Choose the Password you use to connect to the chosen RAS connection.

Choose the Username you use to connect to the chosen RAS connection.

Choose the name of the RAS/DUN connection you wish to use to connect to the Internet.

Choose this option if VSOCKS Light is connecting to the Internet via a LAN connection.

Choose this option if VSOCKS Light is connecting to the Internet via a RAS or DUN connection.

You will also need to configure the RAS parameters below.

Configuring the Client PC

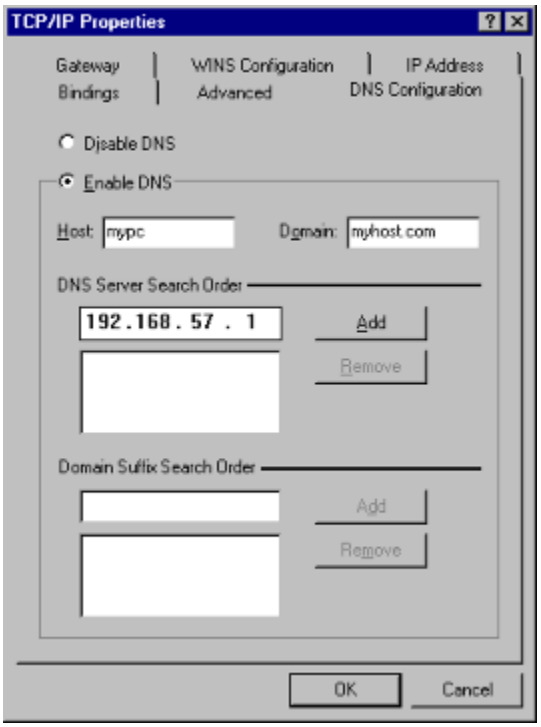
First of all you need to ensure that TCP/IP networking support is installed on each client PC. See here for more instructions on this.

Then each client PC needs to be told to perform DNS queries via the VSOCKS Light server.

To do this in Windows 95, go the control Panel -> Network Settings

Choose **TCP/IP** from the list of Network Components (if you have multiple TCP/IP entries, choose the one which is bound to your Network card). Press the 'Properties' button.

Now choose the **DNS Configuration** tab:



- Select **Enable DNS**.
- In the **Host** and **Domain** fields you can normally enter whatever you want. This setting is only used if some software on your PC asks the operating system what your PC is called. It is not visible to any other machines on the network.
- In the **DNS Server Search Order** enter the IP address of your VSOCKS server, and press the Add button. Note that you must do this *even* if this computer is running VSOCKS.
- You can leave the **Domain Suffix Search Order** blank.

You will now need to reboot the PC.

Once the PC has restarted, check that this part is working by going to a command prompt and running **PING www.pscs.co.uk**

You should see that VSOCKS dials out, and after a short delay, you see a response like this:

```
Pinging www.pscs.co.uk [195.112.13.3] with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
```

This response is correct. The important thing is that VSOCKS has dialled out and VSOCKS has been able to convert the name **www.pscs.co.uk** to the number **195.112.13.3**. The 'Destination host unreachable' error is because VSOCKS is unable to proxy the protocol used by the PING command.

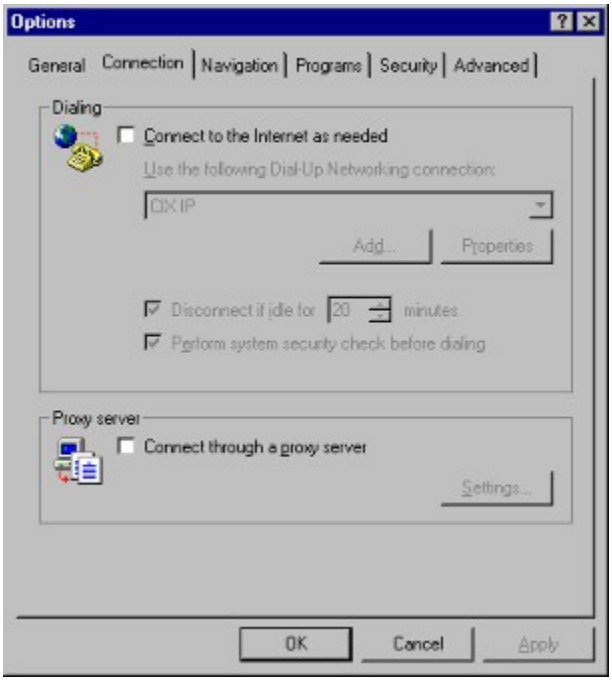
Now go on to configure your web browser or other Internet software.

Configuring Microsoft Internet Explorer 3

Run Internet Explorer 3.

