. ***checklist*** , ***IP configuration*** etc.)

Unidirectional cable modem (modem up, cable down)

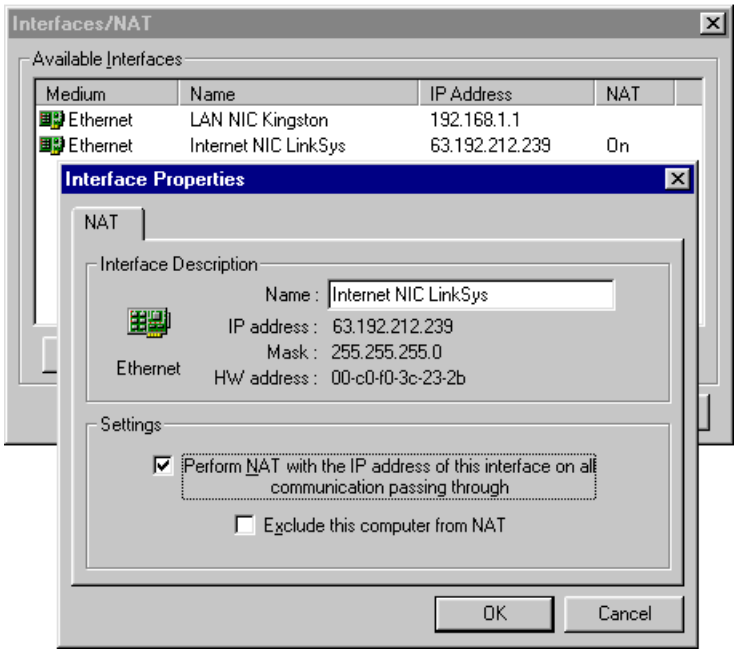
NOTE: This type of Internet connection is **not an "officially supported configuration"** as the settings **may vary** from ISP to ISP. However, we try to provide access solutions to as many scenarios as possible. Many of our users have had success with the following settings when trying to establish a connection.

In general, the data flow is **similar to DirecPC**. Outgoing packets flow through your **dial-up** interface. On the way back they are routed **through a cable**. In fact, your ISP has to associate your two interfaces together. This looks tricky but it is the only way to establish a successful link. For this reason, we advise thorough evaluation before going ahead with your purchase of WinRoute



1. Go to menu *Settings->Interface Table*. You will see a **RAS line** interface (your modem) and two **network card** interfaces - one linking to the cable modem and one linking to your local network.

2. Click on the network card interface linking to the cable modem and go to *"Properties."* Check ON for *"Perform NAT with IP address of the interface on all communication passing through."*



3. Click on **RAS interface** and go to *"Properties."* Check ON *"Perform NAT with IP address of the interface on all communication passing through"*. In **RAS tab** select the connection you will use to connect your ISP, enter your user name and password.

4. Check than NAT is **NOT ON** for the Interface linking to the internal network (go to the properties of this interface)

5. Check that there is **NO gateway** set in TCP/IP properties of the internal NIC (go to network settings) and that NIC has assigned a private class **IP address** (e.g.10.10.1.1).

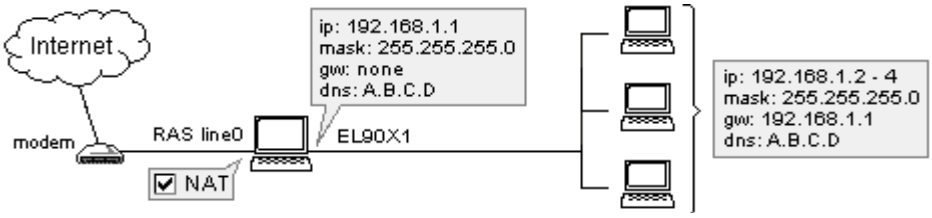
6. Check that the NIC linking to the Internet was properly assigned with data from your ISP (TCP/IP properties.) Note: In case you have a dynamically assigned IP address leave IP address settings blank.

Dial-up or ISDN connection

Connection via Dial-up or ISDN

If you have dial-up access to the Internet (regular 56K or ISDN) on a PC running Win95, Win98 or NT4.0, you have what's needed to run WinRoute. WinRoute must run on a computer that includes:

- Modem attached to the phone or ISDN line
- Network Interface Card (NIC) leading to the internal network.



In case you have an ISDN modem connected to your computer via Ethernet, refer to the chapter for DSL. In that case you will configure WinRoute to work with two Ethernet cards.

Before the connection

Before connecting to the Internet, double check the following:

- · TCP/IP protocol is properly installed and configured (see checklist or Setting up network chapter)
- · Dial-up networking (Windows 95/98) or RAS service (Windows NT) is properly installed and configured
- · Modem is attached to the WinRoute host PC.

WinRoute uses Dial-up Networking or RAS services available in your operating system for Internet connection.

It is recommended that you connect the Internet to the computer where WinRoute is to be installed PRIOR to installing and running WinRoute to insure that the connection is correctly configured and dial-up networking or RAS properly working.

WinRoute configuration

After you've performed all of the configuration described above:

1. Go to menu Settings->Interface table -you should see all network interfaces available in your computer. Dial-up interfaces are named RAS in WinRoute (on both 95/98 and NT) operating systems.
2. Go to the Properties of selected RAS interface
3. Check the button "Perform NAT with IP address of this interface on all communication passing through"
4. Go to RAS table in Properties dialog, choose or create your connection and set options according to your needs. See RAS table for more details.

- ***Remember! NAT has to be checked "ON" on RAS interface while "UNCHECKED" on the interface(s) that is linking to the Internal network.***

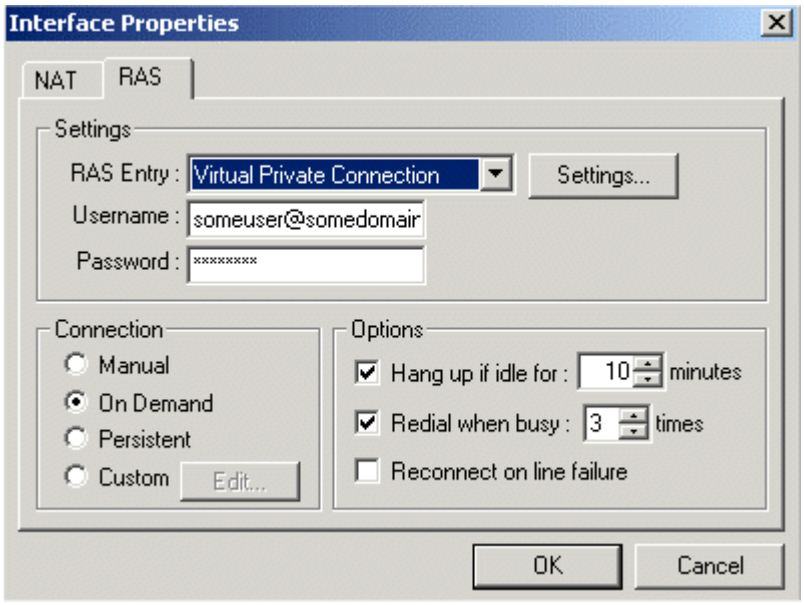
Ethernet interface configuration

1. The Network Interface Card leading to the Internal network has an assigned IP address (private class) and NO assigned gateway!
2. The DNS entries used for this interface are based on data from your ISP. If this data has not been provided to you, please contact your service provider.

You may set WinRoute to provide you with the dial on demand feature, where the connection is established automatically based on the traffic (data) going out of the local network.

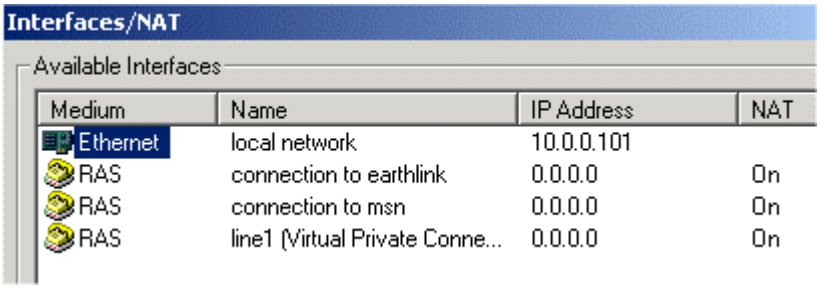
Demand dial

WinRoute is capable of calling an external dial-up connection when a client computer initiates an external web request. This option is located in the RAS properties of the RAS interface located in the interface table.



The following notes/considerations should be taken if dial on demand is not behaving properly.

- If you should have more than one dial-up account you can add another RAS interface from the advanced settings -> interface maintenance to associate dialing properties for your additional dial-up accounts.



- Demand dial is called by one of three ways: A dns request is made specifically to winroute's dns forwarder, a url request is made specifically to winroute's proxy server, or a tcp or udp packet must be routed through winroute. It is important to note that for the third option to work there must be no default gateway on the winroute computer, otherwise winroute will assume that the traffic must go through the default route and not the dial-up connection.
- Some software will auto-update and thus cause winroute to dial the connection. You can disable demand dial for specified domains in the advanced -> miscellaneous options.

AOL connection

Using WinRoute Pro you may connect your network to the Internet via single AOL dial-up account. Note - AOL supports Win95/98 computers only. To connect through AOL follow up these steps:

1. Install AOL client (preferably AOL 5.0 and higher)
2. Connect to the Internet to make sure that the connection is functional
3. Install WinRoute Pro

4 In WinRoute Administration go to menu *Settings->Interface table*

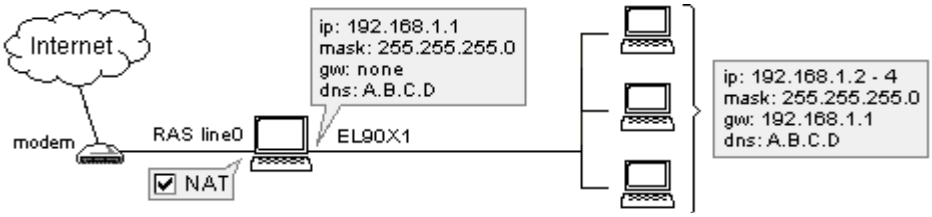
5 You should see AOL adapter among available interfaces. Click on properties of such interface and choose to "perform NAT" on that interface.

Set up you WinRoute computer and client computers according the checklist (see other chapter).

➢ ***Note! Dial on demand will not work. You have to initiate the connection to AOL manually.***

T1 or LAN connection

T1 or LAN connections require two Network Interface Cards (NICs) installed in the WinRoute computer. One NIC will link to the Internet (e.g. router) while another NIC will link to the internal network.



To connect to the Internet:

1 Go to menu Settings->Interface Table

2 Choose NIC linking to the Internet, click on Properties and check ON "Perform NAT with IP address of the interface on all communication passing through". When opening the interface table dialog box you will see NAT ON beside this external line.

3 Check than NAT is NOT ON for the Interface linking to the internal network (go to the properties of this interface in the Interface Table)

4 Check that there is NO gateway set in TCP/IP properties of the internal NIC (go to network settings) and NIC has assigned an internal IP address.

5 Check that NIC linking to the Internet was properly assigned with data from your ISP. In case you have a dynamically assigned IP addresses leave the IP address settings blank.

DirecPC connection

DirecPC uses a modem (analogue, ISDN, ...) or NIC (Ethernet, Token Ring) for uplink while using a satellite dish for downloading data. Your Internet connection is provided by DirecPC itself or you may use your existing ISP for dial-up connection.

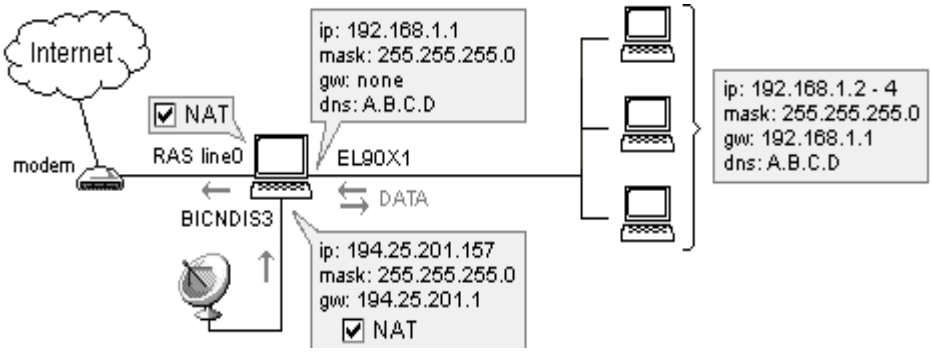
Data is going from your computer via modem to DirecPC Internet service where data is routed to its final destination. On the way back DirecPC associates the packets (data) coming to your computer with different data in order to route them via satellite dish.

WinRoute configuration

First of all you must have all DirecPC software and components correctly installed. Then, go on to configure WinRoute according to your specific requirements.

You may choose either DirecPC dialer or WinRoute RAS for uplink. Using WinRoute you will benefit from the dial on demand feature, this will save you money on your bill.

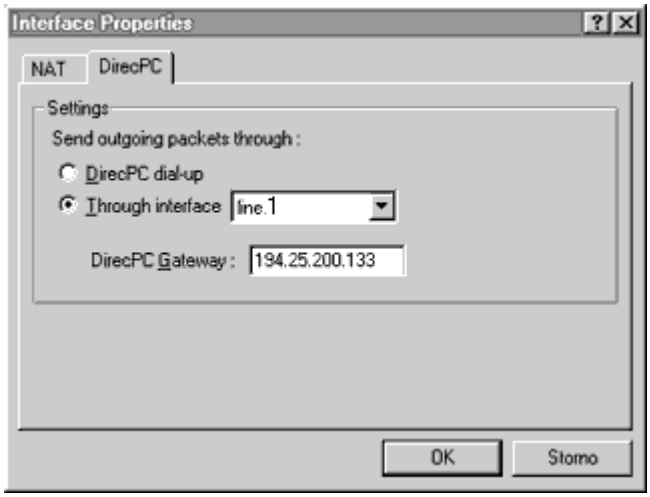
1. Using (RAS line) for uplink



Go to menu *Settings->Interface Table*. You will see the RAS line interface (your modem) and DirecPC interface card.

Click on DirecPC interface card and go to "Properties". You will see two tabs - **NAT** and **DirecPC**.

- In NAT tab check ON the *"Perform NAT with of the interface on all communication passing through"*.
- In DirecPC tab choose, that you will use *line0* for uplink. Enter the *gateway IP address* that was given to you by DirecPC.

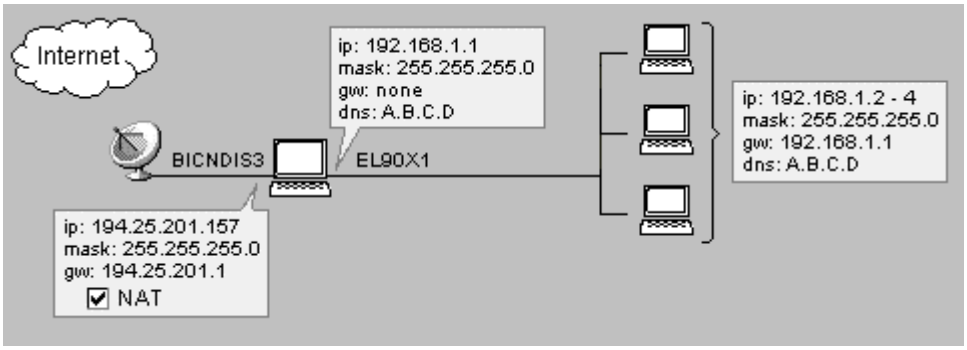


3. Click on RAS interface and go to "Properties". Check ON "Perform NAT with IP address of the interface on all communication passing through". In RAS tab, select the connection you will use to connect to your ISP, then enter your user name and password.

- ***Note! You have to UNCHECK "Use default gateway on remote network" in the properties of dial-up networking account created to connect to the ISP. Set this option in TCP/IP properties of your dial-up interface.***

2. Using DirecPC dialer for uplink

You may use DirecPC's built-in dialer where available. However we recommend using WinRoute RAS line where possible.



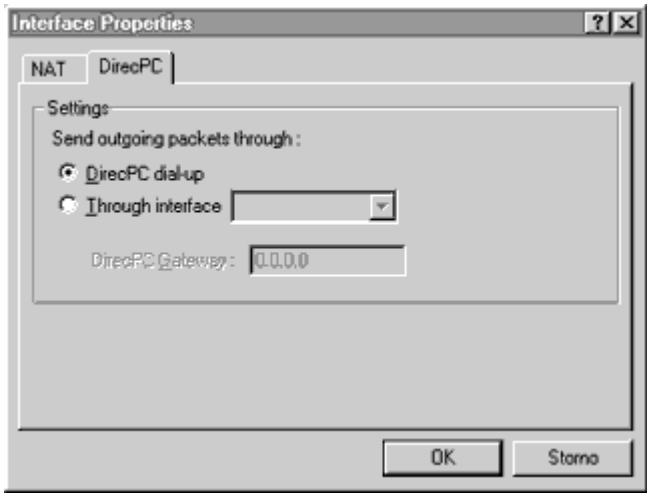
To use DirecPC dialer:

Go to menu *Settings->Interface Table*. You will see RAS line interface (your modem) and DirecPC interface card

Click on DirecPC interface card and go to "*Properties*". You will see two tabs there - NAT and DirecPC.

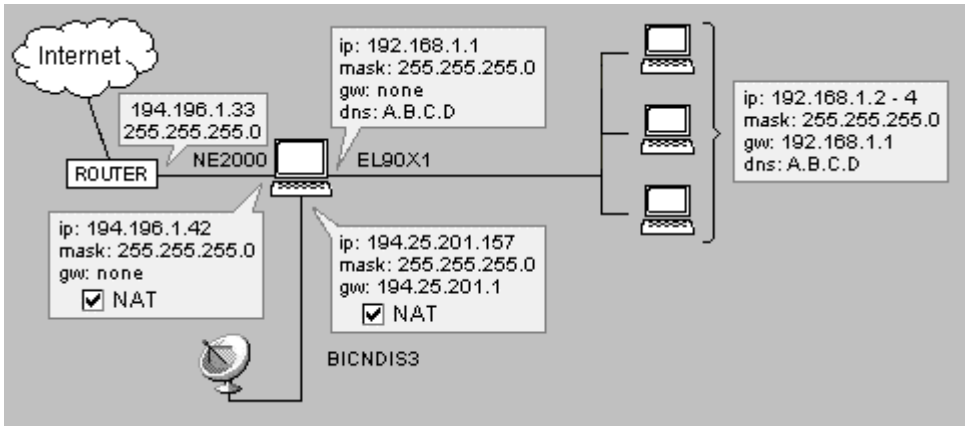
- In the NAT tab, check ON "*Perform NAT with IP address of the interface on all communication passing through*".

- In DirecPC tab choose "*Use DirecPC dialer for uplink*".

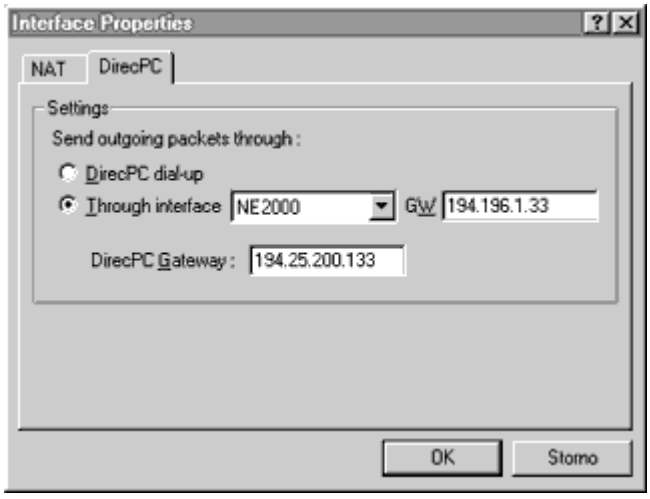


3. Using Ethernet interface for uplink

Sometimes you might want to use the Ethernet Interface for uplink. This happens typically if uplink is realized over ISDN connection (and you have ISDN Router or modem) or V-SAT connection (dish with Ethernet adapter).



Go to the DirecPC interface card properties dialog.



- In the NAT tab, check ON "*Perform NAT with IP address of the interface on all communication passing through*".
- In DirecPC tab choose "*Through interface*" and select the interface linking to the Internet. Then, enter the default gateway of your ISP to the "GW" field (e.g. 194.196.1.33).

Increasing Throughput:

You will probably experience slow speeds and incomplete file transfers from all clients passing through WinRoute. To correct this you will need to make a registry modification that will increase the TCP receive window. To enter the registry go to the start menu -> run, then type "regedit" from the text box.

Important: This must be performed on each computer behind WinRoute.

In Windows **NT/2000**:

Go to the Registry
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Add (if it exists, edit it) an entry named "TcpWindowSize" (it is of type DWORD) in registry. Set its value to "BB80".

In Windows **95/98/ME**:

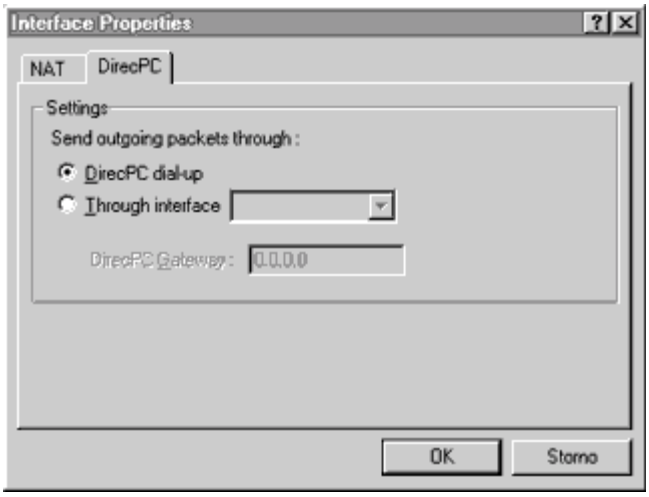
Go to the Registry
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\MSTCP.

Add (if it exists, edit it) an entry named "DefaultRcvWindow" (it is of type string) in registry. Set its value to "BB80".

1 Note: BB80 is in **hexadecimal** format. The **decimal** value is 48000.

Two-Way DirecPC

From the WinRoute administration window proceed to settings -> interface table. You should see the DirecPC USB satellite device. Double click on this device and the properties window should appear. Under the NAT tab make sure you check the box to enable NAT for this device. Under the DirecPC tab specify that you transmit through DirecPC dialup. Note that this does not actually use any dial-up accounts, but it is a necessary setting for WinRoute to function properly with two-way DirecPC.



Increasing Throughput:

You will probably experience slow speeds and incomplete file transfers from all clients passing through WinRoute. To correct this you will need to make a registry modification that will increase the TCP receive window. To enter the registry go to the start menu -> run, then type "regedit" from the text box.

Important: This must be performed on each computer behind WinRoute.

