

WinProxy Help Index

[Contacting Ositis Software](#)

Getting Started

[Network configuration with WinProxy](#)

[Configuring and Installing WinProxy](#)

[Sample client configuration document describes how to configure client computers](#)

Troubleshooting

What is WinProxy..

[What is WinProxy, How does it work, and how can I use it?](#)

[What is HTTP?](#)

[What is FTP?](#)

[What is Telnet?](#)

[What is an Intranet?](#)

[What is an IP Address?](#)

How To ...

[Contact Ositis Software](#)

[Enter a new serial number](#)

[Load WinProxy before logging into Windows 95](#)

[Configure your web browser to support WinProxy](#)

[Configure your FTP client to work with WinProxy](#)

[Use your Telnet client with WinProxy](#)

[Administrate WinProxy remotely](#)

[Use America On Line with WinProxy](#)

Commands

[File menu](#)

[Help menu](#)

User Interface and Configuration

[Main Window](#)

[Properties Wizard](#)

[Advanced Properties](#)

[General Tab](#)

[Multiple IP Setup](#)

[Dial-Up-Networking Setup](#)

[Protocols Tab](#)

[HTTP Setup](#)

[FTP Setup](#)

[Telnet Setup](#)

[Socks Setup](#)

[DNS Setup](#)

[News Setup](#)

[Mail Setup](#)

[RealAudio Setup](#)

[Mapped Ports Tab](#)

[Edit Mapped Ports](#)

[Users Tab](#)

[Edit Users](#)

[Cache Tab](#)

[Enter Serial Number Dialog](#)

[About Box](#)

WinProxy Features

[HTTP Proxy](#)

[America On Line Proxy](#)

[Secure Sockets \(SSL\) Proxy](#)

[FTP Proxy](#)

[Telnet Proxy](#)

[Name Caching](#)

[Blacklist](#)

[Logging](#)

[Proxy Cascading](#)

Contacting Ositis Software

Ositis software can be contacted at:

E-Mail: **Support@Ositis.com**
Fax: **510-734-1904**
Telephone: **510-734-1900.**

Look for our web page at **<http://www.WinProxy.com>**.

Please feel free to contact us with suggestions, feature requests, technical questions or customized versions of WinProxy.

For **Ordering Information:**

You can purchase WinProxy on-line from Maagnum Resources, a WinProxy reseller from a secure site at:

<http://www.WinProxy.com/purchase>

Please send a check or money order for \$299.00 plus \$5.00 shipping and handling (\$15 international) in US funds to :

Ositis Software
6150 Stoneridge Mall Dr #180
Pleasanton, CA 94588

Include your name, company, telephone number, e-mail address and postal address. We will send a permanent serial number via e-mail within 7 days of receiving your order. If you desire the serial number by other means, please specify with your payment. Keep in mind that we must charge sales tax to California residents.

The serial number you receive entitles you to a single license of WinProxy and to upload free upgrades for one month after the serial number is issued. There will be at least three releases in each calendar year and each registered customer will be notified by e-mail when new releases become available. After your year of free upgrades expires, your current version of WinProxy will continue to function, but later versions will require a new serial number. Upgrades that solve critical security problems, will be free of charge to all registered customers.

Non-profit or educational institutions should contact Ositis Software for special pricing information.

For **Technical Support:**

- Look for information on our web page at **<http://www.WinProxy.com>**.
- **Send E-Mail to Support@Ositis.com.** Please include the following information:
 - Your **name, company, e-mail and telephone number.** We will not respond to help requests without this information.
 - Your **serial number** (even if it is an evaluation number)
 - The **operating system** and **type of computer** you are using

The most effective way to contact us is through e-mail.

Common Questions:

Each time I connect to the Internet, I get a new IP address, and WinProxy tells me that my IP addresses have changed. How does WinProxy support dynamically assigned IP addresses?

This problem is generally caused by a misconfiguration in WinProxy.

Select Advanced Properties from the WinProxy File menu, and select the IP address of your network card as the Internal IP address. This address should NOT be the same as your Internet IP address assigned by your service provider. If you do not have a unique IP address assigned to your internal network card, then select Settings/Control Panel from the Start menu, select Networking, and add the TCP/IP protocol to your Internal network card.

I think I have configured WinProxy correctly, but I can't seem to get my client computers to work.

WinProxy can dynamically generate a document that describes how to configure your client computers. Select 'Show Client Configuration' from the WinProxy file menu. A document will be displayed that describes how your client computers should be configured. This document is changed each time you reconfigure WinProxy, so you should consult this document any time you make changes.

Do I need to run WinProxy on all the machines on my network, or only on the computer connected to the Internet?

You only need to run WinProxy on the computer that is connected to the Internet.

How do I use command line FTP clients with WinProxy?

WinProxy uses the user@site method of proxying FTP. You must first connect to the computer running WinProxy, and then instruct it to connect to the site you are interested in.

For example, if WinProxy is running on a machine called "Gateway", then you would do the following to connect to ftp://ftp.WinProxy.com:

```
ftp Gateway<Enter>
220 WinProxy (Version 1.0B5a) ready.
open anonymous@ftp.WinProxy.com<Enter>
Enter password for user anonymous:
username@domain.com
User logged in...
```

This will work from any workstation, including Linux, Windows 3.1, Windows 95, Windows NT, and all UNIX operating systems.

I entered port 21 as my FTP port in my browser. Why is FTP not working?

WinProxy supports three ways of proxying FTP:

The CERN proxy, typically on port 80
The Socks 4 proxy, typically on port 1080
The User@Site proxy, typically on port 21

Internet browsers typically use the CERN proxy to access FTP. This basically means that a request is made for an FTP file or directory, in a manner similar to an HTTP request. WinProxy is then responsible for retrieving the requested file or directory. This has its drawbacks, as you do not see hyperlinked directories.

The second method, is the Socks 4 proxy. Almost all current browsers support the Socks 4 proxy for all protocols, including FTP. This is a very flexible protocol, that allows the browser to establish connections with the FTP server directly and send its own commands to the server. As a result, this protocol allows your browser to create hyperlinks for the directories on the FTP server.

The third method is not used by web browsers at all. This FTP proxy method is used by programs such as CuteFTP or WS_FTP, which provide full access to FTP, including uploading and deleting files on the server.

If you will be using FTP from your web browser, you should enable the Socks proxy in WinProxy (as well as the DNS proxy, which is required by the Socks proxy) and configure your browser to use the Socks proxy for FTP. After you have enabled Socks, select Show Client Configuration from the WinProxy file menu, and it will tell you how to set up your browser to use Socks for FTP access.

Can a Windows 3.1 computer or a Macintosh access the Internet through a gateway running WinProxy?

Absolutely! Just about any operating system can be used behind WinProxy. As long as TCP/IP is properly installed on the computers behind WinProxy, you can access the Internet from that computer.

How do I setup WinProxy to run in the taskbar?

To run WinProxy in the taskbar, select Advanced Properties from the WinProxy File menu, and check the box marked 'Run in the taskbar under Windows 95 or Windows NT 4.0.'

In Windows 95, WinProxy will now load before windows log-on, and it will reside in the task bar when you are logged in. Under Windows NT 4.0, WinProxy still needs to be loaded in the startup group. WinProxy does not yet run as a service under Windows NT, but it will run as a service by mid January.

I configured WinProxy to run in the taskbar, but now I can't turn it off!

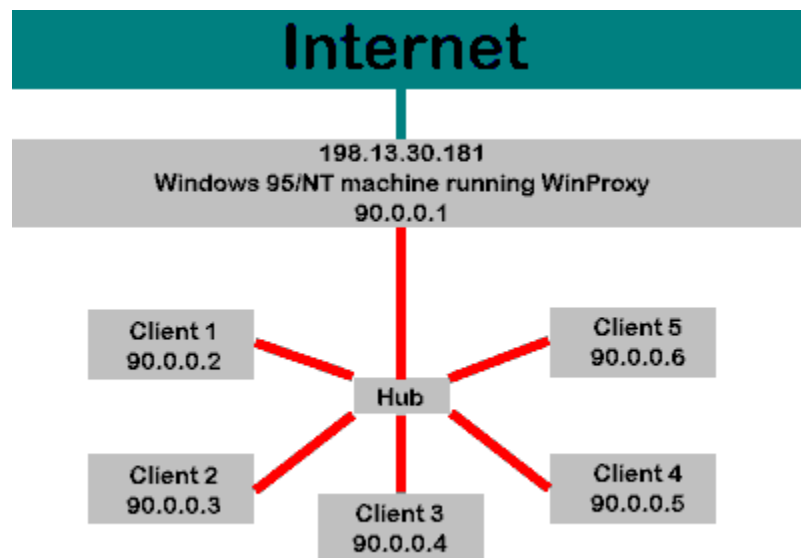
When WinProxy is running in the taskbar, then closing the user interface simply places the application back into the taskbar. To close WinProxy, you must right-click on the icon in the taskbar, and select Close.

I started WinProxy, but there is no window.

You probably have WinProxy configured to hide in the Windows taskbar. Look in your taskbar for an icon that looks like a small mask. Double click on that icon to display the WinProxy window.

Configuring your network with WinProxy

This diagram shows a typical network running WinProxy.



NOTE: This diagram shows a network hub connecting the internal network. If you are using coaxial cable or if you only have two computers with a cross connected cable, you will not need the hub.

In this example, the internal network is using a subnet of 90.0.0, meaning that it uses IP addresses from 90.0.0.1 through 90.0.0.254. The subnet mask used would be 255.255.255.0.

The computer running WinProxy has two network adapters (also known as a [Multi Homed Host](#)). One network adapter is connected to the Internet, and can be a Dial-Up-Adapter or a network adapter that is connected to another network that has Internet access. The Internet IP address is assigned by the Internet authorities. The other settings used for the network adapter that is connected to the Internet will also be assigned by the Network Administrator or the [Service Provider](#).

You should also look at some Security Considerations when configuring the Internet adapter.

Selecting an IP address

The second network Interface is referred to as your Internal network adapter. This adapter MUST have a permanent IP address. The IP address used here can be any address you want as long as the following conditions are satisfied:

It is on a different subnet from your Internet IP address. (In the above example, it can not be 198.13.30.182.

It is not commonly used on the Internet

The first condition is mandatory, as the TCP/IP stack on the WinProxy machine will not be able to determine which network card to use to request documents from the Internet if both network adapters appear to be on the Internet.

The second condition is only a practical one. If you were to assign an IP address that is used on the Internet to your Internal network adapter, then you will not be able to connect to the location on the Internet that does use that address. For instance, if you used subnet 204.71.177.68 in your internal

network, and IP address 204.71.177.68 as your IP address on the WinProxy machine, then you would not be able to connect to the Yahoo search engine, because they use the same subnet. When WinProxy tried to connect to Yahoo.com, the TCP/IP stack would attempt to connect to your internal network.

Other network settings

When configuring the Internal network adapter, you also need to set various other options. Although each network configuration is different, in most cases you should use the following settings:

IP Address: 90.0.0.1, or whatever other subnet you have chosen. This address must be unique on your network, and should not be one used on the Internet.

Subnet Mask: 255.255.255.0. This determines how much of your IP address is defined by your subnet. Using a subnet mask of 255.255.255.0 means you are on subnet 90.0.0 and can use IP addresses 90.0.0.1 through 90.0.0.254. If you change your subnet mask, the IP addresses you can use will also change.

DNS Configuration: You should leave this blank on the Internal network adapter, unless you are using an internal DNS server.

Default Gateway, or Installed Gateways: This should also be left blank, unless you have an internal router and multiple internal [subnets](#). If you do not have multiple subnets, leave this field blank.

WINS Resolution: Unless you are using an internal WINS server, you should leave this blank and disable WINS resolution. You may be running an NT server, which acts as a WINS server, in which case the IP address of that server should be entered here.

IP Forwarding: Unless you are using this computer to route requests between subnets (not recommended) you should disable IP Forwarding. Enabling IP Forwarding can make it possible for people on the Internet to access your computer.

Bindings: Unlike your external network adapter, you can enable all available bindings on this adapter. However, make sure your external network adapter does not have any bindings enabled.

Configuring TCP/IP on your client computers

The TCP/IP settings on your client computers should be the same as the settings on your WinProxy host, except for the following entries;

IP Address: Each client computer should have a unique IP address on the same subnet as the WinProxy host. If your host is using IP address 90.0.0.1 with a subnet mask of 255.255.255.0, then you should use IP addresses 90.0.0.2 through 90.0.0.254 on your client computers.

DNS Configuration: If you have enabled the DNS proxy in WinProxy, you should enter the Internal IP address of the WinProxy machine here. If you are using an internal DNS server, you should enter that address here.

Default Gateway, or Installed Gateways: Leave this blank, unless you have multiple subnets on your Internal network.

Consider implementing some basic [security considerations](#) as well.

Security Considerations

There are several things you can do to improve the security of your network. WinProxy protects the computers behind the server from access from the Internet, but, like all other proxy servers, it does not protect the server it is running on. You must make sure that server is not accessible from the Internet.

Ensure that Microsoft Windows File and Printer sharing is not accessible from the Internet.

Ensure that IP Forwarding is disabled if you are using Windows NT.

Ensure that any HTTP or FTP servers you are running are secure. Especially if you are using Windows NT, which automatically installs and FTP and HTTP server.

If you are using a Windows NT computer, consider enabling security in the Advanced settings for TCP/IP. You should basically disable all ports, except those that should receive incoming connections.

Properties Wizard:

If you are configuring WinProxy for the first time, it is highly recommended that you use the Properties Wizard, as it will guide you through the Installation process, making installation quick and easy.

Although the Properties Wizard allows you to configure the most common features in WinProxy, it is intended to help install WinProxy quickly, and does not offer access to all features. To access several more complex features you will need to use Advanced Properties.

To use the Properties Wizard, do the following:

- Connect to the Internet
- Select "Properties Wizard" from the WinProxy File menu
- Follow the instructions

When you are done, WinProxy will offer to display your [client configuration](#). This will display a document in Notepad, which describes how to configure the applications on the computers that will be connecting to the Internet through WinProxy. This document changes each time you change your WinProxy settings, so you should consult it every time you change your WinProxy settings.

You will then be asked to restart WinProxy. The changes you have made will not be enabled until you restart WinProxy, but restarting will terminate any active connections. If, for instance, somebody is downloading a large file from the Internet, that connection will be dropped when you restart WinProxy, and the user will have to start over. Restarting WinProxy should only take a few seconds, and you do not have to restart the computer.

