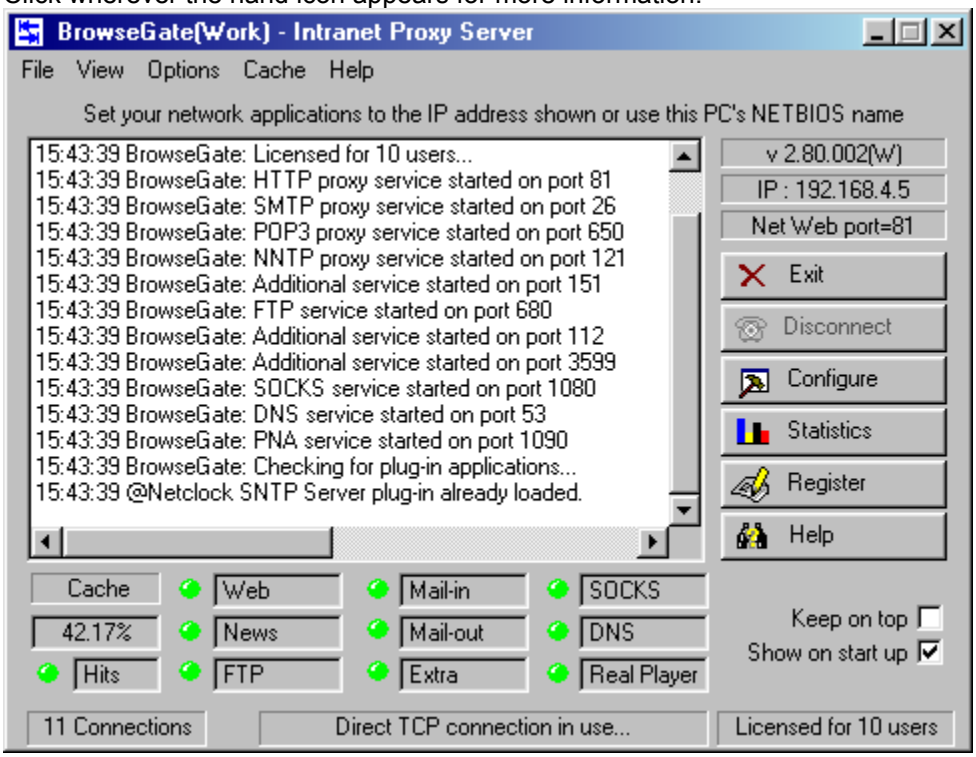
BrowseGate - Contents

Main BrowseGate Window

See Also: Configuring BrowseGate
Registering BrowseGate

Click wherever the hand icon appears for more information.



The main BrowseGate window is shown above. The information panel shows that this is a licensed copy for up to 10 concurrent users. It also shows that it is configured to listen on TCP/IP port 81 for requests for access to the World Wide Web from networked web browsers. The green LED's show that BrowseGate is supporting ALL common protocols.

To toggle the active status of the following proxies quickly, you need only double click the name or the LED alongside them, or you can use the View menu which also contains a list of most settings:

You can double click the LED's (or labels) to enable/disable the following proxies :

Cache
News
Mail (POP3 and SMTP are both switched)
SOCKS 4/5
DNS
(ONLY the EXTERNAL DNS is switched, The Internal DNS is only accessible via the Configuration property sheet.)
Real Player

What is BrowseGate ?

See also: Setting up eMail clients | Setting up Web Browsers | Setting up News clients | Setting up FTP clients | Setting up SOCKS4/5 clients | The built-in Domain Name Server | The built-in cache

BrowseGate is what is generally termed a high level "Proxy Server".

What this really means is that BrowseGate allows multiple networked computers to access the Internet at the same time, using just one "external" connection of nearly any type (modem, ISDN, cable modem, leased line or ADSL/RoadRunner connection, etc.). It will run on any low specification Windows 95/98/or NT4/2000 (Workstation or Server) computer, which does not have to be "dedicated" to the task.

BrowseGate can provide Internet connectivity for any computer that can run the Internet standard protocol - TCP/IP - This includes Apple Mac and Unix/Linux computers as well as Amiga and others, plus of course any Window's based PC's, and provides full access for most popular applications such as Netscape Navigator, MS Internet Explorer, Outlook and Outlook Express, Eudora, Netscape Mail, popular NNTP News programs, Internet Chat programs such as mIRC, communications applications such as ICQ and Yahoo Messenger, plus most popular FTP programs and many, many others.

It is designed to allow as many of your networked PC's as you wish to have (simultaneous) "on-demand" access to virtually all aspects of the Internet using just a single modem or other connection device on a single PC (the PC that BrowseGate is installed on). It can of course also connect to these same services via standard permanent connections such as Routers and ISDN links to the Internet without the need to use a modem if you are fortunate enough to have such a connection, or to local web and email/news servers that are accessible across your intranet without the use of a modem at all.

So what happens once you have installed and configured BrowseGate and setup your Web Browsers and Email/News/FTP/Communications clients on the network to access BrowseGate.?

Each time any of your networked PC's enters a URL into a web browser, or another application wants to connect to some server machine out on the Internet, BrowseGate receives those requests across the network, and it will then fetch the page from the web site specified, or send/fetch mail and news articles etc etc, providing of course that no blacklist or other rules you may have setup in BrowseGate prohibit the request.!!

Modem connections (only)
BrowseGate checks to see if it already has a connection to the Internet and if not it makes a connection by dialing out using the connection you have specified for the Windows/NT dial-up networking system (DUN/RAS).

To save connection costs, you simply set a maximum timeout period (default is 15 minutes). Once that timeout period has expired without any further web browser activity from any connected browser having been received, BrowseGate will automatically attempt to ensure that it's dial up connection is dropped, providing you have "disconnect" option checked (which is the default setting)

General
BrowseGate has been designed especially to work as either a stand alone server or as a plug-in option for our SmartServer3 email server system. This means that you can have BrowseGate installed and operating on the same PC as SmartServer3, using the same modem, and both systems will cooperate to ensure they share the modem connection correctly. You can even have SmartServer connect to the Internet and WWW via BrowseGate if you really wish to !!.

Once you are ready for more powerful control over your network email then we recommend that you check out the details of our SmartServer3 email server system, which is designed especially to work with BrowseGate to provide Industry Standards, full function mail handling for any business network. Full

information and a 5 user evaluation version of SmartServer3 is available from our web site.

Overview - Configuring your new BrowseGate Proxy Server

See Also : Setting up your networked PC's

The following notes are aimed at network administrators, (or even budding network administrators) who wish to provide their entire networks with Internet access via BrowseGate.

They assume that you have at least a basic grasp of TCP/IP and are able to set up Internet applications such as web browsers and email client packages to work successfully on a single PC.

INTRODUCTION

Because a proxy server is a rather clever piece of software that, just like every other Internet application, uses the TCP/IP protocol to connect to both other PC's and to the Internet itself, it requires that you configure, or, as is more often the case, reconfigure your networked TCP applications and possibly some of your network's TCP/IP settings in order that you are able to take advantage of any proxy server such as BrowseGate.

Yes - we know that may sound complex - but it is actually quite simple, and once you have understood the reasons and steps behind it, you should be able to have it all working really quickly. The following notes will try to outline what is necessary, and the steps you need to perform to get it all going .....

It is assumed that you already have TCP/IP installed and working on one or more PC's on your network, including the PC on which you have just installed BrowseGate.

If the BrowseGate PC is THE ONLY one on your network that has TCP installed on it, we suggest that you go through section ONE below, otherwise you can probably skip this and go straight to section TWO (as long as you know what the IP address of the BrowseGate PC is).

SECTION ONE (specifying an IP address on the BrowseGate PC)
Click here for more detailed information on this topic ...

You need to ensure that this PC has been allocated a valid class "C" IP address such as 192.168.100.1 To do so go to the W95/98 Start menu on the task bar, select Settings, then select Control Panel, and finally, double click on the "Network" entry in the list displayed.

Scroll down the list of "Network components installed" until you find an entry that looks something like :- TCP/IP -> network_card_name (where network card name is the typically the manufacturer of your NIC/network card, eg : Artisoft, Dec, etc.)

You DO NOT want to select any entry that says TCP/IP -> Dial-up Adaptor (at least not yet...)

Having selected your network cards TCP entry, click the Properties button, and ensure that you are on the tab labeled "IP Address".

You must have the "Specify an IP address" option checked.

Now if you already have any numbers in the two fields below the option, then just make a note somewhere of the one labeled "IP Address". Why - Well you may well need this later on to configure your other networked PC's. You also need to select the "DNS configuration tab and note down each of the IP addresses that should be in the "DNS Search Order" list box.

If you don't have any numbers in these fields, then read the help system on how to set up TCP/IP on your

network.

SECTION TWO (Domain Name server)
Click here for more detailed information on this topic ...

Now you have to make a very important decision which is - "Do you want to use the built-in Domain Name Server (DNS) in BrowseGate?"

This is actually a simple decision - If you already have a working DNS on your network (such as an NT4 server system), then you should DISABLE the BrowseGate system entirely. Otherwise, we strongly recommend that you should use the DNS in BrowseGate, although it is not mandatory.

Assuming you do accept our recommendation to use the BrowseGate DNS system, click the Configure button on the BrowseGate main window, and then select the DNS tab on the property sheet. Ensure that you have both the "Enable internal" and "Enable external" options checked.

Enter the main IP address of your ISP's DNS server (which they will have given you) in the "external DNS settings" panel below. Unless you have a good reason to needing to do so, do NOT change the port numbers.

Don't worry about having no entries in the Internal list at present.!

Click the Apply button to save the changes.

BrowseGate is now configured to provide all required DNS services for your networked Internet applications.

SECTION THREE (Setting up the Internet access services BrowseGate is to provide)

BrowseGate can provide every PC on your network with on-demand Internet access to perform any/all of the following tasks, and some we haven't mentioned....

Email delivery and collection via POP3, IMAP4 and SMTP.
Web Browsing via HTTP, HTTPS, SOCKS 4/5
NNTP News collection and delivery
FTP (File Transfers via packages such as CuteFTP, WS_FTP, FTP Voyager and Absolute FTP)
Communications systems such as ICQ, Internet Phones etc via SOCKS 4 or 5

3.1. Web access for your networked web browsers.

Many networked users need to access the World Wide Web, and BrowseGate does of course allow them to do so very easily.
Click here to view the "Connect" configuration tab.

On the "Configure" property sheet, click on the "Connect" tab.
Select and enter a port number for BrowseGate to use to connect to all your web browsers. We recommend port 80 or 81.
Make a note of the port you have selected so that you can configure all the web browsers correctly later.

3.2. Email access for networked email clients.

Many networked users have their own email accounts and run a client such as Outlook or other similar email package. If you have your own domain, or your ISP provides you with a mail forwarding account, so that all email from your ISP is held in a single mailbox and you normally download it to to an email

server on your network (such as our own SmartServer email server), then the easiest way to do this is to use the special built-in email proxy in BrowseGate to access this account.
Click here to view the "Email" configuration tab.

On the "Configure" property sheet, click on the "Email" tab.
Enter then name of your Pop3/Imap4 mailbox in the Incoming mail field.
Enter then name of your SMTP mail server in the Outgoing mail field.
These are exactly the same server details as currently set in your email client package(s)
Leave the "Remote" ports set to the default settings.
Select any port number you wish for the local ports, or you may leave them at the default settings.

3.3. NNTP News access for networked email clients.

Many networked users have News clients such as Outlook or other similar News packages. If you wish to provide access to your ISP's News Server then :-
Click here to view the News" configuration tab.

On the "Configure" property sheet, click on the "News" tab.
Enter the name of your News Server in the News Server name field.
This is exactly the same server name as currently set in your news client package(s)
Leave the "Remote" ports set to the default settings.
Select any port number you wish for the local port, or you may leave it at the default setting.

3.4 Collecting mail from multiple different mailboxes/hosts
If many of your networked users each have their own email accounts and run a client such as Outlook or other similar email package, you may wish to allow them all to access their personal mailboxes individually via BrowseGate.
Click here to view the "TCP mapping" configuration tab.

On the "Configure" property sheet, click on the "Map TCP" tab.
Click the New button.
Enter the name of whichever Pop3/Imap4 mailbox you wish to provide access to in the "Connect to host" field.
This will be exactly the same server details as currently set in the relevant email client package.
Leave the "Remote" ports set to the default settings.
Now you need to select any available (free) port number you wish to assign as the local port for this connection. You only have to worry about not selecting any of the default ports normally reserved by TCP as listed in the Ports section (Click here for a list of ports you cannot use). (BrowseGate will warn you when you try to save these if you have accidently duplicated a port number)

3.5. Setting up TCP port mapping

Because BrowseGate provides support for most types of Internet connection, you can create "TCP port mappings" to act as a gateway for almost any internet client application you require BrowseGate to provide a gateway for.
Click here to view the TCP Mapping configuration tab.

On the "Configure" property sheet, click on the "Map TCP" tab.
Click the New button.
Enter the name of whatever host machine it is that you wish to provide a gateway to in the "Connect to host" field.
Set the "Remote" port to the correct port for the service in question (eg :FTP-21, POP3-110, SMTP-26 etc)
Select any available (free) port number you wish to assign as the local port for this connection. Again

you only have to worry about not selecting any port already used, or using one of the default ports normally reserved by TCP as listed in the Ports section (Click here for a list of ports you cannot use). (BrowseGate will warn you when you try to save these if you have accidently duplicated a port number)

3.6. Providing SOCKS 4/5 support

BrowseGate supports both SOCKS 4 and SOCKS 5 for most types of Internet client applications that require this.
Click here to view the "SOCKS" configuration tab.

On the "Configure" property sheet, click on the "SOCKS" tab.
Check the "Run Socks 4/5 proxy server " option
Set the port to whatever you wish. The default is 1080. Please note that some SOCKS applications do not allow you to change this port number.
(Click here for a list of ports you cannot use). (BrowseGate will warn you when you try to save these if you have accidently duplicated a port number)

SECTION 4 (Connecting to the Internet)

BrowseGate can be used to connect via the Window's Dialup Networking (DUN/RAS) system, or via fixed connections such as routers and other fixed connections.

4.1 Dial-up networking

These notes assume that you have already successfully installed dial-up networking, and have a working dial-up connection on the BrowseGate PC.
Click here to view the "Connect" configuration tab.
On the "Configure" property sheet, click on the "Connect" tab.
Select the "Use Dialup networking" option box.
If you have more than a single DUN connection configured, select the one you wish BrowseGate to use.
Enter the number of minutes that you want BrowseGate to stay on line before dropping the phone line when there are no network requests being handled in the "Disconnect after xx minutes" field. We recommend 10 or 15 minutes as being a reasonable time to avoid incessant dials and line drops, but it does of course depend on the level of your network's use of the internet. You can use the modem statistics reports to tune this setting as your network starts to use Browsegate in earnest day on day.
Select any of the other options provided to suit your own preferences.

4.2 Permanent connections to the Internet

Click here to view the "Connect" configuration tab.
On the "Configure" property sheet, click on the "Connect" tab.
Select the "Use standard TCP" option box.
Thats it.....

Configuring BrowseGate to support additional proxy services using TCP port mapping

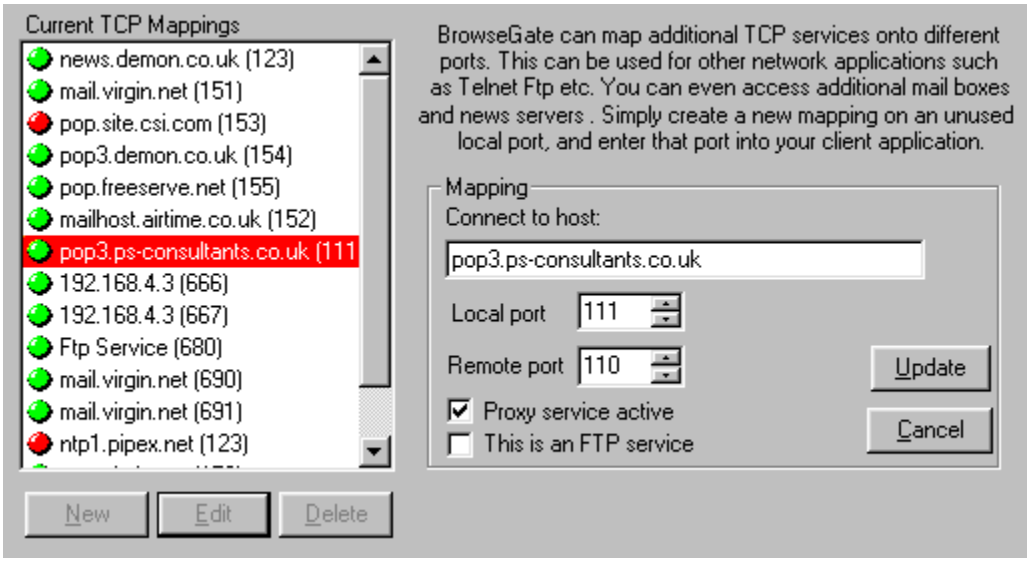
For other Configuration tabs - click on tab shown below...

See Also: Configuring popular FTP clients

Because many intranets have the need to connect to more than a single mail host or different news servers, BrowseGate provides you with the ability to configure (or Map) as many additional ports as you want to act as "proxy services" to your TCP client applications on your network.

The configuration and use of these mapped TCP proxy services is quite simple once you understand the way that ports are used in TCP/IP communications.

Click on a tab to move to that configuration option, or click wherever the hand icon appears for more information.



The property sheet tab above shows 7 extra ports configured, all setup to connect to different email host machines apart from the first one, which is a connection to a news server. Please click on the diagram above for details of how these settings work...

Address alias settings

For other Configuration tabs - click on tab shown below...

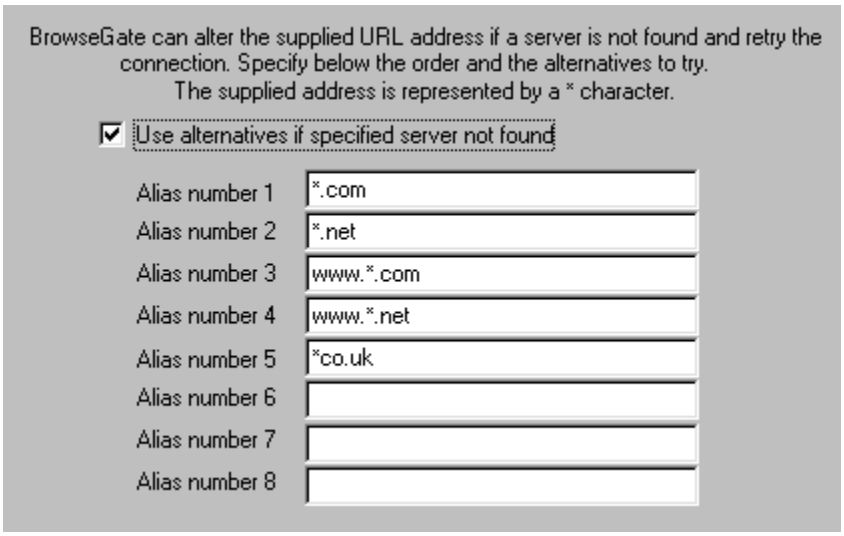
The address aliasing in BrowseGate allows you to type simple commands into the URL field of your browser such as "mywebsite", and let BrowseGate try to find suitable matching "full" URL addresses for you.

In the dialog shown, BrowseGate would try each of the entries shown in sequence attempting to connect to a URL that is comprised of any of the entries, which are used to replace the "*".

So in our example it would try the following in order until it succeeded to connect or had tried all options :

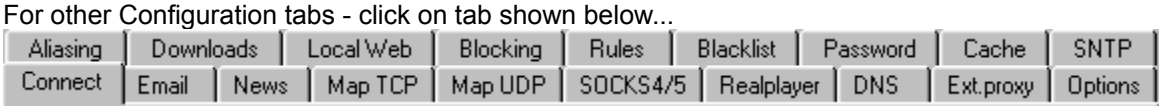
mywebsite.com, mywebsite.net, www.mywebsite.com, www.mywebsite.net

Click on a tab to move to that configuration option, or click wherever the hand icon appears for more information.



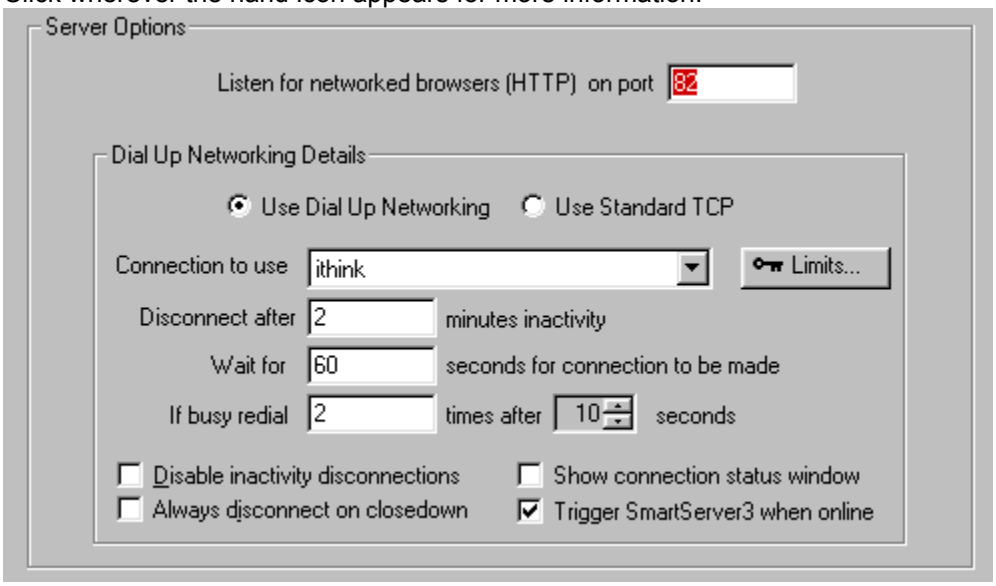
Configuring BrowseGate

For other Configuration tabs - click on tab shown below...



Both standard Dial up connections using the built in Windows Dial Up Networking system (and NT4 RAS system) or direct TCP/IP connections are fully supported. This tab lets you specify and configure the external connection method BrowseGate will use to connect to the Internet or WorldWide Web.

Click wherever the hand icon appears for more information.



Configuring BrowseGate to support NNTP news

For other Configuration tabs - click on tab shown below...

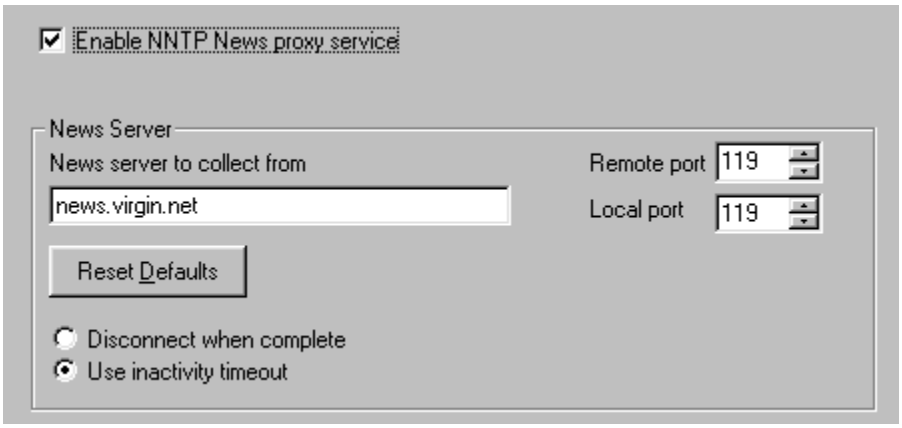
Aliasing | Downloads | Local Web | Blocking | Rules | Blacklist | Password | Cache | SNTP
Connect | Email | News | Map TCP | Map UDP | SOCKS4/5 | Realplayer | DNS | Ext.proxy | Options

See also: Configuring your news clients
Ports - what you need to know

BrowseGate can provide automatic access to a complete network to allow all PC's to fetch and post news articles from the Internet's NNTP news system

To configure this click "Configure" on the main BrowseGate window, and then select the "News" tab.

Click on a tab to move to that configuration option, or click wherever the hand icon appears for more information.

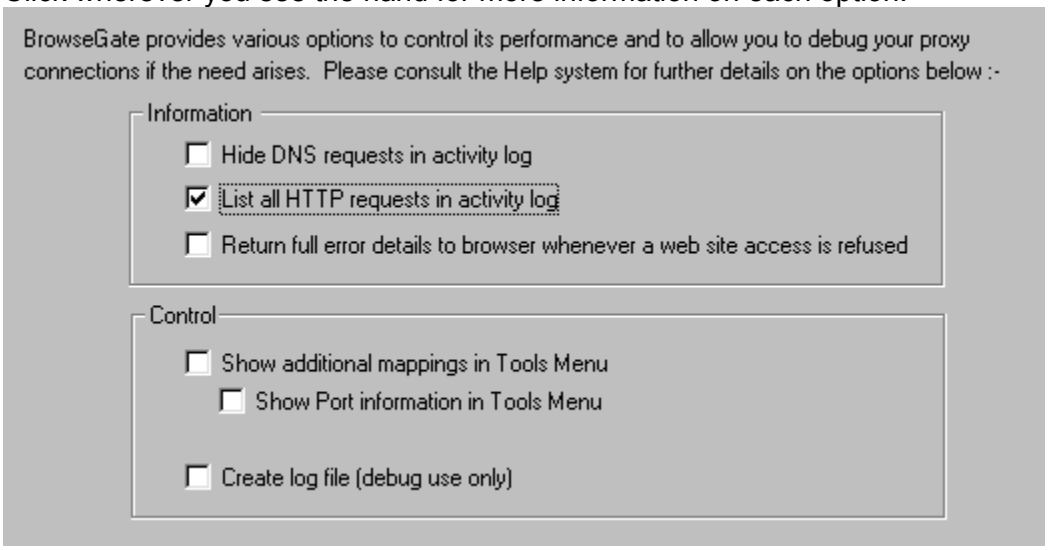


It is most important that you also ensure that the port settings in each your news clients configurations match those you have selected on this tab. See - Configuring your news clients and Ports - what you need to know

Configure - Options

BrowseGate offers various special settings on the Options tab. Most are for advanced uses....

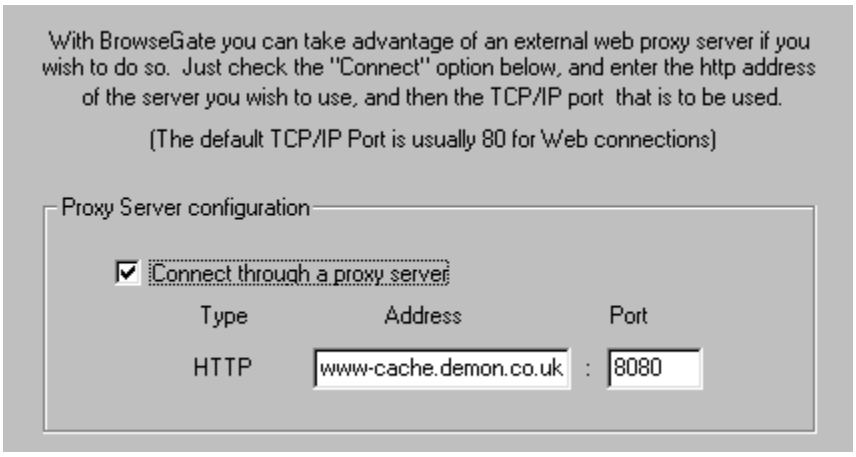
Click wherever you see the hand for more information on each option.



Proxy server settings (Local Web site)

For other Configuration tabs - click on tab shown below...

Click on a tab to move to that configuration option, or click wherever the hand icon appears for more information.



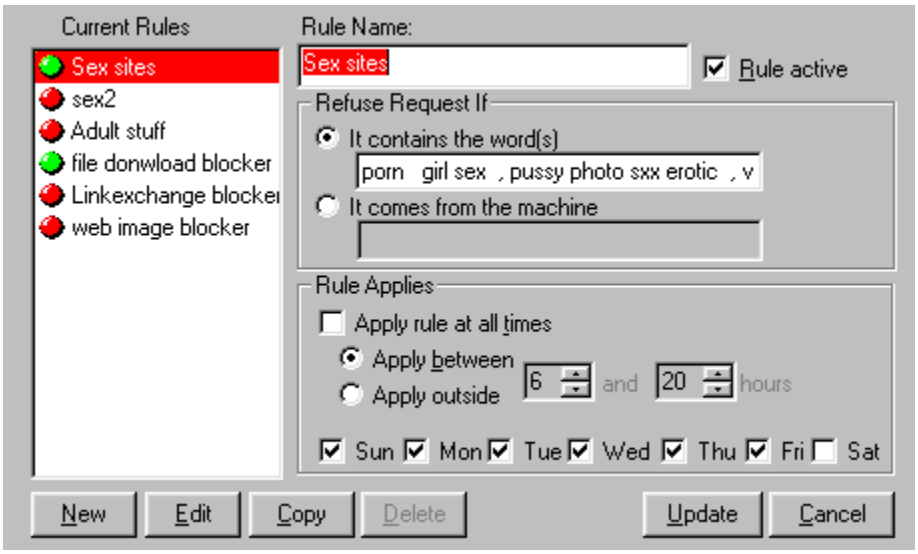
Rules

For other Configuration tabs - click on tab shown below...

