WinRoute Lite 4.2

Kerio Technologies Inc.

Contents

Contents

C H A P T E R   1

BEFORE INSTALLING WINROUTE

In This Chapter

System Requirements

WinRoute Lite supports the following Windows Operating Systems:

- Windows NT 4.0 Workstation/Server
- Windows 98
- Windows Millennium Edition
- Windows 2000 Professional/Server/Adv Server
- Windows XP

➢ *Minimum Hardware Requirements:*

The minimum hardware requirements should meet those defined by Microsoft for your respective Operating System

Choosing the right computer for sharing

WinRoute Lite **MUST** run **ONLY** on the computer that is connected to the Internet.

WinRoute Lite acts as the gateway between the two (or more) networks, where each network is represented by one interface. These interfaces may be two or more network cards or a network card and a RAS adapter (in case of Dial-up).
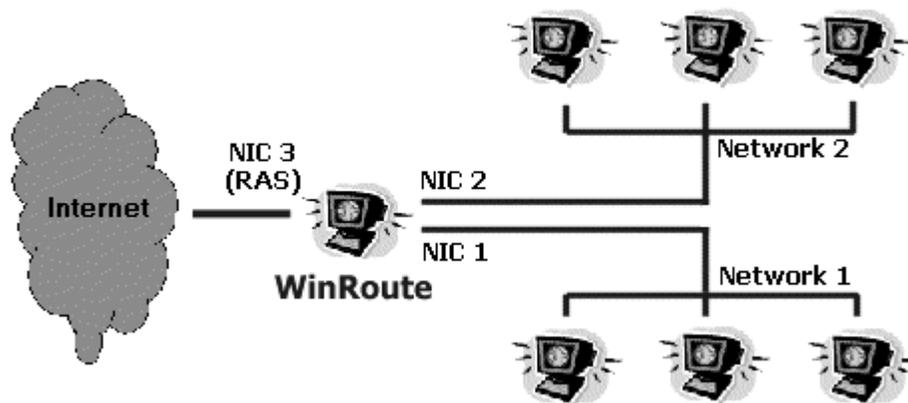
Configure TCP/IP

The Transmission Control Protocol/Internet Protocol (TCP/IP) is the standard for communication over the Internet. In order for the Internet connection to be shared it is necessary to properly configure the gateway PC for network communication. The gateway PC MUST have at least two interfaces, one which connects the gateway to the Internet (Modem, Ethernet, Satellite, USB...) and another interface which connects the gateway to the local area network (LAN). The internet interface should already have TCP/IP settings based on your Internet Service Provider's requirements.

In order for WinRoute to properly communicate with the LAN it is necessary to configure the LAN interface for TCP/IP communication. The basic instructions are provided below. For more detailed instructions refer to support.microsoft.com.

- Proceed to the network control panel.
- Select the TCP/IP properties of the adapter/interface that connects to your local area network.
- Assign an IP address and subnet mask (e.g. 192.168.100.1 mask 255.255.255.0).
- **Do NOT define a default gateway** or any domain name servers (DNS) to this interface! These parameters should be defined only on your Internet interface.

Multi-operating systems environment (Linux, AS400, Apple)

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

WinRoute Lite is suitable for connecting multiple operating system type environments to the Internet. WinRoute Lite acts as a software router. As such, it supports any standard TCP/IP environments. **NOTE**: A Windows based operating system must host the Winroute lite application. Therefore, at least one Windows based computer is required in the Winroute lite network.
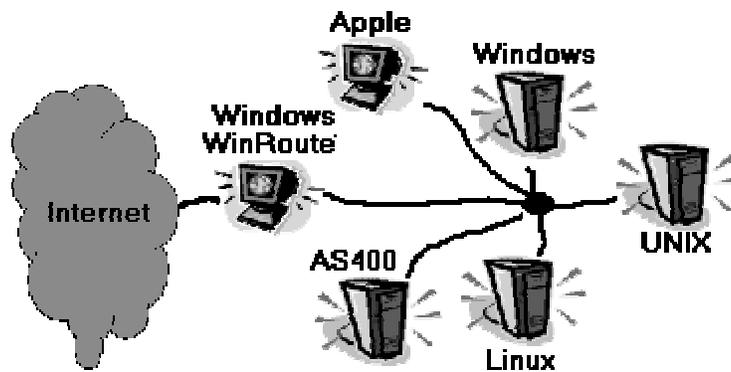
C H A P T E R 2

CONNECTING THE NETWORK TO THE INTERNET

In This Chapter

WinRoute Lite installation and maintenance

The WinRoute Lite installation package is less than one Megabyte and should be obtained from www.kerio.com. After downloading the latest version you can simply double click on the installation package. WinRoute will require you to reboot the computer. After rebooting you will see a small purple icon in the system tray (lower right corner).