See Also: [WinProxy Configuration](#)

Configuring WinProxy

The first thing you should do when you are configuring WinProxy is to **connect to the Internet!** This will make it much easier to configure WinProxy, because you will not have to enter IP addresses for your external servers, such as your mail servers, you will be able to enter the names, and WinProxy will automatically translate them to IP addresses.

All of the servers used by WinProxy are configured with IP addresses, not names. This is done for security reasons. You can, however, enter a name any time you are asked for an IP address, and WinProxy will automatically translate that name to the appropriate IP address, which will be stored.

There are two ways to configure WinProxy: the **Properties Wizard** and **Advanced Properties**.

Properties Wizard:

If you are configuring WinProxy for the first time, it is highly recommended that you use the Properties Wizard, as it will guide you through the Installation process, making installation quick and easy.

Although the Properties Wizard allows you to configure the most common features in WinProxy, it is intended to help install WinProxy quickly, and does not offer access to all features. To access several more complex features you will need to use Advanced Properties.

To use the Properties Wizard, do the following:

- Connect to the Internet
- Select "Properties Wizard" from the WinProxy File menu
- Follow the instructions

When you are done, WinProxy will offer to display your [client configuration](#). This will display a document in Notepad, which describes how to configure the applications on the computers that will be connecting to the Internet through WinProxy. This document changes each time you change your WinProxy settings, so you should consult it every time you change your WinProxy settings.

You will then be asked to restart WinProxy. The changes you have made will not be enabled until you restart WinProxy, but restarting will terminate any active connections. If, for instance, somebody is downloading a large file from the Internet, that connection will be dropped when you restart WinProxy, and the user will have to start over. Restarting WinProxy should only take a few seconds, and you do not have to restart the computer.

Advanced Properties:

More advanced users can use Advanced Properties to configure WinProxy. This option allows you to configure everything the Properties Wizard allows you to configure, in addition to other features.

Although it is not required, you should **connect to the Internet** before using Advanced Properties in WinProxy. This will allow you to enter computer names, instead of IP addresses. If you are not connected to the Internet, you will need to enter IP addresses for any external servers you need to configure.

The Advanced Properties dialog consists of four tabs:

<u>General Setup</u>	General WinProxy configuration.
<u>Protocols</u>	Enable and configure protocols supported by WinProxy
<u>Mapped Ports</u>	Configure mapped ports
<u>Users</u>	User administration to permit or deny access for individual users

Client Configuration Document

To see how to configure your client computers, you can select "Show Client Configuration" from the WinProxy File menu after WinProxy is configured. This will show you how to configure you client computers to access the Internet through WinProxy.

This document is generated dynamically, and will change as your configuration changes. You should print a new version of this document each time you change your WinProxy settings.

The instructions in this document tell you how to configure each client application assuming you are using the application. When it tells you to select Network Preferences from the Options menu in the Netscape description, the document is referring to the Options menu in Netscape, not WinProxy.

This sample document assumes that all protocols are enabled.

WinProxy Client Configuration
Ositis Software
<http://www.WinProxy.com>

This document should help you configure your client computers to use WinProxy. Throughout this document it is assumed that your internal subnets use a subnet mask of 255.255.255.0. If this is not the case, then some of the settings may be incorrect.

This document will change each time you reconfigure WinProxy. You should check to make sure you have accounted for any changes each time you reconfigure WinProxy.

This document is intended as a guide and may not necessarily represent your precise situation.

The IP addresses on your server should be configured such that each network adapter is on its own subnet. If your Internet IP address is 198.13.30.128, then your internal network IP addresses should not start with 198.13.30. We recommend using subnet 90.0.0 (IP addresses 90.0.0.1 through 90.0.0.255) on your internal network, because those addresses are not routable.

For computers connected to subnet 90.0.0, i.e. those directly connected to server IP address 90.0.0.2 :

** IP address configuration:

- * Use IP addresses from 90.0.0.1 through 90.0.0.255, excluding 90.0.0.2
- * Use a subnet mask of 255.255.255.0.

** DNS configuration:

- * Use a DNS server of 90.0.0.2.
- * Give each computer a unique name on your network.

* Select an appropriate domain name that will not conflict with names used on the Internet.

* If you are using other internal DNS servers, not recognized by WinProxy, then those should also be added to the DNS list on your client computers.

** Leave all other TCP/IP settings blank, unless your particular situation requires specific values.

** Applications:

* Netscape 3.0: Under Network Preferences in the Options menu, select the Proxies tab. Select Manual Proxy Configuration. Press View and enter the following information:

FTP Proxy: (leave blank)
FTP Proxy Port: (leave blank)
Gopher Proxy: (leave blank)
Gopher Proxy Port: (leave blank)
HTTP Proxy: 90.0.0.2
HTTP Proxy Port: 80
Security Proxy: 90.0.0.2
Security Proxy Port: 80
WAIS Proxy: (leave blank)
WAIS Proxy Port: (leave blank)
SOCKS Host: 90.0.0.2
SOCKS Host Port: 1080

No Proxy For: Enter the domain name you selected in your IP configuration.

Since you are using SOCKS, you should enter the real name of your mail server if you are using Netscape for mail. Netscape will use the SOCKS proxy to access mail. This way each client can also access a different mail server.

* Internet Explorer 3.0: Under Options in the View menu, select the Connection tab. In the Proxy Server section, check the Connect Through Proxy Server box, and press the Settings button.

Enter the same proxy information described under Netscape configuration.

Do not check the box to use the same proxy for all protocols.

* In your Mail client:

Set the SMTP server to 90.0.0.2.
Set the POP3 server to 90.0.0.2.

* In your IMAP4 client:

Set the IMAP4 server to 90.0.0.2.

* In your News client:

Set the News server to 90.0.0.2.

- * CuteFTP: Under Options from the FTP menu, select the Firewall tab.

Enter 90.0.0.2 as the host, and 21 as the Port.

Select the User@Site proxy type.

Check the box to Enable firewall access

- * WS_FTP: Under Session Properties, select the Firewall tab.

Enter 90.0.0.2 as the Host Name.

Enter 21 as the Port.

Check the box to Use Firewall

Select the "USER with No Logon" Firewall Type.

- * mIRC: Select Setup from the File menu, and select the Firewall tab.

Check the box labeled "Use SOCKS firewall"

Enter 90.0.0.2 as the Hostname

Enter 1080 as the Port

- * RealAudio: Select Preferences from the View menu, and select the Proxy tab

Check the box labeled "Use Proxy"

Enter 90.0.0.2 as the RealAudio Proxy

Enter 1090 as the RealAudio Proxy Port

Enter 90.0.0.2 as the HTTP Proxy

Enter 80 as the HTTP Proxy Port

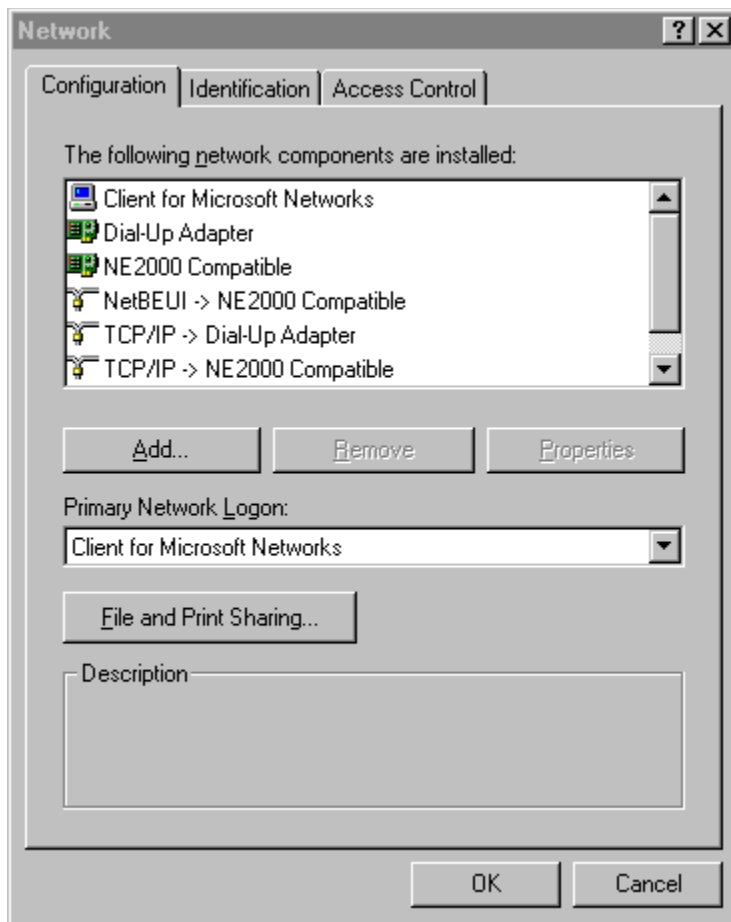
Disable File and Printer Sharing

Windows 95:

There are two things you can do to disable access to your machine from the Internet. The best thing to do is to remove File and Printer sharing from the firewall machine altogether. If the server is sharing files, there will always be a small risk that users on the Internet will gain access. The following instructions should minimize, if not eliminate, that risk if you do require file and printer sharing on your server.

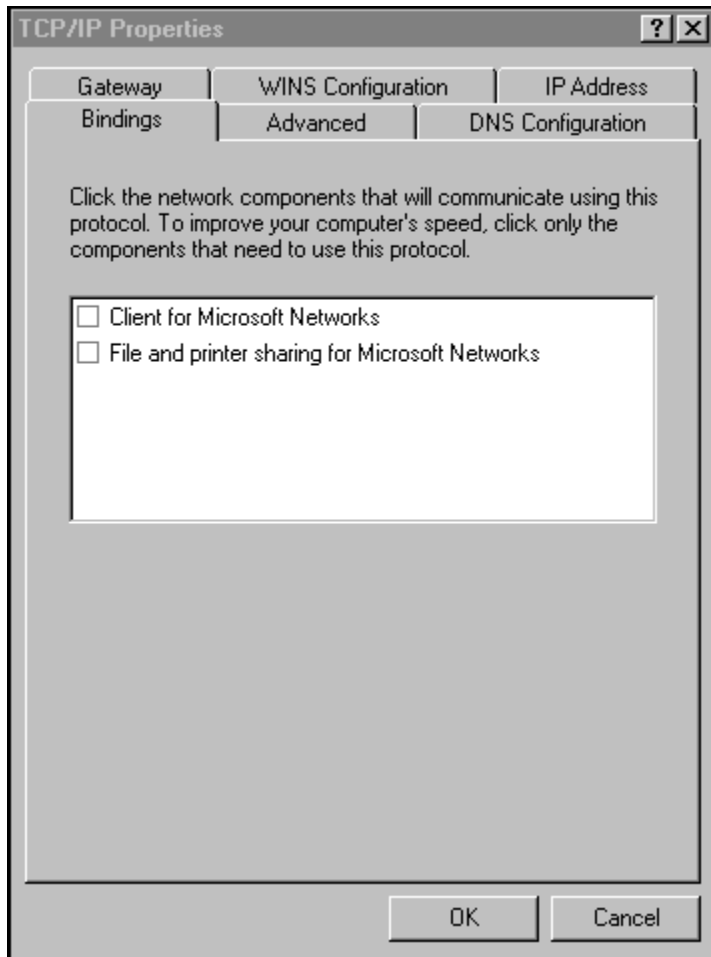
To ensure that file and printer settings are disabled for your Internet connection:

- Select Settings from the Start Menu
- Select Control Panel in the Settings menu
- Double click the Networking icon in the Control Panel to display a dialog similar to this:



In the above dialog, you can see that there are several protocols installed for networking: TCP/IP and NetBEUI. Only TCP/IP, however, is enabled for the external network adapter (Dial-Up Adapter.) If you have an entry in your network configuration that reads "NetBEUI -> Dial-Up Adapter" then you should select it and press the Remove button.

Select the line labeled "TCP/IP -> Dial-Up Adapter" and press properties, to configure the TCP/IP stack used with the Dial-Up Adapter. Select the Bindings tab, and you should get a dialog similar to this one:

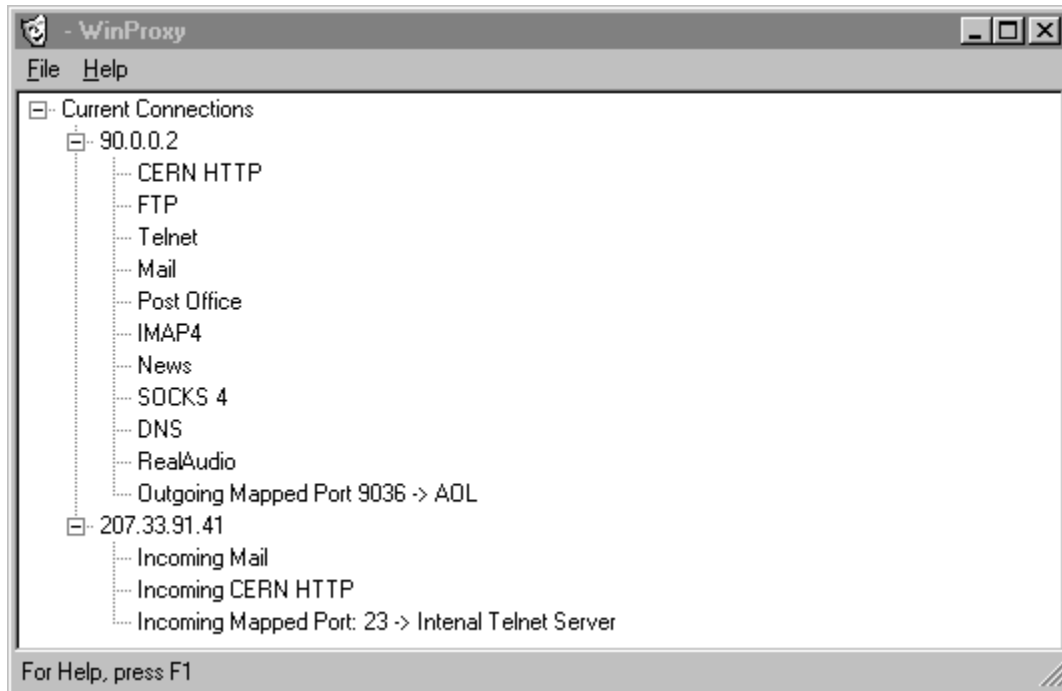


Notice that we have unselected both File and Printer sharing and Client for Microsoft Networks. This will disable access to file and printer sharing in from the Internet. When you leave this dialog, Windows will tell you that you have not configured a protocol for this adapter, "would you like to select one now?" You don't want to select one now! We specifically want these protocols to be disabled.

Press OK until you are asked to restart Windows.