Aliasing | Downloads | Local Web | Blocking | Rules | Blacklist | Password | Cache | SNTP
Connect | Email | News | Map TCP | Map UDP | SOCKS4/5 | Realplayer | DNS | Ext.proxy | Options

See Also: How to create a Rule

Click wherever the hand icon appears for more information.



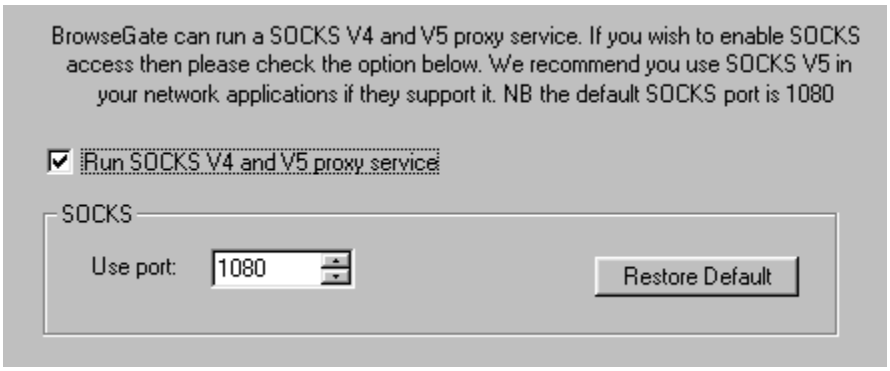
Configure - SOCKS SERVICE

For other Configuration tabs - click on tab shown below...

See also: How to use the SOCKS support

BrowseGate provides full support for both SOCKS4 and SOCKS5.

If you wish to use SOCKS4 however, please ensure that you also have the BrowseGate external DNS system (or another DNS) configured and enabled, as a working DNS capable of resolving Internet addresses is essential for SOCKS4 to work correctly....



Setting a password

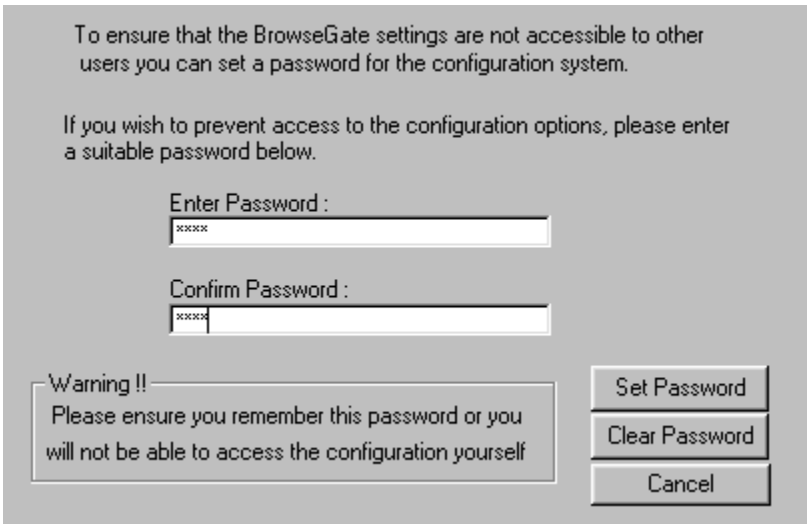
For other Configuration tabs - click on tab shown below...

Aliasing | Downloads | Local Web | Blocking | Rules | Blacklist | Password | Cache | SNTP
Connect | Email | News | Map TCP | Map UDP | SOCKS4/5 | Realplayer | DNS | Ext.proxy | Options

BrowseGate allows you to set an "Administration password" that will ensure that the configuration settings cannot be changed by unauthorized individuals who do not know the password.

If a password is set, it MUST be entered before the system will display the Configuration property sheet.

Click wherever the hand icon appears for more information.



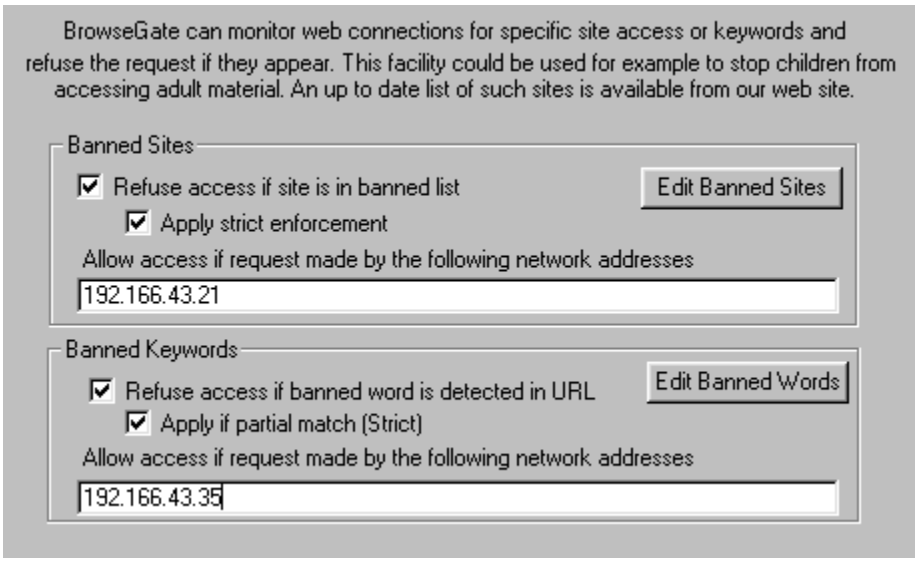
Setting up the use of "Blacklisted" web sites or Words

For other Configuration tabs - click on tab shown below...

Aliasing | Downloads | Local Web | Blocking | Rules | Blacklist | Password | Cache | SNTP
Connect | Email | News | Map TCP | Map UDP | SOCKS4/5 | Realplayer | DNS | Ext.proxy | Options

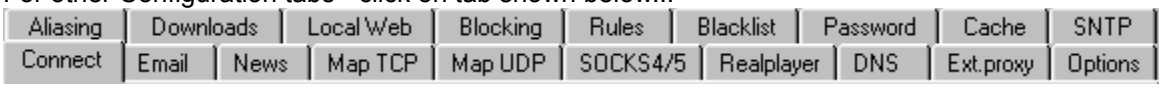
See also: More information on the Blacklist system

Click wherever the hand icon appears for more information.



Setting up Rules to allow connections to specified URL's only !!

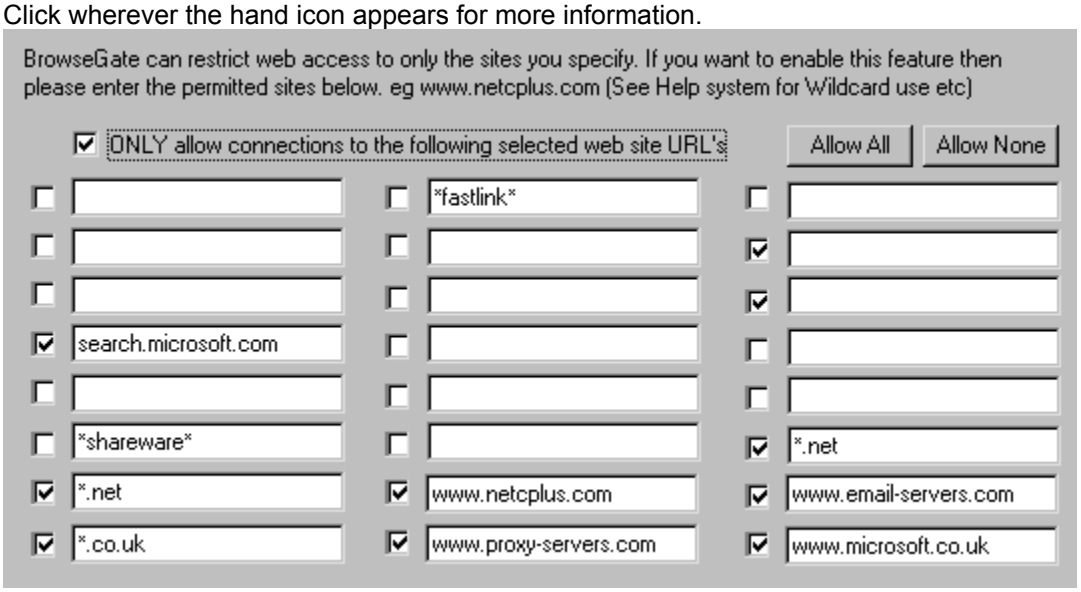
For other Configuration tabs - click on tab shown below...



The "Site Blocking" option allows you to configure BrowseGate to only permit access to sites with URL's that match those you specify.

This puts YOU in total control of the use of the web and the sites that will allow to be visited by any networked user of BrowseGate.

Click wherever the hand icon appears for more information.

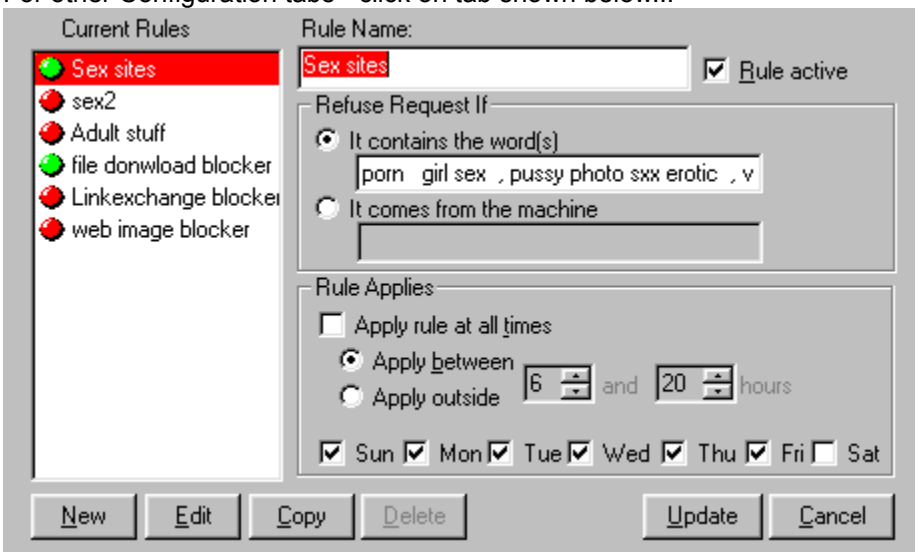


Entries are not position conscious, and may be placed in any of the 24 fields provided.
ALL entries are checked to see if a site is allowed to be accessed.

To provide maximum flexibility, you can also enable or disable any particular entry by simply checking or unchecking the check box to the left of each field.

Setting up BrowseGate to serve a local (intranet) web site automatically

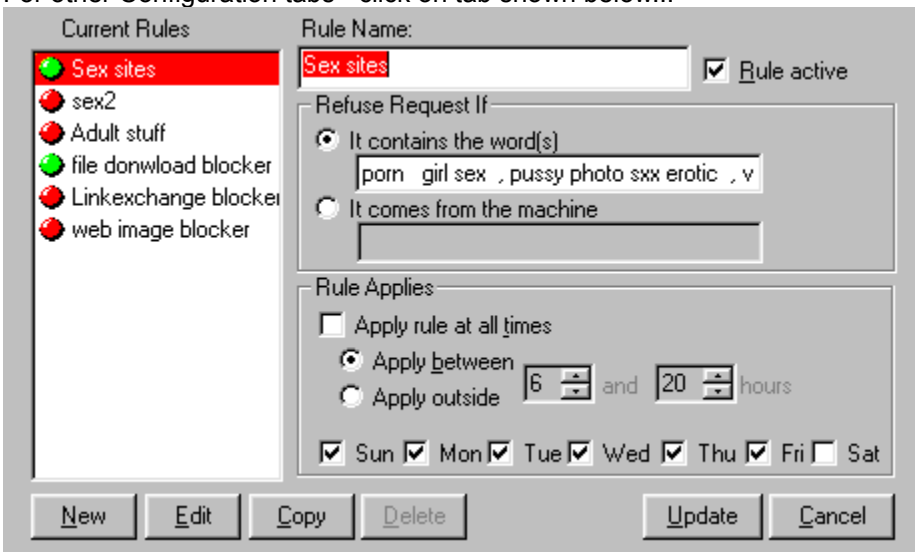
For other Configuration tabs - click on tab shown below...



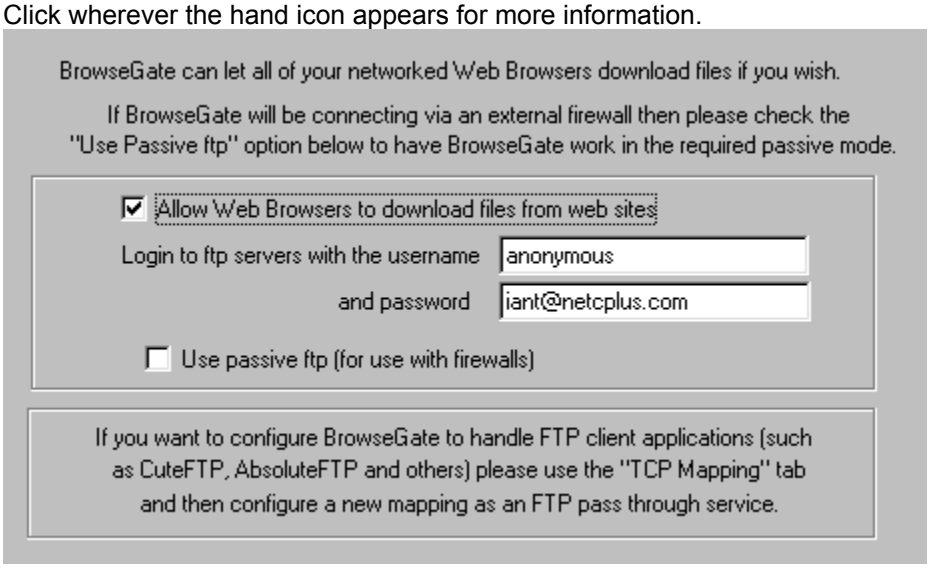
Click wherever the hand icon appears for more information.

FTP settings

For other Configuration tabs - click on tab shown below...



Click wherever the hand icon appears for more information.

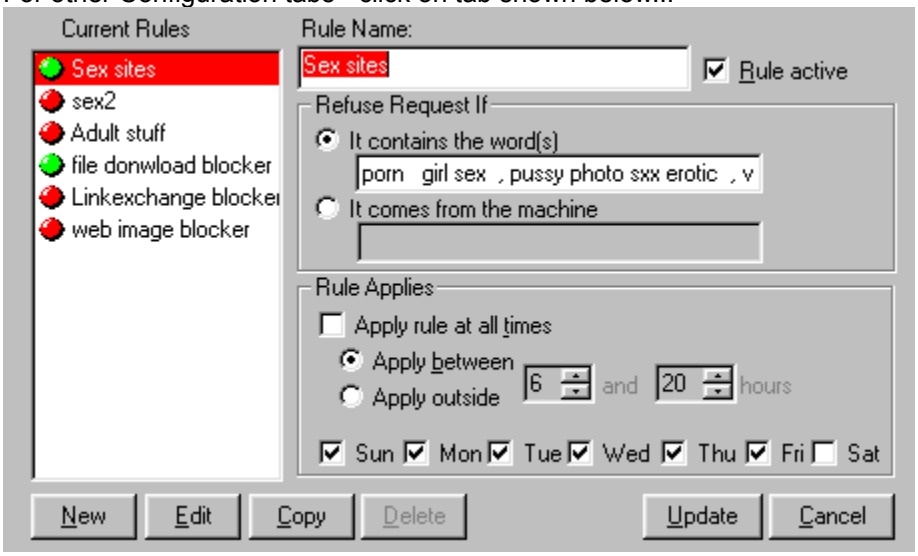


If checked both the log file and the list in the BrowseGate window will show all http data requests rather than the main page requests alone. This includes all graphics images, ASP pages, Java classes etc.

This is useful for checking what a page really has to download.!!!

Configuring BrowseGate to support pop3/smtp email

For other Configuration tabs - click on tab shown below...

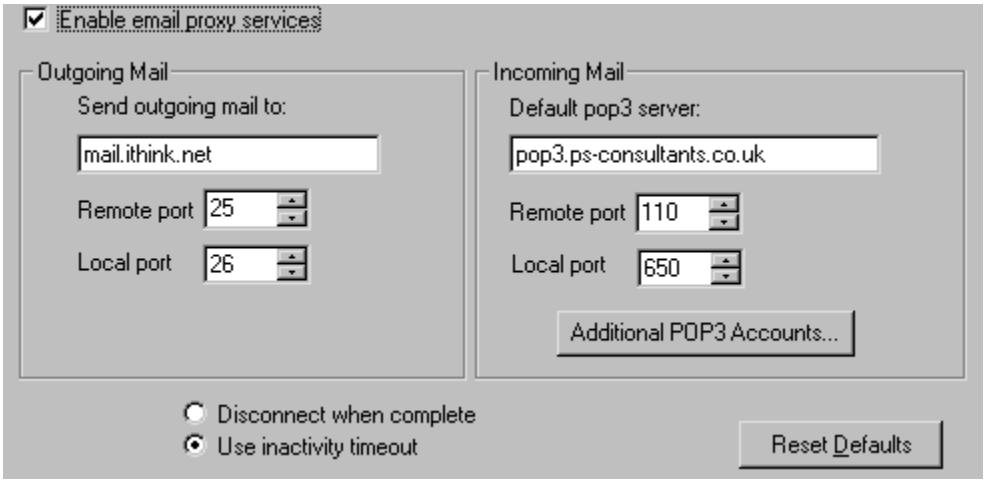


See also: Configuring your email clients
Ports - what you need to know

BrowseGate can provide automatic access for a complete network to allow all PC's to send emails (via SMTP) and collect emails (via POP3) from one or more mailboxes. To configure multiple POP3 mailboxes clcik the "Additional POP3 accounts..." button to dislay the SmartPOP configuration dialog.

To configure this click "Configure" on the main BrowseGate window, and then select the "Email" tab.

Click on a tab to move to that configuration option, or click wherever the hand icon appears for more information.



It is most important that you also ensure that the port settings in each your email client account configurations match those you have selected on this tab.
See - Configuring your email clients and Ports - what you need to know

Configuring a dial up DUN's settings

WARNING - You must ensure that you this PC has windows Dial up networking system installed before you can configure a dial up connection.

Connection to use
Select for the list of available DUN connections the one you want BrowseGate to make use of for it's connections.

Disconnect after...
BrowseGate is designed to automatically disconnect any dial up connection it has started once the period you specify here has expired with no activity having been identified by BrowseGate. You should consider the setting you use here very carefully, as a timeout that is too short will result in BrowseGate making possible too many very short dial up connections. However if the timeout is too long, then your phone charges may be excessive. Typically you will need to monitor this for a while to ascertain the level of use made by your network users. We recommend a setting of 10 or 15 minutes as being a reasonable compromise for most businesses.

Wait for
This setting controls the maximum time that BrowseGate will attempt to make a dial up connection. We recommend 240 seconds as a safe setting.

If busy redial
Sets the number of dial attempts that BrowseGate will make if a connection cannot be made the first time it tries. We recommend the default setting should be left at 3 times.

Disable Inactivity connections
If this option is checked, then BrowseGate will NOT honor the settings in the "Disconnect After" field. This allows you to have a fall back disconnection time set, but to toggle its operation if you have ISDN links or other direct dial up links.

Disconnect on Close Down
If this option is checked, BrowseGate will usually disconnect any dial up connection if you use the EXIT button to close BrowseGate down. The exception to this is if you are also running SmartServer 3 on the same PC as BrowseGate (as a full Internet server system). If this is the case, and SmartServer3 is in the process of a mail collection/delivery, then BrowseGate will naturally enough, ignore this setting.

Show connection status window
If checked, a popup monitor dialog will be displayed to show the dial status.

Trigger SmartServer when on line
Because BrowseGate and our own SmartServer email server can co-operate, and providing that you have installed BrowseGate as a plug-in to SmartServer, then by checking this option SmartServer will automatically check for, fetch and send mail each time BrowseGate starts a dialup connection.

This may be sufficiently often on your network to allow you to not have the server scheduled to send/collect mail at all !!.

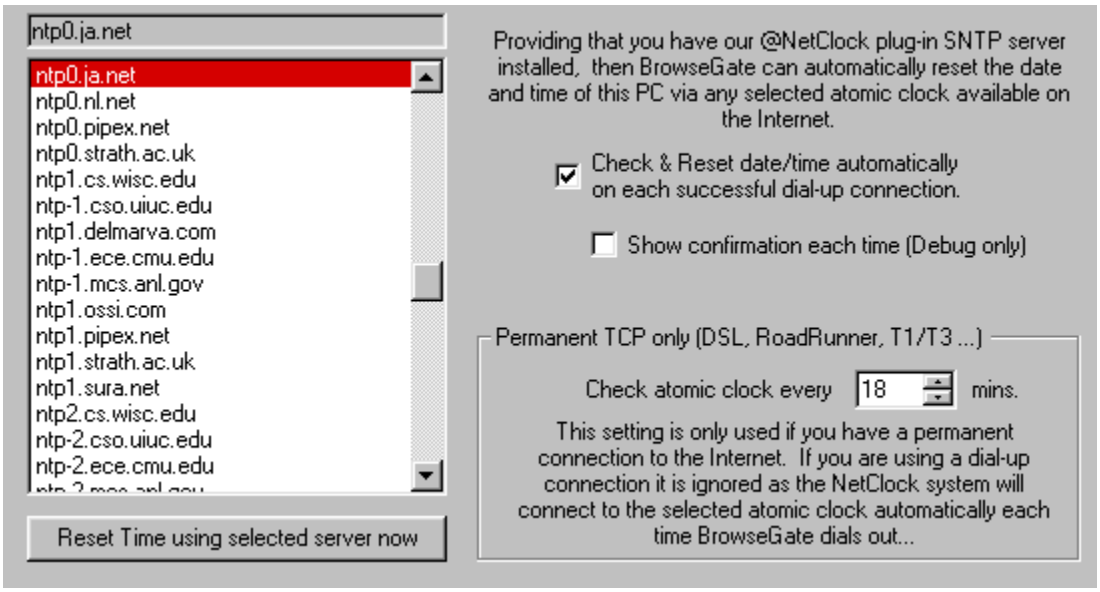
The Configure button will take you to the configuration property sheet, from where you can set all the options you may require to control the way that BrowseGate works.

Configuring @NetClock

See Also: About @NetClock

The following property sheet tab is only enabled if you have our @NetClock Time server plug-in for BrowseGate installed. It allows you to have BrowseGate check and reset the Server PC's clock automatically each time it dials out to connect to the Internet.

The @NetClock plug-in also provides a network Time server that allows all other PC's on your network to set their own clocks to the same time as that on this machine automatically after predefined periods of xx minutes.



Configuring AbsoluteFTP

1. Start AbsoluteFTP
2. Select Menu Options | Global Configuration
3. Select the Advanced Tab
4. Ensure that the "Use Outgoing data connections (PASV)" option is NOT CHECKED
5. Select FireWall Tab
6. Select "USER user@host port" option in the Type frame
   (NB This has a space after Host, please make sure you do NOT
   select the very similar entry with a colon after the word Host)
7. Enter the IP address of the BrowseGate PC in the "Hostname or IP field.
8. Enter the port number you have configured in the TCP Mapping on
   BrowseGate for this FTP connection.

Hereafter you can leave the standard port settings and FTP site names in each preconfigured connection exactly as they were previously (Typically using port 21).

eg: if you have set the firewall access to use port 680, you do not need to change the port number in each FTP connection to 680 as well, although it will still work successfully if you do. The default port setting of 21 will work really fine.....

Configuring BrowseGate remotely

At the time of the release of v 2.70, BrowseGate does NOT yet provide remote access for making changes to it's configuration system.

However this web based facility is under development at present, and will be included in the v3 release.

This will be a FREE upgrade to existing registered users, so you will get this as well providing of course you have registered this version !!!

Configuring CuteFTP

1. Start CuteFTP
2. Select Menu FTP | Settings | Options to display Options dialog.
3. Select the FireWall Tab
4. Select "USER user@site" option in the Type frame
5. Ensure the "Enable FireWall Access" option is checked
6. Enter the PC Name (or IP address) of the BrowseGate PC in the "Host field.
7. Enter the port number you have configured in the TCP Mapping on BrowseGate for this FTP connection in the Port field.
8. Enter a user ID and password if you wish to.

Hereafter you can leave the standard port settings and FTP site names in each preconfigured connection exactly as they were previously (Typically using port 21).

eg: if you have set the firewall access to use port 680, you do not need to change the port number in each FTP connection to 680 as well, although it will still work successfully if you do. The default port setting of 21 will work really fine.....

NB If you happen to encounter partial downloads or uploads. ensure you have UNCHECKED the "Use PASV" option in the properties of each connection in Cute FTP otherwise Cute will try to disconnect too early....

Configuring Eudora

Email setup is the same for all current versions of Eudora.

BrowseGate Setup:

Configure | Email Tab

- Incoming mail tab with remote port set to 110.
- Outgoing mail with remote connection set to port 25.
  Local ports for both set to whatever you wish....

Eudora Setup:

1. From the Eudora Menu bar, under the "Tools" menu, select "Options.."
   This will bring up the "Options" dialog box.

2. In the "Category" menu, choose the "Getting Started" icon.

3. In the "Pop account:" field enter the user name given to you by your POP server,
   your POP server's host name and the BrowseGate machine name.
   Use this form: 'username' # 'host name' @ 'name of BrowseGate machine'.
   For example: billg#microsoft.com@BrowseGateProxy

4. The delimiter character '#' should be that specified in the set-up of the POP3 proxy.

   NB:- It seems Qualcomm have changed this functionality at some time. If you receive
   a password incorrect error, all you need to do is use the following syntax instead. :-
   billg@BrowseGateProxy

5. Still under the "Getting Started" icon, in the "Connection Method:" options, enable "Winsock".

6. In the "Category" menu, choose the "Personal Information" icon.
   Enter the same "POP account:" as above.
   The "Return address:" field should be in the 'user'@'host' format.

7. In the "Category" menu, choose the "Hosts" icon. Once again enter the same "POP account:"
   details. In the "SMTP:" field, enter the machine name or IP address

8. In the "Category" menu, choose the "Checking Mail" icon. Enter the "POP account:"
   details yet again.

9. In the "Category" menu, choose the "Sending Mail" icon. Enter the "Return Address:"
   as above. In the "SMTP server:" field enter 'the machine name or IP address

The rest of the Eudora set up does not relate to BrowseGate.

Configuring FTP clients to use BrowseGate

BrowseGate provides built-in support for FTP client packages to be able to connect to remote FTP sites on the Internet via the proxy. This is configured automatically in the BrowseGate TCP Mapping tab, providing that you ensure that you check the "FTP connection" option.

BrowseGate provides support for the **user@password FTP** for firewall connections. This is available in most well known Windows (and other platform) FTP client programs.

We have tried BrowseGate with the three most popular FTP clients (CuteFTP (32), AbsoluteFTP, FTP EXPLORER and WS_FTP95) and detailed instructions on setting up these packages for use with BrowseGate is available from the pages below :-

CuteFTP (v 1.8)
AbsoluteFTP (v 1 5)
WS-FTP (v 95LE)
FTP Explorer

If your FTP client supports SOCKS4 or SOCKS5 (many don't) you can also select either one of these, and as long as you have the BrowseGate SOCKS support enabled, this will work transparently.

Configuring Forte Free Agent

BrowseGate Setup:

Configure | Email Tab

- Set remote port set to 110.
- Set Local port to whatever you wish....

Mapped link to news-group server (NNTP), accepting connections on whatever local port you have set in BrowseGate.

Mapped link to mail-forwarding server (SMTP), accepting connections on whatever local port you have set in the Outgoing Email setup of BrowseGate.

The 'Free Agent Setup' dialog box will be presented when Agent is loaded, or from the menu bar, under the 'Options' menu, select 'Preferences...' and select the 'System Profile' tab.

In the 'News Server:' field enter the machine name or IP address

In the 'Email Server:' field also enter the machine name or IP address

The rest of the Agent set up does not relate to BrowseGate.

Configuring MS Exchange

BrowseGate Setup:

Configure | Email Tab

- Incoming mail tab with remote port set to 110.
- Outgoing mail with remote connection set to port 25.
  Local ports for both set to whatever you wish....

Exchange setup:

1. From the menu bar, under the "Tools" menu, select "Services..." to bring up the "Services" dialog box.

2. If there is no 'Internet Mail' profile then create one.

3. Highlight the 'Internet Mail' profile and hit the 'Properties' button to bring up the "Internet Mail" dialog box.

4. On the "General" page, in the "Internet Mail server:" field, enter the machine name or IP address

5. In the "Account name:" field, enter your POP user name and your POP server's host name, in the following fashion: 'user name' # 'host name'
   For example: billg#microsoft.com

6. The delimiter character '#' should be that specified in the set-up of the POP3 proxy.

7. On the "Connection" page, enable the 'Connect using the network' option.

8. The rest of the MS Exchange setup does not relate to BrowseGate.

Configuring Microsoft Outlook Express

BrowseGate Setup:

Configure | Email Tab

- Incoming mail tab with remote port set to 110.
- Outgoing mail with remote connection set to port 25.
  Local ports for both set to whatever you wish....