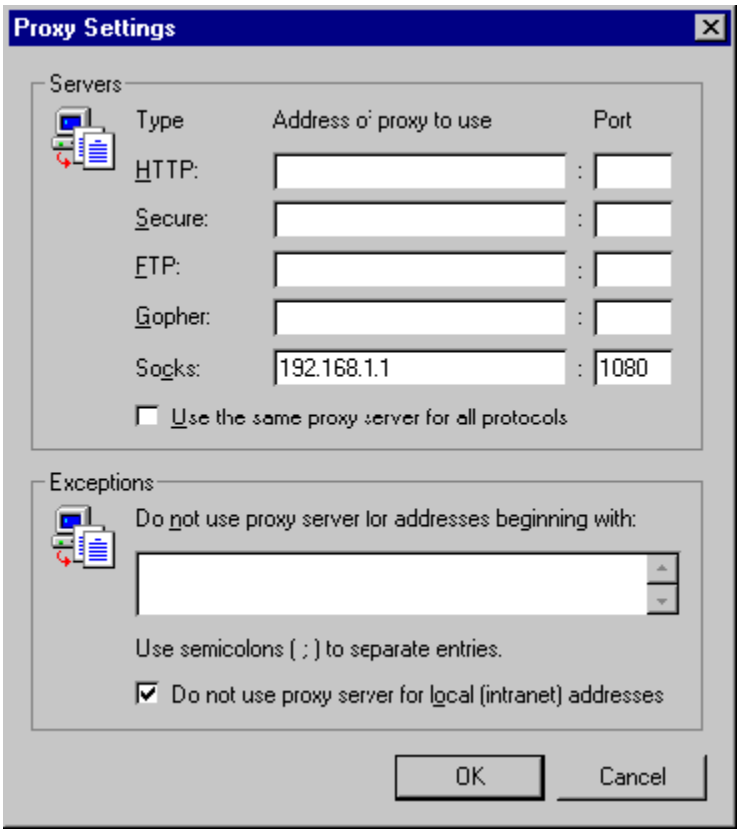
From the menu, choose **View** ->, **Options...**'.

Choose the **Connection** tab.



Disable **Connect to the Internet as needed**.
Enable **Connect through a proxy server**

Press the **Settings** button.

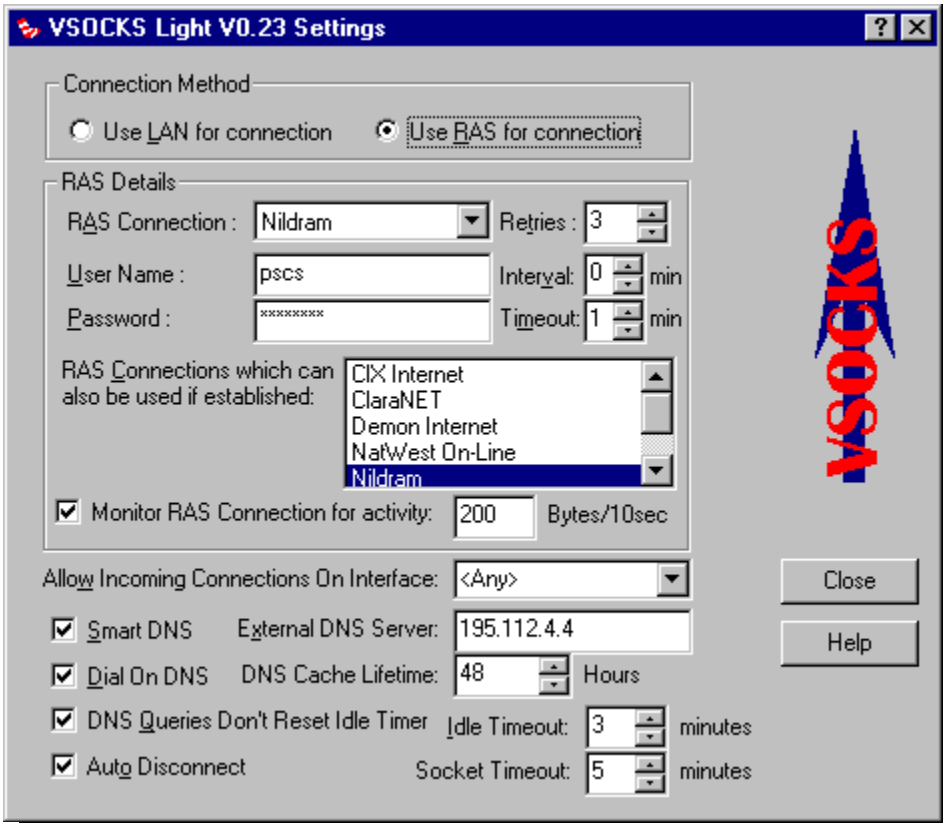


Make sure all the Proxy Server fields are empty, except for the **Socks Server** field.
In the **Address of proxy to use** field for that server enter the IP address of your VSOCKS server.
In the **Port** field enter **1080**.