By right clicking on this icon you can select 'Administration' or you can alternatively access the admin utility by double clicking on the icon.

Other options include 'Startup Preferences', 'Help' and start/stop engine.

> ➢   *Keep Updated - In order to ensure maximum security, you should refer back to our website* www.kerio.com *on a regular basis to get the latest version. To update WinRoute Lite simply download and install the latest version over top of the previous version. All settings and license information will be retained.*

Basic Configuration

After installing WinRoute Lite you can begin configuring WinRoute. To access the WinRoute lite administration simply double click on the WinRoute icon located in the system tray (lower right corner of the screen).

1 **Choose the Internet Interface!** In the *Settings* tab you must tell WinRoute how you connect to the Internet. If you use an Ethernet adapter make sure that you choose the adapter attached to the Internet and not the adapter leading to a local network.

2 **DHCP configuration (recommended)!** In most cases you will use WinRoute Lite's DHCP server for automatic network configuration. In this case, all client computers will be set to receive TCP/IP settings through DHCP. Most operating systems are configured this way by default. You can enable the DHCP server in the advanced settings menu -> DHCP. Make sure you select the correct adapter/interface connecting to the local area network. **Note** - If your LAN adapter is not properly configured for TCP/IP you will not be allowed to select the LAN adapter. In this case refer to the section '*Configure TCP/IP* (on page 6)'.

3 **Manual TCP/IP configuration** In case you don't want to use DHCP on your LAN you can assign TCP/IP settings manually to each workstation. In this case you must assign an IP address and subnet mask in the same IP subnet as the WinRoute computer. The default gateway should be the LAN interface IP address of the WinRoute computer and the domain name server address should also point to the IP address of the WinRoute computer. Alternatively you can use different DNS servers, such as those recommended by your Internet Service Provider.

Dial-up or ISDN connection

Dial-up or ISDN connection

If you have dial-up 56K or ISDN access to the Internet WinRoute Lite must run on a computer that includes:

▪   Modem attached to the phone or ISDN line

▪   Network Card Interface (NIC) leading to the internal network.
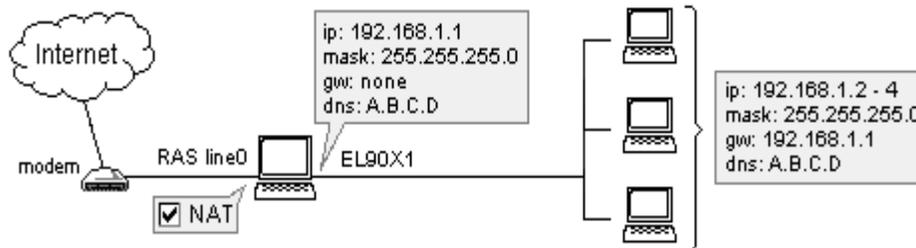
Before the connection

Before connecting to the Internet, double check the following:

▪   TCP/IP protocol is properly installed and configured.

▪   Dial-up networking is properly installed and configured.

▪   Modem is attached to the WinRoute Lite host PC.

WinRoute Lite uses Dial-up Networking or RAS services available in your operating system for your Internet connection. Make sure that you are able to connect to the Internet from the computer where WinRoute Lite is to be installed to assure that the connection is correctly configured and dial-up networking or RAS is properly working.

WinRoute Lite Configuration

1 In WinRoute Lite go to menu Settings and choose that you will connect to the Internet via Dial-UP

2 Choose one of the pre-configured RAS connections and insert the user name and password for that connection.

Dialling Options:

- Dial on demand - Workstations using DHCP, or those configured to use WinRoute as their primary DNS server, can take advantage of Dial on Demand. This feature will allow WinRoute to dial the connection when a workstation on the network opens a web browser or any application trying to resolve an external domain name.

- Hang up if idle for - This will cause WinRoute to close the internet connection if no Internet activity is detected for the defined time period (default = 10 Min)

- Redial when busy - WinRoute will redial the connection if the phone line is busy (default = 3 times)

▪ Reconnect on line failure - If the Internet connection drops, WinRoute will automatically redial the connection.

About DHCP server

Dynamic **H**ost **C**onfiguration **P**rotocol is intended to simplify (through autoconfiguration) the task of TCP/IP assignment. DHCP is used for dynamic configuration of the TCP/IP protocol on computers in a local network. In order to establish functional Internet communication, TCP/IP must be properly configured on each workstation within the local network. The necessary TCP/IP parameters include:

IP address (e.g. 192.168.10.2) - This value uniquely identifies a computer within a Local Area Network.