Outlook Express Setup:

1. Start Outlook Express
2. Select the menu option Tools | Accounts
3. Now for **each email account** you have configured, do the following :-

3a. Select an email account.
3b. Double click on it or click the Properties button.
3c. Select the Connection tab.
3d. Ensure you have the "Connect using my local area network (LAN)" selected
3e. Now select the Servers tab.
3f. Enter the IP address of the PC that is running your BrowseGate server in both the fields in the Server information panel. That is the Outgoing Mail (SMTP) and Incoming Mail (POP3) fields.
3g. Ensure you have selected POP3 as the mail server type.
3h. Ensure that the Account name and password in the Incoming Mail Server panel are correct for the server you are going to collect mail from.
3i. If authentication is required for outgoing mail, check the option at the bottom of the tab.

4. Select the Advanced Tab.
5. Check that the entries in the Server port numbers panel are the same as the **Local Port settings** in the BrowseGate email configuration tab. (The defaults are 25 for SMTP and 110 for POP3, and these are usually OK on most networks - but please check with your network administrator if you are unsure)

6. Click the OK button to save any changes made
7. Make sure you repeat the steps 3a -> 5 for each email account you have in Outlook.
8. When you have configured each and every account, close the account dialog.

Outlook express should now connect via BrowseGate totally automatically.!!!

WARNING Because Microsoft are known to be constantly revising Outlook and Outlook Express, your email account dialogs may well vary in content and name from those described above. If you find this to be the case you need to find the same entries on your particular version and then follow the instructions above.... or contact Microsoft for details of how to configure your version of Outlook to work through a networked proxy server. Please do not send support questions to us on this as we are not able to provide support on Microsoft products directly - for obvious reasons !

Configuring Pegasus mail

BrowseGate Setup:

Configure | Email Tab

- Incoming mail tab with remote port set to 110.
- Outgoing mail with remote connection set to port 25.
  Local ports for both set to whatever you wish....

Pegasus Setup:

1. From the menu bar, under the "File" menu, select "Network configuration..." to bring up the "Configuration for Built-in Internet Mailer" dialog box.

2. In the "POP3 host" entry, enter the machine name or IP address of the BrowseGate PC..

3. In the "User name" field, enter your POP server user name and your POP server's host name, in the following fashion: 'user name' # 'host name'. For example: billg#microsoft.com.

4. The delimiter character '#' should be that specified in the set-up of the POP3 proxy.

5. In the "SMTP host" entry, enter the machine name or IP address of the BrowseGate PC.

6. Hit 'Advanced configuration options...' to bring up the "Advanced Configuration for Built-in Internet Mailer" dialog box.

7. In the "Incoming (POP3) mail" area there is a "Connect to POP3 server on TCP port" entry. In this field, enter the port number that the POP3 proxy in BrowseGate is configured to accept connections on.

The rest of the Pegasus set up does not relate to BrowseGate.

Configuring SOCKS applications to use BrowseGate

We have provided configuration details for the following common SOCKS applications

mIRC - Chat system
ICQ - Communications system
Absolute FTP
Yahoo Messenger
Microsoft Internet Explorer 4
Microsoft Internet Explorer 5

NB The current releases of CuteFTP or WS_FTP do not provide SOCKS support

WARNING

If for whatever reason you decide to use SOCKS 4 as the ONLY protocol between your web browsers and BrowseGate, this will disable the majority of the powerful Web (HTTP) control features built into BrowseGate. The Blacklists and Rules will not be applied to page requests, and the web access statistics will be empty. This is because SOCKS is by definition more of an "open door" protocol which means that it has little concept of what types of data or requests are being processed, but simply passes data back and forth totally transparently, rather like a pair of wide open double doors.!!!!

We recommend that unless you have a very good reason for needing to do so, you do NOT use SOCKS alone for web browser connections thru BrowseGate . The standard HTTP and HTTPS (Secure) protocols work very well and you will still be able to have BrowseGate provide the full power of Blacklisting, Rules and it will log all web access performed by any machine on your network.

Configuring Yahoo Messenger to use BrowseGate

BrowseGate full supports both the HTTP only and (Recommended) the HTTP plus SOCKS4/5 connection methods available with Yahoo Messenger v3.0 and later.

It is very easy to get YM to connect via BrowseGate by following the instructions below.

1. Run YM.
2. Select Edit | Preferences
3. select the "Connection" tab on the property sheet that appears

IF YOU WANT TO USE HTTP + SOCKS:

4. Check the "Use proxies" option
5. Check the "Enable HTTP proxy" option.
6. In the Server name field enter either the IP address of the PC on which BrowseGate is installed.
7. Set the server port number to whatever local port BrowseGate uses for HTTP requests across the network (typically this will be port 80)
8. Check the "Enable SOCKS proxy".
9. Repeat step 6 in the Server name field fo rthe SOCKS configuration.
10. Set the server port number to whatever local port BrowseGate uses for SOCKS requests across the network (typically this will be port 1080).
11. Check the SOCKS version you wish to use. We recommend you use SOCKS 5, but you must have the BrowseGate DNS configured for this to work correctly.
12. Click the OK BUTTON.

IF YOU WANT TO USE HTTP ALONE:

4. Check the "Use proxies" option
5. Check the "Enable HTTP proxy" option.
6. In the Server name field enter either the IP address of the PC on which BrowseGate is installed.
7. Set the server port number to whatever local port BrowseGate uses for HTTP requests across the network (typically this will be port 80)
8. UNCHECK the "Enable SOCKS proxy".
12. Click the OK BUTTON.

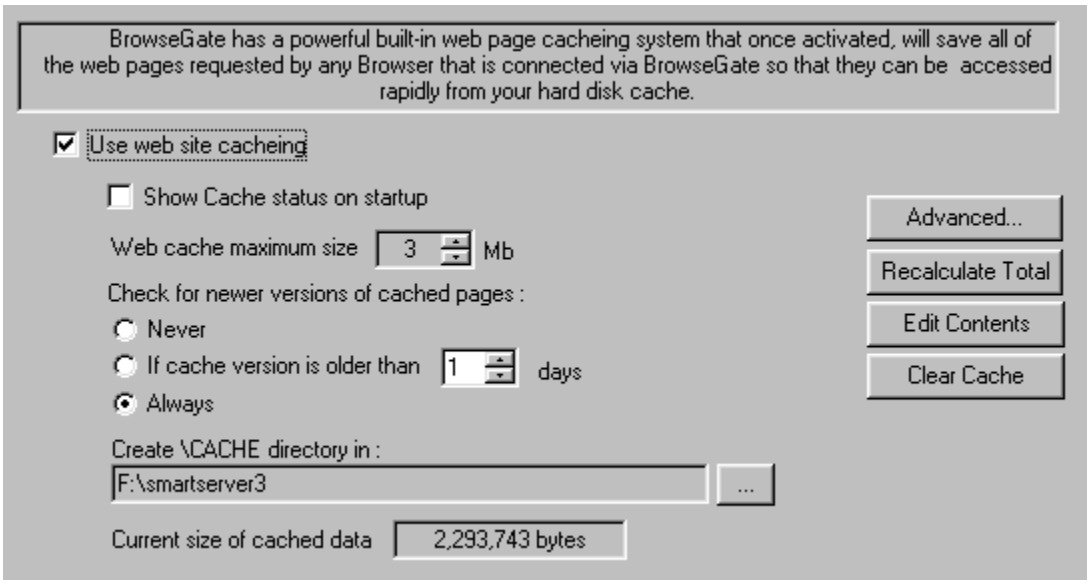
Now test the connection.

If you still have problems, check the Yahoo messenger web site Help system for firewalls and try each of the options listed there.

Configuring the Cache

See Also: Setting the cache size
Editing the cache contents

We have tried to make configuring the BrowseGate cache as easy as possible. We let you specify the Drive and directory the cache sub-system will be stored in, and you can also specify the maximum amount of disk space that it can use, and how often it will check each requested item for currency.



NB For obvious reasons, We STRONGLY recommend that you always assign a cache drive/path that is on the same PC that BrowseGate is running on. Although the Window's drive selection dialog will of course allow you to go to the Network Neighbourhood, and therefore select any accessible remote Drive/Path, BrowseGate will NOT allow you to select a networked drive from here as the location for the cache. For example, if you were to select a network server with a path such as :-

\\ServerOne\webcache

BrowseGate will not accept your selection. But to handle the situation where this may really be necessary to suit your own network topography, you can map a networked drive to any free drive letter on the BrowseGate PC and then select that drive. This means you could get around this apparent "restriction" by mapping a networked drive of say

\\ServerOne\webcache

to say drive x:\ on the BrowseGate PC. However we strongly recommend that you do

not do this as you will almost certainly lose any speed benefits gained from the use of the cache system due to BrowseGate having to first retrieve the required web site data across your network, and then it would still have to feed it back again to the requesting browser - yet again across the network. Not a very effective idea really, even with 100Mb networks !!!!

BrowseGate also checks the drive/path you select and will not allow you to select a CDROM or removable disk of any type. It will also refuse to accept a RAM drive (memory drive) if selected.

Configuring your mail clients

See also : Configuring Outlook Express
Configuring Eudora
Configuring MS Exchange
Configuring Pegasus mail
Configuring Netscape Messenger
Using the TCP Mapping feature for email connections

NB IMPORTANT - in all the example setup details above, we have assumed that the network name of PC on which you have installed the BrowseGate proxy server is named "browsegateproxy". Simply replace this with your own PC's name as appropriate.

Unfortunately, email clients are all very different in the way that you configure them to send and receive mail, so we have given detailed instructions on setting up the free Microsoft Outlook Express that comes with Internet Explorer 4, and our own SmartMail email client. Most others will be similar, although you will have to find the relevant configuration options in other packages for yourself.

Basically, the process is the same for all, and the concepts you need to understand are described briefly below :

When a proxy server is going to handle email access to the "outside" world, you need to change the address of the pop3 and smtp hosts that your email client will try to connect to from the external mail host name to the BrowseGate PC. This can be done using either the IP address (such as 192.168.40.123) of the PC on which BrowseGate is installed, or you can usually make use of that PC's Name (such as DELLPC200).

You must also ensure that the local port number you have configured in BrowseGate is also set to be the same in your email client. Most email clients allow this to be setup for each email account that can be configured. If you have an email client that has the ability to collect mail from multiple accounts, you will need to ensure that the Local port used for each account exactly matches the local port configured in BrowseGate for that particular mailbox !!!!

Configuring your news clients

See also : Configuring Outlook Express to access news
Configuring Forte Free Agent
Using the TCP Mapping feature for News

NB IMPORTANT - in all the example setup details above, we have assumed that the network name of PC on which you have installed the BrowseGate proxy server is named "browsegateproxy". Simply replace this with your own PC's name as appropriate.

Unfortunately, newsreader are all very different in the way that you configure them to access the Internet NNTP news system so we have given details instructions on setting up the newsreader in the free Microsoft Outlook Express that comes with Internet Explorer 4. Most others will be similar, although you will have to find the relevant configuration options in other packages for yourself.

Basically, the process is the same for all, and the concepts you need to understand are described briefly below :

When a proxy server is going to handle news access you need to change the address of the news server that your news client will try to connect to from the external news server name to the BrowseGate PC. This can be done using either the IP address (such as 192.168.40.123) of the PC on which BrowseGate is installed, or you can usually make use of that PC's Name (such as DELLPC200).

You must also ensure that the local port number you have configured on the BrowseGate "News Service" tab is also set to be the same in your newsreader. You will need to ensure that the Local port used for news access exactly matches the local port configured in BrowseGate for News Service !!!!

Microsoft Internet Explorer 3.xx

1. Start MSIE 3.xx
2. Select the menu option "View | Options"
3. Select the Connection tab (2nd from left)
4. Uncheck the top option labeled "Connect to the Internet as needed".
5. Check the option labeled "Connect through a proxy server"
6. Click the "Settings" buttons to the right of the option.
7. Enter into the "HTTP" field the ip address of the PC that BrowseGate is installed on.
8. Enter the port number in the field alongside that is to be used for communication between this web browser and BrowseGate.
   (This may be the default HTTP port in BrowseGate or via a configured "Extra Service")
9. Repeat steps 7 and 8 for the FTP fields.
10. Repeat steps 7 and 8 for the SECURE fields if you wish to access https (secure) sites.
11. All other fields are ignored by BrowseGate, although you may have other servers supporting these.
12. Press OK to save your changes.

Microsoft Internet Explorer 4.xx

1. Start MSIE 4.xx
2. Select the menu option "View | Internet Options"
3. Select the Connection tab (4th from left)
4. Uncheck the option labeled "Connect to the Internet using a modem"
   in the "Connection" group frame.
5. Check the option labeled "Connect to the Internet using a local area network"
6. In the "Proxy Server" frame directly below, check the two options marked
   "Access the Internet using a proxy server" and
   "Bypass proxy server for local (Intranet) addresses".
7. Click the "Advanced" button to the right of these options.
8. Enter into the "HTTP" field the ip address of the PC that BrowseGate is installed on.
9. Enter the port number in the field alongside that is to be used for
   communication between this web browser and BrowseGate.
   (This may be the default HTTP port in BrowseGate or via a configured "Extra Service")
10. Repeat steps 7 and 8 for the FTP fields.
11. Repeat steps 7 and 8 for the SECURE fields if you wish to access https (secure) sites.
12. We recommend that you enter the following ip address into the Exceptions
    field at the bottom of the property sheet "127.0.0.1" (Do not enter the quote marks)
13. All other fields are ignored by BrowseGate, although you may have
    other servers supporting these.
14. Click on the OK buttons to close and save the configuration system.

Microsoft Internet Explorer 5.xx

1. Start MSIE 5.xx
2. Select the menu option "Tools | Internet Options"
3. Select the Connection tab (4th from left)
4. Check the option labeled "Never dial a connection"
   in the "Dial-up settings" group frame.
5. In the "LAN settings" frame directly below, click the button marked
   "LAN Settings"
7. Unless you have centralized network configuration for your browsers,
   ensure you have both entries in the "Automatic configuration" frame
   UNCHECKED.
8. Check the "use a proxy server" option in the "Proxy server" frame
9. Click on the Advanced button
10. Enter the IP address (or machine name) of the BrowseGate Server PC
    into the "proxy address to use" field for the HTTP field.
11. Enter the port number in the field alongside that is to be used for
    communication between this web browser and BrowseGate.
    (This may be the default HTTP port in BrowseGate or via a configured "Extra Service")
12. Repeat steps 10 and 11 for the SECURE fields if you wish to access https (secure) sites.
13. Repeat steps 10 and 11 for the FTP fields.
14. Repeat steps 10 and 11 for the Socks fields (If you want to use SOCKS).

12. We recommend that you enter the following ip address into the Exceptions
    field at the bottom of the property sheet "127.0.0.1" (Do not enter the quote marks)
13. The Gopher fields are ignored by BrowseGate, although you may of course have
    other servers that do support this protocol.
14. Click on the OK buttons (all three of them) to close and save the various configuration dialogs.

Netscape Navigator 4.xx

1. Start Navigator
2. Select the menu option "Edit | Preferences"
3. Click the "+" sign in front of the "Advanced" entry in the list box to open up the tree.
4. Click on the "Proxies" entry that is now visible.
5. Check the option labeled "Manual proxy configuration"
5. This will uncheck the other two unwanted options automatically.
6. Click the "View" button to the right of the option.
7. Enter into the "HTTP" field the ip address of the PC that BrowseGate is installed on.
8. Enter the port number in the field alongside that is to be used for communication between this web browser and BrowseGate. (This may be the default HTTP port in BrowseGate or via a configured "Extra Service")
9. Repeat steps 7 and 8 for the FTP fields.
10. Repeat steps 7 and 8 for the SECURE fields if you wish to access https (secure) sites.
11. All other fields are ignored by BrowseGate, although you may have other servers supporting these.
12. Press OK to save your changes.

CACHE - How to set it up

See Also: Configuring the Cache
When should or shouldn't I use web site cacheing
The Cache status window
Editing the cache contents

About the BrowseGate Cache System

What is a cache ?
A cache is simply a technical term for the process whereby whenever a web site is visited, each and every web page (HTM, HTML etc) that is requested by the browsers on your network, plus all the associated image files (GIF, JPG etc) are not only given to the web browser that asked for them, but are also stored in a special subdirectory on your local hard disk. This means that the next time you want to visit that web site, BrowseGate can provide the pages and images directly from the hard disk, making the process faster and more effective.

BrowseGate provides a highly efficient, optimized and configurable web site caching system that is capable of storing on your local hard disk ALL the web pages and related files that are requested by any web browser that is connected through it.

How does a cache work ?
Providing you have chosen to enable the BrowseGate cache system, then every time a request is received from any web browser for an HTML page, BrowseGate first checks to see if it already has that particular page available in it's own cached data.

If a Cached page is found
BrowseGate checks with the Internet site concerned to ensure that the locally stored page is still up to date, and if so, it simply sends that copy back to the requesting browser, which means the user gets the page faster, and the amount of Internet traffic required is minimized.

What if the page is out of date ?
BrowseGate can be configured to check with the server to see if the page is out of date either

a) all the time,
b) only if the page is older than xx days, or
c) never.

If a check is due, and the page is found to be out of date, it will automatically fetch the latest version from the real web site, give this to the requesting browser, and then update the copy in the cache with this newer version.

What if a cached version of a page is not found
BrowseGate simply fetches the requested page from the Internet web site itself, and after passing it to the web browser that asked for it, stores a copy in the local cache ready for the next time it may be requested.

This process is fully automatic, and once you have some web site data stored in your cache all you will hopefully notice should be considerably faster access to these web pages.

What happens when the cache gets too full ?

The BrowseGate cache has been optimized to operate what is called a high/low water mark system. All this means is that when the cache reaches the high water mark (typically around 95% of the maximum specified cache disk space), it will automatically remove the oldest data in the cache until the used cache disk space is reduced back to the low water mark (typically around 30% of the maximum specified cache disk space).

This involves a complex algorithm so that BrowseGate can decide which files in the cache are the oldest ones, and it then removes these files one by one until the cache's low water mark is reached. This means that many of the newer web site pages s that are already cached will still remain there, but some of the images or pages may then need to be fetched from the Internet again. However, this strategy enables BrowseGate to still provide a faster response than would be the case if the entire site had to be downloaded again.

All of this complex processing by BrowseGate is performed as a background task, and the only indication you will have of it happening is if you are sitting at the PC on which BrowseGate is running, when you will typically notice some pretty frantic disk activity as files are removed, and the Cache level indicator (or percentage display) on the main BrowseGate window suddenly dropping to around 15-20% of the overall cache size.

NB For obvious reasons we strongly recommend that you make sure you have the "Delete to Windows Recycle Bin" option TURNED OFF on the drive that is being used for BrowseGate's web page cache as otherwise your hard disk could fill up quite quickly with old cached web pages that you cannot use for any good purpose !!!!

The BrowseGate Domain Name Server (DNS)

See Also: An Overview of Domain Name Servers
Identifying the local machine's network IP address
Setting up the TCP networking in Windows 95/98 to use the BrowseGate DNS
What is the Internal DNS ?
What is the External DNS ?

BrowseGate offers your Windows 95/98 network a full featured, built-in DNS server that handles both internal resolution and external (DNS forwarding) requests because most (W95/98) networks do not have a DNS built-in such as the one provided as a part of the NT4 operating system.

A DNS is an essential item on your network if you wish to use SOCKS4, and very useful for many other intranet --> Internet communications protocols.

DNS stands for "Domain Name Server", which is just a fancy name for a bit of rather clever software that converts requests for internet (and intranet/network) resources such as web pages and email hosts into the actual TCP/IP addresses that are ESSENTIAL if any internet software is to be able to work.

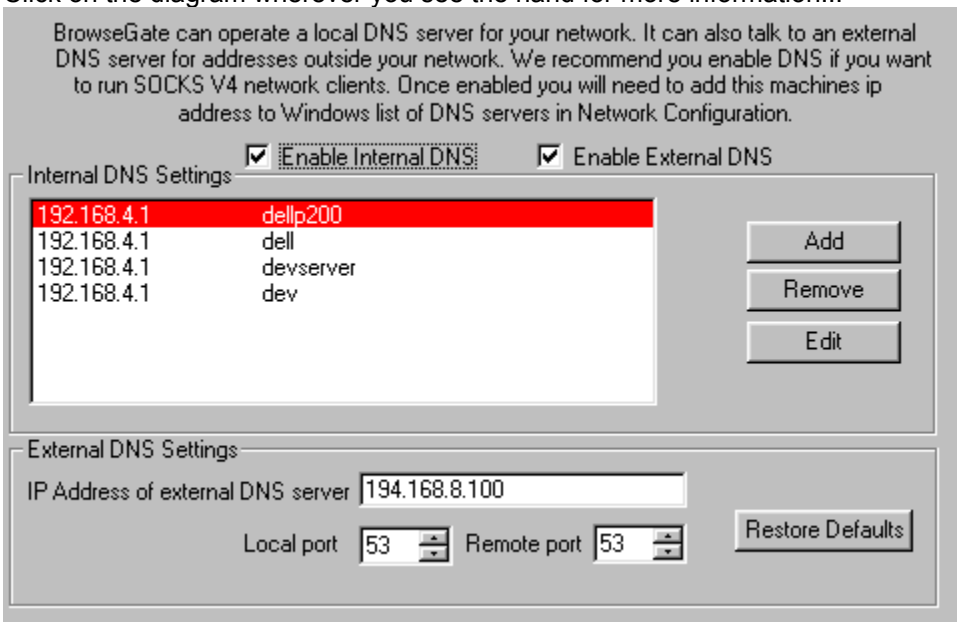
What this means is that when you type into your web browser a URL of say

http://www.microsoft.com

this is really just a "human readable" and meaningful address that HAS TO BE CONVERTED somehow into the correct Internet TCP/IP address such as 192.164.203.126 or whatever the actual physical internet address of that particular web site really is. (This is usually known as "Resolving" the address)

That is exactly what a DNS does, and BrowseGate provides you with your very own DNS !!!

Click on the diagram wherever you see the hand for more information...



BrowseGate actually has two different DNS systems built-in to it, an Internal DNS and an External DNS (DNS forwarding) hence the 2 check boxes shown.

General information
We strongly recommend that you do NOT change the PORT number, but if you do for any reason you

should restart BrowseGate for this to take effect. You can however toggle the DNS On/Off setting without any need to restart BrowseGate.

For the external DNS setting, enter in the field the IP address of your MAIN external/internet based DNS server which will have been given to you by your ISP, but you can also use any other DNS such as the DNS shown above.... (194.159.0.5)

To take full advantage of the BrowseGate DNS service, you also need to edit the Windows "start menu | settings | Networks | TCP/IP - Dial up adaptor" property sheet and insert the IP ADDRESS of your BrowseGate PC as the FIRST (or only if you prefer) entry in the list of available DNS's. This is so that it will force all your applications to request a DNS lookup via BrowseGate.

You can obtain this IP address quickly and easily from the information shown at the top of the main BrowseGate window, or by selecting the "View | Select local IP Address" menu option.

DNS - An Overview

See Also: More information on setting up TCP/IP addresses

The following are the main reasons why you may want to set up DNS on your LAN

1. You want to use SOCKS to access FTP or Gopher or HTTPS URLs in a browser.
2. You want to run some other SOCKS capable software
3. You have a large LAN and you want name resolution for the machines on your LAN.

None of the proxies in BrowseGate other than SOCKS require a DNS to be working on your LAN.

One of the oddities of the SOCKS protocol is that a request for a connection is made in the form of a request for connection to an IP number. What this means is that a SOCKS client must be able to 'look up' addresses in order to supply this IP number to the SOCKS server.

This is the reason we added the built-in DNS server to BrowseGate. If however you already have DNS on your network, and it has the ability to resolve all the names you wish to connect to, then you do not need to run the BrowseGate DNS server in order to use SOCKS client applications. You should not enable the BrowseGate DNS server if you are already running a DNS server on the same machine - this is quite likely to mess up both DNS servers.

You WILL need to enable the DNS on your LAN however.

If you are using the BrowseGate DNS server, you should set the DNS Server settings for your LAN adapters (on all machines EXCEPT possibly the BrowseGate PC) to be the IP number of the BrowseGate PC.

There are a lot of very good resources on the Internet, which will help you to set this all up.
In particular, the following page will most likely be able to help you if you run into difficulties:

http://www.windows95.com/connect/

Remember that IP numbers have to be unique for machines on the same network? Well, you can think of the entire Internet as a single network. But your LAN is probably not on the same network, even if one of the machines (i.e. the BrowseGate PC) is connected to the Internet. It is not so much a computer as a computer interface being visible on the Internet, and it does not matter at all whether this is a LAN card or a modem's serial port. The Internet can see any connected interface, but no further.

This means that you can choose any number you like for the machines on your LAN. However it isn't a good idea to choose just any old thing, because you have to think of the situation the BrowseGate PC is in.

When connected to the Internet the BrowseGate PC can see the entire Internet, and it can of course also see every PC on your LAN. So, you don't want to confuse it by giving your LAN the same addresses that the BrowseGate machine can see on the Internet.

Fortunately some smart person already thought of this one, and so a whole heap of addresses have been kept aside for just this purpose. These addresses are called "private addresses" and are not meant to be available anywhere on the Internet. Therefore, by using them on your LAN, there won't ever be any confusion for the BrowseGate PC.

Click here for more information on setting up TCP/IP addresses

Enter the IP ADDRESS of the main (and secondary if you have one) external DNS you want BrowseGate to use to resolve internet access requests from your networked PC's.

These number will usually have been provided to you by your ISP.

These are the ports to be used for your networked to make DNS request to BrowseGate (internal) and for BrowseGate to connect with the external DNS server as required when it finds it needs to resolve external addresses. (external)

SOCKS - How to use the SOCKS support

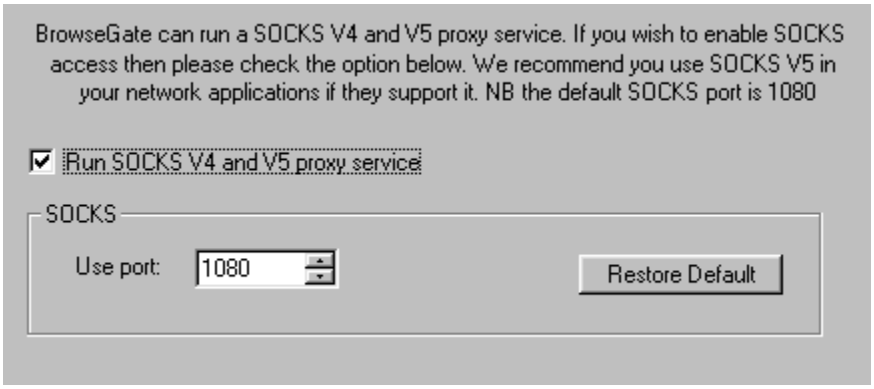
For other Configuration tabs - click on tab shown below...

Aliasing | Downloads | Local Web | Blocking | Rules | Blacklist | Password | Cache | SNTP
Connect | Email | News | Map TCP | Map UDP | SOCKS4/5 | Realplayer | DNS | Ext.proxy | Options

See Also: BrowseGate Domain Name Server

BrowseGate provides full support for applications that require either SOCKS 4 and/or SOCKS 5 protocols.

Click the Configure button, or use the Options | Configure menu option and then select the SOCKS tab, which contains the setup panel shown below...



If you do enable SOCKS support, BrowseGate will automatically enable support for both SOCKS4 and SOCKS5.

Unless you have other TCP/IP applications using port 1080, we strongly recommend that you leave the port setting on this default value.

For applications such as IE4/5, Netscape Navigator and any others that only provide support for SOCKS4 but not SOCKS5, it is **essential** that you also activate the BrowseGate Domain Name Server, as SOCKS 4 will not work because it cannot resolve IP addresses without the built-in DNS support.

Hint:
Although both Microsoft IE4 and Netscape Navigator will happily perform web browsing via a SOCKS proxy connection, we strongly recommend that you should use the HTTP and HTTPS (Secure) protocols rather than SOCKS for normal web browsing. This is because the design of the SOCKS protocol does not allow BrowseGate to perform either its Rules checking or Blacklist checking, and the log files will not contain any web browsing information....

If you wish to take advantage of these control features of BrowseGate, you should NOT configure your web browsers to use the SOCKS protocol alone, although you can have both HTTP/HTTPS and SOCKS configured at the same time which will work fine as the web browsing requests will always be routed via the HTTP protocols first, allowing BrowseGate to provide you with all of the built in control and reporting features....