You may need to close down and restart Internet Explorer for this change to take effect.

Configure VSOCKS Light

- You need to have TCP/IP configured on your LAN.
- Run **SETUP.EXE** which will install VSOCKS Light into a directory on your hard disk..
- Run VSOCKS.EXE.
- A red & white sock should appear in the Windows taskbar.
- Right-Click on this sock and choose 'Properties...'



- Choose the Connection Method (LAN or RAS) as appropriate.
- If you chose 'RAS', then enter the RAS connection details

The **RAS Connections which can also be used if established** option lets you select alternative connections to the Internet which VSOCKS Light can use if the PC is already online.

Monitor RAS Connection for activity tells VSOCKS to continually monitor the dial-up connection to see if any data traffic has gone across the link. If it has, then VSOCKS will keep the link open. This allows you to use other Internet software on the VSOCKS computer without VSOCKS hanging up on it. A possible problem with this is that sometimes computers will periodically send or receive data across the dial-up connection even when there is no obvious use of the Internet. This can cause VSOCKS to stay online longer than necessary.

In **Allow Incoming Connections on Interface**, you normally want to choose the IP address of the VSOCKS server *on your LAN.* This will prevent PCs connecting to it from the Internet.

In **External DNS Server** you MUST enter the IP address of a DNS server on the Internet. Your

ISP will normally have a DNS server which you can use. Ask them if you're not sure.

VSOCKS has a built in DNS cache which remembers recently used DNS query results. This means that VSOCKS does not need to dial the ISP as often as it would otherwise. VSOCKS does not use the 'proper' DNS entry cache lifetime values as these are often shorter than people want (usually 3 hours or less). You can set how long you want VSOCKS to remember entries by setting the **DNS Cache Lifetime** value. Note that if VSOCKS keeps the entries too long, they may have been changed so that VSOCKS actually remembers incorrect values. A reasonable value is from 24 to 72 hours. If you restart VSOCKS it will forget everything in the DNS cache.

Enable **Auto Disconnect** if you want VSOCKS to disconnect from the Internet after a predetermined idle time. If you enable this, then also set **Idle Timeout** - enter the time (in minutes) that you want VSOCKS Light to wait before ending an idle connection. If this is too short, then response will be slow, as VSOCKS Light will constantly be dialling up your ISP. If it is too long, then you will spend more time online than necessary. Two or three minutes is normally a good starting point, and adjust it as you require.

VSOCKS monitors individual TCP/IP connections to see if any data is flowing across them. If no data flows across a connection for the **Socket Timeout** time, VSOCKS will mark the connection as 'idle' (but not close it yet). When all the connections which VSOCKS has open are idle, it will close all the connections and start the **idle timeout** countdown.

VSOCKS Light can occasionally dial up for no apparent reason. This is because Windows 95 & NT can sometimes do DNS queries without you asking it to. VSOCKS Light normally has to query the ISP to get the results of this query (which is often "name doesn't exist" because it's for a name on your LAN). To try and reduce the number of times this happens there are two more options in VSOCKS Light:

1) **Smart DNS**. This tells VSOCKS Light to refuse any DNS queries which are a bit suspicious. These are:

- queries for names which have a section made up entirely of capital letters (eg **COMPUTER.NETWORK**)
- queries for names, where the top level domain (TLD) is less than 2 or more than 3 characters (eg **computer.on.my.network**)
- queries for names which contain two or fewer sections (eg **computer.net**).

If you turn **SMART DNS** on, then any queries to names matching this will fail without having to dial the ISP.

Smart DNS also attempts to catch rogue processes which are issuing DNS queries - see the Smart DNS topic for more details.

2) **Dial on DNS**. If you turn this off, then VSOCKS Light will never dial on a DNS request. This can cause problems because the SOCKS protocol requires the domain name to be resolved before it can be accessed. To get around this there is now a method of explicitly telling VSOCKS Light to connect or disconnect. See remote commands for help on these.

