User's Guide

WinRoute Pro 4.1

Contents

WinRoute administration 4

Get it up and running 11

WinRoute description 32

WinRoute administration

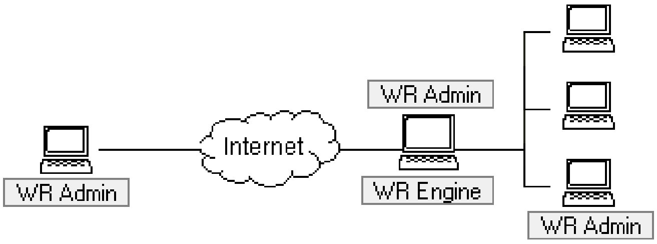
In This Chapter

WinRoute components

WinRoute Pro consists of three parts:

WinRoute Engine performs all routing and analysis operations (NAT, packet filtering, port mapping etc.). You may Start/Stop WinRoute Engine from the WinRoute Engine Monitor or, if running Windows NT, directly from NT services option.

WinRoute Engine Monitor is the monitoring application that shows whether WinRoute Engine is active or not. It appears as a little blue-white icon in the system tray.

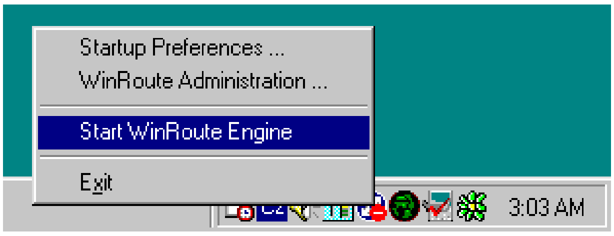


WinRoute Administration program provides the configuration and settings for the WinRoute Engine. WinRoute Administration program is a separate application (wradmin.exe) that may be copied to any computer in your network or in Internet and run from it.

Administration from the local network

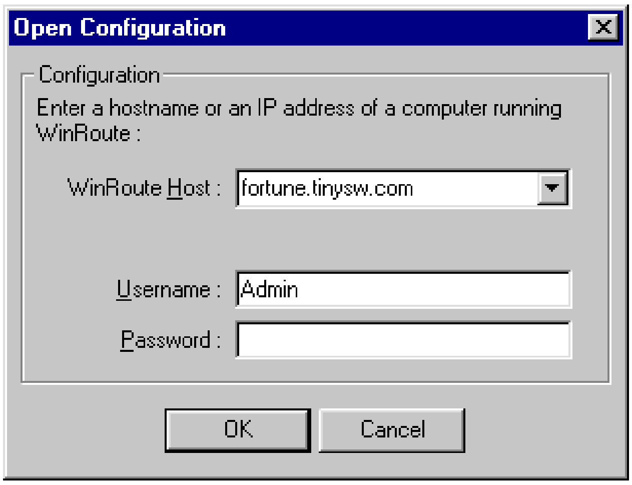
To administer WinRoute from its computer or from any computer in your local network you have to perform the following:

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



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

   A screen with initial login dialog will appear. Either leave preset localhost or enter the IP address of the computer where WinRoute is running here. Enter the user name and password of a user having administration rights.



Enter a hostname or an IP address of a computer running WinRoute :

WinRoute Host : fortune.tinysw.com

Username : Admin

Password :

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

You have to login with administration rights to WinRoute Engine successfully in order to perform settings.

Possible reasons for an unsuccessful login from a local network:

- WinRoute Engine is not running
- Wrong user name and password
- Wrong IP address entered when connecting from another computer
- 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 the network chapter of this help

Administration from the Internet

If you use NAT, Port Mapping must be set on the WinRoute computer (menu Settings=>Advanced=>Port Mapping) in order to administer a WinRoute computer from outside the LAN (from the Internet), Port Mapping must be set on the WinRoute computer (menu Settings=>Advanced=>Port Mapping):

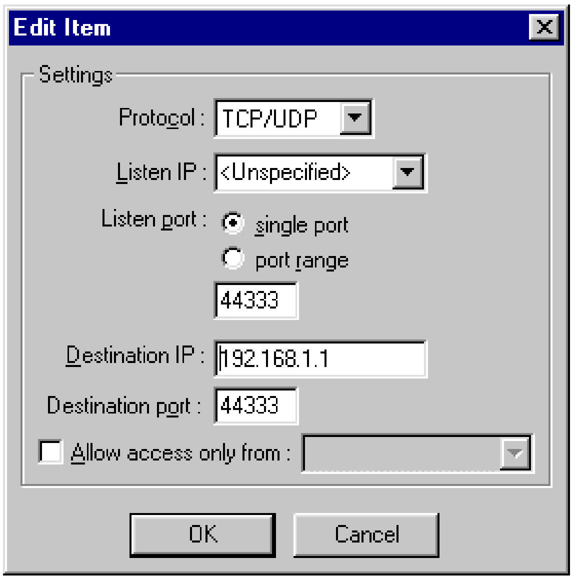
Protocol: TCP/UDP

Listen IP: <unspecified> or the IP address of the Interface connected to Internet

Listen Port: 44333

Destination IP: The IP address of the interface connected to local network

Destination Port: 44333



Edit Item

Settings

Protocol : TCP/UDP

Listen IP : <Unspecified>

Listen port : ● single port ○ port range

44333

Destination IP : 192.168.1.1

Destination port : 44333

□ Allow access only from :

See the Configuration Examples chapter 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 (e.g. 206.86.181.25) 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 an Internet:

- WinRoute Engine is not up and running
- Wrong user name / password combination
- Wrong IP address entered when connecting to WinRoute Engine
- You do not have the rights to administer WinRoute
- There is no or wrong Port Mapping set on WinRoute Engine computer (if using NAT)

Lost Admin password

If you lose the Admin password, follow these steps to regain administrative access:

1. Close Administrator dialog
2. Stop WinRoute Engine
3. Open the system registry (go to Start->Run and type in "regedit")
4. In registry go to HKEY_LOCAL_MACHINE\Software\TinySoftware\WinRoutePro\User
5. Find the key number (most often 0), where the "name" item has the value "Admin"
6. Change this name to any another (e.g. Oldadmin)
7. Go to HKEY_LOCAL_MACHINE\Software\TinySoftware\WinRoutePro, find the item "AdminUserAdded" and change its value to 0.
8. Start WinRoute engine and run WinRoute Administration program

This operation will cause WinRoute to run, as if it were the first time and will create the new administrator account with the default name Admin and no password.

In the menu Settings->User accounts, delete the user Oldadmin.

Get it up and running

In This Chapter

System requirements

To install and run WinRoute Pro 4.1 you will need:

- Pentium class PC (single or dual processor)
- Windows 95/98/NT4.0/2000 OS
- 32MB memory
- 1MB of free disk space
- at least 2 interfaces available. These might be: Ethernet, TokenRing, DirecPC, RAS...

Quick Checklist

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

Perform the settings described below if you want to benefit from using NAT to share an Internet access.

Settings and rules for the WinRoute PC

1 **Two Interfaces (NIC's)**
Check that the WinRoute computer has (at least) two interfaces. One for the Internet connection and one for local (client) connection. They may be network adapters or RAS lines. One interface (Ethernet or RAS/dial-up) is used for Internet connection while the other interface(s) (Ethernet, Token Ring…) for the connection to your network(s).

2 **Enable NAT on INTERNET interface!**
Make sure NAT is checked ON for the interface linking to the Internet (Ethernet, RAS line). Set this in menu **Settings=>Interface table** - properties of desired interface.

3 **Do NOT enable NAT on internal interface(s)!**
Make sure NAT is **UNCHECKED** on the interface or interfaces that link to the internal network.

4 **No Default Gateway on internal interface!**
Check that there is NO default gateway set in Network properties of the interface (network card) 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 **Enter options of DHCP configuration!**
If you want use WinRoute's DHCP server for automated network configuration, double check that you have defined the scope(s) of the IP addresses that you want to assign along with the Options. In Options you can specify other information given to your workstations - like DNS server address, default gateway etc.

Settings and rules for the other computers in your network

1 **WinRoute's PC internal IP address is the default gateway!**
The WinRoute PC acts as the DEFAULT GATEWAY for all computers in your LAN. As a result, use the IP address of the internal interface on the WinRoute host (e.g. 192.168.1.1) as the default gateway on every internal (client) computer. Set this value at each client computer OR assign this value automaticly for all the client computers using WinRoute's DHCP server.
See the Configuration Examples chapter if you need to use a different default gateway!

2 **Check DNS settings!**
In most cases you will use WinRoute's built-in DNS forwarder as a DNS server for your networked computers. Make sure that WinRoute's built in DNS forwarder is ON and configured. Or you may use direct the DNS server of your ISP.

Setting up the network

Using the DHCP server

Using the DHCP server you can significantly simplify configuration of the workstations within your LAN. When using 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 usually 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. It's strongly recommended that only one DHCP server is running on your network at a time.

Default gateway overview

Two basic TCP/IP settings are required on each computer in your network:

- IP address – assigned either manually or from DHCP server (e.g. WinRoute’s DHCP server)
- Default gateway

The Default gateway on each computer accessing the Internet through WinRoute must be set to the **IP address** of the WinRoute computer's interface that links to your LAN.

Example:

Client computer has IP address 192.168.1.23 while WinRoute PC has two interfaces, one linking to the cable modem with an IP from the ISP (203.23.14.232) and another one linking to the private network (192.168.1.1). The default gateway at 192.168.1.23 computer will be set to 192.168.1.1.

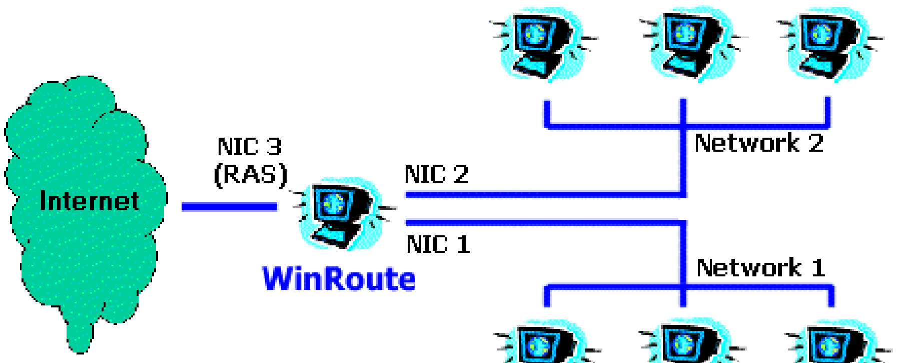
- ***Note 1: When creating IP address space within your local network you must use the IP address from the same subnet. i.e. if the subnet mask you use is 255.255.255.0 then all addresses must be from 192.168.1.1 to 192.168.1.254.***
- ***Note 2: You may have more networks connected to the Internet through WinRoute. You also may have more Interfaces in the WinRoute computer, one for each network. Then each of these interfaces 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 etc.

WinRoute always 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 and/or RAS adapter(s) (in case of Dial-up).

Example:

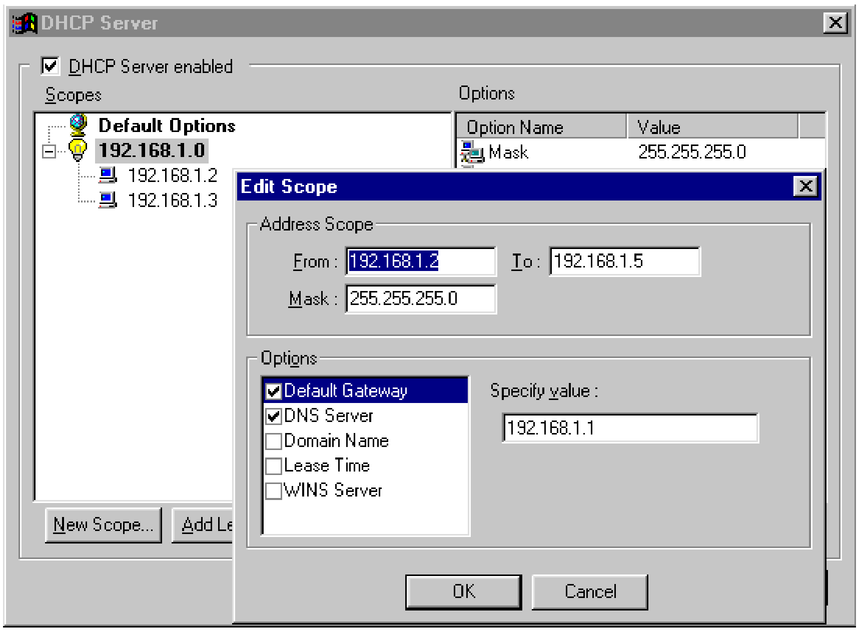


IP configuration using DHCP server

Double check, that your workstations are set to obtain an IP address from the DHCP server (see TCP/IP protocol 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 box) and press the **New Scope** button.
3. **Add Scope**
   Here you will specify the scope of IP addresses which will be assigned to workstations by the DHCP server. 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 example.
4. **Specify Options**
   In Options you can specify what other information will be given to workstations (e.g. default gateway, DNS server address etc.). Check the button beside each component in the dialog box and enter the appropriate information. Usually enter information for default gateway and DNS server here (typically you would use WinRoute PC address in both cases, e.g. 192.168.1.1). You may leave the other options blank.



DHCP Server

☑ DHCP Server enabled

Scopes

- Default Options
- 192.168.1.0
  - 192.168.1.2
  - 192.168.1.3

Options

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

IP configuration using a "third-party" DHCP server

Using a third-party DHCP server for your network configuration requires that special attention be paid to the values issued by such 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. the Default gateway, IP address (and DNS if you use it) must be set to the internal IP address of the WinRoute computer.

Also the IP address issued to the client workstation must be of the same subnet as the WinRoute computer.

DOUBLE CHECK (!!!) that the internal network interface of the WinRoute computer has assigned a **fixed IP address** (e.g. 192.168.1.1) and that this address is issued by DHCP as the default gateway to the rest of your network. The DHCP server there CANNOT assign the IP address to WinRoute PC interface!

Example:

DHCP server 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 the WinRoute DNS Forwarder) information issued to workstations will be 192.168.1.5.

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" (private) type IP address. Usually 192.168.x.x or 10.x.x.x. Assign each system an IP address of the same subnet. For example, once an IP address for WinRoute host is set at 192.168.1.1 with subnet mask 255.255.255.0, you must continue with the same numbering scheme. (e.g.192.168.1.2., 192.168.1.3 etc.)

Set the default gateway

Use the WinRoute host computer IP address as default gateway at 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 internal IP address as the DNS server address for all of your computers. The only exception might be when using the DNS address of your ISP's DNS or another DNS server. Then you will enter DNS details given to you by your ISP (in TCP/IP properties of each workstation).

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

Conflicting software

There are several issues known about incompatible software:

Bay Networks VPN Client

Even though WinRoute supports IPSEC and especially Nortel's implementation (the one used in Bay Networks VPN client) such a client cannot be run on the same computer as WinRoute. The VPN clients must be always run on computers behind WinRoute.

Norton Antivirus

Disable port 110 in Norton Antivirus configuration if you would run WinRoute Mail Server. Keeping port 110 in Norton will cause that computer won't start.

WinGate

Uninstall WinGate prior to installation. Uninstall both server and client software.

SyGate

Uninstall SyGate prior to installation. Uninstall both server and client software.

MS Proxy Server

Uninstall MS Proxy Server prior to installation. Uninstall both server and client software.

Microsoft Internet Connection Sharing

WinProxy from Ositis

All the software mentioned above, are using drivers that work incorrectly the with lower portions of the networking protocol operated by WinRoute.

Proxy client software issue

Client software would have a negative impact on the application software, (e.g. browser) it would not be possible to set it for direct access to the Internet. In fact you would think it was set up, but the installed client software would be trying to send the traffic to the proxy server.

Network card drivers issue

Try to use the most standard network interface cards. If you have special or 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.

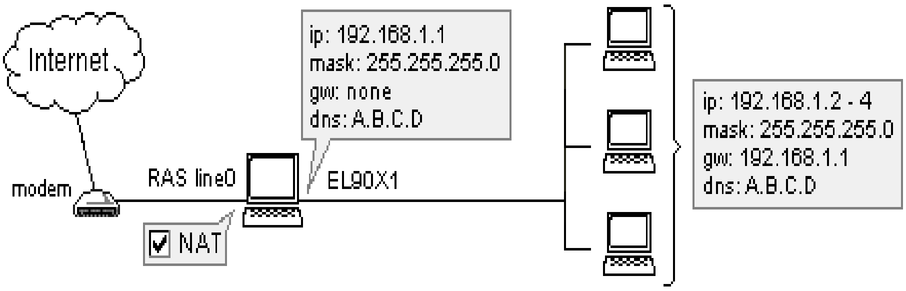
WinRoute is a fully neutral software router/firewall that does not require any client software running on client computers.

Connecting your network to the Internet

Dial-up connection (analogue or ISDN modem)

In this case, WinRoute must run on a computer that includes:

- modem attached to the phone or ISDN line

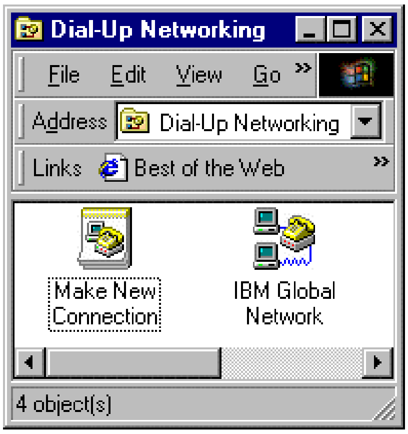


Before the connection

Before connecting to the Internet, double check that:

- TCP/IP protocol is properly installed and configured (see Quick checklist or Setting up network chapter)
- Dial-up networking (Windows 95/98) or RAS service (WindowsNT) 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 connect the dedicated computer to Internet 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 performed all the configuration described above:

1 Go to menu Settings->Interface table -you should see here 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 tab 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) linking to the internal network.***

Ethernet interface configuration

1 The Network Interface Card leading to the internal network must have an assigned IP address (private class) and NO assigned gateway!

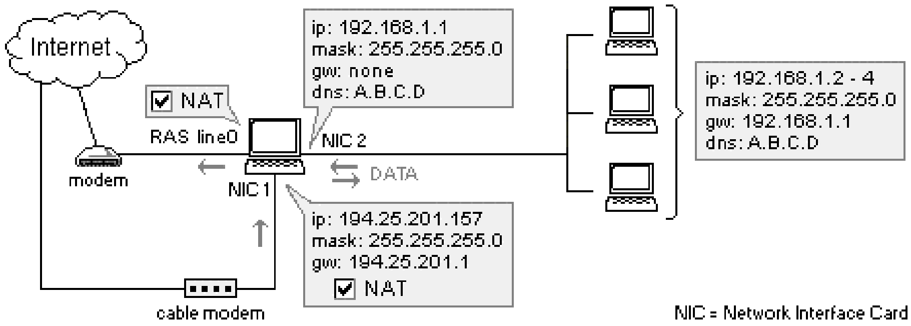
2 The DNS entries used for this interface are based on data from your ISP. If this data has not been provided to you, please contact your service provider.

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.

Unidirectional cable modem (modem up, cable down) connection

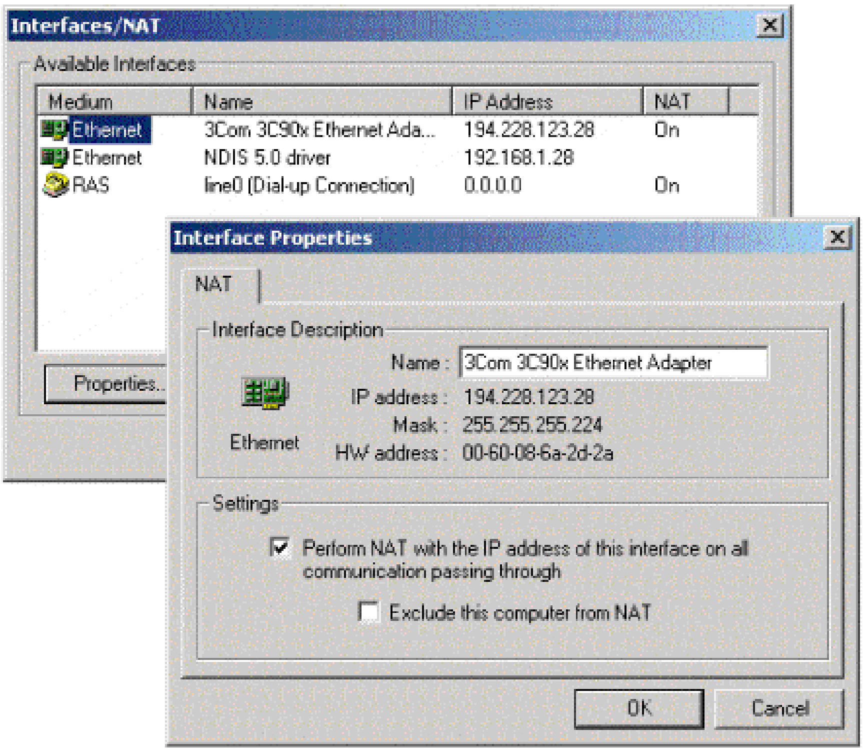
NOTE: This type of Internet connection is **not an "officially supported configuration"** as the settings **may vary** from ISP to ISP. However, we try to provide access solution to as many scenarios as possible. Many of our users have had success with the following settings when trying to establish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

In general, the data flow looks like as follows. Outgoing packets flow through your **dial-up** interface. On the way back they are routed **through a cable connection.** In fact, your ISP has to associate these two interfaces together. For this reason, we advice checking with your ISP before going ahead with your purchase of WinRoute.