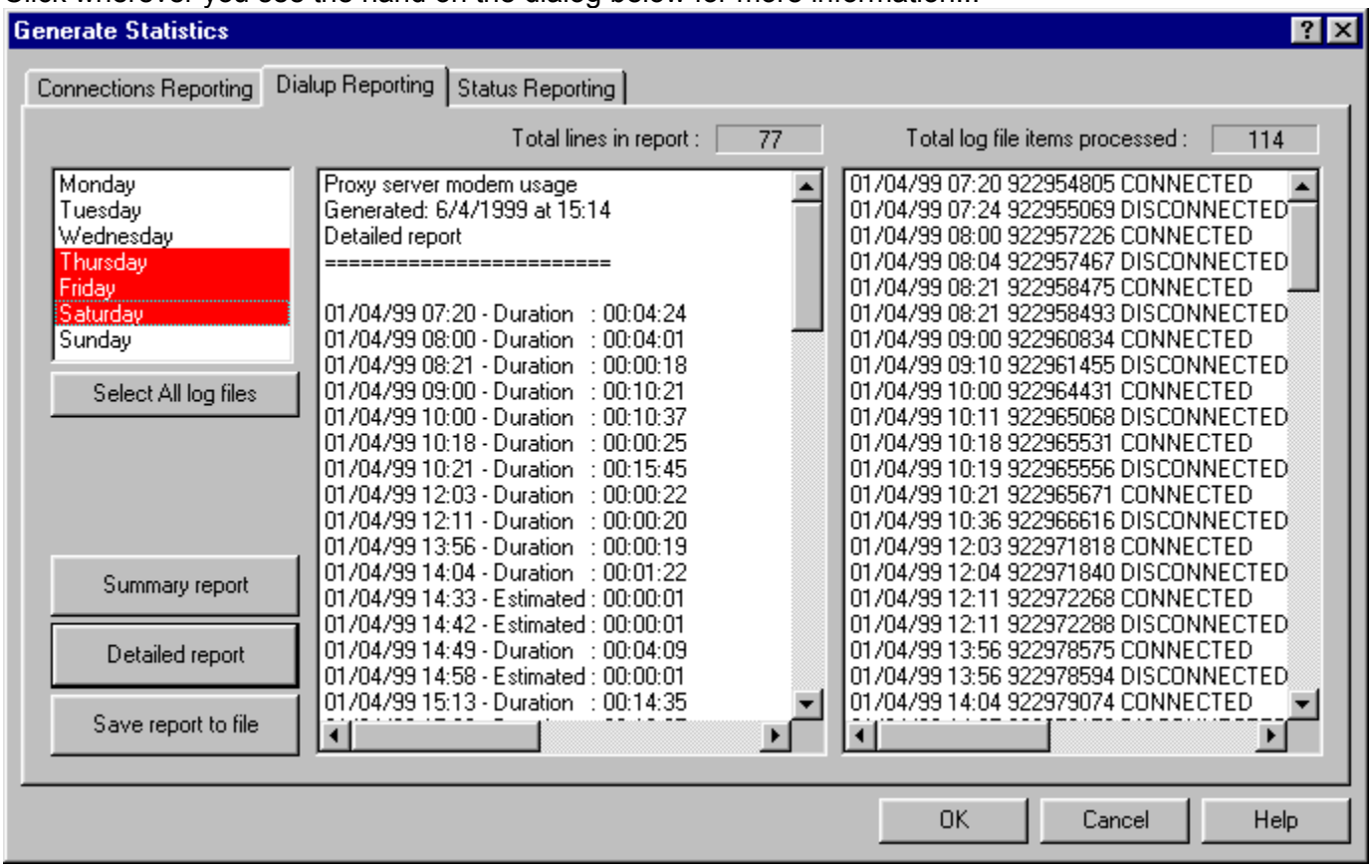
Most SOCKS applications use port 1080, but you may change this
if you wish, providing you ensure that all applications that require
SOCKS support can also use a different port number (some cannot)

Generating dial-up statistics

BrowseGate provides a powerful modem usage reporting facility that allows you to monitor the amount of time that BrowseGate has been connected to the Internet over the last 7 day period.

The statistics option takes advantage of the detailed activity log files that are automatically generated for each of the 7 days of the week, and scans these to produce summary information on the dial-up activity for any/all of the last 7 days

Click wherever you see the hand on the dialog below for more information...



In our example above, a detailed report has been generated for the three available log files, which shows the time and duration of each modem connection that BrowseGate has made.

NB The BrowseGate logging system ONLY logs connections and disconnections that are made by BrowseGate itself. If you start or stop a dial-up connection manually fro the "Dial Up Networking" folder or a desktop shortcut, it will, quite reasonably, NOT be logged by BrowseGate...

ICQ is not quite so easy to configure for use with BrowseGate.
But is still quite straightforward.....
The following instructions apply to v99a(beta)

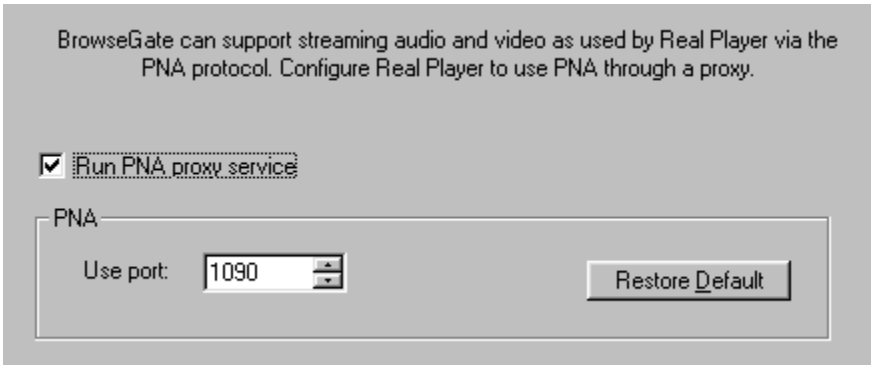
1. Start ICQ
2. Click the ICQ button.
3. Select Preferences
4. Select "Connection" tab on the property sheet
5. Select the "Im using a permanent internet connection (LAN)" option.
6. Then select the "I am behind a firewall or proxy" option.
7. You may need to try the "Always use Real IP option checked and unchecked.
   We suggest you start with it unchecked.
8. Ensure the "Use 16 Bit dialer" option is unchecked.
9. Click the "Firewall Settings" button.
10. On the popup dialog, ensure you select the "I am using a SOCKS5
    proxy server" option
11. Set the "Firewall sessions time out after" option as you require, but ensure
    you make the delay long enough.... We suggest 120 seconds as a minimum.
12. Click the Next button
13. In the "SOCKS5 Host" field the machine name (or IP address)
    of the PC on which BrowseGate is running.
14. Ensure "SOCKS5 Port" is set to 1080.
15. Do NOT check the "Socks External Host IP option or enter anything in that field
16. We recommend you check the "Resolve IP" option...
17. DO NOT check the "use RFC1929..." option.
17. Click Next button
18. Try clicking the "Check my FIREWALL / Proxy Setting" button.
19. After a short while you should get a "Success..." message

Setting up BrowseGate to support Real Player (& other streaming Audio/Video packages)

For other Configuration tabs - click on tab shown below...

Address Aliases | Downloads | Local Server | Site Blocking | Rules | Black List | Password | Cache
Connections | Email | NNTP News | TCP Mapping | SOCKS | Real Player | DNS | Proxy Server | Options

BrowseGate provides PNA support for Real Player G2 to handle streaming Audio and Video. To enable this proxy, simply check the "Run PNA proxy service" option, and if you must, change the port number, although we recommend you accept the default in this case.



To configure Real Player G2 to use this proxy, start RP, select the Options | Preferences menu option, and then on the property sheet, select "Transport".

Select the "Use specified transports" option, and then click the "RTSP settings" button.
Select "Use HTTP Only"
Ignore all other options on this tab.
Press OK

Select the "Use specified transports" option, and then click the "PNA settings" button.
Select "Use TCP to Connect to Server"
Check all three of the available options below this.
Normally we recommend you accept the default times in the fields associated with these.
Press OK

Now select the Proxy Tab.
Under the "PNA and RTSP Options" section :-
Check the "Use PNA proxy" option
In the field to the right of this, Enter the IP address of the PC on which BrowseGate is running.
Enter the same port number as you selected in BrowseGate for RP support

Under the "HTTP Options" section :-
Select either "Use my web browser's HTTP proxy" or "Manually configure HTTP proxy", and then enter the IP address of the PC on which BrowseGate is running.
Enter the same port number as you selected in BrowseGate for HTTP support

Click OK

RP should now work happily with BrowseGate, and you will see the "Real Player" LED flashing intermittently when you have RP running and connected.

What to do if your networked PC's cannot connect to BrowseGate

See Also : Setting up network IP addresses under W95/NT4
Understanding the ports !

BrowseGate, like virtually all other Internet programs, requires all PC's that wish to access it to have the industry standard TCP/IP protocol installed. This is available to all windows users free of charge as it is provided as a part of the Windows 95/98/NT operating system. If the PC on which BrowseGate is installed or the the other PC's on your network do not have this installed as a part of their networking system, then they will definitely not be able to communicate with BrowseGate. On network PC's that do not have a modem, you only need to install the TCP/IP protocol for whatever network card is installed, and do not need to install TCP/IP dial up networking on these machines.

It is assumed that you already have your standard PC networking configured and working correctly.... If not please set up your preferred network system and then return to this help page.

If you have installed BrowseGate on a PC that is not networked you still need to install TCP/IP on this PC as your Browser communicates with BrowseGate using this protocol.

To install TCP/IP on a Windows based PC.
Under W95 and NT4... (ONLY)

Click on Start Menu -> Control Panel -> Network - Configuration

Check for the following entry in the list of protocols that are installed
TCP/IP -> {Your network card name}

If you do not have this entry on your PC, you must add this protocol as follows.

The following instructions assume you are using Microsoft Networking...

Click the "Add" button.
Double click on the "Protocols" entry in the list displayed
Click on the "Microsoft" entry in the next list displayed (or other manufacturer if you are using a different networking system)
Click on the TCP/IP entry in the right hand list.
Click the OK Button.
Follow any instructions that are displayed.

Reboot Windows if told to do so.
After rebooting - you will be ready to set up IP addresses on your PC.

All About TCP/IP etc

TCP/IP

TCP/IP is essential if you want to use the Internet. TCP/IP stands for 'Transmission Control Protocol / Internet Protocol'. TCP/IP (usually called TCP) is the standard method of sending and receiving data on the Internet. It is based on data packets that have a set format, including to and from addresses, similar to a letter. If you want to use the Internet or BrowseGate, then TCP/IP needs to be installed on every machine on your LAN that wishes to connect to BrowseGate. In truth, TCP and IP are actually different protocols, but they are so tightly tied together that they are usually referred to in this way.

Packet

A data packet is a like a 'mail parcel'. Think of a package that gets sent in the post. There are a few things that you have to have. There has to be both a name plus address, possibly a return address, and of course stamps, plus the envelope and/or some wrapping. But, you can put anything you like in the parcel. You can send anything that will is acceptable to your postal system. A data packet is very similar to this. You have to supply certain 'Wrappers' such as 'to' and 'from' fields, but what is sent in it as "data" is entirely up to you. There are different types of packets used on the internet and other networks, but they all use this same idea of a parcel of data.

IP

IP stands for Internet Protocol. This is the method used on the internet (and on many LANs) to communicate. IP is a system of what are called datagram packets. IP is not usually dealt with directly, this is the job of TCP. IP gets datagrams from point A to point B. TCP sends IP a datagram, and a destination. It assembles and sends a packet with information from the source (eg TCP) and a checksum that indicates the integrity of the packet. IP doesn't care what the datagram contains. In fact it does not care if the packet it sends even gets there, and when IP receives a packet, if it has been corrupted somehow, IP throws it away! It is up to the protocol using IP to arrange for the packet to be resent if required.

IP Number / IP Address

An IP number is a simple way for IP to distinguish different computers (actually their Interfaces) that exist on the same network. On the Internet you simply can not have two computers sharing an IP, as this creates havoc when trying to send data to the correct location. All computers that are 'on' the Internet (or LAN) need discrete IPs. There are different types of IP.

You have probably seen IP addresses in the form 128.211.23.45. This is a 32-bit number separated in to four "8 bit" parts. The four parts are similar to a mailing address, except the detail is the other way round. The first number of the IP is the most general, the last is the most specific. Since each computer on the Internet needs a different IP, there has to be some way of allocating the IPs so that large companies and organizations are able to have individual ones for all their machines, while smaller organizations also have some to go around as well. Since there are a small number of Large organizations and a large number of small organizations, ranges of IPs can be allocated accordingly.

In an IP number there are 2 parts, the network and the host identifiers.
There are three ways the IPs can be split in to 2 parts.

Class A nnn.hhh.hhh.hhh
Class B nnn.nnn.hhh.hhh
Class C nnn.nnn.nnn.hhh
where n's=network identifier, h's=host identifier

A huge company with very complex internal networks may be allocated a class A address range such as 105.*.*.* . Only the range 1.*.*.* to 126.*.*.* are available for A class addresses. There are very few A class addresses, and no more are to be allocated, mainly because no-one has 16 million computers on their network!

B class addresses however are common for Large companies, allowing a range of around 65000 IPs. Microsoft and IBM probably have several each. When an B class IP address is allocated, (say 165.103.*.*), the first two numbers identify that companies network. The company can decide what to do with the next two (*'s in this case mean any number), and give any IP in that range to any computer on their network. B class networks addresses have 128 - 191 as the first number in the IP.

Class C addresses, giving 254 possible addresses (0 and 255 are reserved) are the third type. Here, the first 3 8 bit fields are specified, and the remaining field is allocated by the owner of the address. C class licenses are in the range 192.*.*.* to 223.*.*.*

Networks that are directly connected to the internet are connected to an ISP via some full time connection (such as a cable or leased line) and the ISP will inform the network administrator of which IP's can be used on the network. A router is used to 'tell computers how to get to a particular IP'.

ISP's typically have 1-2 C class licenses, providing 250 to 500 IP's. When you dial up an ISP with a modem, you are Dynamically allocated an IP address. This will be in the range of the C class license that they own.

Private IPs

These are the IP addresses you are almost sure to want to use on your network when setting it up to connect to BrowseGate

Private IP numbers are ranges of IP numbers that are 'Known not to exist' on the Internet. What this means is that no computer on the Internet will be assigned these addresses. These can safely be used in internal LANs, as they have no direct connection to the Internet. One example of a Private IP range is the 192.168.0.* range that this manual commonly refers to.

The private IP ranges that will not be allocated on the Internet are

10.0.0.0	to	10.255.255.255	Class A
172.16.0.0	to	172.31.255.255	Class B
192.168.0.0	to	192.168.255.255	Class C

For a private network - do not choose an IP range that is not on this list. Also note that 0 and 255 are reserved in any class.

Netmask

Network masks are IP filters. They are used in directing or 'routing' network traffic. The mask is related to whether you are on an A B or C class network.

localhost

localhost is a special term in TCP/IP. 127.0.0.1 is the localhost (loopback interface) this is a software only interface internal to the stack itself, and is not accessible over any interface. It doesn't matter what your LAN card IP really is, 127.0.0.1 will always refer to the local machine. This means that this interface can only be accessed from the machine itself. It is like saying "ME" or "I" in reference to yourself. TCP/IP often uses localhost if a machine wants to talk to itself on a different port it can say "localhost:<port#>". The TCP stack looks at this, realises it refers to itself, and directs to the correct port, with out sending anything on the network.

Setting up IP addresses under W95/NT4

See Also: Setting up your browsers to access BrowseGate
What to do if your networked PC's cannot connect to BrowseGate

The creation and assignment of TCP/IP addresses are a widely misunderstood area of intranet systems.

The following information should hopefully clarify the position for you...

The first thing to understand is that if you intend to use TCP on your Intranet system (in-house network), then it is mandatory that each and every PC is assigned a unique address. These ALWAYS come in the format shown below :-

158.152.45.2 or similar type of numbers.

There are ALWAYS 4 groups of digits, and each of these groups may contain 1 or more digits within the group. Typically the first two groups tend to always contain 3 digits,and the last two groups vary quite a bit....

So 158.152.45.2 and 158.152.459.213 and 158.152.4.2 are all valid IP addresses.

If you have a registered Domain (with Internic) and have been allocated a publically recognized IP number, and you ARE PERMANENTLY connected to the Internet, then your Server PC would HAVE to be assigned this "public" IP Address.

If you have a registered Domain (with Internic) and have been allocated a publically recognized IP number, but you are NOT PERMANENTLY connected to the Internet, then your Server PC would NOT HAVE this "public" IP Address assigned to it.

The Internet has provided three different groups of IP addresses that should ALWAYS be used for intranet PC's that are NOT PERMANENTLY connected and known globally to the Internet itself. These are :-

Starting at		Ending with
10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

(Source of information - RFC 1918)

You can select any numbers you wish, but all PC's on a network MUST be assigned DIFFERENT numbers BUT FROM THE SAME GROUP if they are to communicate with each other, and with the server PC. Also you should always set the Subnet mask to 255.255.255.0 (see below for more info on this)

As an example, lets assume you have decided to use numbers form the 172.16.0.0 group for your Intranet, and you have 5 PC's plus your SmartServer PC to configure. You might choose the following set of IP addresses :-

VALID ADDRESSING SCHEME		INVALID ADDRESSING SCHEME		
SmartServer PC	172.16.100.1	SmartServer PC	172.16.100.1	
Client PC 1	172.16.100.2	Client PC 1	172.16.100.2	
Client PC 2	172.16.100.3	Client PC 2	172.16.100.3	
Client PC 3	172.16.100.4	Client PC 3	172.16.100.4	
Client PC 4	172.16.100.5	Client PC 4	192.168.100.2	<- this is INVALID
Client PC 5	172.16.100.6	Client PC 5	172.16.100.5	

or

VALID ADDRESSING SCHEME		INVALID ADDRESSING SCHEME		
SmartServer PC	172.16.100.1	SmartServer PC	172.16.100.1	
Client PC 1	172.16.100.2	Client PC 1	172.16.100.2	
Client PC 2	172.16.100.35	Client PC 2	172.16.100.35	
Client PC 3	172.16.100.46	Client PC 3	172.16.100.46	
Client PC 4	172.16.100.52	Client PC 4	192.168.100.52	<- this is INVALID
Client PC 5	172.16.100.68	Client PC 5	172.16.100.68	

You will see from the above that typically you would simply increment the last group of digits to assign a different IP address to each PC on you network, but they DO NOT have to be sequential if you do not want to do so. They must all be in the same IP group however.

To configure each PC on your network with these IP Addresses, follow the instructions below.

Click on Start Menu -> Control Panel -> Network - Configuration

Find and highlight the following entry in the list of protocols that are installed

TCP/IP -> {Your network card name}
If you do not have TCP/IP setup on a PC, you need to do this by following the instructions on How to Configure your PC to run TCP/IP first, and then follow the instructions below.

Click on Properties.
Click on the IP Address Tab in the properties dialog.
Make sure you check the "Specify an IP Address" option.
Enter the chosen address for this PC (remember - each PC must be different) in the "IP address" field.
You should ALWAYS Enter 255.255.255.0 in the "Subnet mask" field This is a standard value that ensures the PC's cannot be seen externally... (Unless you want your PC's visible externally and you have a permanent connection to the Internet)

Click the OK button on this dialog, and then on the main dialog. Windows 95/NT4 will almost certainly load new files, and may ask you for the Windows CDROM when you do this. Once the files have been updated it will then usually tell you that you need to restart Windows before the settings will be valid. Once you have restarted Windows, the PC will be capable of Sending and receiving mail using the TCP protocol.

Repeat this process, with different IP addresses, on each PC on your network.

Setting up Microsoft Internet Explorer 4 to use SOCKS 4

1. Start MSIE 4.xx
2. Select the menu option "View | Internet Options"
3. Select the Connection tab (4th from left)
4. Uncheck the option labeled "Connect to the Internet using a modem"
   in the "Connection" group frame.
5. Check the option labeled "Connect to the Internet using a local area network"
6. In the "Proxy Server" frame directly below, check the two options marked
   "Access the Internet using a proxy server" and
   "Bypass proxy server for local (Intranet) addresses".
7. Click the "Advanced" button to the right of these options.
8. Enter into the "Socks" field the ip address of the PC that BrowseGate
   is installed on.
9. Enter the port number (usually 1080) in the field alongside that is to be used for
   SOCKS communication between this web browser and BrowseGate.
10. Enter the IP address and port for any other protocols you wish to use, but you
    should NOT need to use any others!!!!
12. We recommend that you enter the following ip address into the Exceptions
    field at the bottom of the property sheet "127.0.0.1" (Do not enter the quote marks)
13. All other fields are ignored by BrowseGate, although you may have
    other servers supporting these.
14. Click on the OK buttons to close and save the configuration system.

Setting up Microsoft Internet Explorer 5 to use SOCKS 4

1. Start MSIE 5.xx
2. Select the menu option "Tools | Internet Options"
3. Select the Connection tab (4th from left)
4. Check the option labeled "Never dial a connection"
   in the "Dial-up settings" group frame.
5. In the "LAN settings" frame directly below, click the button marked
   "LAN Settings"
7. Unless you have centralized network configuration for your browsers,
   ensure you have both entries in the "Automatic configuration" frame
   UNCHECKED.
8. Check the "use a proxy server" option in the "Proxy server" frame
9. Click on the Advanced button
10. Enter the IP address (or machine name) of the BrowseGate Server PC
    into the "proxy address to use" field for the SOCKS field.
11. Enter the port number in the field alongside that is to be used for
    communication between this web browser and BrowseGate.
    (This will usually be 1080)
12. We recommend that you enter the following ip address into the Exceptions
    field at the bottom of the property sheet "127.0.0.1" (Do not enter the quote marks)
13. The Gopher fields are ignored by BrowseGate, although you may of course have
    other servers that do support this protocol.
14. Click on the OK buttons (all three of them) to close and save the various configuration dialogs.

Setting up News clients to connect through BrowseGate

This shows how to configure Microsoft Outlook Express, but the settings will be similar in most other news reader packages.

BrowseGate Setup:

Configure | Email Tab

- Incoming mail tab with remote port set to 110.
- Outgoing mail with remote connection set to port 25.
  Local ports for both set to whatever you wish....

Outlook Express Setup:

1. Start Outlook Express
2. Select the menu option Tools | Accounts
3. Click the News tab
4. For each News account you have configured, do the following :-

5a. Select a news account.
5b. Double click on it or click the Properties button.
5c. Select the Connection tab.
5d. Ensure you have the "Connect using my local area network (LAN)" selected.
5e. Now select the Server tab.
5f. Enter the IP address of the PC that is running your BrowseGate server in the Server Name field in the Server information panel.
Finally - Check the "Server log on" box if appropriate.
6. Select the Advanced Tab.
7. Check that the entries in the Server port numbers panel are the same as the **Local Port settings** in the BrowseGate News configuration tab. (The default is 119 for NNTP, which is usually OK on most networks - but please check with your network administrator if you are unsure)
8. Select any other options you wish to use on the advanced tab.
9. Click the OK button to save any changes made
10. Make sure you repeat the steps 5a -> 9 for each news account you have in Outlook.
11. When you have configured each and every account, close the account dialog.

Outlook express should now connect to your specified news server via BrowseGate totally automatically.!!!

WARNING Because Microsoft are known to be constantly revising Outlook and Outlook Express, your news account dialogs may well vary in content and name from those described above. If you find this to be the case you need to find the same entries on your particular version and then follow the instructions above.... or contact Microsoft for details of how to configure your version of Outlook to work through a networked proxy server. Please do not send support questions to us on this as we are not able to provide support on Microsoft products directly - for obvious reasons !

Setting up email clients to connect through BrowseGate

All email clients on your network that are to use BrowseGate to send and fetch email using the industry standard POP3 and SMTP protocols will need to have some very simple changes made to their settings to enable them to connect via BrowseGate.

Full configuration details are provided for :-

Microsoft Outlook Express

Other mail clients will (very probably) be similar.....

Setting up the TCP networking in Windows 95/98 to use the BrowseGate DNS

Because BrowseGate provides both internal and external DNS services, you will very probably need to change the TCP/IP settings in each of your networked PC's.

If a PC has previously had TCP/IP dialup facilities, it will almost certainly have one or more DNS addresses setup in the TCP/IP setting property sheet. To check these and to change them to allow each PC to use the BrowseGate DNS, simply follow the instructions below for each networked PC.

Go to the PC on which BrowseGate is running, and select the "View | Select local ip address" menu option.
Carefully note down the number that is highlighted (It will always be a set of 4 groups of digits looking something like "xxx.yyy.zzz.aaa")
This is the BrowseGate Server PC IP ADDRESS (hereafter called the "server-ip")
Then:-

1. Go to the Start Menu and select Settings
2. Select Control Panel
3. Double click on the Network entry from the list shown
4. Select the Configuration tab if not already selected
5. Locate and select the entry that looks like "TCP/IP -> network_card_name"
6. Make sure you have NOT selected the entry that has "Dial-Up Adaptor in it....
7. Click on the Properties button
8. Select the DNS Configuration tab on the property sheet.
9. Make sure you have the "Enable DNS" option selected.
10. If the "Host" field is empty, enter the name of that PC in the field.
11. Leave the Domain field empty.
12. If there are any entries in the "DNS Server Search Order" listbox, highlight each one and use the Remove button to delete them until the list it empty.
13. Carefully type the "server-ip" into the top field (the one with the dots already in it)
14. Click the Add button
15. Finally click the OK button on each dialog that appears.
16. Windows will load (or reload) some files, and will almost certainly then ask you to reboot the PC.

That's it !!!!!!!!!

Once you have rebooted, that PC _should_ then be able to connect to the BrowseGate PC for all future DNS requests for any/all of the Internet applications that may be run on it.

Setting up your networked PC's to connect to BrowseGate

See Also: BrowseGate's internal address Domain Name Server
BrowseGate's external address Domain Name Server

The following information assumes that you already have TCP/IP configured and working on your PC network.

Overview

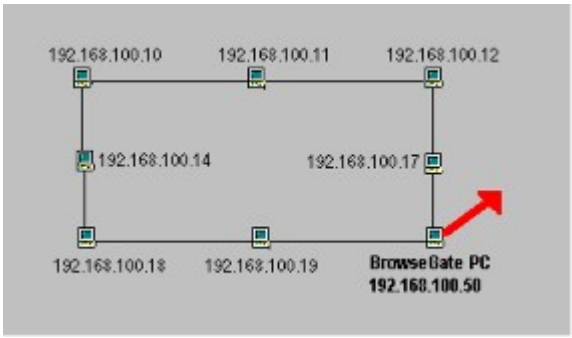
Every PC, (or other computer) on a TCP/IP network must be given a unique, network wide IP address in the format xxx.xxx.xxx.xxx. Most will also have been given a "human readable" name such as "Dellp200" or "MyDell".

TCP/IP is capable of utilizing both of these as a means of client applications addressing a specific computer, but if you prefer to use the machine names rather than having to try to remember long and complex number series, then it requires the installation of a Domain Name Server (DNS) which is able to identify a machine via it's name and "resolve this" to the correct IP address, which is what the computer itself uses to communicate across the network under TCP.

To make you life as easy as possible, BrowseGate comes with it's own built-in DNS system capable of handling both internal (machines on your private network) and external (all other computers out there on the Internet) IP address resolution.

To take advantage of this powerful system is quite easy, but you will need to have a basic understanding of what it all means, and you will need to change a single setting on each networked PC, including the PC on which BrowseGate is installed.

The following diagram illustrates a typical office network, with each machine having it's own unique TCP/IP address (which do not need to be sequential) The BrowseGate PC has (totally arbitrarily) been given the IP address of **192.168.100.50**



All the other machines on the network will have similar addresses, normally all will need to use the same first 3 groups of numbers eg: "192.168.100" but the last group is varied for each machine, which is standard TCP/IP addressing practice. In the example here our example network has machines with a final 'group' ID of 10, 11, 12, 14, 17, 18, 19. Let us also assume for the sake of this example that each PC has been given a name of netpcxx, where the 'xx' is the same as it's last group of the IP address.

