WinProxy 1.5.x

User's Manual

Martin Viktora Paul Marrington Last modified : August 31, *2001*

Authentication and cache management use MD5 algorithm.
Derived from RSA Data Security, Inc. MD5 Message-Digest Algorithm.

Content

1. Introduction

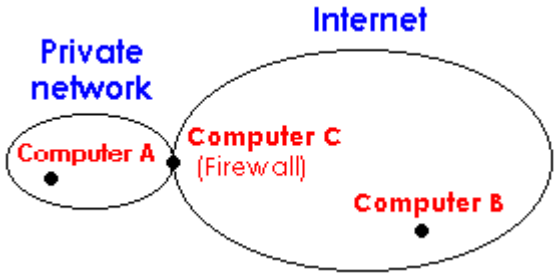
This document is intended for WinProxy users. It describes WinProxy, its method of operation and configuration details. We will be changing this manual as we add new information. The latest version will always be available on the web. If there are inaccuracies or insufficient information in this manual, please let us know. We welcome your suggestions.
Our Address is: winproxy@winproxy.cz
Authors

2. WinProxy - Method of Operation

A proxy server allows many computers on a local area network Internet access from a single point. A proxy server also provides a firewall, a computer placed between the local area network and the Internet. Firewalls provide protection from the open nature of the Internet. Commonly firewalls turn off packet routing on the host preventing access through the IP network layer. Attacks based on IP spoofing cannot reach the local area network. Communication through the firewall requires one of the following:-

- **Proxy server**
- **Gateway**
- **SOCKS server**

These are programs running on the firewall host that connected directly to the Internet or Intranet. Computers on the local area network access the Internet indirectly through the firewall/proxy host.



For computer **A** to connect to computer **B**, it must connect to computer **C** first. After this connection is established **A** sends **C** a request to connect to **B**. **D**ata exchange between **A** and **B** is now possible. **C** can relay data between **A** and **C** without any conversion, or provide protocol transformations.

Computer **C** can check authorization of the request, using predefined rules. This provides control over user access to the Internet services.

A proxy server introduces other interested features :

- **The need for a single IP address**
  The computers on the local area network can have any IP address. An actual Internet IP address is needed only for computer **C**. For example:
  A local area network with one computer connected to the Internet via a dial-up link (modem) or
  A local area network with one computer having two network interfaces (e.g. ethernet cards). One interface is connected to the local area network while the second is connected to a public access segment.

- **Use of a shared cache**
  Computer **C** can store data in shared cache. Repeated requests are retrieved from the cache instead of from the original sites. It conserves line bandwidth while decreasing response times.

3. Basic Information

3.1 System requirements

Operating system :

Windows 95/98/ME or Windows NT/2000/XP with the TCP/IP protocol installed (see TCP/IP Configuration).

Hardware :

WinProxy requires the basic hardware configuration for the given operating system with sufficient disk space for a cache. With larger numbers of users and larger caches, requirements for memory, disk, processor speed and line bandwidth will also increase.

We recommend the following as a minimum:

- 5 users: 20 MB cache, 486 66Mhz processor with 8 MB RAM
- 10 users: 80 MB cache, Pentium 60Mhz processor with16 MB RAM
- over 10 users: dedicated NT Server or NT workstation with a low load, Pentium 120 MHz with 32 Mb RAM

3.2 Installation and file descriptions

Download the WinProxy archive from the Internet and run it. Set the destination directory in which you want to install WinProxy to and select **Install**.

If your are installing on Windows NT and you have Administrator privileges, you can install WinProxy with service support. WinProxy can then be run both as a common application and as a service. As a service it can be set to start automatically when NT starts, allowing the proxy to be used by other workstations even when none is logged in on the host. Use the *Services* icon in the *Control Panel* to set the WinProxy service to run when the host starts.

Once the files are copied you will be asked to create a Program Manager group. The group will be named WinProxy and will include the version number. If you installed WinProxy with service support then this group will be common to all users.

WinProxy installs the following files :

winproxy.exe	- Application
proxy.pac	- autoconfiguration file (needs to be edited if you plan to use it)
config.htm	- on-line help for configuration
readme.txt	- basic information

---

4. Configuration

For WinProxy to work, the TCP/IP protocol must be installed on all computers. For TCP/IP LAN installation instructions read 5. TCP/IP Configuration before continuing. Please note that this is different to installing TCP/IP for a dial-up adapter.

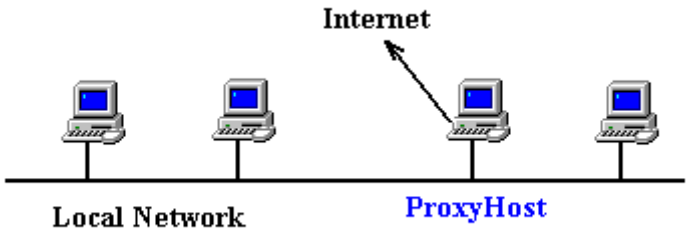
WinProxy is configured using web pages using a browser. Open your browser and ask for **http://host:3129/admin** as a URL, where **host** is the TCP/IP name of the computer running WinProxy. You need a browser that will show framed documents. For configuration, there are online help pages available.