In Windows **NT/2000**:

Go to the Registry
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Add (if it exists, edit it) an entry named "TcpWindowSize" (it is of type DWORD) in registry. Set its value to "BB80".

In Windows **95/98/ME**:

Go to the Registry
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\MSTCP.

Add (if it exists, edit it) an entry named "DefaultRcvWindow" (it is of type string) in registry. Set its value to "BB80".

Note: BB80 is in **hexadecimal** format. The **decimal** value is 48000.

DNS solutions

DNS Forwarding

WinRoute's built in DNS forwarder provides you with the forwarding of DNS queries to a regular DNS server for domain name resolution. It is capable of resolving local DNS queries (when using the name of the local computer). However, DNS queries such as *www.whatever.com* must be resolved by the regular DNS server. WinRoute's **DNS Forwarder** will **forward** DNS queries to the **DNS server**.

The DNS forwarder is configured using the menu: *Settings => DNS forwarder*.

- ***NOTE: The DNS forwarder is only activated for computers pointing to the IP address of the WinRoute computer as their primary DNS server.***
- ***Note that the cache only stores the answers which are of the "Name => IP address" type. The answers are stored until they expire.***

"Enable DNS forwarding"

This option controls whether the DNS server is switched on or off.

"Forward DNS queries to the server automatically selected from the DNS servers known to operating system."

If selected, all DNS queries are forwarded to the DNS server chosen from the TCP/IP configuration of the Internet interface or Dial-Up networking

"Forward DNS queries to"

Enter the numeric IP address of the DNS server to which you want to forward the DNS queries. Choose an address of your ISP's DNS server or of a server to which you have a quick access.

"Enable lookup in HOST file"

With this option checked, the DNS server is allowed to use data from the HOSTS file when answering the queries.

"Edit HOSTS file..."

This button launches an external text editor in which you may edit the HOSTS file.

"DNS domain"

Enter your domain name (e.g. "acme.com") here. When answering DNS queries, the domain name is appended to host name obtained from the HOSTS file or from the DHCP lease table.

"Enable DNS cache"

This allows answers to DNS queries to be stored in internal cache. Subsequent queries are then processed using the contents of the cache, without waiting for an answer from the DNS server outside your network.

"When resolving name from HOSTS file or leased table combine it with DNS domain"

This feature may be better understood from an example - you may want to resolve a DNS query for computer JOHN. In the HOSTS file you entered that your domain mydomain.com is associated with a specific IP address. Then JOHN.mydomain.com will resolve to John's IP address.

DNS server and WWW behind NAT

If you run your own DNS server and WWW server on the same private network you may ask the following questions:

How do I manage DNS queries for www.mydomain.com coming from my LAN? How will they be answered by the web server's private network IP address while DNS queries coming from the Internet will be get a regular Internet IP address associated with www.mydomain.com?

This assumes you have already made a port mapping for UDP port 53 for DNS resolution, and also TCP port 80 for HTTP services.

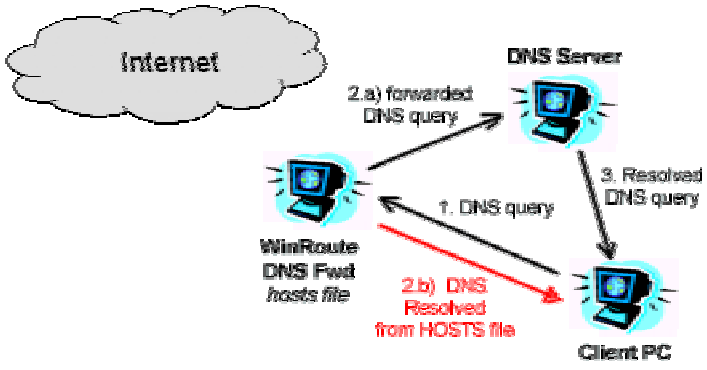
You will use WinRoute's built-in **DNS forwarder** to resolve the problem. At all client PCs you will set WinRoute's DNS forwarder as the DNS server. On the WinRoute PC you will have to perform the following settings:

- Switch ON WinRoute's DNS forwarder
- Edit HOSTS file:

  In HOSTS file add record saying that www.mydomain.com is at specific private IP address (the one where your web server runs - e.g. 10.10.10.8). The HOSTS file is found in the root of your windows directory (where windows is installed - c:\Windows or c:\win98 etc.). You may access HOSTS file also from WinRoute DNS forwarder dialog by clicking button "Edit HOSTS file".

How will it work?

All DNS queries sent by the client computers from your LAN will be resolved by WinRoute's DNS forwarder first. All queries will be checked against the records in the HOSTS file first. If the corresponding record is found, the query will be answered by the details in the HOSTS file (private IP address in our scenario). Inversely, all DNS queries from the Internet to your DNS server will be mapped directly to the local DNS server, bypassing WinRoute's DNS forwarder.



If there won't be any record matching the query in HOSTS file the query will be further checked against to the records in WinRoute's DNS cache (that is included in WinRoute DNS forwarder). If DNS cache won't contain matching record the query will be sent further to DNS server that is set in WinRoute DNS forwarder for sending DNS queries to.

All DNS queries coming from the Internet will be forwarded based on Port Mapping settings directly to DNS server and resolved based on its records.

- ***Note! In such scenario you cannot run DNS server at the same computer as WinRoute. It is because both services - WinRoute's DNS forwarder and your DNS server would run on the same port - UDP 53.***

HOSTS

Running a Web server (or FTP etc.) on a PC behind WinRoute

You may want to run your web server on a PC behind WinRoute (with a private IP address e.g. 10.10.10.8). You may also want a domain for your server. For this to work, the domain e.g. yourdomain.com must resolve to the Internet routable IP address that must be associated with the WinRoute computer. WinRoute's NAT and port mapping will allow traffic destined to a particular port to be forwarded to the internal server at 10.10.10.8. In order for port mapping to work however, traffic must arrive at the NAT'd interface. When local computers on the 10.10.10.0 subnet try to connect to www.yourdomain.com they get the public/Internet routable address, which is the address of the WinRoute computer. Since this traffic arrives to WinRoute through the non-NAT'd interface it will not be mapped to the actual server. To compensate for this situation you must configure all local users to use the IP address of WinRoute as their primary DNS server. This is easily done through DHCP. Then you will use WinRoute's built in **DNS forwarder** as the DNS server for your computers.

In the **HOSTS** file you will add another entry where you will say that **www.yourdomain.com** is operating at the appropriate **internal** (private class) IP address. You will let the DNS forwarder look at your HOSTS files before it will send a DNS query to the regular server.

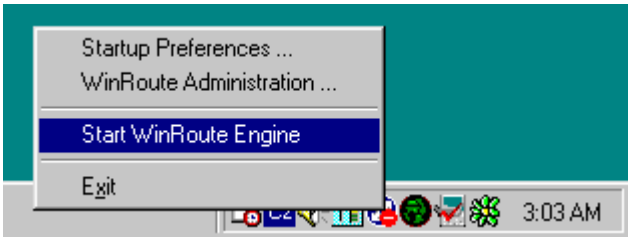
Then every time users send a request for **www.yourdomain.com** such requests will be answered by the appropriate local address.

Administration in WinRoute

Administration from local network

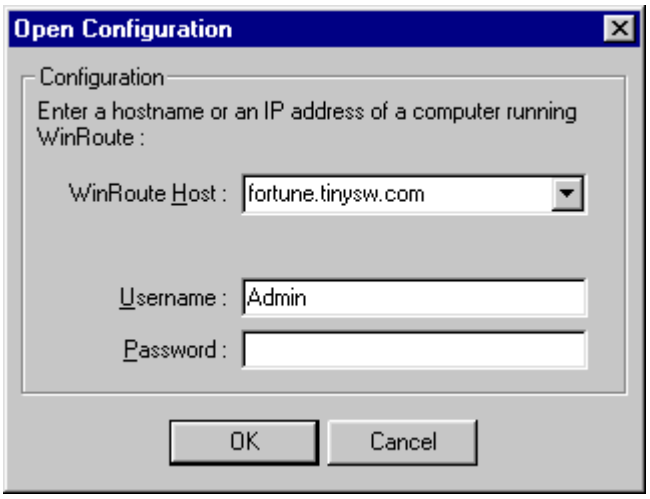
To administer WinRoute from the local network or from the computer running WinRoute you have to perform the following:

1. **Verify that WinRoute Engine is up and running**
   To check that WinRoute has been started, run WinRoute Engine monitor from the WinRoute Program group. A small, round blue and white icon will appear in the system tray of the task bar (lower right corner of the desktop). This indicates that the application is running. A red cross through the icon indicates that WinRoute is stopped. To start the WinRoute Engine simply **right- click** on the icon and choose Start WinRoute Engine from menu that popped up.



2. **Start WinRoute Administrator**
   To start WinRoute Administration module, launch the application from menu Start=>Programs=>winroute professional=>wradmin.exe or by right-clicking on the WinRoute Engine Monitor icon and choosing *WinRoute Administration* from the pop-up menu. You may also copy the *WRAdmin.exe* file to any other computer in your network and run it from there.

When the Admin window pops up, either leave preset local host or enter the IP address of the computer where WinRoute is running. Enter a user name and the password used for administration.



Note: If connecting for the first time, you may use "Admin" as the user name and leave the password blank. See User configuration for further details regarding User name and password policy for administration.

You have to login as Administrator to WinRoute Engine successfully in order to perform settings.

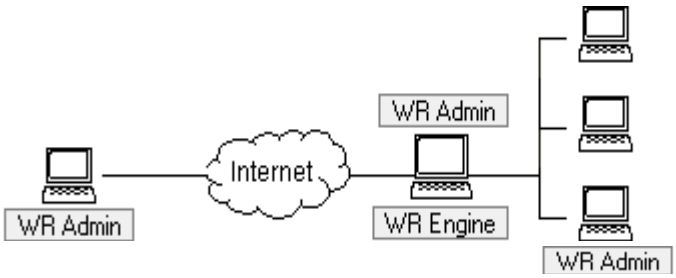
Possible reasons for an unsuccessful login from a local network:

- WinRoute Engine is not up and running
- Wrong user name and password
- Wrong IP address entered when connecting to WinRoute's Engine
- You do not have the rights to administer WinRoute

- There is NAT switched on the interface linking to your network – see Checklist and Setting up network chapter of this help
- You have disabled remote administration over network from the remote administration options in the advanced settings

Administration from the Internet

You may administer the WinRoute Pro Engine from any computer in the world as long as there is a TCP/IP connection in place. The administration is secure (encrypted) and controlled via user name and password.



In order to administer a WinRoute computer from outside the LAN (from the Internet) Port Mapping must be set on the WinRoute computer (assuming you're using NAT and the host computer isn't excluded). With NAT enabled on the interface linking to the Internet (necessary for Internet sharing) your entire network including WinRoute computer is fully protected and therefore no one has the access to it.

To set Port Mapping for remote administration go to menu *Settings=>Advanced=>Port Mappin*g, press add and set:

Protocol: TCP/UDP

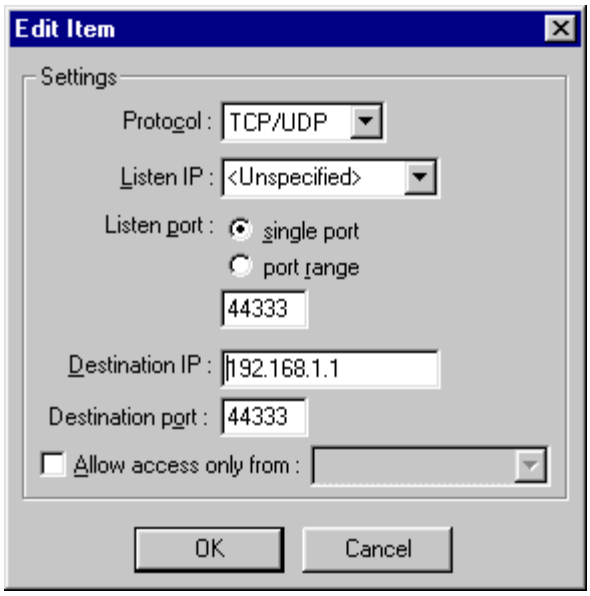
Listen IP: <unspecified> (recommended) or the IP address of the Interface.

Listen Port: 44333

Destination IP: The IP address of the interface linking the WinRoute computer to the local network (private class IP address)

Destination Port: 44333

Allow access only from: If checked you may further limit the access to the WinRoute Engine. You have to predefine IP addresses allowed to access WinRoute Engine from the Internet in menu *Settings=>Advanced=>Address Groups*. You may group together separate IP addresses, ranges of IP addresses and networks.



See examples for more details about Port Mapping. If you have everything set accordingly just run WinRoute Administration program from any computer and enter the IP address of the computer running WinRoute and also the user name and password used for administration at that computer. See User configuration for further details regarding User name and password policy for administration.

Possible reasons for an unsuccessful login from the Internet:

- WinRoute Engine is not up and running
- Wrong user name and password
- Wrong IP address entered when connecting to WinRoute Engine
- You do not have the right to administer WinRoute
- There is no or wrong Port Mapping set on a computer running WinRoute Engine

Restricting access to administration

➢ ***Restricting administrative rights at an application level***

When defining WinRoute users you have the option to define three levels of administrative rights for each user: Full access, log viewing only, or mail transfer/dial up control. For configuration manipulation and log viewing the administrator must use the administration program **wradmin.exe**. This application is just under one megabyte and can be run from any PC running Windows 95/98/ME/XP/NT/2k. It is possible to completely disable remote administration through the settings -> advanced -> remote administration. From this same dialog you can also restrict access to a particular pre-defined address group.

➢ ***Restricting administrative rights at a network level***

WinRoute uses TCP and UDP protocol both over port 44333. It is only necessary to open UDP port 44333 if you would like to view log window data in real time. If NAT is enabled, inbound access to port 44333 on the NAT'd interface will be refused. If NAT is not enabled or you wish to restrict access to a selected group of IP addresses you can set up filters in the settings -> advanced -> packet filter. For more information refer to the section 'Setting Up Security' in this Chapter.

Web administration

Users defined in WinRoute may be configured with the ability to control dial up status and mail transfers. These actions may be performed by connecting remotely to the WinRoute computer through wradmin.exe, or through the web admin interface. The web admin interface can be accessed by any web browser by connecting to http://winroute:3129, where 'winroute' is defined as the netbios name or IP address of the winroute computer. The web administration is a simple dialog that allows a WinRoute user to dial\hang up a ras connection, or initiate mail transfer (only applicable when using WinRoute's built-in mail server). Access rights to this feature can be set in the settings -> advanced -> remote administration dialog.

Lost Admin password

First stop the winroute engine, then go to the registry editor by going to the start menu -> run and type 'regedit'. Proceed to hklm/software/kerio/winroute/user/0. Delete the '0' key. Then select the 'user' key and export it to a file. Then go back into regedit to hklm/software/kerio/winroute. In the right hand window you'll see 'adminuseradded'. Modify it to '0'. Then start the engine and log in as admin with no password. Then stop the engine. Once the engine is stopped import the registry file and restart the engine.

Users and Groups

About user accounts

WinRoute - User Accounts

WinRoute can be programmed with individual user accounts that can be grouped (configured under the Settings | Accounts… | Users tab). Existing Windows NT/2000 users can be imported via the Advanced tab under the Settings | Accounts… menu.

What is a user

As a user of WinRoute you may participate in WinRoute administration, have a mailbox and participate in access restriction policies in WinRoute's Proxy.

Users may create groups and apply above mentioned privileges or restrictions to them.

Adding a user

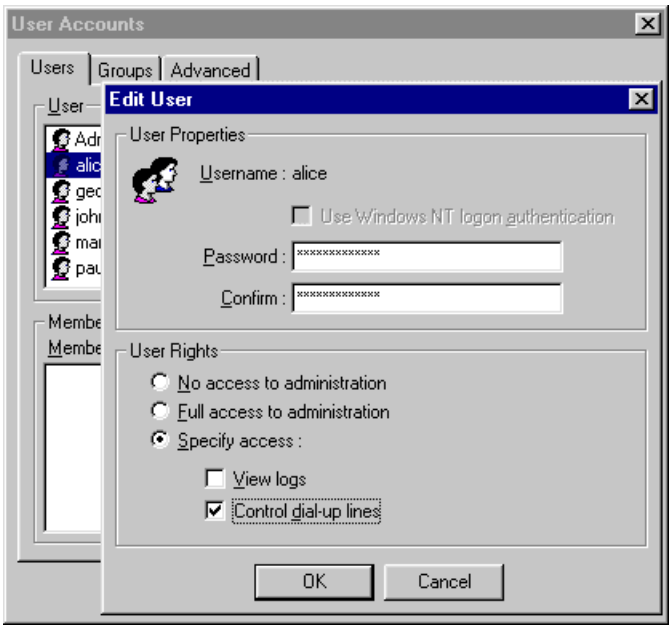
To add a user:

1. Go to menu **Settings->Accounts**
2. Press **Add** button
3. Define **user name** and **password**
4. Assign user with **rights**:

   User has no right to administer WinRoute.

   User has full access to administration

- **View logs:** User has the right to login to WinRoute administrator and to see the log windows only (debug information, proxy log, mail log etc.). User does not have further access to change the other settings.
- **Control Dial-up lines:** User has the right to login to WinRoute administrator and to establish – disconnect the Internet connection. User does not have further access to change the other settings



Groups of users

In WinRoute you may group users into different groups. A user may be a member of more groups simultaneously.

You may assign the group with **rights**.

➢ ***Note: the rights assigned to a group "overwrite" the rights assigned to a user.***

Group members may have the following **rights**:

User has no right to administer WinRoute.

User has full access to administration

- **View logs:** User has the right to login to WinRoute administrator and to see the log windows only (debug information, proxy log, mail log etc.). User does not have further access to change the other settings.
- **Control Dial-up lines:** User has the right to login to WinRoute administrator and to establish – disconnect the Internet connection. User does not have further access to change the other settings

Proxy server

Proxy overview

The **main purpose** of a proxy server is to **save** you the **bandwidth** of your Internet connection. If users access the Internet through a proxy, the proxy server can **store** the various requested objects passing through (like HTML pages, images, and other kinds of files) in its **cache**.

If the pages or images are requested again by the same user or by someone else, the proxy server will provide the requested item from its cache. This **decreases** the load on the Internet connection and the entire operation is also much faster than downloading images from the Internet again.

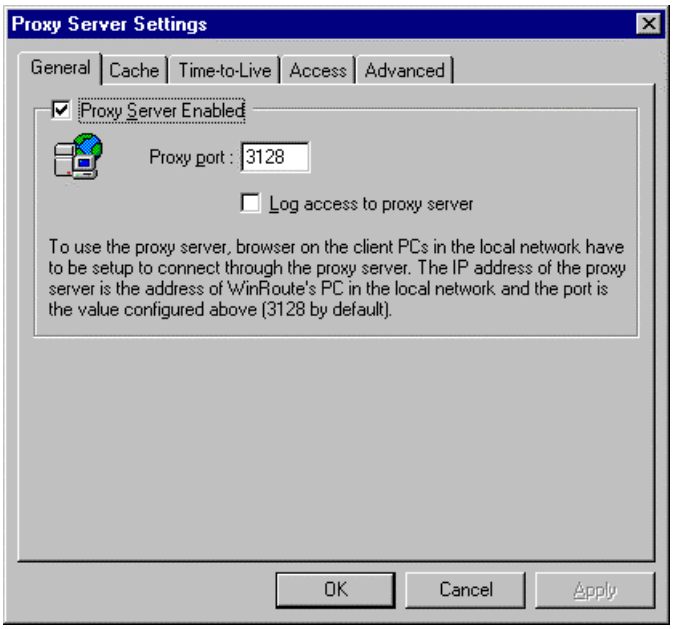
On the other hand, objects stored in cache, of a proxy server get outdated. You have to balance **TTL** (Time-To-Live) of stored documents carefully to avoid misunderstandings arising from the fact that you just read yesterdays CNN news - as an example.

Quick setup

First of all - with WinRoute you **don't need** the Proxy Server to access the Internet. Your Internet connection is well maintained by the **NAT router** that WinRoute includes. NAT is far better for Internet sharing than Proxy technology. However WinRoute also includes a Proxy Server in order to offer caching functionality where required.

To start using the Proxy server in WinRoute, follow these simple steps:

1. In WinRoute Administration select *Settings -> Proxy Settings -> General* tab. Check the "Proxy Server Enabled" option. The proxy server will bind to port 3128 by default, however the user may choose another port if necessary.



2 In your Internet browser (Explorer, Netscape, Opera...), go the to proxy settings, choose manual proxy configuration and enter WinRoute's PC address as the proxy server's address for HTTP, HTTPS, FTP, and Gopher protocols. Enter 3128 as the proxy port number for all the protocols.

3 Test the setup by accessing some web page from the browser.

General Properties Tab

Proxy Server Enabled

Use this to switch the Proxy Server on and off.

Port number

The port number on which the Proxy Server listens for requests. Usually, there is no need to change the default number, 3128.

Log access to proxy server

With this option enabled, all URLs requested from the proxy by the browsers are recorded to the http log.

User Access Control

WinRoute's Proxy server allows the administrator to control access to Web pages. The administrator may decide that access to certain web pages or domains will only be allowed to specified users and/or user groups.

Access List

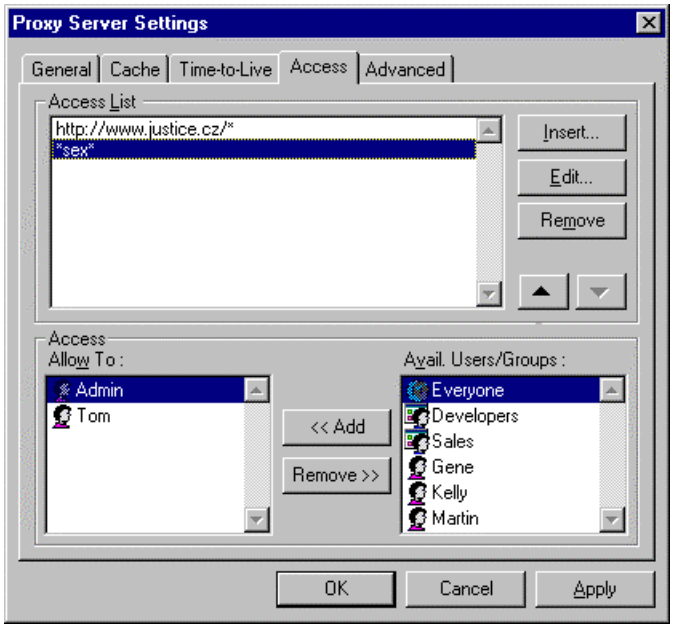
The list of URLs that are restricted. You may use asterisk as a wild card in the URL. For example, to match all computers in somedomain.com, use the string "*.somedomain.com". WinRoute also uses sub string tests to match the URLs, so for example if the string "sex" matches the same set of URLs as the string "*sex*" (only the latter variant was supported in previous versions of WinRoute)

Allow To

The list of users and/or user groups allowed to access the particular URL.