Network mask (e.g. 255.255.255.0) - This value is combined with the IP address to determine the group of IP addresses to which the computer belongs. In the provided example, computers having IP addresses of 192.168.10.1-192.168.10.254 are all in the same group or IP subnet.

Default gateway (e.g. 192.168.10.1) - This is the IP address of a router (i.e. WinRoute) who is responsible for forwarding packets to the correct destination address. When a workstation wants to establish communication with a computer outside of its local IP subnet (i.e. an unknown address) is sends the packet to its default gateway or router.

DNS server (e.g. 192.168.10.1) - This is the IP address of a server that is able to translate names (e.g. www.kerio.com) into an IP address. WinRoute Lite has a built-in DNS proxy that will take requests from the local network and forward them to the correct DNS servers assigned by your Internet Service Provider.

Before you can enable WinRoute's DHCP server on your LAN interface you must have TCP/IP properly configured. If you do not, WinRoute will not allow you to enable DHCP on that interface until you've configured an IP address and subnet mask. For configuration of IP addresses refer to section '***Configure TCP/IP*** (on page 6)'.
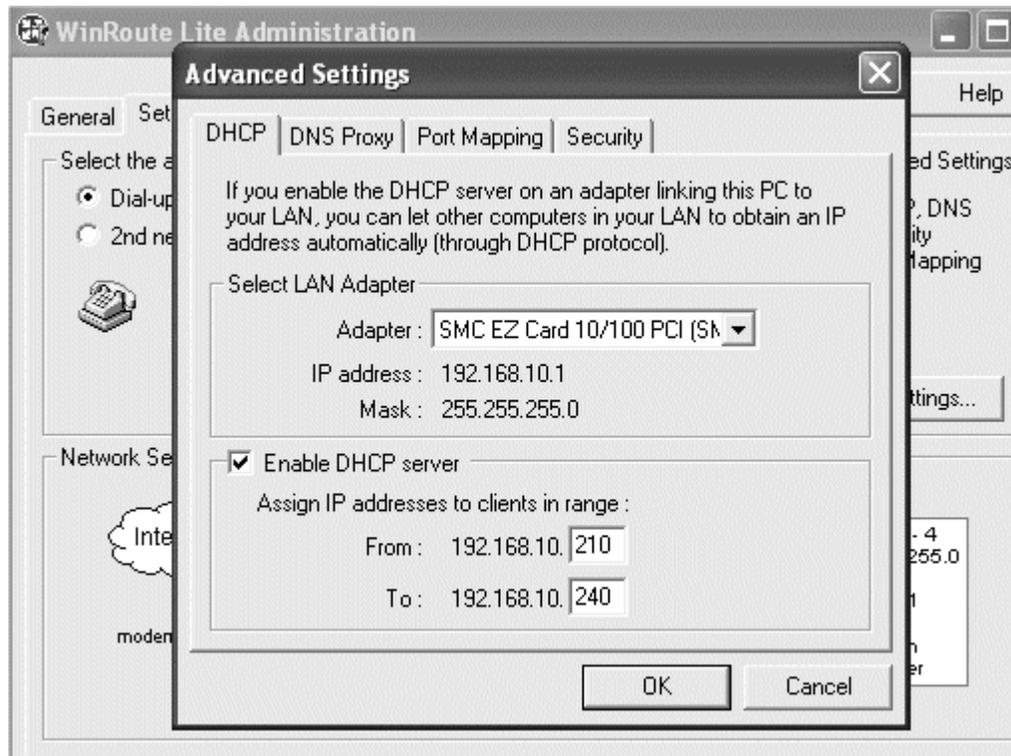
About DNS proxy

DNS Proxy/Forwarding

The **D**omain **N**ame **S**ervice is a system designed to allow the identification of Internet servers to be based on names rather than IP addresses. Because Internet communication is based on IP addresses, all names must be translated into an IP address. This is the purpose of a Domain Name Server.