WinProxy Main Window

WinProxy has a feature called ConnectionView, that allows you to see what connections are being made through WinProxy, and who is making the connections. As connections are established they show up in the view, and they disappear shortly after they are complete. This feature requires quite a bit of processor power, and can slow down WinProxy. If you feel that WinProxy is running a little slow, you should turn off this feature in the Advanced Properties menu.



This is a typical view of the WinProxy screen when no connections are active. The top two entries, 90.0.0.2 and 207.33.91.41 show the connections that WinProxy is accepting. Each entry shows the name of the proxy protocol, that is listening for connections.

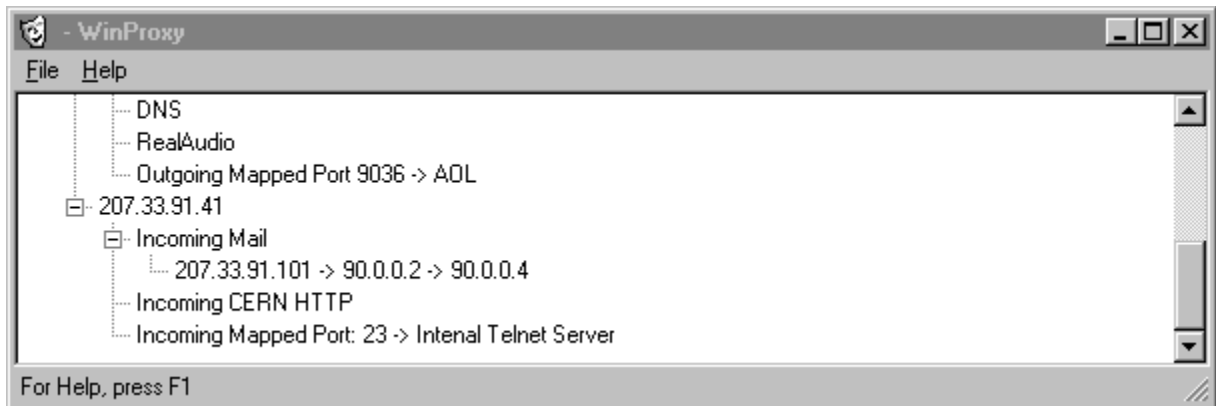
If you do not have any incoming proxies configured, you will only see a node for each internal IP address, usually there will only be one.

In this example, 90.0.0.2 is the Internal IP address and 207.33.91.41 is the external IP address. If you do not have any incoming protocols configured, you will not see the second entry for incoming connections. WinProxy Lite does not support incoming connections.

When a connection is established on each of the protocols, this screen will be updated with the IP address of the user requesting the connection, the IP address of the network interface establishing the connection, and the IP address of the destination. In most cases it will also describe the connection, and the document being requested.



In this example, you can see that the user at 90.0.0.2 (in this case the same computer as the one WinProxy is running on) is requesting the document <http://www.WinProxy.com/WProxyB5f.exe>. The IP address for www.WinProxy.com is 206.86.186.189 and the IP address used to connect is 207.33.91.41. If the requested page were internal, then the second IP address could be 90.0.0.2.



In this example, you can see that an external user has connected to the reverse mail proxy to send mail. The Incoming Mail proxy allows users on the Internet to connect to an internal SMTP server. In this case, a user at 207.33.91.101 has connected to the external IP address for WinProxy. WinProxy then forwarded the connection to the Internal Mail server at 90.0.0.4. The reverse proxy feature is only available in the unlimited user version of WinProxy.

Using America On Line with WinProxy

Although America On Line claims that it is not possible, WinProxy supports proxying of AOL sessions. **No other proxy server supports this feature!!!**

To use AOL with WinProxy, you will need to enable the following:

- Enable America On Line in the [Protocol Tab](#) (either in the [Setup Wizard](#), or [Advanced Properties](#))
- Enable the [DNS](#) proxy in WinProxy.
- Enter [DNS Setup](#), and set the external DNS server to the DNS server provided by your [Service Provider](#).
- Configure the client computers that need to use AOL to use WinProxy as the Name Server. (Detailed information on configuring client applications can be found in the [Client Configuration Document](#), by selecting "Show Client Configuration" from the WinProxy [File Menu](#))

You will need to restart each client computer after changing the name server to point to WinProxy. You will then be able to simply start up America On Line, and connect via TCP/IP.

To configure America On Line to use TCP/IP, do the following:

- Press the Setup button in the AOL sign-on screen
- Select the location you typically use, or create a new one.
- Press "Edit Location"
- For each list box labeled "Network:" select the option called TCP/IP.

Network Setup

Location: Network Connection

Phone Type: Touch Tone Pulse

Phone Number: Phone Number:

Modem Speed: 2400 bps Modem Speed: 2400 bps

Network: TCP/IP Network: TCP/IP

Use the following prefix to reach an outside line: 9,

Use the following command to disable call waiting: *70,

Save Swap Phone Numbers Cancel

- Press "Save"
- Press OK to get out of Network & Modem Setup
- Press Sign On to connect to AOL!!

File menu commands

The File menu offers the following commands:

<u>Properties Wizard</u>	Starts a configuration wizard that will walk you through configuring WinProxy. The properties wizard allows you to configure the most common settings. For more detailed configuration, use Advanced Properties.
<u>Advanced Properties</u>	Allows detailed configuration of WinProxy.
<u>Set New Serial Number</u>	If you are running the demonstration version of WinProxy, this menu is present and allows you to enter a new serial number. If your current serial number is not a demonstration serial number, this menu item is not present.
<u>Exit</u>	Exits WinProxy.

Help menu commands

The Help menu offers the following commands, which provide you assistance with this application:

[Help Topics](#) Offers you an index to topics on which you can get help.

[About](#) Displays the version number of this application.

Set New Serial Number (File menu)

Use this command from the *file menu* to enter a new [serial number](#) or change your registration information.

This will initiate a [Registration Dialog](#) box requesting a serial number and your registration information. If you already have a permanent serial number, leave the serial number field blank, but you should keep your registration information updated to receive technical support.

If you have not yet entered a Serial Number, then this menu will allow you to enter a serial number to allow permanent usage of WinProxy.

[Contact Ositis Software](#) to purchase a permanent serial number.

Exit command (File menu)

Use this command to end your WinProxy session. You can also use the Close command on the application Control menu. WinProxy prompts you to save documents with unsaved changes.

Shortcuts

Mouse: Double-click the application's Control menu button.



Keys: ALT+F4

Using Help command (Help menu)

Use this command for instructions about using Help.

About command (Help menu)

Use this command to display the copyright notice and version number of your copy of WinProxy.

Help Using Help Command



Use the Context Help command to obtain help on some portion of WinProxy. When you choose the Toolbar's Context Help button, the mouse pointer will change to an arrow and question mark. Then click somewhere in the WinProxy window, such as another Toolbar button. The Help topic will be shown for the item you clicked.

Shortcut

Keys: SHIFT+F1

Title Bar

The title bar is located along the top of a window. It contains the name of the application.

To move the window, drag the title bar. Note: You can also move dialog boxes by dragging their title bars.

A title bar may contain the following elements:

- Application Control-menu button
- Document Control-menu button
- Maximize button
- Minimize button
- Name of the application
- Name of the document
- Restore button

Move command (Control menu)

Use this command to display a four-headed arrow so you can move the active window or dialog box with the arrow keys.



Note: This command is unavailable if you maximize the window.


Shortcut

Keys: CTRL+F7

Minimize command (application Control menu)

Use this command to reduce the WinProxy window to an icon.

Shortcut

Mouse: Click the minimize icon  on the title bar.

Keys: ALT+F9

No Help Available

No help is available for this area of the window.

No Help Available

No help is available for this message box.

What is an Intranet?

An Intranet is a network of computers that connects all of the computers in an organization and is generally not accessible to computers outside of that organization.

Multi-homed host

A multi-homed host is a computer that resides on two [subnets](#) and, therefore, has at least two [IP addresses](#).

IP Address

An IP Address is a 32 bit number, usually expressed as four numbers separated by periods, such as 192.0.0.12. This is a unique number in which some of the most significant bits define a [subnet](#).

Subnet

A subnet is a network of computers that communicate with each other directly. In a TCP/IP network, a number of significant bits in the IP Address define the subnet. IP Addresses that are not on the same subnet must be reached by going through a router, which forwards network packets between subnets.

Connection

A TCP/IP connection is a link between two [IP Addresses](#). An application can [listen](#) for a connection on a specific IP address and [port number](#). Other computers can then establish a connection to that application by connecting to the specific IP address and port number.. If the receiving computer is willing to establish a connection, it will [accept](#) the request, completing the link.

Port Number

Each time a computer accepts or listens for a connection on a specific [IP Address](#), it is using a [Port Number](#). The port number distinguishes various [connections](#) or network processes on a computer.

Although all connections have a unique port number, the port number is usually used to allow one process to connect with another specific process on a computer. [HTTP](#), for instance, uses port 80 to listen for connections. By having a port number as well as an IP address, many processes can be listening for connections on a single computer.

HTTP

HTTP (HyperText Transfer Protocol) is the name of the protocol used by the World Wide Web . This is a client/server based protocol that allows computers to retrieve documents from another computer. The World Wide Web uses, but is not limited to, HTML documents.

HTTP servers usually listen for [connections](#) on [port](#) 80.

HTML

HTML (HyperText Markup Language) is a document encoding format, that allows documents to be written with links to other documents, images and bookmarks. This format is used in the World Wide Web to format documents in a device and application independent way.

World Wide Web

The World Wide Web is a network of computers on the Internet that uses HTTP and HTML to provide graphical documents to Internet users.

FTP

FTP (File Transfer Protocol) is the name of the protocol used in the internet to transfer files between computers. Although HTTP can also be used to receive files, FTP allows users to browse directories and upload and download files to a remote computer.

FTP servers usually listen for connections on port 21.

Telnet

Telnet is the name of the protocol used in the internet to connect to other computers through a remote connection.

The Telnet Protocol provides a standard way to communicate with another computer as if you were typing at the console of that computer. Telnet does not, however, provide a graphical interface such as the [World Wide Web](#) or X-Windows.

CERN

CERN (European Laboratory for Particle Physics) is the birthplace of the World Wide Web .

The CERN group, including Tim Berners-Lee, known as the father of the World Wide Web, devised the HTTP protocol and the protocols used to proxy with it. The CERN proxy protocol includes a method to proxy HTTP, FTP and other protocols through a HTTP proxy server.

This is the proxy protocol used by Netscape's Navigator® and Microsoft's Internet Explorer®.

Mail

Electronic mail is transmitted over the internet using two protocols: [SMTP](#), and [POP3](#). [IMAP4](#) is also occasionally used.

When you send electronic mail, your e-mail client application first connects to its designated SMTP server, gives it your e-mail name the destination name and the text of the document you are sending. The SMTP server then reads the text behind the '@' in the destination address and connects to the POP3 server at that location and gives it the message you are transmitting.

The user on the other end later opens another e-mail application, which connects to the same POP3 server to determine if any mail has arrived. The server responds with a message stating that mail has arrived and the e-mail client retrieves the mail.

Essentially, the SMTP server acts as a delivery agent to assist in sending mail. An SMTP server, may, in fact, transfer the mail to another SMTP server before it stops at a POP3 server.

The POP3 Server is merely a post office that holds mail until a user is ready to read it. This allows mail to be delivered to a computer that is not currently on-line, because when that user DOES come on-line, the mail will be waiting. The POP3 server is always on-line.

SMTP

SMTP or Simple Mail Transport Protocol is the protocol used to transmit mail to the receiving mail server. Usually mail sent using SMTP ends up in a [POP3](#) server where it can be retrieved by a user.

Mail may travel through multiple SMTP server before reaching a post office.

See also [Internet Mail](#)

POP3

POP3 or the Post Office Protocol is the protocol used to receive mail that is stored in a post office. Since most mail recipients are not constantly on-line,

to the receiving mail server. Usually mail sent using SMTP ends up in a [POP3](#) server where it can be retrieved by a user.

Mail may travel through multiple SMTP server before reaching a post office.

See also [Internet Mail](#)

IMAP 4

IMAP 4 is a new post office protocol similar to POP 3. It offers better mail retrieval capabilities than POP 3 services which, generally, results in faster access.

If you do not know what it is, you probably don't need it.

RealAudio

RealAudio is a protocol developed by Progressive Networks which allows you to listen to streaming audio on the Internet. The latest versions of real audio enable you to receive CD quality sound over connections as slow as 28.8kBPS! You can learn more about RealAudio on Progressive Networks' web site at: <http://www.RealAudio.com>.

Serial Number

WinProxy requires a serial number in order to function beyond the 30-day trial period. If you have not yet purchased WinProxy, you can leave the serial number field blank and use WinProxy during the trial period.

When you purchase WinProxy you will need to enter the serial number into the software, by selecting Set New Serial Number from the [File menu](#). After entering your registration information and your serial number, WinProxy will automatically upload your registration to our database. Only the information entered will be sent and the information is encrypted for privacy.

[Contact Ositis Software](#) to purchase a permanent serial number.

Internal IP Address

The Internal IP address is the IP address which WinProxy will use to listen for connections. This value should be set to the IP address that is directly connected to the **internal network**.

WinProxy will only accept connections on the internal IP address. All other connections will be refused.

CERN Proxy Port

The [port](#) on which WinProxy listens for [connections](#), using the [CERN](#) Proxy specification.

WinProxy supports the CERN Proxy protocol for [HTTP](#) and [FTP](#). A CERN proxy server will usually listen for connections on the HTTP port and proxy other protocols using the HTTP protocol. Hence, it only listens for connections on a single port.

This is the proxy protocol used by Netscape's Navigator® and Microsoft's Internet Explorer®.

The range of valid values is from 1 through 32000.

Logging Port

WinProxy can log all activity that takes place through the proxy server. [Logging](#) is done by establishing a [connection](#) between WinProxy and the WinProxy sample [logging application, ProxyLog](#). The connection is established when WinProxy is started or when it is specifically requested through [remote configuration](#). If WinProxy is unable to connect to a logging application, then it will continue to function with logging disabled. For security reasons, WinProxy does NOT listen for a connection from the logging application.

The ProxyLog application listens for a connection on the [port number](#) specified here and writes all logging information to the screen as well as to a log file, if requested. **Although it is possible to send logging information outside of the intranet, this is not recommended, since it would be a significant security risk.**

This parameter, along with the [Logging IP Address](#), tells WinProxy the location of a logging application, which can even be located on the same machine as WinProxy. Placing the logging application on the same machine as ProxyLog can reduce the bandwidth used for logging, but may open a security hole when the connection has not been established. ProxyLog can be modified to prevent this problem, by requiring logging connection only from the local computer.