Avail. Users/Groups

The list of users and groups defined in WinRoute.



If a user tries to access a web page that falls in the category of restricted pages, the user will be prompted for authentication by his or her browser. WinRoute will check whether the user name and password are correct and whether the user is allowed to access the particular web page.

The browser stores the user name and password in its memory. All subsequent requests for authentication are answered automatically so that the user does not have to enter the name and password again and again.

On the other hand, the users should be aware of this feature. If you entered your user name and password sometime during your browser session, you should terminate the browser when leaving the computer to remove your authentication data from computer memory.

About Cache

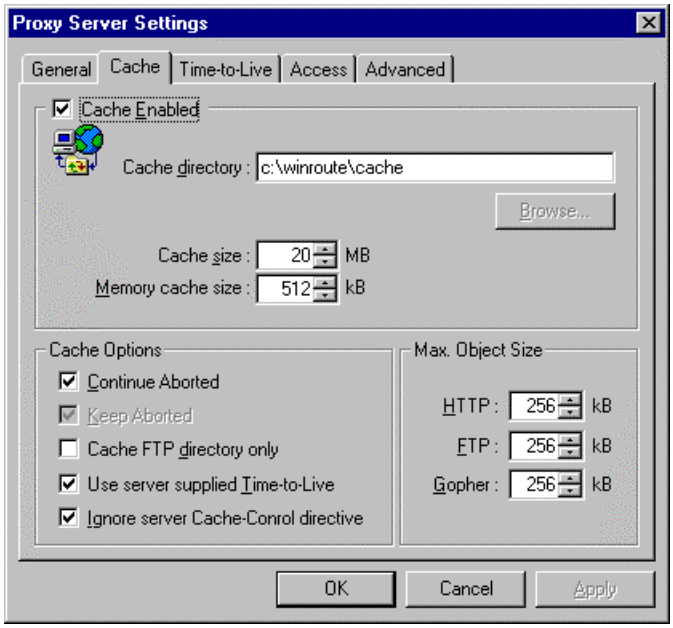
The WinRoute's Proxy Server uses a **very economic** way of storing data. All cached objects are stored in **one fixed-length file**. In contrast, the usual approach used by many proxy servers is to store each object in a separate file.

If the disc uses **large allocation units** (like FAT16), this method results in a **significant waste** of disc space because a lot of web page components are very small. Usually 50% of the objects are smaller than 6 kilobytes, while the allocation unit size on a large disc is 32 KB (with the FAT file system).

The fact that WinRoute Cache stores data in a single file, having all the cached objects in one file saves a lot of disc space - as much as 10 times less space is required when compared to the usual approach.

The single fixed-length file also allows WinRoute to use very efficient indexing techniques that make the cache in WinRoute very fast.

Cache settings



Cache Enabled

Switches the cache on and off. If disabled, each web page is always retrieved directly from the Internet.

Cache Directory

The directory in which the cache will be stored.

Cache size

The amount of disk space that will be used by the proxy cache. When deciding about the size, consider the number of your users, the traffic they generate, etc. If you have enough free space you may set a larger cache. The maximum size is **2000** megabytes.

Continue Aborted

If checked, the Proxy server will always finish downloading an object from the Internet, even if the user's browser aborts the request (the user hits the stop button, or follows a link to another page without waiting for the current page to be downloaded in full). Subsequent visits to the same page are thus much faster.

Keep Aborted

This instructs the WinRoute's Proxy server to cache even incomplete objects (web pages, images). This provides for at least partial speed-up when the web page is revisited. If "Continue Aborted" is checked, the setting of "Keep Aborted" is ignored.

Cache FTP directory only

When browsing FTP servers, use this option to only cache the directory listings. If you wish to cache the files downloaded from a FTP servers as well, switch this option off. The decision whether a particular file will be cached also depends on its size, please refer to "Max. Object Size" bellow.

Use server supplied Time-to-Live

Time-to-Live is the period of time after which a particular web page is considered obsolete and its contents must be re-fetched from its server. This option instructs the WinRoute's Proxy server to obey the Time-to-Live (TTL) that comes with the individual pages. If a page has no TTL, the Proxy's default TTL is used.

Ignore server Cache-Control directive

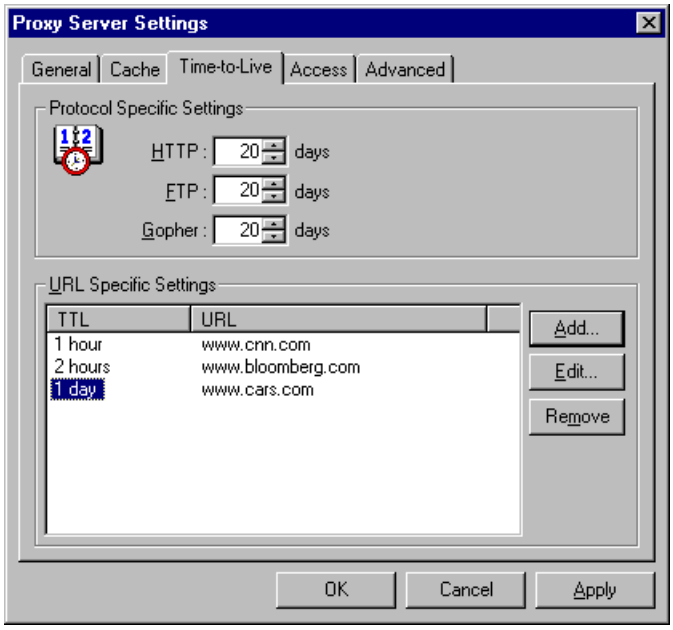
If the contents of a web page changes very often, the author of the page may decide to set the "no-cache" directive for it. This is a very useful feature, however some web sites use the directive much too often, sometimes for all their pages, effectively eliminating the purpose of proxy servers. If you need to protect against such behavior enable this option.

Max. Object Size

The maximum size of objects to be stored in the cache. Larger objects will be passed to user's browser, but not recorded in the cache. Usually you do not need to cache large objects (like program archive files), since you do not download them repeatedly.

Time-to-Live

You may define the default Time-to-Live (TTL) values that are used if a web page has no TTL defined for it or if you decide to ignore the server supplied TTL values (see the option "Use server supplied Time-to-Live" on Cache tab).



Protocol Specific Settings

Here you may set the default Time-to-Live in days for the HTTP, FTP, and Gopher protocols.

URL Specific Settings

If you need to set individual Time-to-Live for some domains, web servers, or individual pages, put the values for individual URLs here. You may set the TTL in days and/or hours.

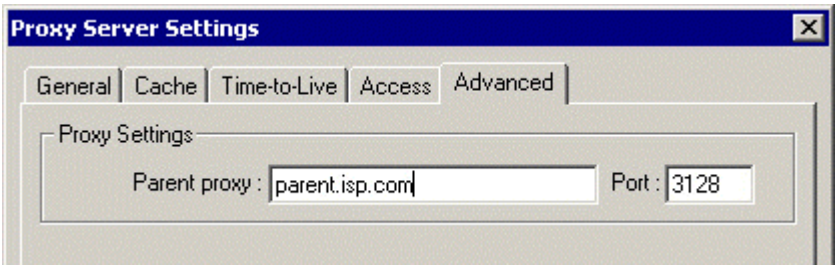
You may use an asterisk as a wild card in the URL. As a new feature in WinRoute, a sub string test is also used to match the URLs, so you may enter just "ftp" to match all servers that have "ftp" in their names. Previously, you had to enter "*ftp*" to cover this case).

Please note that if you have enabled "Use server supplied Time-to-Live" on the Cache tab, the server supplied TTL has higher priority than "URL Specific Settings".

Using a Parent Proxy Server

Parent Proxy Server

In some cases, you will need the WinRoute Proxy Server to connect to an "upper-layer" proxy server, the so-called **parent proxy**. Go to the menu *Settings / Proxy Server*, choose the *Advanced* tab and enter the parent proxy server IP address and port here.



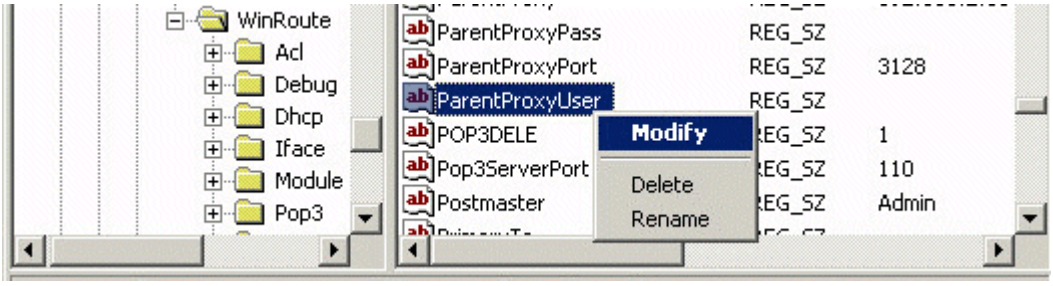
Parent proxy user name and password

The parent proxy server might require user to authenticate in order to access certain (or all) web sites, in the similar way as WinRoute does (see the chapter *Proxy Access Control* for details). WinRoute Pro 4.1 includes such authentication since build 22.

To set up authentication:

- Stop the WinRoute Engine (from Windows Services or using the WinRoute Engine Monitor program)
- Start the Windows Registry Editor (regedit.exe)
- Find the key *HKEY_LOCAL_MACHINE\Software\kerio\WinRoute*
- In the right field, find the text items **ParentProxyUser** and **ParentProxyPass** and change their contents to the appropriate user name and password.
- Close the Registry Editor and start the WinRoute Engine.

After this procedure WinRoute's proxy server will authenticate itself at the parent proxy server.



Setting Up the Mail Server

Mail users

There are several basic rules about users, email addresses and mailboxes in WinRoute.

One User = One mailbox...

Each user of WinRoute has a **mailbox** created. The mailbox keeps the name of the user. In case you have an Internet domain registered and entered in WinRoute the user email address is automatically user@domain.com.

One User = More addresses

To use different email addresses and build general mailboxes like sales@..., support@...., info@... you may define aliases. The combinations are virtually endless.

To add users:

1. Go to menu **Settings=>Accounts**
2. Add **Users**
3. Group users into **Groups** if necessary

Example:

Company has domain brutus.com. User John will have email address john@brutus.com. For other addressing options see Aliases.

- ***Note: The mailboxes are kept in a separate directory. Typically in c:/Program files/WinRoute/Mail. The mailboxes are physically created AFTER the first email comes in.***

Sending email to other WinRoute users

To send email to other users **within** your LAN use the **WinRoute user name** of the recipient rather than its full **Internet email** address.

Example: The user name of the recipient is John and his full email address is john@company.com. You may enter only *john* into *To:* field of the email message.

Note: Some email clients will require the full email address (user@somedomain.com). Therefore it is necessary to configure aliases.

Aliases issue

If you use the **full email address** of a local user the message will go **through** the Internet, i.e. to the relay SMTP server of WinRoute and then back to WinRoute. To avoid this you have to specify aliases.

- ***Remember! You must set the WinRoute PC as your outgoing mail server (SMTP).***

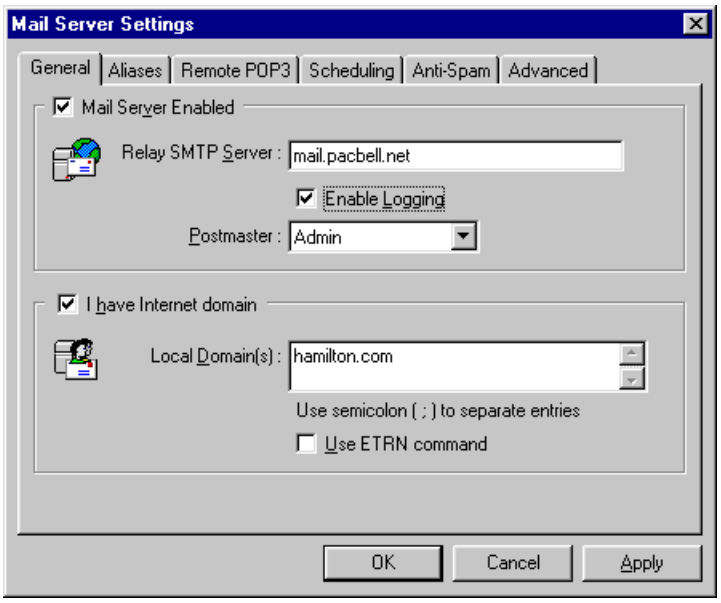
Sending Email to the Internet

You may use WinRoute as your **SMTP server** for outgoing mail. WinRoute uses the **SMTP server** of your ISP to send email out instead of using MX records. In other words - all outgoing email will be sent through the other mail server that you enter (usually the Mail Server of your ISP). The same rules may be applied to your email clients - WinRoute Mail Server may be their relay SMTP server.

To set the relay SMTP server for outgoing mail:

1 Go to menu *Settings=>Mail Server*

Enter the outgoing mail server of your ISP into *Relay SMTP Serve*r field



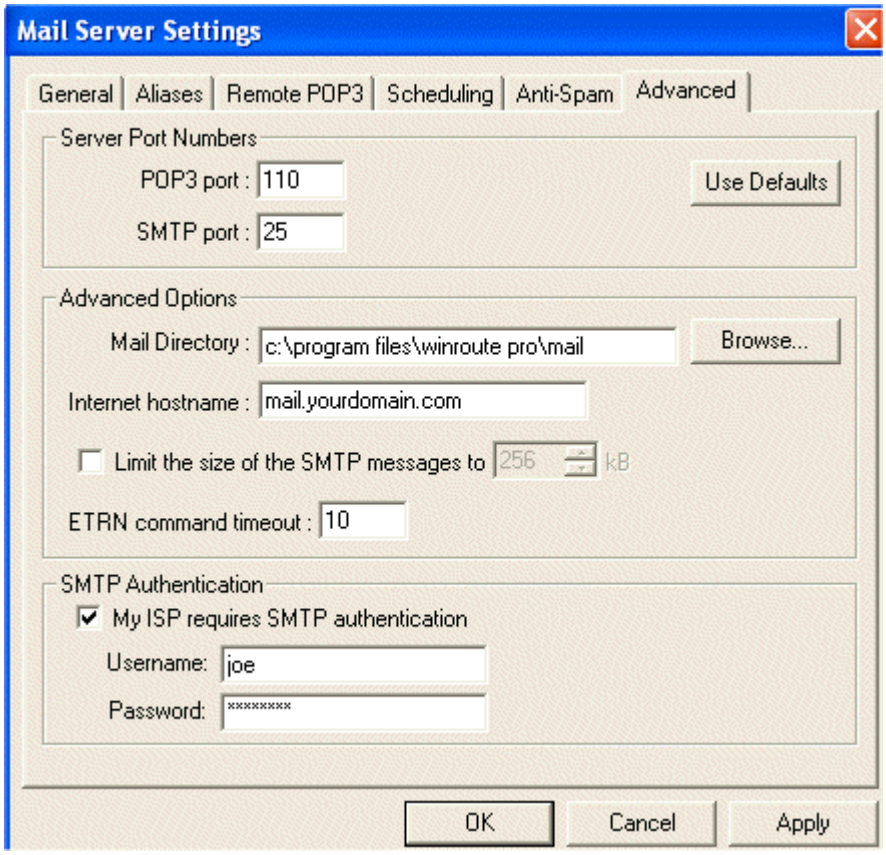
SMTP Authentication

Authentication

To prevent spam and mail abuse, most Internet Service Providers who offer email services will require authentication for mail relay. To configure WinRoute to authenticate when sending outgoing mail

1. Go to *Mail Server->Advanced tab* window

2. Enter desired **host name** into the Internet host name field. This value is not necessary, however it is recommended because it is used to identify the WinRoute mail server to other mail servers.



If your ISP does require authentication they must provide you with this information. Usually if you have at least one POP3 account you can use these credentials within the SMTP Authentication option shown above.

Aliases

Aliases in WinRoute are used for **additional** addressing of users of WinRoute and also for email address **substitution**.

Through **Aliases** you may:

- Assign user with more addresses
- Assign one email address to more users
- Assign one email address to group of users
- Assign group with addresses

Example:

This example shows that the possibilities are virtually endless.

The company has 2 domains:

- Company.com
- Company2.com

User *John* should receive email for:

john_speaker@company.com

john@company2.com

sales@company.com

support@company.com

Email for *sales@company.com* should also be delivered to group *[Sales]*.

Solution:

1. Go to menu *Settings=>Mail server=>Aliases tab*.

2. Add following aliases:

*john** deliver to *John* -

This would deliver all email coming in from the Internet where john appears in the recipient. I.e. *john_speaker@company.com* as well as *john@company2.com* will be delivered to a user *John.* This will also prevent email sent from local users to recipient *john@company.com* from going through the Internet but the email will be delivered straight to John's mailbox on WinRoute.

sales deliver to *John* -

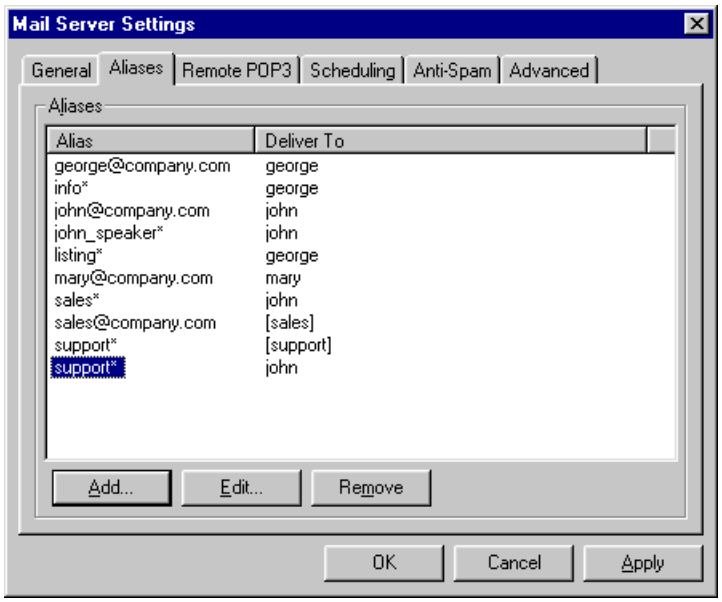
This will deliver all email for *sales@…..*.. to a user *John*

Support deliver to *John* -

This will deliver all email for *support@…..*… to *John*

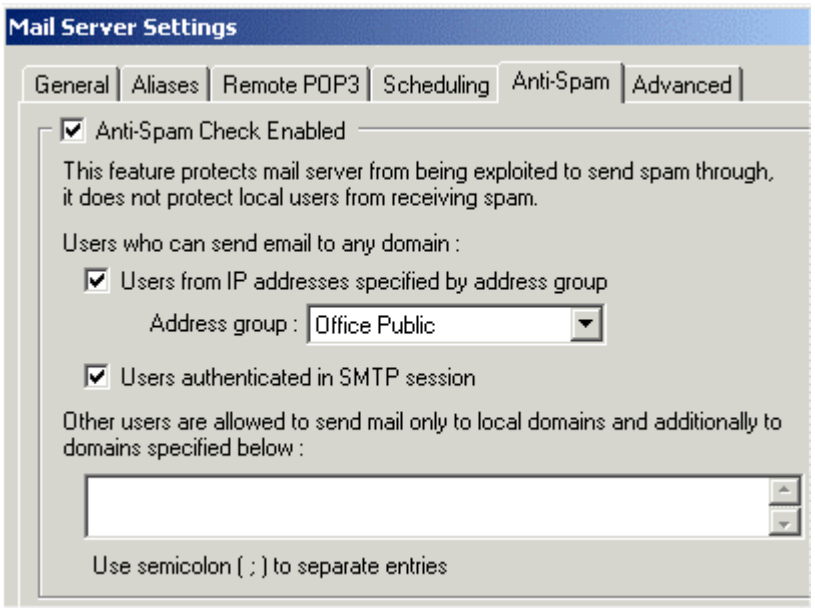
Sales deliver to *[Sales]* -

This will deliver email for *sales@….* to all members of the group *[Sales]*


Mail Server Settings
General
Aliases
Remote POP3
Scheduling
Anti-Spam
Advanced
Aliases
Alias
Deliver To
george@company.com
george
info*
george
john@company.com
john
john_speaker*
john
listing*
george
mary@company.com
mary
sales*
john
sales@company.com
[sales]
support*
[support]
support*
john
Add...
Edit...
Remove
OK
Cancel
Apply

Anti-Spam

This feature is vitally important if WinRoute, as an email relay server, is publicly available. In other words, if you have created a port mapping for TCP port 25 for incoming email. By default, WinRoute's SMTP relay will allow anyone to send email through WinRoute. The anti-spam feature will restrict users that can relay email through WinRoute. As stated within the interface, it does not restrict users from receiving undesired spam email.



The first option 'Users from IP addresses specified by address group' makes reference to any address groups you may have created from the settings -> advanced -> address groups. It is recommended that you create at least one address group that includes the IP range of your local area network. By enabling this option and referencing an address group, IP addresses defined in that group may relay through WinRoute. All other IP addresses will be denied the ability to relay through WinRoute.

If you have remote users that wish to relay through WinRoute, but have dynamic IP addresses that cannot be defined in an address group, it is necessary to enable the second option 'Users authenticated in SMTP session'. This will require users to specify a user name and password in their email client for sending email. Note that if both options are enabled, users with IP addresses defined within the address group will not need to authenticate, however they still may be configured to do so.

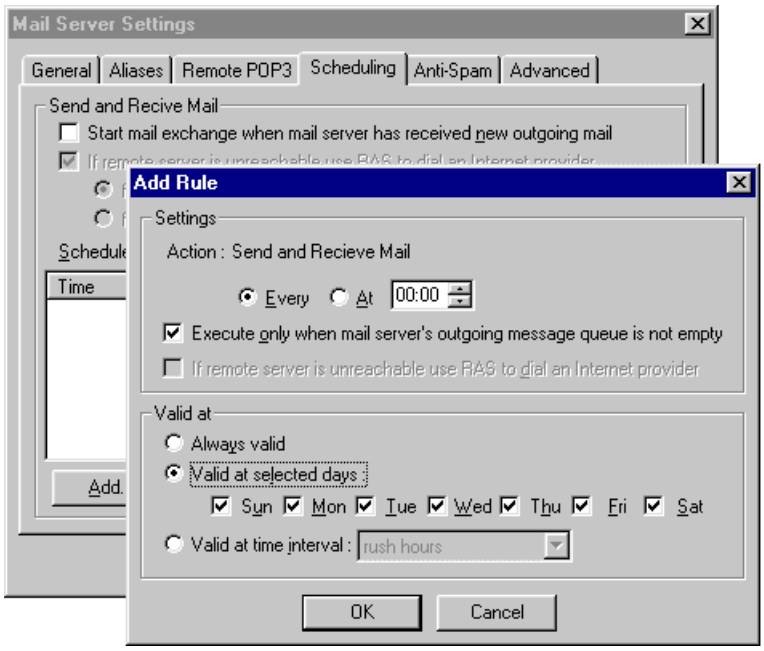
Scheduling Email Exchange

Scheduling in Mail Server settings gives you the option to set:

- Regular intervals to check email at your ISP (whether POP3 or SMTP using ETRN)
- Rules for sending out email
- The time intervals when the rules are valid. You may pre-define the time intervals at menu *Settings->Advanced->Time intervals*

You may decide whether to send new outgoing email immediately after it reaches the Mail server or to send it out in predefined periods of time.