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

2 Click on the network card linking to the Internet and click Properties. Check ON for "Perform NAT with IP address of the interface on all communications passing through".



Medium	Name	IP Address	NAT
Ethernet	3Com 3C90x Ethernet Ada...	194.228.123.28	On
Ethernet	NDIS 5.0 driver	192.168.1.28	
RAS	line0 (Dial-up Connection)	0.0.0.0	On

Interface Description

Ethernet

Name : 3Com 3C90x Ethernet Adapter
IP address : 194.228.123.28
Mask : 255.255.255.224
HW address : 00-60-08-6a-2d-2a

Settings

☑ Perform NAT with the IP address of this interface on all communication passing through

☐ Exclude this computer from NAT

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

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

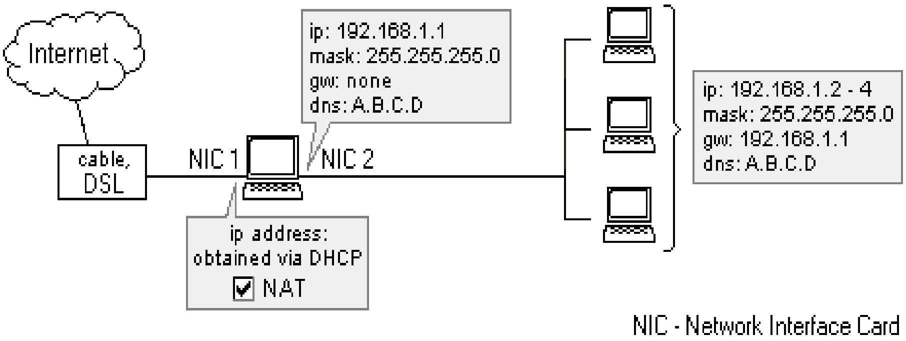
5 Check that there is **NO default gateway** set in TCP/IP properties of these internal interface(s), and that these interfaces(s) have assigned a **private class IP address(es)** (e.g. 192.168.1.1).

6 Check that the network card linking to the Internet is properly configured with the data from your ISP (TCP/IP properties).

In general - NAT should be switched ON on both interfaces linking to the Internet - RAS and network card.

xDSL connection

xDSL (ADSL, SDSL, ...) connection requires two Network Interface Cards (NIC) installed in the WinRoute computer. One NIC will link to the Internet (xDSL modem) while another NIC will link to the internal network.



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.

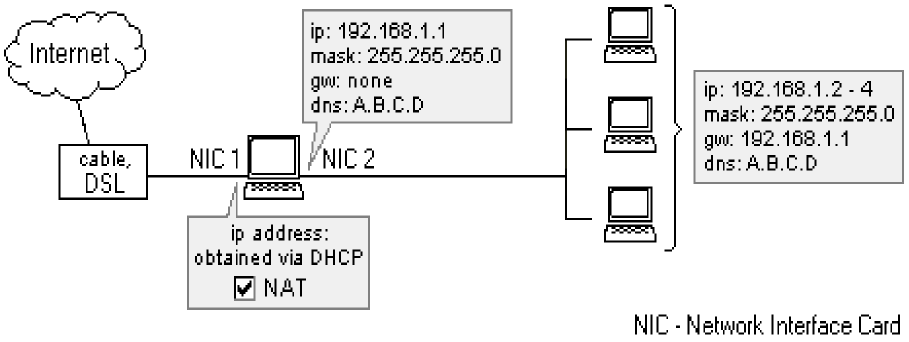
3 Check than NAT is NOT ON for the Interface linking to the internal network (go to the properties of this interface in Interface Table)

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 configured with data from your ISP. In case you have a dynamically assigned IP addresses leave the IP address settings blank.

Bidirectional cable modem connection

Cable modem connection requires two Network Card Interfaces (NIC) included in the WinRoute's 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) see please the appropriate chapter.



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)

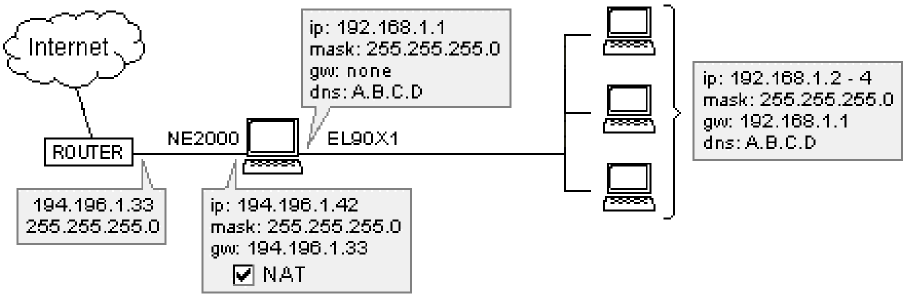
4 Check that there is NO gateway set in TCP/IP properties of the internal NIC (go to network settings) and that this NIC has assigned an internal (private class) IP address.

5 Check that the NIC linking to the Internet was properly configured 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. ***Quick Checklist*** , ***IP configuration*** etc.).

T1 or LAN connection

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



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 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.

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

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.

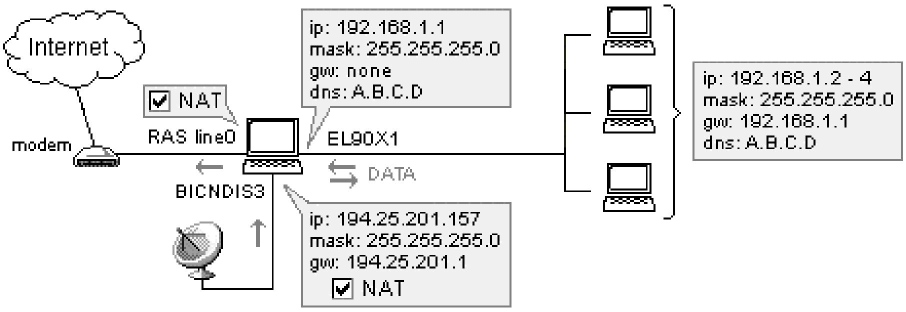
Data is going from your computer via modem to DirecPC Internet service where data is routed to its final destination. On the way back DirecPC associates the packets (data) coming to your computer with different data in order to route them via satellite dish.

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

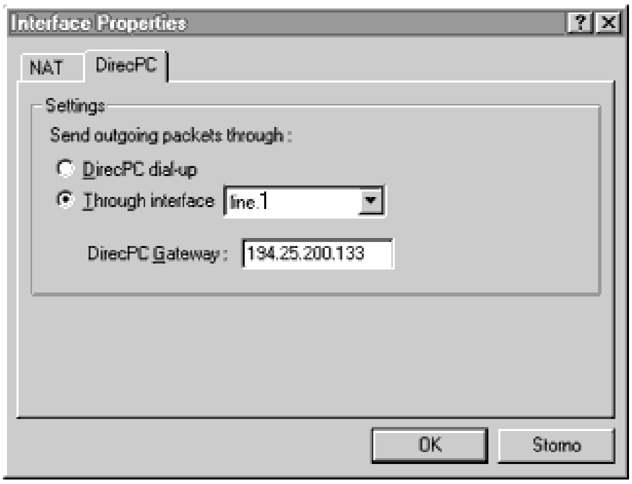


1 Go to menu **Settings->Interface Table**. You will see the RAS line interface (your modem) and DirecPC interface card.

2 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 IP address 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.



Interface Properties

NAT | DirecPC

Settings

Send outgoing packets through :

○ DirecPC dial-up

● Through interface line.1

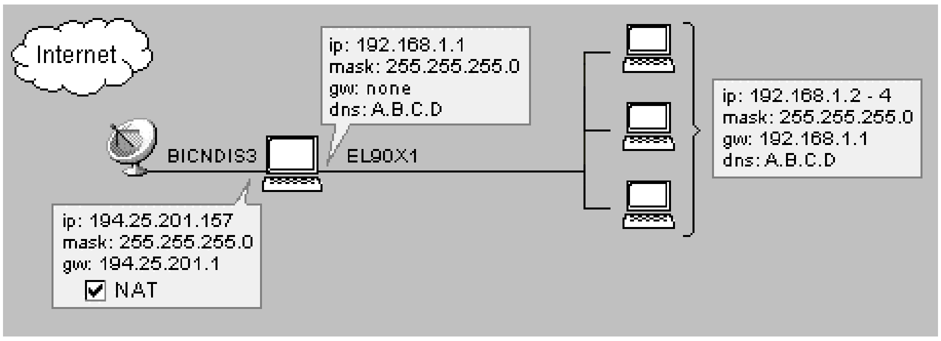
DirecPC Gateway : 194.25.200.133

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 TCP/IP properties of dial-up networking account created to connect 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.



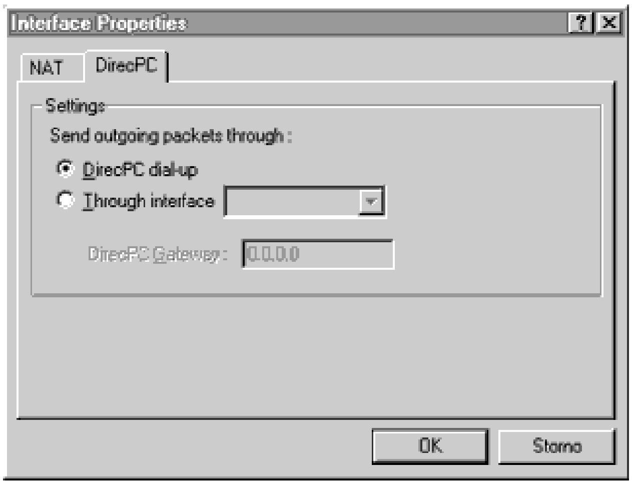
To use DirecPC dialer:

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

2 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".



Interface Properties

Settings

Send outgoing packets through :

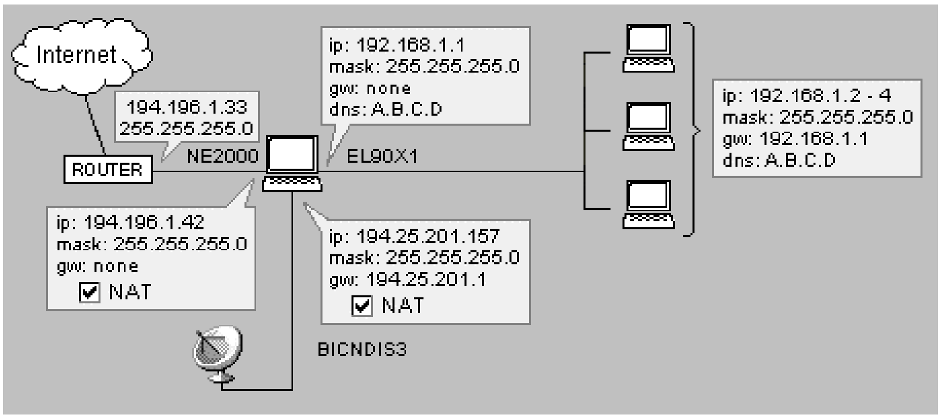
● DirecPC dial-up

○ Through interface

DirecPC Gateway : 0.0.0.0

3. Using Ethernet interface for uplink

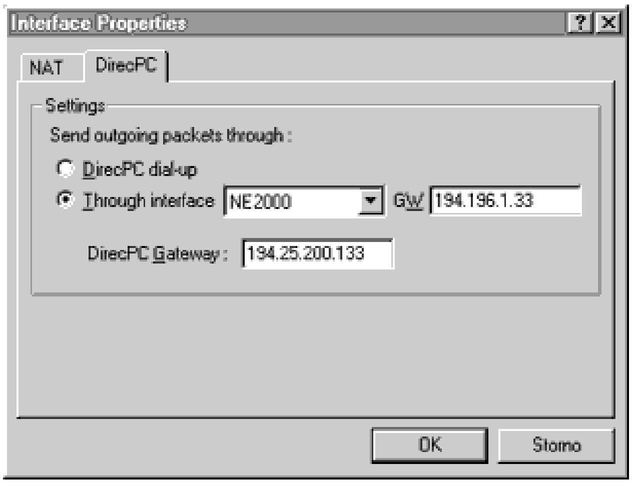
The third way is to use your Ethernet (cable) connection.



1 Go to the DirectPC interface card properties dialog.

2 · 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).



Settings

Send outgoing packets through :

○ DirecPC dial-up

● Through interface NE2000 GW 194.196.1.33

DirecPC Gateway : 194.25.200.133

WinRoute description

In This Chapter

Interface table

Interface table is a dialog where WinRoute displays all interfaces available in the computer that it could recognize. If you 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.

Interface table window:

Name of the interface

This name is for user purposes only. It helps you to recognize the interface (NIC / dial-up line, internal / external etc.). You can change the name by selecting “Properties” and rewriting the name.

IP address

The IP address 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 (or 0.0.0.0, when for example the dial-up line is not connected or the interface is not working properly).

NAT “On” or “Off”

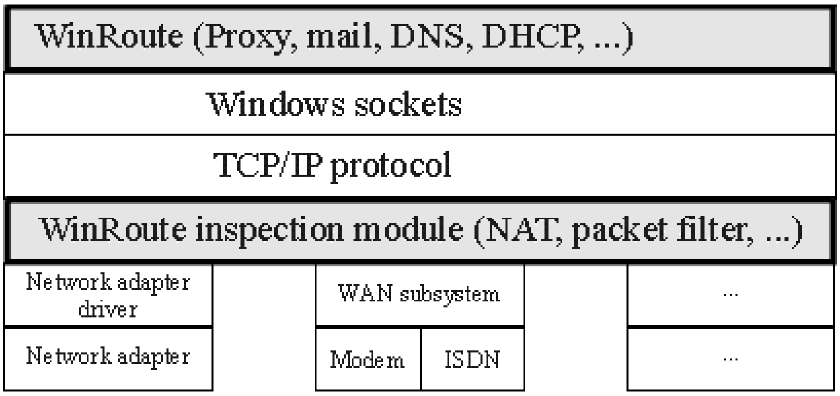
If NAT is set to be performed on the interface then “On” is displayed in this column. If NAT is set ON, but the WinRoute computer is excluded from NAT, you can see "On!" here. Otherwise, nothing is displayed.

NAT router

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.

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



This advanced design mades WinRoute's security almost **unbreakable**.

2. **Total Protocol Support**
   WinRoute is a **software router**. As such, unlike Proxy servers like WinGate or WinProxy, 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.

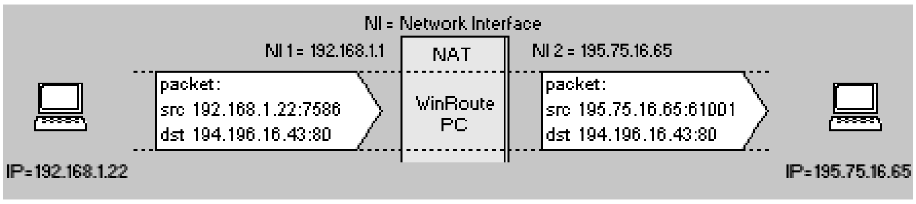
How NAT works

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 replaced by (public) IP address of the "NAT" computer.

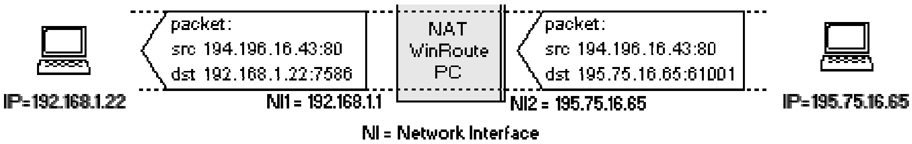
The NAT engine also creates a record table of information for each packet that passed through to the Internet.



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 that 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.

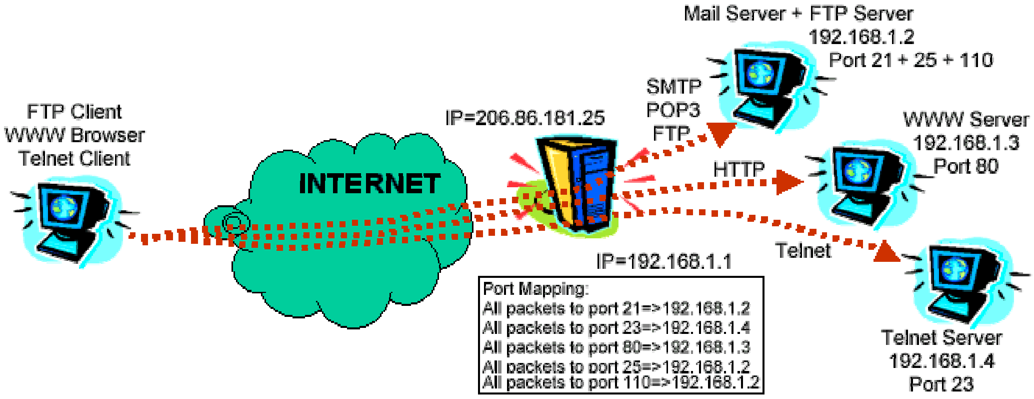


Port Mapping

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/or 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 type, 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 sent to the IP address of the protected network defined as the "Destination IP" in the table's entry and to the port defined as "Destination port".



Port Mapping:
All packets to port 21=>192.168.1.2
All packets to port 23=>192.168.1.4
All packets to port 80=>192.168.1.3
All packets to port 25=>192.168.1.2
All packets to port 110=>192.168.1.2

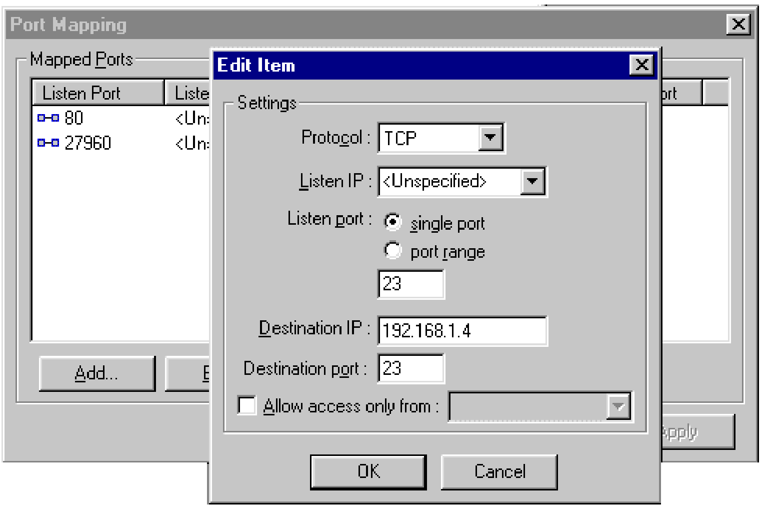
For example if you run a web server at internal IP 192.168.1.3 and you want to allow users from the Internet to access it. There will be requests from Internet users coming to your WinRoute computer with external IP address that is equal to the DNS record for your web server www.yourdomain.com. As all requests to web server are coming on port 80 you will set up port mapping saying that all TCP communication on port 80 will be diverted to the internal IP address 192.168.1.3.

Port Mapping Configuration

To set Port Mapping:

1. Go to menu *Settings->Advanced->Port Mapping*

2. Add a new port mapping entry:



Listen Port	Liste
80	<Un
27960	<Un

Protocol : TCP

Listen IP : <Unspecified>

Listen port : ● single port ○ port range

23

Destination IP : 192.168.1.4

Destination port : 23

□ Allow access only from :

Protocol

Select the protocol used by application/service. Some applications/services use TCP and UDP protocol together (e.g. WinRoute Administration program). Choose "TCP/UDP" in this case.

Listen IP

The IP address the incoming packets are coming to. Usually it is the IP address associated with your Internet interface. Note: you may have more than one IP addresses associated with this interface (if you have more web servers etc.). Choose "<Unspecified>" in this case. That means, all your public adresses will be listen to.

Generally, you can use the "<Unspecified>" option in any case (with one public address too), if you don't want to listen on one specific IP address only.

Listen Port

The port number the packets are coming to.