If this value is left blank (or invalid) then logging will be disabled. This is an option when monitoring network traffic is not necessary.

The range of valid values for this setting is from 1 through 32000.

Logging IP Address

WinProxy can log all activity that takes place through the proxy server. [Logging](#) is done by establishing a [connection](#) between WinProxy and the WinProxy sample [logging application, ProxyLog](#). The connection is established when WinProxy is started or when it is specifically requested through [remote configuration](#). If WinProxy is unable to connect to a logging application, then it will continue to function with logging disabled. For security reasons, WinProxy does NOT listen for a connection from the logging application.

The ProxyLog application listens for a connection on the [port number](#) specified here and writes all logging information to the screen as well as to a log file, if requested. **Although it is possible to send logging information outside of the intranet, this is not recommended, since it would be a significant security risk.**

This parameter, along with the [Logging Port](#), tells WinProxy the location of a logging application, which can be located anywhere on the network or on the same machine as WinProxy. See [Logging Port](#) or [Logging Application](#) for more information on logging.

This value must be a valid [IP Address](#) and should be somewhere within the intranet for security. The Logging Port must also be specified for logging to be enabled.

Cascading Port

WinProxy can be run on a [subnet](#) behind another proxy server, providing an additional layer of security for that subnet. In this case computers outside of the subnet will not have access to the computer inside of this subnet, and computers inside this subnet can communicate with other computers beyond a second firewall.

See [Proxy Cascading](#) for more information on cascading.

This value must be set to the [port number](#) of the next proxy server. If this is left blank (or is invalid), then proxy cascading is disabled. The [Cascaded Proxy IP](#) Address must also be configured for Proxy Cascading to function.

The allowed values are from 1 through 32000.

Cascading Proxy IP Address

WinProxy can be run on a [subnet](#) behind another proxy server, providing an additional layer of security for that subnet. In this case computers outside of the subnet will not have access to the computer inside of this subnet, but computers inside this subnet can communicate with other computers beyond a second firewall.

See [Proxy Cascading](#) for more information on cascading.

This value must be set to the [IP Address](#) of the next proxy server. If the [Cascading Port](#) is left blank, then proxy cascading is disabled.

Administration IP

Some WinProxy features can be configured through [remote configuration](#). Since there is some security risk in allowing anybody to perform these actions for WinProxy, it is possible to limit this function to be allowed only from a specific [IP address](#).

If this value is set to 0.0.0.0 or left blank, then administration can be done from any computer behind the firewall. Administration can NEVER be done from outside of the firewall, because WinProxy does not accept connections from outside the firewall.

If administration is to be disabled, then this value should be set to an invalid IP Address. 127.0.0.0 is a good choice, since it is not a valid IP Address.

Use Dial-Up-Networking

Check this box if you want WinProxy to automatically connect to the Internet when it is required. The Dial-Up-Networking set allows you to configure where WinProxy should dial, what user name and password should be used and when the connection should time-out and be disconnected.

Verify IP Addresses With Reverse Name Lookup

A popular way of breaking into a firewall is to use [DNS Spoofing](#) or [IP Spoofing](#). By performing a [Reverse Name Lookup](#) on each connection and caching the results, WinProxy significantly reduces the risk of retrieving invalid information or connecting to a different network than was requested.

This checkbox enables this additional security feature in WinProxy. If this is not selected, WinProxy will continue to cache names, but will not verify their validity through a Reverse Name Lookup.

If WinProxy finds that the Reverse Name Lookup does not return the requested name, the name and BOTH [IP Addresses](#) will be placed in the WinProxy [blacklist](#). They can be removed from the blacklist using [remote configuration](#) or by restarting WinProxy.

This feature protects people inside the firewall from receiving invalid information by connecting to a web server, that is masquerading as another. For instance, a hacker could create a news report stating that the stock market has crashed, and pretend to be serving the web page for Reuters News Service. The Reverse Name Lookup feature will add that IP Address to the blacklist, preventing users from receiving invalid information.

Another potential security risk in [JAVA](#), which is usually allowed to connect only to the IP Address from which it was delivered. Without this feature and [Name Caching](#) JAVA applets could connect to another IP Address, causing a security risk.

Some Windows TCP/IP packages do not support aliases correctly, and it may be the case that a reverse name lookup fails on a valid name. When this happens that name and IP Address will be placed in the blacklist. If this happens often, this feature should be disabled. When this DOES happen, the blacklist should be reloaded from disk, using [remote configuration](#).

Supported Protocols

This is a list of all supported protocols. Each protocol can be enabled or disabled by using its checkbox on the left and can be configured by pressing the button on the right.

Each protocol has a different set of configuration options.

In the future other protocols will be added to this area.

HTTP Protocol

This checkbox enables or disables proxying of the [HTTP](#) protocol.

If this box is not checked, then the [CERN](#) HTTP proxy feature of WinProxy will be disabled.

FTP Protocol

This checkbox enables or disables proxying of the [FTP](#) protocol.

This enables both the [CERN FTP](#) proxy as well as the regular FTP proxy features of WinProxy.

The regular FTP proxy uses the name@host type of proxy server. It does NOT use a PASV proxy method. To use the FTP proxy, it is recommended that you use an FTP client that is capable of using the name@host method, such as **CuteFTP**, available from <ftp://papa.indstate.edu/winsock-l/ftp>

Telnet Protocol

This checkbox enables or disables proxying of the [Telnet](#) protocol.

The Telnet protocol proxy accepts [connections](#) on the specified [port](#), presents instructions for the user and requests the name of the Telnet host.

Because the Telnet protocol basically enables anybody inside the firewall to establish an unfiltered bi-directional connection to the outside of the firewall, MIS managers should consider disallowing this protocol for security reasons.

The Telnet proxy requires the destination connection to be on the Telnet port, 23.

WinProxy Blacklist

WinProxy provides the ability to blacklist a series of [host names](#) and/or [IP Addresses](#). WinProxy compares all requests to the names and IP Addresses in the blacklist before completing the connection. If the host name, IP Address or an [alias](#) is in the blacklist, then the [connection](#) will be forbidden.

The following is an example of a blacklist file:

```
; Comments in the blacklist file should be prefaced with a semi-colon
badhost.com
www.otsobadhost.com

; All connections to Latvia will be denied
lv

; Blacklist a specific IP Address
198.105.232.5

: Blacklist a name along with an IP Address
playboy.com          205.216.146.202

; Blank lines are ignored

; Bad blacklist string, only one name allowed per line,
; only microsoft.com will be blacklisted:
microsoft.com        msn.com
```

In the above example, the following requests would be allowed or denied:

www.badhost.com	Denied because of badhost.com
www.reallybadhost.com	Allowed , reallybadhost is a different domain from badhost.com
mail.otsobadhost.com	Allowed , only www.otsobadhost.com is disallowed.
web.otsobadhost.com	Denied , if web.otsobadhost.com is an alias for www.otsobadhost.com
www.latnet.lv	Denied , this is in the lv network.
lv.yahoo.com	Allowed , lv only restricts the network name
198.105.232.5	Denied , the IP address is blacklisted
www.playboy.com	Denied , in the playboy.com domain.
205.216.146.201	Denied , Reverse name lookup shows the name to be www1.playboy.com, which is a blacklisted name
205.216.146.202	Denied , the IP Address is blacklisted.

To deny access to a specific computer, it is recommended that the actual IP Address be used, since aliases are not always reported correctly in Windows TCP/IP stacks. A hacker could use an alias to circumvent the blacklist.

The blacklist is read from a file named **blacklist.pxy** located in the working directory of WinProxy. If you use a shortcut to execute WinProxy, then you should make sure that blacklist.pxy is located in whatever working directory is specified in the shortcut.

Logging Application

WinProxy ships with the source code and binary for a [Logging](#) console application called **ProxyLog.EXE**.

Registered WinProxy users (with a permanent serial number) are free to modify and distribute the ProxyLog source code and the binaries created from it. In fact, we will be happy to help you distribute your logging application through our web site as soon as it is operational.

When WinProxy loads, it establishes a [connection](#) to a [port](#) and [IP Address](#) specified in the [properties dialog](#). If the connection is lost, [remote configuration](#) can be used to instruct WinProxy to re-connect to the logging application.

Once the connection is established, WinProxy will send logging information to the Logging Application, which can display it on the screen, save it in a file and sort or highlight it in any way desirable. The current version of ProxyLog simply outputs all of the events to the screen and a file specified on the command line.

There is no communication from the logging application to WinProxy.

IP Spoofing

Since [IP Addresses](#) can be assigned by anybody to anything they desire, it is possible for a hacker, to publish themselves under an IP Address used by a legitimate business. [Connections](#) requesting that IP Address, could fail to connect to the appropriate computer. The hacker can then appear to be somebody else.

This is usually used with incoming [connections](#), rather than outgoing connections, where a specific IP Address is required to gain access to a [subnet](#).

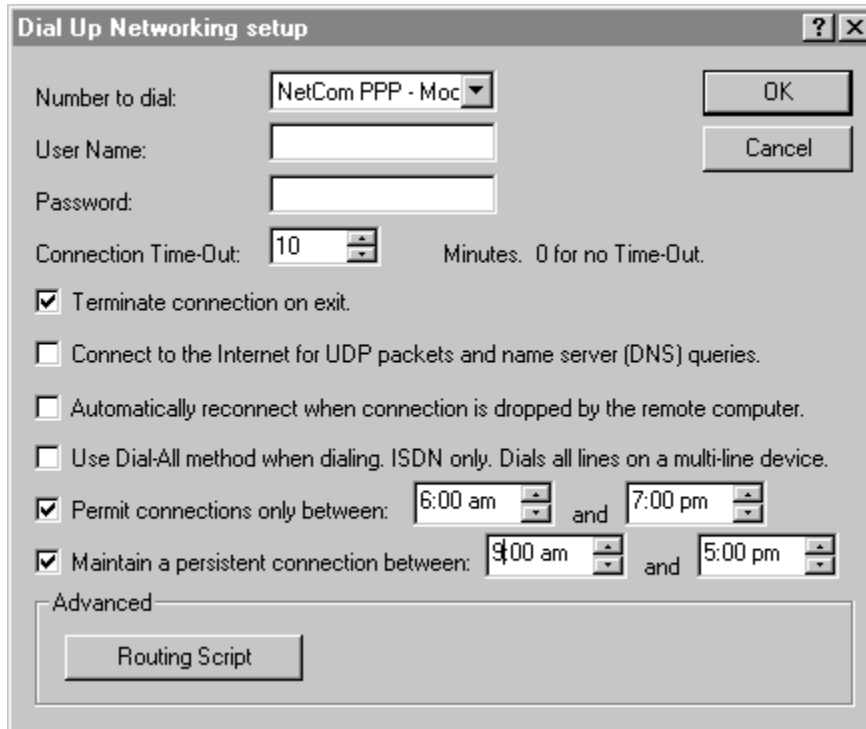
WinProxy does not accept connections from anybody outside the intranet, and is, therefore, not susceptible to being fooled by incoming connections masquerading as another IP Address, but if the logging application is external to the intranet, a hacker could gain access to your private logging information.

Without authentication it is impossible to completely shield a company from IP Spoofing, but it is very difficult to do without direct access to an access provider or other key routers on the backbone. Since the greatest danger is for incoming connections WinProxy is as safe a firewall as is possible.

Dial Up Networking Setup

Dial Up Networking enables WinProxy to connect to the Internet as necessary. When a user connects to WinProxy, then WinProxy will automatically use Microsoft's Dial-Up-Networking to dial the modem and connect to your [service provider](#).

To enable Dial-Up-Networking, check the "Use Dial Up Networking" box in the [General Properties](#) dialog or in the [Properties Wizard](#), and then press the Dial-Up Setup button, to configure dialing.



Number to dial Select the number to dial from the phone book. The drop down list shows all the entries in your dial-up networking phone book. Select the entry you wish to dial to connect to the Internet. WinProxy will dial this number in order to connect to the Internet.

User Name Select the logon name to use when connecting to the Internet. This name was assigned by your [service provider](#), and will be used when WinProxy logs onto the Internet.

Password Enter the password to use when logging into the Internet. This is required for WinProxy to automatically connect to the Internet. If you change your password, be sure to change it in this field as well.

Connection Time Out WinProxy can disconnect from the Internet when you are not using it. This can significantly reduce your online time, and charges. When a user requests a connection, WinProxy will return a document stating that it is connecting (only for [World Wide Web](#) access), connect to the Internet, and establish the connection.

Set this number to 0 if you want WinProxy to stay connected permanently.

- Terminate on exit Check this box if you want WinProxy to close its connection when you exit WinProxy. If you do not check this box, the connection will be left active when you exit WinProxy. This can be convenient when you are configuring WinProxy.
- Connect for UDP Check this box if you want WinProxy to connect to the Internet for any connection it receives, including name lookup requests and other unconnected requests. If this box is checked WinProxy may appear to connect to the Internet for no reason.
- Automatic Reconnect Check this box only if you want WinProxy to automatically reconnect to the Internet when the connection is dropped. Otherwise WinProxy will automatically cancel the connection, reconnecting only when a request demands it. Unless it is important that the Internet connection stay connected at all times, you should leave this box unchecked.
- Use Dial-All Method This option is only available under Windows NT 4.0. Windows NT 4.0 Dial-Up Networking provides two dialing methods for lines, such as ISDN, that have multiple bandwidth capabilities. If you check this box, WinProxy will change the dialing options for the selected entry, to use the Dial All method. Depending on your hardware, this will cause multiple lines to be dialed when connecting.

The alternate method uses the Dial As Needed method of dialing. As far as we can tell, that option does not actually work as specified in Windows.

DNS Spoofing

DNS (Domain Name Server) Spoofing is similar to [IP Spoofing](#) **except** that instead of pretending to be a different [IP Address](#), a name lookup is faked to return an incorrect IP Address. This is a fairly common way for hackers to gain access to proprietary information, including credit card numbers and bank accounts.

Each time the computer looks up a name, such as WWW.OSITIS.COM, it makes a request to a domain name server, which, if it does not know the IP Address, makes a request to another domain name server. At any point, a hacker can intercept the request and provide a fake response pointing to their own IP Address. Then when a request is made to that computer, instead of requesting a document from the computer specified by the name, the request will be made of the hackers' computer.

WinProxy provides three types of protection against this type of attack:

Reverse Name Lookups are used to verify that the IP Address really represents the name that was requested. This feature is enabled by the [Verify IP Address](#) option in the [Properties](#) dialog.