All totally valid, resulting in a network that has the following unique TCP/IP addresses and machine names :

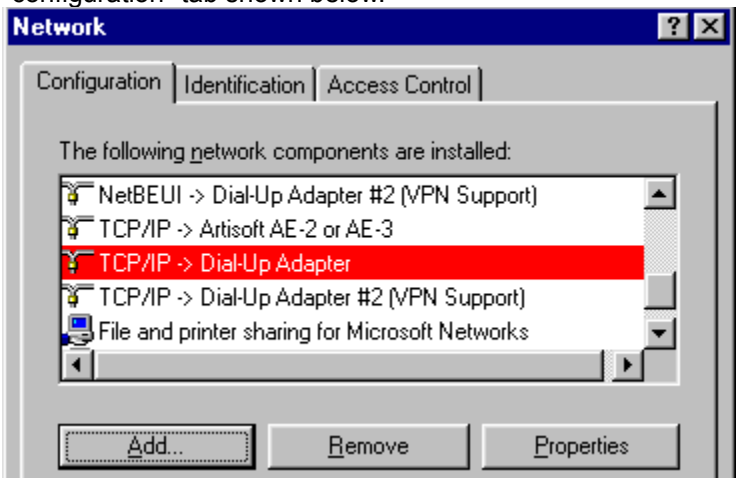
IP Address	Name
192.168.100 10	netcpc10
192.168.100 11	netcpc11
192.168.100 12	netcpc12

192.168.100 14 netcpc14
192.168.100 17 netcpc17
192.168.100 18 netcpc18
192.168.100 19 netcpc19
192.168.100 50 netcpc50 (This is the BrowseGate Server PC)

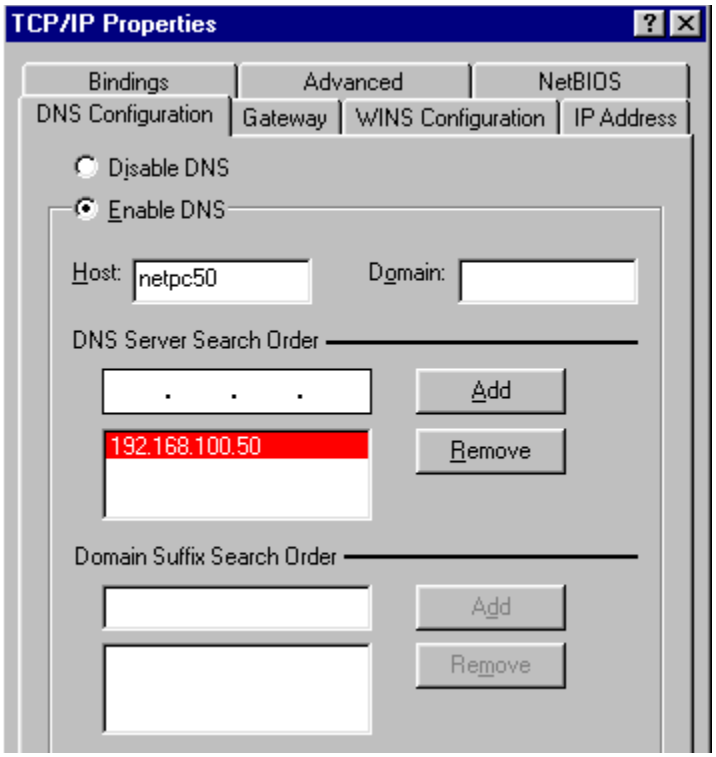
So far - so good !!!!

Now we can see that "netpc50" with an ip address of 192.168.100.50 is the machine on which we have installed BrowseGate. So we need to tell all the other PC's on the network how to connect to it.....

This involves selecting Start Menu | Settings | Control Panel | Network, and then selecting the "configuration" tab shown below.



Locate and highlight the same entry as shown above, and click on Properties, then select the DNS configuration tab, which will look like the dialog below.



You can see that we already have the PC name (in the Host field) and have entered the IP address of the BrowseGate server in the DNS search order list. If you currently have other DNS entries in here, we suggest that you make a note of them (just in case) and then highlight and remove each one before entering the ip address of the BrowseGate server PC.

Thats all there is to it - once you have done this, this PC will always pass ALL DNS requests from any/all applications that require it to the BrowseGate PC.

Click the OK button(s) until all property sheets have been closed and the changes saved. This will usually result in Windows updating some files from your CAB files or the Windows CDROM, and you will then have to reboot the PC before the changes will take effect.

Repeat this process, **with exactly the same entries**, on all other networked PC's apart from (possibly) the PC on which BrowseGate is running.

On the BrowseGate PC itself, you can, if you wish, use exactly the same entries, but if you have any internet type client applications that will not be using BrowseGate for whatever reason, you can add up to 2 external DNS address to this list after the BrowseGate PC's IP address. This will allow these "rogue" applications to connect via your ISP's DNS system as normal.

Setting up your networked browsers to use BrowseGate

See also: Using the TCP Mapping feature for News

The Web Browser on each PC on your network that is to use BrowseGate to access the World Wide Web will need to have some very simple changes made to it's settings to enable it to connect via BrowseGate.

Full configuration details are provided for :-

Other browsers will (very probably) be similar.....

About the Windows HOSTS file

A HOSTS file acts as a local database that tells your computer where to go when it's looking for a certain address, kind of like a "mini-domain name server." Using NOTEPAD, create a new text file. The only entry in this file should be the IP address and name of the BrowseGate PC, separated by at least one space.

It should be in the format shown below :
IPNUMBER<tab>NAME<enter>
IP Name to use for the BrowseGate machine

So your entry might look like this:

192.168.0.1 browsegate

Make sure you press ENTER at the end of the line of text, otherwise Windows 95/98NT4 may not recognize it.

Now save your file in the \WINDOWS directory in Windows 95 or the \system32\drivers\etc directory in NT, with the filename HOSTS with NO file extension (for your information, the HOSTS file entries do not replace or interact with NetBIOS names in any way). To save a file name with no extension in Notepad, surround the name in quotes, and add a dot to the end.

Usually there is a hosts.sam (sample) file in the same directory as the hosts file, so if you cant find hosts or you mess up your copy, you can look at this sample file to see how they are laid out. Any line with a # at the front is a comment. You only need the one line (as above) to get resolution for the name of the BrowseGate machine.

LMHOSTS - What is it and do you need one ?

If your organizations network does not have a DNS systems installed, then you will not normally be able to use PC names in the "Host" fields of most typical TCP/IP packages such as email, NNTP news and FTP clients. To overcome this Windows has a special facility called an LMHOSTS (and also a HOSTS) file that lets you provide a simple text file that is used to "map" all the names of the machines on your network to their actual IP addresses.

We strongly recommend that you take advantage of the built-in DNS servers in BrowseGate, which means that you can /(and indeed should!!!) discard any HOSTS or LMHOSTS files on your system, unless of course they are specifically required by any other applications.

However - if you still want to play with these files, you may just find the following information useful.....

According to the best Windows documentation around, the choice as to which of these two files you should create/use depends on various Windows network setup options, so we recommend that you create both, with identical contents, which we can guarantee will not have any detrimental effect on any other installed DNS type lookup system.

Most Windows installations have a sample version of these files (with suitable annotation), which can usually be found in the \Windows directory with the name LMHOSTS.SAM or HOSTS.SAM (Samples!!)

We suggest you open these and have a look through them first, and then you can create your own 'usable' LMHOSTS (and/or HOSTS) file by opening Notepad or a similar *ASCII TEXT* editor and making one or more entries similar to those shown below.

```
192.168.44.21   DELLPC166
192.168.44.25   GATEWAY2100
192.168.44.27   GATEWAY2200
....
```

Naturally, you will replace the ip number and names with those of the PC's on your own network....

The format of this file is that the first entry in column zero will be the IP address of one of your PC's on your network/intranet.

Next will be a tab.

The second entry after the tab is the machine name of the PC that has that particular IP address.

So in our example above, the DELLPC166 has an IP address of 192.168.44.21, the Gateway 2100 laptop has an IP address of 192.168.44.25 and so on.

You may enter comment lines or disable an entry if you wish by starting any line with '#' eg:
#192.168.44.23 mylaptop

Each and every PC on your network SHOULD have an entry in this LMHOSTS (and HOSTS) file.

You should save the resulting file to your \windows directory with the correct name of
    lmhosts.
and/or
    hosts.

Yes, that is a period at the end..... !!!!

To achieve this, you need to enclose the entire name in quotes in the filename field of the "Save File As"

dialog - eg: "LMHOSTS." or "HOSTS." and then press OK.

Restart Windows after doing this and you should be able to use PC names rather than the less understandable IP addresses in all of your TCP/IP client packages with no problems.

Each PC on your network should have an identical copy of these files....

NB Please note that the whole file is parsed including comments on each lookup,so keeping the number of comments to a minimum will improve performance.

Absolute FTP is pretty easy to configure for use with both the SOCKS4 and/or SOCKS 5 support in BrowseGate.
The following instructions apply to Absolute FTP v1 .5(32bit)

1. Start AbsoluteFTP
2. Select Options | Global fro the menu.
3. Select FireWall tab on property sheet
4. Select the "SOCKS version x" option you wish to use (4 or 5)
5. Enter in the "Hostname or IP" field the machine name (or IP address) of the PC on which BrowseGate is running.
7. Ensure "Port" is set to 1080.
8. Normally you should leave Username and Password blank for public IRC servers.
10. Click OK.
11. Try connecting to an FTP site of your choice from the button bar - it should all work !!!

The activity indicators show you at a glance which of the main proxy services are available . If a red LED is visible, it denotes that the service concerned has been disabled in the configuration.

When activity takes place on any of these connections, the green LED's will flicker to show that the proxy server is working and using those particular proxy connections.

You may double click many of these indicators to toggle their status between active and disabled.

This panel shows you the IP address of the PC on which BrowseGate is running, together with the TCP port it is using to connect to each of the browsers on your network. You should set up all other tcp/ip applications that wish to use the BrowseGate services to use this same IP address. (see networking with TCP)

Click the OK button to save all changes made.
If you click the CANCEL button, no changes made will be saved,

This field allows you to change or add new entries in the relevant list.

Click the Edit button to modify the currently selected entry, or Add button to add a new word or URL to the list.

Once finished, press Save. The entry you have added or changed will always be placed in the list in alphabetical order. If you do not wish to save any changes made, press the cancel button.

Refuse access if site is in banned list
If checked, BrowseGate will check the entire list of sites in the provided NNSITES.BAN file and if any site in the list exists in the requested URL it will display a suitable web page informing the user that the site they have requested is banned due to it's presence in the current Blacklist of web sites.

Apply Strict enforcement
If this option is checked, BrowseGate will check the web site domain alone for matches in the blacklist. This means that if a banned web site entry of say

"www.dirtygirls.com/female/porno/dirty.htm"

is not in your list of banned web sites, BUT you have one or more entries that DO CONTAIN the domain "www.dirtygirls.com", then the requested page will **still be banned** because the main domain of "www.dirtygirls.com" matches, and the actual page entry etc is simply ignored.....

Banned words configuration

Refuse access if banned word is detected in URL

If checked, BrowseGate will check the entire list of words in the NNWORDS.BAN file and if any word exists in the requested URL it will display a suitable web page informing the user that the site they have requested is banned due to the presence of the word identified in the current Blacklist of words.

Apply if Partial match (Strict)

If this option is checked, BrowseGate will check the requested web site URL for any substring match from the blacklist of words. For example, if you have the Strict words option checked, and you had a word in your list of "girl", then if a URL entry of say

"www.dirtygirls.com/female/porno/dirty.htm"

was requested, the page would **be banned** because the word "girl" can be found as a substring in the URL.

However if you have Strict unchecked, then this URL would **not be banned** because the checking algorithm looks for the characters immediately prior to and immediately after the match, and then will only ban the request if both of these are one of the following characters :-

"." Period
"/" Forward Slash
"%" Percent
"?" Question mark.

So in our example URL, although the following character is indeed a period, the immediately preceding character is actually "y", so the match would FAIL and the URL would not be banned.

BrowseGate commands

See also: Adding BrowseGate commands to the favorites list in IE4/Netscape

BrowseGate provides a set of commands that let you interrogate the proxy server to find out what settings apply to the PC you are working on, or even to force BrowseGate to hang up the telephone line....

The commands shown below should be typed into your browser exactly as shown, or with "//" before the commands. You do not need to type "http://" at the start of the URL.

PLEASE MAKE SURE YOU DO **NOT** type "www" into the URL field as this will always force BrowseGate to attempt to connect externally to try to resolve this as an external URL.

Available Commands

[bg-help] Shows these commands
[bg-log] Displays a list of available BrowseGate activity log files
[bg-hangup] Drops a modem connection
[bg-rules] Shows any rules that apply to this connection
[bg-allrules] Shows all rules that exist
[bg-alias] Shows any address aliases that will be used
[bg-connect] Details what internet connection BrowseGate is using
[bg-proxy] Details the external proxy server that may be in use
[bg-cache] Shows the current cache system status.
[bg-downloads]Details the FTP setting that are in use
[bg-local] Details the local web server settings
[bg-about] Displays registration and serial number information
[bg-blacklist] Displays the status of the BlackList system
[bg-ports] Displays a list of the current ports configured for standard services by BrowseGate
[bg-tcpmap] Displays settings for all "extra Service" ports configured
[bg-socks] Displays settings for the SOCKS 4/5 support
[bg-real] Displays Real Player settings that will be used
[bg-dns] Displays settings for the BrowseGate DNS configuration
[bg-modem] Displays the current modem settings and online status for BrowseGate

eg: 

You will see that each of these commands is a link to the command, so you can simply click on any command to see what it does from the Help screen that is displayed.

Fuller information on each command

BG-HELP
Displays a page showing the list of commands as shown above

BG-LOG
lists all available BrowseGate activity Log files
eg:

The following log files are available :

Thu.log is dated Thu 25 Feb

The log files are detailed and can grow quite large, but contain considerable information on all services provided by BrowseGate during the period concerned. This includes the IP address of the requesting PC, the Web site URL requested and the date/time of the request.
eg:

See: Example of a log file

BG-HANGUP
Forces BrowseGate to arbitrarily hang-up the phone even if other users are browsing the Web via BrowseGate at that time, but if our SmartServer3 email server system is installed on the same PC, and is also using the same dial-up connection at the time, then the disconnection request is correctly ignored.
eg:

Command [hangup] received and actioned...

BG-RULES
Lists any Rules that have been set up for that specific PC on the network.
eg:

Your server administrator has set the following rules which apply to your connection...

Rule Name: Sex ban 1
Contains the word: sex
Rule Status: Active
Rule Applies: between 9:00 and 17:00 hours
Rule Applies On: Sun, Mon, Tue, Wed, Thu, Fri, Sat
Please contact your server administrator to have settings changed...

BG-ALLRULES
Displays a full list of all Rules that have been set up (for any PC on the network). NB Rules can be set to be both Network wide and/or only applicable to a specific PC.
eg:

Your server administrator has set the following rules...

Rule Name: Sex ban 1
Contains the word: sex
Rule Status: Active
Rule Applies: between 9:00 and 17:00 hours
Rule Applies On: Sun, Mon, Tue, Wed, Thu, Fri, Sat

Rule Name: searches
Originates from the address: 192.143.55.118
Rule Status: Inactive
Rule Applies: between 9:00 and 17:00 hours
Rule Applies On: Sun, Mon, Tue, Wed, Thu, Fri, Sat
Please contact your server administrator to have settings changed...

BG-ALIAS
Lists complete current Alias settings
eg:

Aliasing is enabled

Alias No. 1 : *.com
Alias No. 2 : *.net

Alias No. 3 : www.*.com
Alias No. 4 : www.*.net
Alias No. 5 :
Alias No. 6 :
Alias No. 7 :
Alias No. 8 :

BG-CONNECT
Lists the current external connection configuration of the BrowseGate proxy server you are connected to.
eg:

Listening on port 80
Connect using Virgin net
Inactivity timeout is 30 minutes
Seconds to wait for connection to be made is 120
Number of redial attempts is 1
Delay between redial attempts is 5 seconds

BG-PROXY
Lists the current settings of any external proxy that the BrowseGate proxy server you are connected to may be using.
eg:

External proxy Disabled...

BG-CACHE

Lists the current settigns for the web site cache system.
eg:

The cache is currently Enabled...
Path to \Cache directory is [F:\SMARTSERVER40059]
Max disk space to be used by cache is set to [3] Mb
Current size of the cached data is 460,915 bytes
When cache is purged, 13% of newest data will be retained

BG-DOWNLOADS
Lists the details of the (Browser) FTP configuration of the BrowseGate proxy server you are connected to.
eg:

FTP access type Passive
FTP username ftp
FTP password wwwuser@here.com

BG-LOCAL
Lists the details of the local web site that BrowseGate will connect to if asked
eg:

Local server root directory C:\netc web sites\Public Web Site
Local server default page home.htm

BG-ABOUT
Lists version information for the BrowseGate proxy server you are connected to.
eg:

Version number: 1.05
Registered serial no 15000001

Maximum number of users 25
Using port 80

BG-BLACKLIST
Lists information on the Blacklist settings for the BrowseGate proxy server you are connected to.
eg:

Blacklisting from banned SITES file is Enabled...
Strict blacklisting is Enabled...
Blacklisting of Sites from banned WORDS file is Enabled...
The following PC's will NOT be blacklisted from entries in banned SITES file :-
192.168.4.3 192.168.4.1
The following PC's will NOT be blacklisted from entries in banned WORDS file :-
192.168.4.3 192.168.4.1

BG-PORTS
List the ports that are configured for standard services
eg:

Configured services are as follow

WWW service listening on port 81
SMTP service listening on port 26 connecting to pop3.ps-consultants.co.uk on port 25
POP3 service listening on port 111 connecting to pop3.ps-consultants.co.uk on port 110
NNTP service listening on port 121 connecting to news.demon.co.uk on port 119

BG-TCPMAP
Lists information on the TCP Port Mappings configured for the BrowseGate proxy server you are connected to.
eg:

Configured TCP Mappings are as follows

Connection No. 1 : news.demon.co.uk, Local port - 123, Remote Port - 119, Connection ACTIVE
Connection No. 2 : mail.virgin.net, Local port - 151, Remote Port - 110, Connection ACTIVE
Connection No. 3 : pop.site.csi.com, Local port - 153, Remote Port - 110, Connection ACTIVE
Connection No. 4 : pop3.demon.co.uk, Local port - 154, Remote Port - 110, Connection ACTIVE
Connection No. 5 : pop.freeserve.net, Local port - 155, Remote Port - 110, Connection ACTIVE
Connection No. 6 : mailhost.airtime.co.uk, Local port - 152, Remote Port - 110, Connection ACTIVE
Connection No. 7 : pop3.ps-consultants.co.uk, Local port - 221, Remote Port - 110, Connection ACTIVE

BG-SOCKS
Lists information on the TCP port Mappings configured for the BrowseGate proxy server you are connected to.
eg:

SOCKS V4 and V5 service: Enabled...
SOCKS port number 1080

BG-REAL
Lists information on the port settings configured for RealPlayer to use the BrowseGate proxy server you are connected to.
eg:

Real Player (PNA) service: Enabled...
PNA port number 1090

BG-DNS
Lists information on the TCP Mappings configured for the BrowseGate proxy server you are connected to.
eg:

Internal DNS service Enabled...
External DNS service Enabled...
Primary DNS server 194.168.8.100
Secondary DNS server 158.152.1.58
DNS service running on port number 53
DNS service external port number 53

BG-MODEM
Lists information on the current modem settings and status for the BrowseGate proxy server you are connected to.
eg:

The specified RAS/DUN connection to be used is [Virgin net]
The modem connection timeout is set to [10] minutes
The modem is NOT on-line at this time...

Cache maintenance

Use the Browse button to select the drive and directory you want to be used for the Cached data. BrowseGate automatically creates a subdirectory called \CACHE underneath the selected directory.

This panel can be toggled to show the current level of web page data stored in the BrowseGate internal cache as a numeric percentage (xx%) or as shown here, with Green, Yellow and Red bands to provide a very visual indicator as to how full your cache is at any time.

The graphic here shows the cache to be almost full...

We strongly recommend that you check our web site on a regular basis to ensure that you have the latest version of BrowseGate.

We issue regular upgrades to all their products with Service Packs and new versions. If you don;t check the site regularly, you just won"t know if you have the latest released version ..... !!!!

Checking the BrowseGate settings remotely with a browser

See also: Adding BrowseGate commands to the favorites list in IE4/Netscape
The BrowseGate URL commands

BrowseGate does of course give you the ability to use any connected web browser to check it's current configuration settings via a simple set of URL commands. These will return a page for most settings.

You can even use the BG-HANGUP command to force BrowseGate to hang up the telephone line immediately....

The easiest way to access any of these commands is to simply type into your browser the following URL :-

BG-HELP (Just enter it EXACTLY as shown above...)

You should NOT enter it as WWW.BG-HELP as BrowseGate will recognize this as an external web page request, causing the command to be ignored by BrowseGate.

This command URL will display a special page in your browser window that contains all the available BrowseGate URL commands, and as each command is already highlighted as a jump to the specific command you can just point and click directly from here to try all of the available commands.

Contacting Us

NetcPlus offer unlimited support to registered users via email (see below).
If you are really stuck you may also call our US support centre between the hours of 9 - 5 at +1 - 727 391 5872 (EST)

Please send support questions by email to the following addresses. They will normally be answered within 24 hours at the latest.

bg**support@netcplus.com**

IMPORTANT - Before technical support questions will be answered via email or phone, you will need to ensure you have provided us with your product name, the version you have, and your serial number (or Product ID in later versions)

If you are only evaluating BrowseGate, please state that you are running an EVALUATION version in your support request.

Sorry, but unless we have this information, support will not be provided.

Our support policy provides all registered users with unlimited support for the life of the product. This is from the date of that versions release up until 3 months after the date of release of the next version.

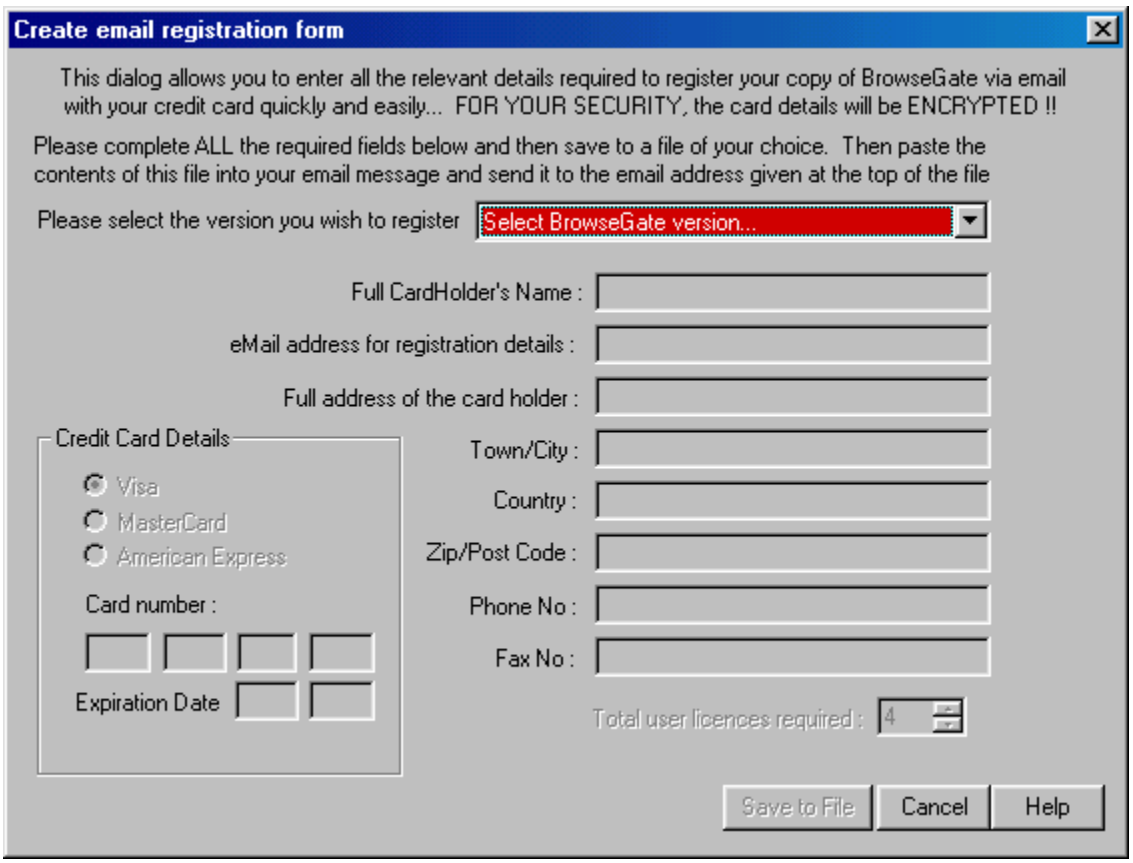
Further information on our products can be obtained by pointing your web browser at our web sites as shown in the Help | About box

Sales information, pricing, and upgrade information can all be obtained from the same addresses and phone/fax number show on the Help | About box.

Create eMail dialog

This dialog can be reached from the Register | Create eMail buttons.....

Please ensure that all Registrations are sent to the relevant address(s) as shown on the Help | About dialog



Please note that you must complete ALL fields but the phone/fax numbers to enable us to get your credit card payment authorized.

To activate the entry fields, just select the type of BrowseGate system you wish to register.
If you select the BrowseGate(Work) then you can also select the total number of licences you require in any multiple of 5. all other versions provide only the total user licenses shown in th euser license field at the bottom right.

Please ensure that the email address you provide is correct, as we use this to mail your registration codes to you via that mail box address.

This option will create a very detailed, and consequently rather large "debugging" text file that shows all the low level activity performed by BrowseGate. It will also slow down the operation of BrowseGate quite noticably.

We recommend you only check this option if asked to do so by NetcPlus Technical Support staff, who may request this to enable them to identify a problem.

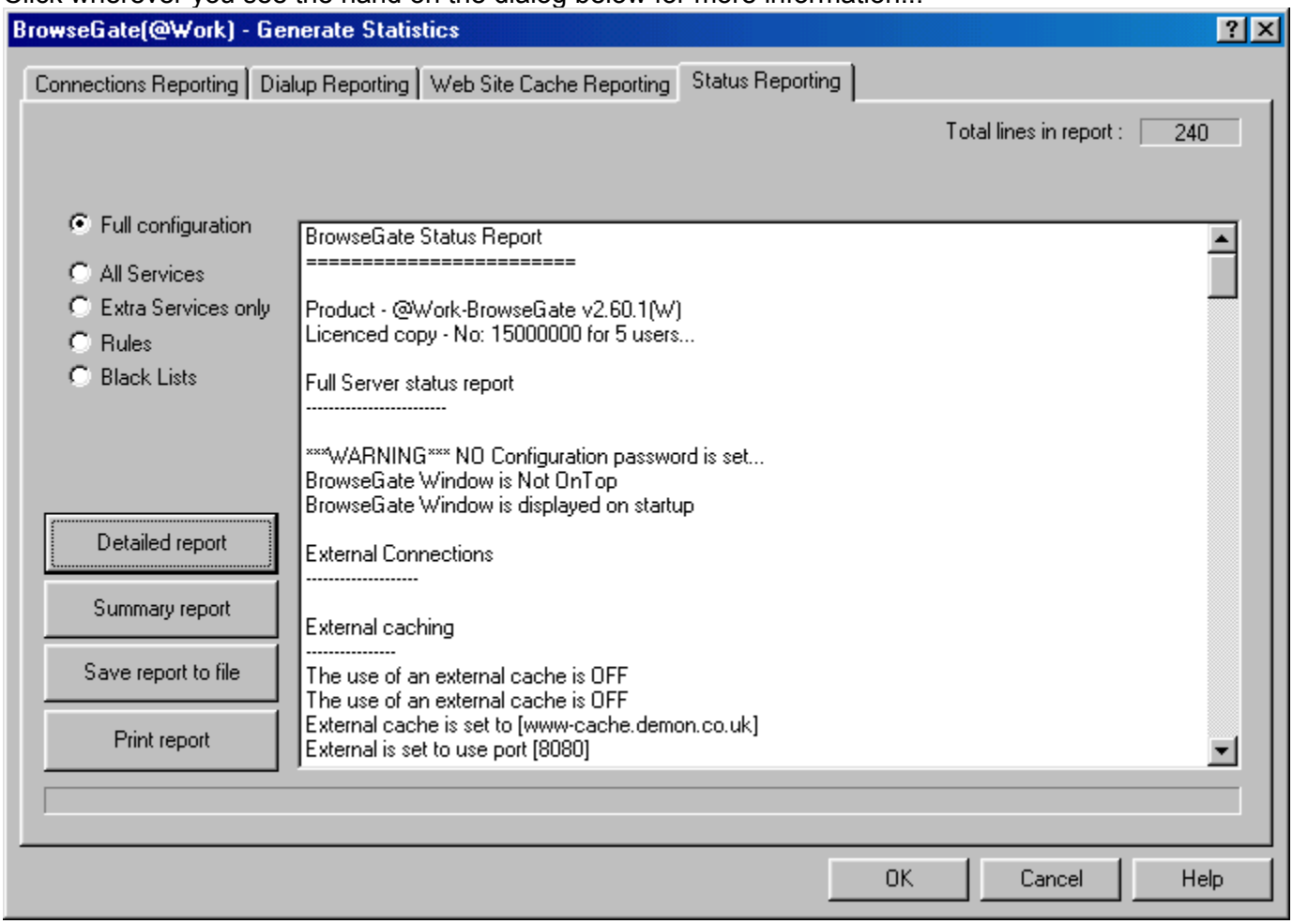
If you do, please ensure you uncheck it again as soon as you have can to preserve your free disk space and to let BrowseGate run at its designed speed.

Creating status reports

See Also: Sample full status report

BrowseGate lets you generate configuration reports that can be saved as files and printed for later reference.

Click wherever you see the hand on the dialog below for more information...



This panel shows the current size of the data that is cached.

Lets you quickly restore all default settings for the DNS system

You can enable or disable either / both the internal
or external DNS facilities provided by BrowseGate if required.

Simply check/uncheck the options here, but please note
that if you do DISABLE the external DNS, you will almost certainly
need to change the entries on your network card's TCP/IP DNS
settings also....

What is an Internal DNS

This is normally what is used to resolve the addresses of each and every PC on your internal network. You enter the TCP/IP address and also the name that has been given to that PC in the maintenance dialog, and then when you enter a meaningful address into one of your internet client applications such as "myserver:1080" this will be resolved by the internal DNS system to be the IP address of that PC on your network - perhaps 192.168.345.123... You can see that it is much easier to remember (and to type without errors) a server with the name "myserver" rather than trying to remember 192.168.345.123 all the time.