Destination IP

The IP address of the server in your local network answering incoming packets (web server, FTP server etc.).

Destination Port

The port on which the destination application is listening. Typically the same as the Listen Port number, but it's not required.

Allow access only from

You may specify the IP addresses (address group) which you want to allow access from. This is very important for increasing security, in case you set port mapping for remote management applications such as WinRoute Administration, PC Anywhere etc.

You must create an address group in "Address Groups" dialog box first.

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.

Example: 5 WWW servers scenario

As an example let consider that you want to run 5 web servers in your internal network where each of them has a separate domain associated with different IP addresses.

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.

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 a Port Mapping dialog. For each web server (domain) you will define:

- Listen IP address (public IP address associated with the domain)
- Listen port: 80 in our scenario
- Destination IP address: the IP address of the computer which runs the web server
- Destination port: 80 (for www)

For more examples about Advanced Port Mapping see More Advanced (Inter)networking chapter.

Multi NAT

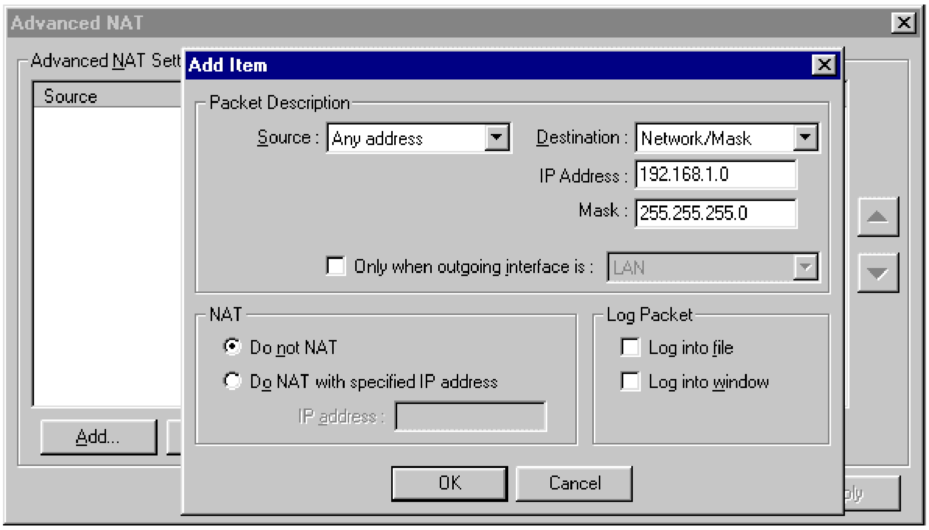
WinRoute allows simple **NAT** (Network Address Translation) and also more complicated settings. You may specify, based on **source** or **destination** IP address of the packet, that NAT would be provided with some **other IP address** (i.e. packets would look as if they originate from another IP address)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

Such settings are of great importance by setting up 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 you want to share **one** Internet access for all of them

You may find more examples of using "Advanced NAT stings" in More Advanced (Inter)networking chapter.

These features you can set in the Settings->Advanced->NAT menu.



Add Item

Packet Description

Source : Any address

Destination : Network/Mask

IP Address : 192.168.1.0

Mask : 255.255.255.0

□ Only when outgoing interface is : LAN

NAT

● Do not NAT

○ Do NAT with specified IP address

IP address :

Log Packet

□ Log into file

□ Log into window

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 to (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.

Only when outgoing interface is...

With this option, you can say that the defined NAT rules will be performed only in the case, that the packet goes through the specified interface. This is naturally only usable, if you have two or more interfaces with NAT on (e.g. if you use unidirectional cable modem or DirecPC).

Do not NAT

If selected, the packets passing through the Internet interface will not be changed.

Do NAT with specified IP address

If selected, the packets passing through will be changed as if they had originate from the desired IP address.

DHCP Server

In a network, each computer has to have the 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 larger number of workstations, it is difficult to avoid mistakes, eg. using an address twice - which may cause collisions and consequently also an incorrect function of the entire network.

To simplify the task, Dynamic Host Configuration Protocol has been developped. DHCP is used for a dynamic configuration of the TCP/IP protocol on computers. During start-up, the DHCP client computer sends a configuration request. When the DHCP server receives the request, it chooses TCP/IP configuration parameters for the requesting client. The parameters are IP address, network mask, default gateway, DNS server address, client's domain name, etc. Using these parameters, the server creates an answer and sends it to the client.

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

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

About WinRoute DHCP server

WinRoute contains a full-featured DHCP server which is able to dynamically assign TCP/IP configuration parameters to DHCP clients. If you want to use the WinRoute DHCP server, you must configure it accordingly (see bellow) and switch on the "Obtain IP address from DHCP server" option in the TCP/IP configuration of the client computers.

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 collide with the ones used in the fixed configurations.

DHCP configuration

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

Then, in the WinRoute Administration program:

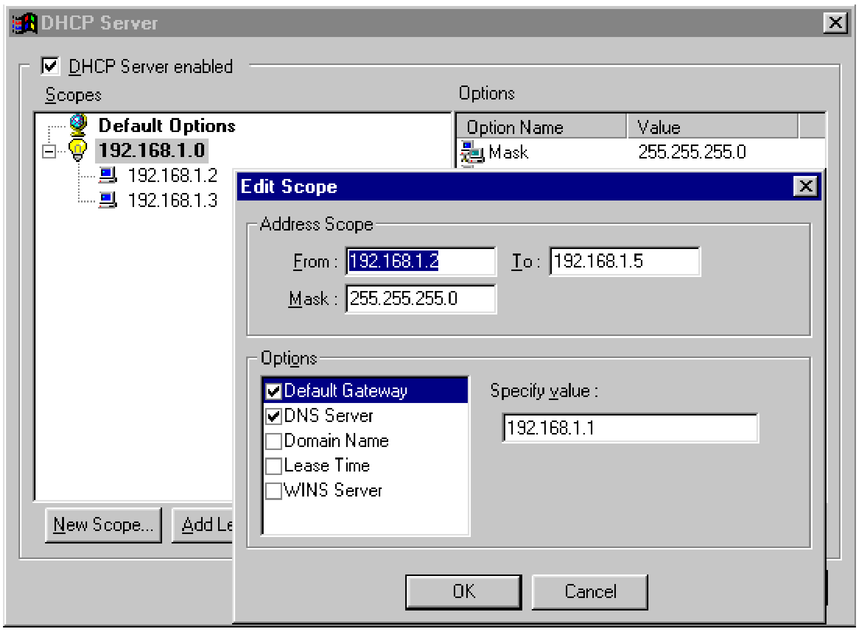
1. Go to menu Settings=>DHCP server.
2. Switch DHCP server ON (check the button DHCP Server Enabled) and press **Add New Scope** button.

3. Add Scope

Here you will specify the scope of IP addresses used by the DHCP server you want to give out to workstations. Remember that one IP address is already used by the WinRoute computer so avoid using that address. The IP address range must be of the same subnet. See below for example.

4. Specify Options!

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 and enter the appropriate information. Usually enter the information for the default gateway and DNS server (typically you would use WinRoute as DNS server) where you will use the IP address of your WinRoute computer (e.g. 192.168.1.1). You may leave the other options blank.



DHCP Server

☑ DHCP Server enabled

Scopes
- Default Options
- 192.168.1.0
  - 192.168.1.2
  - 192.168.1.3

Options

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

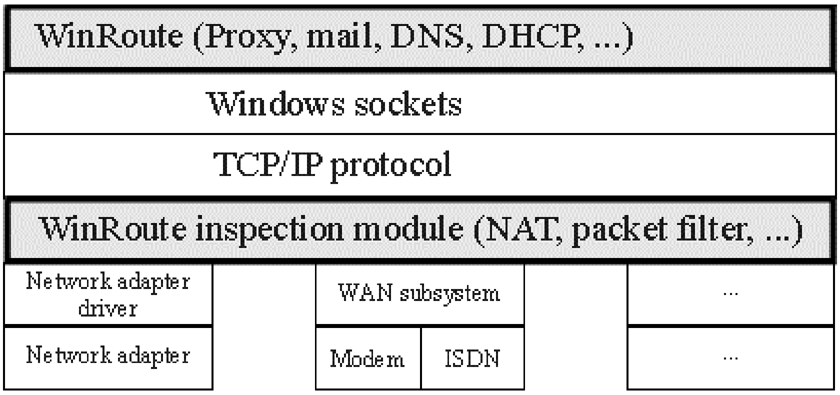
☑ Default Gateway
☑ DNS Server
□ Domain Name
□ Lease Time
□ WINS Server

Specify value : 192.168.1.1

Firewall

About WinRoute firewall

The basic firewall functionality is provided by NAT (Network Address Translator) itself. When using NAT, all packets are modified and checked before they reach your computer. As a result, there is almost no chance for anyone to break into your WinRoute computer and internal network.



Quite often you need to open certain **ports** or range of ports to allow access to local resources. As an example, using **PC Anywhere** for remote management. For this type of access, you want to control who is allowed to access the network and who is not.

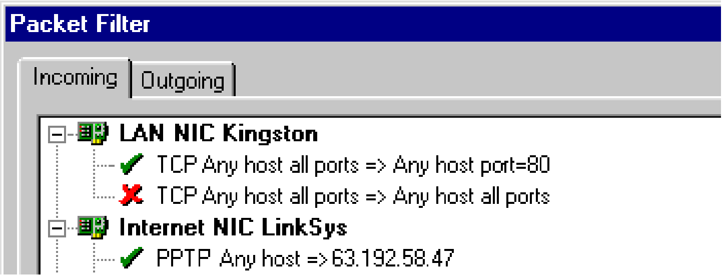
Similarly, you may want to limit some internal users from accessing the Internet. This is no problem for WinRoute. Included in the WinRoute application is a powerful **packet filter** based firewall. This easy to configure filter allows for very sophisticated security rules.

Packet filtering

You can define the packet filtering rules in the menu Settings->Advanced->Packet Filter.

Rules set per interface

The security rules are defined separately for individual computer you have in your computer. This is a very important feature when administering multi-segment networks.



- LAN NIC Kingston
  - ✓ TCP Any host all ports => Any host port=80
  - ✗ TCP Any host all ports => Any host all ports
- Internet NIC LinkSys
  - ✓ PPTP Any host => 63.192.58.47

Separate rules for Outgoing and Incoming packets

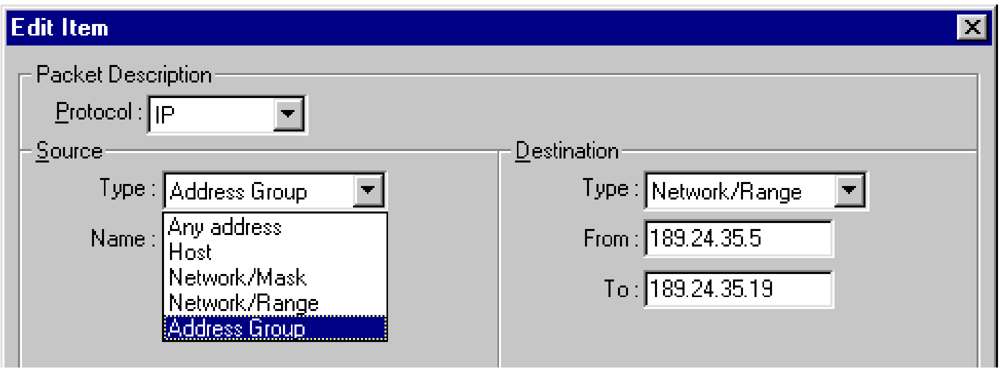
WinRoute applies specific rules for outgoing packets and incoming packets. A table is created within WinRoute for each interface. In this table both incoming packets and outgoing packets are recorded. In other words, each packet has two entries, one for outgoing and one for incoming.

RULES APPLICATION: From TOP to BOTTOM

Rules are defined in a list and applied from the Top to Bottom. After the packet arrives at the interface, it is checked against to the list of the defined criteria. The audit looks at the top criteria first and goes down the list to the lowest rule. When the packet meets the criteria of checked rule, the rule is applied and the rest of the rules are omitted.

Rules may be applied to:

- range of IP addresses
- a defined group of IP addresses (to define a group of users refer to the reference part of this manual)
- the whole subnet or network



Edit Item

Packet Description

Protocol : IP

Source

Type : Address Group

Name : Any address
Host
Network/Mask
Network/Range
Address Group

Destination

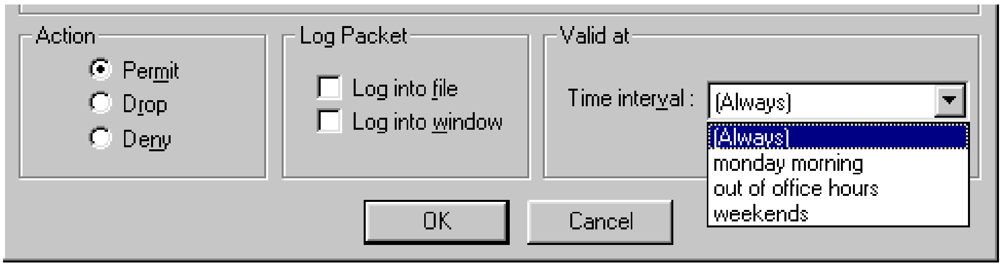
Type : Network/Range

From : 189.24.35.5

To : 189.24.35.19

Rules may be applied in predefined time zone

In some cases, it may be useful to apply specific rules during office hours and different criteria for after hour access. Or, you may want to allow certain users web access during the lunch time and during work hours, limit access to only specific resources.



Action

● Permit
○ Drop
○ Deny

Log Packet

□ Log into file
□ Log into window

Valid at

Time interval : (Always)

(Always)
monday morning
out of office hours
weekends

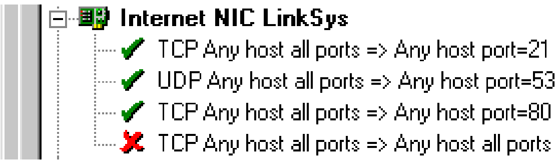
OK Cancel

Example:

Total control of user access: The network administrator wants the internal network to be inaccessible from the Internet. However, the are WWW, FTP and DNS servers behind WinRoute, that need a public access.

In this case, rules would be set in the following order for incoming packets:

1. Allow TCP packets from any host going to port 80 (for WWW)
2. Allow TCP packets from any host going to port 21 (for FTP)
3. Allow UDP packets from any host going to port 53 (for DNS queries)
4. Deny all other packets



Internet NIC LinkSys
- ✓ TCP Any host all ports => Any host port=21
- ✓ UDP Any host all ports => Any host port=53
- ✓ TCP Any host all ports => Any host port=80
- ✗ TCP Any host all ports => Any host all ports

If the arriving packet meets rule 1, 2 or 3, it is allowed to pass and rule 4 is not applied. If it does not meet 1 to 3, it is denied.

Security settings example

In this example, you want to apply the following rules:

- maximum security
- allow access to your web server
- allow communication with your SMTP server
- allow email to be picked up from the Internet at your mail server
- allow access to your FTP server

Maximum security:

Incoming tab

Protocol: TCP, Deny all incoming packets

Source IP – Any	Destination IP - Any
Source Port – Any	Destination Port - Any

This rule must always be the lowest from the rules available on the interface.

Allow access from the Internet to your web server:

Incoming tab

Protocol: TCP

Source IP - Any	Destination IP - IP address of the web server
Source Port - Any	Destination Port - 80

Allow access from the Internet to your FTP server.

Incoming tab

Protocol: TCP

Source IP - Any	Destination IP - IP address of the FTP server
Source Port - Any	Destination Port - 21

Source IP - Any	Destination IP - IP address of the FTP server
Source Port - Any	Destination Port - 20

Allow your SMTP server to communicate only with your relay SMTP server (at ISP):

Incoming tab

Protocol: TCP

Source IP - ISPs relay SMTP server	Destination IP - IP address of SMTP server in your LAN
Source Port - Any	Destination Port - 25

Outgoing Tab

Protocol: TCP

Source IP - your SMTP server	Destination IP - IP address of SMTP server at ISP
Source Port - Any	Destination Port - 25

Allow you to pick up the mail from your mail server from the Internat

Incoming Tab

Protocol: TCP

Source IP - Any	Destination IP - IP address of POP server in your LAN
Source Port - Any	Destination Port - 110

DNS forwarder

About DNS forwarder

Each computer connected to the Internet is identified by a unique numeric IP address. In order to connect to a computer in 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 (DNS) 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 able to answer DNS queries according to the user-defined HOSTS file. After DNS query arrives, WinRoute looks at the HOSTS file first prior to forwarding the DNS query to the Internet. If the corresponding record is found the query is answered by its value, if not is is forwarded to the Internet DNS server.

Setting up the DNS forwarder

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

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 the specific DNS servers(s)

Enter the numeric IP address of the DNS server(s) 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. You may enter here more addresses separated by the semicolon (;). This has a following meaning: normally, all the queries will be forwarded to the first server given. If this server becomes unaccessible, then the DNS forwarder will try the second one etc.

Enable cache for faster response of repeated queries

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.

HOSTS file

With this option checked, the DNS server is allowed to use data from the HOSTS file (located in your Windows directory) when answering the queries.

HOSTS file "Edit" button

This button launches an external text editor (typically Windows Notepad) in which you may edit the HOSTS file.

DHCP lease table

This option is only available if the WinRoute DHCP server is enabled. If checked, the DNS forwarder will look for the queried name to the DHCP lease table before forwarding the query to the Internet.

When resolving name from HOSTS file or lease table combine it with DNS domain below

If using a HOSTS file or DHCP lease table for DNS resolution (previous two options), write the name of your local domain (e.g. DOMAIN.COM) here.

This feature may be better understood from an example. Your domain is DOMAIN.COM and there is a computer called JOHN in your local network. In the HOSTS file you specified the IP address for the computer JOHN.

Then, when the DNS forwarder gets a query of "JOHN.DOMAIN.COM", it must recognize, that JOHN is a computer in the local network. So it finds the name "JOHN" e.g. in the HOSTS file, appends the specified domain name ("DOMAIN.COM") to it and answers the query correctly.

- ***Note that the cache only stores the answers which are of the "Name => IP address" type. The answers are stored until they expire. The expiration time is supplied by the DNS servers together with each answer.***

User accounts

What is a user account

WinRoute user accounts are primarily designed as e-mail accounts in the mail server. Additionaly, some users may log into WinRoute Administration program and view or change the WinRoute settings, depending on assigned access rights.

After WinRoute has been installed, there is one default user account named **Admin**. It's strongly recommended NOT TO DELETE THIS ACCOUNT and assign some "unforgettable" password to it. If you though forget it, see the Lost Admin Password chapter.

The users may be created and authenticated locally (in WinRoute), or imported from your NT domain and/or authenticated in the domain. It's recommended leave the basic Admin users to authenticate locally, to you could use it when solving any problems.

Adding, editing and deleting a user account

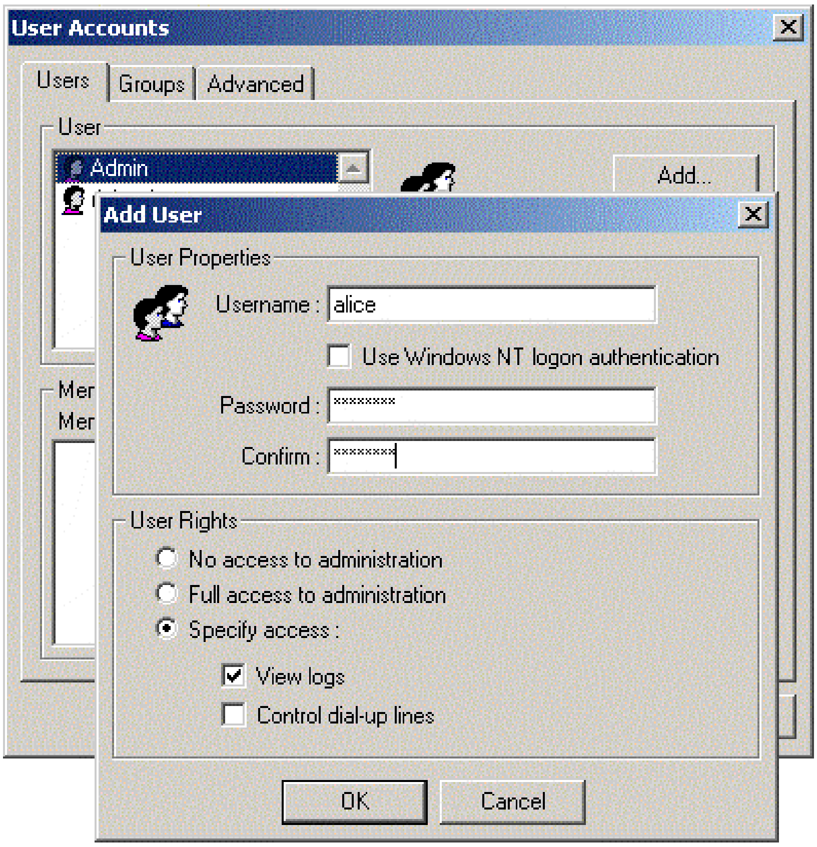
To add a new user:

1. Go to menu **Settings->Accounts**, **Users** tab
2. Press **Add** button
3. Define **user name** and **password** (or select to authenticate the user in Windows NT)
4. Assign desired **rights** to the user:

   The user will have no rights to administer WinRoute. In this case, he won't be able to log on to the WinRoute Administration program at all.