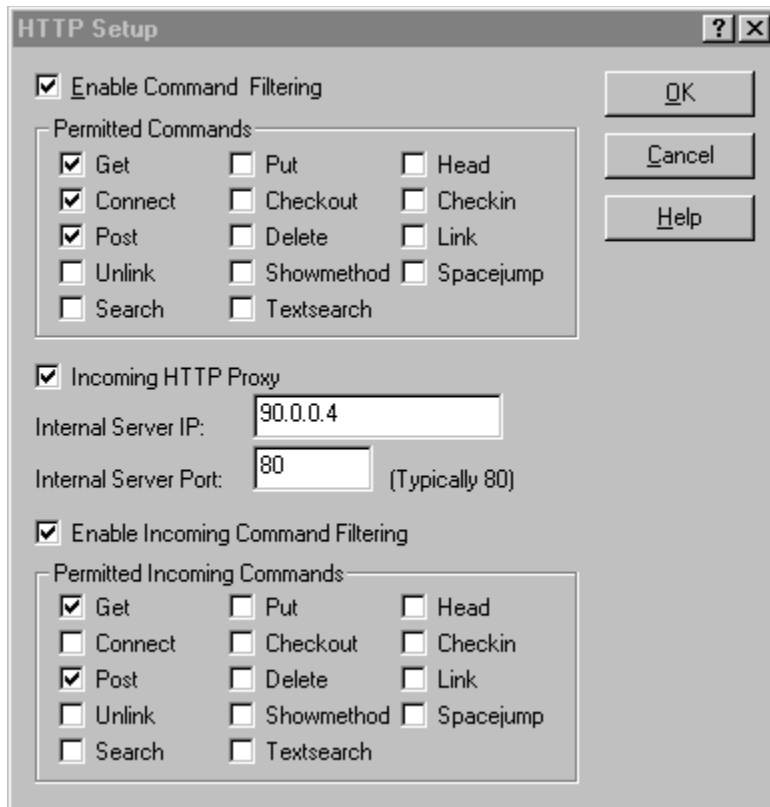
Name Caching remembers names that have been verified, reducing the number of name requests and, hence, reducing the risk of retrieving a false response.

Blacklisting is used to prevent subsequent requests to an IP Address that has been spoofed or to domain names that have been spoofed. All names and IP Addresses that do not pass the Reverse Name Lookup are immediately Blacklisted.

HTTP Setup Dialog

Invoke this dialog by pressing the HTTP Setup button in the [Protocols Tab](#) in Advanced Properties.

The [HTTP](#) Setup Dialog allows you to configure command filtering and a reverse proxy for HTTP.



Check the box to Enable Command Filtering if you want to limit the commands permitted through WinProxy. If you do not check this box, WinProxy will still ensure that all HTTP requests are valid, but it will not limit the commands used.

To enable command filtering check the "command filtering" checkbox at the top of the dialog. When command filtering is enabled, only the commands checked will be allowed in HTTP. Most of the commands are proposed HTTP extensions and are not generally used.

This is a description of the most common commands used in HTTP:

- | | |
|---------|--|
| Get | Retrieve a document from the server. This is the most common command |
| Put | Put a document onto the server. Used when authoring a web page. This should only be permitted if it is necessary. |
| Connect | Used to establish a secure sockets connection. WinProxy supports secure sockets proxying. To disable secure sockets, disable this command. |
| Post | Used when filling out a form on the web and submitting the results. If this is disabled, many standard web features will also be disabled. |

If you want to disable use of [secure sockets](#), enable Command Filtering, and permit all commands except for Connect, which is used for secure sockets,

If command filtering is disabled, then all commands will be permitted, even those that are not recognized.

The Incoming HTTP proxy allows you to permit incoming connections to an internal web server. People accessing the internal web server would connect to the proxy machine as the web server, which can validate the request, and pass it through to the Internal web server.

You can also enable command filtering for the internal web server by checking the box labeled Enable Incoming Command Filtering.

The following is an example of an incoming proxy:

```
Joe User on the Internet
Connects to Proxy.YourCompany.com
|
WinProxy receives connection
forwards connection to Internal Web Server
|
Internal Web Serverreceivess request, and returns
requested document.
```

In this example, the web server is behind the firewall, and is secure from Internet hackers, so the database and file system on that computer is not available on the Internet. Additionally, the location of the web server can be changed at any time, without changing the name registered with the InterNic.

Telnet Setup Dialog

Invoke this dialog by pressing the Telnet Setup button in the [Protocols Tab](#) in Advanced Properties.

The [Telnet](#) Setup Dialog allows you to configure the [port number](#) used to listen for Telnet [connections](#).

The standard port number used is port 23. For security reasons, the Telnet proxy will only connect to Telnet servers on port 23. This, however, determines on which port Telnet is listening.

FTP Setup Dialog

Invoke this dialog by pressing the FTP Setup button in the [Protocols Tab](#) in Advanced Properties .

The [FTP](#) Setup Dialog allows you to configure the [port number](#) used to listen for FTP [connections](#).

The typical port number used is port 21, but if your firewall is already running an FTP server on port 21, you may want to choose another port. Alternate ports typically used are 8021 or 1021.

Mail Setup Dialog

Invoke this dialog by pressing the Mail Setup button in the [Protocols Tab](#)

The [Mail](#) Setup Dialog allows you to configure the [port number](#) and [IP Address](#) used to connect to an external [SMTP](#) [POP3](#) and [IMAP4](#) server.

The screenshot shows the 'Mail Setup' dialog box with the following fields and values:

- Mail Host IP: 198.13.48.12
- Mail Proxy Port: 25 (Typically 25)
- POP 3 Server IP: 198.13.48.12
- POP 3 Proxy Port: 110 (Typically 110)
- Use IMAP 4
- IMAP4 Server IP: 198.13.48.13
- IMAP4 Server Port: 143 (Typically 143)
- Incoming Proxy for SMTP
- Internal Server IP: 90.0.0.4
- Internal Server Port: 25 (Typically 25)

Buttons: OK, Cancel, Help

Mail Host IP: This specifies the [IP Address](#) used to connect to an external [SMTP](#) server. WinProxy will always use the SMTP port, 25, to connect to this server.

Mail Proxy Port: This is the port number on which WinProxy listens for SMTP connections. All connections will be forwarded to the SMTP port on the IP Address specified by the Mail Host IP. The default value for this field is 25.

POP 3 Server IP: This specifies the IP Address used to connect to an external [POP3](#) server. WinProxy will always use the POP3 port, 110, to connect to this server.

POP 3 Proxy Port: This is the port number on which WinProxy listens for POP3 connections. All connections will be forwarded to the POP3 port on the IP Address specified by the POP3 Server IP. The default value for this field is 110.

Use IMAP 4: Check this box if you are using [IMAP 4](#). Unless you specifically know otherwise, you will probably not need this.

IMAP 4 Server IP: This specifies the IP Address used to connect to an external IMAP 4 server. WinProxy will always use the IMAP 4 port, 143, to connect to this server.

Incoming SMTP Proxy: WinProxy can work as a reverse proxy for SMTP, allowing you to place an internal SMTP server behind the firewall. This protects the server from unauthorized access, while permitting people to send mail to it from the Internet.

Internal Server IP: This specifies the IP Address of the Internal SMTP server. When a connection is received on the external port 25, then WinProxy will forward the connection to this server.

Internal Server Port: This specifies the port number of the Internal SMTP server. When a connection is received on the external port 25, then WinProxy will forward the connection to this port number on the server specified. This port number is typically 25.

Users should configure their e-mail mail servers to use the proxy server as their Mail and Post Office hosts. Even though all e-mail transactions will take place with another computer, outside the firewall, to the e-mail application, WinProxy will appear to be the server.

Command filtering is not currently implemented for the mail protocols.

RealAudio Setup

Invoke this dialog by pressing the RealAudio Setup button in the [Protocols Tab](#) in Advanced Properties .

The [RealAudio](#) Setup Dialog allows you to configure the [port number](#) used to listen for RealAudio [connections](#).

The typical port number used is port 1090. In recent versions, Progressive Networks changed their default port number to 1080, which conflicts with the port number typically used for Socks. (This was pretty dumb... we still default to 1090, which does not conflict with Socks.)

The RealAudio proxy in WinProxy supports both TCP and UDP (connected and streaming) types of data streams. To configure your RealAudio client, select the Proxy tab in your the preferences, and enter the IP address of the WinProxy server, along with port 1090 as the port number.

NNTP - Network News Transfer Protocol

NNTP is the protocol used for News on the Internet. The news services, also known as UseNet groups, are essentially bulletin boards on the Internet, which allow Internet users to exchange ideas and have discussions. Some news groups are read only, and provide actual news as well. Reuters and Associated Press, for instance publish much of their news in news groups.

News Setup Dialog

Invoke this dialog by pressing the News Setup button in the [Protocols Tab](#) in Advanced Properties.

The Internet News ([NNTP](#)) Setup Dialog allows you to configure the [port number](#) and [IP Address](#) used to connect to an external News server.

News Server IP: This is the IP Address of the external News server. WinProxy will always use port 119 to connect to this computer.

News Proxy Port: This is the port number on which WinProxy listens for News requests. All connections will be forwarded to the News port on the IP Address specified by the News Server IP. The default value for this field is 119.

Users should configure their news readers to use WinProxy as their News server. Even though all News responses will ultimately come from the external News, outside the firewall, to the News clients, WinProxy will appear to be the server.

Command filtering is not currently implemented for the news protocol.

DNS - Domain Name Service

DNS is the protocol used on the Internet to translate names, such as www.WinProxy.com to [IP addresses](#) . This protocol is required to use the [Socks](#) proxy in WinProxy.

IRC - Internet Relay Chat

IRC is a popular chat protocol used to have text conversations on the Internet. Users can connect to a chat server, which has several "rooms" and they can enter each room and talk to others in the same room. Many users can have live conversations in these rooms. To use IRC through WinProxy, you will have to enable the [Socks](#) and [DNS](#) proxies, and configure your IRC client to use the Socks protocol to connect the ther server.

Socks

Socks is a very flexible proxy protocol used for several types of connections. Netscape and Internet Explorer can use the Socks protocol to connect to every protocol they support. The Socks proxy protocol requires support for [DNS](#).

The socks proxy is required to support the following protocols, among others:

[IRC](#)

Gopher

WAIS

ICQ

The Socks proxy will also allow you to have a more flexible interface to FTP in web browsers such as Netscape and Internet Explorer.

Socks Setup Dialog

Invoke this dialog by pressing the Socks Setup button in the [Protocols Tab](#) in Advanced Properties .

The Socks Setup Dialog allows you to configure the [port number](#) used to listen for [Socks connections](#).

The typical port number used is port 1080. If you enable the Socks proxy, be sure to also enable the [DNS](#) proxy, as it is required to use Socks.

The WinProxy Socks Proxy support both Socks 4 and Socks 5 protocols, allowing most applications to use it. The Socks 5 proxy adds the ability to proxy UDP packets, typically used for streaming audio and streaming video.

For example, Mirabilis ICQ uses the Socks 5 proxy to relay UDP data.

DNS Setup Dialog

Invoke this dialog by pressing the [DNS Setup](#) button in the [Protocols Tab](#) in Advanced Properties .

The DNS Setup Dialog allows you to add or remove DNS servers to the list used by WinProxy. The servers will be tested in the order that they appear in the list. If you have multiple DNS servers available, add the Primary DNS server first, and the secondary DNS servers in the order you want them searched.

The [DNS](#) server IP addresses should be available from your [service provider](#). In order to make it easier to configure DNS, WinProxy can link you to a web page that will show you the IP addresses used by your service provider. Press the "Find my Name Server" button to have WinProxy help you locate the proper DNS servers to use in this dialog. However, if this information is readily available from your service provider, it is highly recommended that you use that information.

To add a server to the list, type the name of the server into the box on the left, and press the Add button to add it to the list of servers. To remove a server, select it in the list on the right, and press the Remove button.

WinProxy can also function as a full Domain Name Server, resolving names for computers inside your firewall. In order for WinProxy to do this efficiently, it needs to know the domain that you use to refer to your network. This does not have to be a domain recognized on the Internet.

Enter the domain name you wish to use in the "Domain" field in this dialog. You should enter the same domain name in your TCP/IP configuration on each of your internal computers. You should then enter the names and IP addresses of those computers in NameList.pxy, the file used to configure WinProxy's name services. If your domain is MyDomain.com, and your computer is called MyComputer, then you would enter MyDomain.com as the domain in the DNS configuration, and specify an IP address for MyComputer. WinProxy will then resolve the name for MyComputer, as well as MyComputer.MyCompany.com. Computer names are not case sensitive.

You can automatically jump to the NameList.pxy file to further configure name services by pressing the button labeled "Edit Name List". This will bring up notepad with the NameList.pxy file. A sample file is included, and contains detailed instructions on configuring names.

The last check box allows you to disable the TCP proxy for [DNS](#). DNS is typically transmitted through UDP, and the TCP method is very rarely used. Unless you know you need it, it is recommended that you leave it disabled. This will save system resources and improve performance.

Host Name

Since [IP Addresses](#) are not easy to remember, users can identify computers by names instead. The TCP/IP protocol can convert a name into an IP Address using a process called name resolution. Names are organized in a hierarchical structure with a network name, a domain name, and a computer name. For example in the name WWW.OSITIS.COM, COM is the network name, OSITIS is the domain name and WWW is the computer name. Multiple names can point to the same computer, using aliases

URL

A URL (Universal Resource Locator) is a string that identifies a specific document on the network. A full URL consists of a protocol, such as [HTTP](#) or [FTP](#), a [host name](#) and a document path. As an example:

HTTP://www.WinProxy.com/index.htm

is a full URL. the characters before the "/" designate the protocol, **HTTP** in this case, the subsequent string, **WWW.OSITIS.COM**, before the next slash are the host name and the remainder, **Welcome.html**, designate the document. Any computer on the internet can use this URL to retrieve the same document.

Aliases

Computers on the internet can be referred to by [names](#), which can be translated to an [IP Address](#) of the serving computer. Several names, however can point to a single computer. When this is the case, then one of those names is specific to that computer, and the others are [aliases](#).

Reverse Name Lookup

Computers on the internet can be referred to by [names](#), which can be translated to an [IP Address](#). After the name is translated to an IP Address, a [Reverse Name Lookup](#) can be used to translate the IP Address into a name, as well as its [aliases](#). This allows WinProxy to verify that the computer it is connecting to really is the computer that is expected.