You may also select whether the email server should dial out in case there is a new outgoing email or not. If you select this option WinRoute's Mail Server will establish the connection every time any of your users should send out new email.



To receive email you may specify the whole calendar saying exactly when you would like to pick up the mail. You may combine different rules to make your email retrieval as effective as possible.

1 Go to menu *Settings->Mail Server->Scheduling*

2 Specify options of your choice and add new rules to check out the email.

➢ ***Note! "Time Intervals" rules must be set in menu Settings->Advanced->Time Intervals***

Receiving email

You have domain (SMTP)

WinRoute's Mail Server is fully ***SMTP***[1] and ***POP3***[2] compliant. You may have registered your own **Internet domain** and receive email via SMTP and/or WinRoute may automatically pick up email from the POP3 account of your ISP.

If you have an Internet domain registered to your external (public) IP address WinRoute may receive email by SMTP protocol. In the general tab in the Mail Server dialog box enter the name of the domain you have registered.

- ***Do not forget to map TCP protocol port 25 to the private class IP address of your WinRoute box! Otherwise SMTP protocol will not be allowed to go through WinRoute's NAT!***

Based on your Internet connection you may consider the following:

1 You have a permanent connection

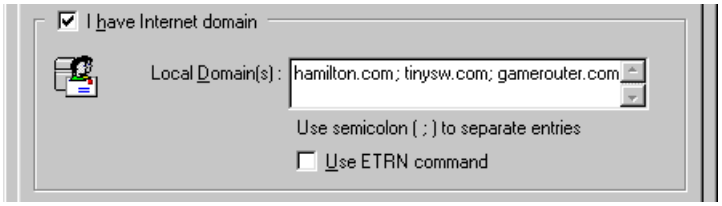
No specific setting is required. Just the domain(s) entered

2 You have a dial-up or ISDN connection (ETRN command)

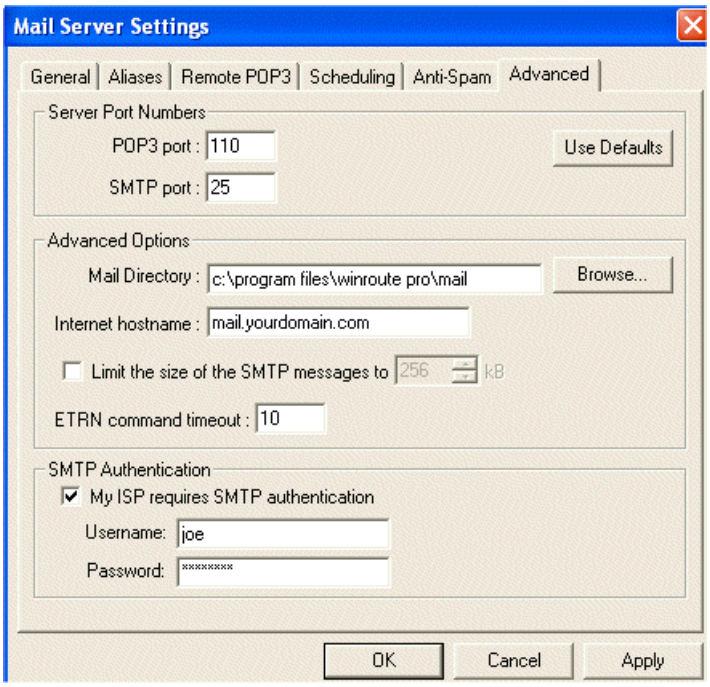
[1] The Simple Mail Transfer Protocol (SMTP) protocol is a TCP protocol that uses port 25. All email is sent using SMTP. SMTP servers inspect the email header and may generate more pieces of the same email if there are multiple recipients. The destination address is analyzed and either delivered to a local mail box or forwarded to another SMTP server. When the email reaches the SMTP server occupying the domain for which the email was intended, the email is stripped of specific header information and delivered to a local user account, whereupon the user must initiate a connection to the server to access the email via POP3, IMAP, or HTTP.

[2] The (Post Office Protocol) POP3 protocol is a TCP protocol using port 110. It is used to gather email. WinRoute functions as both a POP3 server and client.

In case you are not permanently connected your email is temporarily stored at the ISP. The email is transferred when you are connected. Some ISPs require using the ETRN command to send email. WinRoute mail server supports the ETRN command. You may check on the option in the *General tab* of the **Mail server** dialog box.



If you need to, you may set up ETRN time out interval (go to *Advanced tab*).



ETRN command time out

This entry specifies how much time after establishing a connection; WinRoute's SMTP server should make an enquiry for SMTP mail.

Multiple domains

Multiple domains

You may have several domains assigned to your Internet connection. If you have several domains enter all of them into the menu *Settings=>Mail Server=>General* tab and divide them by semicolon.

Issues with multiple domains

There are two ways to arrange multiple domains assigned to your network:

1. Each domain is associated with its own IP address

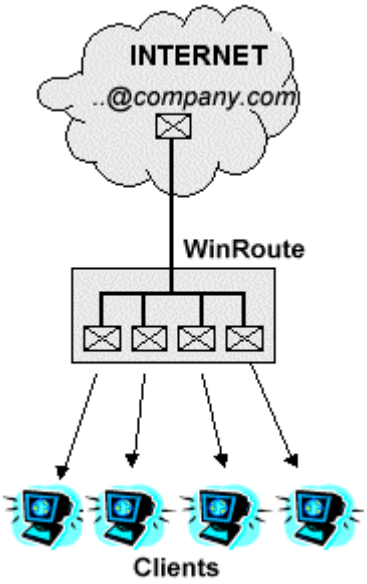
   In this scenario you have to have more public IP addresses mapped to the Interface used by WinRoute for Internet connections. Then you use more port mapping settings - one for each IP address - with the same destination IP address of the WR computer.

2. All domains are associated with one IP address

   There are no special settings required other than to set up port mapping for protocol TCP on port 25 to the local IP address of your WinRoute computer.

You have domain assigned to POP3 account

You may arrange with your ISP that all email for your domain come into a single account. WinRoute may check such an account, pick up the messages and automatically distribute them into the mailboxes of local users.

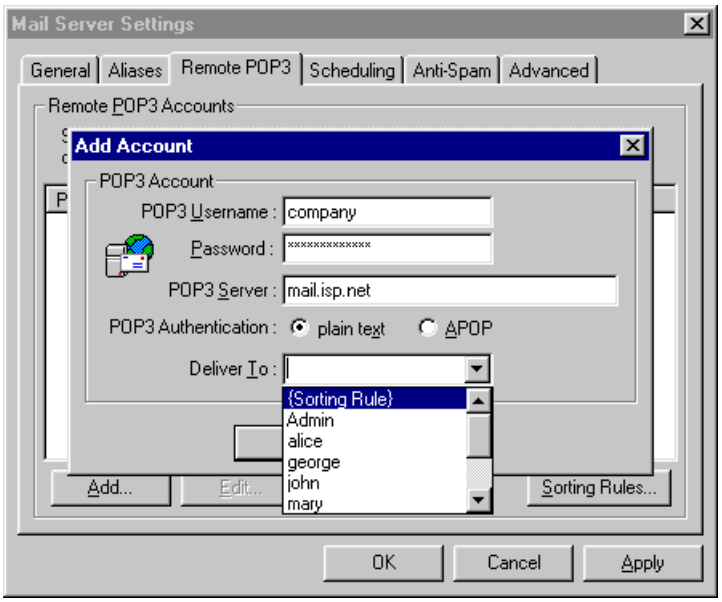


Example

Your ISP arranged mailbox company@mail.isp.net. You may have domain company.com but all email for your domain (sales@domain.com, john@domain.com) comes to the mailbox company@mail.isp.net at ISP.

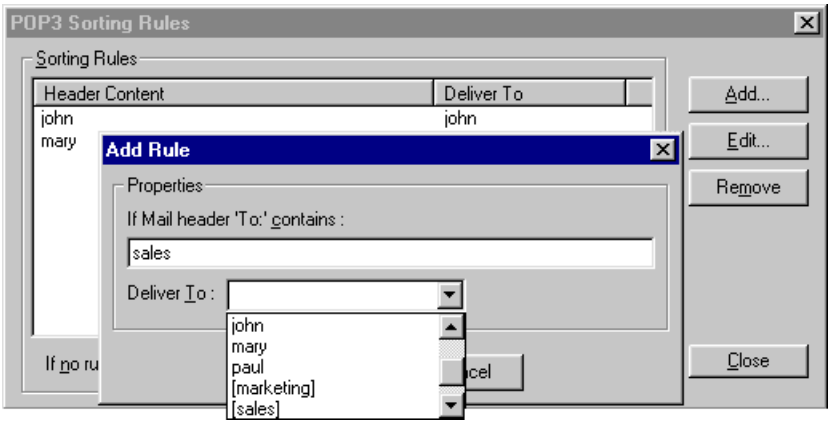
1 Go to menu *Settings=>Mail Server=>Remote POP3*, add new account and enter its details

2 In "Deliver to:" field select "Sorting Rules"



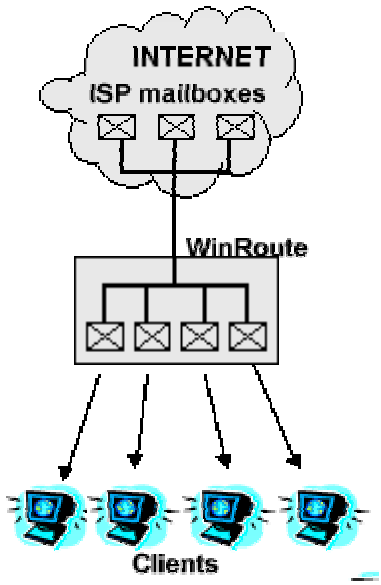
3 Press Sorting Rules button and add new criteria. WinRoute will deliver email based on the email address of recipient, sender or subject

4 In the same dialog select a user or group of users the email should be delivered to.

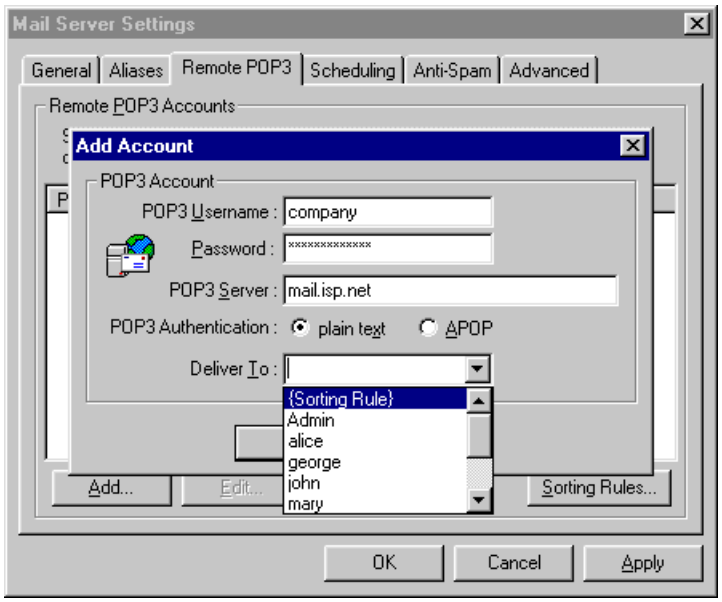


Receiving email - You have several mailboxes at ISP

WinRoute can check several accounts at various ISPs and automatically deliver received email to the mailboxes of local recipients.



1. Go to menu *Settings=>Mail Server=>Remote POP3*, add new account and enter its details.
2. In "Deliver to:" field select the recipient or the group of recipients



Email client software settings

Going through WinRoute Mail Server

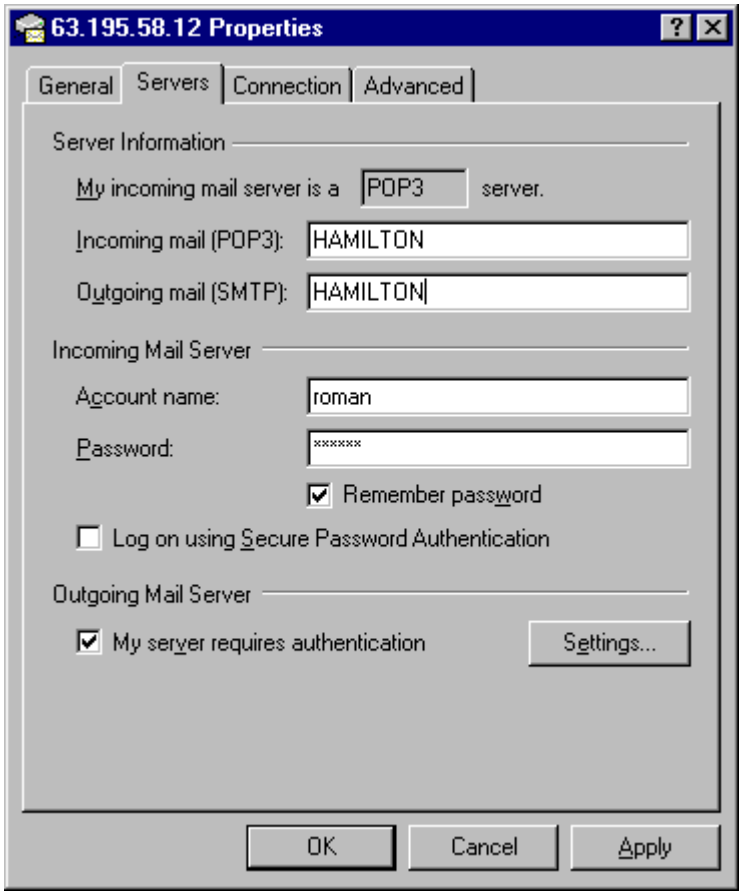
Email through WinRoute's Mail Server

In order to use WinRoute's mail server you must configure your **email client software**. The WinRoute computer will act as the **Incoming** and **Outgoing** Mail Server. As a result, you must enter the WinRoute computer name into the proper field in your email software. If you experience problems sending and receiving mail, we recommend entering the IP address instead of the computer name prior to further investigation. Sometimes the problem is with DNS resolution in your local network.

Example:

WinRoute Mail Server is running on a computer with a dynamically assigned public IP address and a private IP address of 192.168.1.1. The computer name is Hamilton (see Network in Control Panel).

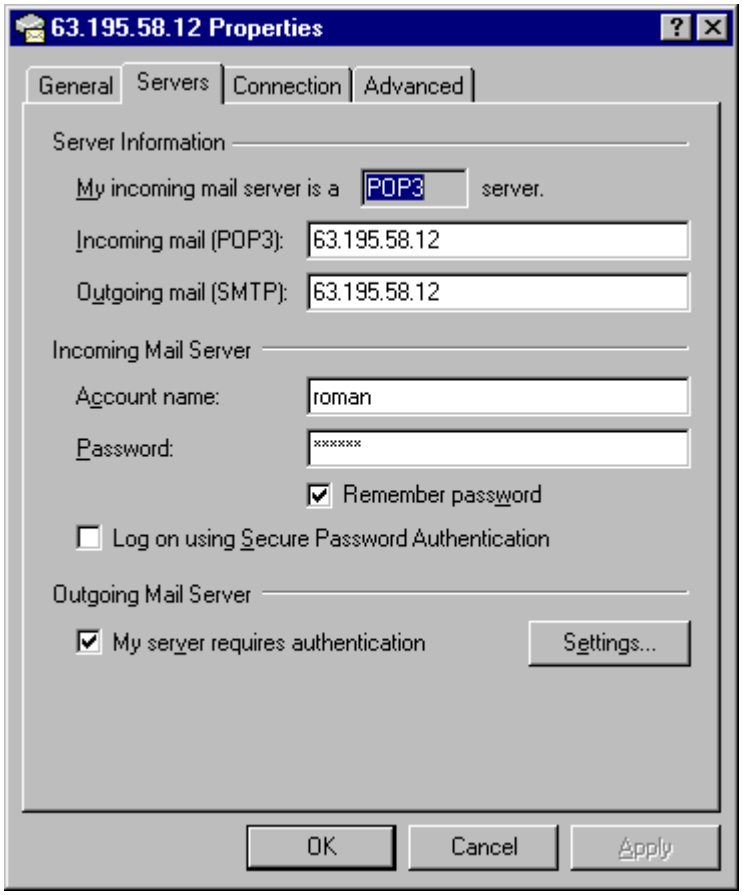
You may enter either HAMILTON or 192.168.1.1 into the Incoming (POP3) and Outgoing (SMTP) Mail Server fields of your email software.


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

Bypassing WinRoute's mail server

You may want to bypass WinRoute's mail server and receive or send email directly from an email client through the mail server of your ISP.

In such a case enter into the outgoing and incoming mail server settings, the appropriate name of the mail servers of your ISP.



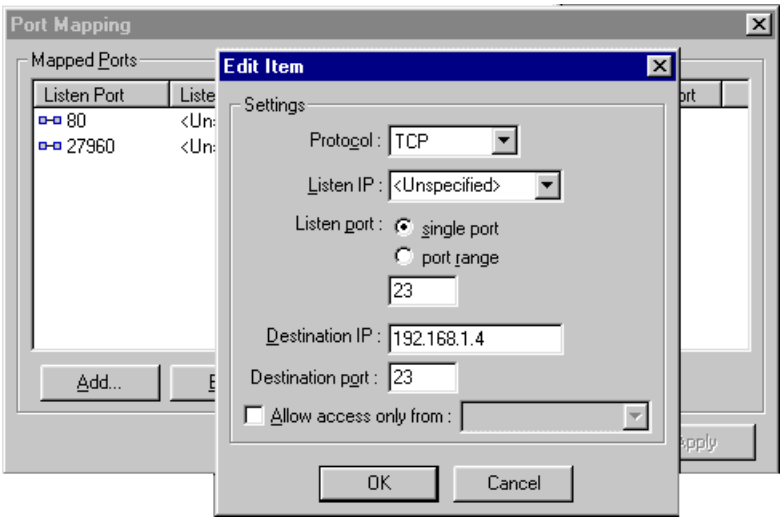
- ***Note! Do not set your email client software to use the Proxy! You must use WinRoute's NAT for Internet access and set your client software to have direct access to the Internet. Your inability to establish email exchange means that NAT is not properly configured.***

Port Mapping/Forwarding

Item Descriptions

To set Port Mapping

1. Go to menu *Settings->Advanced->Port mapping*
2. Add new port mapping:



Protocol

Select the protocol used by application/service. Some applications/services use TCP and UDP protocol together.

Listen IP

The IP address the incoming requests are coming to. Usually it is the IP address associated with your Internet interface. Note: you may have more than one IP address associated with the Interface (if you have more web servers etc.) In most cases you will leave this option unspecified, especially if you receive your IP address dynamically.

Listen Port

The port number that requests will be coming to (e.g. 80 for http).

Destination IP

The IP address within your local network that is running the server (service) answering incoming requests (web server, FTP server etc.)

Destination Port

The port that the destination application is listening on. Typically the same number as the listen port

Allow access only from

You may reference a pre-defined address group so that the port will only be open to the IP addresses included in that address group. The address groups are defined in the advanced settings.

Port Mapping for multi-homed systems (more IP addresses)

You may have more IP addresses assigned to the Internet interface, and run multiple services inside of your network that you want to make accessible from the Internet.

5xWWW servers scenario

As an example let's consider that you want to run 5 Web servers, where each of them has a separate domain associated with a different IP address.

Windows networking will allow you to bind additional IP addresses to a single interface. WinRoute requires that you do this before creating mappings for each IP address.

In such a scenario you will assign 5 IP addresses to your external Interface (linking to the Internet) and run web servers on other computers within your Internal network on private IP addresses such as 10.x.x.x or 192.x.x.x.

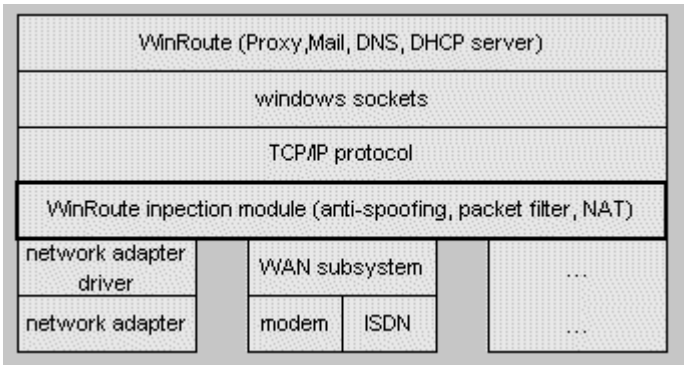
Each Web server may run on a separate computer or you may assign more IP addresses to one computer on your internal network and run all web servers on such a computer.

Then you will define 5 port mappings in the Port Mapping dialog. For each web server (domain) you will define:

- Listen IP address: (IP address associated with the domain name. This IP must be bound to the external adapter).
- Listen port: 80 in our scenario
- Destination IP address: the IP address which runs the web server
- Destination port: 80 (HTTP)

Setting up security

NAT Security

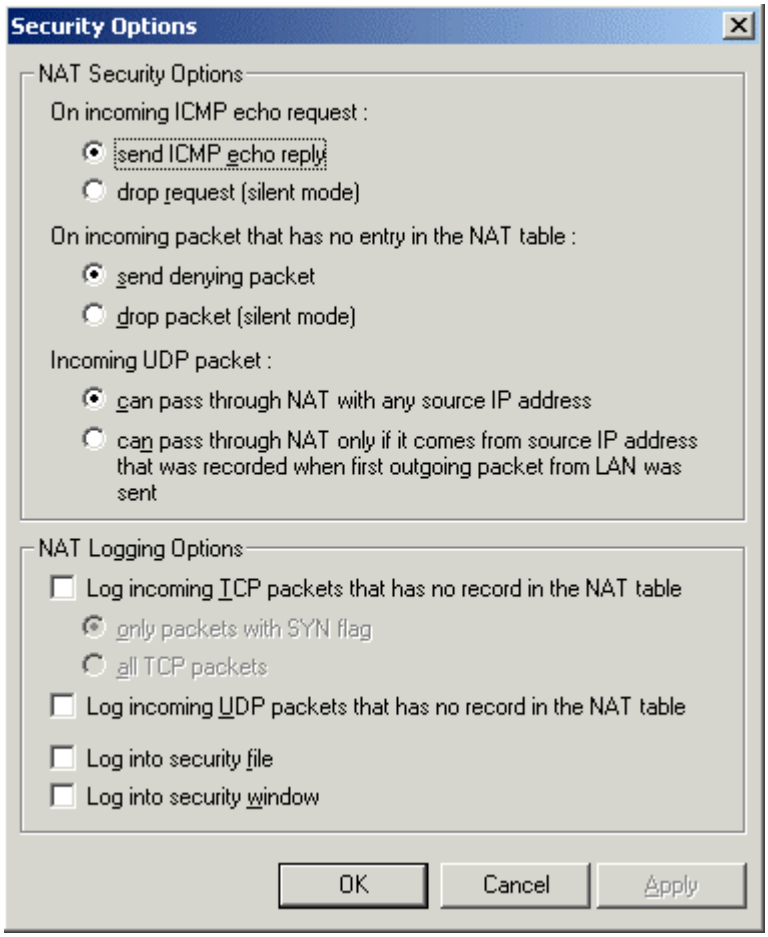


The primary security function that NAT provides is its **Stateful Inspection** of incoming packets. NAT is a process of translating and recording the packet header information of all traffic leaving your local network. This means that WinRoute knows of all communication that was initiated locally. When incoming traffic arrives to the NAT'd interface, WinRoute compares the header information to its records. If there is a match WinRoute retranslates and forwards the packet to the client. If there is no match, WinRoute deems the packet as suspicious and will either deny or drop such traffic. These suspicious connection attempts can also be logged. Refer to the next section for details.