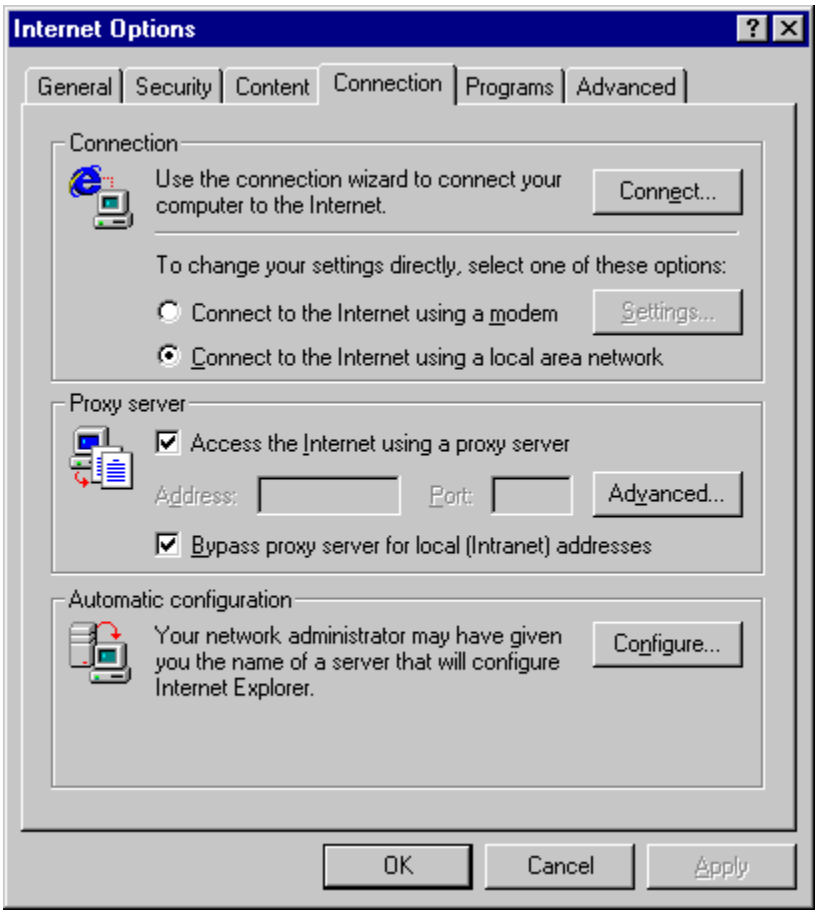
Some computers (especially NT computers) or software (eg Internet monitors) can periodically

do DNS queries to check response times or to download web pages when you're not otherwise using the Internet. The VSOCKS DNS Cache will reduce the effect of these queries, but you will still have VSOCKS dialing the ISP for no apparent reason. The **DNS.LOG** file will show which computers are doing which DNS queries at what times.

Configuring Microsoft Internet Explorer 4

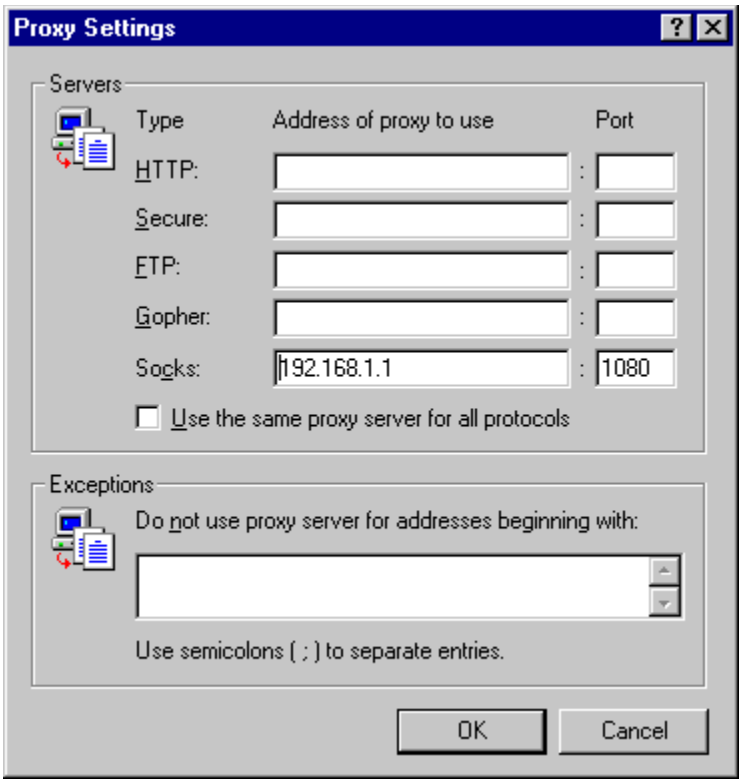
Run Internet Explorer 4

From the menus choose 'View' → 'Internet Options', and choose the **Connection** tab.