Secure Sockets

In order to facilitate secure [connections](#) on the internet, the Secure Sockets (SSL) protocol was invented. This protocol is used on a separate connection than regular HTTP and is encrypted to prevent hackers who have access to the network from tapping the connection. This is often used to purchase products on the internet when private information such as credit card numbers must be exchanged.

WinProxy supports proxying of secure sockets. This feature is automatically enabled with [HTTP](#) and can be disabled by enabling [HTTP command filtering](#) and refusing the connect command.

To allow access to the secure sockets protocol on ports other than the standard ports, check the box in HTTP setup to Enable Secure Connections to Non-standard Ports. If this box is not checked, secure connections will only be permitted to the standard ports specified in the SSL protocol.

Telnet Proxy

WinProxy supports proxying of the [Telnet](#) protocol. Since there is no industry standard way of proxying Telnet, WinProxy implements its own method of doing it. To use the Telnet proxy, make sure that it is enabled in the [Properties Dialog](#) and perform the following steps in your Telnet application.

No special configuration is necessary to make your Telnet client work with WinProxy.

- 1) Connect to the Telnet port (usually 23, but this can be [configured](#) in WinProxy) on the WinProxy server
- 2) When prompted, enter the [name](#) of the Telnet server you wish to [connect](#) to.
- 3) When the connection is established, log onto the external server, as if you were directly connected to it.

The Telnet proxy requires the external server to be listening for a connection on the standard port, 23. Other ports will not be allowed for security reasons.

Once the connection is established, the communication between the Telnet client and the host is not monitored or logged by WinProxy.

The Telnet Proxy feature of WinProxy can be enabled and configured from the [Properties Dialog](#).

HTTP Proxy

WinProxy supports proxying of the [HTTP](#) protocol. The method used is the industry standard [CERN](#) proxy method, and includes support for a CERN [FTP](#) proxy as well.

When a computer inside the firewall wants to view a document on the [World Wide Web](#) it makes a request to WinProxy, which makes a request on the network on its behalf. If the request is for an FTP document, then WinProxy establishes a [connection](#) with the specified FTP server and returns the requested document in HTTP.

The HTTP Proxy feature of WinProxy can be enabled and configured from the [Properties Dialog](#).

Configuring Netscape (version 3.0b4) to support the HTTP Proxy

- 1) Select *Network Preferences* from the *Options* menu.
- 2) Select the *Proxies* tab
- 3) Select *Manual Proxy Configuration*
- 4) Press the *View* button
- 5) In the *HTTP Proxy*: edit box, enter the [host name](#) or [IP Address](#) of the WinProxy server.
- 6) Enter the [port number](#) specified for the [CERN](#) proxy in the WinProxy [Properties dialog](#).
- 7) Enter the same information in the *Security Proxy*: section. See [SSL](#)
- 8) Enter the same information in the *FTP Proxy*: section.
- 9) Select *OK* in the *Manual Proxy Configuration* dialog
- 10) Select *OK* in the *Preferences* dialog.
- 11) Use

Configuring Internet Explorer (version 3.0b1) to support the FTP Proxy

- 1) Connect to a web page. Internet Explorer can not be configured until it has successfully read a web page. (I know, how do you connect to a web page without configuring the proxy?... Maybe later releases will fix this problem)
- 2) Select *Options* in the *View* menu.
- 3) Select the *Connection* tab
- 4) Check the box near the bottom labeled *Connect to the internet through a proxy server*
- 5) Press the *Change Proxy Settings* button.
- 6) If you are using WinProxy to proxy all protocols, check the box labeled *Use the same proxy server for all types of addresses*. If you check this box, you will need to enter the data in the next step in the [HTTP](#) line of the configuration.
- 7) In the FTP line of the list of servers, enter the [host name](#) or [IP Address](#) of the WinProxy server in the first space and the [port number](#) of the [CERN](#) proxy, specified in the WinProxy [Properties dialog](#) in the second space.
- 8) If you did not select the option to use the same proxy for all protocols, then you will need to enter the same information for the FTP and Security ([SSL](#)) lines, if desired.
- 9) Press the *OK* button for the *Proxy Settings* dialog.
- 10) Press the *OK* button for the *Options* dialog
- 11) Use

FTP Proxy

WinProxy supports two methods for proxying of the [FTP](#) protocol.

The first method is the industry standard [CERN](#) proxy method which allows popular browsers to access FTP documents through [HTTP](#) requests.

The second method supports FTP clients using the "user@host" method. With this method the FTP client must connect to WinProxy, and when a user name is requested, respond with user@[host](#). For example, if the client wants to log in as **anonymous** at **FTP.CDROM.COM** then they would respond with a user name of **anonymous@ftp.cdrom.com**. WinProxy then establishes a connection to the specified host, and enters the requested name. All future requests are passed through to the FTP client.

Configuring Netscape (version 3.0b4) to support the FTP Proxy

- 1) Select *Network Preferences* from the *Options* menu.
- 2) Select the *Proxies* tab
- 3) Select *Manual Proxy Configuration*
- 4) Press the *View* button
- 5) In the *FTP Proxy*: edit box, enter the [host name](#) or [IP Address](#) of the WinProxy server.
- 6) Enter the [port number](#) specified for the [CERN](#) proxy in the WinProxy [Properties dialog](#).
- 7) Select *OK* in the *Manual Proxy Configuration* dialog
- 8) Select *OK* in the *Preferences* dialog.
- 9) Use

Configuring Internet Explorer (version 3.0b1) to support the FTP Proxy

- 1) Connect to a web page. Internet Explorer can not be configured until it has successfully read a web page. (I know, how do you connect to a web page without configuring the proxy?... Maybe later releases will fix this problem)
- 2) Select *Options* in the *View* menu.
- 3) Select the *Connection* tab
- 4) Check the box near the bottom labeled *Connect to the internet through a proxy server*
- 5) Press the *Change Proxy Settings* button.
- 6) If you are using WinProxy to proxy all protocols, check the box labeled *Use the same proxy server for all types of addresses*. If you check this box, you will need to enter the data in the next step in the [HTTP](#) line of the configuration.
- 7) In the FTP line of the list of servers, enter the [host name](#) or [IP Address](#) of the WinProxy server in the first space and the [port number](#) of the [CERN](#) proxy, specified in the WinProxy [Properties dialog](#) in the second space.
- 8) Press the *OK* button for the *Proxy Settings* dialog.
- 9) Press the *OK* button for the *Options* dialog
- 10) Use

Configuring CuteFTP to support the FTP Proxy.

In the Windows environment, we recommend using the CuteFTP proxy client. This is, by far, the most reliable and convenient FTP server that we have evaluated.

- 1) Select *Options* from the *File menu*.
- 2) Select the *Firewall* tab.
- 3) Enter the [host name](#) of the WinProxy server in the *Host* field.
- 4) Enter the [port number](#) specified in the WinProxy [FTP Setup](#) dialog (usually 21)
- 5) Set the *type* to USER user@site.
- 6) Check the *Enable firewall* access button.

- 7) Press the *OK* button.
- 8) Use

JAVA

JAVA is a programming language and environment invented by Sun Microsystems which provides a compatible environment over multiple platforms, allowing code written on one platform to be compatible over multiple platforms and easily retrieved over the network.

JAVA requires network support and primarily uses the [HTTP](#) protocol to exchange information among computers.

Remote Configuration

WinProxy provides the ability to do routine maintenance on the proxy server by remote configuration. The features that can be accessed remotely are:

Flush the [name cache](#)
Open the [logging connection](#)
Reload the [blacklist](#) from file
Display the current blacklist

Remote configuration can only be done from [behind](#) the firewall and, if an [Administration IP Address](#) is specified, then the configuration can only be done from that [IP Address](#).

To use Remote Configuration, execute a [World Wide Web](#) browser such as Netscape or Mosaic, which is configured to proxy through WinProxy, and request the [URL](#)

HTTP://Proxy.Command/Help

The browser will display a menu of options and how to use each one of them. selecting any of the specified links will perform the requested action. Any document requested from the Proxy.Command host name will respond with the help menu, unless the requested document is, in fact, one of the commands listed here.

1) Flushing the name cache

WinProxy performs a name lookup and a reverse name lookup for each [host name](#) that is requested and places the results in a [name cache](#). Unless the cache overflows, the name is maintained in the cache for up to three hours. This reduces the risk of retrieving incorrect [IP Addresses](#) from name lookups, accelerates access by reducing name queries, and increases security by causing one name to be guaranteed to resolve to the same address on multiple accesses (a feature that is especially important in [JAVA](#) security requirements.)

However, if the name of a server has recently changed, then it may be desirable to flush it from the cache, to allow future [connections](#) to retrieve the new IP Address.

2) Re-open the logging port

WinProxy provides [logging](#) of all transactions that pass through it. This allows a network administrator to monitor network access to ensure it is not being abused and to trace any inappropriate activities. Logging is done by [connecting](#) to a process either on the same computer as WinProxy or elsewhere on the network. If the [logging application](#) is closed or the connection is lost, then this command can be used to re-establish the connection.

This command may NOT be used to terminate the connection to the logging application. If WinProxy is already connected to a logging application, then this command will have no effect, and will report a failure to connect.

3) Reload the IP and URL blacklist

WinProxy provides the ability to [Blacklist](#) a list of [IP Addresses](#) and [URLs](#). Since the [IP Verification with Reverse Name Lookups](#) feature can automatically add [names](#) and IP Addresses to the Blacklist, and may even add valid names to the blacklist, it may be necessary to occasionally reload the Blacklist from disk.

When this command is issued, the blacklist will be purged and re-read directly from disk, as though WinProxy were restarted.

While the blacklist is being re-loaded, no [connections](#) will be accepted in order to prevent allowing connections that are in the blacklist. This, however, should provide no inconvenience since the blacklist is read very quickly.

4) Display the IP and URL blacklist

Since it is possible for [names](#) and [IP Addresses](#) to be added to the [Blacklist](#) by means of the [IP Verification with Reverse Name Lookups](#) feature, it may sometimes be necessary to view the current blacklist to determine if a specific IP Address or name is in it. This command provides the ability to view the blacklist from any browser inside the firewall.

Network administrators should also use this function to verify that the blacklist was correctly read from the blacklist file.

Serial Number Dialog

This dialog requests a new [serial number](#) for WinProxy. The serial number is separated into three groups of four, eight and three characters.

If there is currently no serial number, then any valid serial number will enable the use of WinProxy.

If an evaluation serial number has already been entered, then only a permanent serial number will be accepted.

When a permanent serial number has been entered, you will not see this dialog.

[Contact Ositis Software](#) to receive a permanent serial number.

What is WinProxy, How does it work and how can I use it?

WinProxy is a secure firewall proxy server for Windows `95 and NT. Although it allows people behind the firewall to contact the network on the other side, it does not allow people outside to connect to the inside of the firewall. Essentially it behaves like a diode for network traffic.

WinProxy is a proxy server that acts as a proxy on the network for users who are behind the firewall. In essence, all of the users behind the firewall appear, to the external network, to be at the same IP address, hence the term proxy, as well as the mask icon. As an example, when accessing the World Wide Web, your browser, Netscape for instance, connects to the proxy server, WinProxy, and makes a request for a specific web page, or URL. WinProxy then creates a connection between itself and the web server, on behalf of your browser. Retrieves the requested document, and forwards it to Netscape. All of this happens behind the scenes and the user can use the browser as if they are directly connected from their machine, and computers on the internet, can serve documents, thinking they are serving the firewall machine.

Since no requests are made on the network that mention the IP address of the requesting machine, the IP addresses used behind the firewall do not need to be valid internet IP addresses. In fact, it is a good idea to use invalid IP addresses to make sure that the operating system the firewall is running (Windows NT can do routing, although Windows `95 can not) does not route the packets. Good choices for IP addresses are subnets 192.0.X.X and 127.X.X.X, which are reserved as a test network and loopback tests. 127.X.X.X may not work on some networks.

Name Cache

WinProxy provides a [name](#) caching feature that caches names and [IP Addresses](#) that have been verified using a [reverse name lookup](#).

Each name is placed into the cache and stored for up to three hours, or until the cache is full and older names are purged from the cache. Only names that have been verified are stored in the cache.

This security feature significantly reduces the risk of being served a bad name and improves performance by reducing the requirement for repeated name requests. The [JAVA](#) virtual machine requires this feature to enforce its security, which requires that a JAVA applet only connect to the server from which it came. Without name caching that can not be guaranteed, creating a security risk.

Since all names are cached, however, it is sometimes necessary to purge the name cache when a server's IP Address has been changed, and the change needs to be implemented immediately. This can be done through [Remote Configuration](#).

Proxy Cascading

It is sometimes necessary to secure a network within another network, but still maintain the ability to access the internet behind another firewall. WinProxy provides this feature with Proxy Cascading.

Proxy Cascading enables WinProxy to forward requests from itself to another proxy server. If, for instance, WinProxy is located between Network A and Network B. Network B is connected to the internet through another WinProxy or other proxy firewall.

Net A -> Cascading WinProxy -> Net B -> Second Firewall -> Internet

Using proxy cascading the appearance to the users in Network A will be as though Net B were not even there.

Net A -> Cascading WinProxy -----> Internet

In reality all requests are still proxied through the external firewall, but users of Network A only have to configure their systems to proxy to the cascading WinProxy.

Cascading can be configured in the [Properties dialog](#) with the [Cascading Port](#) and [Cascaded Proxy IP Address](#).

Cascaded proxies can be nested as deeply as desired, but network administrators should keep in mind that it degrades performance each time a proxy is cascaded.

Proxy cascading is currently only supported for [HTTP](#) and [Secure Sockets](#) requests. Other protocols can be supported indirectly such as [Mail](#) and News, by pointing to the external proxy as the server. [Telnet](#) can be done by logging into the first proxy, connecting to the second proxy and then outside. Cascading does not provide access to the intermediate network, unless the next firewall provides access to it (which will be true in most cases, including the case of WinProxy serving as the external firewall.)

If you desire WinProxy to provide a more complete cascading solution, please [contact Osis Software](#).

Logging

WinProxy provides the ability to log all network activity that passes through it.

When WinProxy starts, it attempts to establish a connection with another application on the network on a [IP Address](#) and [port number](#) designated in the [Properties Dialog](#). When this connection is established, all logging information is transmitted to that application. This application can be run anywhere on the network.

All HTTP requests and commands, FTP requests, and Telnet connections are logged with the date and time that they occurred.

The logging application can be located anywhere on the network and only needs to store or report the data it receives. A sample [logging application](#), [ProxyLog.EXE](#) is included with WinProxy complete with source code. This program is written as a Windows `95/NT console application and outputs all logging information to standard out, and optionally writes it to a file.