What is an External DNS

Whenever a request is received for a non numeric URL, BrowseGate will always check it's internal list first, but if the URL requested does not have an entry in the internal list, BrowseGate will then automatically connect to the Internet (if not already connected) and then ask whatever external DNS server you have specified to resolve the address.

This is all handled totally transparently as far as the networked users are concerned.

The Disconnection indicator shows you how long it will be before BrowseGate will automatically disconnect any active dial-up connection IF there are no more network requests made...

Double clicking on this label will toggle the auto disconnection feature ON/OFF

Discussion on Ports

See also: List of default ports

Ports are the key to all TCP/IP communications. As you may be aware there are several predefined "default" ports for most TCP operations such as HTTP, FTP, POP3, SMTP and NNTP, but actually you can select almost any number of different settings/port numbers on your intranet/network system if you find that you need to do so. However, there are few rules involved in this process, the selections you make being pretty arbitrary.

The key point to always remember is that no two applications (on the same PC) can be monitoring or intercepting the same port at the same time, and whatever port you choose to handle a certain operation (eg pop3 mail) in BrowseGate is the one you MUST also configure each of your email clients (or news clients or web browsers etc) to use

What this means in the real world is that if you encounter a clash where two applications are intercepting and handling the same port, you can simply select almost any other unused port number. However you must ensure that all applications on the entire network that are using the same services are also configured to use the same port number you have decided on.....

As far as BrowseGate is concerned, it treats the internal port connection (local port) to your network applications totally separately to the external port (remote port) it is using to communicate with whatever external server(s) it is configured to work with. That is why it is usually only necessary to change the "local port" setting in BrowseGate to handle any internal network port clashes on your network.

Most external servers use the predefined "standard" ports, so you will be unlikely to need to change the remote port settings in BrowseGate.

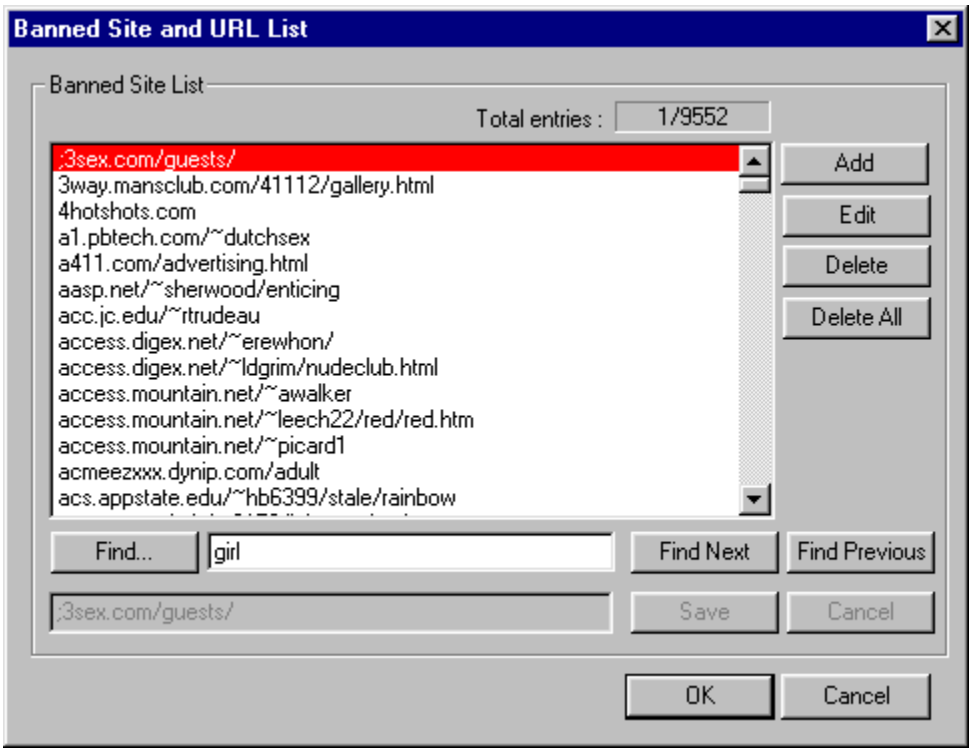
If this is checked, the BrowseGate window will be displayed each time it is run. If not, BrowseGate loads directly into your system tray and does not display the main window. It can be displayed at any time by left clicking the tray icon.

Editing banned sites/words lists

See Also: Maintaining/using the banned lists

BrowseGate lets you modify the content of both the Blacklist Sites and Blacklist Words using the same editor dialog shown below.

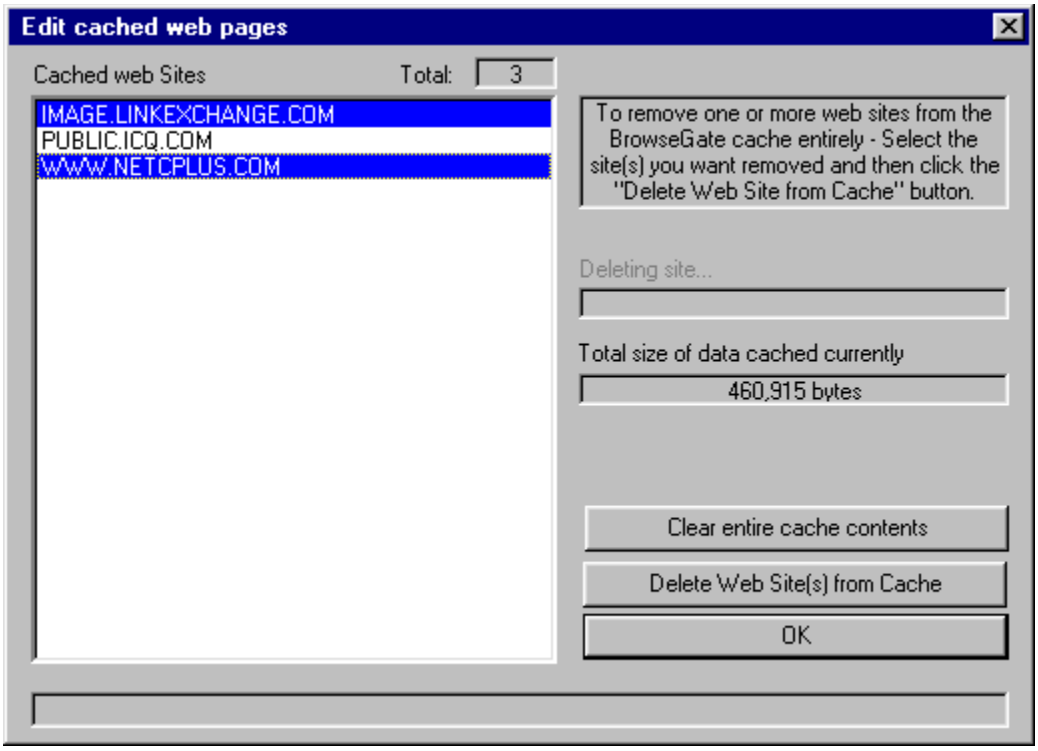
Click wherever the hand icon appears for more information.



These buttons allow you to Add/Edit the list of local DNS entries.

A dialog is displayed to let you add or edit machine names and their respective IP addresses.

Editing the cache contents



The dialog provides a list of each and every web site that is held in the BrowseGate cache system.

You can select one (or more) sites in the list box, and once you press the "Delete Web Site" button, you will be asked to confirm, and then each of the selected web site(s) and all the data stored for it will be deleted form the cache system and removed from your hard disk.

This puts you in control of the cache contents, and lets you quickly and easily remove any web site(s) you decide you no longer wish to keep cached on your hard disk.

The Exit button will close down BrowseGate, and it will also normally disconnect any active dial up connection. However, if you close BrowseGate this way you should also ensure that any dun connection has been closed down correctly.....

TCP Mapping buttons

Checking this option allows you to stop all connected web browsers from performing FTP style file downloads from web sites.

Please note that this will **not** however stop browser users from being able to download files from web sites that use the newer http://xxxxx form of FTP. You can however block this by setting up a new entry on the "Rules" tab that contain the file suffixes of those files you wish to stop being downloaded.

In this case for security the entries MUST include the leading period - for example, a typical rule to stop downloads of common files types might contain the following line:

.EXE .COM .TAR .ZIP .GZ

This would automatically ban any URL that contained a filename which included any of the above 5 common download types.

List of all commands matching those available in BrowseGate

This is the new folder we created for the BrowseGate commands

To find an entry in the selected banned items lists you need only type the phrase to be searched for in the field provided alongside the Find button, and then click the Find button.

The first matching entry will be highlighted automatically. You can also use the Find Next and Find Previous buttons to navigate through all matches in the list.

Glossary

A

B

Binding
A binding is a ‘requirement to use’. In the case of a service (or protocol) to interface binding, it is a requirement for the service to use the specified interface. Binding a service to an interface causes the service to listen on the specified interface. BrowseGate usually binds to all interfaces by default. Services only listen to interfaces for which they have a binding.

C

Cascading
Using one proxy to connect via another proxy is called cascading. It is commonly done when an ISP has a WWW proxy for its customers to use. To cascade the BrowseGate WWW Proxy to the ISPs proxy, simply enter the ISPs proxy details on the Configure | Proxy Server tab.

Client
A client is a recipient of a service. With computers, client machines are PC’s on networks that are generally used by a single person. That computer can access BrowseGate if it requires data or a service that is not part of the client system. For example, when a client computer wants Internet access, it will ask the BrowseGate server for a connection. Client software is a program that makes use of Server software to obtain the required data or service.

Connection
A connection can mean several things. At a physical level it means a joining of two devices, by cable, plug or similar. With Modems, a connection made on a successful dialing of another modem. At a Internet software level it commonly means a channel of communication between the client and server has been established.

D

Dialer
The dialer is software that tells the modem who and when to dial. BrowseGate comes with SmartDun, a System tray module that accesses the standard Window's Dial up networking / Remote Access system and handles your modem transparently.

Dun
This stands for Dial-Up-Networking, a Microsoft term for the part of the operating system used to get modems to talk to each other in Windows 95. In NT the dialing is controlled by RAS, which is very similar to DUN.

E

F

Firewall

A firewall is a barrier between your network and the Internet, through which only authorized traffic can pass. As traffic passes between your network and the Internet it's examined by the firewall which follows the strict guideline of "whatever is not expressly permitted is denied."

Most firewalls screen traffic between a company's internal network and the Internet, however firewalls can also secure on part of a network from another. For instance securing your corporate accounting department or your network from your subsidiary's network.

FTP

FTP stands for File-Transfer-Protocol. This is a method by which files are up/down loaded from the internet. Many client applications exist to make the process easy.

G

H

hosts file

The hosts file is a file that resides in your windows (In 95) or system32\drivers\erc directory (In NT4). This stores some info about where certain machines are.

HTTP

HTTP is the Protocol used for World Wide Web browsing, but many other programs are starting to use HTTP. The BrowseGate WWW proxy allows HTTP access to LAN users so they can view World Wide Web sites.

HTTPS

This is secure http. Netscape and other browsers have built in encryption, to make data exchange more secure. This is commonly used for Online purchasing, especially where Credit cards are involved.

I

IP Number

An Internet protocol number is unique identifying Internet address.

Interface

An interface is a ‘network connection’. That may be a network card, an online Dialer profile, or your localhost loopback.

ISP

This stands for Internet Service Provider. ISPs are companies that have a connection to the internet and provide dial-up or direct connections to customers. Typically ISPs have many modems that customers can dial up with a PPP account. Dialing up an ISP usually gives you direct access to the internet. Many ISPs also offer ISDN T1, or other connections for improved speed.

L

Leased line
A Leased line is a full-time network connection to the internet where you are given an IP number (or a range of IP numbers) for your LAN. There are different methods of connection including ISDN, modem and ethernet. Basically they give you guaranteed access to the internet. Full-time connections are often called 24/7, meaning 24 hours, 7 days a week.

License

BrowseGate licenses are sold in different counts in multiples of 5 users. This number represents the number of client machines that can connect to BrowseGate simultaneously. It is not the number of machines on you network. It is quite common, and permissible, to have a network of over 10 users, but to have only a 5-user license. This is a way of limiting Internet use. A 5 user license allows the BrowseGate machine + 5 other machines to access the Internet at any one time.

Localhost

localhost is a special term in TCP/IP. 127.0.0.0 is the localhost (loopback interface) this is a software only interface internal to the stack itself, and is not accessible over any interface.

N

NIC

Network Interface Card.

P

Packet

A data packet is a like a ‘mail parcel’. Think of a package that gets sent in the post. There are a few things that you have to have, requirements. There has to be a name and address for the recipient, a return address, there have to be stamps, and of course the envelope or wrapping paper. But, what you put in the parcel is up to you. You can send (with in reason) anything that will be accepted by the port office. A data packet is very similar to this. You have to supply certain ‘Wrappers’ like to and from fields, but what is sent as the payload is up to you.

There are different types of packets used on the internet and other networks, but all of them use this idea of a parcel of data.

Ping

Ping is a command available on most TCP/IP capable systems including DOS. It is a command line program that tests a TCP connection between locations, and gives feedback on the speed of the link.

```
Usage:  ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS
        [-r count] [-s count] [[-j host-list] | [-k host-list]]
        [-w timeout] destination-listOptions:
-t              Ping the specified host until interrupted.
-a              Resolve addresses to hostnames.
-n count        Number of echo requests to send.
-l size         Send buffer size.
-f              Set Don't Fragment flag in packet.
-i TTL          Time To Live.
-v TOS          type Of Service.
-r count        Record route for count hops.
-s count        timestamp for count hops.
-j host-list    Loose source route along host-list.
-k host-list    Strict source route along host-list.
-w timeout      timeout in milliseconds to wait for each reply.
```

As an example, to test for a connection to ftp.microsoft.com, type at a command prompt:

ping ftp.microsoft.com <enter>

From a machine that is directly connected to the internet you will get a response such as

Pinging [198.105.232.1] with 32 bytes of data
Reply from [198.105.232.1] : Bytes=32 time 40ms
Reply from [198.105.232.1] : Bytes=32 time 20ms
Reply from [198.105.232.1] : Bytes=32 time 20ms
Reply from [198.105.232.1] : Bytes=32 time 30ms

You will notice that the name you typed is converted to an IP number. This is where DNS comes in. With out DNS you can only ping IP's.

From a workstation that is connected through BrowseGate you would get a result similar to

Pinging [198.105.232.1] with 32 bytes of data
Destination host unreachable
Destination host unreachable
Destination host unreachable
Destination host unreachable

(You may get 4 Request timed out message, they are basically the same thing)

This indicates that DNS is working. BrowseGate can't proxy ping packets, so you can't get the other data from the ping.

If you get a result like

Bad IP address ftp.microsoft.com

Then your DNS probably isn't working, so go back and check where you may have gone wrong.

POP3

Used for retrieving mail from mail servers. A simple protocol that was preceded by the even simpler POP2, and the positively prehistoric POP. POP3 is used by Outlook (& Express), Eudora and most other eMail clients to talk to POP3 servers for retrieving mail.

Ports

A port can be thought of as a channel of communications to a machine. Similar to telephones, it is like a companies PABX that has several lines. Packets of information coming into a machine are addressed not only to that machine, but to that machine on a specified port. You can think of a port as a radio channel if you like, but the fundamental difference between a radio receiver and a computer, is that the computer can listen to any / all of 65000 possible channels at once! A Port is a logical TCP/IP connection. Any TCP/IP program needs to use a port to communicate with any other program or Computer. Certain ports are set aside for certain TCP/IP operation, eg 80 for HTTP.

Protocol

See Unix. A Protocol is a method by which 2 or more parties can communicate or organize their communication. Network protocols are very strict. If an application does not follow the agreed style of communication, then they are unlikely to be understood. Protocol includes such things as greeting a server, logging on with a name and password, requesting and sending information, and saying 'good bye' when closing the connection. This is a similar idea as when one writes a letter. First one writes ones own details, then the recipients name and address, then you greet them with their correct title. Then the bulk of

the letter is written. At the end, a suitable sign off such as ‘Your sincerely’ and then a signature close the communication. Proxy servers typically need one proxy per supported protocol. Examples of Protocols are POP3 Post office protocol and http hypertext transfer protocol.

Proxy

The normal meaning of the word proxy is someone who does something on behalf of someone else, e.g. voting by proxy. The Internet use of the word means basically the same thing, in relation to a software program. BrowseGate does things on behalf of other software programs. Specifically BrowseGate makes Internet requests on behalf of Internet clients to Internet servers.

Proxy Request

This is the action taken when a proxy aware program ‘talks’ to a proxy and asks for a resource.

R

RAS

Remote access service. An NT term, more or less the same as DUN. This is the modem controlling software in Windows.

Resource

A resource is a term used to mean any data item or hardware processing/storage. On a machine, resources are the memory, disk space, or processing time. An Internet resource is a Graphic, an HTML page, a downloadable file, live streaming video or any other available data. BrowseGate has internal resources, images, used to display in listings and other places.

S

Scope
A Scope is a range of IP addresses sharing common properties. The DHCP servers Auto mode will use the 192.168.0.1 to 192.168.0.254 scope. A DHCP scope comprises a group of computers running DHCP clients in a subnet.

Server

A machine and/or software that is set up to provide a service to assist you. Examples are FTP, Email, or Web servers.

Service

A service is something that helps or serves you. In BrowseGate, each proxy you set up are services provided to help you connect to the internet.

SMTP

Simple Mail Transfer Protocol is the method used on the internet for sending mail. BrowseGate fully supports SMTP.

Subnet
A subnet is a group of computers that are directly connected via coax or a hub. A computer with two network adapters will be on 2 subnets.

T

TCP/IP

TCP/IP is essential if you want to use the Internet. TCP/IP stands for ‘Transmission Control Protocol / Internet Protocol’. TCP/IP (usually called TCP) is the standard method of sending data on the Internet. It is based on data packets that have a set format, including to and from addresses, similar to a letter. If you want to use the Internet or BrowseGate the TCP/IP needs to be installed on every machine on your LAN.

Actually TCP and IP are different protocols, but they are so tied up that they are usually referred to in this way.

Telnet

Telnet is a command line program used to access remote computer and run programs on them. Telnet was the method by which the internet was first used. BrowseGate supports Telnet proxies.

Terminator

A small device used at each end of a coaxial cabled network. Terminators are essential.

U

This panel shows you at a glance which HTML port in use for web requests from your networked users.

The Help Button takes you to this Help System.

How to access your local intranet web site

Once you have configured the local web site details, you can type a simple URL into any of your networked Web browsers that are using the BrowseGate proxy server.

URL's look like this :-

//DELLPC

which will force BrowseGate to display the specified default page for the directory you have specified.

You can also use URL's such as //DELLPC/home.htm or even //DELLPC/info.htm to force the loading of a specific web page from the local site providing you know the correct page name.

Click here for full details on how to create the most effective rules...

Registering your copy of BrowseGate

If you have already registered !

Browsegate is easily registered at any time by the entry of the unlock codes that are provided to you (when you pay the registration fee) into the special registration dialog accessed from the Options | Register menu or the "Register" button on the main BrowseGate window.

If you want to register !

You can pay for your registration by email or telephone. If you are using a credit card we have provided a special credit card registration dialog that is accessed from the Register dialog that lets you enter all the credit card details we require and save this to a file that can be sent to us via email. Just click the "Create eMail" button on the register dialog to complete this form and then simply paste the file created for you into an email message.

Your credit card details are encrypted by the registration email form for your additional security.

For all payment methods, please ensure you provide us with a valid eMail address to which we can send your registration unlock codes !!

Full details of all email addresses and phone numbers to send registrations to can be found by clicking the "Help | How to Register" menu option

The Work version of BrowseGate starts with 5 users and can be increased thereafter in increments of a further 5 users, (10, 15, 20 etc) all at small incremental costs.

The Home version of BrowseGate only provides a maximum of 4 users. If later on you require more users, you can upgrade your system to the Personal or Work version by paying the relevant registration upgrade charge and entering the new serial number provided.!!

In addition to the Wizard that will run automatically when you first run BrowseGate, and to make it's initial configuration as easy as possible for you initially, we have included a file called SETUPINFO.WRI which you will find in the BrowseGate installation directory you chose if you did not print it out during the installation process.

We recommend that you print this out and use it as a quick reference guide to help you find your way around the initial settings of your new BrowseGate proxy server quickly and easily.

It is also a good idea to decide whether you are going to take advantage of the built-in DNS in BrowseGate as this will effect the way you configure your networked client applications.

How to specify permitted web URL's

The check boxes to the left of each field allow you to enable or disable each entry independently, thus providing the maximum flexibility in the use of the powerful site blocking system in BrowseGate

If you have one or more of the site blocking fields in BrowseGate set this will limit access to any web site URL by checking each and every request received from your networked users, and looks for a complete match of the main URL entry itself (this is the bit after"http://" prefix and up to, but not including the next "/")

It then compares this URL to each of the Site Blocking entries you have made. The match is NOT case sensitive. The asterisk can also be used as a wildcard to expand the scope of a rule limit for maximum flexibility (see below)

If whatever you have entered in any of the fields provided does match the complete requested URL, the request will be allowed and the web page fetched for the user concerned...

For example, the entry "www.microsoft.com" in Site 3 above would allow access to
http://www.microsoft.com/uk/nt4/downloads.htm
(because the URL to be checked is the bit between the "//" and the following "/" ONLY.... eg "www.microsoft.com")
and it would allow access to variations such as
http://www.microsoft.com//w95/downloads?search=NetcPlus?xcvdef,
but it would REFUSE a request for
http://searchengine.www.microsoft.com/uk/nt4/downloads.htm

because none of your entries contain the complete URL of "**searchengine.www.microsoft.com**"
(The word "searchengine" is missing)

However, if for example a network user were to click on the search option on the Microsoft site, they would not be allowed to perform this based on the allowed "www.microsoft.com" entry, as this URL is actually changed by the Microsoft site to http://search.microsoft.com/...., which does NOT of course match the originally permitted site name of www.microsoft com.

There are two ways you can overcome this problem. :-
Add a new entry (see Site 4) to permit this URL,
or
Take advantage of the wildcards !!!!

Using Wildcards

BrowseGate allows you to add an "*" (asterisk) character as either the first or last character (only) of a blocking entry. Please do not put one in the middle of an entry as it will not work as expected

This allows you to perform substring matches such as
microsoft
which WOULD match both **"www.microsoft.com"** AND **"searchengine.www.microsoft.com"**,
or
www.microsoft.*
which WOULD match both **"www.microsoft.com"** AND **"www.microsoft.co.uk"**, but NOT **"searchengine.www.microsoft.com"**

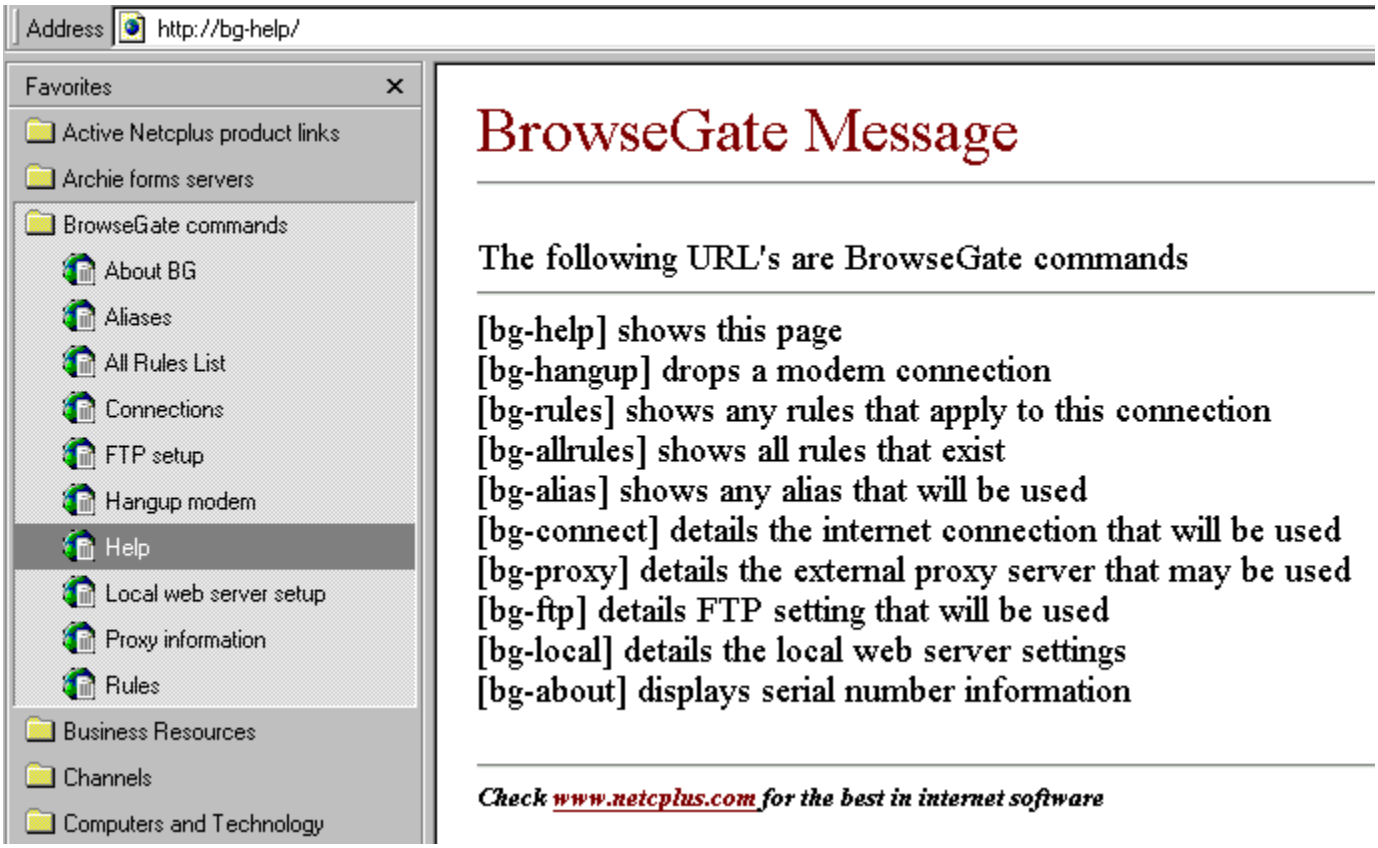
WARNING
Because many web sites collect data automatically from other sites, such as images, visitor counters and advertising links, you may well see one or more "error" message or blank image frames in your browsers when these URL's are requested by the pages being loaded. Typically these are the now familiar Java

script errors, or Unable to connect to site xxx.xxx.xxx messages. If for any reason you DO WANT to allow these links, you must add the relevant URL details into your list of allowed sites on this configuration tab.

In our example dialog, we have added an entry for ***fastlink*** to allow our own web page to display our visitor counter.

The screen shot below is just a suggestion for using the favorites menu in IE4 and Netscape for quick access to BrowseGate Commands

Click anywhere you see the hand icon for further information....



How to set up common internet/intranet applications

Detailed instruction are provided for all of the following applications :-

NB If you choose to use the Window's Machine name (NetBios name) to identify the BrowseGate PC in any of th efollowing configurations, you will need to go to Control Panel | Networks and install the Netbeui protocol in addition to TCP as the name resolution for Window's machine names is not available through TCP.

WEB BROWSERS
Microsoft Internet Explorer 3.xx
Microsoft Internet Explorer 4.xx
Microsoft Internet Explorer 5.xx
Netscape Navigator 4.xx

EMAIL CLIENTS
Outlook Express
Eudora
MS Exchange
Pegasus mail
Using the TCP Mapping feature for email connections

NNTP NEWS CLIENTS
Outlook Express
Forte Free Agent
Using the TCP Mapping feature for News

FTP CLIENTS
CuteFTP (v 1.8)
AbsoluteFTP (v 1 5)
WS-FTP (v 95LE)
FTP Explorer

SOCKS 4/5 CLIENTS
mIRC - Chat system
ICQ - Communications system
Absolute FTP
Yahoo Messenger
AOL 4 (and later)
Netscape AOL Messenger v3.xx
Microsoft Internet Explorer 4
Microsoft Internet Explorer 5

REAL PLAYER
RealPlayer

By unchecking this option you can disable all limitations on dial-up connections

If you check the "Keep on top" option, the BrowseGate window will remain on top of all other non topmost applications windows.

Limitations in Evaluation version.

This evaluation copy of BrowseGate allows you to run the program for up to 15 days before needing to register it. It allows you to have up to 5 users connected to it concurrently so that you are able to prove to yourself what BrowseGate can do for you.....