Choose **Connect to the Internet using a local area network**

Enable **Access the Internet using a proxy server**, then press the **Advanced...** button.



Leave all the proxy server address boxes empty, apart from the **Socks** proxy server box, put the IP address of the VSOCKS computer into this box, and then in the **Port** box type **1080**.

You may need to restart IE4 before the settings take effect.

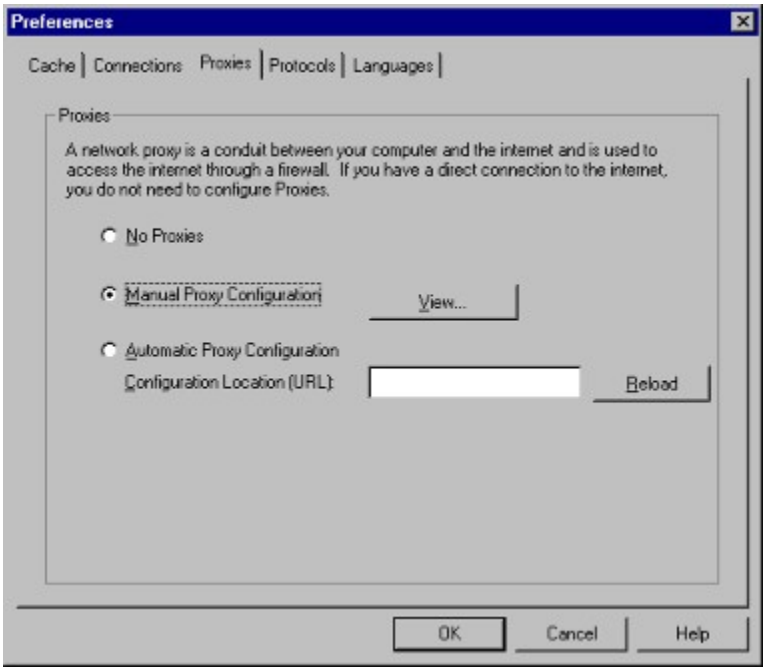
Note: IE4's support for SOCKS proxies is flaky and some people find that even though it is configured correctly, IE4 will not work through a SOCKS proxy. This problem is not a VSOCKS specific problem as a problematic IE4 will not work through any SOCKS proxy at all. So far, noone has come up with a reason why this only affects some IE4 installations. Hopefully it will be fixed with IE5.

Configuring Netscape Navigator 3

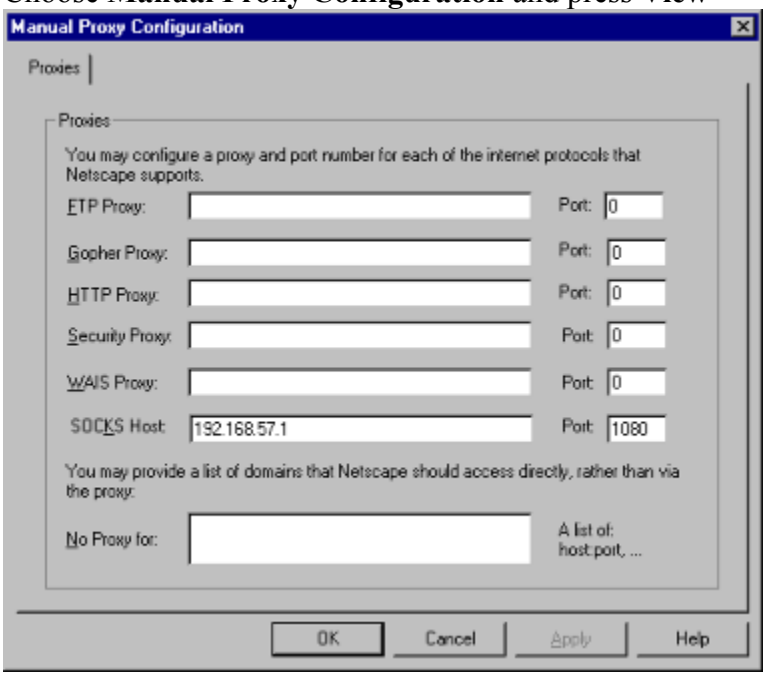
Run Netscape Navigator.

From the menus choose **Options** -> **Network Preferences**.

Choose the **Proxies** tab.



Choose **Manual Proxy Configuration** and press **View**



Make sure all the Proxy server fields are blank, except for the **SOCKS Host** field.
In the **SOCKS Host** field enter the IP address of your VSOCKS Server.
In the **Port** field, enter **1080**.

You may need to close down and restart Netscape Navigator for this change to take effect.