Winproxy provides the following functions :

- proxy server for the HTTP, HTTPS, FTP and GOPHER protocols
- a shared cache for all these protocols
- gateway for the Telnet, FTP, SMTP, NEWS and POP3 services
- Mail Server
- SOCKS server v4, v5 and DNS forwarder
- dial-up connections on demand
- user and group management with access restrictions
- secure local area network access to the Internet

Each item represents a subsystem within WinProxy. The behavior of these subsystems is controlled by values set on the WinProxy configuration pages.

Important : For convenience we will call the computer running WinProxy *ProxyHost*, representing the **DNS name** or **IP address** of the computer that is running WinProxy. We will also assume that WinProxy is being run on a computer with access to the Internet via either a dial-up line or a second ethernet interface.



4.1.1 Proxy - General

Setting up WinProxy

A proxy server provides users on a local area network with Internet access services such as WWW, FTP and GOPHER from their browsers. Normally WinProxy listens for requests on port 3128. This default value can be changed on the **Network**, field Proxy Port.

Your browser will need to be configured for use with WinProxy. Below are some sample configurations for popular browsers:

Setting up clients

MS Internet Explorer 5.X

1. Select the menu items Tools>Internet Options>Connections>LAN Settings
2. Select Use a proxy server
3. Enter the host computer name in Address field. The port number to use is 3128.
4. Click on Advanced button
5. Check Use the same proxy server for all protocols
6. Enter the Proxy Host IP address in Do not use proxy server for addresses beginning with:
7. In case of dial-up connection in Dial up setting enter again the Proxy host IP address and port.

MS Internet Explorer 4.X

1. Select the menu items View->Internet Options->Connection
2. Check Access the Internet using a proxy server
3. In Address field enter the proxy host IP address and in Port field enter 3128
4. Check Use the same proxy server for all protocols
5. Enter the Proxy host IP address in Bypass proxy server for local (Intranet) addresses

Netscape Navigator

1. Select the menu items Options->Network Configuration->Proxies
2. choose Manual Proxy Configuration
3. push the View button
4. Enter the proxy host computer name for the HTTP, FTP, GOPHER and Security Proxy fields. The port number to use is 3128.

Alternatively, use an autoconfiguration file. The location for this file is set on the **Advanced** page.You can find a template of this file in directory in which WinProxy was installed. Edit this file and enter the name of the computer that hosts WinProxy. Choose *Automatic Proxy Configuration* in your Navigator Proxy Dialog Box and set the field *Configuration Location (URL)* to ProxyHost:3129/autoconfig.

NCSA Mosaic

1. Select the menu items Options->Preferences->Proxy
2. Enter the proxy host computer name for the HTTP, FTP, GOPHER and Security Proxy fields. The port number, 3128 is entered following a colon as part of the name (e.g. ProxyHost:3128)

MS Internet Explorer 3.0

1. Select the menu items View->Options->Connections
2. For the Windows 95 version, press the Proxy button
3. Enable the check box for *Use the same proxy for all protocols*.
4. Enter the proxy host computer name and port number in the space provided.

Parent Proxy

If your ISP runs a proxy server on fast machine with a big cache and you have a high-speed connection you can set it as a parent proxy on the **Advanced** page. All requests will be retrieved through this server.

4.1.2 Proxy - Cache, Cache TTL

Data collected by the proxy server from the Internet and passed to browsers on the local area network can be stored in a shared cache. If the same, or another browser on the network, requires the same information it is retrieved from the cache. Since the cache is on a local computer this is far quicker than accessing the Internet.

Setting up Cache Parameters

The size of the cache can be set on the **Cache** page. This value is the maximum size in Megabytes. After reaching this limit garbage collection is performed with the oldest objects deleted first. The cache is reduced by this garbage collection to 85 percent of the maximum size.

Values for Max.HTTP Size, Max.FTP Size and Max. GOPHER Size determine the maximum size of objects stored in the cache for these protocols. Larger objects are passed through without being cached. Do no set the value for FTP too high as a big archive file will purge many smaller HTTP objects.

If you don't wish to cache stored data turn caching off by unckecking the *Enable Caching* box.

The other two check boxes determine what to do when the user breaks a connection by using the browser stop button or by selecting a new page

before the current page has been completely loaded. If option *Continue Aborted* is checked, WinProxy will continue loading pages into the cache. With this option enabled it is easy to build up a large number of concurrent connections while skipping between pages. If the check box *Keep Aborted* is checked WinProxy will store incomplete objects (pages).

Time To Live on WinProxy Side

Values on the **Time-To-Live** page determine the number of days that objects (web pages) are kept in the cache. Any requests for objects older than this are reloaded from the Internet. TTL can be set the for individual protocols and/or for individual URLs. To specify individual URLs use the *TTL Advanced* section. Each entry is of the form days@url, where url can include asterisks to specify a group of related URLs.