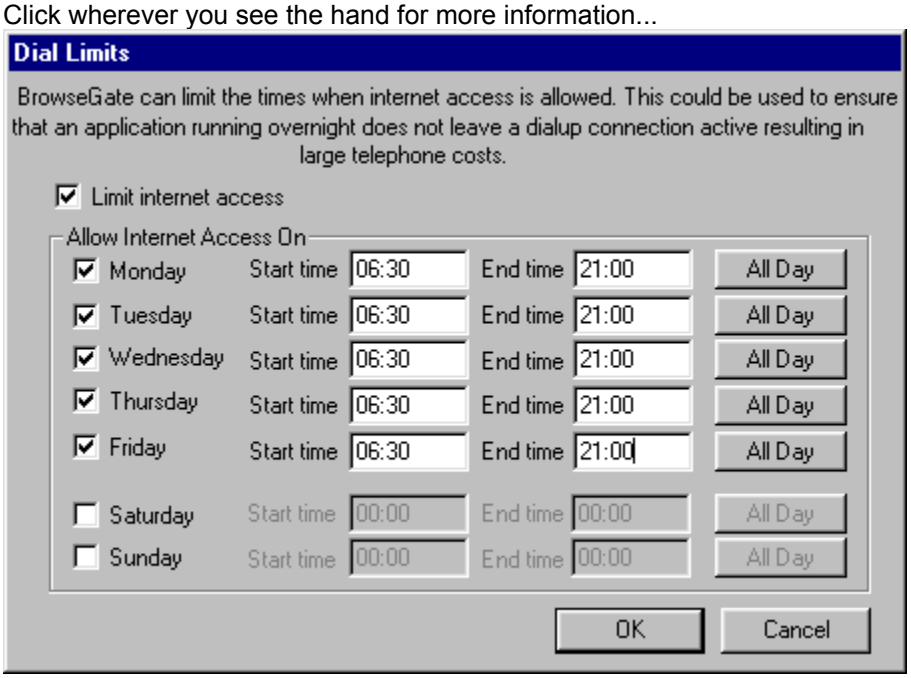
BrowseGate can be registered in multiples of 5 users to suit your own network requirements.

Limiting dialup access to specified times/days

See Also: Other Configuration tabs - click on tab shown below...

Aliasing | Downloads | Local Web | Blocking | Rules | Blacklist | Password | Cache | SNTP
Connect | Email | News | Map TCP | Map UDP | SOCKS4/5 | Realplayer | DNS | Ext.proxy | Options

Click wherever you see the hand for more information...



By clicking the "Limits..." button on the initial "Connect" tab of the BrowseGate configuration property sheet, the dialog shown above will be displayed.

If you are using a dial-up connection to the Internet, you will probably want to limit this access to certain days or times of certain days.

This is because of the problems that both Web Browser and Real Player "Channels" can cause, plus the inummerable "tickers" and other real time, Internet based facilities currently available that will make requests on a rather too regular basis for a connection to the Internet to enable them to update whatever data they are using.

BrowseGate puts you in control of your dial-up access by providing you with the ability to specify both the times between which, and the days on which, it will honor dial-up internet access requests to any of your networked users.

This means that you can easily enable or disable all internet access that may be provided by BrowseGate for any day of the week by simply checking or unchecking the relevant day, and you can also limit the hours between which BrowseGate will allow dial-up requests.

You can even disable these limits globally quickly and easily without losing the settings you have already entered (Great when the network

administrator has to work late....!!)

The option allows the server administrator to limit the amount and details contained in the information returned to a browser user when access to a site is refused due to blacklist entries, IP address etc.

If this option is checked, NO details are returned except a confirmation that BrowseGate has refused the requested web site.

This indicator shows you the currently selected entry and the total entries in the list you are editing.

TCP/IP ports - what you can use !!

For your Reference - the following is a pretty exhaustive
list of the standard TCP ports used by most external (Remote) hosts:

Most commonly used ports

```
Service     Port# Description
FTP         21    File Transfer Protocol - for transferring files
Telnet      23    for logging into an account on a Remote Host
SMTP        25    For Sending mail
Gopher      70    Text menu based browser
HTTP        80    WWW protocol - Netscape, Mosaic
POP 3       110   Downloading Mail
NNTP        119   Internet Newsgroups
IRC         6667  Internet Relay Chat
Compuserve  4144  Compuserve WinCIM communications
AOL         5190  America Online
MSN         569   Microsoft Network
```

Other Ports

```
# Format:
#
# <service name>  <port number>  [aliases...]   [#<comment>]
#

echo                7
discard             9     sink null
systat             11
systat             11     users
daytime            13
netstat            15
qotd               17     quote
chargen            19     ttytst source
ftp-data           20
telnet             23
time               37     timserver
name               42     nameserver
whois              43     nicname       # usually to sri-nic
domain             53     nameserver    # name-domain server
nameserver         53     domain        # name-domain server
mtp                57                   # deprecated
rje                77     netrjs
finger             79
link               87     ttylink
supdup             95
hostnames         101     hostname      # usually from sri-nic
iso-tsap          102
dictionary        103     webster
x400              103                   # ISO Mail
x400-snd          104
csnet-ns          105
pop               109     postoffice
pop2              109                   # Post Office
portmap           111
portmap           111/udp
sunrpc            111
auth              113     authentication
```

```
sftp              115
path              117
uucp-path         117
nbsession         139
NeWS              144     news
tcprepo           158     repository    # PCMAIL
print-srv         170                   # network PostScript
vmnet             175
vmnet0            400
exec              512
login             513
shell             514     cmd           # no passwords used
printer           515     spooler       # line printer spooler
efs               520                   # for LucasFilm
tempo             526     newdate
courier           530     rpc
conference        531     chat
rvd-control       531/udp    MIT disk
netnews           532     readnews
netwall           533/udp                  # -for emergency broadcasts
uucp              540     uucpd         # uucp daemon
klogin            543                   # Kerberos authenticated rlogin
kshell            544     cmd           # and remote shell
remotefs          556     rfs_server rfs# Brunhoff remote filesystem
garcon            600
maitrd            601
busboy            602
kerberos          750     kdc           # Kerberos authentication--tcp
kerberos_master   751                   # Kerberos authentication
krb_prop          754                   # Kerberos slave propagation
erlogin           888                   # Login and environment passing
kpop             1109                   # Pop with Kerberos
ingreslock       1524
knetd            2053                   # Kerberos de-multiplexor
eklogin          2105                   # Kerberos encrypted rlogin
rmt              5555     rmtd
mtb              5556     mtbd          # mtb backup
man              9535                   # remote man server
w                9536
mantst           9537                   # remote man server, testing
bnews           10000
queue           10001
poker           10002
gateway         10003
remp            10004
qmaster         10012
```

This is a full list of any additional proxy connections (TCP mappings)
you may have configured.

Click on any one and press the edit button below the list to change the settings.
You will see that the entry includes details of the host to be connected to, plus
the local port number to be used to connect with any network client that wishes
to use this connection.

This is a list of local IP addresses which should contain a
name and IP address for each and every PC on the network
that is using BrowseGate.

WARNING - If you have entered a domain name in the Window's
TCP/IP settings on the TCP/IP->Dial-up adaptor tab of the Network
property sheet, then you will need to add this in each of your aliases
otherwise they will not get resolved correctly by the BrowseGate
internal DNS system.

eg:
With no Domain entry.....
Server alias : Myproxyserver

With a Domain entry of "SalesGroup".....
Server alias : Myproxyserver.salesgroup

This is because Windows will automatically append any domain name
to each and every DNS request in this same format...

See Also: How to access the local web site

Enter, or browse for the drive and directory of the "home.htm" or "index.htm" page of the web site you want to make available via BrowseGate to your intranet/networked users.

Because many web sites have differing names for the base page, you can enter the correct name of the page you wish BrowseGate to provide as the Home page. (This can be any existing page in the directory you have specified)

This option is only for debugging purposes, and unless asked to do so by our Support staff we recommend that you do not check this. A low level and highly detailed communications file is generated which can grow very large - very rapidly, and it will also adversely effect the performance our your proxy operations.

However, BrowseGate automatically generates a daily activity log report that gives you a full trace of all server activity. A separate log file is created for each day of the week (Mon - Sun) and these are placed in a special \BGLOGS subdirectory in the BrowseGate installation directory on your hard disk. These log files are also used by the Statistics feature to summarize the throughput.
You cannot turn this daily logging off !!

To view these logs at any time, you can use any web browser that is connected to BrowseGate by typing the following URL into that browser :

BG-LOG

This will generate a clickable list of all the currently available log files with their dates, and you can click on whichever log file you wish to view in your browsers window.

These logs contain detailed entries including information whenever a request has to be refused by BrowseGate so that you can check how your rules are working and which networked PC is attempting to perform these "banned" tasks.

If, which is most unlikely, you need a low level log of server activity for debug purposes, you can create one by selecting the Configure button on the main BrowseGate window, and then checking the "Keep log file" option on the Connections tab.

This is normally only ever needed if you are asked to do so by a member of the technical support staff.

The log file generated is highly detailed, and can
get very large very rapidly....

We strongly recommend that you do not check this option unless asked to do so by our support personnel, and that you always uncheck it again as soon as you are able to do so.

This panel shows the current connection status when BroweGate is configured to be used as a dial-up gateway. It will show "Disconnected" when not on-line, but when a connection is active, it will indicate the time left before BrowseGate will disconnect the dial-up connection automatically in MM:SS format.

If checked, the News proxy will be available to your networked users to access the NNTP news system.

Other configured Favorites folders

Output of the highlighted Help command...

Some FTP servers, particularly those on private networks, may require that you use Passive FTP. Try changing the setting of this check box if you encounter a web site that does not respond.

Protocols active status

See also: Discussion on Ports

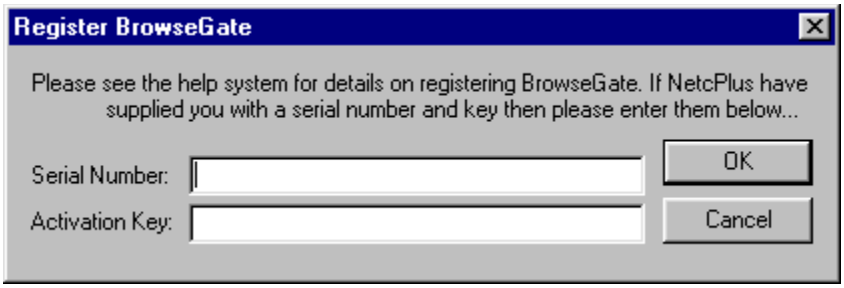
These four indicators show you which of the available protocols (HTTP, POP3, SMTP, NNTP) are active or inactive whenever BrowseGate is running. The HTTP should always be active, but the other three may display a red (Inactive) LED icon even thought you have them activated in the configuration property sheet. This may be because BrowseGate has identified a port conflict when it was started.

If you have enabled one of these protocols and expect it to be active, but it is shown with the red icon, this is almost certainly the problem. To overcome this, check the status window which should be reporting "Error - could not open port xx - yyyy Service suspended". If so, you need to identify what other application is using the selected port and adjust the settings in it or BrowseGate so that no clash exists.

When any particular protocol is actually being used, you will notice that the GREEN LED will flicker to indicate this activity !

Clicking the Register button will load the registration dialog that lets you enter the serial number and key that is provided to you once you have paid for your copy of BrowseGate.

Registering BrowseGate



Simply enter the serial number and activation key provided to you when you registered and paid for your copy of BrowseGate with NetcPlus in the fields above.

Please ensure that you take great care with the activation key as each letter is case sensitive, and the complete entry will be refused if you do not enter it correctly.

Routing for advanced networks

This is the run-down on route tables for multi-homed hosts (more than one interface).

Interface

An interface is a logical interface associated with a piece of communications hardware that has a TCP/IP stack. These bits of hardware include things like Modems, ethernet cards, ethernet interfaces on a router etc. The logical interface always has an IP address associated with it. These IP addresses must be unique within any connected network.

Route tables

When you want to make a TCP/IP connection, or just send some packets to a machine, you have to figure out which interface to send the packets out of. It is obviously no good sending packets out your LAN adapter when you are trying to say connect to an internet site. Conversely, it is no good sending packets out your modem when you are trying to access a machine on your LAN.

For this reason there are routing tables. The routing table is a table that the TCP/IP stack looks at when it wants to send a packet somewhere, and the routing table tells the stack which interface to pump the packets out of in order to get to the desired destination.

So route table entries specify:

1. A range of destinations (made up by network address / subnet mask - see later)
2. Which router (gateway) to send packets to for these destinations.
3. Which interface to send packets out to get to these destinations

in Win95, the syntax to check the current routing table is just :-

```
route
```

and to ADD a new entry to the routing table is :-

```
route ADD networkaddr MASK subnetmask gateway
```

subnetmask is a way of saying which bits to ignore in the address when checking for a match. So if the subnetmask is 255.255.255.0 then we ignore the last 8 bits of the address (last octet) when checking to see if this route table entry applies to the destination or not.

E.g.

This is a route table when online with my modem

Active Routes:

Network Address	Netmask	Gateway Address	Interface	Metric
0.0.0.0	0.0.0.0	203.96.10.254	03.96.10.51	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.0.0	255.255.0.0	192.168.0.4	192.168.0.4	2
192.168.0.4	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.0.255	255.255.255.255	192.168.0.4	192.168.0.4	1
203.96.10.0	255.255.255.0	203.96.10.51	203.96.10.51	1

203.96.10.51 255.255.255.255 127.0.0.1 127.0.0.1 1
203.96.10.255 255.255.255.255 203.96.10.51 203.96.10.51 1
224.0.0.0 224.0.0.0 203.96.10.51 203.96.10.5 1

224.0.0.0 224.0.0.0 192.168.0.4 192.168.0.4
1
255.255.255.255 255.255.255.255 192.168.0.4 192.168.0.4
1

I have 2 interfaces on my box - a LAN adapter with IP address 192.168.0.4 and a modem PPP interface with address 203.96.10.51

You will see that there is an entry in the table for both of these, plus some others.

If we look at the 4th entry, that is the definition of the entry for the LAN card. What it is saying is that if we get a packet that we want to send to 192.168.0.4 MASK 255.255.255.255 (which means that it must match the whole address), then we send the packet over interface 192.168.0.4 - the gateway is ignored. That is the easy one.

The next significant one is the 3rd entry. That is saying that if we have a packet for 192.168.0.0 MASK 255.255.0.0 (that means anything from 192.168.0.1 to 192.168.254.254 since 255 is reserved as is 0) then we send it out interface 192.168.0.4 - so this means all our LAN traffic goes out of the LAN card.

By comparison, the 7th entry is the same as the 4th entry, but for the PPP interface (modem) and the 6th entry is the same as the 3rd entry, but applies to the range 203.96.10.1 to 203.96.10.254 which is a subnet on our service provider. This will probably give us access to their router.

The other VERY significant entry is the 1st one. The effect of having a destination of 0.0.0.0 with MASK 0.0.0.0 means any IP address at all. This is called the DEFAULT ROUTE. This one is the last route used if there is no match on the others. This is the one that causes problems in multi-segment networks when you dial up, because it is changed by the PPP login process. What this means is that if we don't have a static route (like the other entries) for a destination, we send it out over the default route to 203.96.10.254 (our ISPs router) which is accessible through the interface 203.96.10.51 (our modem).

What this is saying, is that everything goes out over our modem, except things that match a static route - so this includes our LAN (local subnet only).

The other entries are.

127.0.0.0 is the localhost (loopback interface) this is a software only interface internal to the stack itself, and is not accessible over any interface. This means that this interface can only be accessed from the machine itself.

192.168.0.255 is the broadcast address for broadcast packets on our LAN. 203.96.10.255 is the broadcast address for broadcast packets on the LAN segment on our ISP.

224.0.0.0 is another broadcast (or perhaps multicast) address on both our LAN and the ISPs

LAN. The effect of two matching entries means any packets sent to this destination will be broadcast on our LAN and the ISPs LAN.

255.255.255.255 is the global broadcast address.

Route table when off-line

Active Routes:

Network Address	Netmask	Gateway Address	Interface	Metric
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.0.0	255.255.0.0	192.168.0.4	192.168.0.4	1
192.168.0.4	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.0.255	255.255.255.255	192.168.0.4	192.168.0.4	1
224.0.0.0	224.0.0.0	192.168.0.4	192.168.0.4	1
255.255.255.255	255.255.255.255	192.168.0.4	192.168.0.4	1

So these are all the same except for the PPP interface addresses, since we are off-line there is no PPP interface.

Routes automatically created by the OS

There are a number of routes created automatically by the OS. Whenever an interface is added, you get a route for the interface, one for the subnet the interface is on, and one for the broadcast address for that interface. If you look at the route table above, the interface 192.168.0.4 results in the addition of route entries 2, 3, 4, 5 and 6.

The OS also creates the localhost interface (1st one).

Important

If you specify a default gateway for your LAN adapter (i.e you have a router on your LAN), then you also get a default route entry. this is the entry that is used to access the other subnets on your LAN.

What this all means

Well, what it means is that your PPP login when it changes your default route. So by default all your packets go to your ISPs router (so you can access internet sites). This makes the rest of your LAN segments inaccessible, since unless you have manually entered a static route to those subnets, they will have been dependent on the default route.

So, if you have other subnets, you need to add a static route to your route table with the ROUTE ADD command.

You can be smart about it. if you have numbered your segments say like this:

Segment A (BrowseGate machine): 192.168.0.0 mask 255.255.255.0
(this means 192.168.0.1 to 192.168.0.254)
Segment B : 192.168.1.0 mask 255.255.255.0
Segment C : 192.168.2.0 mask 255.255.255.0
Segment D : 192.168.3.0 mask 255.255.255.0
Segment E : 192.168.4.0 mask 255.255.255.0
Segment F : 192.168.5.0 mask 255.255.255.0
Segment G : 192.168.6.0 mask 255.255.255.0
and the router is on 192.168.0.254

Then you can either do it the hard way and add a route for each of B to F - e.g.

route ADD 192.168.1.0 MASK 255.255.255.0 192.168.0.254
route ADD 192.168.2.0 MASK 255.255.255.0 192.168.0.254
route ADD 192.168.3.0 MASK 255.255.255.0 192.168.0.254
route ADD 192.168.4.0 MASK 255.255.255.0 192.168.0.254
route ADD 192.168.5.0 MASK 255.255.255.0 192.168.0.254
route ADD 192.168.6.0 MASK 255.255.255.0 192.168.0.254

Or, you could combine these to a single entry by setting the mask to ignore the second to last octet of the address as well.

e.g

route ADD 192.168.0.0 MASK 255.255.0.0 192.168.0.254

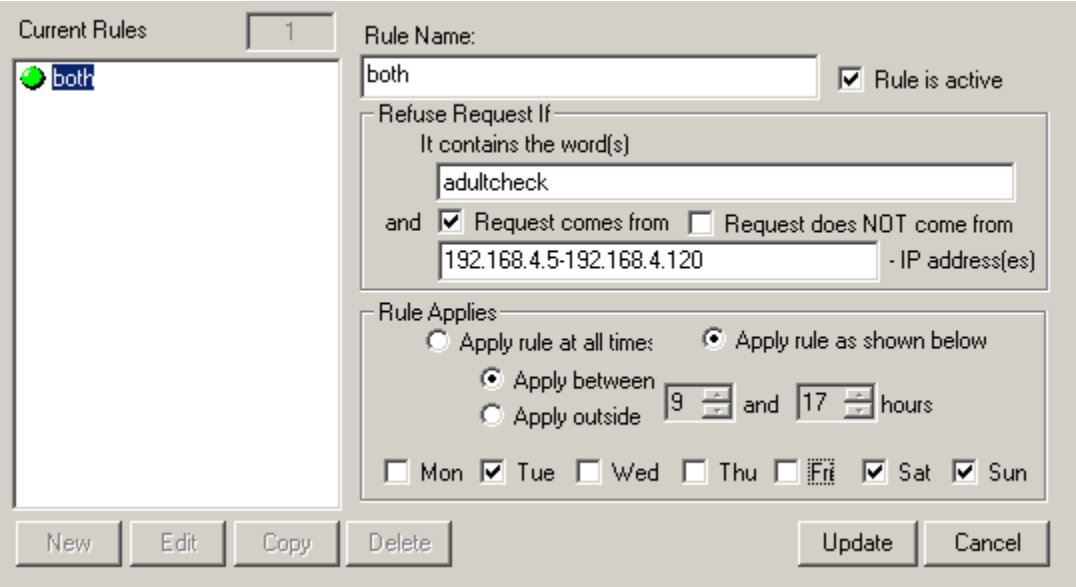
This would cover segments B to F.

If some of the segments B to F are only accessible through another router somewhere else, you can either add route statements to the router on 192.168.0.254 or put in different route table entries for these ones.

When matching, the stack looks for a match in this sequence.

1. Look for a match with an interface address (mask of 255.255.255.255 - exact address)
2. Look for a match with a subnet
3. use the default route.

BrowseGate offers very powerful Rules to either stop or allow certain of your network's machines to access various web sites.



Three fields are provided, the first for the Rule name,and then one for one or more words, the other for single or ranges of IP addresses.
if required, you can use just words, just ip address(s) or both, and you can specify that the IP address(s) are to either be matched (inclusive) or not be matched (exclusive) before the rule is applied....

Rule Name
This is provided solely to let you give each rule a "human readable name" This name is displayed in the refusal page in the requesting web browser when access is denied if you have this option enabled in BrowseGate.

Field 1. It contains the word(s)
You can enter one (or more) words in this field, and any URL that contains any of these words anywhere in them will (potentially) be banned. As in our example above, if a request is received by BrowseGate to connect to a URL of say :

http:www.adultchecksystem.com/home.htm

then because we have the word "adultcheck" in this field, BrowseGate would ban access to it due to the word "adultcheck" matching in "adultchecksystem"

These words are not case sensitive, so any combination of upper and lower case letters will still be matched by the BrowseGate rules control system.

You can also enter multiple words (up to 1024 characters per entry are allowed) providing that you leave at lease one space or insert a comma between each individual word. This means that you can set up a single rule that would stop access to most sex sites with an entry such as shown below :-

sex porn, xxx fetish , adult girl boy hot woman,foot

This gives you the maximum control over your network user's web access using potentially only a few rules....

1a. Stopping HTTP/FTP downloads
If you want to stop all of your networked web browser users from being able to download files from web sites that use the newer http://xxxxx form of FTP file downloading, you can do so easily by simply setting up a new entry on the "Rules" tab that contain the file suffixes of those files you wish to stop being

downloaded wit a space between each one.

In this case for security the entries MUST include the leading period - for example, a typical rule to stop downloads of
common files types might contain the following line:

.EXE .COM .TAR .ZIP .GZ
This would automatically ban any URL that contained a filename which included any of the above 5 common download types.

USING THE IP ADDRESS FIELD

Option box. Request comes from
If this is checked, AND if you have entered an IP address or range in the field below, then these are also checked by the BrowseGate Rules system. This works by first checking to see if there is a match on any of the word(s) you have entered in the first field, and then it also will check to see if the IP address of the requesting computer ALSO matches the single or range of IP address(s) entered. **ONLY IF both match will access be refused.**

Option box. Request does not come from
If this is checked, AND if you have entered an IP address or range in the field below, then these are also checked by the BrowseGate Rules system. This works by first checking to see if there is a match on any of the word(s) you have entered in the first field, and then it also will check to see if the IP address of the requesting computer DOES NOT match the single or range of IP address(s) entered. **ONLY IF a word DOES match and the ip address DOES NOT MATCH will access be refused.**

2a. How to use the ip address field

BrowseGate lets you enter ip addresses in many different formats to allow you th emaximum flexibilty in using the Rules.
the following formats are permitted :-

we have used arbitrary numbering as examples, and these could all be different in your installation.

192.168.4.100 - a single ip address
Self explanatory, but itmust consist of all 4 octets to be valid
192.168.4.* - a single ip address with "wildcard" as last octet
The first three octets must be matched exactly,
but any value is accepted as matching for the fourth octet.
192.*.4.* - a single ip address with two "wildcards" in 2nd and 4th octets
The first and third octets must be matched exactly,
but any value is accepted as matching for the second and fourth octets.
192.168.4.100-192.168.4.250 - a range of ip addresses
Any addresses in the entire range shown will match
NB: You cannot use wildcards (*) in ranges.
It is also illegal to use different values for any BUT the last set of octets eg:
192.168.**4**.100-192.168.**4**.250 is a completely valid range
192.168.**4**.100-192.168.**6**.250 is NOT a valid range due to the "6" in the third octet of the 2nd ip address

Specifying computers to be blocked
If you only want any particular Rule to apply to a single computer, then just enter that computers IP address in the second field and select the "Request comes from" option above it.

If you want to **block an entire range of IP addresses**, you can enter into the "comes from machine" field

an IP address that contains one or more asterisks eg : 192.168.4.* which would immediately stop all and any computers with any IP addresses in the range 192.168.4.0 thru 192.168.4.255 from accessing the web via BrowseGate.

You can also **block a limited range of IP addresses** by entering a range of IP addresses into field in the following format :- 192.165.1.1-192.168.4.45
This will stop all and any computers with any of the IP addresses in the range 192.165.1.1 to 192.165.1.45 from accessing BrowseGate to access the web.

You should bear in mind that by use of the "Request is from" and "request is NOT from" options, it is easy to set up very powerful rules.
For example, a rule that specified one or more words plus an ip range such as 192.168.4.1-192.168.4.50 would normally simply block all computers with an ip address in the range specified. However, if you were to check the "Request is NOT from" option, then all machines that DO NOT HAVE an ip address in that range will be banned from accessing that web site. Thsi would mean any computer with an ip address from 1.1.1.1. to 192.168.1.0 and also 192.168.4.46 thru 999.999.999.999 would be banned by BrowseGate by this Rule (rather a lot of computers)

Rule Applies
These options allow you to specify that any rule is to be applied either at all times (permanent block) or only between certain hours of the day and/or on certain days of the week. This allows you to control which networked computers in your business are permitted or blocked from accessing the web, and between which hours, which enables you to control which staff can browse for their own private reasons or not.

Possible scenarios are to disable some ranges of PC's during the standard lunch hours or at any time out of standard office hours, but to still allow others access at all times, or to allow other ranges to be controlled by a different rule.

Check or uncheck this to activate/disable the selected rule

Apply Rule at all times
If checked, this rule will always be applied.
Apply Between
If checked, this rule will only be applied between the hours specified.
Apply outside
If checked, this rule will only be applied outside of the hours specified.
Days of week.
Check each day that you want the selections above to be applied on.

If you add or edit a Rule, you MUST press the UPDATE button to save that entry...

Each rule must be given some "human readable" name. This name should of course be unique.

This page shows the contents of the file SETUPINFO.WRI for you convenience

BrowseGate Proxy server v 2.70

We recommend that you print this file out for reference while you complete the installation of your BrowseGate proxy server...

Installation and setup guidance.

Despite BrowseGate being a very powerful network/intranet proxy server, it is really quite simple to install and configure, providing you follow a few basic rules that will certainly be familiar to any of you that understand TCP/IP networking, but may be less obvious to those of you who are fairly new to TCP/IP networking.

These notes are aimed primarily at those who are not too familiar with TCP/IP on Windows PC's, and we therefore ask for the forbearance of those for whom some of the following information may appear to be blatantly obvious.....

The Help System provided with BrowseGate contains a great deal of information on how to setup TCP/IP networking, so we recommend that you first have a look through this for any information you may require. These notes will hopefully give you a quick reference to reach the relevant areas in the BrowseGate Help System.

FINALLY - DON'T DESPAIR !!!! It really is quite simple once you get stuck into it. Most customers report to us that they usually have BrowseGate configured and all the basic proxy clients up and running in less than an hour or so..... So go for it NOW !!!!!!

If you REALLY are stuck, then you can always send an email to our tech support people. They love a challenge, and are sure to be able to put you right quickly and easily. They will usually get back to you on the same day.

However, if you are having problems with the configuration of Windows itself - PLEASE CONTACT the Microsoft support group and not our own people. Microsoft are responsible for providing you with technical support on setting up any Windows components themselves....

We are more than happy to provide you with unlimited and free email support for life -
But can only do so for current registered releases of our own software.

##
1 - Finished the BrowseGate Installation

To be reading this you must have already installed BrowseGate :-))

The only things you may have setup in the initial configuration is the HTTP port to be used by BrowseGate, and the DUN/RAS options to connect with your modem system.

Now you are wondering what you should do next ???

These notes assume that you already have your Windows network and TCP/IP networking installed. If not, please read the Help System provided in your version of Windows. The sections shown below in the BrowseGate Help System, which are accessible from the main Contents page, may also be helpful.

General Technical information
What to do if your networked PC's cannot connect to BrowseGate
How to set up TCP/IP on your network

If you want an overview of the most important TCP/IP configuration items, check out the following Help Topics :-

General Technical information
Ports - What are they and how do you configure them ?
What to do if your networked PC's cannot connect to BrowseGate
All About TCP/IP etc
About the Windows HOSTS file

##

2 - What networked internet applications do you want to support ?

BrowseGate will act successfully as a proxy server for almost all types of internet applications, but naturally enough you need to configure it to provide the various types of support your networked users are going to require.

To find out how to set up proxies for any of these :-
Check the information given in the Help System under the sub heading of:-

Configuration

Web browsing
WEB BROWSERS - setting the communications port

Email clients or servers (POP3 and SMTP)
EMAIL -supporting the POP3/SMTP email service

NNTP Internet News Clients
News - supporting the NNTP news service

FTP Client applications
TCP MAPPING - support for additional proxy services

Other Client applications
TCP MAPPING - support

SOCKS 4/5 client applications
SOCKS SERVICE - support for the SOCKS protocol

##
3 - How to set up your client applications

Most email, news, FTP and similar clients have their own help systems that should provide information on what you need to do to make them work with BrowseGate. This will typically be found under the headings of either PROXY or FIREWALL in those help systems.