WinRoute Lite has a built-in DNS proxy that can take DNS queries from the local network and forward them to an Internet Domain Name Server. By default the DNS Proxy is enabled and WinRoute will forward all requests to the servers detected by the operating system (usually assigned by your ISP). Alternatively you can choose to forward DNS queries to specified servers.
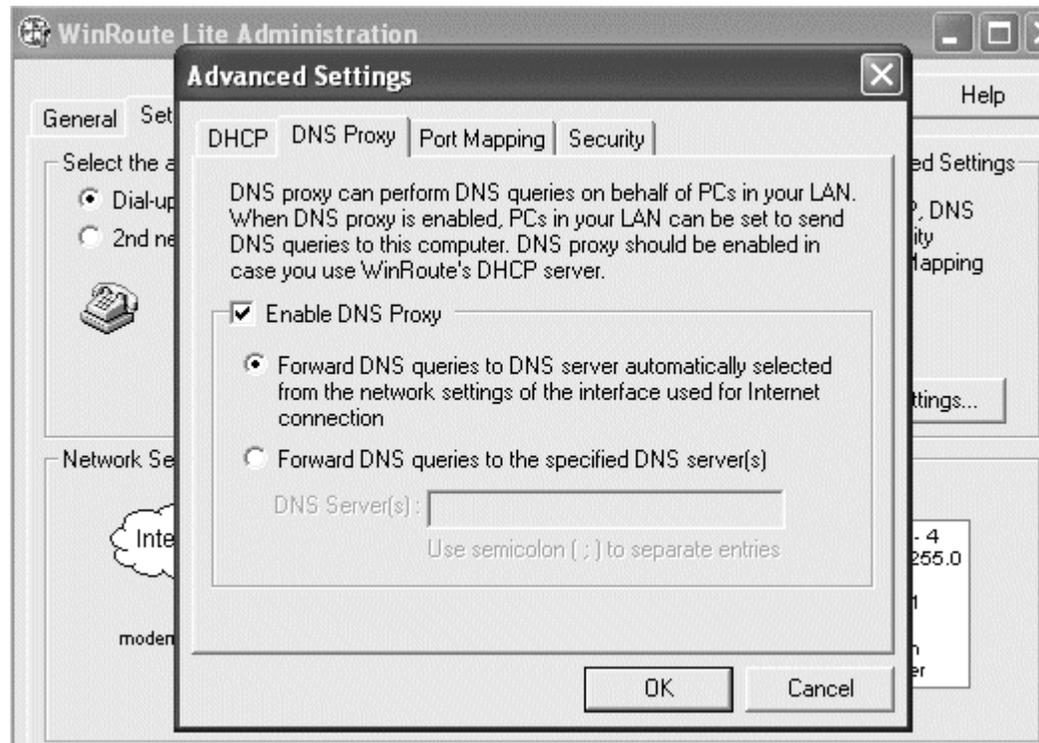
About Port Mapping

WinRoute Lite's primary security/routing component is based on a technology referred to as Network Address Translation (NAT). NAT allows a local network to use private (non-routable) IP addresses, yet still communicate out to the Internet. In other words, connections may be established outbound to the Internet, but connections arriving from the Internet are not allowed. By using port mapping however, public services like a WWW server or an FTP server, and others running on your private network may become accessible from the Internet.

What is Port Mapping?

Port Mapping is an advanced WinRoute feature that allows servers to be hosted securely behind NAT. Internet servers listen on well known ports for uninitiated connections. In other words, the server does not know in advance where a connection may come from. Examples of well known ports include HTTP (TCP port 80), SMTP (TCP port 25), Telnet (TCP port 23). If these types of well known services should be available to the Internet, then port mapping must be used to allow NAT to make exceptions for these services by redirecting these inbound connections to the appropriate local server.
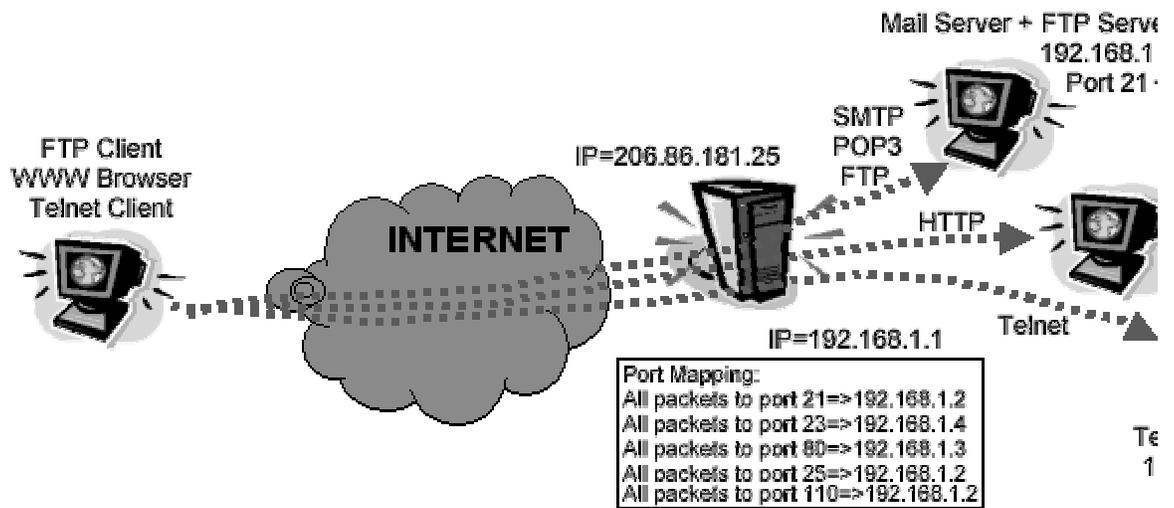
Port Mapping Configuration