Users of WinProxy are permitted and encouraged to augment the ProxyLog application to better support their needs. If you make improvements to the ProxyLog application and wish to distribute your program in binary or source code form, please [contact Ositis Software](#) and we will consider assisting those efforts. Any programs based on the ProxyLog source code must display a message stating that the code was based on ProxyLog, developed by Ositis Software.

ProxyLog.EXE

The [Logging](#) feature of WinProxy requires a logging application to display and save the logging information. A Windows 95/NT program, called [ProxyLog](#), is included with WinProxy to facilitate this capability.

Users of WinProxy are permitted and encouraged to augment the ProxyLog application to better support their needs. If you make improvements to the ProxyLog application and wish to distribute your program in binary or source code form, please [contact Osis Software](#) and we will consider assisting those efforts. Any programs based on the ProxyLog source code must display a message stating that the code was based on ProxyLog, developed by Osis Software.

Service Provider

Your network service provider is the organization that provides your Internet Access.

If you are using a dial up connection, such as modem or ISDN, then the service provider is the company that you dial into.

If you have a permanent connection such as a Frame Relay or T1 link, then the organization that you are connected to is your service provider.

If your internet connection is part of a LAN then you should consider the administrator of that lan your service provider. This may be the case if you are administering a workgroup that is connected to the Internet through your company LAN.

In any case, your service provider should provide you with the necessary information to configure the network adapter that is connected to the Internet. This information should include the following:

IP Address
Subnet Mask
DNS server
Domain Name
Default Gateway

If your Service Provider assigns this information automatically, then you will only need the IP address of the DNS server, and the rest of the information will be assigned when you connect.

System Tray

The system tray is on the right side of the [taskbar](#) in Windows 95 or Windows NT 4.0. When WinProxy is running in the system tray, it will show up as a small white mask on your [TaskBar](#).

Taskbar

The taskbar exists in Windows 95 and Windows NT 4.0, and provides an interface to access most of the features of Windows. It typically resides at the bottom of the screen, and can be configured to hide when it is not in use. The Start Menu resides in the taskbar.

On the left side of the taskbar, you can occasionally see some icons or the time. This is referred to as the [System Tray](#).

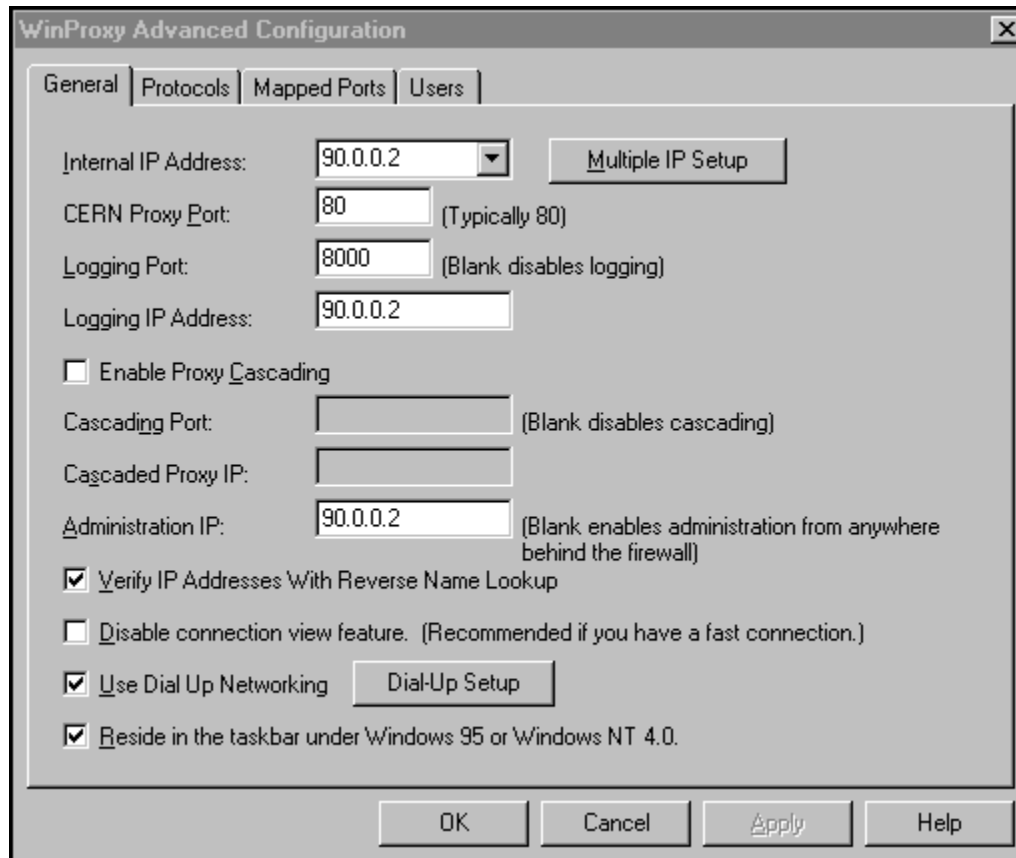
Loading WinProxy before logging into Windows 95

WinProxy can be configured to load before you log onto Windows 95. This allows you use WinProxy after a power failure without interruption. If the system is shut off for a power failure, then as soon as it comes back up, WinProxy will be running in the background, regardless of whether you have logged into Windows or not.

To enable this feature, select the option to "Reside in the [taskbar](#) in Windows 95 or NT 4.0" in [the general configuration tab](#) in [Advanced Properties](#).

General Tab in Advanced Properties

This tab in advanced properties allows you to configure the basic behavior of WinProxy. It is highly recommended that you connect to the Internet before changing any of these settings.



Internal IP Address This selects the [IP address](#) that WinProxy will use to listen for connections. You should enter the IP address that WinProxy will use to listen for connections. You should NOT select the IP address that is connected to the Internet here. If you have multiple internal IP addresses, you will have to configure them in Multiple IP Setup. If multiple IP addresses are configured, then this field will be grayed out. For more information on the Internal IP address and configuring WinProxy, see the [Network Configuration Diagram](#).

It is not necessary to enter the IP addresses of all your users here. You should only enter the address that your internal network is connected.

Multiple IP Setup If you have multiple [internal IP addresses](#) on your computer, press this button to add multiple addresses to the list of Internal IP addresses. Usually you will never have to use this.

CERN Proxy Port This is the [port number](#) that WinProxy will listen to for [CERN](#) proxy connections. The CERN proxy supports HTTP and FTP services for browsers such as Netscape and Internet Explorer. If you are running a web server on port 80 already, then you should choose an alternate port here. Typical alternates are 81 and 8080.

Logging Port This is the [port number](#) that WinProxy will try to connect to for [logging](#). Typically this value is set to 8000, as that is the default address that the [logging application](#) listens to. If you do not need logging, leave this field blank, and logging will be disabled.

Logging IP This is the IP Address used for logging in WinProxy. When WinProxy attempt to connect to the [logging application](#) it will connect to this IP address. In the example shown the IP address is the same as the address that WinProxy is running on, but it can be anywhere on the [internal network](#).

Enable Proxy Cascading If you are running WinProxy behind another proxy server, then you should enable [proxy cascading](#) to tell WinProxy to cascade requests to the next proxy server. When you check this box, the [Cascading Port](#) and [Cascaded Proxy IP](#) fields will be enabled. This feature is rarely used.

The most common usage for this feature is if your service provider is running a proxy server. This is common in Europe and South America.

Cascading Port This allows you to configure the [port number](#) for a [cascaded proxy](#).

Cascaded Proxy IP This allows you to configure the [IP address](#) for a [cascaded proxy](#)

Administration IP WinProxy allows you to do some simple [administration](#) from any machine on the Internal Network. If this field is left blank, then that administration can be done from any machine on the Internal network. If you enter an IP address into this field, then Administration will be permitted from only that computer.

Verify IP Addresses This check box enables a security feature in WinProxy that causes all name lookups to be verified with a [reverse lookup](#). This adds security to the system by making it very difficult for hackers to use [IP spoofing](#).

This feature may also restrict access to valid web pages, that are not properly configured. If you have trouble accessing certain sites, disable this feature.

Disable ConnectionView [ConnectionView](#) is the ability for WinProxy to display all connections on the main display. This display can slow down the system. If you are running on a slower machine with a fast Internet connection, it is recommended that you disable that feature by checking this box, as it will speed up your Internet access.

Dial-Up Networking WinProxy can use Dial-Up Networking to connect to the Internet automatically as it is needed. If you have a permanent connection, or if you connect to the Internet manually, leave this box unchecked. If you want WinProxy to automatically establish connections as it is needed, check this box, and configure Dial-Up Networking by pressing the Dial-Up Setup button.

Dial-Up Setup Press this button to configure Dial-Up Networking.

Reside in [taskbar](#) WinProxy can reside in the [taskbar](#) or [system tray](#) under Windows 95

and Windows NT 4.0. When WinProxy is running in the system tray, then it will show up as a small icon on the right side of your taskbar. You can double click on this icon to display the [main window](#), and double click on it again to hide the main window.

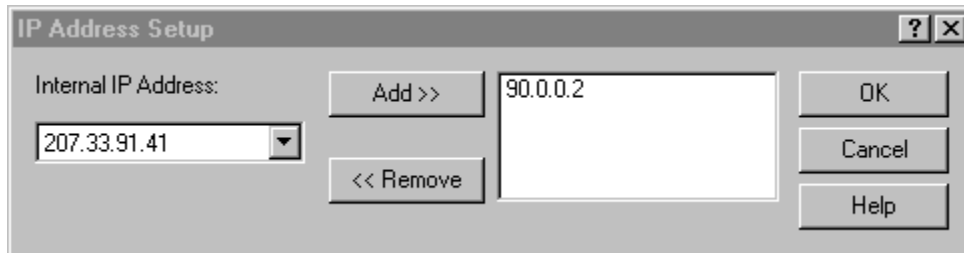
Under Windows 95, checking this option will also cause WinProxy to [load before you log into Windows](#). This allows WinProxy to run even after a power failure, when nobody has logged into Windows yet.

Permit Domain Names If this box is checked, then you will be able to enter domain names in your mail, news and mapped port settings, instead of using IP addresses. This is slightly more convenient for the administrator at the expense of security. If you use IP addresses, you will be much less susceptible to IP spoofing attacks.

Multiple IP Setup dialog

This dialog allows you to configure multiple IP addresses for your Internal network. You do not need to use this unless you have at least three network adapters (including your Internet adapter) on the WinProxy computer.

You should only use this dialog if you have more than one IP address connected to your internal network.



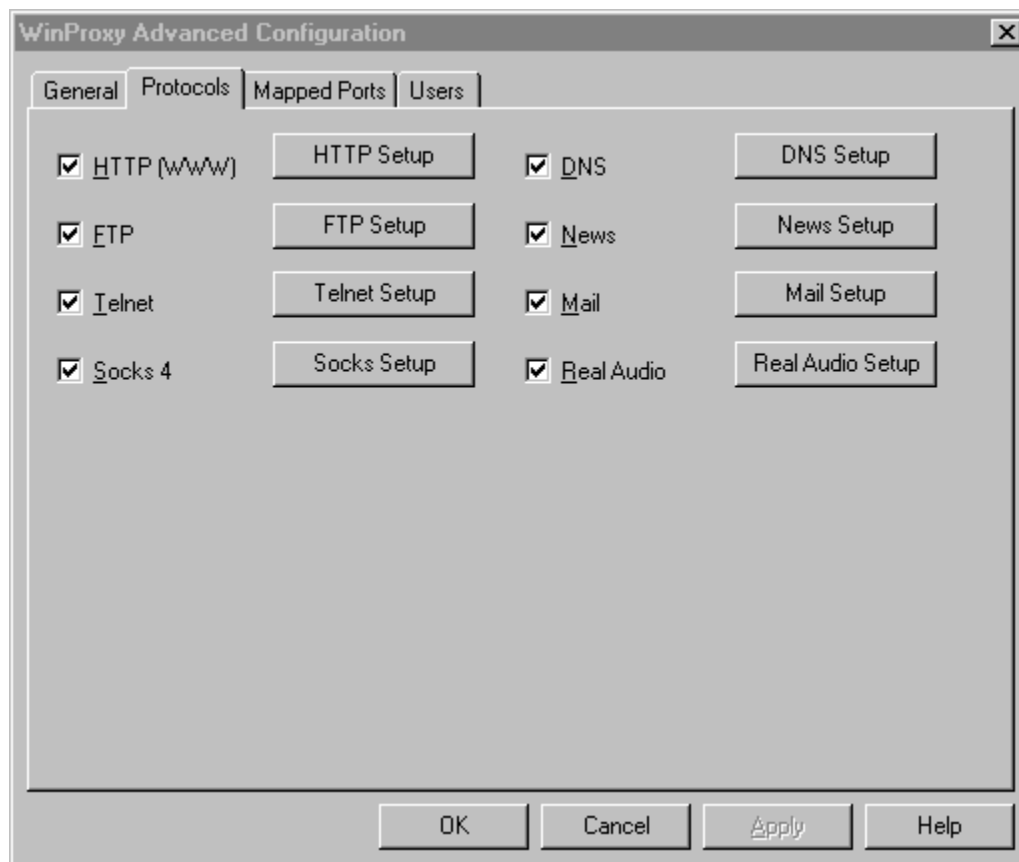
The list on the left allows you to select the IP addresses of the network adapters on your machine are connected to your internal network. Once an IP address is added to the box on the right, it will disappear from the list on the left.

The addresses in this list represent the Internal network adapters on your proxy server. You should NOT add the IP address that represents the network adapter that is connected to the Internet. This would allow users on the Internet to access WinProxy and, hence, your internal network.

To add IP addresses to the list, select the address on the left, and press the Add button. The address will be added to the list on the right, and removed from the list on the left. To remove addresses from the list of IP addresses, select the address you want to remove, and press the Remove button. This will remove the address from the list on the right, and put it back in the list box on the left.

Protocols Tab in Advanced Properties

This tab in Advanced Properties allows you to configure the protocols that you want supported in WinProxy. It is highly recommended that you connect to the Internet before changing any of these settings.