Configuring Netscape Navigator 4

To configure Netscape Navigator 4 to connect to the Internet via VSOCKS Light, go to:

Edit -> **Preferences** -> **Advanced** **Proxies** -> **Manual Proxy Configuration**

Press **View**.

Leave all the fields blank, except for the **SOCKS Host** setting, type the IP address of the computer running VSOCKS Light here, and in the **Port** field type *1080*.

Configuring other Client Software

To use other TCP/IP software through the VSOCKS server, you will probably need to install some SOCKS client. There are two packages which are recommended. Both are quite easy to set up, and allow you to access the Internet via VSOCKS just as if you were connected directly to the Internet, with any TCP/IP software.

These packages are both **Free**, and they are surprisingly easy to set up, the documentation with these packages tells you how to do it.

1) Hummingbird SOCKS Client at **http://www.hummingbird.com/freestuff.htm**.

2) SOCKSCAP at **http://www.socks.nec.com**

FTP Clients

Because of the way the FTP protocol works, you will need to set your FTP client to use the 'PASV' transfer method. If your FTP client doesn't support this, then I'm afraid it will not work with VSOCKS Light.

This is necessary because normally the FTP protocol requires the server to make a connection back to the FTP client, and VSOCKS Light does not allow incoming connections for security reasons.

ICQ/NetMeeting/RealAudio etc

These programs use the UDP protocol as well as TCP/IP. VSOCKS Light does not support proxying of UDP, so you cannot use these programs through VSOCKS Light.

You can still use them on the PC which VSOCKS Light is running on, but not on other computers on your LAN.

Contents

VSOCKS Light is a basic SOCKS proxy server for Windows 95, 98 & NT 4.0.

The SOCKS protocol supports proxying of *any* TCP/IP protocol, such as HTTP, FTP, TELNET, etc, with client software which supports the SOCKS protocol. If your client software doesn't support the SOCKS protocol directly, other software is available to 'SOCKSify' it's TCP/IP commands to make it work through a SOCKS proxy like VSOCKS Light.

Enter the IP address of a DNS server on the Internet. Normally this server is supplied by your ISP.

You MUST enter a valid DNS server address here!

Enter the number of times VSOCKS Light should attempt to try to connect to the Internet.

Enter the time (in minutes) between VSOCKS Light attempting to connect to the Internet.

Enter the time (in minutes) which VSOCKS Light will allow for making a connection to the Internet.

Enter the time (in minutes) which VSOCKS Light will wait before terminating an idle connection.

2 or 3 minutes is a reasonable starting point for this value.

Remote Operation Commands

You can control VSOCKS Light's dialing remotely by using it to perform queries for the **connect.now** and **disconnect.now** domain names.

For instance, if you run **PING CONNECT.NOW**, VSOCKS Light will dial up the ISP, and if you run **PING DISCONNECT.NOW** it will disconnect from the ISP if it can (eg if no-one else is using it).

To make life easier, you can also use the **Connect.exe** and **Disconnect.exe** programs which were installed into the VSOCKS Light directory at installation time. These programs can be copied onto the other client PCs on your network if you want the users to be able to tell VSOCKS Light to dial out.

Select alternative RAS/DUN connections which VSOCKS Light can also use to proxy requests to the Internet.

(VSOCKS Light will not attempt to initiate any of these connections, but it will use one if it sees it already active).

Select the IP address of the connection on which VSOCKS Light will allow incoming connections.

Normally you will want to specify the IP address of the VSOCKS Light server on your LAN.

Setting up local DNS names in VSOCKS Light

Normally, if a client PC asks VSOCKS Light to look up a domain name, VSOCKS Light will connect to your ISP, and ask their DNS server to look up the name.

Sometimes this can be undesirable, either because you want to have your own local names, or because some software on your PCs is doing a DNS look up for no apparent reason.

To help to solve these problems, VSOCKS Light contains a very basic DNS server as well as the DNS proxy which is normally used.

(Also see the Smart DNS topic for more ways which VSOCKS can stop spurious DNS queries from triggering a dial to the ISP.)

To configure the DNS server, you need to create a text file called **DOMAINS.LST** in the current directory when VSOCKS Light is run (this is normally the directory containing VSOCKS.EXE). The format of this file is very simple:

DomainName IPAddress

For instance:

www.intranet 192.168.0.1

vpop3.intranet 192.168.0.2

You can also specify the ***** wildcard instead of any section of the name, so you could have

***.intranet 192.168.0.1**

This would mean that *www.intranet*, *vpop3.intranet*, *fred.intranet* etc. would all resolve to the address 192.168.0.1

Note that *www.fred.intranet* would **not** resolve to 192.168.0.1 using this method. The '*' only matches a single section of the name.