1   Go to menu *Settings->Advanced->Port mapping*

2 Add new port mapping:
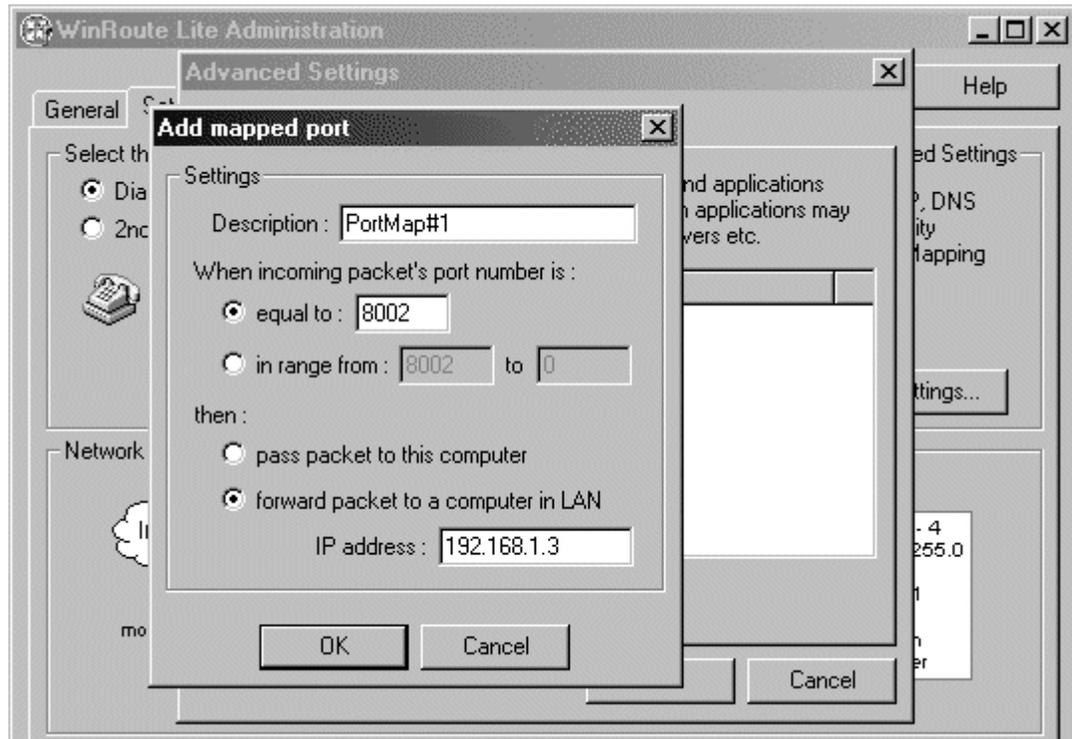
Description

Assigns your specific Port Mapping setting with the name (e.g. the name of the game application).

Incoming packet's port number

This is the application you want to pass through the Firewall. Depending on the type of hosted service, inbound TCP or UDP packets will arrive at the WinRoute computer on a specific port number. Based on this port number you may specify that certain packets will be routed to a specific computer/server behind the firewall.

Forward to the local computer with IP address

Here you must specify the local server IP address that is listening for connections from the Internet. If the service is hosted on the WinRoute computer itself you can simply enable the option 'pass packet to this computer'.

C H A P T E R   3

INSIDE WINROUTE LITE

In This Chapter

The Architecture

WinRoute Lite Architecture

For advanced Internetworking, it's helpful to understand how WinRoute Lite works.