For most small networks NAT is sufficient security. For larger networks hosting services such as dns, mail, web... the packet filtering is an extended measure of security that can help lock down servers so that only the necessary services may be used, while all other communication is restricted.

NAT Security Options

In the advanced settings of WinRoute's build 20 and above is a NAT security options menu that incorporates a **silent mode**. **Silent Mode** means that for incoming connection attempts, WinRoute can "drop" packets so that your network will appear invisible to the outside world.



Incoming ICMP echo request:

Internet Control Message Protocol (ICMP) is used by routers for sending control information across networks. Ping is one of the most commonly used utilities within ICMP and is used to test connectivity between nodes. In some cases you may want to drop ping requests. This can be configured in the packet filters, or more easily from the advanced security options.

- If you select the *"send ICMP echo reply"* WinRoute will allow echo reply messages.
- If you select the *"drop request (silent mode)"* the datagram will be dropped, simply lost in transit. The requesting party will then receive the message *"request timed out."*

Incoming packets with no entry in the NAT table:

When a packet arrives to a NAT'd interface, WinRoute checks the header against the NAT table. If the packet doesn't meet any port mapping criteria and there is no record of its existence, then WinRoute can be easily programmed to respond using either of the two following methods.

- The "send denying packet" option will simply return a packet to the sender saying that a connection could not be established.
- The "drop packet (silent mode)" will eliminate the packet and send no returning packet. This way the WinRoute host, as well as the LAN behind it, will seem non-existent.

On Incoming UDP packets:

- Using this example, if you select "*can pass through NAT with any source IP address*" the UDP packet will pass through NAT if the UDP port number exists in the NAT table. This option is necessary for certain media or gaming applications where communication is initiated with a particular IP, however the incoming UDP stream may come from one or several other hosts.

- To enhance security, you may select "*can pass through NAT only if it comes from source IP address that was recorded when first outgoing packet from LAN was sent.*" This would allow only UDP packets from the IP host address to which the internal client initially contacted. Note that some games or messaging programs may not function with this option enabled.

NAT logging options:

Within the advanced security dialog is the ability to record information of packets arriving to the WinRoute firewall that were not originally requested by someone from inside the LAN. This is useful for detecting port scans and incoming connection attempts to unauthorized services.

Logging incoming packets with no entry in the NAT table:

WinRoute offers two options for logging TCP packets that aren't in the NAT table.

- If you choose to log "*only packets with SYN flag*" (synchronize), WinRoute will log only the initial connection attempt, marked by a SYN flag. This is the recommended option.
- The "*all TCP packets*" option simply logs all incoming TCP packets. This includes both connection attempts and acknowledgements. This option is generally not preferred because it will generate extraneous logs.

Logging to a file or window:

- If you select "*log into security window*" you can choose to view log information from the WinRoute administration application by specifying view-logs-security log.
- If you choose to "*log to a file*", WinRoute will save the log information to the security log located in the logs folder of WinRoute Pro (typically c:/Program Files/WinRoute Pro/Logs)

Excluding the host from NAT

NAT can be enabled on any interface located in settings -> interface table. An additional option "Exclude this computer from NAT" is also available. As mentioned in previous chapters, NAT's firewall capabilities are based on its stateful inspection filter. When the WinRoute computer is 'excluded from NAT', traffic initiated from that machine will not be recorded. Therefore, incoming traffic with a destination address of the WinRoute computer will be allowed even though a NAT entry does not exist. This option should only be used in rare circumstances where certain applications do not function properly through NAT or you are behind another NAT product. For all intensive purposes this option is **NOT RECOMMENDED!**

Setting up Packet Filters

Packet Filter Overview

It is important to understand the logic of WinRoute's packet filters before creating any rules. This section will help outline the concepts Inherent to WinRoute's filtering.

What is an Interface?

An interface is any medium, physical or virtual, through which the operating system will be transmitting/receiving IP traffic. WinRoute will display all interfaces that it identifies in the interface table within the settings menu. Note that you can rename interfaces from the interface table. It is recommended that you create new names for each interface for easier administration when creating filter rules.

What is OUTGOING/INCOMING?

WinRoute always considers its engine as the centerpiece of the entire system. As such, traffic passes THROUGH WinRoute (incoming to one interface and outgoing from the other). As an example, a client computer makes an http get request for some object from yahoo.com. The packet is generated at the client and forwarded first to WinRoute (the default gateway). This packet is incoming to the LAN interface. It is then forwarded to WinRoute's default gateway in which case it is outgoing traffic from the Internet interface. When Yahoo.com sends back the object in a sequence of packets they are incoming to the Internet interface. These packets are then routed back to the client as outgoing traffic from the LAN interface.

What are all possible actions that can be taken by WinRoute?

Each packet filter rule will follow one of three actions: **Permit**, **Deny**, or **Drop**. If you choose to deny a packet, WinRoute will send back a response to the requesting host indicating that the connection attempt was refused. If you choose to Drop a packet, the requesting client will receive no response from the WinRoute firewall, as if the WinRoute computer was physically disconnected from the network or not powered. Permit simply allows the packet to be routed to its destination.

Rules set per Interface

WinRoute can define separate security rules for each interface you have in your computer. This is useful for networks with DMZ segments, or multiple subnets that are segmented through WinRoute.

RULES APPLICATION:

From TOP to BOTTOM

Rules are defined in a list and applied from top to Bottom. When a packet reaches an interface, it is checked against the list of rules. The filter looks at the top criteria first and goes down the list checking the lowest rule last. If a packet meets the criteria, the rule is applied and the rest of the rules are omitted. For this reason it is best to place all allow rules on top and create a single drop rule at the bottom for all IP traffic.

Rules may be applied to:

- Stand-alone IP hosts
- Range of IP addresses
- A user defined group of IP addresses
- The whole subnet or network

Rules may be applied in predefined time intervals

In some cases, it may be useful to apply specific rules during office hours and different criteria for after hour access. These intervals can be created in the advanced settings and referenced by individual filter rules.

TCP flags

One of the unique features of WinRoute's packet filter is the ability to check for SYN/ACK TCP flags. Before all TCP connections there is an initial connection, the 'hand-shake'. This process begins when the connecting client sends a packet to the server with a synchronization (SYN) flag. The server then replies with a synchronize and acknowledgment (SYN/ACK). The client and server both proceed with acknowledgments and the connection is established. WinRoute denotes the **SYN** and **ACK** flags with the terms '**establishing**' and '**established**'. Note that If both flags are checked WinRoute will apply the rule only for the server response packet, where both flags are set in the TCP header.

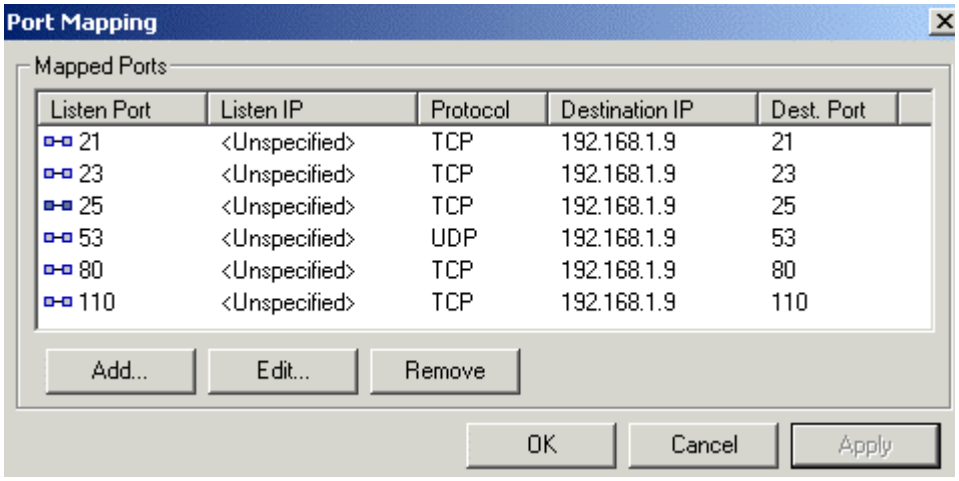
Securing servers behind NAT

Securing Local Servers using NAT and IP filtering:

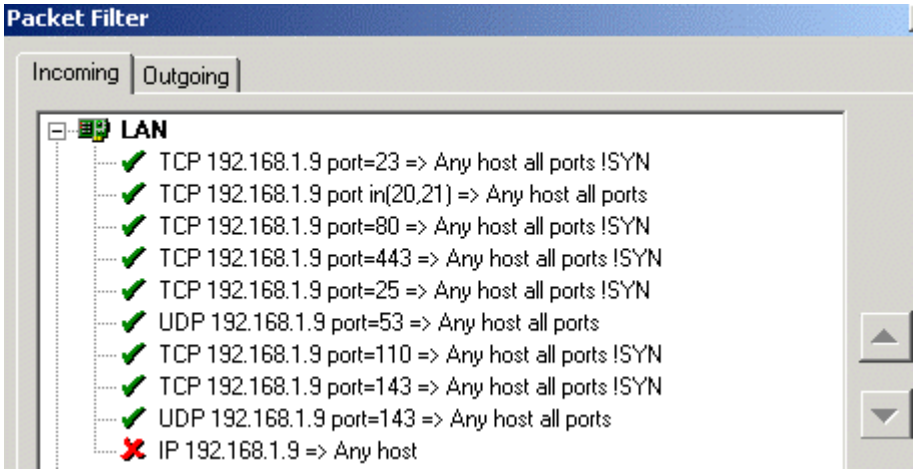
Many WinRoute networks involve servers placed behind WinRoute that are only accessible through port mappings so that the necessary services are publicly available, while all other connection attempts are denied by NAT's stateful inspection. NAT protects the server from inbound traffic arriving from the Internet or any other public network, however WinRoute will (by default) allow all outbound IP communication. For most cases NAT security is sufficient, however it may be desirable to restrict everything except that which is absolutely necessary. In other words, only returning traffic (server response) will be allowed out to the Internet.

Consider the following example.

Let's assume there is a server at 192.168.1.9 hosting the following services (TELNET/FTP/HTTP/HTTPS/SMTP/DNS/POP3/IMAP). NAT with port mapping will allow only the necessary inbound services. For port mapping configuration see the 'Port Mapping/Forwarding' section in this chapter.



To ensure that only the necessary server response packets are passed through the WinRoute firewall back to the requesting client the following packet filter rules are necessary.



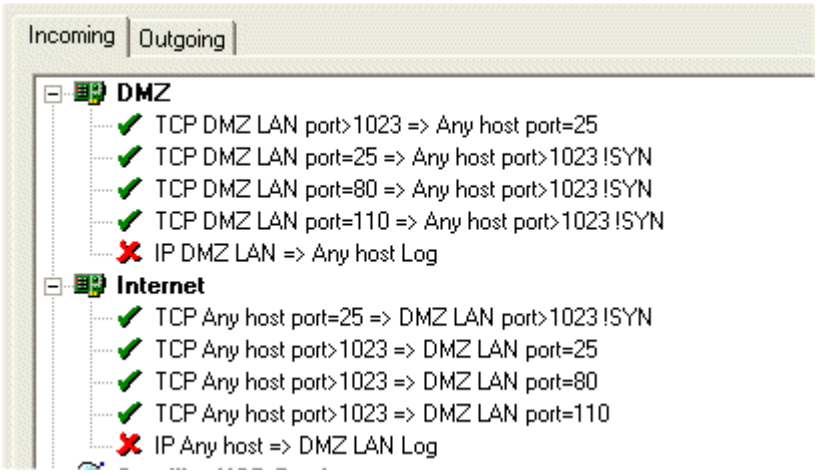
Note that in each case we are concerned with only the source information because it will always be the same. The destination information will be variable so we cannot define values based on this criteria. Note that for most of the TCP rules the '!SYN' is used to represent 'established' connections. In this case the server will not be able to establish outbound communication, rather it can only answer queries issued to it by remote clients. This type of policy would block some viruses such as 'Code Red' which was designed to pass through most firewalls. In this example FTP (passive mode) will be denied by the catch-all rule because it requires a connection back to the client that is dynamically negotiated and therefore cannot be pre-defined.

Securing servers without NAT (DMZ)

Securing Public Servers (DMZ):

Sometimes it is preferred to host servers on a public segment or De-Militarized Zone (DMZ) using packet filters to secure them. Most protocols (e.g. HTTP/POP3/TELNET/IMAP/SMTP) can be sufficiently secured using the packet filtering. FTP is an example of a protocol that cannot be sufficiently secured with packet filtering because it uses dynamic port addressing (passive mode). If you would like to host an FTP server behind WinRoute we recommend using NAT with port mapping for TCP port 21. WinRoute has a special module that allows FTP to function in both active and passive mode behind NAT.

In the following example we will assume that a predefined address group called DMZ LAN was defined with the IP subnet of the DMZ. The DMZ must be allowed to send and receive email using SMTP and will allow connections for HTTP and POP3. This will require four permit rules incoming to the Internet and DMZ interfaces to ensure that only the necessary services are allowed to and from the DMZ.



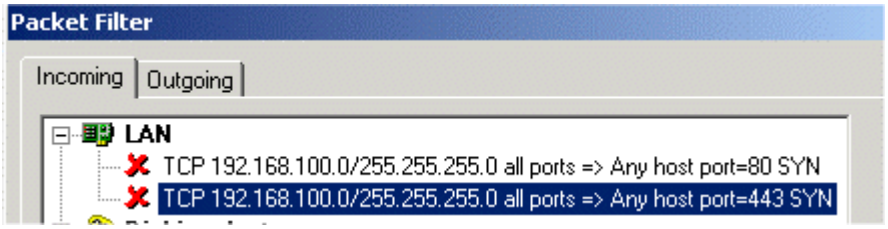
As based on the above screenshot, the first set of filters will allow email to be sent from the DMZ to other Internet mail servers. The next set of rules allows for the DMZ to receive emails from other Internet mail servers. The next two sets of rules allow for connections to HTTP and POP3 services hosted on the DMZ. The final rule of each Interface is the catch-all rule that denies any IP traffic that was not allowed by the above filters.

Usually in a DMZ scenario the WinRoute computer would have at least three interfaces: the Internet interface, the DMZ interface, and a LAN interface that services the private network. In the above scenario both inbound as well as outbound filters are specific to/from the address group 'DMZ' so it should not effect the private network. Note that you will need to configure advanced NAT rules to exclude the DMZ segment from NAT. For DMZ network configuration refer to the section 'Deployment Examples -> Connecting Multiple Networks -> Connecting Public and Private Segments (DMZ)'.

Forcing users to use the Proxy Server

With NAT enabled clients may access web pages without any configuration to their web browser. In some environments it may be more desireable to monitor and regulate the web sites visited by local users by pointing their web browsers to use WinRoute's built-in proxy component. To prevent users from re-configuring their browser you must prohibit access to http protocol through WinRoute's packet filter by applying the following rules.

Let's assume your LAN segment uses a 192.168.100.0/24 subnet. The following rule would be applied as incoming to the LAN interface.



For further configuration on restricting user access to web sites refer to the 'Proxy Server' section within this chapter.

Creating logs

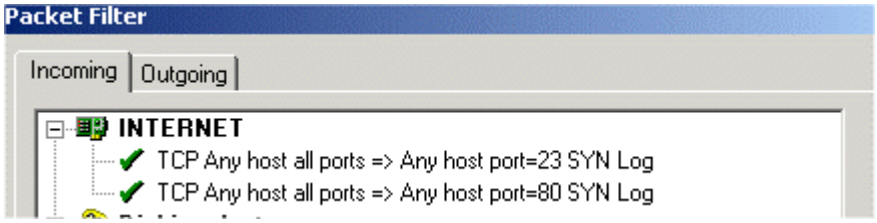
WinRoute can reject inbound packets either through NAT, or through Packet Filtering. It is important to note that WinRoute considers these as separate components. In other words, NAT may allow some traffic to pass through while a packet filter rule may deny the same packet. The reverse is true as well, a packet filter rule may allow some traffic while NAT will deny the same traffic.

➢ *Creating NAT log data*

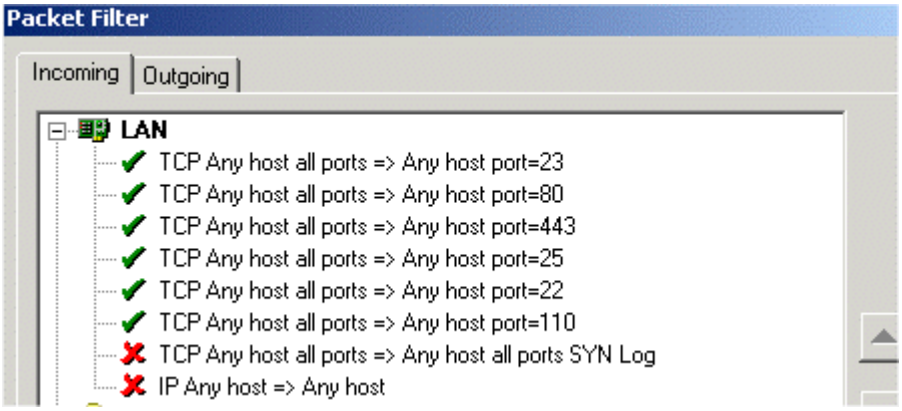
By default, neither the NAT nor Packet Filter facilities will log to the security log. To enable logging of traffic denied through NAT proceed to settings -> advanced -> security options from the winroute administration program. From this dialog "NAT Logging Options" you have the option to log inbound TCP or UDP packets with no entry in the NAT table. This information can be logged to the security log file and/or the security log window. For explanation of the log data refer to the next section 'Viewing logs'. For most users it is recommended to enable logging of only TCP packets with a syn flag. This will log any inbound connection attempt such as an external port probe. Logging all TCP packets will usually log packets that have timed out from the NAT table. Logging UDP can also create a large amount of extraneous log data, for example netbios broadcasts can produce several lines per minute.

➢ *Creating Packet Filter log data*

When creating packet filter rules you have the option to log into the security log file and/or the security log window. Any IP protocol has the ability to be logged. When creating logged filter rules it is necessary to log only relevant information. For example let's assume you have opened ports 23 and 80 through NAT using the port mapping feature. It may be beneficial to log the IP address of each connection to these services. In this example you would need to create two packet filter rules that allow inbound access to the NAT'd interface where the destination port is equal to 23 and 80 and the TCP flag is 'establishing'.



In some network configurations you may have a policy that allows the local network to have Internet access to specific protocols while all other IP traffic is denied by a catch-all rule at the bottom of the list. Depending on the allowances defined in the rules above the catch-all rule, it may not be beneficial to log the catch-all rule. As an alternative consider placing a TCP deny rule just above the catch-all rule that will log restricted connection attempts from the LAN to the Internet.



Viewing logs

All security related events are logged into the security log. The security log file is located in the WinRoute Pro/logs directory. The security log can also be accessed from the WinRoute administration program from view -> logs -> security log. Note that the security log window is limited to 500 lines of data. When the limit is reached old entries will be replaced by new entries. This log is also cleared each time the WinRoute engine/service is restarted.

The security log reports information generated by the following components: NAT module, individual packet filter rules, anti-spoofing rules, and administrative events. By default, WinRoute will only log administrative events. Logging of NAT events can be enabled through the WinRoute administration program in settings -> advanced -> security options and additionally from settings -> advanced -> NAT. Note that the advanced NAT logging should only be used for diagnostic purposes. Packet filters are created in settings -> advanced -> packet filter. For details regarding the concept and configuration of packet filters refer to the chapter **Setting up Packet Filters.** Anti-spoofing rules are defined in settings -> advanced anti-spoofing.

- ***Explanation of NAT Log events***

[21/May/2002 18:17:05] NAT: Attempt to establish TCP connection through NAT (in). The following line contains suspicious packet dump: [21/May/2002 18:17:05] NAT: + proto:TCP, len:62, ip+port:192.168.10.1:3051 -> 10.10.10.1:139, flags: SYN , seq:33710428 ack:0, win:65535, tcplen:0

The preceding log entry includes, from left to right, a time stamp, the module responsible for the log event (NAT), the protocol (TCP), the direction (in), the action taken (dump = drop or deny, refer to section **NAT Security Options** in this chapter), the source IP and port (192.168.10.1:3051), the destination IP and port (10.10.10.1:139), and the flag (SYN) if it is TCP protocol. The remaining data includes TCP specific information such as the sequence number, window size, and TCP length. In the advanced security options of the WinRoute administration you may choose to send a denying response or to silently discard the packet. In either event the log data would appear similar to the sample log data in the above example.

[23/May/2002 11:23:31] NAT advanced: ACL 0:0 LAN: do nat with 10.0.0.104 packet out UDP 10.0.0.103:1075 -> 10.0.0.1:1900

The preceding log event was generated by an advanced NAT rule. The access control list (ACL) is a specific reference maintained internally to WinRoute. (LAN) in this case refers to the name of the interface as indicated within the interface table. The remaining information indicates the translated source address followed by the original source and destination address.

- ***Explanation of Packet Filter log events***

[22/May/2002 17:32:27] Packet filter: ACL 1:1 INTERNET: deny packet in id=20122827 : TCP 67.114.19.218:64632 -> 24.219.8.236:113

[22/May/2002 17:31:30] Packet filter: ACL 1:0 INTERNET: permit packet in id=20122681 : TCP 67.114.19.218:64624 -> 24.219.8.236:25

The information displayed in these logs includes the time stamp, the Packet Filter rule access control list, the action taken (refer to section **Packet Filter Overview**), the packet id, the protocol, and the source and destination IP address. If the protocol is UDP or TCP the IP address will be followed by the port number. Note that the ACL references first the interface number followed by the rule number. These numbers are assigned and maintained internally to WinRoute.