Examples :

12@*www* sets a cache life of 12 days for all objects with a URL containing www (all World Wide Web pages).

2@ftp://*.zip sets a cache life of 2 days for all objects downloaded via FTP with an extension of .zip

Time To Live on Web Server Side

Remote web server can itself determine the number of days that objects (web pages) are kept in the cache, which is especially important for dynamically generated sites (ASP, PHP, CGI), that are not suitable to be stored in cache. Nevertheless, in case of slow dial-up connection it would be sensible to activate ignoring Time To Live information **(Cache>Cache pages marked as non-cachable by web server)** and that way it will lower the necessity of dial-up to the minimum.

4.1.3 Proxy - Access

WinProxy supports management of users and groups of users. These are used to determinate restrictions for selected WWW pages and for the Mail Server settings.

Users and Groups are managed on the page **Accounts**. WinProxy has a built-in group called Admins which cannot be deleted. Users belonging to the Admins group have no access restrictions.

Access List

This is a list of URLs restricted to specific users or groups. Each entry is in the format **scheme://host/path**. Asterisks may be used for an arbitrary string. If a user attempts to access a URL that matches one in the list, the user is required to enter a name and password. In order to access the URL, the user must be present in the Access List or be a member of a group that is present in Access List for a required URL. Push the Edit button to see a list of users and groups allowed to access selected URL. Groups are shown first and are enclosed in brackets. When you add a new URL, no one has access to this URL.

WinProxy's web interface access restriction

Access restrictions also apply to the WinProxy web interface. The host name of the computer running WinProxy is converted to WinProxy before testing the Access List. To limit users' access to the WinProxy administration web interface add the following line to the Access List: http://WinProxy/admin/* If you intend to restrict the access to the web interface, don't forget to add at least one user who would have access to it or would be a member of Admins group. If you forget this, nobody would be able to access the web interface.

Notes

- Not all browsers or clients' programs support the authentication functions needed for proxy access. In these cases the browser cannot access any URLs in the Access List. They can access any other URL. Proxy authentication is supported by Netscape Navigator and MSIE 3.0.
- A user is asked for his username and password only once a browser is started. Than browser adds automatically the username and the password with each request.

Examples

1. We need users of **[users]** group to have an access to the following domains only : **domain.com**, **work.com** and the user **boss** to have access anywhere. We should set Access List and user / group access according to the following table **:**

Access List	users / groups
*	boss
.domain.com	[users]
.work.com	[users]

2. We need nobody could access domain **bad.com :**

Access List	users / groups
.bad.com	

4.2 Network

4.3.1 Telnet gateway

The Telnet protocol allows users on a local area network to connect to an arbitrary host on the Internet and to work with it in remote mode. It is usually used to connect to UNIX machines, assuming a user has an account on that machine. To use Telnet through WinProxy turn the *Telnet Gateway* check box in the **Network** page on. Telnet gateways listen on port 23. This

value can be changed in the Port field. To use a Telnet gateway run a telnet client and connect to the computer *ProxyHost* first. You will then be challenged to enter the name of the host you wish connect to.

 Ftp gateway

FTP (File Transfer Protocol) is a protocol used to transfer files between computers. The WinProxy Ftp gateway allows users on the local area network to access ftp servers on the Internet. If you plan to use a FTP gateway, activate the *Ftp Gateway* check box on the **Network** page. Normally Ftp gateways listen to port 21. This value can be changed in the Port field.

To use the Ftp gateway, run a ftp client and connect to the computer hosting WinProxy first. At the ***username***: prompt type ***user@host*** where ***host*** is the machine you want to connect to and ***user*** is an account name (e.g. anonymous@ftp.bestsite.com).

You can also use WS_FTP. To set WS_FTP: set the Host Name to the computer *ProxyHost* in the Firewall information and the Firewall type to USER with no logon. If you direct WinProxy to use different port for the Ftp gateway, than set this in the Port field.

RealAudio gateway (proxy)

RealAudio gateway allows to receive live sound from the Internet. WinProxy support both TCP and UDP transport . If you plan to use a RealAudio gateway, activate the *RealAudio gateway* check box on the **Network** page. Normally RealAudio gateway listens to port 1090. Setting of your RealAudio Player is following : menu View -> Preferences -> Proxy, activate Use Proxy, enter computer ProxyHost to the host field and port number set to 1090.

News

News gateways provide users on a local area network with access to USENET News services. To enable the News gateway enter the name or IP address of your News host on the **Network** page. In the news-reader client program set *ProxyHost* as the News server.

SOCKS Server and DNS

If you wish to use WinProxy as a SOCKS server, check appropriate version box on the **Network** page. The default SOCKS server port of 1080 can be changed in the entry SOCKS port field.