WinRoute Lite works **below the TCP/IP stack** at the driver level. In other words - it captures both **outgoing** and **incoming** packets **BEFORE** any application). This advanced design makes WinRoute Lite security almost **unbreakable**
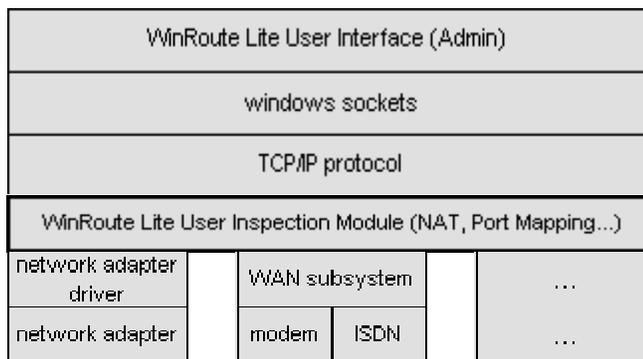
WinRoute Lite is an extensive software router that supports almost any Internet protocol. At the same time, Winroute lite checks each packet, utilizing the advanced security and firewall features inherent in the software design. With systems running Windows 95 and 98, Winroute lite handles the routing of packets. On systems running Windows NT, the NT operating system performs the routing and WinRoute Lite manages the NAT functionality and other data.

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" computer.

The NAT engine also maintains a table of information for each packet that passes through to the Internet.
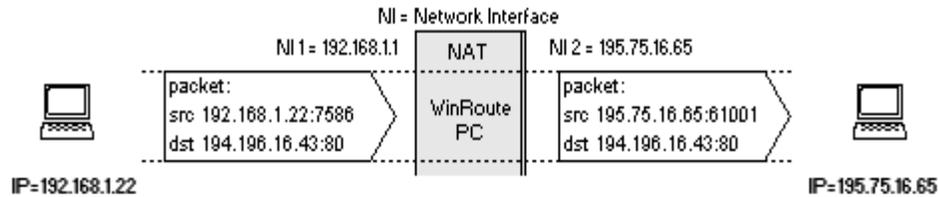
On the way back

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

Remember the packet came with the public IP address of the NAT computer as a "destination" originally. The NAT engine had to change this information in order to deliver the packet to the correct recipient within the local network.
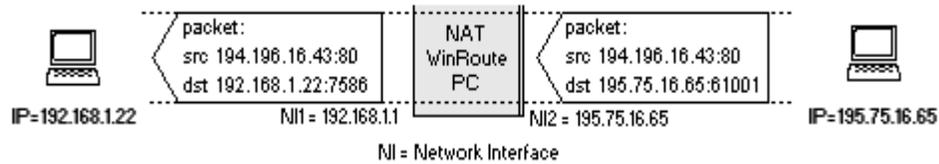
Logs and packet

How to read the log?

analysis

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

From the left you may see the 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, TCP, UDP, ARP, ICMP etc.

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 - Are the extended information of the packet. They keep additional information about the packet used by routers or in standard TCP communication. Here is the list of flags displayed by WinRoute:

SYN - 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

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

C H A P T E R   4

RUNNING ICQ, VOICE OVER IP, VIDEO CONFERENCING

In This Chapter

Running ICQ behind NAT

Running ICQ

WinRoute Lite offers this unique support for ICQ users. Most ICQ services including direct chat and file transfer are available for each user without any configuration. If any component of ICQ does not work we recommend installing the latest version of ICQ.

IRC - Internet Relay Chat

There are no special settings for IRC required. It will work automatically if you connect to standard server ports (6661,6662,6663,6665,6666,6667,6668)

Even DCC (Direct Chat/Send(Receive) Files) will work automatically if you use the standard port 6667 in you IRC.

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

PPTP over NAT

There are no settings required to run PPTP clients behind WinRoute Lite. Outbound connections can be established from workstations behind WinRoute Lite without any configuration.

CITRIX Metaframe

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

For CITRIX Metaframe:

Description: Enter CITRIX Metaframe

When incoming packet's port number is equal to: 1494

Forward packet to local computer with IP address: 192.168.1.1

Advanced Setting This rules applies to protocol:

Protocol: TCP

MS Terminal Server

For MS Terminal Server:

Description: Enter MS Terminal Server

When incoming packet's port number is equal to: 3389

Forward packet to local computer with IP address: 192.168.1.1

Advanced Setting This rules applies to protocol:

Protocol: TCP

Internet telephony - BuddyPhone

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 a user on the list.

There are no settings required as long as you use BuddyPhone and ICQ together. The destination port is 700. This is the port number used by BuddyPhone.

Using BuddyPhone without ICQ

WinRoute Lite allows you to divert the calls coming from the Internet to the right recipient in the local network based on the port number. To enter port numbers go to, settings=> Advanced settings=> Port Mapping=> Add=> Edit mapped port.

Under description you will enter: BuddyPhone, the incoming port number is equal to: 710 for the first user with BuddyPhone, forward packets to the user's internal IP address 192.168.1.2 Advanced Settings: the protocol that applies is UDP.

It will be necessary to configure each user individually in WinRoute Lite with their port number and local IP address.