   The user will have full access to administration - will be able to modify any WinRoute settings.

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



User Properties

Username : alice

□ Use Windows NT logon authentication

Password : ********

Confirm : ********

User Rights

○ No access to administration

○ Full access to administration

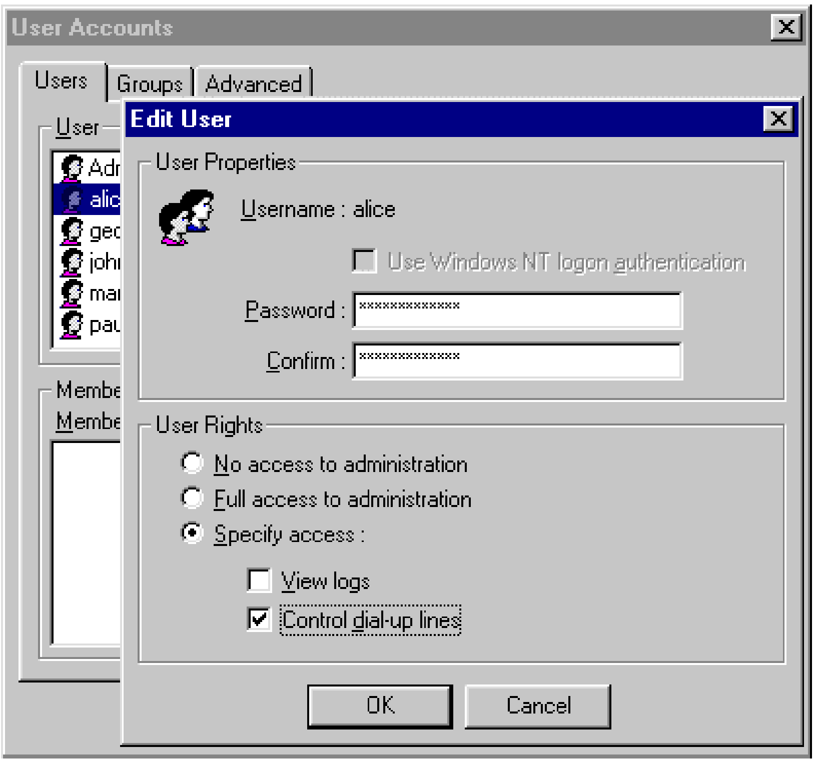
● Specify access :

☑ View logs

□ Control dial-up lines

Editing a user

You can change the desired user properties (e.g. password, access rights etc.) selecting the user and pressing the Edit button. The Edit User dialog is quite similar to the Add User dialog.



User Properties

Username : alice

□ Use Windows NT logon authentication

Password : *************

Confirm : *************

User Rights

○ No access to administration

○ Full access to administration

● Specify access :

□ View logs

☑ Control dial-up lines

Deleting a user

You can simply delete the user account by selecting the user and pressing the Remove button.

Groups of users

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

You may assign the group with **rights**. The are the same as in case of a single user.

Create the desired user groups in **Settings->Accounts**, **Groups** tab. The options are quite equal to single user options, except the password.

Note: The rights assigned to a group "overwrite" the rights assigned to users in it (they are of a highest priority).

Mail server

About WinRoute mail server

WinRoute includes a full-featured SMTP/POP3 mail server. You may use it the same way you would use the mail server of your ISP. WinRoute's Mail Server provides you the ability to send e-mail out to the Internet and to local users within your LAN. It also allows receiving of e-mail and storing it in the mailboxes of WinRoute users. WinRoute also includes a scheduler that allows you to start mail exchange at certain time (e.g. every hour).

If you don't want to use the WinRoute mail server

It is not necessary to use WinRoute 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 e-mail client software to communicate with the email server of your ISP.

Mail users

There are several basic rules about users, e-mail addresses and mailboxes in WinRoute.

One user = one mailbox...

Each user in 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 e-mail address is automatically user@domain (e.g. john@company.com).

One user = more addresses

To use different e-mail 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

For details, see please the chapter User accounts.

Example:

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

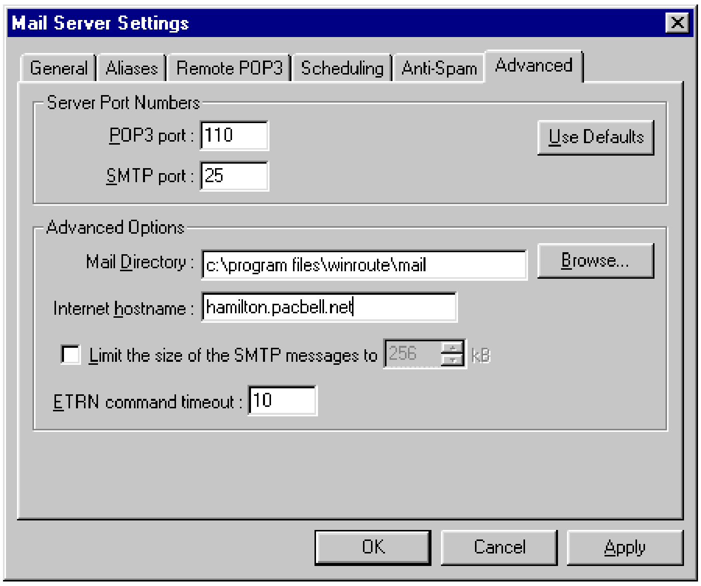
➢ ***Note: The mailboxes are kept in a separate directory, typically in c:\Program Files\WinRoute\Mail. The mailboxes are physically created AFTER the first email comes in.***

Mail server host name

Many of the ISP's mail servers require the Internet host name in the incoming SMTP packet (to avoid spamming etc.). You should set this information properly.

1 Go to menu Settings->Mail Server, Advanced tab

2 Enter the desired **host name** into the Internet hostname field. Usually this is the Internet name of the WinRoute computer, e.g. *host.isp.com*.



POP3 port : 110

SMTP port : 25

Mail Directory : c:\program files\winroute\mail

Internet hostname : hamilton.pacbell.net

□ Limit the size of the SMTP messages to 256 kB

ETRN command timeout : 10

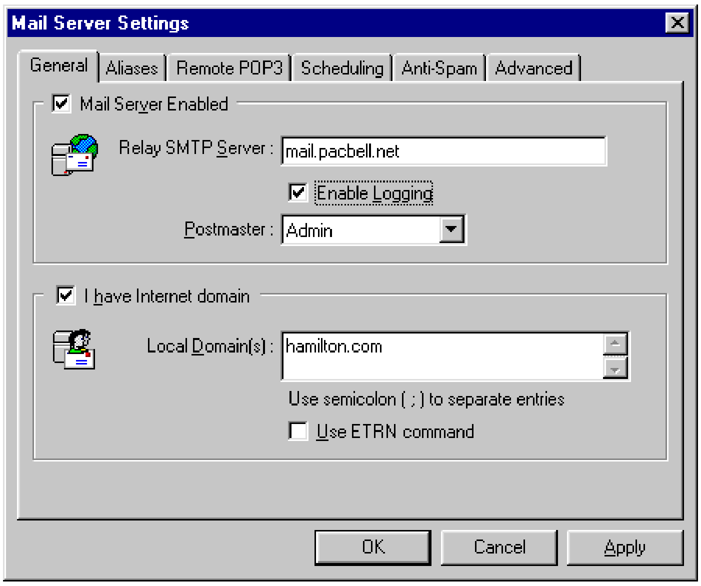
Sending e-mail

WinRoute acts as your **SMTP server** for outgoing mail. WinRoute uses the **relay SMTP server** of your ISP to send the mail out. In another words - all outgoing mail will be sent through the other mail server that you enter into the Relay SMTP Server field (usually the mail server of your ISP).

To set the relay SMTP server for outgoing mail:

1 Go to menu *Settings->Mail Server*

2 Enter the outgoing mail server of your ISP into the *Relay SMTP Server* field



Mail Server Settings

☑ Mail Server Enabled

Relay SMTP Server : mail.pacbell.net

☑ Enable Logging

Postmaster : Admin

☑ I have Internet domain

Local Domain(s) : hamilton.com

Use semicolon (;) to separate entries

☐ Use ETRN command

Receiving e-mail

One Internet domain

WinRoute's Mail Server is fully ***SMTP***[1] and ***POP3***[2] compliant. If you have an Internet domain registered, it can recevive the mail via SMTP or/and it can receive it from any Internet POP3 account.

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 INTERNAL IP address of your WinRoute box! Otherwise, the SMTP protocol will not be allowed to go through WinRoute's NAT!***

Based on your Internet connection you may consider the following:

1 Permanent connection

No specific setting is required. Just the entered the domain (e.g. hamilton.com).

[1] **SMTP** (Simple Mail Transfer Protocol) is used for direct communication between mail servers (such as the Winroute mail server and the mail server of your ISP) and for sending out the e-mail from your e-mail client software.

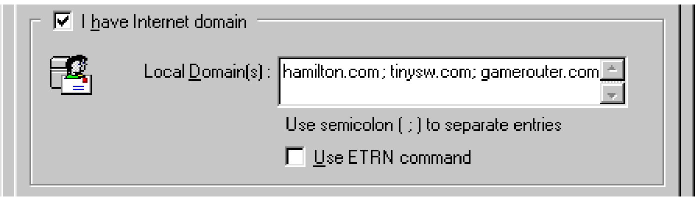
SMTP protocol uses the TCP protocol, port **25**. If you want to access the mail server running behind or on the WinRoute computer using this protocol (to allow other mail server to send the e-mail for you), you have to perform the **port mapping** for TCP protocol, port 25, to an IP address of the PC running the mail server (e.g. the internal interface of the WinRoute PC, if using the built-in mail server).

[2] **POP3** protocol is used mostly by e-mail client software to pick up the e-mail from mailboxes at the POP3 compliant mail server. WinRoute mail server has such capability too, i.e. it can pick up the e-mail automatically from any POP3 compliant mail server and further distribute it to the mailboxes of local recipients.

POP3 protocol uses a **TCP** protocol **port 110**. If you want to access using this protocol a POP3 mail server running behind or on the WinRoute computer (to pick up your e-mail FROM the Internet) you have to perform **Port Mapping** for TCP protocol, port 110 sent to **private class** IP address of the PC running the mail server.

2 Dial-up or ISDN connection (ETRN command)

Normally, the relay (ISP's) SMTP server can send the mail to your server at any time. In case you are not permanently connected, your email is temporary stored there. When you connect, your SMTP server can send the ETRN command to say "Now I'm ready, send me the mail". Allow this feature checking the **Use ETRN command** option.



☑ I have Internet domain

Local Domain(s) : hamilton.com; tinysw.com; gamerouter.com

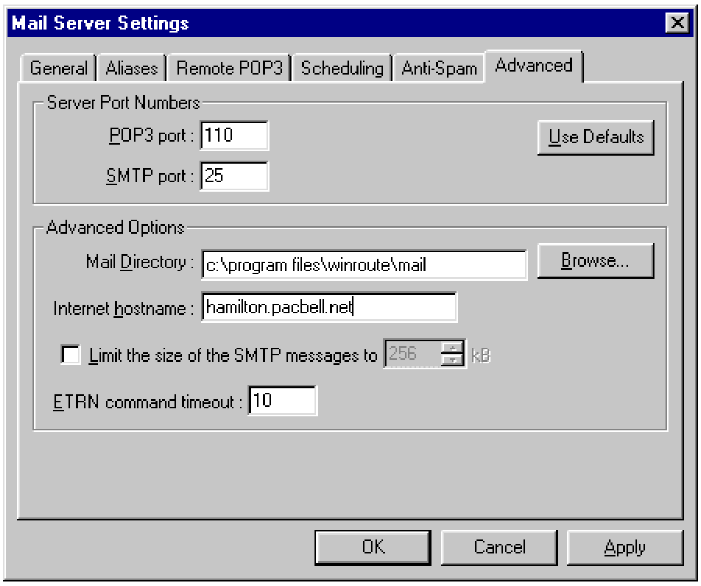
Use semicolon (;) to separate entries

□ Use ETRN command

ETRN command time out

There is no reply to an ETRN command, if the relay SMTP server doesn't have any mail to send. So there must be a timout defined, in which your SMTP server closes the connection, if it didn't receiver any mail.

You can set this timeout in the **Advanced** tab. The default value 10 seconds should be enough in most cases.



Mail Server Settings

Server Port Numbers

POP3 port : 110

SMTP port : 25

Advanced Options

Mail Directory : c:\program files\winroute\mail

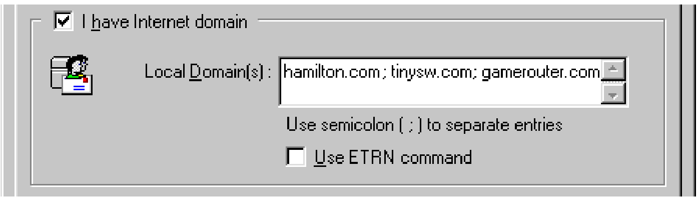
Internet hostname : hamilton.pacbell.net

□ Limit the size of the SMTP messages to 256 kB

ETRN command timeout : 10

Multiple domains

You may have several domains assigned. In that case, enter all of them into the Local Domain(s) in *Settings->Mail Server->General* tab and divide them by semicolon.



☑ I have Internet domain

Local Domain(s) : hamilton.com ; tinysw.com; gamerouter.com

Use semicolon (;) to separate entries

□ Use ETRN command

There are two ways the multiple domains can be arranged:

1 Each domain has assigned it's own mail server address

In this scenario you have to have more public IP address assigned to the WinRoute PC external (Internet) interface. For EACH of these adresses define the port mapping as follow:

Protocol: TCP

Listen IP: one of the external adresses

Listen port: 25

Destination IP: WinRoute PC INTERNAL address (e.g. 192.168.1.1)

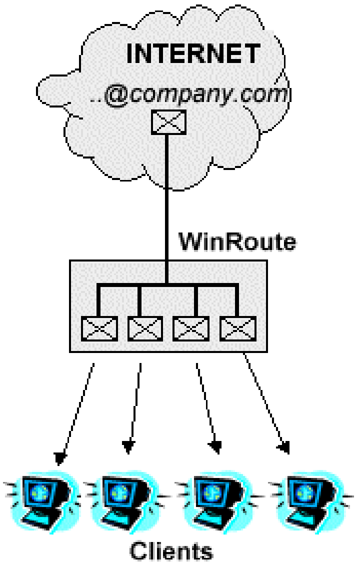
Destionation port: 25

2 All of the domains have assigned one common mail server address

Define only one port mapping (accordingly to the previous section) for this one address.

POP3 account for your domain

You may arrange with your ISP that all email for your domain come into a single POP3 account. WinRoute may check such account, pick up the messages and automatically distribute them into the mailboxes of local users.



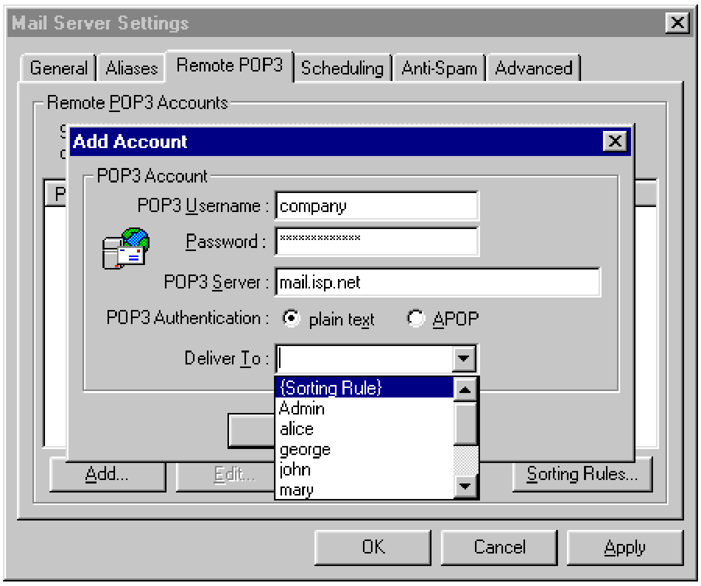
Example

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

You can set your WinRoute mail server to receive and distribute mail from such an account in the Remote POP3 tab of the Mail Server Settings dialog.

1 In the menu *Settings->Mail Server->Remote POP3*, add new account and enter its details (user name, password).

2 In "Deliver to:" field select "{Sorting Rule}"



POP3 Username : company

Password : **************

POP3 Server : mail.isp.net

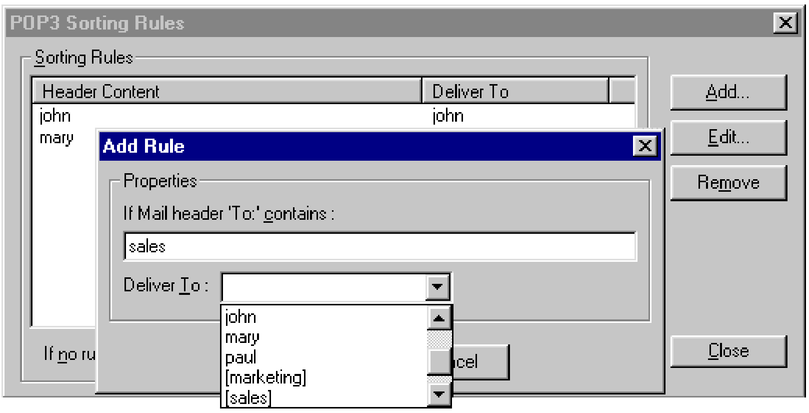
POP3 Authentication : ● plain text ○ APOP

Deliver To :

- {Sorting Rule}
- Admin
- alice
- george
- john
- mary

3 Press the Sorting Rules button and add new sorting criteria. This criteria is based on the "To:" field of the e-mail header. You can write a complete e-mail address (e.g. sales@company.com) or any substring of it (e.g. sales) here.

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



Header Content	Deliver To
john	john
mary	

If Mail header 'To:' contains : sales

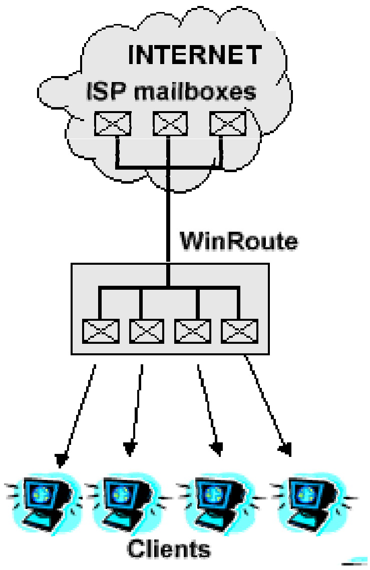
Deliver To :

- john
- mary
- paul
- [marketing]
- [sales]

TIP: You can also use the aliases (defined in the Aliases tab) here. These are not offered in the option list, but you can type any of them by hand into the "Deliver To:" field.

Several mailboxes at your ISP

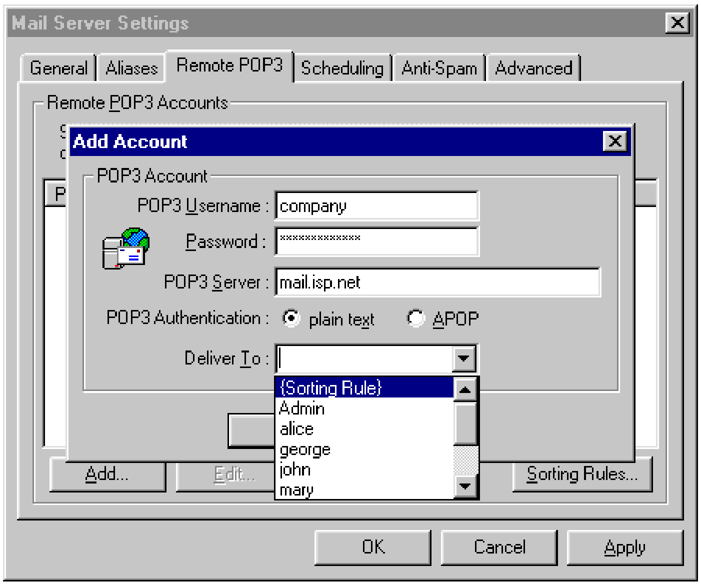
WinRoute can check several POP3 accounts (on the way described in the POP3 account for your domain section) at various ISPs and automatically deliver received email to the mailboxes of local recipients.