- ***Explanation of Anti-spoofing log events***

[23/May/2002 11:04:23] Anti spoofing: LAN: mode net, drop packet TCP 64.12.25.64:5190 -> 10.0.0.103:1041

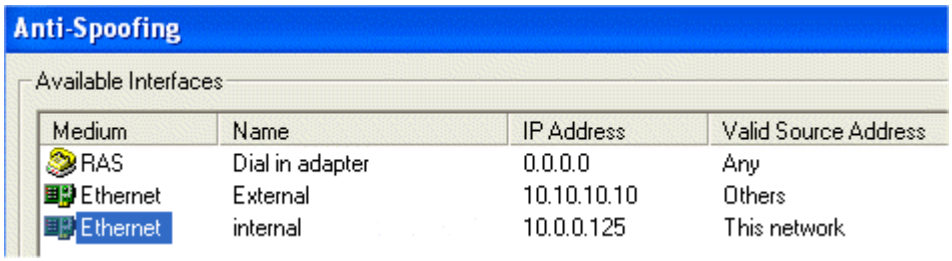
The preceding log event was generated by an anti-spoofing rule. Only rejected traffic will be logged. The only available action is to drop traffic rejected by the anti-spoofing rule. For explanation of this event refer to section **Packet Filter Overview**.

- ***Explanation of Administrative events***

WinRoute logs service startup and termination as well as each login to the administration (failed or successful). There is one additional log event (introduced in build 21) as follows: "Detected MS Outlook security vulnerability in packet". This event resolves a vulnerability in the date and time buffer in older builds of MS Outlook.

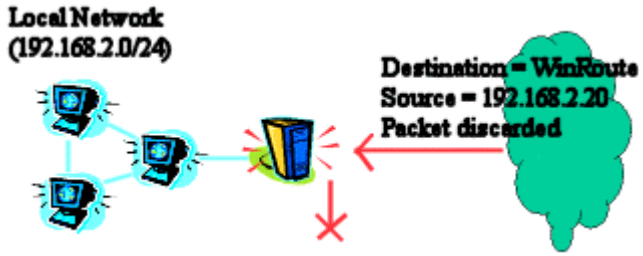
Anti-Spoofing Configuration

IP address spoofing involves the falsification of a source IP address in order to transmit packets through a firewall or to confuse a server into responding back to the incorrect address. If NAT is used, Anti-Spoofing is not entirely necessary unless you've configured port mappings. WinRoute can be configured to prevent IP address spoofing through the administration program, settings -> advanced -> anti-spoofing.



The example above demonstrates a normal anti-spoofing configuration. For the interface connected to the local area network WinRoute should only allow communication from workstations in the same IP subnet as the internal interface. This policy is only necessary in cascaded network segments, where additional network segments exist behind an internal interface, and these additional network segments should not have the ability to route through WinRoute. The option 'This network (from the network connected to this interface), should be enabled only on the internal interface. The option 'or additionally from' allows you to define an address group that is allowed to route through WinRoute. For details on address group configuration refer to chapter 'Address groups'.

The external interface should never receive packets from the Internet with a source address that belongs to a workstation connected to the internal side of WinRoute. Such an event would cause a local workstation to reply to another workstation within the LAN. If large amounts of these non-routable packets are allowed into the network it can cause problems, especially if all of the spoofed packets are directed to a single server inside the LAN.



To prevent spoofing from the Internet you must choose the option 'Others (only those that are not permitted on other interfaces), from the settings dialog of the interface connected to the Internet.

Address groups

Address group overview

An address group is a way of defining IP addresses that can be referenced by other components of WinRoute. The purpose of address groups is to simplify administration. If an address group is not referenced by another WinRoute component then it will be an idle setting. WinRoute does not include any default address groups, they must be defined by the administrator.

Creating address groups

Address groups can be created from the WinRoute Administration in Settings -> Advanced -> Address Groups. WinRoute allows address groups to be defined as hosts, network ranges or a network/mask. A host is defined as a single IP address such as 192.168.2.2, a range is a contiguous group of IP addresses such as 192.168.2.111-192.168.3.54 and a network/mask is the network number followed by the mask such as 192.168.4.32 255.255.255.224. If you are unfamiliar with IP subnetting you can use IP ranges which provide the same level of flexibility. It is important to note that WinRoute allows you to create multiple IP groups within a single address group. When you select 'add' the address group name appears as a drop down menu. The last created address group will appear in the drop down menu, meaning that when you apply the new host/range/network entry it will be added to the group displayed in the drop down menu. If you would like to create a new group simply rename the value in the drop down menu to the desired address group name.

Uses of address groups

The following WinRoute components may reference address groups:

Port Mappings: "Allow access only from". If this box is checked, and you have pre-defined at least one address group you may reference that group from this dialog. Port Mappings allow a permanent entry to NAT so that all inbound connections to the specified port/ports will be redirected to some internal server. "Allow access only from" will restrict access to the opened port so that only the IP addresses defined in the address group may have access to the opened port. All other connection attempts will be either dropped or denied, as specified from the advanced -> security options.

Advanced NAT: This feature is a way to make exceptions to NAT. When you apply NAT to an interface from the settings -> interface table WinRoute will translate the source address of all IP packets leaving the specified interface to the IP address displayed in the interface table. If you have multiple IP addresses assigned to the NAT'ed interface, and you would like to use one of the other IP addresses for specific traffic you can create a rule where either the source and or destination is a pre-defined address group that you may choose not to perform NAT or to perform NAT with a specified IP address.

Anti-Spoofing: This feature is a compliment to packet filtering. It specifies, based on the source IP address (e.g. a pre-defined address group), what traffic is permitted through an interface.

Packet Filters: This component is the heart of WinRoute's firewall because it is a way for an administrator to define what IP traffic may pass in and out of the network. Depending on the number of rules, it may be practical to pre-define address groups that include some of the following examples: The local area network, remote offices, individual hosts, clusters of servers, clusters of administrators, clusters of end users. Any rule can reference these pre-defined groups as either the source or destination.

Mail Server: If you have enabled WinRoute's mail server and you have opened port 25 to allow for inbound reception of email it is recommended that you create an address group for the local area network. In the anti-spam tab of WinRoute's mail server you would choose to allow the address group to relay mail to any domain. This way users in the address group do not need to authenticate when sending outbound mail through WinRoute.

CHAPTER 3

DEPLOYMENT EXAMPLES

In This Chapter

IPSEC, NOVELL and PPTP VPN solutions

IPSEC VPN

WinRoute Pro 4.1 supports IPSEC in so called "**Tunnel mode**". The "**Tunnel mode**" should support any IPSEC client that will allow for the transport IP address to be changed.

Note about IPsec: Some IPsec clients have a specific policy to close all IP traffic except that which is carried over the tunnel. For obvious reasons, IPsec clients of this nature must be run on a computer other than WinRoute.

In WinRoute Pro 4.2.4 and later the following settings are not necessary. The forwarding of protocol 50 (ESP) is automatically handled by WinRoute during the IKE negotiation.

WinRoute settings:

Create mapped port for ESP:

Protocol: Other 50

Listen IP: <unspecified>

Destination IP: the private IP address of the client PC

We also suggest creating a mapped port for IKE. This is not necessary in cases where the communication is initiated FROM behind WinRoute to the Internet, however certain implementations of IPSEC may require this setting:

IKE port mapping:

Protocol: UDP

Listen IP: <Unspecified>

Listen port: 500

Destination IP: the private IP address of the client PC

Destination port: 500

Some IPsec clients may also use the General Routing and Encapsulation protocol (GRE)

GRE port mapping:

Protocol: Other 47

Listen IP: <unspecified>

Destination IP: the private IP address of the client PC

General information about IPSEC

IPSec is a security encryption protocol used for secure communication between two computers.

IPSec uses either AH (Authentication Header) or ESP (Encapsulating Security Payload). AH verifies the identity of the sender and the content of the packet only. Data is not encrypted.

ESP encrypts the data. ESP allows for the use of a so-called "Tunnel Mode" that is similar to the PPTP protocol. The packet then includes the IP header (necessary for transport) that is not encrypted and the data portion that includes the whole encrypted original packet.

The protocol IKE (sometimes called ISAKMP) is used for authentication (exchange of security keys). IKE runs on protocol UDP port 500. This port is used as source and destination.

AH uses protocol 51, ESP uses protocol 50. IPSec may further communicate with the entire certification authority using other protocols that do not interfere with NAT.

Novell Border Manager VPN

Using WinRoute Pro with Novell BorderManager VPN (IPSEC)

This document describes the setup that makes it possible to connect a local network that uses NAT to share a single IP address provided by ISP to a remote network that uses Novell BorderManager Enterprise Server for VPN connectivity.

According to the README.TXT file supplied on the installation diskette of the Novell BorderManager VPN Client,

"You cannot use NAT in the path between a VPN client and a VPN server. This is because when the IP and IPX packets are encapsulated and encrypted at the VPN client, the source IP address that is used for the encapsulation is the address of the VPN client. The IPSEC Authentication Header calculation of the packet is based on this address and the address of the destination VPN server. Therefore, if either address (the VPN client or the VPN server) is modified by NAT, the calculation will fail when it gets to the destination VPN server and the packet will be discarded. Most likely, however, NAT will drop the IPSEC packets because it only handles TCP, UDP, and Internet Control Message Protocol (ICMP) packets.

When you have workstations in an intranet that must communicate securely with networks protected by a VPN server across the Internet, we suggest you use the Novell BorderManager Enterprise Edition site-to-site VPN feature (instead of the client-to-site VPN)."

However, the Novell BorderManager Enterprise Server is very expensive for the home user. Additionally, it requires extensive setup of the static routes on the remote network that is being accessed. The solution suggested above by Novell is therefore not feasible for the person who would like to connect his local network that uses NAT to a remote network via Novell BorderManager VPN.

Amazingly, it is possible to connect the local network that uses NAT to a remote network using WinRoute Pro and Novell BorderManager VPN Client. This configuration allows any computer on the local network to access the resources on the remote network when the VPN tunnel has been established on the router computer. No remote network configuration is required.

Below are the configuration steps for the local network.

Step 1: Install and configure Novell BorderManager VPN Client software on the computer that is going to be used as a router. Ensure that a VPN connection to the remote network can be successfully established and the resources on the remote network can be accessed.

Step 2: Install WinRoute Pro on the router computer. Follow the instructions found in the Administrator's Guide for configuring the WinRoute Pro and configuring the computers on the local network to work with WinRoute Pro. Use the regular configuration for single IP address sharing. Ensure that the resources on the Internet can be accessed from any computer on the local network.

Step 3: When you need to access the resources on the remote network, run the Novell BorderManager VPN client on the router computer and login to the remote network.

This is made possible by the architecture of WinRoute Pro. Because it works on the IPSEC level, address translation occurs before the packet is routed to the virtual network adapter. Therefore the packets sent to the VPN server have the real source IP address. On the way back the packets received from virtual network adapter pass through the address translation layer and are routed to the correct computer on the local network.

The limitations of this setup are that the VPN login must be performed manually on the router computer and that the VPN connection will time out after a certain period of inactivity that is set on the VPN server. Also, the IPX packets aren't going to be routed even if the VPN tunnel has IPX protocol enabled. Therefore, the IPX tunneling will be available only on the router computer.

Overall, this setup provides cost-effective and convenient way to connect a local network that uses NAT to a remote network using Novell BorderManager VPN.

Running PPTP server behind NAT

In order to run a PPTP server on the Network behind WinRoute (including the computer where WinRoute is running) you have to set up two Port Mappings.

Additionally, you must **DISABLE NAT** from the interface table for the **RAS** interface handling the VPN connection. This applies to both Dial-In and Dial-out connections and only if the WinRoute computer is hosting the PPTP server/client.

If the PPTP server resides on a computer other than WinRoute you need to add a persistent route on the WinRoute computer so that all IP traffic intended for the VPN will be forwarded to the PPTP server for encapsulation. Example, WinRoute is located at 192.168.1.1, the PPTP server is 192.168.1.2, and the remote network is a range from 10.10.10.1-10.10.10.254. The route would look as follows: "route add -p 10.10.10.0 mask 255.255.255.0 192.168.1.2".

Important: If the VPN server is located on the WinRoute host machine, you must map the destination IP to the **public address***, not the private. The listen IP should remain unspecified, or you may use the public address specified as the destination.*

For the control connection:

- Protocol: TCP
- Listen IP:
- Listen Port: 1723
- Destination IP: IP address of your PPTP server (e.g.192.168.1.2)
- Destination Port: 1723

For the GRE (PPTP) packets:

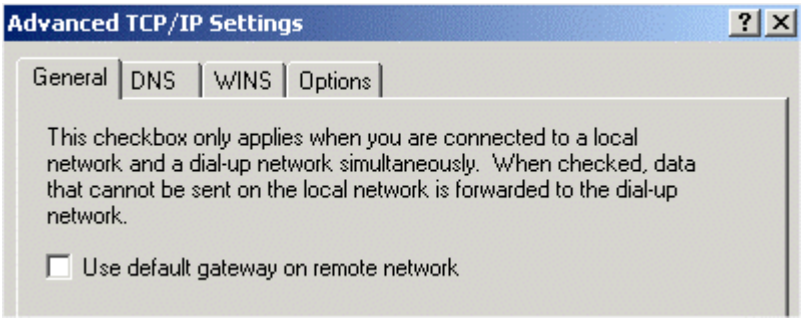
- Protocol: PPTP
- Listen IP:
- Destination IP: IP address of your PPTP server (e.g.192.168.1.2)

After setting up Port Mapping as shown above you will be able to place your PPTP server anywhere behind WinRoute INCLUDING the computer WITH WinRoute. The users will access your PPTP server by "dialing-in" to the external (public) IP address of your network. When the packets reach WinRoute's computer they will automatically be forwarded to the proper computer behind the firewall.

Running PPTP clients behind NAT

There are no settings required to run PPTP clients behind WinRoute (NAT) accessing the PPTP server outside on the Internet.

If the VPN connection is placed on the WinRoute computer you must make sure that the Interface Table shows a new RAS interface. Make sure that in the properties of the RAS interface you have selected the proper connection and supplied a user name and password. You must also disable NAT for this interface. This will allow all clients behind winroute to access the VPN tunnel. Also consider that the Microsoft VPN adapter, by default, will change the default gateway for the machine on which it is installed, to that of the remote VPN gateway. It is recommended that this option be disabled. It is called 'use default gateway on remote network' and is found in the advanced TCP/IP properties of the VPN dial-out connection. Note that this is a setting in Microsoft networking properties, not WinRoute.



WWW, FTP, DNS and Telnet servers behind WinRoute

Running WWW server behind NAT

To run the web server behind NAT:

1. Go to menu *Settings ->Advanced ->Port Mapping*
2. Add new Port mapping:

   Protocol: TCP

   Listen IP: unspecified or IP address associated with the domain. Such an IP address must be associated with the Interface

   Listen Port: 80

   Destination IP: enter the IP address of the WEB server (e.g.192.168.1.10)

   Destination Port: 80

The users accessing these services will access them using either domain name or public IP address of your network. After the packets reach WinRoute they are automatically diverted to the internal computer with the appropriate internal IP address.

Running DNS server behind NAT

Running the DNS Server behind NAT (WinRoute)

In order to run the DNS server behind NAT/WinRoute you have to set Port Mapping as described below. The DNS servers communicate with each other through the **UDP** protocol on **port 53**.

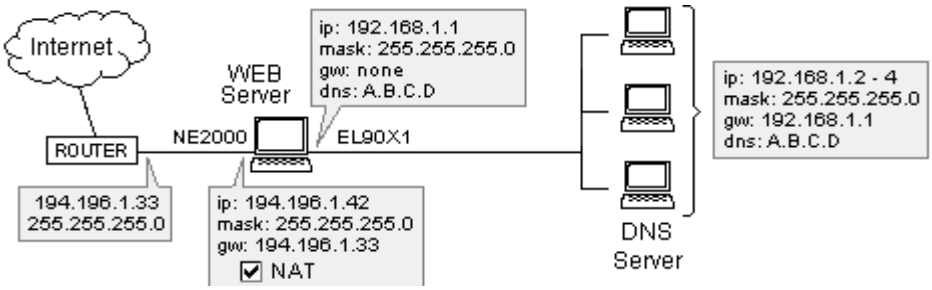
Protocol: UDP

Listen IP: unspecified or public IP address of DNS server you want to operate

Listen port: 53

Destination IP: public or private IP address of domain name server

Destination port: 53



Running FTP server behind NAT

To run a FTP server behind NAT:

1. Go to menu *Settings ->Advanced ->Port Mapping*
2. Add new **Port mapping**:

Protocol: TCP

Listen IP: unspecified or IP address associated with the domain. Such IP address must be associated with the Internet Interface

Listen Port: 21

Destination IP: enter the IP address of the internal FTP server (e.g.192.168.1.10)

Destination Port: 21

Note: Clients in passive mode will try to open a new connection on port 20. WinRoute will dynamically allocate this port so there is no need to create an additional port mapping.

Running Mail server behind NAT

In order to run a Mail Server behind WinRoute it is necessary that you create at least two Port Mapping entries - one for the SMTP protocol (which runs on port 25) and one for the POP3 protocol (which runs on port 110). This will allow other SMTP servers to reach your SMTP server and also you will be able to pick up your email by POP3 from the Internet. Some mail servers may use additional ports for web mail or IMAP, in which case you will need to make additional port mappings for those protocols.

SMTP protocol:

Protocol: TCP

Listen IP:

Listen Port: 25

Destination IP: enter the IP address of the SMTP Mail server (e.g.192.168.1.10)

Destination Port: 25

POP3 protocol:

Protocol: TCP

Listen IP:

Listen Port: 110

Destination IP: enter the IP address of the POP3 Mail server (e.g.192.168.1.10)

Destination Port: 110

Running Telnet server behind NAT

Telnet is widely used by many companies to operate data remotely. Especially AS400 servers that use this protocol.

To run a Telnet server from behind WinRoute it is necessary to set up a Port Mapping for TCP protocol on port 23. There are no settings required for running a Telnet client accessing a Telnet server on the Internet.

Protocol: TCP

Listen IP: unspecified, or any public address that may be assigned to the public interface

Listen Port: 23

Destination IP: enter the IP address of the Telnet server (e.g.192.168.1.10)

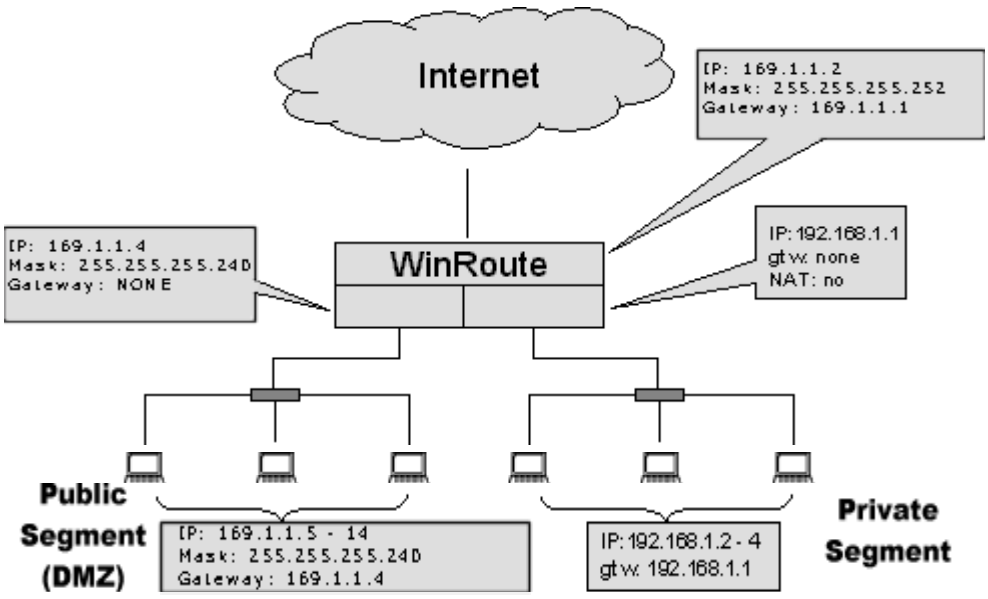
Destination Port: 23

Connecting multiple networks

Connecting Public and Private Segments (DMZ)

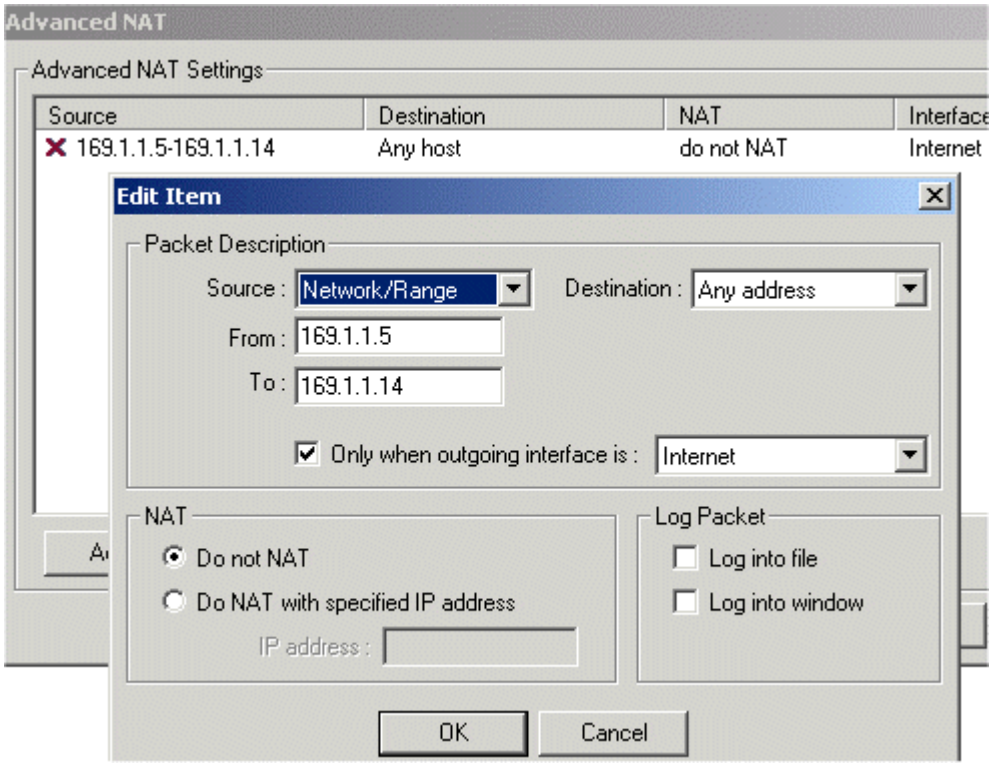
The following example takes a commonly issued block of 14 IP addresses and breaks it into two subnets. This type of configuration is quite advanced and requires prior knowledge of IP subnetting. As an alternative one may consider assigning additional IP addresses to the Internet interface and have WinRoute perform port mapping by listening on specified IP addresses.