If you specify the address relating to a name as **0.0.0.0**, then VSOCKS Light will report authoritatively that the name does not exist.

After changing the **DOMAINS.LST** file, you need to restart VSOCKS Light for the changes to take effect

Note that VSOCKS Light will also read your existing **HOSTS** file which Windows understands. However, that is not sufficient for all uses, as it does not support wildcards or the **0.0.0.0** address, so you can have some entries in the **HOSTS** file and some in the **DOMAINS.LST** file if you wish.

Setting up your LAN

The network where VSOCKS Light is to be installed needs to support TCP/IP. TCP/IP is the protocol used on the Internet. A full discussion of setting up a TCP/IP network is too complex to go into here, but a quick introduction will take place.

Installing TCP/IP support on the networked machines

First of all, you need to ensure that all the machines which will need to connect to VSOCKS Light support TCP/IP. In Windows 95, you install TCP/IP support by going to the *Network* applet in the control panel. In the list of 'Network Components', there should be an entry 'TCP/IP', or 'TCP/IP via <network adapter>'. If this entry doesn't exist, then press the 'Add' button, followed by 'Protocol', then choose 'Microsoft' from the list and choose 'TCP/IP'.

Assigning IP addresses

Secondly, each machine on the network needs to be given a unique IP address. This is a number made up of four parts (e.g. **192.168.65.120**). If two machines on a network have the same number, then they won't work correctly.

For these instructions we will assume that you have a network which is **not** directly connected to the Internet. We will also assume that you have a relatively small network (less than approx. 250 PCs) all on the same network segment.

In this case, a set of IP numbers have been assigned which you are allowed to use, with no risk of them conflicting with 'real' Internet addresses. These numbers start with **192.168** (there are a couple of other sets you can use instead if you wish, but we prefer the **192.168** set). If you add another number (between 0 and 255) to these numbers you have chosen your *Network* address. For this example we will use **1**, so our network address is **192.168.1.0**. (the trailing '0' means that this address refers to a network, rather than a single machine). You can use this network address, or choose your own third number of the address. To go with this network address, the complementary number is the *Subnet Mask*; in this case, the *Subnet Mask* is **255.255.255.0**.

Now, you just need to assign a number between 1 and 254 ('0' means the network, as described above, and '255' signifies a broadcast address), and put this in place of the '0' in your chosen network address. It is best, at this point, to get a paper and pen, and make a note of all the addresses you assign, to ensure that you won't reuse an address if you add another PC in the future (if you do reuse an address, you'll spend many entertaining hours trying to work out why your network has stopped working...). This means, that in our example, the first PC could have the address **192.168.1.1**, the second PC could have **192.168.1.2**. *Note: All the machines on this network have a **Subnet Mask** of 255.255.255.0!*

Note that there is no need to run sequentially, as long as the last number is unique, you can use whichever number you want between 1 and 254. Therefore it is often useful to divide numbers into logical groups, for instance, numbers 1 - 10 might be Intranet servers, 11 - 30 might be in one office, 31 - 50 might be in another office etc.

Testing your TCP/IP LAN

Once you have set up at least two PCs with TCP/IP support it is best to start testing it as you go along. The basic way of doing this is by using the **PING** tool which comes with Windows 95 and Windows NT. **PING** basically sends a short message (a 'ping') from one machine to another, the

target machine responds, and the first machine tells you that it has got a response and how long the message took.

So, if you've just set up machines with IP addresses **192.168.1.1** and **192.168.1.2**, you would type '**PING 192.168.1.1**' in a DOS box on the machine with address **192.168.1.2**. You should get a response something like:

```
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<10ms TTL=32
Reply from 192.168.1.1: bytes=32 time<10ms TTL=32
Reply from 192.168.1.1: bytes=32 time<10ms TTL=32
Reply from 192.168.1.1: bytes=32 time<10ms TTL=32
```

If you do get a response like this, then all is well. Any other response means that something is wrong. Check physical network connections first, then panic...

Every time you configure a new machine, you should check that you can **PING** the same machine - so always check that you can **PING** the first machine you set up. This way, if all machines can **PING** a single machine, it is very likely that all machines can **PING** each other as well.

This field indicates the current state of any connection to your Internet Provider. Normally it will show "Offline" indicating that there is no current connection. If it shows "Online" then a connection is currently established. Other messages show the current state whilst setting up a RAS connection.