For each of your POP3 accounts, do the following:

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 or use an alias in this field.



POP3 Account

POP3 Username : company

Password : **************

POP3 Server : mail.isp.net

POP3 Authentication : ● plain text ○ APOP

Deliver To :

{Sorting Rule}
Admin
alice
george
john
mary

E-mail client software settings

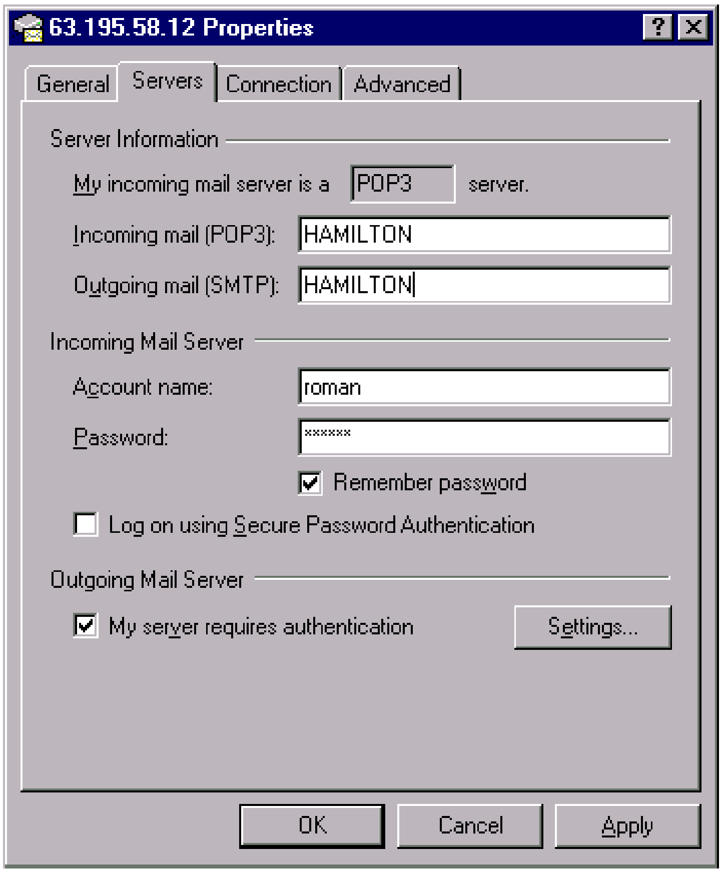
Going through WinRoute mail server

In order to use WinRoute mail server you must configure your **e-mail client software** properly. The WinRoute computer will act as the **Incoming** and **Outgoing** mail server. As a result, you must enter the WinRoute computer name or IP address 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 problems is with DNS resolution in your local network it may appear as if you are not using the WinRoute DNS server.

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 e-mail software.



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

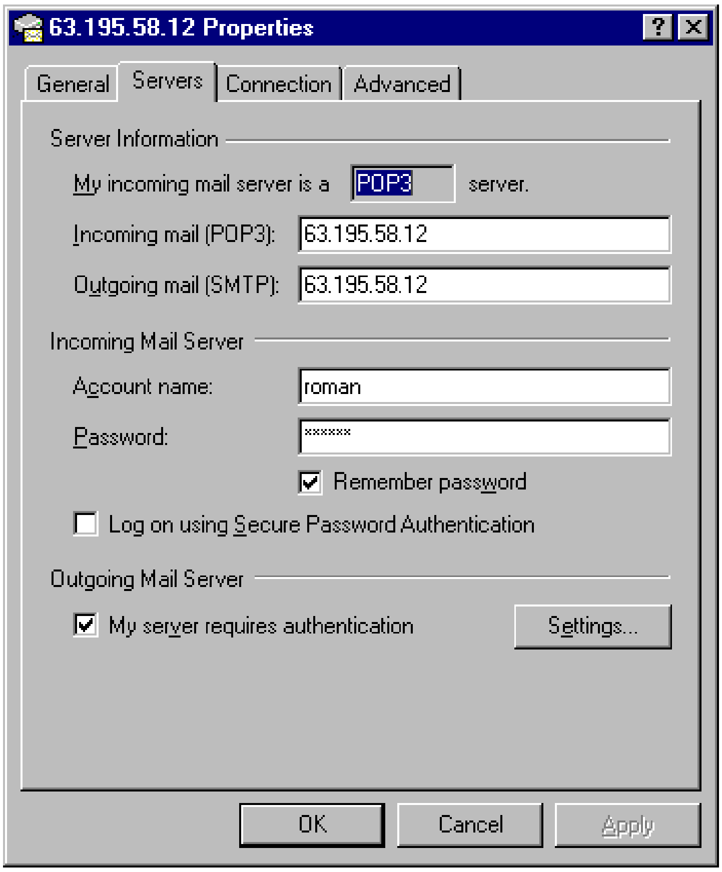
Outgoing Mail Server

☑ My server requires authentication

Bypassing WinRoute mail server

You may want to bypass WinRoute mail server and receive or send email directly from through the mail server of your ISP or any other mail server .

In such a case, please enter the appropriate name of these mail server(s) ISP into the Incoming and Outgoing mail server fields.



63.195.58.12 Properties

Server Information

My incoming mail server is a POP3 server.

Incoming mail (POP3): 63.195.58.12

Outgoing mail (SMTP): 63.195.58.12

Incoming Mail Server

Account name: roman

Password: ******

☑ Remember password

□ Log on using Secure Password Authentication

Outgoing Mail Server

☑ My server requires authentication

- ***Note! Do not set your email client software to use the Proxy Server! Use WinRoute's NAT for Internet access instead of Proxy and set your client software to have direct access to the Internet. Your inability to establish e-mail exchange means that NAT is not properly configured. Follow up the*** Quick CheckList ***to configure it properly!***

Aliases

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

Using **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 the group *[Sales]*.

Solution:

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

2. Add the following aliases:

support deliver to *John*

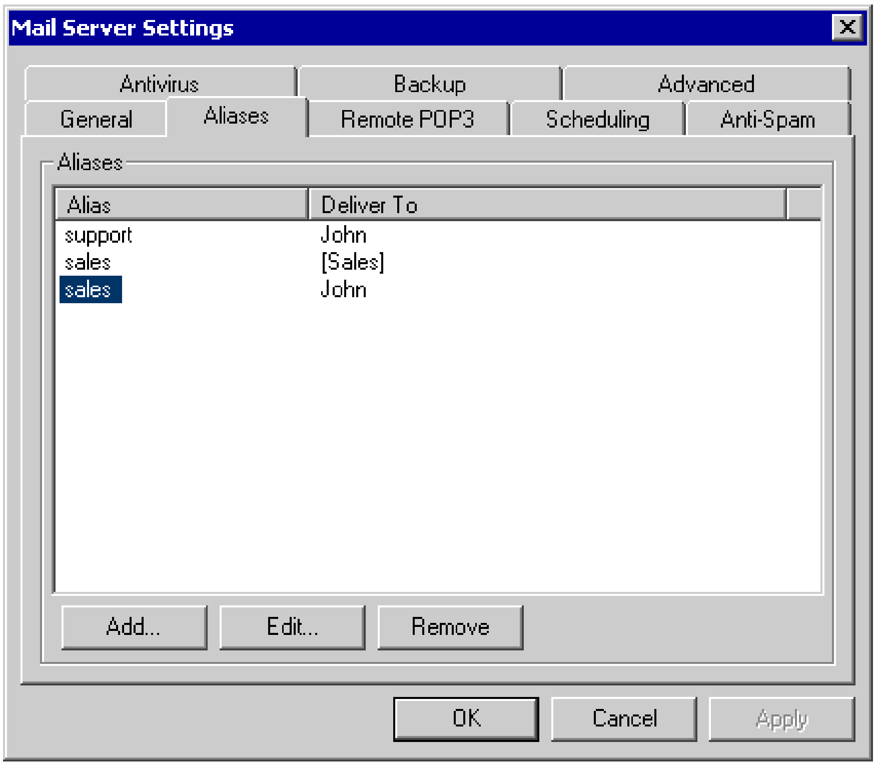
this will deliver all email for *support@...* to *John*

sales deliver to *John*

this will deliver all email for *sales@...* to a user *John*
(where "..." means any of the local domains - company.com or company2.com)

sales deliver to *[Sales]*

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



Alias	Deliver To
support	John
sales	[Sales]
sales	John

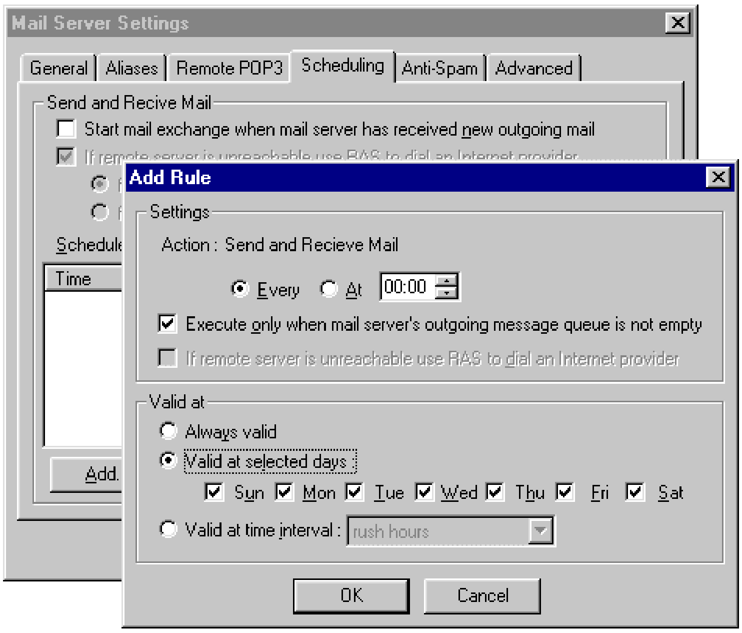
E-mail exchange scheduling

Scheduling in the Mail Server Settings gives you these options to set:

- regular intervals to check e-mail at your ISP (whether POP3 or SMTP using ETRN)
- rules for sending the outgoing e-mail
- the time intervals when the rules are valid. You may pre-define the time intervals in the menu *Settings->Advanced->Time intervals*

You may decide whether to send new outgoing e-mail immediately after the WinRoute mail server receives it or to send it out in a predefined time or period of time.

If using the dial-up Internet connection, you also may select whether the mail server should dial or not to start the e-mail exchange. If you select this option, WinRoute mail server will establish the connection every time it will want to send the e-mail. If you don't, the mail server will be able to send the mail only



Mail Server Settings

General | Aliases | Remote POP3 | Scheduling | Anti-Spam | Advanced

Send and Recive Mail

□ Start mail exchange when mail server has received new outgoing mail

☑ If remote server is unreachable use RAS to dial an Internet provider

Add Rule

Settings

Action : Send and Recieve Mail

● Every ○ At 00:00

☑ Execute only when mail server's outgoing message queue is not empty

□ If remote server is unreachable use RAS to dial an Internet provider

Valid at

○ Always valid

● Valid at selected days

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

○ Valid at time interval : rush hours

You may specify the whole calendar saying exactly when you would like to start the e-mail exchange. You may combine different rules to make your e-mail exchange 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 e-mail.

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

Proxy server

About WinRoute proxy server

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

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 passed through (like HTML pages, images and other kinds of files) in its **cache**.

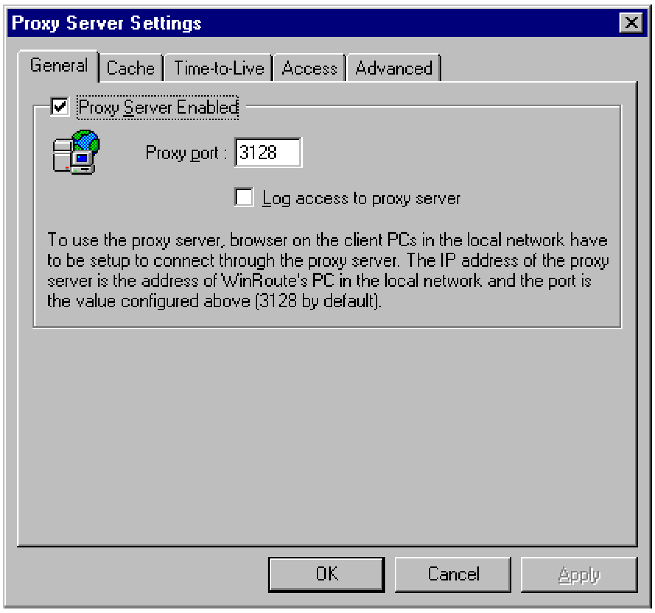
If the pages or images are requested again (by the same user or by someone else), the proxy server will provide the requested item from its cache. This **decreases** the load of the Internet connection and the entire operation is also much faster than downloading the objects from the Internet again.

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

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

1 In WinRoute Administration program select *Settings -> Proxy Settings -> General* tab. Check the "Proxy Server Enabled" option. Keep the original port number 3128 if possible.



Proxy Server Settings

☑ Proxy Server Enabled

Proxy port : 3128

□ Log access to proxy server

To use the proxy server, browser on the client PCs in the local network have to be setup to connect through the proxy server. The IP address of the proxy server is the address of WinRoute's PC in the local network and the port is the value configured above (3128 by default).

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

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

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 needed 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 a Proxy server log.

Proxy access control

WinRoute's Proxy server allows the administrator to control the 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.

Forcing users to use Proxy server

If you decide to use the Proxy's access control, you also need to block direct access to web pages, so that access through the proxy is the only remaining alternative for Internet browsing. To block direct access, define a packet filtering rule. To set up please refer to the ***Packet Filter*** (see "Security settings example" on page 48) section of WinRoute's user guide.

Configuring the Proxy access control

To configure the WinRoute's Proxy access control, go the "Access" tab of the Proxy Server Settings.

Access List

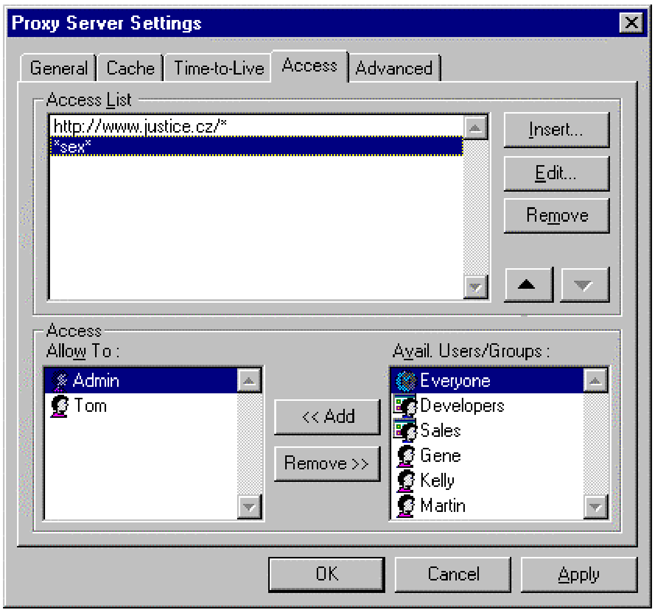
The list of URLs that are restricted. You may use asterisk as an wild card in the URL. For example, to match all computers in somedomain.com, use the string "*.somedomain.com". WinRoute 4. also uses sub string test to match the URLs, so for example the string "sex" matches the same set of URLs as the 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.



Access List:
http://www.justice.cz/*
sex

Allow To:
Admin
Tom

Avail. Users/Groups:
Everyone
Developers
Sales
Gene
Kelly
Martin

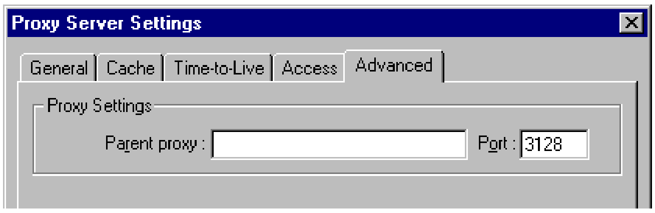
If a user tries to access a web page that falls in the category of restricted pages, the user will be prompted for authentication by his browser. WinRoute will check whether the user name and password are correct and whether the user is allowed to access the particular web page.

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.

Advanced properties

On the "Advanced" tab of the Proxy Server settings, you may instruct WinRoute to use a Parent Proxy server.



Parent proxy :

Port : 3128

Sometimes, you may have access to a proxy server that has a considerably **large cache** or that has a **fast** Internet connection, and your connection to that server is also reasonably fast, for example using an additional link besides the one you use for your own Internet connection.

To improve your data throughput, you may decide that WinRoute's Proxy should forward all request to this Parent Proxy server. To do this, simply enter the **Parent Proxy's** name and port number in the fields on the Advanced tab.

About cache

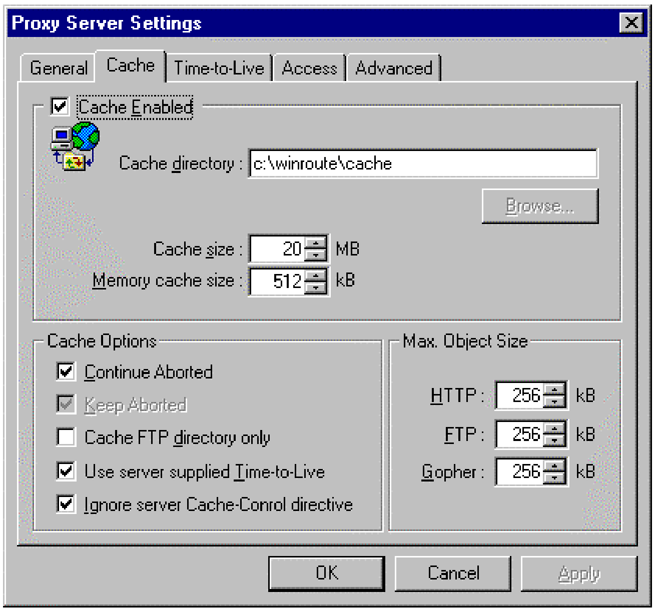
The WinRoute Proxy server uses a **very economic** way of storing data. All cached objects are stored in **one fixed-length file**. In contrast, the usual approach used by many proxy servers is to store each object in a separate file.

If the disc uses **large allocation units** (like FAT16), this method results in **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 object in one file saves a lot of disc space - as much as 10 times less space is required when compared to the usual approach. This means you need less disc space or you may use the same space much more efficiently.

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

Cache directory : c:\winroute\cache

Cache size : 20 MB

Memory cache size : 512 kB

Cache Options

☑ Continue Aborted

☑ Keep Aborted

□ Cache FTP directory only

☑ Use server supplied Time-to-Live

☑ Ignore server Cache-Conrol directive

Max. Object Size

HTTP : 256 kB

FTP : 256 kB

Gopher : 256 kB

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 2048 megabytes (2 GB).

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

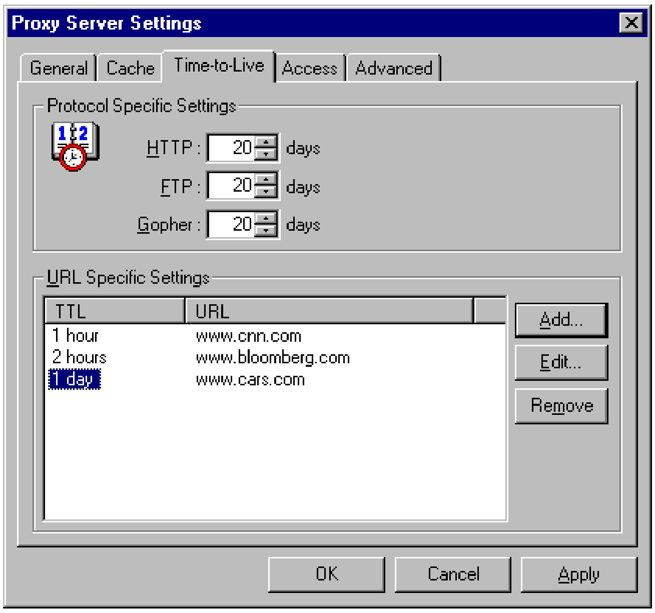
If the contents of a web page changes very often, the author of the page may decide to set the "no-cache" directive for it. This is a very useful feature, however some web sites use the directive much too often, sometimes for all their pages, effectively eliminating the purpose of proxy servers. If you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



Protocol Specific Settings

HTTP : 20 days

FTP : 20 days

Gopher : 20 days

URL Specific Settings

TTL	URL
1 hour	www.cnn.com
2 hours	www.bloomberg.com
1 day	www.cars.com

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 Pro 4.x, 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 "Use server supplied Time-to-Live" on Cache tab enabled, the server supplied TTL has higher priority than "URL Specific Settings".