Public and Private networks scenario:



WinRoute settings:

It is necessary to perform advanced NAT settings so WinRoute will not perform NAT for packets going to and from the public segment. To do this go to menu Settings=>Advanced=>NAT.



In the advanced NAT settings you will specify that any traffic leaving the NAT'd interface that has a source IP address of the DMZ segment must not be NAT'd. At that point WinRoute becomes a neutral router for the DMZ segment, as incoming traffic to an IP address in the DMZ will pass through NAT. Under this scenario you may consider packet filters to firewall the DMZ.

The final step in the DMZ configuration requires the addition of static routes to WinRoute's default gateway. Most ISPs will require you to contact them to have such routes added. In the example above the router at 169.1.1.1 will have a mask of 255.255.255.240. It will therefore have a route statement indicating that for the destination network 169.1.1.0/28 to use the interface at 169.1.1.1. By inserting the WinRoute PC between the DMZ and the Internet gateway (your ISP's router) it is necessary to add static routes to the Internet router/gateway indicating that for each IP host on the DMZ it must use the WinRoute computer (e.g. 169.1.1.4) as the gateway. An example route would look as follows: network 169.1.1.5 mask 255.255.255.255 gateway 169.1.1.4 interface 169.1.1.1.

If you have additional questions regarding this type of scenario please email your network diagram to support@kerio.com.

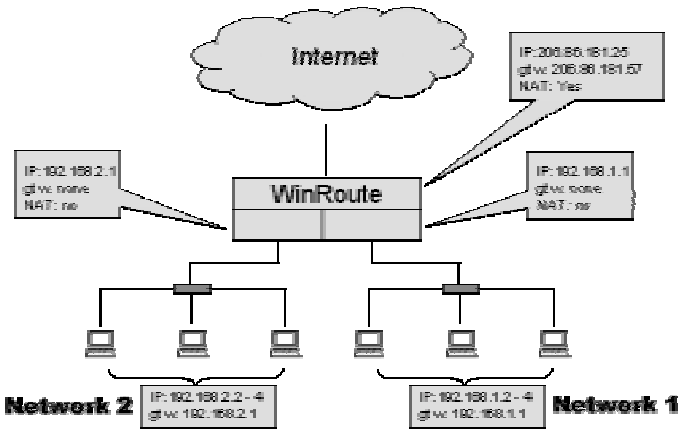
- ***Important: Do not include any IP address of the WinRoute computer within the DMZ when defining your advanced NAT rule. In the above screen shot notice the first IP of the range does not include 169.1.1.4!***

Sharing the Connection for Two Networks with 1 IP Address

In case you have two networks connected to the Internet via one computer running WinRoute, there are no specific settings. Basically there are several segments leading to the WinRoute computer, each has a separate network interface. In our example there are three network interfaces in the WinRoute computer:

- Internet interface
- Network 1 interface

- Network 2 interface



The only necessary settings to keep in mind are:

Internet interface

NAT is enabled
IP address is set according to your ISP
Gateway is set according your ISP

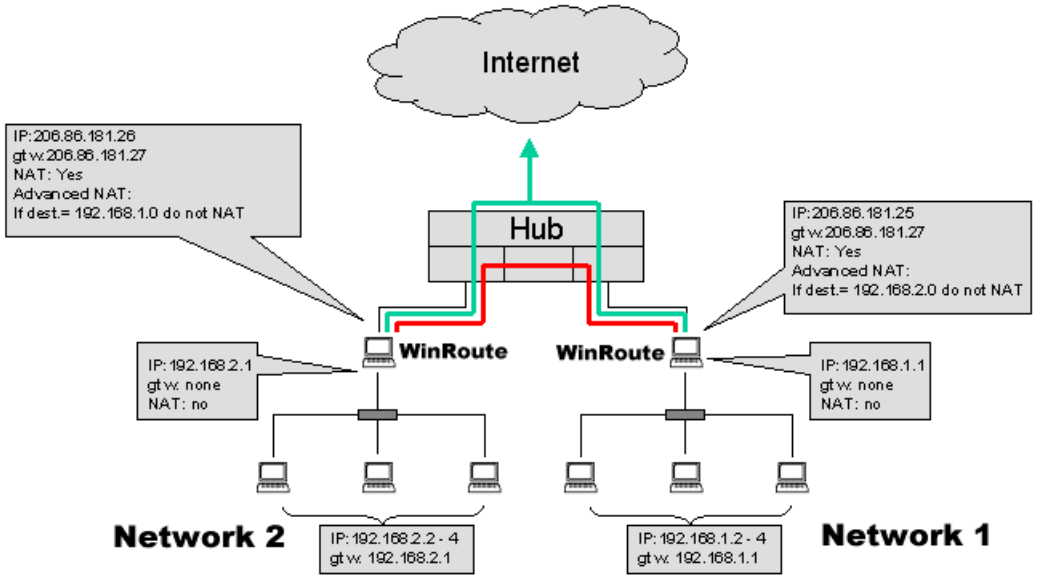
Internal interfaces

NAT is NOT enabled
There is NO default gateway set on both interfaces
IP address is set to the internal type (e.g.192.168.1.1)

Other settings are the same as described in other sections of this manual. The traffic arriving from each subnet is routed to the other subnet or to the Internet and vice versa.

Sharing the Connection for Two Networks with 2 IP addresses

You may want to share one Internet access between two networks when each network is behind separate public IP address. At the same time you may want to access the computers in both private networks.

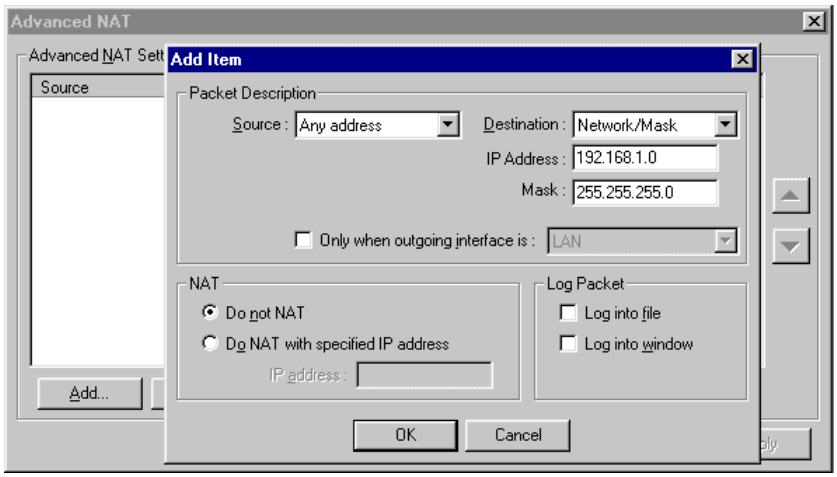


By enabling NAT on the public/external interface, WinRoute will perform NAT on ALL IP traffic leaving that interface. By adding an advanced NAT rule you will specify that if the destination is the opposing network, NAT will not be performed.

To set WinRoute to not perform NAT based on the destination of the packet:

- Go to menu Settings->Advanced->NAT.
- Enter the destination criteria of the opposing network - usually the subnet or range of IP addresses.

- Select the "Do not NAT" option.
- You may want to add an additional advanced NAT rule for the host IP address of the opposing winroute computer.
- These advanced NAT rules should be applied to both WinRoute computers.



Adding Routes

In order for this scenario to work it is necessary to add a persistent route to each winroute computer. Without the route in place, if a node from network 1 wishes to contact a node from network 2 the packet will be sent to the default gateway of the winroute computer on network 1. This packet must rather be forwarded to the opposing WinRoute computer. Based on the example above you would add the following route to the winroute computer of network 1: route add -p 192.168.2.0 mask 255.255.255.0 206.86.181.26. On the WinRoute computer of network 2 the route would look like this: route add -p 192.168.1.0 mask 255.255.255.0 206.86.181.25.

Remote Access Server (dial-in and access the Internet)

Remote Access Server solution

At times it may be necessary to access your corporate network from the outside world via telephone and use that Internet access. WinRoute provides this functionality on WindowsNT with RAS services installed and configured.

There are specific rules that need to be applied:

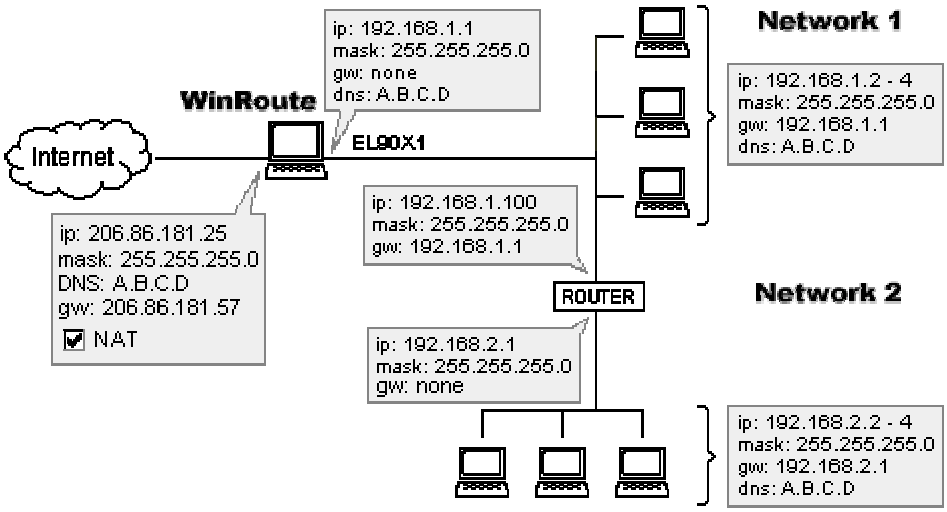
- Your corporate network has one subnet (e.g. 192.168.1.0)
- WindowsNT DHCP server is giving users coming through RAS IP addresses from a different subnet (e.g. 192.168.2.0)
- NAT will be performed only on the Interface leading to the Internet

In another words, the network card (NIC) leading to your local network must have the IP address from one subnet (e.g. 192.168.1.1) while the user connecting to your server via RAS must get an IP address from a different network (e.g. 192.168.2.1). WinRoute acts as the router - it can route the packets between two or more interfaces from different networks - not from the same one.

This type of setup mirrors that of a small ISP. WinRoute does not limit the number of users accessing your NT server simultaneously. Note that each RAS user, if accessing the Internet through WinRoute, is being NAT'd and therefore counts as a WinRoute user.

Connecting Cascaded Segments via 1 IP Address

WinRoute can be installed on a network that is segmented into different subnets by an additional router behind WinRoute. This is called cascading. In this type of scenario there would be at least one network segment that is in a different subnet than WinRoute, 192.168.2.2/24 in the example below. This means that the WinRoute computer is not aware to the presence of the second network. To understand what that means in terms of communication between the two networks we must consult the routing table, as WinRoute relies on this information for its routing decisions. In simple terms, the routing table, as based on the example below, would state that any traffic that is intended for 192.168.1.2-192.168.1.254 must go out the interface with 192.168.1.1. Traffic with a destination of 206.86.181.1-206.86.181.254 will be sent out the interface with 206.86.181.25. All other traffic will be sent directly to 206.86.181.57 out the interface 206.86.181.25. This means that traffic with destination 192.168.2.1-192.168.2.254 will be sent out the interface with 206.86.181.25, which is not the desired effect. Therefore, the WinRoute computer must be informed that traffic intended for 192.168.2.1-192.168.2.254 needs to go out the interface 192.168.1.1 and go to the router/gateway at address 192.168.1.100, as this is the device that communicates with the 192.168.2.x subnet. This is accomplished by adding a persistent route from the command prompt that will appear, for our example, as follows "route add -p 192.168.2.0 mask 255.255.255.0 192.168.1.100". Note that for Windows 9x systems you cannot make routes persistent, so the route will not remain after a reboot.


Network 1
ip: 192.168.1.1
mask: 255.255.255.0
gw: none
dns: A.B.C.D
WinRoute
EL90X1
Internet
ip: 192.168.1.2 - 4
mask: 255.255.255.0
gw: 192.168.1.1
dns: A.B.C.D
ip: 192.168.1.100
mask: 255.255.255.0
gw: 192.168.1.1
ip: 206.86.181.25
mask: 255.255.255.0
DNS: A.B.C.D
gw: 206.86.181.57
NAT
ROUTER
Network 2
ip: 192.168.2.1
mask: 255.255.255.0
gw: none
ip: 192.168.2.2 - 4
mask: 255.255.255.0
gw: 192.168.2.1
dns: A.B.C.D

Token Ring networks

Connecting Token Ring networks

On the WinRoute computer go to menu Settings->Advanced->Misc.Options and check on 'Support for Token Ring networks'. Because Token Ring uses frames that are larger than ethernet you may need to enable an option of WinRoute located only in the registry.

Stop the WinRoute engine.

Open up the registry editor. In Windows click on the Start button go to “Run” type in “regedit” click OK

Expand “HKEY Local Machine / Software / kerio / Winroute”

Change the value of the IpFragMode key to “1”

Close the registry editor and restart WinRoute

If this does not work you will need to lower the MTU on each Token Ring enabled PC to 1500.

Multiport Ethernet Adapters

Of the 170,000+ networks currently relying on WinRoute Pro as their router/firewall solution, the most common configuration involves two Network Interface Cards (NICs), one to the Internet and the other to a Local Area Network (LAN). This basic configuration filters packets going to and from the Internet; however, it cannot filter packets traveling between local segments because they do not pass traffic through WinRoute. An example of this configuration is illustrated below in Figure 1.

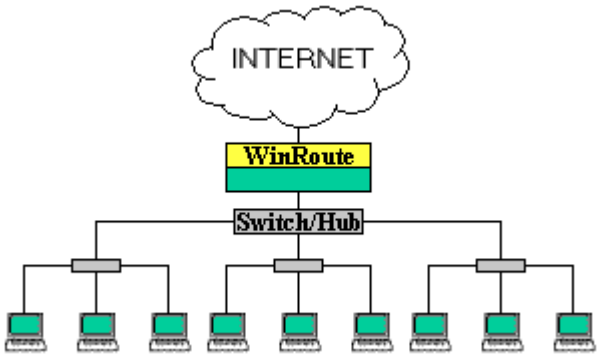


Figure 1. The most common configuration of WinRoute Pro.

In some cases, a third NIC will be added to the WinRoute machine allowing for a separate, secured segment. In such a scenario packets going to and from the secured segment from both the Internet and other local segments are filtered through WinRoute, providing an extra level of security.

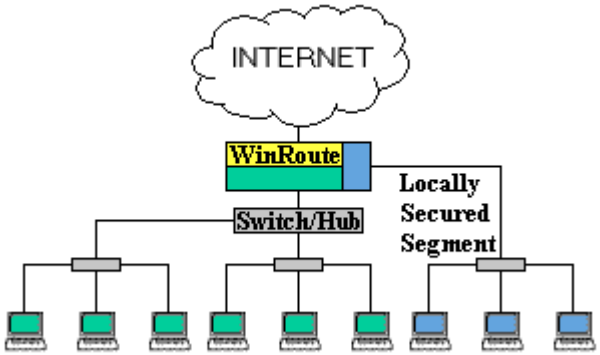


Figure 2. A separate segment to the LAN can be added using a third NIC.

For larger networks, that may have several separated segments with their own unique security policies, the problem arises that the number of these separated segments is limited to the number of ports on the WinRoute machine. Because of this, additional hardware is required to appropriate further routing/switching and security policies. With the recent introduction of multi-port Ethernet NICs provides the opportunity for WinRoute to be the singular controller of network traffic. Because multi port cards can allow the WinRoute machine upwards of 24 ports, depending on the number of card slots on the motherboard, the WinRoute machine can also be the server, router, domain controller, etc. This way network management can be centralized and controlled through a single point. Figure 3 illustrates WinRoute Pro using a multi-port Ethernet NIC to control three separate networks.

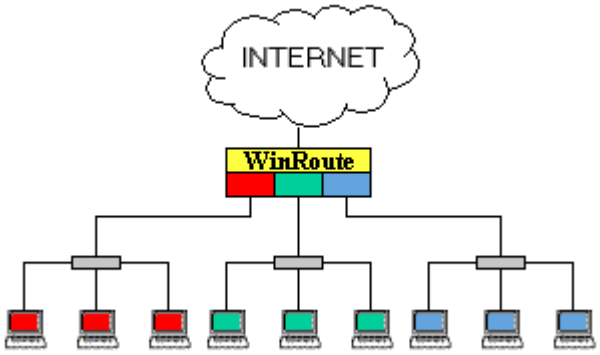


Figure 3. WinRoute Pro equipped with a multi-port Ethernet NIC.

In addition to enhanced security and centralized management provided by multi-port Ethernet NICs, additional benefits include load balancing and fail-over protection. Note the assignment of three ports to the middle segment in Figure 4.

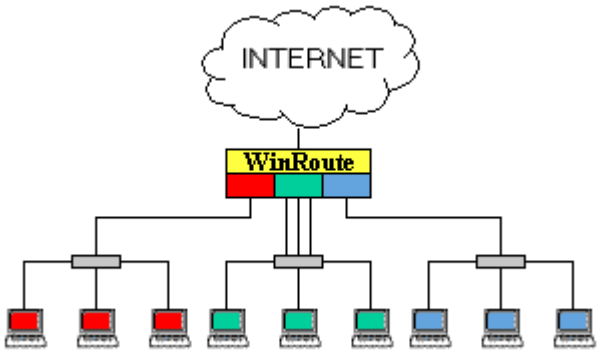


Figure 4. Middle segment is assigned three ports for port aggregation.

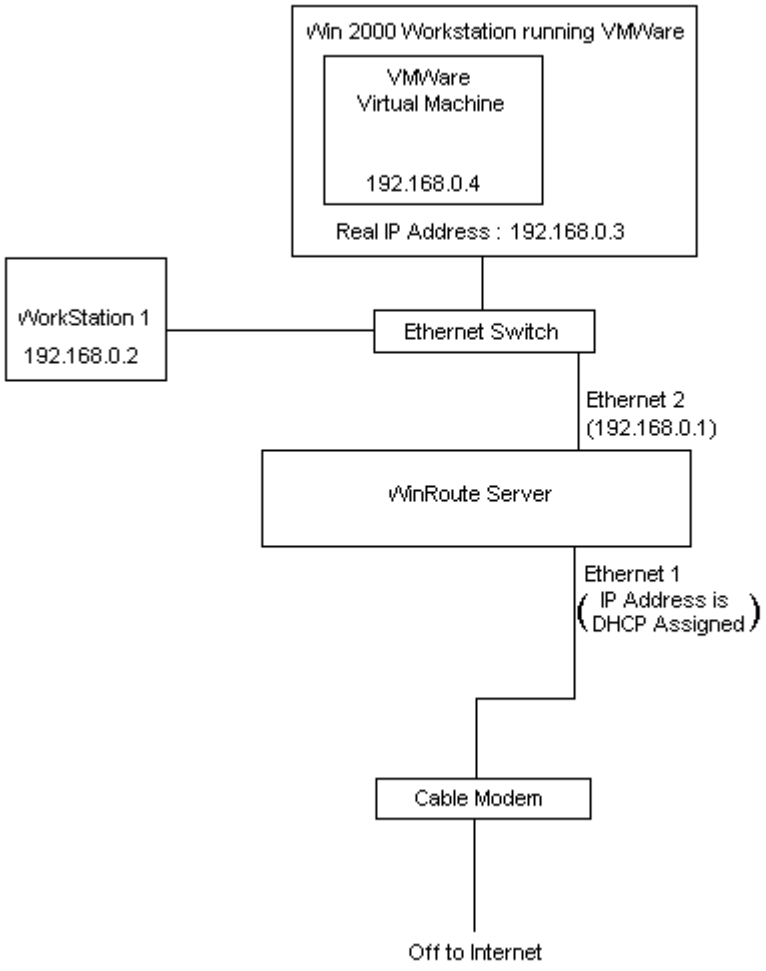
Load balancing can be accomplished by aggregating ports. For example, in the picture above the middle network segment is assigned three ports. If this segment uses a switch to connect to the WinRoute machine, all three computers can retrieve data each at 100 Mbps. The other two segments can only retrieve a combined total of 100Mbps each because only one port from that segment is attached to the WinRoute machine. A bonus functionality of port aggregation is the protection against port failure. If a line becomes disconnected, traffic will then be rerouted through the next available port.

Using multi-port NICs with WinRoute can provide an effective, yet very efficient, multi-routing system at a much more affordable price all under on single administrative umbrella. WinRoute has currently been tested successfully with the **D-Link 4 port DFE 570 TX** and the **Adaptec 2 port Duralan ANA-62022**. No other cards have been tested.

It should be noted that this type of network design requires different subnets for each network segment attached to the WinRoute machine.

VMWare

VMWare is an application that can emulate the PC that it is installed on down to the hardware level. To the network, this virtual computer is seen as a completely separate entity. Since the virtual computer has its own network properties, WinRoute will count the virtual machine as an additional computer.