If you want users to authenticate with SOCKS version 5, enable *Use SOCKS5 Authentication* checkbox. Than you can also control the access to the destination hosts/ports by the Access List. Lines for SOCKS5 access control are of the form : socks://host:port.

If you plan to use SOCKS version 4, you will probably need to set the DNS server. Enter the IP address of an Internet DNS server. WinProxy will forward DNS requests to this host.

4.2.2 Mapped links

Mapped links enable an additional support of other protocols by mapping the relevant port to the remote server. **Local port** is a local port number in WinProxy, **Remote Port** is a port on the remote server. Incoming requests from the client program to the WinProxy address and the local port are by means of WinProxy tunneled to the remote port of remote server. It's possible to map TCP and UDP protocols. In client program it is always essential to change the server address to the WinProxy address.

That way it's possible to run e.g. mIRC (TCP port 6667), **News server** (remote port TCP 179, local port any free), download e-mail from POP3 server, which is not set up in mail server (remote port TCP 110, local port any free) and the like.

4.3 Dial

WinProxy can establish dial-up connections to your Internet provider. There are three ways to initiated a connection:

- ***On Demand*** - connection is initiated when a DNS name is unknown on the local area network or the destination host is unreachable.
- ***Scheduled Dial*** - connections are made at defined intervals

Note: *If Dial On Demand is on and you type wrong DNS name for a local computer, WinProxy dial up your ISP to look on the Internet for the name. It can look as if connections were initiated without reason.*

4.3.1 General

Configuration for a dial-up connection can be set on the WinProxy Dial page. Test direct dial-up before trying it with WinProxy.

1. choose the desired RAS connection name from the list provided.
2. enable or disable automatic connection
3. set the timeout value in the **Hang up After** field. If no traffic occurs on the line for this period of time the connection will automatically be closed.
4. enter your user name and password in the fields **Username** and **Password** for the connection selected in (1) above.

Note : *If your ISP does not support PAP or CHAP authentication protocol and you have to connect to your ISP through a Terminal window, try the following:*

- *Windows NT 3.51 - create a log-on script suitable for your connection. A template is in WINNT35\system32\ras\switch.inf file. If you have any problems, contact your ISP.*
- *Windows 95 - enter the required information in the Terminal window on the computer ProxyHost.*
- *Windows 95 - you can also create log-on script for this operating*

system. See the WinProxy home page for details.

4.3.2 Demand Dial

On **Demand Dial** page there is an option of time intervals, when an atomatic connection to the Ineternet is allowed with a request not being in local network or cache. Default set-up is daily 00:00-23:59. It is possible to set it up differently for each day of the week. Time intervals within one day are separated with a comma.

Example of set-up

Monday: 7:30-11:00, 15:00-16:45

Tuesday: 00:00-23:59

4.4 Accounts

WinProxy supports management of users and groups of users. These are used to determinate restrictions for selected WWW pages and for the Mail Server settings.

Users and Groups are managed on the page **Accounts**. WinProxy has a built-in group called Admins which cannot be deleted. Users belonging to the Admins group have no access restrictions.

4.5 Mail

SMTP (Simple Mail Transfer Protocol) is the protocol most commonly used on the Internet for e-mail.E-mail messages can be passed along to several computers before getting to the destination on the e-mail address. SMTP protocol requires that messages to delivered within a time limit, typically 3 days. If the destination host is unreachable when this time limit expires, the message is returned to the sender.

SMTP is not suitable for single workstations or for dial-up lines because:

- computers working as SMTP servers must have a permanent connection to the Internet to receive e-mail.
- SMTP servers are responsible for message delivery. If the destination host is unreachable, they must hold the message and try to deliver it again at regular intervals.

This is why the message "journey" via SMTP ends on bigger continuously running computers at large organizations or at ISP sites. Users download their e-mail from these hosts using a POP3 protocol. This protocol allows users to connect to the server at any time and download their e-mail on demand.

A dial-up e-mail account will send e-mail via SMTP and receive it from the

Internet via POP3. WinProxy can be installed to provide e-mail support in one of three ways:

4.5.1 Mail Gateway

SMTP and POP3 requests from local area network are forwarded to the computers specified in the WinProxy configuration.

Setting up WinProxy
Turn on the **SMTP/POP3 Gateway** option on the **Mail** page and save it. Follow the **Settings** link. Enter your Internet SMTP and POP3 server in the matching fields.

Setting up clients
There are many client programs for sending and receiving e-mail from the Internet (*e.g. MS Outlook, MS Outlook Express, Netscape Messanger, Pegasus mail for Windows, Netscape Navigator, MS Explorer 3.0 - Internet Mail, MS Exchange, Eudora*). Please refer to the documentaion available for these programs. You are required to enter the address of an SMTP and a POP3 server. Set this address to the computer *ProxyHost*. The POP3 User-name (account) and the Password should be set to the value valid for the **Remote POP3 Server**.