Proxy versus NAT

Even though **NAT** gives you excellent Internet connection capability, sometimes you may find it useful to force users to use the **Proxy Server** in order to access the **World Wide Web**. Usually, this is e.g. if you have 56KB/s access for the entire company and the Cache becomes very useful or if you want to **control user access** through a built-in **URL filter**.

In order to use a Proxy to access the WWW, you have to set all user browsers to use the proxy server. Keep in mind the default WinRoute proxy server port is **3128**. You may change this port number if necessary. The users will be able to bypass the proxy and go directly to the Internet through the NAT. To avoid this you will need to set the packet filtering. Please see the ***Packet filtering*** (on page 45) and ***Security settings examples*** (see "Security settings example" on page 48) chapters.

Logs and packets analyses

About WinRoute logs

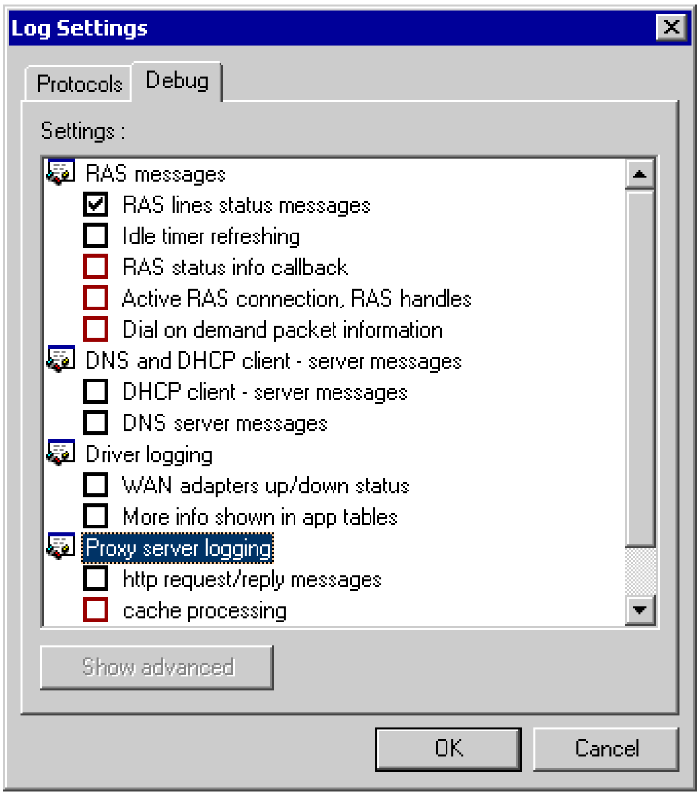
The logs in WinRoute is a tool that makes you possible to see what is going "inside WinRoute". You can monitor the packets going through it, user activities, NAT and firewall actioning etc.

Select the log type you want to view in the View -> Logs menu. The window will appear and when an event comes, the appropriate log appears in it. You can save the logs into a file or clear the window by pressing the right button on it and choosing the action from the context menu.

Debug log

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

The Debug log can contain very wide scale of information. But in most cases, you will want to know certain information only (e.g. DNS queries). For this reason, the Debug log can be customized (you can choose, what information you want to display in it). Select the desired packets/events in the Settings -> Advanced -> Debug Info dialog.



RAS messages
- ☑ RAS lines status messages
- □ Idle timer refreshing
- □ RAS status info callback
- □ Active RAS connection, RAS handles
- □ Dial on demand packet information

DNS and DHCP client - server messages
- □ DHCP client - server messages
- □ DNS server messages

Driver logging
- □ WAN adapters up/down status
- □ More info shown in app tables

Proxy server logging
- □ http request/reply messages
- □ cache processing

In the Protocols tab you can select, which protocol's packets will be debugged. In the Debug tab, there can be selected more detailed information (independent on the protocols choosen). Pressing the "Show advanced" button the further options will appear.

Beside of these selected information, Debug log shows some information as default, e.g. version info and running modules every time the WinRoute Engine has started, unsuccessfull login attempts.

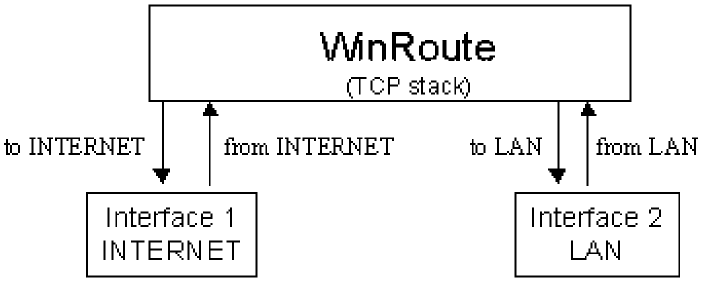
How to read the Debug log?

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 - protocol dependent information (e.g. TCP protocol, SYN flag means that the connection is being established now)

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
```

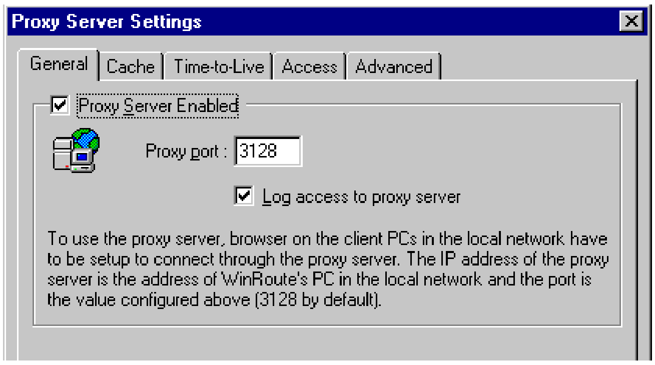
HTTP (Proxy) log

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 use this log, you should force your users to go through the Proxy server. See the ***Proxy server*** chapters.

You also have to enable the Proxy server logging (check this option in Settings -> Proxy Server -> General tab.



☑ Proxy Server Enabled

Proxy port : 3128

☑ Log access to proxy server

To use the proxy server, browser on the client PCs in the local network have to be setup to connect through the proxy server. The IP address of the proxy server is the address of WinRoute's PC in the local network and the port is the value configured above (3128 by default).

How to read the HTTP (Proxy) log?

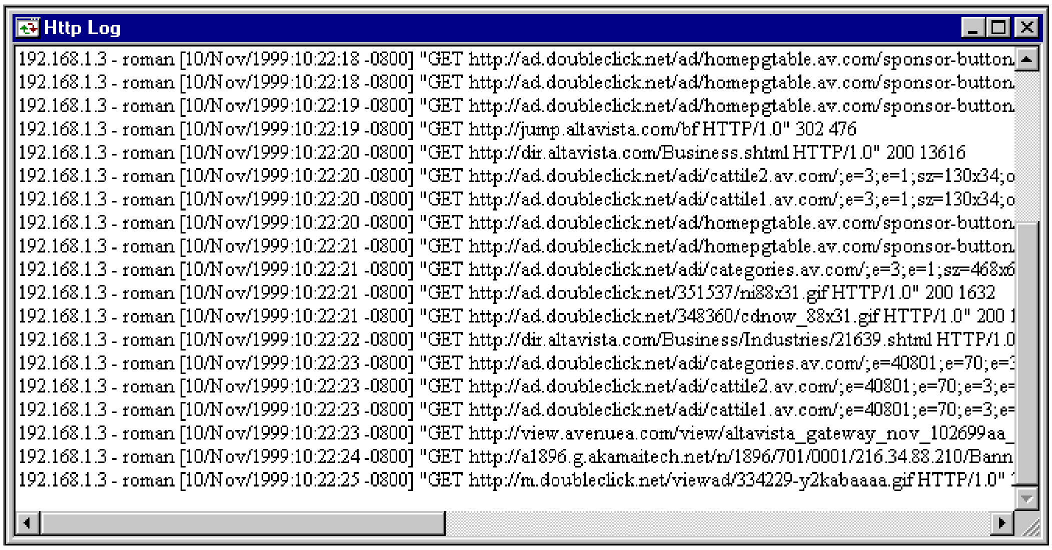
```
192.168.1.3 - roman [10/Nov/1999:10:22:20 -0800] "GET
http://dir.altavista.com/Business.shtml HTTP/1.0" 200 13616
```

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

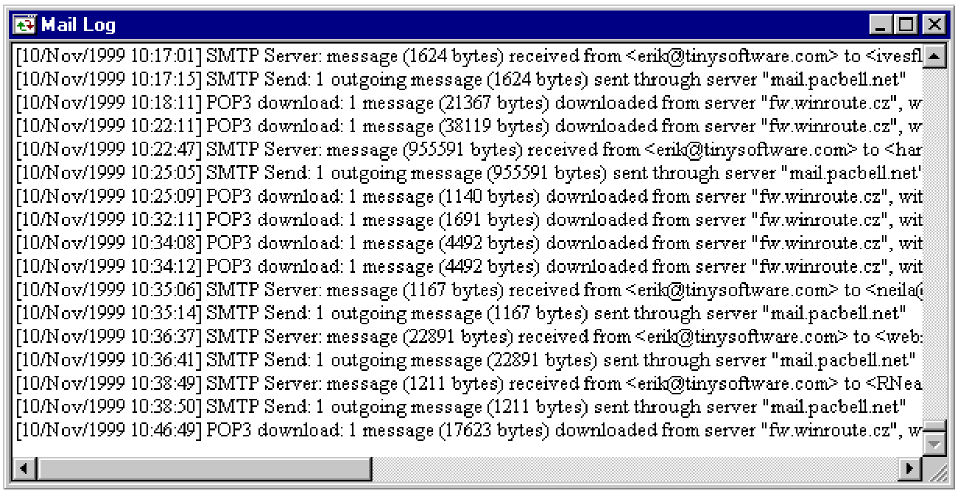
GET "http..." - the HTTP query for the target



```
192.168.1.3 - roman [10/Nov/1999:10:22:18 -0800] "GET http://ad.doubleclick.net/ad/homepgtable.av.com/sponsor-button
192.168.1.3 - roman [10/Nov/1999:10:22:18 -0800] "GET http://ad.doubleclick.net/ad/homepgtable.av.com/sponsor-button
192.168.1.3 - roman [10/Nov/1999:10:22:19 -0800] "GET http://ad.doubleclick.net/ad/homepgtable.av.com/sponsor-button
192.168.1.3 - roman [10/Nov/1999:10:22:19 -0800] "GET http://jump.altavista.com/bf HTTP/1.0" 302 476
192.168.1.3 - roman [10/Nov/1999:10:22:20 -0800] "GET http://dir.altavista.com/Business.shtml HTTP/1.0" 200 13616
192.168.1.3 - roman [10/Nov/1999:10:22:20 -0800] "GET http://ad.doubleclick.net/adi/cattile2.av.com/;e=3;e=1;sz=130x34;o
192.168.1.3 - roman [10/Nov/1999:10:22:20 -0800] "GET http://ad.doubleclick.net/adi/cattile1.av.com/;e=3;e=1;sz=130x34;o
192.168.1.3 - roman [10/Nov/1999:10:22:20 -0800] "GET http://ad.doubleclick.net/ad/homepgtable.av.com/sponsor-button
192.168.1.3 - roman [10/Nov/1999:10:22:21 -0800] "GET http://ad.doubleclick.net/ad/homepgtable.av.com/sponsor-button
192.168.1.3 - roman [10/Nov/1999:10:22:21 -0800] "GET http://ad.doubleclick.net/adi/categories.av.com/;e=3;e=1;sz=468x6
192.168.1.3 - roman [10/Nov/1999:10:22:21 -0800] "GET http://ad.doubleclick.net/351537/ni88x31.gif HTTP/1.0" 200 1632
192.168.1.3 - roman [10/Nov/1999:10:22:21 -0800] "GET http://ad.doubleclick.net/348360/cdnow_88x31.gif HTTP/1.0" 200 1
192.168.1.3 - roman [10/Nov/1999:10:22:22 -0800] "GET http://dir.altavista.com/Business/Industries/21639.shtml HTTP/1.0
192.168.1.3 - roman [10/Nov/1999:10:22:23 -0800] "GET http://ad.doubleclick.net/adi/categories.av.com/;e=40801;e=70;e=
192.168.1.3 - roman [10/Nov/1999:10:22:23 -0800] "GET http://ad.doubleclick.net/adi/cattile2.av.com/;e=40801;e=70;e=3;e=
192.168.1.3 - roman [10/Nov/1999:10:22:23 -0800] "GET http://ad.doubleclick.net/adi/cattile1.av.com/;e=40801;e=70;e=3;e=
192.168.1.3 - roman [10/Nov/1999:10:22:23 -0800] "GET http://view.avenuea.com/view/altavista_gateway_nov_102699aa_
192.168.1.3 - roman [10/Nov/1999:10:22:24 -0800] "GET http://a1896.g.akamaitech.net/n/1896/701/0001/216.34.88.210/Bann
192.168.1.3 - roman [10/Nov/1999:10:22:25 -0800] "GET http://m.doubleclick.net/viewad/334229-y2kabaaaa.gif HTTP/1.0"
```

Mail log

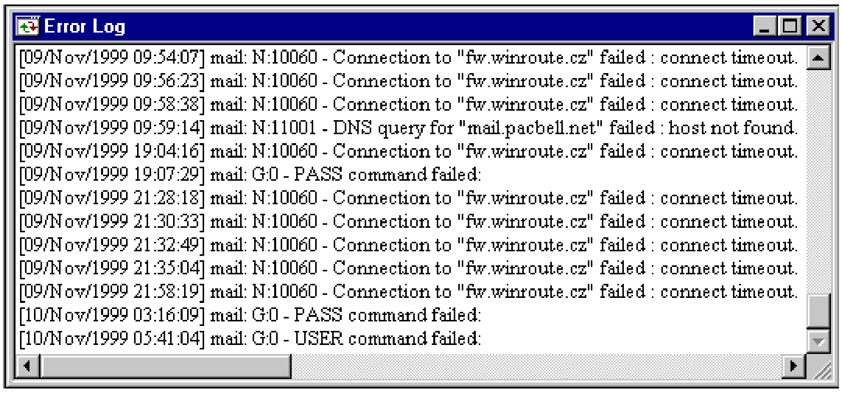
Mail log records all operations of WinRoute's built-in Mail Server. You can see how many messages were sent, received, where the messages were sent etc. All operations are time stamped.



```
[10/Nov/1999 10:17:01] SMTP Server: message (1624 bytes) received from <erik@tinysoftware.com> to <ivesfl
[10/Nov/1999 10:17:15] SMTP Send: 1 outgoing message (1624 bytes) sent through server "mail.pacbell.net"
[10/Nov/1999 10:18:11] POP3 download: 1 message (21367 bytes) downloaded from server "fw.winroute.cz", w
[10/Nov/1999 10:22:11] POP3 download: 1 message (38119 bytes) downloaded from server "fw.winroute.cz", w
[10/Nov/1999 10:22:47] SMTP Server: message (955591 bytes) received from <erik@tinysoftware.com> to <har
[10/Nov/1999 10:25:05] SMTP Send: 1 outgoing message (955591 bytes) sent through server "mail.pacbell.net'
[10/Nov/1999 10:25:09] POP3 download: 1 message (1140 bytes) downloaded from server "fw.winroute.cz", wit
[10/Nov/1999 10:32:11] POP3 download: 1 message (1691 bytes) downloaded from server "fw.winroute.cz", wit
[10/Nov/1999 10:34:08] POP3 download: 1 message (4492 bytes) downloaded from server "fw.winroute.cz", wit
[10/Nov/1999 10:34:12] POP3 download: 1 message (4492 bytes) downloaded from server "fw.winroute.cz", wit
[10/Nov/1999 10:35:06] SMTP Server: message (1167 bytes) received from <erik@tinysoftware.com> to <neila(
[10/Nov/1999 10:35:14] SMTP Send: 1 outgoing message (1167 bytes) sent through server "mail.pacbell.net"
[10/Nov/1999 10:36:37] SMTP Server: message (22891 bytes) received from <erik@tinysoftware.com> to <web:
[10/Nov/1999 10:36:41] SMTP Send: 1 outgoing message (22891 bytes) sent through server "mail.pacbell.net"
[10/Nov/1999 10:38:49] SMTP Server: message (1211 bytes) received from <erik@tinysoftware.com> to <RNea
[10/Nov/1999 10:38:50] SMTP Send: 1 outgoing message (1211 bytes) sent through server "mail.pacbell.net"
[10/Nov/1999 10:46:49] POP3 download: 1 message (17623 bytes) downloaded from server "fw.winroute.cz", w
```

Error log

Error log displays all unsuccessful operations in any of WinRoute modules running. You can see here e.g. RAS errors, unsuccessful connections to the relay SMTP or DNS server etc.



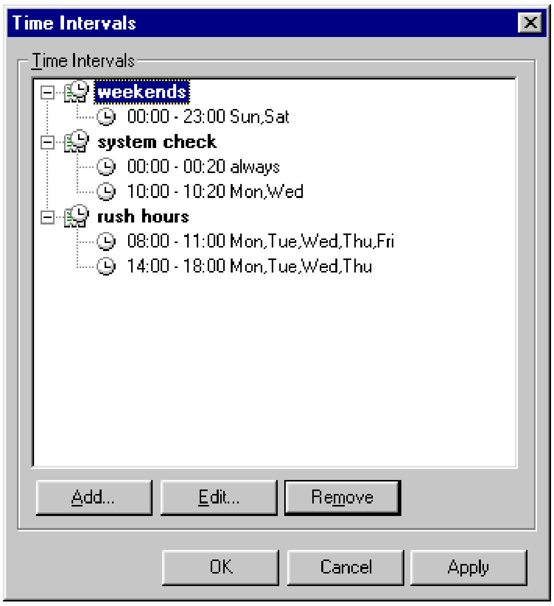
```
[09/Nov/1999 09:54:07] mail: N:10060 - Connection to "fw.winroute.cz" failed : connect timeout.
[09/Nov/1999 09:56:23] mail: N:10060 - Connection to "fw.winroute.cz" failed : connect timeout.
[09/Nov/1999 09:58:38] mail: N:10060 - Connection to "fw.winroute.cz" failed : connect timeout.
[09/Nov/1999 09:59:14] mail: N:11001 - DNS query for "mail.pacbell.net" failed : host not found.
[09/Nov/1999 19:04:16] mail: N:10060 - Connection to "fw.winroute.cz" failed : connect timeout.
[09/Nov/1999 19:07:29] mail: G:0 - PASS command failed:
[09/Nov/1999 21:28:18] mail: N:10060 - Connection to "fw.winroute.cz" failed : connect timeout.
[09/Nov/1999 21:30:33] mail: N:10060 - Connection to "fw.winroute.cz" failed : connect timeout.
[09/Nov/1999 21:32:49] mail: N:10060 - Connection to "fw.winroute.cz" failed : connect timeout.
[09/Nov/1999 21:35:04] mail: N:10060 - Connection to "fw.winroute.cz" failed : connect timeout.
[09/Nov/1999 21:58:19] mail: N:10060 - Connection to "fw.winroute.cz" failed : connect timeout.
[10/Nov/1999 03:16:09] mail: G:0 - PASS command failed:
[10/Nov/1999 05:41:04] mail: G:0 - USER command failed:
```

Time intervals

You may define Time intervals in order to say when or how often should certain actions be performed. These actions may be:

- Packet filtering
- E-mail exchange (sending and receiving)
- Connecting to the Internet (in case of the dial-up connection)
- Advanced NAT settings

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



weekends
00:00 - 23:00 Sun,Sat
system check
00:00 - 00:20 always
10:00 - 10:20 Mon,Wed
rush hours
08:00 - 11:00 Mon,Tue,Wed,Thu,Fri
14:00 - 18:00 Mon,Tue,Wed,Thu

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

To define time zone:

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

2 Name the time zone

3 Add the desired time intervals

Configuration examples

In This Chapter

Connecting multiple networks

WinRoute is a software router that allows you to connect multiple networks to the Internet via a single shared connection (and IP address). Usually it is difficult to connect and configure the connection of such environments. WinRoute provides the ability to connect these networks with ease.

These networks might be connected together via Ethernet, Token Ring, Frame Relay, Microsoft PPTP or even dial-up RAS line. It means that companies with more branch offices may benefit from their private WAN securely connected to the Internet via a single connection with minimum cost.

Connecting Cascaded Segments via 1 IP address

The network setup, where all networks that are to be connected do not lead directly to the WinRoute computer, while being connected through a router is called Cascaded Segments.

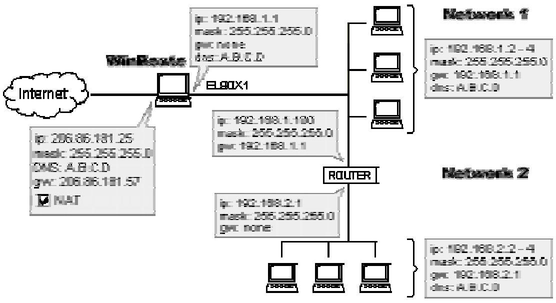
The router between the two networks may be any hardware router, WindowsNT or any Windows 95/98 computer with WinRoute. WinRoute will act as a router with or without performing NAT.

In general it is necessary to "tell" the WinRoute computer where the incoming packets for the other networks will be sent, while for the outgoing packets there must be similar link on the router (dividing two networks) specifying where the packets going out from the second network would be sent to. This can be done through adding of new routes - one at the WinRoute computer (for incoming packets) and one at the router (for outgoing packets).

- ROUTE at the WinRoute computer (member of Network1) will route IP packets for the other network (Network2) to the outer connecting Network1 and Network2. This router will carry these packets further.
- DEFAULT ROUTE at the router (connecting both networks) will route all packets coming from Network2 to Internet to the WinRoute computer. Then WinRoute will provide NAT on these packets and send them to the Internet.

Example

Our example has two networks 192.168.1.x and 192.168.2.x., the router is at 192.168.1.100 in the first and 192.168.2.1 in the second of them.



Network1 (primary network) settings

- You have to tell the WinRoute computer: "All packets going to network 192.168.2.0 have to go through the router 192.168.1.100":
- In Windows NT/2000, go to the Command prompt and enter the following command:

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

In Windows 9x, add the command