CHAPTER 4

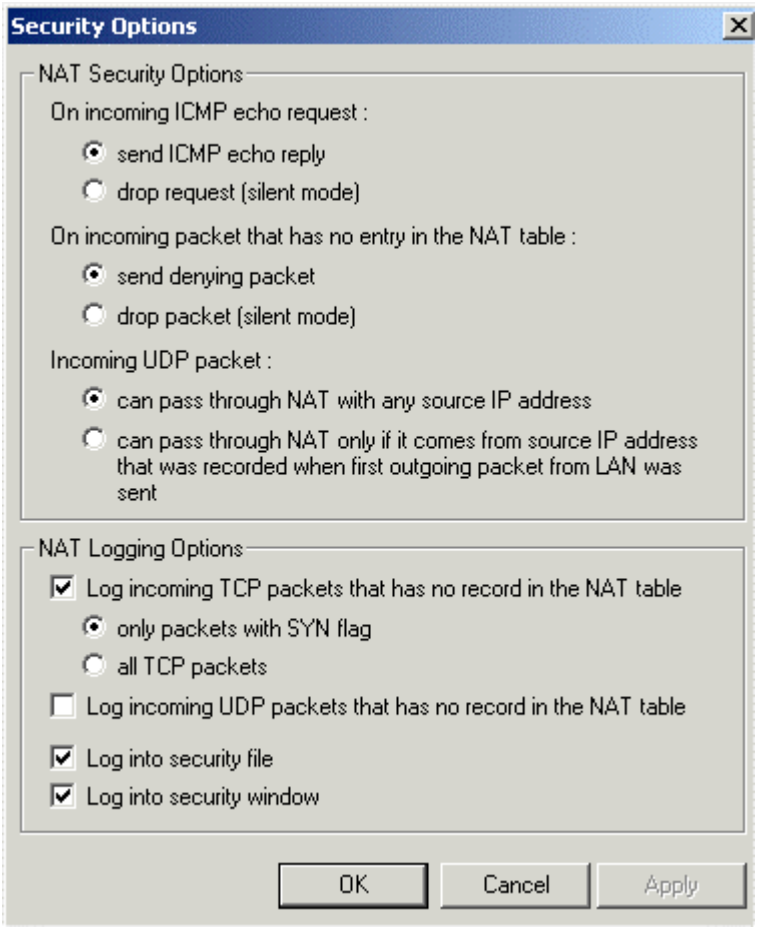
PORT MAPPING EXAMPLES

In This Chapter

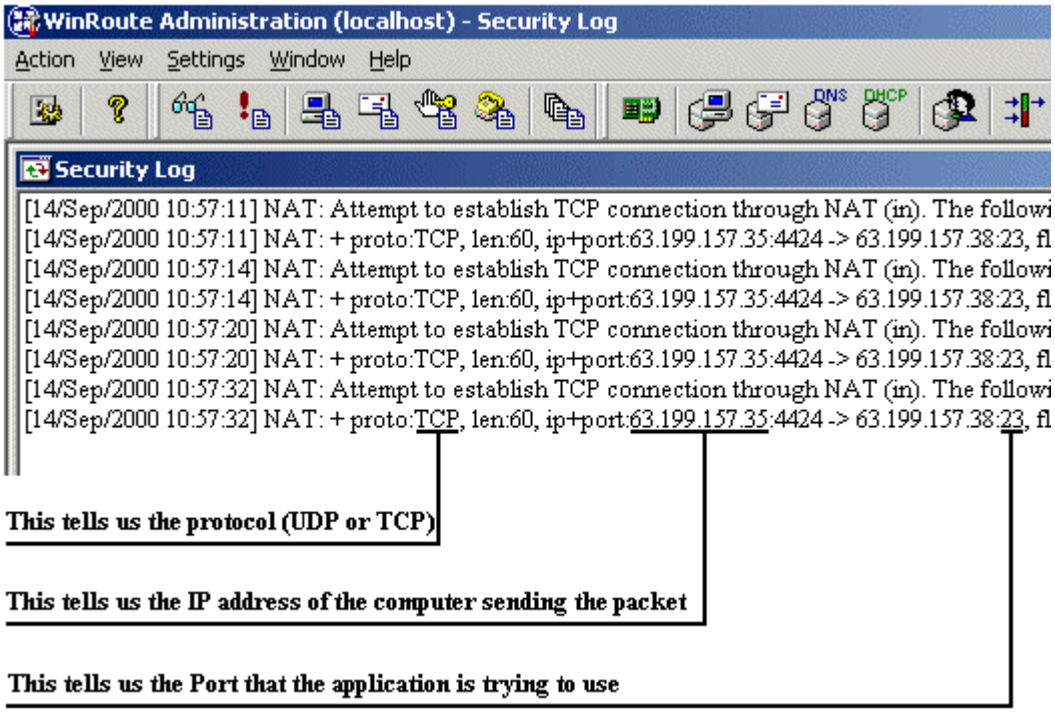
Find the correct port allocation

➢ ***If you have build 19 or higher>***

In the Administration window select Settings-> Advanced-> Security Options



At the bottom of the security options window are a few logging options. Enable logging of TCP packets with a SYN flag to the security window. This will log all connection attempts that WinRoute will drop. The next step is to open the security log from the view-> logs menu.



In this case, a computer at 63.199.157.35 sends out a packet from port 4424 to a computer at 63.199.157.38 to port 23. Port 23 is the standard port for telnet. If you had a telnet server running on some private address such as 192.168.1.3 it would be listening on port 23. Therefore you would map TCP packets on port 23 to 192.168.1.3.

Messaging and Telephony Services

There are currently several Instant messaging services that support file transfer as well as pc to pc or pc to phone chat. WinRoute Pro has been tested successfully with the following configurations of **AOL's instant messenger**, **Yahoo instant messenger**, **MSN Messenger**, and **ICQ**.

AIM does not require any specific settings. Use the default connection settings and make sure that you do not specify that you are using a proxy server.

Yahoo IM users must change the login preferences -> connection to "No network detection". All Yahoo IM services should work properly behind NAT with this setting.

MSN Messenger works best using HTTP proxy. Enable WinRoute's proxy on the default port 3128 (In addition to Network Address Translation). The voice features do not work behind NAT.

ICQ works in most cases with the default settings of the **latest** version. If you have complications using file transfer we recommend using HTTPS proxy found in the preferences -> connections -> server and firewall. Enable WinRoute's proxy on the default port 3128 (In addition to Network Address Translation).

Note: You should not need to map any ports for any of these applications.

H.323 - NetMeeting 3.0

WinRoute includes support of H.323 protocol. This means that all voice-over-ip applications may communicate through WinRoute. Such applications are Microsoft NetMeeting, CuSeeMee, internet telephony (you may run Siemens IP phone through WinRoute for example) and others.

If the communication is initiated from behind WinRoute

In such a case there are no settings required. Winroute will support virtually unlimited simultaneous connections.

If the communication is established from the Internet to a PC behind WinRoute

In such a case it is necessary to create a Port Mapping to tell Winroute where to route incoming H.323 packets. You must to set up following Port Mapping:

Protocol:	TCP
Listen IP:	Unspecified of the IP address used for H.323 communication in case of multihome system
Listen Port:	1720
Destination IP:	The LAN IP address of the H.323 application
Destination Port:	1720

H.323 protocol is not running on port 1720 only - WInRoute will add the other connections automatically. Because of H.323 protocol limitations, only one workstation may communicate at a time.

IRC - Internet Relay Chat

There are no special settings required to run an IRC client . Even DCC (Direct Chat/Send(Receive) Files) will work automatically if you use the standard port 6667.

To run the IRC **server** behind NAT please map the following ports:

Protocol: TCP

Listen IP: unspecified or IP you want to use for IRC server

Listen Port: 6667

Destination IP: IP address of PC with your IRC server

Destination Port: 6667

Using anything other than the standard port will cause DCC to not work.

CITRIX Metaframe

WinRoute fully supports **CITRIX Metaframe** protocol. To access CITRIX Metaframe server running inside of the WinRoute network from the Internet you will have to perform the following Port Mapping:

For CITRIX Metaframe:

Protocol: TCP

Listen IP: unspecified or public IP address you want server to use

Listen port: 1494

Destination IP: private class IP address of the server inside of the network

Destination port: 1494

You may create more mapped ports and access more servers simultaneously. In order to do this you will need to pre-set on the client computer which port they will use to access the server. This may be specified in .ini file of the client - when you create the connection icon.

MS Terminal Server

WinRoute fully supports **MS Terminal Server** protocol. To access MS Terminal server running inside of the WinRoute network from the Internet you will have to perform the following Port Mapping:

For MS Terminal Server:

Protocol: TCP

Listen IP: unspecified or public IP address you want server to use

Listen port: 3389

Destination IP: private class IP address of the server inside of the network

Destination port: 3389

You may create more mapped ports and access more servers simultaneously. In order to do this you will need to pre-set on the client computer which port they will use to access the server. This may be specified in .ini file of the client - when you create the connection icon.

Internet telephony - BuddyPhone

WinRoute is the industry's first software router/firewall that brings the Internet telephony to the serious business level. BuddyPhone allows you to place a call through the Internet from one network to another.

Support for BuddyPhone works best with ICQ. Register this free instant messenger software and you will enjoy "one-touch-button" operation when calling your friends.

All users' active in your ICQ buddy list will appear in your BuddyPhone phone book and placing a call is as easy as selecting such a user in the list.

There are no settings required as long as you use BuddyPhone and ICQ together.

Using BuddyPhone without ICQ

WinRoute can divert the calls coming from the Internet to the right recipient in the local network based on the port.

Use ports 710 and up to assign the local users with their unique port.

Example:

You have three users in your LAN using BuddyPhone.

User name	User's IP internal IP address	Port assigned to user
John	192.168.1.2	710
Quido	192.168.1.3	711
Bob	192.168.1.4	712

Then you will set the Port Mapping:

Listen Port	Destination IP	Destination Port
710	192.168.1.2	700
711	192.168.1.3	700
712	192.168.1.4	700

Placing a phone call to the user will be as easy as entering company.com:port# in the BuddyPhone direct dial dialog. For example kerio.com:711.

- ***Note! It is not a mistake in our documentation! The destination port is really 700. This is the port number used by BuddyPhone to work. WinRoute will provide the routing based on the Listen Port.***

CU-YouSeeMe

The following Port Mapping is necessary to receive **CU-SeeMe** calls through NAT:

Protocol: UDP

Listen IP: <unspecified>

Listen Port: 7648

Destination IP: the IP address of the workstation that runs the CU-SeeMe client

Destination Port: 7648

Protocol: UDP

Listen IP: <unspecified>

Listen Port: 7649

Destination IP: the IP address of the workstation that runs the CU-SeeMe client

Destination Port: 7649

Limitations:

- At present, it is not possible to run more that one CU-SeeMe client on the one local area network
- It is not possible to connect to a "reflector" protected by a password.

VNC

Protocol: TCP

Listen IP: Unspecified

Listen Port: 5900 (depending on the display number)

Destination IP: IP address of the machine that is running the application

Destination Port 5900

PC Anywhere gateway

Running pcAnywhere in Gateway mode on the WinRoute firewall will allow the remote client to retrieve a list of available pcAnywhere hosts running behind the firewall. From this list you can manage any one of the pcAnywhere hosts behind the WinRoute firewall.

These steps assume you are using pcAnywhere 9.0 and are not filtering any incoming/outgoing packets at the WinRoute firewall.

- Managed computers behind the WinRoute firewall will run PC Anywhere Host using TCP/IP
- Remote computer will run PC Anywhere Remote using TCP/IP
- pcAnywhere is installed on WinRoute firewall using the Gateway mode. When configuring the Gateway device both the Incoming and Outgoing devices should be set to TCP/IP
- On the WinRoute firewall, pcAnywhere must be configured to listen on the internal NIC (e.g.192.168.1.1). Directions on how to configure pcAnywhere to listen on a specific IP address/NIC can be found on Symantec's web site
- Add the specific IP address(s) of the computers to be managed in Network Options of pcAnywhere. To scan the whole subnet use 255 as the last octet (192.168.1.255).
- Configure port mapping in WinRoute this way:

  Protocol: TCP/UDP

  Listen IP: External NIC (206.86.181.25)

  Listen Port: RANGE (5631-5632)

  Destination IP: Internal NIC (192.168.1.1)

  Destination Port: 5631-5632

PC Anywhere

WinRoute includes the best support for Symantec's pcAnywhere of any software router on the market. pcAnywhere allows the user to access and manage computers inside of the network. In order to do this you have to apply the following scenario:

1. Managed computer will run pcAnywhere Host.
2. Remote computer will run pcAnywhere Remote
3. Port Mapping on WinRoute's computer will be configured this way:

   Protocol: TCP/UDP

   Listen IP: unspecified

   Listen Port (range): 5631-5632

   Destination IP: IP address of pcAnywhere Host inside of your network (e.g.192.168.1.12)

   Destination Port: 5631-5632

Security issue

To increase security and to avoid opening your network to the outside world, WinRoute allows users to choose a specific IP address from where the access through specific ports is allowed. This configuration allows for only certain computers or networks to access your system from the Internet.

To setup computers that are allowed to access your network, you have to define an Address Group first (even if you enter only a single computer). To configure this go to menu Settings=>Advanced=>Address groups.

Changing the access to different computers

You can setup the Administrator rights in WinRoute to enable a connection directly to the WinRoute host. While in the host, you can change the destination IP in Port Mapping and access directly the PC you choose. Amazing!

Gaming section

About running games behind NAT

Playing Games

Many games today support a multi-user environment. Users may fight each other over the Internet, LAN or they can join one of the existing game servers on the Internet. Users can also host their own game servers and allow friends, family or total strangers the excitement of playing the games together.

There are many games that do not require any settings in WinRoute. Prior to attempting to configure WinRoute for a specific game, we recommend you demo the game first. Unlike Proxy Servers, the basic architecture of WinRoute supports many games directly "off the shelf."

Certain games require a specific port configured in WinRoute in order to get them up and running. Ports are used for further identification of the player at the game server (in general).

If the game has a specific port associated with it, this is not a problem for WinRoute! Just configure WinRoute's Port Mapping to forward packets arriving at your network to the player's computer behind the firewall.

The ports used vary game to game. Please refer to the documentation accompanying each game or call technical support of the game vendor for more information. This manual contains just several examples of settings of the most popular games.

Asheron's call

Asheron's call is a popular game on Microsoft Gaming Zone. In order to play this game from the computer behind WinRoute you have to perform the following Port Mapping settings:

1. Go to menu *Settings->Advanced->Port Mapping*
2. Perform following settings:

Name:	S1	S2	S3	S4	S5
Port number:	2300-2400	9000-9013	6667	28800 - 29000	
Destination IP:	IP of PC with game	IP of PC with game	IP of PC with game	IP of PC with game	IP c wit gan
Protocol:	TCP/UDP	UDP	TCP	TCP	

Battle.net (Blizzard)

Following Port Mapping must be set in order for you to play games on battle.net. Only one player may play at a time.

Protocol: TCP/UDP

Listen IP: unspecified

Listen Port: 6112

Destination IP: IP address of gamer's computer (e.g.192.168.1.6)

Destination Port: 6112

Half-Life

Half-Life

Protocol: TCP/UDP

Listen IP: unspecified

Listen Port: 27015

Destination IP: IP address of gamer's computer (e.g.192.168.1.6)

Destination Port: 27015

MSN Gaming zone

The following configuration has been tested with MechWarior3 thoroughly on **MSN Gaming Zone**. Only one machine can access MSN at a time.

1. Go to menu *Settings->Port Mapping*
2. Add new Port Mapping

Protocol: TCP

Listen IP: "unspecified"

Listen port: range 2300 to 2400

Destination IP: the local IP address of the machine you want to connect to MSN

Destination port: range 2300 to 2400

3 Add another Port Mapping

Protocol: UDP

Listen IP: "unspecified"

Listen port: range 28800 to 28912

Destination IP: the local IP address of the machine you want to connect to MSN

Destination port: range 28800 to 28912

Quake

Quake 3

Quake 2/3 clients

No special settings necessary

Quake 2/3 Server

For Master server:

Protocol: UDP

Listen IP: Unspecified

Listen port: single 8002

Destination IP: x.x.x.x

Destination port: 8002

For clients connecting to Quake3 Arena server:

Protocol: UDP

Listen IP: Unspecified

Listen port: single 27960

Destination IP: x.x.x.x

Destination port: 27960

StarCraft

Playing StarCraft

WinRoute Pro includes unique support for all StarCraft (Blizzard Entertainment) players. Multiple players on the network connected to the Internet through WinRoute Pro may enjoy the fun when playing the game with their virtual "enemies" on the Internet.

At present, fully automatic support works only in the case that all players joining the game from one network are on computers behind WinRoute Pro and not on the host machine.

For more details visit www.kerio.com

Additional mappings for common games/apps

Ports for various applications

Age of Empires II - 2 port mapping necessary

Protocol: TCP

Listen IP: Unspecified

Listen Port: 47624

Destination IP: IP address of the machine that is running the application

Destination Port: 47624

Protocol: TCP/UDP

Listen IP: Unspecified

Listen Port: Range 2300 - 2400

Destination IP: IP address of the machine that is running the application

Destination Port: Range 2300 - 2400

Delta Force

Protocol: TCP

Listen IP: Unspecified

Listen Port: Range 3568 - 3569

Destination IP: IP address of the machine that is running the application

Destination Port: Range 3568 - 3569

Dial Pad

Protocol: UDP

Listen IP: Unspecified

Listen Port: Range 51200 - 51201

Destination IP: IP address of the machine that is running the application

Destination Port: Range 51200 - 51201

Kali - 3 port mappings necessary

Protocol: UDP

Listen IP: Unspecified

Listen Port: 2213

Destination IP: IP address of the machine that is running the application

Destination Port: 2213

Protocol: UDP

Listen IP: Unspecified

Listen Port: 6666

Destination IP: IP address of the machine that is running the application

Destination Port: 6666

Protocol: UDP

Listen IP: Unspecified

Listen Port: 57

Destination IP: IP address of the machine that is running the application

Destination Port: 57

Accessing FTP server with non-standard ports

If you are behind WinRoute and you are trying to access an FTP server with a port number different from 21, you will not receive a directory listing. In order for this to work you must do the following:

1. Go to the WinRoute machine
2. Turn off the WinRoute engine
3. Go to menu Start->Run
4. Type regedit to access the Registry Editor
5. Find HKEY_LOCAL_MACHINE/SOFTWARE/kerio/WinRoute/Module/0
6. Modify SpecParams so that the value is equal to the port number of the FTP server you would like to access
7. Turn WinRoute engine back on.

This should allow anyone behind WinRoute to access an FTP server that uses the non-standard ports specified in SpecParams.

- ***Note! You can specify multiple ports by placing a space between each value.***

GLOSSARY OF TERMS

A

ARP

Address Resolution Protocol associates an IP address to a hardware address called a Media Access Control (MAC) address.

B

BOOTP

The Bootstrap Protocol is a variant of DHCP. Clients must be enabled to use this protocol.

C

Cache

Refers to a file where data is temporarily stored. WinRoute uses caching for the temporary storage of web pages to maintain bandwidth.

D

DHCP

Dynamic Host Configuration Protocol is a protocol for organizing and simplifying the administration of IP configuration for computers in a network. A DHCP server such as WinRoute maintains the settings that are issued to each client within the network that is configured as a DHCP client. These settings define, among other things, where the client must send requests for Domain Name resolution and to whom the client should send all IP traffic that it does not know how to route.

DNS

Domain Name System is a naming scheme for IP addressing. For example www.kerio.com is a domain name and has an associated IP address. A DNS server matches domain names to an IP address. We use the domain name system because it is easier to remember a domain name than a string of numbers.

E

ETRN

The ETRN command is used when an SMTP server is not online 24 hours a day. An ETRN enabled SMTP server will hold messages in the queue until another SMTP server uses the command to have them flushed.

F

Firewall

A filtering module located on a gateway machine that examines all incoming and outgoing traffic to determine if it may be routed to its destination. WinRoute provides an extensive firewall via: NAT's functionality, the assignment of rules for specified IP addresses, and the ability to record certain information going one way so it may be authorized on the way back.

Flags

TCP uses the following flags as a means of client/server communication.

SYNC - Synchronize - the establishing packet from a TCP connection

ACK - Acknowledge - acknowledgement about the data exchange

RST - Reset - request for re-establishing of the connection

URG - Urgent - urgent packet

PSH - Push - request for immediate delivery of the packet to the higher layers

FIN - Finalize - finalize the connection

FTP

File Transfer Protocol is an application protocol used to transfer, update, delete, move, rename or copy data across the internet.

G

Gateway

The point of entrance from one network to another. A gateway is responsible for the proper distribution of data coming in and going out of a local area network. WinRoute must be installed on the gateway machine, also referred to as the host computer.

I

ICMP

Internet Control Message Protocol uses datagrams to report information between routers.

IP address

An IP address is a unique 32-bit number, which identifies a computer in an IP network.

IPSEC

Internet Protocol Security allows for virtual private networking using authentication and encryption between IP networks.

L

LAN

A Local Area Network (LAN) is a group of interconnected computers with the ability to share resources.

M

MAC address

Media Access Control address is more specific than an IP address and cannot be changed because it is specific to each network hardware device. While routers such as WinRoute use IP addressing for routing decisions, switches use MAC addressing for path determination.

MX records

MX (Mail Exchange) records contain the information about other mail servers on the Internet. MX is a type of name resolution that places the mail domain i.e. mail.yourdomain.com to an IP address. SMTP servers rely on MX records to send email.

N

NAT

NAT - Network Address Translation - also called IP masquerade, is a process of translating the source header of IP packets so they will be routable across wide area networks.

Network interface

A network interface is any device that connects a computer with other computers by means of a communication medium. A network interface may be an Ethernet card, modem, ISDN card, etc. The computer sends and receives data by means of a network interface.

Network Mask

Network mask is used to group IP addresses together. There is a group of addresses assigned to each network segment. For example, the mask 255.255.255.0 groups together 254 IP addresses. If we have, as another example, a sub-network 192.168.16.64 with mask 255.255.255.224, the addresses we may assign to computers on the sub-network are 192.168.16.65 to 192.168.16.94, with a broadcast address of 192.168.16.95.

P

Packet

A packet is a basic communication data unit used when transmitting information from one computer to another. The maximum length of a packet depends on the communication medium. As an example, in Ethernet networks the maximum length is1500 bytes. A data packet can be divided into two parts: the header part and the data part. The header contains information needed for communication between nodes; the data is the body of the packet that is ultimately received by the application.

POP3

The (Post Office Protocol) POP3 protocol is a TCP protocol using port 110. It is used to gather email. WinRoute functions as both a POP3 server and client.

Port

A port is a 16-bit number (the allowed range being 1 through 65535) used by the TCP and UDP protocols at the transport layer. Ports are used to address applications (services) that run on a computer. If there was only a single network application running on the computer, there would be no need for port numbers and the IP address only would suffice for addressing services. However, several applications may run at once on a particular computer and we need to differentiate among them. This is what port numbers are used for. Thus, a port number may be seen as an address of an application within the computer.

Port Mapping

Port mapping (or Port Address Translation - PAT) is the process where packets arriving to a particular IP address/port can be translated and thus redirected to a different IP/port. This functionality is a way to create a persistent passage through NAT. Port Mapping is only necessary for incoming connections, not returning traffic.

PPTP

PPTP - Point To Point Tunneling Protocol - is the Microsoft protocol for Virtual Private Networking.

Protocol

Defines rules for the transmission of data.

Proxy

Proxy is another method of sharing of Internet access. Proxy operates with the data on a higher protocol level so that Internet sharing with Proxy servers was never reliable and also required a special application gateway for each networking protocol.

R

RAS

Remote Access Service refers to the ability to dial into another computer or network remotely. In the context of WinRoute, RAS simply refers to a dial-up connection.

Routing Table

The Routing Table defines which interface should transmit an IP packet based on destination IP information.

S

SMTP

The Simple Mail Transfer Protocol (SMTP) protocol is a TCP protocol that uses port 25. All email is sent using SMTP. SMTP servers inspect the email header and may generate more pieces of the same email if there are multiple recipients. The destination address is analyzed and either delivered to a local mail box or forwarded to another SMTP server. When the email reaches the SMTP server occupying the domain for which the email was intended, the email is stripped of specific header information and delivered to a local user account, whereupon the user must initiate a connection to the server to access the email via POP3, IMAP, or HTTP.

T

TCP/IP

TCP/IP is a sum of networking protocols used for communication across wide area networks such as the Internet.

U

UDP

(User Datagram Protocol) Uses a special type of packet called a datagram. Datagrams do not require a response; they are one way only (connectionless). Datagrams are usually used for streaming media because an occasional packet loss will not affect the final product of the transmission.

V

VPN

Virtual Private Networking allows local area networks to communicate across wide area networks, typically over an encrypted channel.

INDEX

E

F

G

H

I

L

M

N

P

Q

R

S

T

U

V

W

Y