4.5.2 Mail Server

WinProxy can work as SMTP/POP3 server. the WinProxy SMTP server is designed for dial-up connection. E-mail can be sent through the local area network at any time. When WinProxy is connected to the Internet it will pass on waiting e-mail and collect in-coming e-mail from the specified POP3 servers. This can be accomplished manually or at specific times or time intervals.

- Users need not be aware when the connection to the Internet is established to send and receive their e-mail. Their e-mail is downloaded from their POP3 servers itself when WinProxy connects to the Internet and the e-mail they sent to WinProxy is sent to the Internet. So they can send and receive mail at any time whether WinProxy is connected to the Internet or not.
- E-mail from one mailbox can be copied to a group of WinProxy users.
- If any user wishes to receive e-mail from several Internet mailboxes, WinProxy can store them to one local mailbox.
- You can have your own Internet domain (e.g. company.com). You can create any number ofof e-mail addresses within that domain (e.g. sales@comany.com, boss@company.com, ...). E-mail for that domain is being stored is one mailbox on your ISP host. When WinProxy downloads e-mail from that mailbox it can sort the messages according to **To:** header and deliver the messages to the appropriate local mailboxes.

Note: You must ask your ISP to provide you with a domain.

To summarize : WinProxy downloads e-mail from remote mailboxes (POP3 servers) and delivers thento local WinProxy's mailboxes. Users can download e-mail from these local mailboxes to their computers. Outgoing e-mail is sent to WinProxy and later passed to the SMTP server on the Internet.

Setting up clients
There are many client programs for sending and receiving e-mail from the Internet (*e.g. MS Outlook, MS Outlook Express, Netscape Messanger, Pegasus mail for Windows, Netscape Navigator, MS Explorer 3.0 - Internet Mail, MS Exchange, Eudora*). Please refer to the documentation available for these programs. You are required to enter the address of an SMTP and a POP3 server. Set this address to the computer *ProxyHost*. The POP3 User-name (account) and the Password should be set to your **WinProxy username** and **password.**

See Appendix B for a sample Mail Server configuration.

4.5.2.1 General

Turn on the **SMTP/POP3 Server** option on **Mail** page and **Save** it. Follow the **Settings** link. Enter your Internet SMTP address in the field **Remote SMTP server**. E-mail can be sent and received from the Internet at specific times. The **every** option will process e-mail at the specified time intervals. The time field is of the form **hh:mm** where **hh** is hours and **mm** is minutes. The **at** option will process e-mail at a specified time of day. You can provide more than one time of day by separating each time by a space. If you turn on the **Allow to Dial** option WinProxy will dial-up your ISP for mail processing to reach remote SMTP and POP3 servers.

4.4.2.2 POP3 Downloads

Information about local and remote mailboxes are stored in the **Account List**. Items can be added and removed from this list. **Remote POP3 account** specifies remote mailboxes. The entry is of the form username@pop.server. Set the **Password** entry for that account. The **E-mail** entry specifies the Internet e-mail address. If this entry is the same as the **Remote POP3 Account**, leave it blank. This entry is used to recognize e-mail for local users. When anyone sends e-mail to WinProxy, WinProxy goes through all records and if finds a matching one the e-mail is immediately delivered to appropriate local mailbox. The last entry, **Move To Local Account** specifies the WinProxy user (set on the **Users** page) who actually gets the e-mail. If you choose a group of users, e-mail is delivered to each user in the group. There is a special option called { RULE }. Use it when you receive e-mail for your own domain from one mailbox. In this case e-mail is sorted according to **To:** header.

4.5.2.3 Sorting Rules

Sorting rules are defined on the **Sorting Rules** page. E-mail with addresses

that cannot be resolved are stored according to the rule with @ by itself (if present) or according to the **Report Problems To** (with error description).

To check validity of the records in the **Account List,** invoke e-mail processing from the **Manual** page.

4.5.2.4 SMTP Relay restrictions

In case the computer running WinProxy has a permanent connetion (Leased line, ISDN, wireless connection, cable modem) there is danger of spamming. In mail server you can set up such ristrictions, which will prevent that.

In the first fiels enter a list of IP addressed of all computers in local network. From these addresses you can send mail to any domain. In the second field enter your local domain (e.g. firm.net) or damains. To this damain you can send a mail from anywhere, not only from local IP addresses then.

Example of a list of local IP addresses:

147.228.5.18 192.168.2.1 192.168.1.0/255.255.255.0

Note: IP addresses are separated by a space and an extent is specified by a subnet mask separated with a slash.

Example of a list of local damains:

firm.net company.com association.com

Note: Local domains are separated by a space and are without @.

4.6 Security

If you are concerned about security, the WinProxy firewall will provide peace of mind. Today's trend is not to use direct connectivity where it is not absolutely necessary. With WinProxy you can easily build an effective Firewall. You must also turn off packet routing on *ProxyHost*. This is not necessary for Window 95 as it doesn't have routing capabilities.