Use ports 710 and up to assign the local users with their proprietary 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:

Port number	Local IP address	Destination Port
710	192.168.1.2	710
711	192.168.1.3	711
712	192.168.1.4	712

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

video conferencing

For the first time ever you may establish a video conference call from one private network to another. To use the ICUii application you have to map the following ports:

Description: Enter ICUii

When incoming packet's port number in range from: 2000-2038

Forward packet to local computer with IP address: 192.168.1.2 (client computer)

Advanced Setting This rule applies to protocol:

Protocol: TCP

PC Anywhere

PC AnyWhere allows the user to access and manage computers inside of the network. In order to do this you have to apply the following configuration:

1 Managed computer will run PC Anywhere Host.

2 Remote computer will run PC Anywhere Remote

3 Port Mapping in the WinRoute Lite computer will be configured this way:

Description: PC AnyWhere

When incoming packet's port number in range from: 5631-5632

Forward packet to local computer with IP address of PC Anywhere Host inside of your network (e.g.192.168.1.12)

CU-SeeMe

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

Description: CU-SeeMe

When incoming packet's port number is equal to: 7648

Forward packet to local computer with IP address of the workstation that runs the CU-SeeMe client

Description:CU-SeeMe

When incoming packet's port number is equal to: 7649

Forward packet to local computer with IP address of the workstation that runs the CU-SeeMe client

Limitations:

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

CHAPTER 5

GAMING SECTION

In This Chapter

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 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 games together.

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

Certain games require that specific ports be configured in WinRoute Lite 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 lite! Just configure WinRoute Lite's Port Mapping to forward packets arriving at your network to the player's computer behind the firewall. This is typically only necessary when hosting games, in which random access must be granted to your local machine.

The ports used will vary from game to game. This manual contains examples of settings for the most popular games.

MSN Gaming zone access only

The following configuration was tested to play 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

For clients connecting to MSN Gaming Zone

Description: Enter MSN Gaming Zone

When incoming packet's port number in range from: 28800-28912

Forward packet to local computer with IP address of the machine you want to connect to MSN

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 Lite you have to perform following Port Mapping settings:

1 Go to menu *Settings->Port Mapping*

2 Add new Port Mapping

Name:	S1	S2	S3	S4	
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	

MechWarrior3

1 Go to menu *Settings->Port Mapping*

2 Add new Port Mapping

For clients connecting to MechWarrior3

Description: Enter MechWarior3

When incoming packet's port number in range from 2300-2400

Forward packet to local computer with IP address of the machine you want to connect to MechWarior3

Quake

Quake 3

Quake 2/3 clients

No special settings necessary

Quake 2/3 Server

For clients connecting to Master server:

Description: Enter Quake Master Server

When incoming packet's port number is equal to 8002

Forward packet to local computer with IP address of the machine you want to connect to Quake

Advanced Setting This rules applies to protocol:

For clients connecting to Quake3 Arena server:

Description: Enter MSN Gaming Zone

When incoming packet's port number is equal to 27960

Forward packet to local computer with IP address of the machine you want to connect to Quake3 Arena server:

Advanced Setting This rules applies to protocol:

Half-Life

Setting up a Half-life game server behind WinRoute

1   Go to menu *Settings->Port Mapping*

2   Add new Port Mapping

   When incoming packet's port number is equal to 27015

   Forward packet to local computer with IP address of the machine you want to connect to Half-Life

   Advanced Setting This rules applies to protocol:

Battle.net (Blizzard)

Serving Battlenet games behind WinRoute

The following Port Mapping must be set in order to play games on battle.net.
Only one player can play at a time.

Description: battlenet game

When incoming packet's port number is equal to 6112

Forward packet to local computer with IP address of the machine you want to
connect to Starcraft

Advanced Setting This rules applies to protocol:

Additional Mappings

Necessary Ports for various applications

Age of Empires II - 2 port mapping necessary

Protocol: TCP

Source IP: Unspecified

Source Port: 47624

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

Destination Port: 47624

Protocol: TCP/UDP

Source IP: Unspecified

Source 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

Source IP: Unspecified

Source 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

Source IP: Unspecified

Source Port: Range 51200 - 51201

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

Destination Port: Range 51200 - 51201

Gamespy

Registration

Protocol: UDP

Source IP: Unspecified

Source Port: 25635

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

Destination Port: 25665

For the Games themselves

Protocol: UDP

Source IP: Unspecified

Source Port: Range 25000 - 30000

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

Destination Port: Range 25000 - 30000

Kali - 3 port mappings necessary

Protocol: UDP

Source IP: Unspecified

Source Port: 2213

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

Destination Port: 2213

Protocol: UDP

Source IP: Unspecified

Source Port: 6666

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

Destination Port: 6666

Protocol: UDP

Source IP: Unspecified

Source Port: 57

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

Destination Port: 57

Mplayer

Protocol: TCP/UDP

Source IP: Unspecified

Source Port: 8000 - 9000

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

Destination Port: 8000 - 9000

Oracle

Protocol: TCP

Source IP: Unspecified

Source Port: 5000

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

Destination Port: 5000

PCanywhere versions 2.0 - 7.51 - 2 port mappings necessary

Protocol: TCP

Source IP: Unspecified

Source Port: 65301

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

Destination Port: 65301

Protocol: UDP

Source IP: Unspecified

Source Port: 22

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

Destination Port: 22

Quicktime - 2 port mappings necessary

Protocol: TCP

Source IP: Unspecified

Source Port: 554

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

Destination Port: 554

Protocol: UDP

Source IP: Unspecified

Source Port: Range 6970 - 6999

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

Destination Port: Range 6970 - 6999

RTSP

Protocol: UDP

Source IP: Unspecified

Source Port: Range 6970 - 7170

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

Destination Port Range 6970 - 7170

VNC

Protocol: TCP

Source IP: Unspecified

Source Port: 59xx (depending on the display number)

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

Destination Port 59xx

Protocol: TCP

Source IP: Unspecified

Source Port: 58xx

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

Destination Port 58xx

GLOSSARY OF TERMS

A

ARP

Address Resolution Protocol associates an IP address to a hardware address by requesting the sending machine for additional information called a MAC address. This only applies to ethernet based networks.

D

DHCP

Dynamic Host Configuration Protocol is a protocol for organizing and simplifying the administration of IP addresses for local machines. In many cases (such as with WinRoute) A DHCP server is built into the gateway for further simplification.

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.

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 Lite is a simple Firewall based on Network Address Translation.

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 or network router.

I

ICMP

Internet Control Message Protocol uses datagrams to report errors in transmission between the host and gateway.

IP address

An IP address is the unique 32-bit number, which identifies a computer in a network. In order to communicate across wide area networks, each computer must have a unique IP address. Local area networks cannot directly communicate across wide area networks because they are defined by a private class of IP's.

L

Local Area Network

A Local Area Network (LAN) is a group of interconnected computers with the ability to share resources without having to access a wide area network.

M

MAC Address

A Media Access Control (MAC) address is a hard-coded interface identification used by layer 2 devices (switch or bridge) for proper forwarding of frames between computers on a network.

N

NAT

Network Address Translation is an advanced feature of certain routers. If NAT is enabled, the control information in the header will actually be recorded to a table in memory, then changed so that it will appear as if the packet was sent from the gateway machine. When a packet arrives at the router, it can refer to the table to determine who originally sent the packet so it may be routed back to the right computer. Otherwise the packet will be discarded.

Network interface

A network interface may be an Ethernet card, modem, ISDN card, etc. The computer sends and receives packets by means of the network interface.

Network Mask

A Network mask is used to group IP addresses together. Routers use a subnet mask to define the group (or IP subnet) to which an IP address belongs so that it can identify the correct interface from which it should forward an IP packet.

P

Packet

When data is transmitted over the network it is broken up into smaller pieces called packets and individually routed to their destination. This way if one packet is not properly received, the receiving party can request resubmission of the single packet, as opposed to the entire piece of data. Each packet contains headers, which are responsible for the successful transmission of the packet, and a data part, which contains a portion of the original data being transmitted over the network. The term packet is used when referring to layer 3 devices (i.e. a router). A frame is the term used when referring to layer two devices (i.e. a switch).

Port

A port, in terms of TCP/IP, is a 16-bit number (the allowed range being 1 through 65535) used by the protocols of the transport layer - the TCP and UDP protocols. Ports are used to address applications. In other words, when a packet is received by the computer, the operating system uses port information to determine which application will receive the data within the packet.

Port Mapping

Port mapping is an advanced feature of WinRoute that allows servers to be hosted securely behind NAT. When a packet is received by the WinRoute host it can be forwarded (by translating the destination information in the packet header) to another computer in the local network.

Protocol

Defines rules for the transmission of data.

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.

T

TCP/IP

TCP/IP is a suite of networking protocols used for communication across networks. It is the standard form of communication over the Internet. The two most significantly used Internet Protocols are TCP and UDP. Transmission Control Protocol (TCP) is a connection oriented protocol intended to provide reliability and to ensure that all data is transferred successfully from one computer to another. User Datagram Protocol (UDP) is a connectionless protocol that does not require any confirmation from the receiving party. UDP is more commonly used for multimedia and streaming applications.

INDEX