- HTTP** Enable [World Wide Web](#) access. Press [HTTP Setup](#) to change some of the settings of the protocol, including command filtering and reverse proxy.
- FTP** Enable the File Transfer Protocol access. Press [FTP Setup](#) to change the [port number](#) that is used for the FTP Proxy.
- Telnet** Enable the Telnet Proxy. Press [Telnet Setup](#) to change the [port number](#) that is used for the Telnet proxy.
- Socks 4** Enable the Socks 4 Proxy. Press [Socks Setup](#) to change the port number that is used for the Socks proxy. The Socks proxy requires [DNS](#) services, so if you enable Socks 4, be sure to enable and set up the DNS proxy.
- DNS** Enable the DNS proxy. Press [DNS Setup](#) to configure your external DNS servers. You must configure DNS before it will work.
- News** Enable the News ([NNTP](#)) proxy. Press [News Setup](#) to configure your external News server. You must configure an external News server to use News.
- Mail** Enable the Mail ([SMTP](#), [POP3](#) and [IMAP 4](#)) proxy. Press [Mail Setup](#) to configure your external Mail servers. You must configure an external Mail server

to use the Mail proxy.

[RealAudio](#)

Enable the RealAudio proxy. Press [RealAudio Setup](#) to configure the port number used by the RealAudio proxy.

Other Advanced Properties tabs: [General](#), Mapped Ports, Users

Mapped Ports

Mapped ports are basically a passthrough proxies for allowing users to connect to the services on the Internet that are not supported directly by WinProxy.

In a typical mapped port, WinProxy would listen for a connection on a specific port, when a connection is received, WinProxy then establishes a connection with the server it is mapped to, and the application receives a response from the external server, as if it had connected to it directly.

What happens:

Application ->
9096

WinProxy Port 9096 ->

External Server Port

What the application perceives:

Application -> WinProxy Port 9096, which behaves exactly like the external server.

Mapped Ports Tab in Advanced Properties

This tab in Advanced Properties allows you to configure [Mapped Ports](#). It is highly recommended that you connect to the Internet before changing any of these settings.

This dialog shows you the currently configured Mapped Ports and allows you to add new ones.

To Add a new mapped port, press the New button.

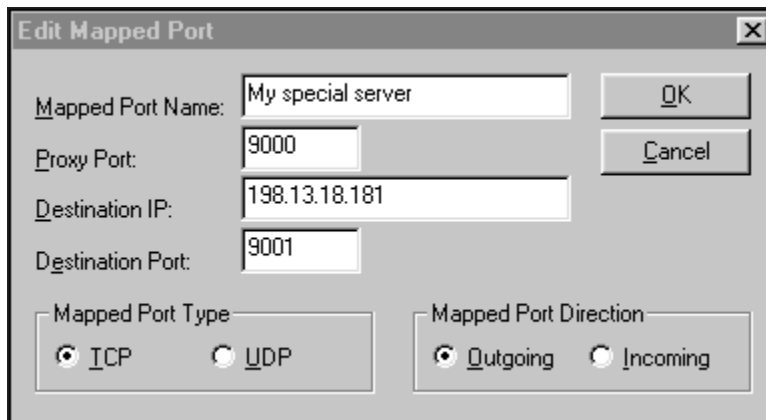
To Modify an existing mapping, select the mapping you wish to modify, and press the Edit button.

To Remove an existing mapping, select the mapping you wish to modify, and press the Delete button.

When you press Edit or New, you will see the [Edit Mapped Port Dialog](#), which allows you to enter the information required to set up a mapped port.

Edit Mapped Port

This dialog allows you to modify an existing [mapped port](#), or create a new one.



Mapped Port Name Enter a name for this mapped port. After the mapping is installed, this is the name that will be displayed in the [main window](#). You can enter any name you like, and you should use something that briefly describes the type of connection.

Proxy Port Enter the [port number](#) that WinProxy should listen on for mapped connections. This is the port number which you need to tell your application to connect to, but it does not have to be the same as the destination port.

Destination IP Enter the [IP address](#) of the server that you are mapping to. When WinProxy receives a connection on the Proxy Port, it will connect to this IP address.

Destination Port Enter the [port number](#) of the server you are mapping to. When WinProxy receives a connection on the Proxy Port, it will connect to this port number on the specified server.

Mapped Port Type Select from TCP or UDP to choose the type of mapping to use. TCP is the most common type of connection, which is used in most Internet protocols. UDP is streaming data, and is typically used for protocols such as RealAudio, which transmit continuous data. The primary difference is that UDP packets do not guarantee delivery. In most cases, you should use TCP, unless your application specifically states that it uses UDP.

Mapped Port Direction Select from Outgoing and Incoming. This option is not available in WinProxy Lite, which only permits outgoing mappings. An incoming mapping is essentially a reverse proxy. It will accept connections from the Internet, and forward them to an internal server. These should be used with care, but can be very useful when you want to permit limited access to a service that needs to be behind the firewall.

Bi-directional UDP WinProxy supports two types of UDP mapping. Unidirectional (this box is not checked) mapping will pass UDP packets in one direction to a

specific server, regardless of the source. A bi-directional mapping, however, will allow one application to send UDP packets to a specific source, and any packets that are returned to the same location in the next two minutes will be passed back to the original sender. This makes it possible to conduct several independent UDP conversations simultaneously through a single mapping.

Cache Tab in Advanced Properties

This tab in Advanced Properties allows you to configure the behavior of the WinProxy cache.

The first thing you must understand is the basic behavior of a web cache. Not all proxy servers work the same, and many do not fully support HTTP caching extensions like WinProxy does. When a document is retrieved from the Internet, there are several instructions sent to the browser and proxy server. Among those are: The document length, whether the document should be cached, when the document should be considered obsolete and the type of the document.

WinProxy will not place documents into the cache if the web server has instructed it not to do so, and it will not cache documents that do not report their content length. Documents without a content length are not stored because without that length there is no way for WinProxy to know if the document was completely retrieved. If a document were truncated due to a network error, then the bad version of the document would be stored in the cache, and users would not be able to access the correct document.

When a document is stored in the cache, WinProxy can check for newer versions of the files, without requesting the entire file. If the document is not modified, a message is returned stating that the document has not changed, and WinProxy returns the cached document to the browser. Alternatively WinProxy can return the document to the browser without checking its validity. Documents that are a response to a query are also not cached, because they are assumed to be dynamically generated.

WinProxy's ability to accurately verify documents depends on the accuracy of the system clock. If the time on the WinProxy system is not correct, or if the time-zone is not correct, WinProxy will not be able to properly request modified documents. The Internet exchanges time information in "Universal Time", or Greenwich Time. This basically means that all time information in WinProxy is communicated on the English time zone. If your time-zone is not correctly set in the computer, WinProxy will not be able to calculate the proper time and your documents may not get refreshed properly, or they may get refreshed too often.

Cache Options

The first option in the Cache Tab is how often WinProxy should check for modified files. If 'Each time the file is requested' is selected, then WinProxy will verify documents each time they are requested. This can significantly slow down access to Internet files, but it will guarantee that you always get the most current file.

If "When the file is older than XX hours" is selected, then WinProxy will check for newer files when the files are older than the specified time. This value is typically set to 12 or 24 hours, so that documents are verified every day, but in a single day, files are unlikely to change. This value can be set to verify documents when they are more than one hour old, or a whole week.

The slider and edit box below that allow you to configure the cache size. The number displayed in the edit box represents a byte size in kilobytes (1024 bytes). For instance, if you set the size to 100,000 KB, then your cache will be 100 Megabytes large. It is typically impractical to make your cache larger than 100 megabytes, because a larger cache will reduce system performance. If your cache is too small, however, then you may not have enough space to fully optimize your usage.

The last item allows you to change the location of the WinProxy cache. You can type in the new location, or you can press the browse button to find a directory to use for the cache.

Remember that if you change the cache location before emptying the cache, you will need to delete the old files yourself.

You can empty the cache by pressing the "Empty Cache" button.

If you want to view the contents of the WinProxy cache, or statistics on its usage, request the document <http://Proxy.Command/> from your administration machine, and you will have three options: to view cache statistics, Browse cached files or delete the files from the cache.

The first option in this dialog allows you to configure when WinProxy checks for modified files.

which users have access to WinProxy. It is highly recommended that you connect to the Internet before changing any of these settings.

There are two ways to administer users in WinProxy.

1) Allow access to all users, unless they are listed here with restrictions.

This option basically assumes that everyone on your network is allowed to use the Internet. If you choose to restrict an individual user, you can add them to the user list with their restrictions, without changing the ability for other users to access the Internet.

2) Restrict all users, except those listed here.

This option only permits access for those users who are listed in the User List. You can add or delete users, and change the access rights. If a user is not in the list, then they will not be permitted to access the Internet.

User administration can be done on a user basis or a group basis. Each entry in this list is essentially a group, which can have up to 500 users. If you do not have very many users, you can assign a different group for each user.

This dialog shows you the currently configured Users and allows you to add new ones.

To Add a new user group press the New button.

To Modify an existing group, select the group you wish to modify, and press the Edit button.

To Remove an existing group, select the group you wish to modify, and press the Delete button.

When you press Edit or New, you will see the [Edit Users Dialog](#), which allows you to enter the information required to set up a user group.

Users Tab in Advanced Properties

This tab in Advanced Properties allows you to configure which users have access to WinProxy. It is highly recommended that you connect to the Internet before changing any of these settings.

There are two ways to administer users in WinProxy.

- 1) Allow access to all users, unless they are listed here with restrictions.
This option basically assumes that everyone on your network is allowed to use the Internet. If you choose to restrict an individual user, you can add them to the user list with their restrictions, without changing the ability for other users to access the Internet.
- 2) Restrict all users, except those listed here.
This option only permits access for those users who are listed in the User List. You can add or delete users, and change the access rights. If a user is not in the list, then they will not be permitted to access the Internet.

User administration can be done on a user basis or a group basis. Each entry in this list is essentially a group, which can have up to 500 users. If you do not have very many users, you can assign a different group for each user.

This dialog shows you the currently configured Users and allows you to add new ones.

To Add a new user group press the New button.

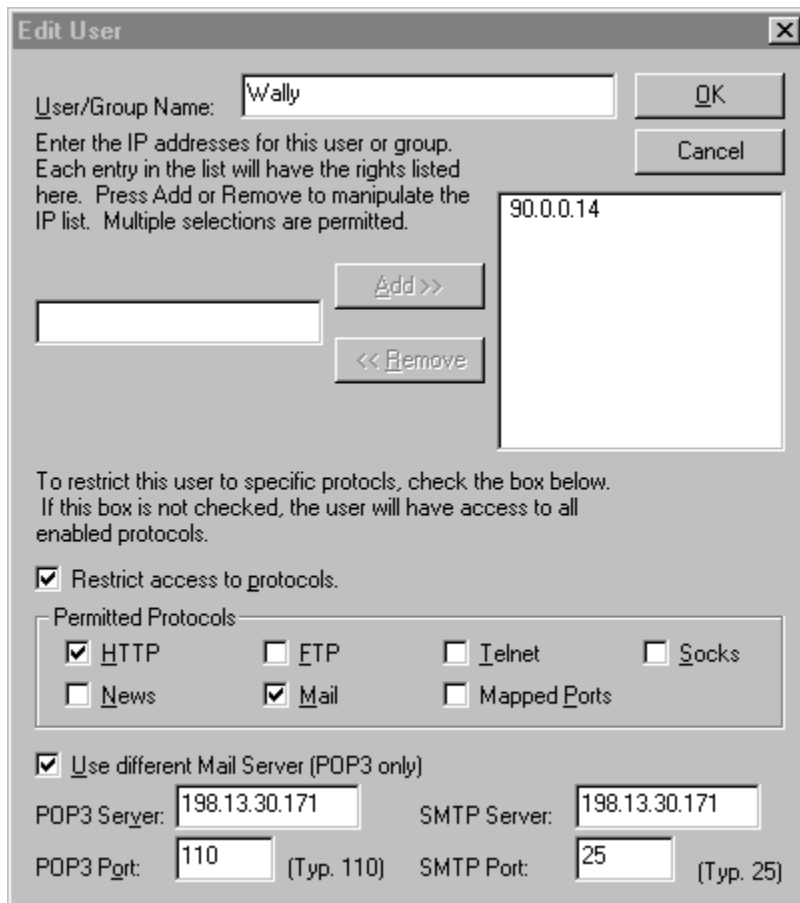
To Modify an existing group, select the group you wish to modify, and press the Edit button.

To Remove an existing group, select the group you wish to modify, and press the Delete button.

When you press Edit or New, you will see the [Edit Users Dialog](#), which allows you to enter the information required to set up a user group.

Edit Users Dialog

This dialog allows you to edit a user group. A group has a group name, and a list of IP addresses which are in that group. Each group has from 0 to 500 users, who can access the Internet under the same rights.



Edit User

User/Group Name:

Enter the IP addresses for this user or group. Each entry in the list will have the rights listed here. Press Add or Remove to manipulate the IP list. Multiple selections are permitted.

To restrict this user to specific protocols, check the box below. If this box is not checked, the user will have access to all enabled protocols.

Restrict access to protocols.

Permitted Protocols:

HTTP FTP Internet Socks
 News Mail Mapped Ports

Use different Mail Server (POP3 only)

POP3 Server: SMTP Server:
POP3 Port: (Typ. 110) SMTP Port: (Typ. 25)

In the above example, Wally is restricted to [Mail](#) and [World Wide Web](#) access. He also has a different mail server assigned, which means that a mail connection from Wally does not get forwarded to the default mail server configured in the Mail Setup, but it is connected to the mail server designated in this dialog.

In this case there is only one user in the group, and the group is named after that user. To add users to the group, you can simply enter the IP address of that user in the box in the center left, and press the Add button. The next user will be added to the list.

User/Group Name This field is the name of the group, which is displayed in the Users tab in properties. You can assign any name you like.

IP Address List Add and remove IP addresses from this list to add users to this group. If you add a user that is already in another group, you will get a warning message, but you will not be prevented from adding the user. The results in this case will be unpredictable, and you should resolve the conflict as soon as possible.

You can add up to 500 users to this list.

To add an entire subnet to a specific group, you can use a wildcard in the IP address. For instance, to restrict access to the entire 90.0.0.X subnet, you would enter 90.0.0.*. You can even specify * to include everyone. If two groups overlap, such as 90.0.0.* and 90.0.*, then the most specific group that matches will be used. For instance, if * is granted access to only HTTP, but 90.0.0.* is granted access to all protocols, then users matching 90.0.0.* will be granted full access, while others will only have access to HTTP.

Restrict access Check this box if you want to restrict access for a particular user. When this box is checked, all of the protocols will be enabled, and you will be able to check which protocols are to be allowed. Any protocol that is not checked will not be permitted from any of the IP addresses in the user list.

Use different mail server Select this item if this group requires a different mail server. Although most users can be accommodated with a single mail server, there are occasions where a particular user needs access to a different mail server. This is where the address of the [POP3](#) and [SMTP](#) server should be entered. All users in this group will be connected to the specified POP3 and SMTP servers. This feature is not supported for [IMAP4](#).