If packet routing is turned off, the only way in to your system from the Internet is to use a service running on the firewall host. To disallow possible intruders accessing your system through WinProxy, set the address of the secure Interface. This is an IP address of a network interface (network card) which can be considered as secure. Usually this the IP address of your computer in the local area network The address of the secure interface can be set on **Advanced** page in the field **Secure Interface.** If you host is multihomed you can enter a list of IP addresses separated by semicolons.

4.7 Advanced (further set-up)

On this page you can enter **Timeout**, which means how long WinProxy waits

until it reports an error. Furthermore a number of dial-up attempts, as long as the first connection failed. **(Connect Rety). Internal DNS Resolver** was expained in **Network** chapter. **Reverse DNS** converts the IP addresses into names, which can be used in log files. Route, where log files are stored, you can enter in **Logs Directory**.

If your Internet provider operates his own proxy server with a large cache, you can set his address and port in **Parent Proxy** and **Parent Proxy Port** fields. Requests will be passed on this server.

If you check **Run as service**, it will start Windows without user's having to log into Windows. This only applies to Windows 95/98. In Windows NT/2000/XP can WinProxy run as a full service.

5. TCP/IP Configuration

TCP/IP must be correctly configured on the computer *ProxyHost* and on all computers that will access the Internet through Winproxy.

ProxyHost must run on a computer using Windows NT or Windows 95. The computers that will access the Internet through WinProxy can use any operating system supporting TCP/IP (Windows, Unix, Macintosh, VMS, ...).

If TCP/IP is not installed, either:

1. ask your system administrator to install it or
2. install it yourself according to following directions

Let's consider a local area network with four computers. The (Netbios) names of these computers are : Chris, Eric, Jack and Allan. Computer Jack is used to connect to the Internet via a modem. These computers use Windows 95, Windows NT and Windows 3.1.

5.1 IP addresses

All computers in a TCP/IP network require a unique IP address. An IP address is 32 bit number. For convenience it is written as decimal numbers with each byte separated by a dot in format a.b.c.d .

The document RFC 1597 recommends that selection of addresses for LANs be taken from a private address space. The organization IANA has reserved three blocks of addresses to be used in private networks. The first block is a single class A network address, the second block is a set of 16 contiguous class B network addresses, and the third block is a set of 255 contiguous class C network addresses.

The addresses are :

- Class A : 10.0.0.0 - 10.255.255.255
- Class B : 172.16.0.0 - 172.31.255.255
- Class C : 192.168.0.0 - 192.168.255.255

These addresses are not used anywhere in the Internet.

We will use class C for our example (a network of up to 255 computers). Let's select a network address 192.168.1.0 . The following table shows IP addresses of our computers :

Computer name	Operating system	IP address
Chris	Windows 95	192.168.1.1
Eric	Windows 95	192.168.1.2
Jack	Windows NT	192.168.1.3
Allan	Windows 3.1	192.168.1.4

To set these addresses for each operating system use the following instructions:

1. **Windows 95 and Windows NT 4.0**
2. From the Start button, select **Settings** -> **Control Panels** -> **Network**
3. Select **TCP/IP** protocol. If this protocol is not in the list, select **Add** -> **Protocol -> Add.** From the list presented, select **Microsoft** as the vendor and then the network protocol **TCP/IP**.
4. Select **Properties** and the **IP address** sheet. Enable the option **Enter the IP address**
5. In the **IP address** field enter the address from the table. For the **subnet mask** field enter the value 255.255.255.0 . Press **OK** to complete the installation. Insert your Windows 95 diskettes or CD on request.
6. Enter the same IP address for the **Default Gateway**
7. Restart the computer

Windows NT 3.51

1. From **Program Manager,** group **Main** select **Control Panel** then the **Network** icon
2. From the list **Installed Network Software** select **TCP/IP protocol** and push **Configure**. If the TCP/IP protocol is in the list, skip to point 4.
3. Press **Add Software**. From the **Network Software** list select **TCP/IP Protocol and related components**, Insert installation disks. After the necessary files have been loaded, press **OK** in **Network Settings** dialog.

4. In the **IP address** field enter the value from the table. For the **Subnet Mask** field enter 255.255.255.0 . Press **OK** to complete installation.
5. Restart computer

Windows 3.1

TCP/IP protocol is not a part of this operating system. To run TCP/IP you require an external TCP/IP implementation such as Microsoft TCP/IP or Trumpet Winsock. Configuration details are documented with these packages. The Microsoft TCP/IP drivers are available at the Microsoft anonymous ftp site under the name WFWT32.EXE. The Microsoft ftp site can be accessed from www.microsoft.com uner the heading *free software*

Now you can use TCP/IP on your local area network. To test it, run the ***ping*** utility from a command prompt. You should be able to reach the other computers on the LAN.

```
Try :
C:\WINDOWS>ping 192.168.1.1
C:\WINDOWS>ping 192.168.1.3
C:\WINDOWS>ping 192.168.1.3
C:\WINDOWS>ping 192.168.1.4
```

Note : At this point you can only use IP addresses. In all places in this document where you are asked to enter the computer name *ProxyHost* you would have to use the IP address of computer Jack : 192.168.1.3 . To give the computers names, follow the instructions below.