```
route add 192.168.2.0 mask 255.255.255.0 192.168.1.100
```

to the AUTOEXEC.BAT file and restart the computer.

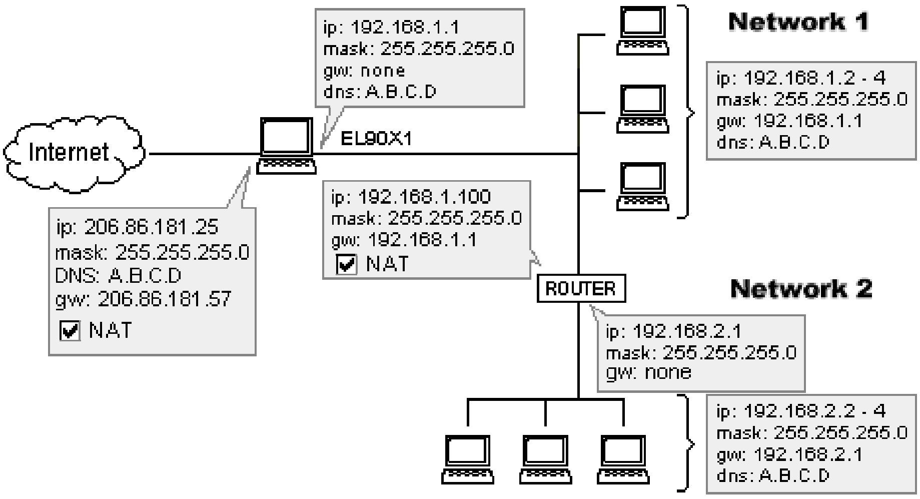
- On the router 192.168.1.100, the default route must lead to the computer with WinRoute, i.e. 192.168.1.1. In another words you have to tell your router to route all packets going to the Internet through the WinRoute PC.
- All other network settings will be done as described in other chapters (Setting up network).

Network2 (secondary network) settings

All settings can stay the same as before WinRoute installation. The Default gateway at all Network2 computers should be set to Network2 IP address of the router (192.168.2.1 in our example).

NAT between Network1 and Network2

You may use WinRoute with NAT turned "ON" to connect the primary and secondary networks. The secondary network will look like a single computer, you will benefit from easier administration and higher security of the secondary network. You should properly set Advanced NAT settings as you would not like to modify the traffic between these two networks.



Advanced NAT settings on the WinRoute PC dividing Network1 and Network2

Based in the destination IP address you will or won't perform NAT. In our example, if the destination of the packet are on the 192.168.1.0 network then packets won't be NATed. This will allow for communication between these two networks as if there was no NAT.

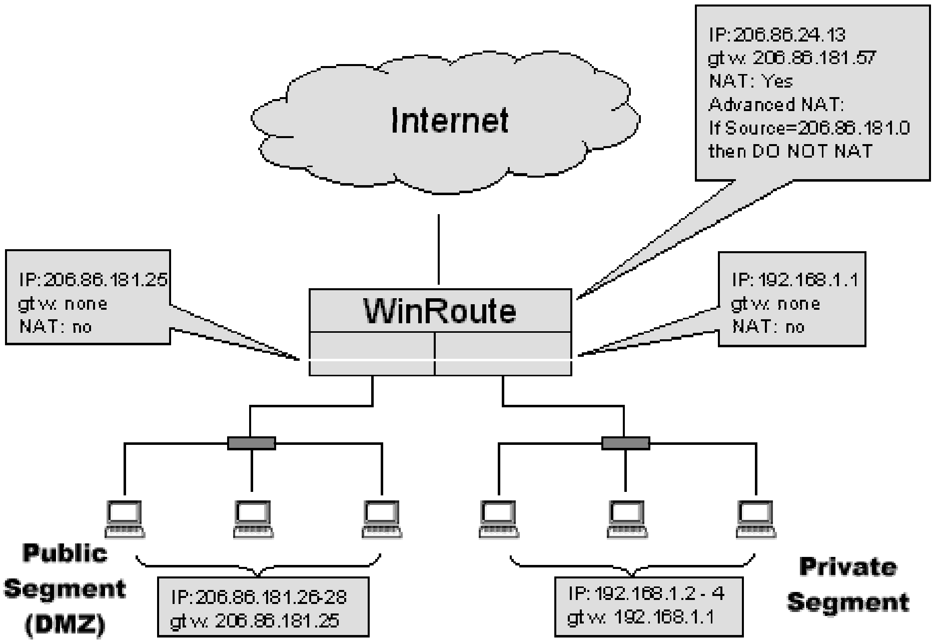
For the network settings follow the rules described in the rest of this mannual.

Connecting public and private segments (DMZ)

A private segment consists of computers that use private type of Internet addresses. Such addresses are dedicated to private networks and cannot be used in the Internet. That's why you need NAT to translate these private addresses into public which allows you a way to connect the Internet. The computers with private address are not directly accessible from the outside (Internet).

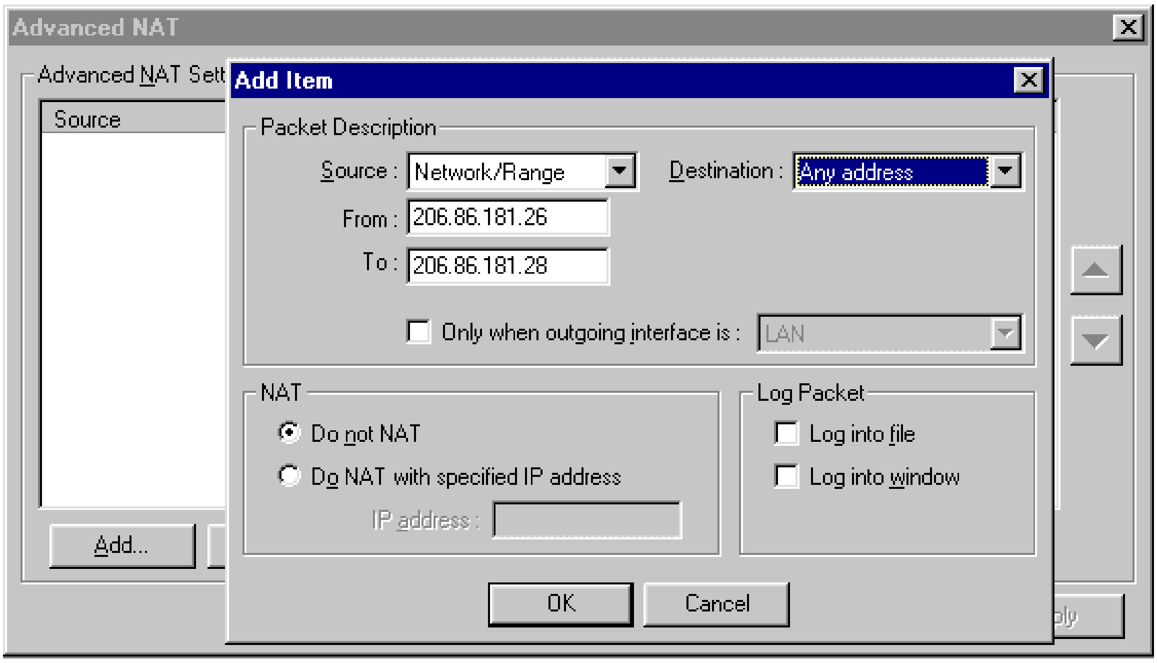
A public segment (so-called Demilitarized Zone, abb. DMZ) consists of computers where each computer has a public IP address. These systems, if your security rules allow, may be directly accessible from the Internet

Each segment has to have its own network interface in the WinRoute computer. Then the WinRoute engine allows your private and public segments to share one Internet connection.



WinRoute settings

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



Source : Network/Range

Destination : Any address

From : 206.86.181.26

To : 206.86.181.28

□ Only when outgoing interface is : LAN

NAT

● Do not NAT

○ Do NAT with specified IP address

IP address :

Log Packet

□ Log into file

□ Log into window

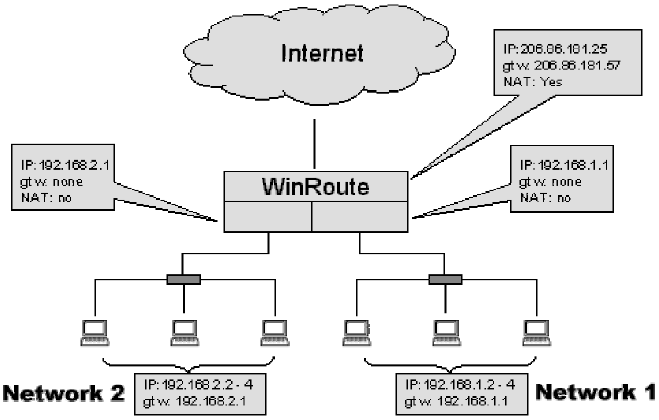
Public and Private networks settings

There are no special settings for the computers in these segments. Use the IP address of the WinRoute computer's interface linking to the appropriate segment as the default gateway in this segment. For the public segment the only difference is that you will use public IP addresses on it.

Sharing the connection with 1 IP address by two networks

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 connected to 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 ON
IP address is set according your ISP
Gateway is set according your ISP

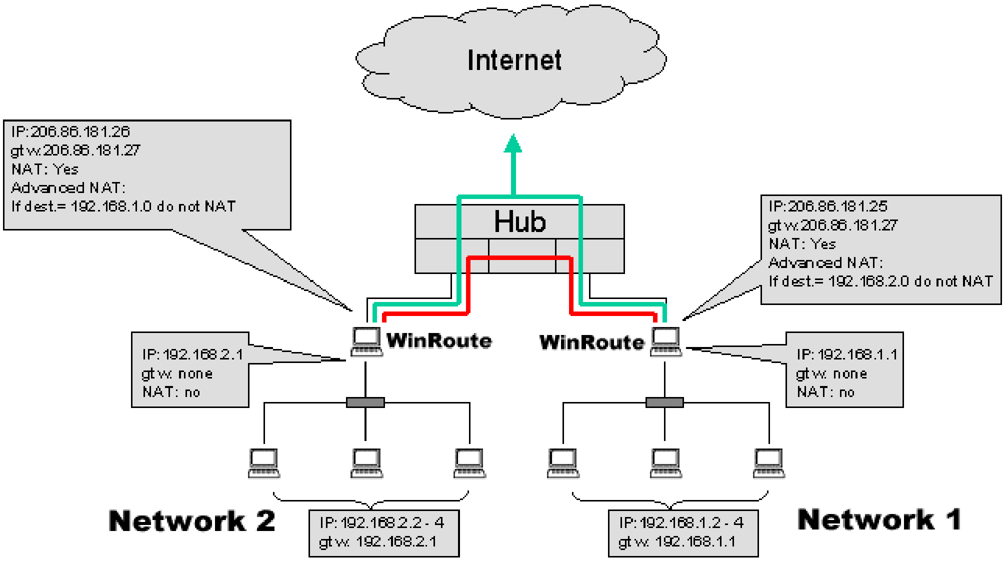
Internal interfaces

NAT is OFF
There is NO default gateway set on both interfaces
IP address is set to the internal type (e.g.192.168.1.1 and 192.168.2.1)

The traffic arriving from each subnet is routed to the other subnet or to the Internet and vice versa.

Sharing the connection with 2 IP addresses by 2 networks

You may want to share one Internet access between two networks where each network is behind separate public IP address. The computers in both private networks will be accesible at the same time.



Then it is VERY important to perform the following routing scenario:

- DO NOT NAT with all packets going to the other local network.
- DO NAT with all packets going to the Internet

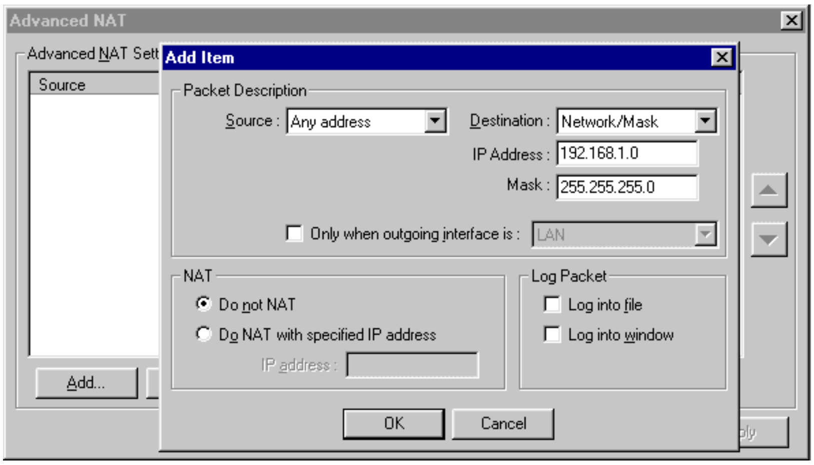
In another words WinRoute will perform NAT based on the destination address of passing IP packets. Packets going to the second local network will not be changed while packets going to the Internet will be fully NATed.

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

1 Go to menu Settings->Advanced->NAT.

2 Enter the destination criteria - usually the subnet or range of IP addresses

3 Select "Do not NAT" option



Source : Any address

Destination : Network/Mask

IP Address : 192.168.1.0

Mask : 255.255.255.0

□ Only when outgoing interface is : LAN

NAT

● Do not NAT

○ Do NAT with specified IP address

IP address :

Log Packet

□ Log into file

□ Log into window

If you do not NAT with specific packets, the source would remain as an internal IP address and they will never get responses back. In another words - such a user may try to connect to the Internet forever without a chance of getting an access.

Remote Access Server (dial-in) solution

In some cases 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 (NOT on the dial-in adapter)

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. As long as your NT server gives out remote users IP addresses from different subnets (other than the main network) the number of RAS interfaces you have installed limits the number of users.

WWW, FTP, DNS and Telnet servers behind WinRoute

WinRoute allows you to make computers in your network running important services (servers) that are accessible from the outside world. The services (servers) must be running on a specific port or the range of ports and you have to set up the appropriate Port Mapping in order to allow external users to reach your services.

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 that should be associated with the web server (one of your public IP addresses assigned to the external WinRoute interface).

Listen Port: 80

Destination IP: the IP address of the WEB server in your network (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 WinRoute computer. After the packets reach WinRoute they are automatically diverted to the appropriate internal computer.

DNS issue

Running a Web server (or FTP etc.) and DNS server on the same private network behind WinRoute NAT

You may want to run web server named www.mydomain.com behind NAT and use your DNS server running on the same network for the name resolution.

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

If you will run web server on the WinRoute PC you will not have any problems with local queries. All DNS queries for www.whatever.com coming to your DNS server will be answered by the regular Internet IP address associated with this domain. Such an IP address must be associated with the network interface linking from WinRoute's PC to the Internet and the WWW servers can listen on both public and private interfaces.

If the local PC sends a DNS query to resolve www.whatever.com it gets a public IP address associated with this domain as a result and connects the web server to the IP address (that is assigned to the Internet interface as described above).

Running a Web server (or FTP server 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). Then you will experience typical problem - the web server with www.mydomain.com is physically at a private IP address 10.10.10.8 but your DNS query will be resolved with a regular IP address (like 206.86.181.25) that is associated with this domain as a result.

Then your browser or ftp client will approach the public address, where there is no server running as the web server is inside your network.

Solution

To resolve this matter you must 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.mydomain.com** is operating at the appropriate **internal** (private class) IP address.You will let 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.mydomain.com** such requests will be answered by the appropriate local address.

DNS server and WWW behind NAT

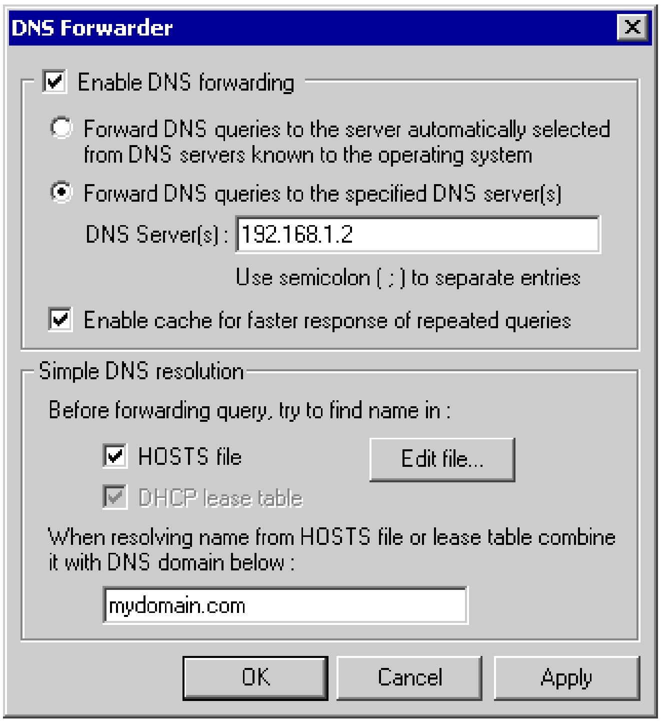
If you run your own DNS server and WWW server at the same private network you might want to rise the following question:

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 are coming from the INTERNET will be getting a regular INTERNET IP address associated with www.mydomain.com?

The solution is quite simple and 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
- Enter the IP address of your DNS server (e.g. 192.168.1.2) to the "Forward the queries to the specified DNS server(s)" field
- Edit the HOSTS file:

  Add a record saying that www.mydomain.com is at specific private IP address (the one where your web server runs - e.g. 192.168.1.10). HOSTS file are 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 server dialog by clicking button "Edit HOSTS file".



DNS Forwarder

☑ Enable DNS forwarding

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

● Forward DNS queries to the specified DNS server(s)

DNS Server(s) : 192.168.1.2

Use semicolon (;) to separate entries

☑ Enable cache for faster response of repeated queries

Simple DNS resolution

Before forwarding query, try to find name in :

☑ HOSTS file

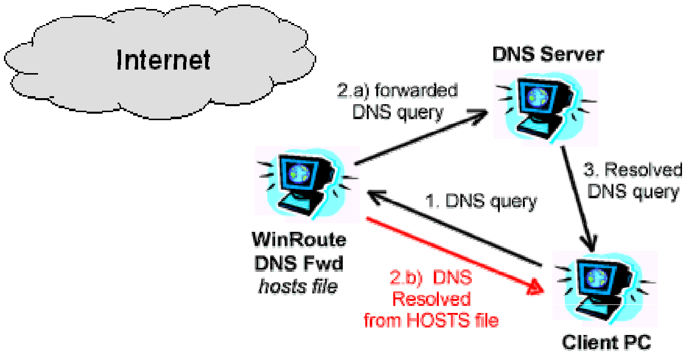
☑ DHCP lease table

When resolving name from HOSTS file or lease table combine it with DNS domain below :

mydomain.com

How will it work?

All DNS queries sent by the client computers from your LAN will be resolved by WinRoute DNS forwarder first. All queries will be checked against to the records in HOSTS file first. If the corresponding record finds the query it will be answered by details in such records (private IP address in our scenario).



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 on the same computer as WinRoute. It is because both services - WinRoute's DNS forwarder and your DNS server - would run on the same port (53). This would cause fatal problem.***

Running DNS server behind NAT

WinRoute's built in DNS forwarder provides you with the forwarding of DNS queries toa 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**.

Running the DNS Server behind NAT (WinRoute)

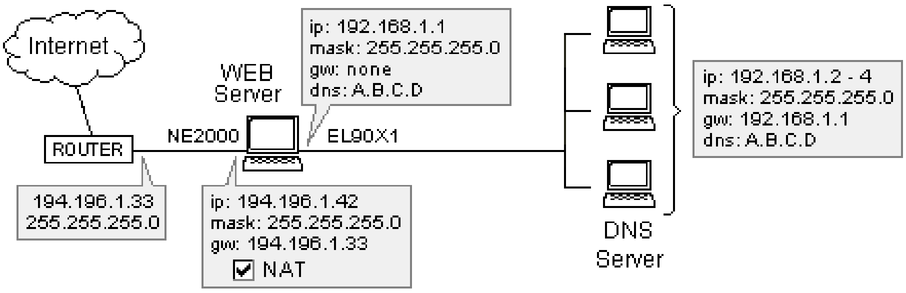
In order to run the DNS server behind NAT you have to set Port Mapping as described below. The DNS servers communicates with each other through the **UDP** protocol on **port 53**. If you do not perform this setting your DNS server will not be functional. You must perform this setting also when running the DNS server on the same computer as WinRoute, because WinRoute inspection module performs NAT **BEFORE** packets reach any application, including the DNS Server.

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

Listen port: 53

Destination IP: address of your DNS server (e.g. 192.168.1.2) or private (internal) IP address of WinRoute PC, if it's running on the same computer

Destination port: 53



- ***Note! If your DNS server is running on the same computer as WinRoute, the built-in DNS forwarder MUST BE switched OFF, because both of these services use the port 53. Running both DNS services on the same PC would cause fatal problems.***

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 you want to associate with the server (one of the adresses of the Internet interface)

Listen Port: 21

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

Destination Port: 21

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

Running Mail server behind NAT

In order to run Mail Server behind WinRoute it is recommended you create two port mapping entries - one for the SMTP protocol (which runs on port 25) and one for 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.

It is necessary to set up port mapping also in case the mail server is running on the WinRoute computer. This is because of the position of WinRoute inspection module which works below the TCP stack so the packets are changed/refused before they reach the operating system.

SMTP protocol:

Protocol: TCP

Listen IP:

Listen Port: 25

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

Destination Port: 25

POP3 protocol:

Protocol: TCP

Listen IP:

Listen Port: 110

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

Destination Port: 110

Running Telnet server behind NAT

Telnet is widely used by many systems to operate data remotely. E.g. all Unix servers use this protocol.

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

Protocol: TCP

Listen IP: <unspecified> (or one of the public IP addresses)

Listen Port: 23

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

Destination Port: 23

Running ICQ, voice over IP, video conferencing behind WinRoute

ICQ

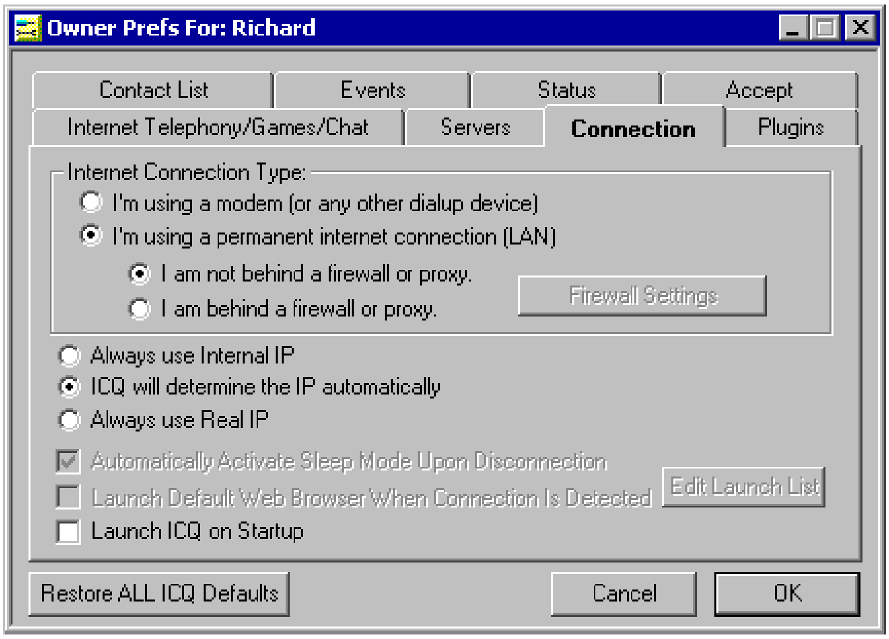
ICQ is the online chat system that establishes either direct connection between two users or they communicate via ICQ server. Basically users have to have a direct connection to the Internet or their Internet sharing solution must support Port Mapping.

WinRoute settings

There are no specific settings to use ICQ since the version 4.1 of WinRoute Pro.

ICQ client settings

Set the client up as if the computer would be connected directly to the Internet (do not use any Proxy).



Internet Connection Type:

○ I'm using a modem (or any other dialup device)
● I'm using a permanent internet connection (LAN)
● I am not behind a firewall or proxy.
○ I am behind a firewall or proxy.

○ Always use Internal IP
● ICQ will determine the IP automatically
○ Always use Real IP

☑ Automatically Activate Sleep Mode Upon Disconnection
□ Launch Default Web Browser When Connection Is Detected
□ Launch ICQ on Startup

IRC - Internet Relay Chat

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

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

Protocol: TCP

Listen IP: <unspecified> (or one of your public IP's you want to use for the IRC server)

Listen Port: 6667

Destination IP: IP address your IRC server (e.g. 192.168.1.10)

Destination Port: 6667

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

CITRIX Metaframe

WinRoute fully supports **CITRIX Metaframe** protocol as well as **MS Terminal Server** protocol. To access CITRIX Metaframe server or MS Terminal server running inside of your private network from the Internet you will have to perform following port mapping:

For MS Terminal Server:

Protocol: TCP

Listen IP: <unspecified> or public IP address you want to use for the server

Listen port: 3389

Destination IP: IP address of the server inside of the network (e.g. 192.168.1.10)

Destination port: 3389

For CITRIX Metaframe:

Protocol: TCP

Listen IP: <unspecified> or public IP address you want to use for the server

Listen port: 1494

Destination IP: IP address of the server inside of the network (e.g. 192.168.1.10)

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 the client computers which port they will use to access the server. This is usually specified in the .ini file of the client.

Internet telephony - BuddyPhone

WinRoute has become industries first software router/firewall that brings Internet telephony to a serious business level. Together with the BuddyPhone application (www.buddyphone.com), WinRoute allows you to place the call through the Internet from one network to another.

There are no specific settings to use BuddyPhone since the version 4.1 of WinRoute Pro.

ICUii video conferencing

WinRoute has become industries first software router/firewall to bring video conferencing to a serious business level. Together with ICUii video conferencing application (www.icuii.com) WinRoute allows you to establish video conferencing session through the Internet from one network to another.

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

Protocol: TCP

Listen IP: <unspecified> or public IP address you want to use for the server

Listen port: 2000-2038

Destination IP: IP address of the call recipient in your network (e.g. 192.168.1.22)

Destination port: 2000-2038

PC Anywhere

WinRoute includes the best support for Symantec's PC AnyWhere of any software router on the market. 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 scenario:

1 Managed computer will run PC Anywhere Host.

2 Remote computer will run PC Anywhere 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 PC Anywhere 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 set up computers that are allowed to access your network, you have to define 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 set up yourself the Administrator rights in WinRoute to enable a connection directly to the WinRoute host. Before connecting the PC Anywhere host, you can connect to WinRoute and change the destination IP in Port Mapping to access directly the PC you choose. Amazing!

CU-YouSeeMe

The following port mapping is necessary to receive the **CU-YouSeeMe** calls through the NAT:

Protocol: UDP

Listen IP: <unspecified>

Listen Port range: 7648-7649

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

Destination Port range: 7648-7649

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.

H.323 IP Gateway

The following port mapping is necessary to run **H.323 IP Gateway** through the NAT:

Protocol: TCP

Listen IP: <unspecified>

Listen Port: 1720

Destination IP: IP address of the workstation that runs the H.323 IP Gateway

Destination Port: 1720

Limitation:

Only one H.323 IP Gateway can be run in your network at a time.

PPTP VPN solution

Running PPTP server behind NAT

In order to run a PPTP server in the network behind WinRoute (including the computer where WinRoute is running) you have to set up the following port mapping.

For the control connection:

- Protocol: TCP
- Listen IP: <unspecified>
- Listen Port: 1723
- Destination IP: IP address of your PPTP server (e.g.192.168.1.12)
- Destination Port: 1723

For the GRE (PPTP) packets:

- Protocol: PPTP
- Listen IP: <unspecified>
- Destination IP: IP address of your PPTP server (e.g.192.168.1.12)

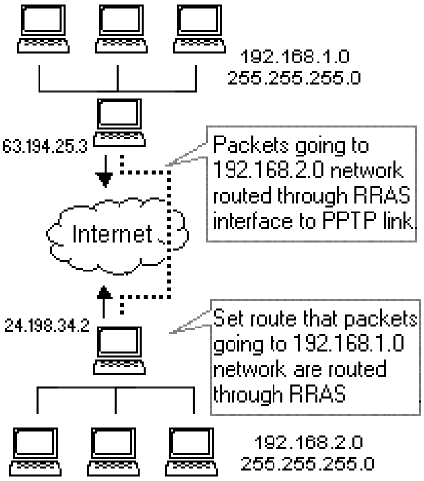
After setting up the port mapping as shown above you will be able to place your PPTP server anywhere behind WinRoute. The users will access your PPTP server by "dialing-in" to the external (public) IP address of your network. When the packet reaches the WinRoute computer it will automatically be forwarded to the proper computer behind the firewall.

Running a PPTP server on a WinRoute computer

There are no special limitations. You can still use the port mapping settings described above - you will use the WinRoute computer's internal IP address as the destination IP address.

PPTP solution example

WinRoute allows very cost effective way of creating your own WAN between branch offices connected to the Internet. We assume that the readers of this document have a basic knowledge about networking and WindowsNT.


192.168.1.0
255.255.255.0
63.194.25.3
Packets going to 192.168.2.0 network routed through RRAS interface to PPTP link
Internet
24.198.34.2
Set route that packets going to 192.168.1.0 network are routed through RRAS
192.168.2.0
255.255.255.0

To create such a WAN is possible in several easy steps:

1 Check the environment:

NT server on both ends

WinRoute Pro installed on both ends

RRAS (Stealhead) installed on both NT servers

2 Create a persistent route on both NT servers specifying that packets going to opposite networks are going through RRAS interface. Then - if you display TCP properties in the debug log of WinRoute Administrator you should see a dial-in interface listed among available interfaces.

3 In WinRoute Administration go to the Interface Table and display the properties of the RAS interface used for the PPTP link. Make sure that you will not perform NAT on this interface.

4 In RAS tab of the RAS interface properties select the PPTP connection among the RAS entries. If you don't see the RAS connection, make sure that you have set the correct phone book. Go to menu *Settings -> Advanced -> Misc. Options* and select the correct RAS phone book to use.

5 Test the connection - you should be able to ping to the opposite network and at the same time you should be able to access the Internet.

Running PPTP clients behind NAT

There are no settings required to run PPTP clients behind WinRoute (NAT) accessing corporate resources out of the local area network. However there are certain limitations:

- There is only one connection possible at a time.
- When two or more users want to use PPTP simultaneously and access the same remote network it may be worth it to establish a PPTP "server-to-PPTP" (server type) connection rather than run a PPTP client on each machine.

IPSEC VPN

WinRoute Pro 4.1 supports IPSEC in so called "**Tunnel mode**". The "**Tunnel mode**" should support any IPSEC client that allows the change of IP address.

WinRoute settings:

Create mapped port for ESP:

Protocol: Other 50

Listen IP: <unspecified>

Destination IP: the IP address of the client PC

We may also suggest to create mapped port for IKE. This is not necessary in case when the communication is initiated FROM behind WinRoute to the Internet however certain implementations of IPSEC may require this setting:

Port mapping for IKE:

Protocol: UDP

Listen IP: <Unspecified>

Listen port: 500

Destination IP: the private IP address of the client PC

Destination port: 500

Running multiple IPSEC sessions simultaneously

Should be there more IPSEC clients you need to use separate IP address for each client. Note - WinRoute NAT will allow to pass through as many clients simultaneously as you want as long as the connection is initiated FROM the local network and each client is "using" one IP address assigned to WinRoute's external interface.

General information about IPSEC

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

IPSEC is using either AH (Authentification 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 though encrypts the data. ESP allows to use so called "Tunnel Mode" that is similar to 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 as ISAKMP) is used for authentification (exchange of security keys). IKE is running on protocol UDP port 500. This port is used as source and destination.

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

We will incorporate protocol 50 into WinRoute automatically so that there will be no need for Port Mapping at all. The only condition to establish the connection automatically would the initiation of the connection FROM the local network.

Most of the IPSec vendors are using algorithm MD5 and SHA1 for authentification and DES, 3DES and Blowfish for the ecryption. IPSec is not tightly connected to any specific algorithm so that the solutions of different vendors might be incompatible.

Novell Border Manager VPN

This document describes the setup that makes you 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 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 the 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.

Gaming section

About running games behind NAT

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 in the Internet. The 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 try demo of the game first. Unlike Proxy servers, the basic architecture of WinRoute supports many games directly "off the shelf."

Certain games require specific port mapping configured in WinRoute in order to get them up and running. If the game has a specific port associated with it, this is not a problem for WinRoute! Just configure Port Mapping to forward packets arriving to 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 for the most popular games.

MSN Gaming zone

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

1 Go to menu *Settings->Port Mapping*

2 Add a 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 2/3 clients

No special settings are necessary.

Quake 2/3 Server

For Master server:

Protocol: UDP

Listen IP: <unspecified>

Listen port: 8002

Destination IP: the IP of the Master Server (e.g. 192.168.1.22)

Destination port: 8002

For clients connecting to Quake3 Arena server:

Protocol: UDP

Listen IP: <unspecified>

Listen port: 27960

Destination IP: the IP of the client computer (e.g. 192.168.1.11)

Destination port: 27960

Half-Life

Protocol: TCP/UDP

Listen IP: <unspecified>

Listen Port: 27015

Destination IP: IP address of the gamer's computer (e.g.192.168.1.11)

Destination Port: 27015

Battle.net (Blizzard)

Following port mapping must be set in order 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.192.168.1.11)

Destination Port: 6112

Special networks

Token Ring networks

Connecting Token Ring networks

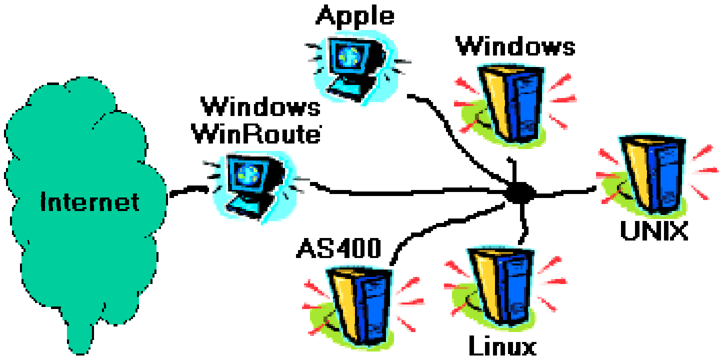
Token Ring is a very specific network type. As a result, we assume that only network professional's deal with Token Ring and do not go into a detailed explanation here.

- All computers within the Token Ring need the MTU (maximum transmission unit) set to 1500
- On the WinRoute computer go to menu Settings -> Advanced -> Misc. Options and check on "Support for Token Ring networks"
- Follow-up other setting instructions specific for each type of Internet connection

Multiple operating systems environment (Linux, AS400, Apple, ...)

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

NOTE: A Windows based operating system must host the WinRoute application. Therefore, at least one Windows 95/98/NT based computer is required in the WinRoute network. The host cannot be a UNIX system. However, UNIX can operate as a client system.



Appendix

In This Chapter

WinRoute key shortcuts

In the WinRoute Administration program, the are some predefined key shortcuts for the most often used settings.

Ctrl + I	Interface Table (Interfaces/NAT)
Ctrl + D	DNS Forwarder settings
Ctrl + H	DHCP Server settings
Ctrl + A	Save As... (saving current log window into a file)
Ctrl + M	Mail Server settings
Ctrl + S	Configuration dump (cfgdump.txt)

Literature

Windows NT Server Resource Kit

Microsoft Press

TCP/IP Network Administration

Graig Hunt, O'Reilly 1992

Building Internet Firewalls

D. Brent Chapman, Elizabeth D. Zwicky, O'Reilly 1995

Glossary of terms

E

ETRN command

In case that the mail is received via SMTP and the SMTP server is not full-time connected to the Internet (typically if using a dial-up connection), then the relay SMTP server temporarily stores the mail at itself. When you connect, your SMTP server will use the ETRN command (one of the SMTP protocol commands) to ask the relay SMTP server for a new mail.

There is no reply to an ETRN command in the case that no mail is actually stored at the relay SMTP server. So there must be a timeout defined, in which your SMTP server closes the connection if no new mail is received.

F

Flags

Flags are the extended information part of the packet. They keep additional information about the packet type. Here is the list of TCP flags displayed by WinRoute:

SYN - Synchronize - the connection establishing packet

ACK - Acknowledgement - acknowledgement of a data packet

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

I

IP address

IP address is the unique 32-bit number, which identifies the computer in an IP networks. Each packet passing across the Internet contains the information, from which address it was sent (source IP address) and to which address it should be delivered (destination IP address).

M

Mailboxes in WinRoute

The mailboxes are kept in a separate subdirectory of the directory where WinRoute is installed. Typically in c:\Program files\WinRoute\Mail.

There are no mailboxes created after installation even if the users are created. The mailbox is physically created AFTER the first e-mail for a user comes in.

MX records

MX records are records in the DNS, that contain the information about mail servers in the Internet. They contain an IP address of a mailserver(s) for the appropriate domain.

N

NAT

With NAT - Network Address Translator - you may connect a local network to the Internet looking like a single computer with one IP address. The computers in the connected subnet can access the Internet as if they were connected directly to it (certain limitations applies).

The connection of an entire network using a single registered IP address is made possible since the NAT module rewrites the source address in the packets sent from computers in the local area network with the address of the computer WinRoute is running on.

NAT differs significantly from various proxy servers and application-level gateways they will in principle never be able to support so many protocols as NAT does.

Network interface

The network interface is the device which connects the computer with other computers using some type of a communication medium. A network interface may be an Ethernet card, Token ring card, modem etc. The computer sends and receives packets by means of the network interface.

Network/subnet 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 there's for example a sub-network 194.196.16.0 with mask 255.255.255.0, the addresses of computers in this sub-network can be 194.196.16.1 through 194.196.16.254.

P

Packet

A packet is a basic communication data unit used when transmitting data from one computer to another. Each packet contains a certain amount of data. The maximum length of a packet depends on the communication medium. As an example, in Ethernet networks the maximum length is 1500 bytes. At each network model layer, the contents of the packet can be divided into two parts: the header part and the data part. The header contains control information of the particular layer, the data part contains data belonging to the upper layer.

POP3

POP3 protocol is used mostly by e-mail client software to pick up the e-mail from mailboxes at the POP3 compliant mail server. WinRoute mail server has such capability too, i.e. it can pick up the e-mail automatically from any POP3 compliant mail server and further distribute it to the mailboxes of local recipients.

POP3 protocol uses a **TCP** protocol **port 110**. If you want to access using this protocol a POP3 mail server running behind or on the WinRoute computer (to pick up your e-mail FROM the Internet) you have to perform **Port Mapping** for TCP protocol, port 110 sent to **private class** IP address of the PC running the mail server.

Port

A port is a 16-bit number (the allowed range being 1 through 65535) used by the protocols of the transport layer - TCP and UDP - to address applications (services) on a computer.

If there were 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 is the process where the packets arriving to the interface are checked by port number they want to reach. If the port number is found in the mapping table, the destination IP adress of the packet is replaced by the address in the mapping table. So the packets coming to WinRoute external interface can be redireted to the desired computer in the protected local network.

PPTP

PPTP - Point To Point Tunnelling Protocol - is a protocol used by Microsoft operating systems to create the encrypted connection between two computers.

Proxy

Proxy is another method of sharing the 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

Routing table

Routing table is the set of rules how to send the packets between the network interfaces in the system. It is generated by the operating system based on the TCP/IP protocol settings of the interfaces. To see routing table go to MS-DOS Prompt window and type in `route print` command.

S

SMTP

SMTP (Simple Mail Transfer Protocol) is used for direct communication between mail servers (such as the Winroute mail server and the mail server of your ISP) and for sending out the e-mail from your e-mail client software.

SMTP protocol uses the TCP protocol, port **25**. If you want to access the mail server running behind or on the WinRoute computer using this protocol (to allow other mail server to send the e-mail for you), you have to perform the **port mapping** for TCP protocol, port 25, to an IP address of the PC running the mail server (e.g. the internal interface of the WinRoute PC, if using the built-in mail server).

T

TCP/IP

TCP/IP is a common name for the networking protocols used for communication in the Internet (e.g. IP. TCP, UDP, ICMP etc.). All protocols are packet based, i.e. all data sent through are divided into the small parts and sent across the network.

Index