Whilst a connection is in progress, you should see two coloured bars in this field. The upper green bar shows the progress of the current POP3 connection (retrieving messages) and the lower blue bar shows the progress of the SMTP connection (sending messages)

Web Browser Configuration

Most Web Browsers support the SOCKS protocol directly, so configuring your web browser is a simple case of telling the web browser to connect to the Internet over a network (instead of a dial-up connection), and to use **only** a SOCKS proxy at the IP address of the VSOCKS computer, with a port number of 1080.

See below for more specific information on the most popular web browsers

- Internet Explorer 3.x
- Internet Explorer 4.x
- Netscape Navigator 3.x
- Netscape Navigator 4.x
- Opera (Unfortunately Opera does not yet support the SOCKS protocol directly, so you need to set up the client PC as for *other Internet software)*

Access Logging

VSOCKS creates a file called **ACCESS.LOG** in the VSOCKS directory. This contains information about which users have used VSOCKS and for what.

Each line in the VSOCKS.LOG file contains a data record. A typical line is shown below:

29/6/1999 18:16:58.718 - 192.168.57.100 195.112.5.192 80 310 5391 16

1) **29/6/1999** is the date

2) **18:16:58.718** is the time this TCP/IP link *finished*

3) **192.168.57.100** is the *client* (ie user's) computer IP address

4) **195.112.5.192** is the remote computer IP address

5) **80** is the remote computer TCP/IP port number (see below)

6) **310** is the amount of data *sent* to the remote computer

7) **5391** is the amount of data *received* from the remote computer

8) **16** is the length of time, in seconds, that this TCP/IP link lasted

Port Numbers

The remote computer's TCP/IP port number usually indicates the type of data transfer which was taking place. The common ones are listed below:

- 21 FTP. Note that this is the FTP control channel. FTP data is transferred on another port which changes each time
- 25 SMTP - mail sending
- 80 HTTP - web access
- 110POP3 - mail receiving
- 389LDAP - directory server

Enable this option if you want VSOCKS to hangup the dial-up connection after the specified **Idle Time**.

(Default = ON)

Enable this option if you want VSOCKS to dial the ISP when it receives a DNS query.

(Default=ON)

Enter the time (in hours) that you want VSOCKS to remember previously requested DNS entries.

Choose this option if you want VSOCKS to monitor the dial-up connection to see if any other data is being sent or received over it. If VSOCKS sees other data being transferred, it will keep the link open even though nothing is connecting trhough VSOCKS.

NOTE: Windows can sometimes receive or send small data packets over the connection which can cause VSOCKS to keep it open longer than necessary if this option is enabled.

This option makes VSOCKS look at DNS queries to see if they match certain criteria, if they do, it assumes that the DNS query is actually for a local computer name rather than an Internet name, so it will not dial the ISP to resolve the query.

The following types of DNS queries are filtered out:

- queries for names which have a section made up entirely of capital letters (eg **COMPUTER.NETWORK**)
- queries for names, where the top level domain (TLD) is less than 2 or more than 3 characters (eg **computer.on.my.network**)
- queries for names which contain two or fewer sections (eg **computer.net**).

Smart DNS will also attempt to filter out rogue processes which are continuously doing a DNS query. The logic it uses is:
- if a particular computer has looked up the same name twice in succession, then

1) look at the time difference between the two lookups. If it is more than 5 minutes, then let the second query go through.

2) if the computer has looked up the same name at least 10 times and has been doing so for over 5 minutes, VSOCKS will mark it as 'potentially rogue'

3) If a 'potentially rogue' DNS query would make VSOCKS dial the ISP then it will just discard the query. If VSOCKS has the response in the DNS cache or in the DOMAINS.LST file, then it will still process the query.

This timeout is how long an specific TCP/IP connection is allowed to have no data transferred across it before VSOCKS decides that it is idle. If all the connections through VSOCKS are idle, then it will close all the connections and start the **Idle Timeout** countdown.

VSOCKS Log Files

VSOCKS produces 3 main log files:

- ACCESS.LOG This contains a summary of VSOCKS usage by client computers
- DNS.LOG This contains a list of all the DNS names which have been looked up by client computers
- ONLINE.LOG This contains a summary of the time which VSOCKS has been online

These log files are all stored in the VSOCKS directory and are all timestamped. When the files reach a certain size (100k) VSOCKS will rename them to <something>.OLD and start a new .LOG file.

This option will prevent VSOCKS from resetting the idle timer when a DNS query is processed. This can be useful if something is making VSOCKS stay online because of spurious DNS queries.

Also see the Smart DNS topic for ways which VSOCKS can prevent spurious DNS queries from making it stay online.

The **Monitor RAS** option can be too sensitive sometimes since Windows can sometimes send data over the dial-up link when it is apparently idle. Setting a threshold will tell VSOCKS to ignore data transfers smaller than this amount (counted on 10 second intervals).