5.2 DNS

Because IP addresses are difficult to type or remember, TCP/IP networks provide a means to assign names to the IP addresses. Names in TCP/IP networks are organized using a Domain Name System or DNS. These names can be different from the Netbios names (the names you can see as "Network Neighbors" in Windows 95 or NT 4).

Each IP address can be assigned one name and, optionally, several aliases. There are two ways for computers to translate DNS names back into IP addresses.

1. through a DNS server
2. using static tables located on each computer on the local area network

DNS servers are used in large networks with dedicated server computers. Because our sample network is small we will use static name tables. We will assign DNS names that are the same as the Netbios names.

The TCP/IP software reads a text file called ***hosts*** on the local computer to find DNS names. This file is in different directories, depending on which operating system is used:

Windows 95	\Windows
Windows NT	\WINNT\SYSTEM32\DRIVERS\ETC
Windows 3.1	\ETC

Each line of this file contains a record of the form:

```
IP_address DNS_name [aliases]
```

Lines beginning with a # are used for comments. Edit this file with a text editor such as NotePad.

Our sample file would look like :

```
# file hosts
# this file translate DNS names into IP addresses
#
127.0.0.1      localhost
192.168.1.1    chris
192.168.1.2    eric
192.168.1.3    jack     winproxy
192.168.1.4    allan
# end if hosts file
```

This file can be copied to the correct directores on all the computers.

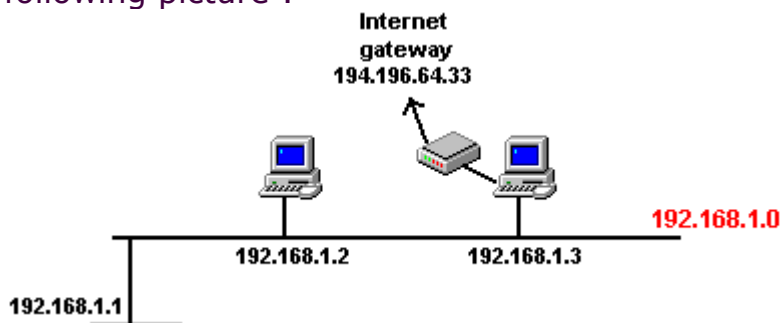
Now you can use DNS names for the computers on the local area network You should be able to ping other computers using their names.

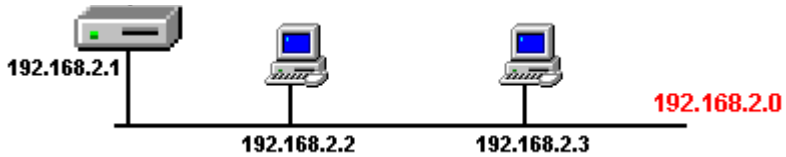
```
Try :
C:\WINDOWS>ping chris
C:\WINDOWS>ping eric
C:\WINDOWS>ping jack
C:\WINDOWS>ping allan
```

Now you can use **jack** everywhere you were asked for *ProxyHost*.

A. Multisegment networks

This appendix explains a problem which often appears on multisegment networks when used with a dial-up connection. For convenience let's consider following picture :





There are two networks; the first network has address 192.168.1.0, the second 192.168.2.0. The networks are interconnected by a router which IP addresses of 192.168.1.1 and 192.168.2.1. Computer 192.168.1.3 is used to connect to the Internet.

In this example we will refer to the computers by their IP addresses. *ProxyHost* would be 192.168.1.1 .

The problem is that the computers uses a default route to reach the other network. The default route points to the appropriate router interface. At the moment when computer 192.168.1.3 connects to the Internet, the default route is overwritten and points to the Internet gateway. Now computer 192.168.1.3 can't "see" computers on 192.168.2.0 network. As a consequence computers from the 192.168.2.0 network can't connect to the computer 192.168.1.3.

To overcome this, replace the default route with a normal one in the routing table. On computer 192.168.1.3 type the following command at a command prompt:

```
c:\>route ADD 192.168.2.0 MASK 255.255.255.0 192.168.1.1
```

If a packet appears destined for the 192.168.2.0 network with netmask 255.255.255.0 it is sent through the router with IP address 192.168.1.1. Use switch -p under Windows NT to make this route persistent between system boots. For Windows 95, add this command to your AUTOEXEC.BAT file.

After this command computer 192.168.1.3 will "see" computers on the network 192.168.2.0.

B. A Sample Mail Server configuration

I. A simple example

Let us consider 4 users. Each of them has a WinProxy account, created on **Users** page. These names are: **boss, peter, bob** and **martin**.There is also a group **[sales]** with **boss** and **peter** as members. We would like to process e-mail according to the following table :

POP3 Username	POP3 Server	E-mail	Who will get the e-mail
bob	mbox.dsf.com	bob@computers.com	bob
geiger	pop.serv.com	geiger@mbox.serv.com	martin
martin	mbox.prov.com	martin@mbox.prov.com	martin
peter	bigboy.uni.edu	peter@bigboy.uni.edu	peter
sales	mbox.prov.com	sales@mbox.prov.com	boss, petr
smith	mbox.prov.com	smith@mbox.prov.com	boss

Records int the **Account List** should look like :

Account List

```
bob@mbox.dsf.com (bob@computers.com) >> bob
geiger@pop.serv.com (geiger@mbox.serv.com) >> martin
martin@mbox.prov.com (martin@mbox.prov.com) >> martin
peter@bigboy.uni.edu (peter@bigboy.uni.edu) >> peter
sales@mbox.prov.com (sales@mbox.prov.com) >> [sales]
smith@mbox.prov.com (smith@mbox.prov.com) >> boss
```

To check the validity of records in the **Account List** invoke e-mail processing from the **Manual** page.

II. A complex example using sorting rules

Let us consider a company with 6 users. Each of them has a WinProxy account with names of: **boss, peter, bob, martin, david** and **jane**.The **[sales]** group has**boss** and **peter** as members. The **[developers]** group has **martin, bob** and **jane** as members. The**[users]** group has all users as members. The company has it's own domain name called **company.com**. E-mail for this domain is delivered to the single mailbox **company** on the ISP computer **mbox.prov.com**. Each user has its own e-mail address within that domain. The company also created e-mail addresses for information about sales called**sales@company.com.** E-mail from this address should be delivered to users in group **[sales]**. Users **martin** and **bob** receive e-mail from other computers. **bob** also subscribes to a mailing list **conf-l@prov.com**. We want e-mail from this mailing list to be delivered to users **martin** and **jane** also. The company also wants to have an internal mailing list with an e-mail address of **info-l@firma.cz**.

The **Account List** should look like **:**

Account List

```
bob@mbox.uni.com (bob@mbox.uni.com) >> bob
company@mbox.prov.com (@company.com) >> { RULE }
geiger@pop.serv.com (geiger@mbox.serv.com) >> martin
```

And Rule List like **:**

Rule List

```
bob@company.com >>bob
boss@company.com >> boss
conf-l@prov.cz >> [developers]
david@company.com >> david
info-l@company.com >> [users]
jane@company.com >> jane
martin@company.com >> martin
peter@company.com >> peter
sales@company.com >> [sales]
```

Take a look at the second line in the **Account List**.The e-mail address is just **@company.com**. All users in **company.com** are local.

To check the validity of records in the **Account List** invoke e-mail processing from **Manual** page.

Notes:

- It should not be a problem to have own domain to receive e-mail. For an ISP it is no more demanding than a single mailbox. The cost should be similar to a single mailbox. If your ISP is unwilling, choose another ISP.
- ***(for specialists)*** The e-mail header **To:** needn't contain the receiver's e-mail address. In most cases e-mail going from mailing lists contain in this header e-mail address of the list. This example solved this problem in the following way : one user (**bob**) was a member of the mailing list and e-mail from this mailing list were copied. to other users (**bob, martin, jane**). E-mail from the mailing list comes in as a single copy.

  There is a problem when two or more users are subscribed to the same mailing list. E-mail is received more than once. It is impossible to decide who the e-mail is for. E-mail can be sorted according to the header **X-Envelope-To:**. This header must be taken from the e-mail envelope before the e-mail is stored in the mailbox. Please let us know if you need more information about this solution.

C. Information for ISPs

- ***How to setup sendmail to store e-mail for a domain into a single***

mailbox (UNIX, sendmail)

You need to add following line into the /etc/sendmail.cf file, ruleset S98:

```
R$*<@company.com.>$*                    $#local $: company
```

How to add an X-Envelope-To header into an e-mail (UNIX, sendmail)

You need to modify sendmail.cf: in the following way:

1. into the ruleset S0 (or S98) add following line :

```
R$*<@company.com.>$*     $# xlocal $@ company $: $1<@company.com.>$2

$# xlocal ... our "fake" mailer
$@ company .... the name of local mailbox
$: $1<@comany.com.>$2 ... recepient's address, which will be in X-Envelope-To he
```

2. into the mailers definition:

```
Mxlocal,        P=/usr/local/etc/bin/xlocal, F=lsDFMA, S=10/30, R=21,
                T=DNS/RFC822/SMTP,
                A=xlocal $u procmail $h

$u ... the address which will be in X-Envelope-To:   $1<@company.com.>$2
$h ... mailbox's name
A=xlocal $u procmail $h ... command line; we use procmail as local mailer

  Mailer's flags:
l  local mailer
s  clean address from garbage
D  add Date: header (if exists)
F  add From: header (if exists)
M  add Message-Id: header (if exists)
A  ARPA compatible mailer
```

Here is the source code for **xlocal** "fake" mailer.
Compilation:

```
cc xlocal.c
mv a.out xlocal
```