The BrowseGate Help system also contains detailed information on how to configure many of the most popular internet applications to work with a proxy server - (Just in case you are unable to find the information you need in their own help systems)

These include instruction for all of the following applications at the time of writing.

Microsoft Internet Explorer 4.xx and 5.xx
Netscape Navigator 4.xx

Absolute FTP
CuteFTP
WS_FTP
Microsoft Outlook (and Express)
Qualcomm Eudora
MS Exchange
Pegasus mail
Forte Free Agent

Please check out the following BrowseGate Help Topics :-

Configuration
Configuring SOCKS applications to use BrowseGate

Setting up your network clients to use BrowseGate
Setting up your web browsers to connect to BrowseGate
Configuring your eMail clients to connect to BrowseGate
Configuring NNTP News clients to connect to BrowseGate
Configuring common FTP clients to use BrowseGate

##

The rest of the BrowseGate configuration is slightly more advanced, but a quick browse through the Help system should be all you need to sort it all out.

April 1999
Support Group
NetcPlus Internet Solutions.

If you uncheck this option, it will disable the time checking performed by BrowseGate entirely.

Press OK to save any changes, Cancel to discard any changes
The Help button brings you this help page.....

To test the SNTP support, or to test for the existence of a different time server from the list provided, you can check this option, which will ALWAYS display a windows message box to either confirm that the PC's clock has been reset, or that a connection to the server failed.

If a server does fail to respond, you may have to wait up to 90 seconds or so before the "failure" message box is displayed.....

This option is only for debugging, and should normally be **UNCHECKED**

SNTP test button

Sample full status report

Below is shown a full status report on a working BrowseGate system...

```
NetcPlus - BrowseGate Proxy Server
==================================
Full Server status report
-------------------------

Configuration password is set to [iant]
BrowseGate Window is Not OnTop
BrowseGate Window is displayed on startup

External Connections
--------------------
DUN/RAS is in use for external connections
Dialup connection in use is [Virgin net]
Connection will be hung up after [10] minutes inactivity
Connection will NOT be hung up when BrowseGate is closed down
BrowseGate will attempt 3 dial retries

External caching
----------------
The use of an external cache is OFF
The use of an external cache is OFF
External cache is set to [www-cache.demon.co.uk]
External is set to use port [8080]

URL Aliasing
------------
URL aliasing is OFF
Alias 1 is set to [*.com]
Alias 2 is set to [*.net]
Alias 3 is set to [www.*.com]
Alias 4 is set to [www.*.net]
Alias 5 is set to [*co.uk]

Browser File Downloads
----------------------
Downloading of files via browser based FTP requests is ON
FTP user ID is set to [ftp]
FTP password is set to [wwwuser@here.com]

POP3/SMTP Mail support
----------------------
eMail proxy is ON
POP3 email requests will be sent to [pop3.ps-consultants.co.uk]
Local port for POP3 client applications is port [650]
POP3 request will connect externally on port [110]
SMTP email requests will be sent to [smtp.ps-consultants.co.uk]
Local port for SMTP client applications is port [26]
SMTP requests will connect externally on port [25]

NNTP News Support
-----------------
NNTP News proxy is ON
```

News Server requests will be sent to [news.virgin.net]
Local port for News Server client applications is port [121]
News Server requests will connect externally on port [119]

Additional services (proxies) Support

Proxy service 0 connects to [news.demon.co.uk] on port 119
    Local port for client connections to use this proxy is [123]
    This proxy service is ACTIVE
Proxy service 1 connects to [mail.virgin.net] on port 110
    Local port for client connections to use this proxy is [151]
    This proxy service is ACTIVE
Proxy service 2 connects to [pop.site.csi.com] on port 110
    Local port for client connections to use this proxy is [153]
    This proxy service is NOT Active
Proxy service 3 connects to [pop3.demon.co.uk] on port 110
    Local port for client connections to use this proxy is [154]
    This proxy service is ACTIVE
Proxy service 4 connects to [pop.freeserve.net] on port 110
    Local port for client connections to use this proxy is [155]
    This proxy service is ACTIVE
Proxy service 5 connects to [mailhost.airtime.co.uk] on port 110
    Local port for client connections to use this proxy is [152]
    This proxy service is ACTIVE
Proxy service 6 connects to [pop3.ps-consultants.co.uk] on port 110
    Local port for client connections to use this proxy is [111]
    This proxy service is ACTIVE
Proxy service 7 connects to [192.168.4.3] on port 25
    Local port for client connections to use this proxy is [666]
    This proxy service is ACTIVE
Proxy service 8 connects to [192.168.4.3] on port 110
    Local port for client connections to use this proxy is [667]
    This proxy service is ACTIVE
Proxy service 9 is an FTP client proxy connecting externally on port 21
    Local port for client connections to use this proxy is [680]
    This proxy service is ACTIVE
Proxy service 10 connects to [mail.virgin.net] on port 110
    Local port for client connections to use this proxy is [690]
    This proxy service is ACTIVE
Proxy service 11 connects to [mail.virgin.net] on port 25
    Local port for client connections to use this proxy is [691]
    This proxy service is ACTIVE

URL Rules

Rule 1 - [Sex sites] is NOT Active
- Bans entries containing the following words :
- porn girl sex , pussy photo sxx erotic , voyeur
- Ban is applied at following times:
- Between the hours of 6 and 20 on the following days :
- Sun Mon Tue Wed Thu Fri

Rule 2 - [sex2] is NOT Active
- Bans entries containing the following words :
- girl fanny sex sxx whore woman fetish
- Ban is applied at following times:

- Between the hours of 9 and 17 on the following days :
- Sun Mon Tue Wed Thu Fri

Rule 3 - [Adult stuff] is NOT Active
- Bans entries containing the following words :
- adult
- Ban is applied at ALL TIMES

Rule 4 - [file download blocker] is NOT Active
- Bans entries containing the following words :
- .exe .zip .gz .tar leader.linkexchange.com
- Ban is applied at ALL TIMES

Rule 5 - [Linkexchange blocker] is NOT Active
- Bans entries containing the following words :
- linkexchange
- Ban is applied at ALL TIMES

Rule 6 - [web image blocker] is NOT Active
- Bans entries containing the following words :
- .gif .jpg
- Ban is applied at ALL TIMES

Site Blocking

Site Blocking is NOT Active
Site 1 allowed is [www.netcplus.com]
Site 2 allowed is [www.proxy-servers.com]
Site 3 allowed is [www.email-servers.com]
Site 4 allowed is [search.microsoft.com]
Site 5 allowed is [www.microsoft.com]
Site 6 allowed is [*shareware*]
Site 7 allowed is [*fastlink*]
Site 8 allowed is [*microsoft*]

Black Listing

Use of Blacklisted URL'S is on STRICTLY
The following sites are EXCLUDED from URL blacklisting :
192.168.4.1

Use of Blacklisted WORDS is on (but not STRICTLY)
The following sites are EXCLUDED from WORDS blacklisting :
192.168.4.1

Local Server

The following local (network) web site is supported
C:\netc web sites\Public Web Site
The default home page for this site is [home.htm]

BrowseGate can be configured to work via a standard Windows Dial up networking connection, or via a direct connection to any other server via a direct TCP link. Select the connection type you want to use here.

To enable PNA support, check this option, and then select the port you wish to use with it.

Use the spin buttons, or type in a value (in Megabytes) that is the maximum amount of disk space you want the BrowseGate cache system to use on the specifed hard disk.

BrowseGate allows you to specify how often any of the cached items are checked for currency with the actual web site(s) to ensure you have the latest copy of the data.

Never - If a cached page exists it is always used and never checked for currency.
Older than xx days - Only if any requested page or item is older than the number of days you have specified will the Internet site will be checked for a newer version.
Always - All cached items are checked for currency each time they are requested.

Use this field to enter the port number to be used for SOCKS communication

Unless you have a very good reason to do so, we recommend that you should leave this set to the default value of 1080.

In this field you should enter the number of the TCP/IP port you want to use to allow each of the web browsers (that are using HTTP and/or HTTPS protocols) on your network to connect with BrowseGate. The standard default port is set to 80, but you may change this if you wish to or have a good reason for needing to do so.

Please remember that each of the web browsers on your network will also need to be reconfigured to use the SAME port number you set here.

Setting the HTTP port

In this field you should enter the number of the TCP/IP port you want to use to allow each of the web browsers (that are using HTTP and/or HTTPS protocols) on your network to connect with BrowseGate. The standard default port is set to 80, but you may change this if you wish to or have a good reason for needing to do so.

Please remember that each of the web browsers on your network will also need to be reconfigured to use the SAME port number you set here.

Setting the cache size

We recommend that for maximum efficiency you allow sufficient hard disk space to be able to allocate a maximum disk cache size of at least 10Mb per typical single PC that will use it's web browser via BrowseGate. What this means in a typical environment is that you need to multiply this cache maximum cache size by at least the number of users you have accessing the web via BrowseGate to gain the maximum benefit from the cacheing system. eg: a 5 user BrowseGate should have 50Mb of cache space available.

If you are unable to allocate sufficient disk space to the cacheing system, you will probably find that it will spend rather too much time refreshing and then removing files, and you will loose any benefits you may have gained from the use of cacheing in the first place..

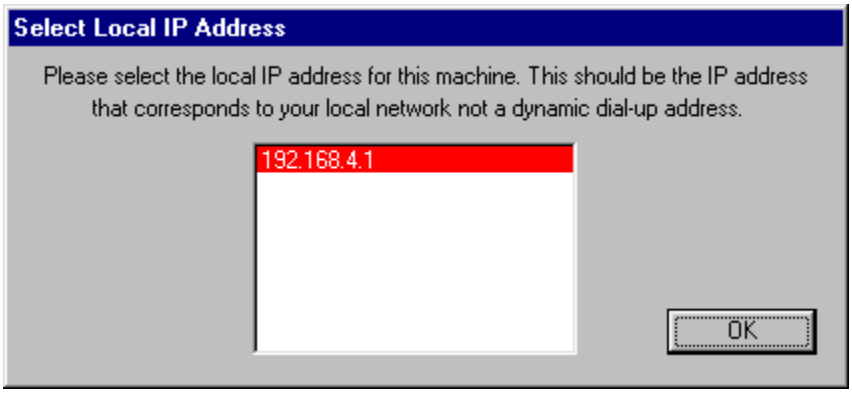
However, If all your web users tend to visit much the same sites, then you do not need to use this multiplier as BrowseGate will only ever cache any web site exactly once....., not once for each user that may access it.

Setting the local machines IP address

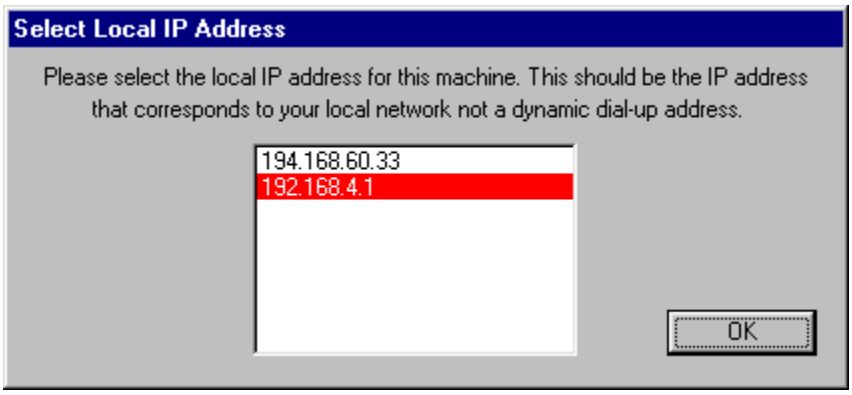
Because BrowseGate has to negotiate with both fixed and dynamically assigned IP addresses when connected to the Internet, plus communicating with other networked machines, BrowseGate needs to ensure that it knows the internal/network IP address of the machine it is running on because the Windows implementation of the Winsock cannot identify this information at all times,

You may well never ever see this dialog or have any need to look at it, as In most situations BrowseGate will do this totally automatically, but if you select the "View | Select local IP address" menu option a dialog as shown below is displayed.

In this example it can be seen that there is only a single Internet Class "C" IP address of 192.168.4.1, which has been selected automatically, which means that this MUST be the IP address of the local machine.



However, once you dial out or otherwise connect to the Internet you will normally see entries similar to those shown below, where a new IP address of 194.168.60.33 has appeared and been inserted into the list. Providing BrowseGate has already been able to identify the local machine automatically, it will simply highlight the correct entry automatically as shown below. You do not need to do anything more.....



There are however, more complex scenarios where it may be necessary for the system administrator to physically identify and specify to BrowseGate which of several available/listed IP addresses is actually the correct one for the PC on which BrowseGate is running.

Typically this is when a PC has more than one network card (NIC) installed (multi-hosted systems), or if it is fortunate enough to be connected to an ASDL connection. In these cases, if you do not actually have a note of the IP address of the BrowseGate PC, you will need to identify the correct IP address by going to the Windows Start Menu, and then selecting Settings | Networks, and finally checking the entries on the relevant TCP/IP entry for the correct "internal/networking" adaptor (NIC) and then select this address

in the list provided by BrowseGate.

You should normally only ever need to do this once as BrowseGate automatically stores the information for later reuse. If you happen to change the IP address of the PC, then you will of course also need to reset this in this BrowseGate configuration option.

Setting up FTP Explorer

FTP Explorer (We configured the version 1 .00 Build 010) does not appear to support totally global configuration of the use of a proxy server/firewall. Therefore the notes below must be applied to each and every FTP connection you use, at least the first time you wish to connect to that site via BrowseGate.....

1. Start FTP EXPLORER
2. Select View | Options and then select the FireWall Tab
3. Check the "Use Firewall" option
4. Ensure you check the"Use PASV Mode"
5. Ensure you check the "Use Firewall" option
5. Enter the host name or ip address of the BrowseGate PC in the "Host" field.
6. Set the Port to the same value as the local port of any assigned FTP connection in BrowseGate.
8. Ensure you select the "USER user@hostname " option for firewall type.
11. Click the OK button to close the options properties dialog.

Don't forget that each time you choose a new or existing connection from the "Connect" dialog under FTP EXPLORER, you should check that both the "Use PASV Mode" and the "Use Firewall" options on the right hand side are checked.

The port should typically be left at port 21, as the main firewall setting holds the local port for BrowseGate.

How to set up Internet access limitations

Check each and every day that you want BrowseGate to provide dialup access to the Internet, ensuring that any days on which you do not want it to allow this are unchecked.

If you want to allow 24 hour access, you can click the "All Day" button, which will set both start and end times to 00:00, which BrowseGate recognizes automatically as meaning that you want to provide dial-up access for the entire 24 period of that day.

If you want to set start and end times, simply enter the relevant time in the fields provided in the standard time format of HH:MM. BrowseGate will also let you enter a period between the hours and minutes if you prefer.

To disable all limits entries, uncheck the "Limit Internet access" option, which will preserve your current settings, but will still allow unlimited access until you recheck this option.

The settings you need to enter for an extra service entry are quite straightforward for most connections

FTP connections (Firewall).
Handling FTP connections is slightly more complex than most other connections, as BrowseGate is actually acting as a "FireWall", and has to perform some special handling of these types of connections.

You must first ensure that you check the "THIS IS AN FTP SERVICE" option to let BrowseGate know this is an FTP connection via a firewall.

This will disable the host name field as it is not used for connections from FTP client packages. BrowseGate automatically allocates each FTP connection the name of "FTP Service (xxx)" where (xxx) is the local port you have assigned to be used. The local port is the port number that will be used for all communications between BrowseGate and the FTP client package that wishes to access this extra connection. This means that you must configure your FTP client application(s) to use this same port number (and like any other "Service" you can use any available port number you wish for local ports).

The "Service Active" check box allows you to enable/disable any TCP port mapping you have set up, but you can also more easily just double click on an entry on the list to achieve this.

You will also need to configure your FTP client to work through a firewall, and select the host + password option.

Once you have added or edited an entry, please ensure that you click the Update button. You also must click the main OK button before any changes will be saved to the configuration system. Pressing Cancel will discard all changes made...

All other "pass through" connections
The host name is the usual name of the mail host or news server machine in exactly the same way as you might enter it into a mail or news client. The **local port** is the port number that will be used for all communications between BrowseGate and the client package that wishes to use this extra connection. This means that you must configure your client application(s) to use the same port number as the port you select here (and you can use any free port number you wish).

The "Service Active" check box allows you to enable/disable any TCP port mapping you have set up, but you can also more easily just double click on an entry on the list to achieve this.

Once you have added or edited an entry, please ensure that you click the Update button. You also must click the main OK button before any changes will be saved to the configuration system. Pressing Cancel will discard all changes made...

Enter whatever port you wish BrowseGate to use to communicate with the streaming audio/video package that you wish to use this proxy.

If this option is checked, Browsegate will only allow URL's that match those specified to be viewed.

Please note that any Rules you have set up will still be applied to URL requests even when you have site blocking activated.!!

If this is checked, BrowseGate will automatically provide full SOCKS 4 and SOCKS5 support.

NB - If any of your networked applications (such as web browsers) and many other communications applications, require to use SOCKS4, you will need to ensure that you have the BrowseGate DNS turned on and configured as this is required by the SOCKS4 protocol.

Allow access if request made by following network address

This field allows you to EXCLUDE certain PC's on your network from the bans imposed by the sites or words Blacklist entries. This can contain one or more IP addresses of PC's that you wish to be excluded from the limitations imposed by the Blacklist system. Multiple IP address entries in this field can be separated by spaces or commas or commas + spaces.

eg: 192.123.100.1, 192.123.100.5 192.123.100.7

The entering of the IP address of any PC on your network in this field will mean that the PC concerned will not be limited in any way, or have ANY URL REQUEST CHECKED OR LIMITED by the Blacklist sites list.....

This option allows the network administrator to decide whether BrowseGate will return a full page of infornmation specifying the reason that any URL has been refused by BrowseGate

If **checked** - full details are displayed in the requesting web browser.
If **unchecked** - Only a single line notifying of the refusal is displayed in the requesting web browser.

The OK or Cancel button will close the Statistics dialog. Always make sure you have saved any report(s) you may wish to keep before closing the window.

Statistics - Create Reports button

Once you click either button, the report generation process will be started.

Both lists to the right will first be cleared and then refilled with
the results of any new log file(s) selection.

Create Summary Report for all selected log files
This button will generate a report containing only the summary of site
requests or modem activity for the day(s) selected

Create Detailed Report for all selected log files
This button will generate a comprehensive report containing fuller
details of the activity that is being reported up

NB The detailed report can get quite large if any of the requested connections have been very active in the periods requested.....

The Help Button probably brought you here in the first place ??

This pane contains the last report generated...

This pane contains the output for each report type you select.
Use the Save to file button if you wish to save the content of this list.

The following report options are available :-

Full configuration
Selecting this option will allow you to generate either a Full or Summary report for all BrowseGate's configuration settings.
The full reports gives full details of all settings and complete lists of all proxy services, ports used etc.
The Summary Report omits the detailed information to give an overview of the current server status

All Services
Only a full report is available for this option.
This report lists in detail all of the TCP Mappings, and the email and News settings

TCP Mapping only
Only a full report is available for this option.
This report lists in detail all of the TCP port mappings.

Rules
Only a full report is available for this option.
This report lists in detail all of the Rules that are configured.

Black Lists
Only a full report is available for this option.
This report lists all of the Blacklist settings and machine exceptions

Clicking this check box allows you to quickly select or deselect all of the available log files shown in the list below.

This pane contains a list of all the available log files that can be used for the generation of reports.

This is a multiple selection list that lets you select any combination of log files for the days you wish to see statistics on by using the standard Windows CTRL+CLICK. or SHIFT+CLICK mouse combinations.

If you would like to view any specific log file from here, you can just double click on the log file name in this list and it will be displayed using whatever default application you have set in Windows to view .LOG files.

This is a counter of the total number of log entries processed in the last report generated

This pane contain a list of the log entries that have been used to generate the report in the left hand pane. This allows you to scroll through and check any entries you might wish to.

If you want to save a report as a file on your hard disk, just click here.

A standard Windows "Save to file" dialog will be displayed with a default file name, and once the report has been saved, it is automatically loaded and displayed to let you print or check it's content, using whatever default application you have Windows configured to use for a TXT file.

Normally under W95/98/NT4 this will be WordPad.....

These options allow you to select any single connection to be reported upon if required.

Selecting the "All connections" option will force the report to include all connections that are found in the log file(s) requested

Selecting the "Single IP Only" option will force the report to only include details of the connection you specify in the field below. This field requires that you enter the IP address of the computer you are interested in in the format xxx.xxx.xxx.xxx

Show the total lines contained in the current report

The @NetClock SNTP time server Plug-in

See also: Configuring @NetClock

Due to the many well documented problems with various versions of Windows being unable to maintain the time on a PC system clock correctly, NetcPlus have now released their @NetClock SNTP server/client system to overcome these problems.

@NetClock is an intelligent "plug-in" designed specifically for our BrowseGate proxy server (and SmartServer3 email) that can automatically, and totally transparently, take advantage of the dial-up connections made by BrowseGate to check with any one of several hundred atomic clocks that are freely available on the Internet worldwide.

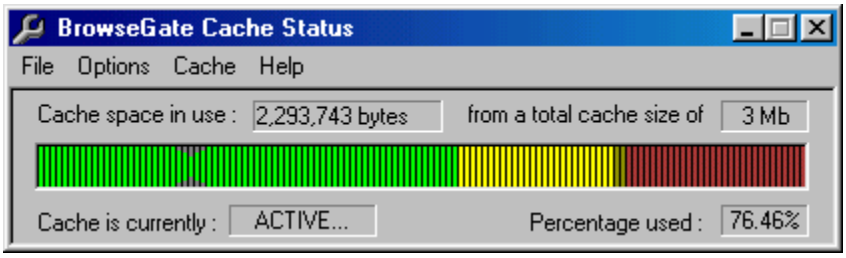
Once installed, you simply select the atomic clock server you wish to use for verification, and then install a copy the @NetClock client (NCCLIENT.EXE) on each and every other PC on your network. You will normally run them via a shortcut in the \Windows\Startup directory - which enables every other PC on the network to benefit from always having the correct date and time - taken from the BrowseGate PC that will of course, always have the right settings.....

An evaluation copy of @NetClock can be downloaded from our web site as shown in the About box.

The Cache status window

See Also: Editing the cache contents

To allow you to easily see what is happening in the web site cache system, you can display the window shown below by clicking the Cache | Show Cache status window option on the main BrowseGate menu. This will also "check" this option, which tells BrowseGate to automatically load the cache status each time it is started....



The coloured "slider" is updated in real time, and shows exactly how full the disk cache is at any point in time. The gray "Up & down arrow indicators" show the current "Low Water" level, which shows the percentage of newest data that will be preserved whenever the specifed cache space is totally filled and BrowseGate automatically purges older data.

There are also indicators to show you in Mb's the maximum cache space allocated currently, and the actual amount of data that the cache contains in bytes.

The menus contain the following options.:-

File
Show Main Window - redisplays the main BrowseGate window...
Close Cache Display - Shuts the cache status window.

Options
Keep window on top - if checked, makes the status window remain on top of all other "non topmost" windows.

Cache
Web Page Cache Active - A toggle that allows you disable/enable the cache system at any time. The check mark will change automatically. (This operation can also be done from the cache menu of the main BrowseGate window if required.)
Show Cache Information - Displays a dialog with all the current cache settings
Edit cache contents - This option allows you to optionally remove one or more cached web sites from the cache entirely. Useful if you want to save disk space and have visitied a web site you do not want to keep in your cache...
Clear all cache contents - CAUTION - This will REMOVE ALL of the cached data for all web sites currently held in the cache.
Recalculate Cache total - A useful option that scans the entire cache control database and recalculates the exact size of the data held in the cache. You should however rarely need to use this.
Cache properties - Provides immediate access to the property sheet with the cache tab activated to let you change any of the cache settings you wish.

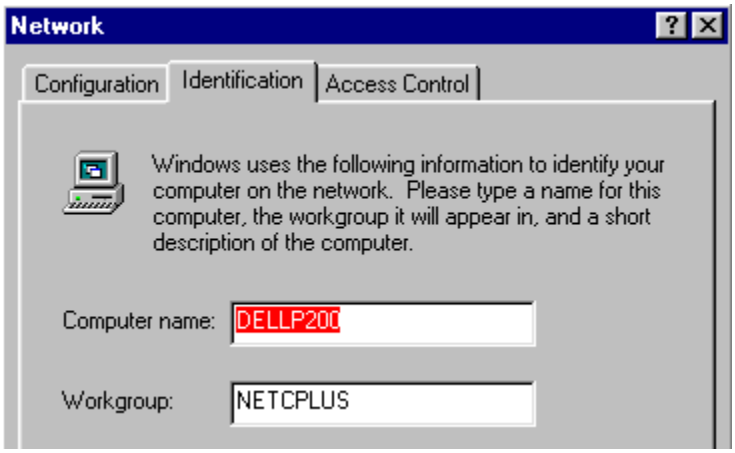
Help
Brings you to this help system.

The DNS System - Important information

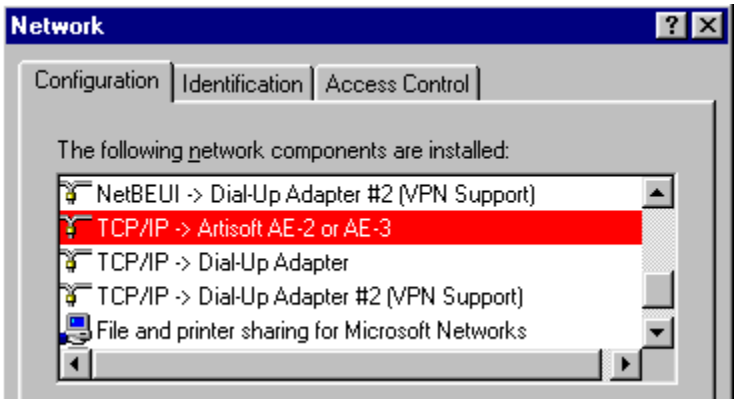
Potential problem when running Internet client applications on the BrowseGate server PC itself.

NB This situation only occurs when attempting to run client applications
on the SAME PC as the one on which BrowseGate is running.

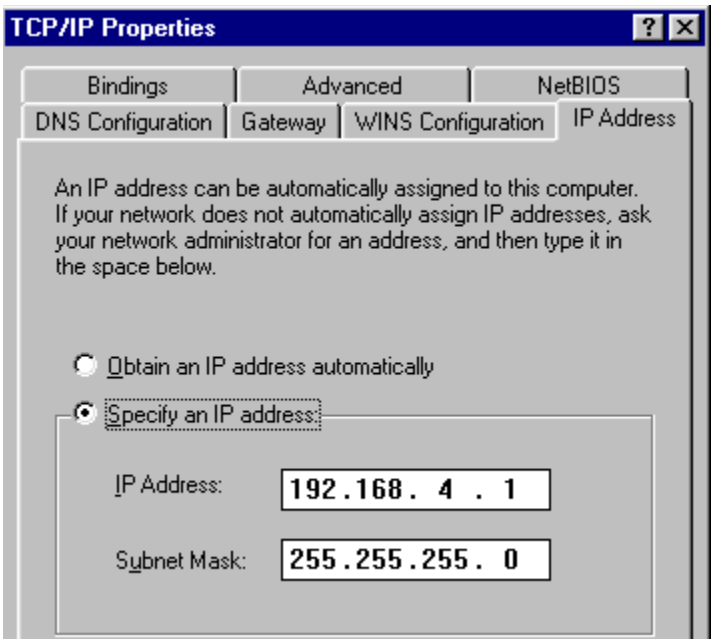
Each and every PC that has the TCP/IP protocol installed will have been given a "name" such as "myserver", or "Dellp200" or a similar unique name that Window's always uses for it's internal address resolution system. This Computer name can be seen in the property sheet shown below that can be reached from Start Menu | Settings | Network



If you then click on the Configuration tab, and locate an entry that looks similar to the one shown below (but for your particular network card)



Now click the properties button, and you will see a panel similar to this one :-



You can see that this is where the actual IP address of this PC has been entered.

Although the Windows 95/98 operating systems do not have a DNS system, they do have an internal caching and DNS resolution system for the use of "locally" executing applications, and this will correctly resolve the machine name (DELLP200) in our example as having an IP address of 192.168.4.1.

However, this will cause you problems because if you happen to use the actual "name" (DELLP200 in this case) of the local machine when attempting to configure any Internet client application such as email, news, web browsers etc to be run on the same PC that BrowseGate is installed on, Windows will always perform the IP address resolution, rather than letting BrowseGate handle it for you. The problem with this is that you will never get an external connection via this form of resolution as Windows does not pass it on to BrowseGate and so it does not know the request has been received.

This can be very confusing when you are assuming (perfectly reasonably) that the BrowseGate DNS system will be handling ALL DNS requests.

Lets assume as per our examples above that the name of your BrowseGate server PC is "DELLP200"

Do NOT use this actual machine name in your list of internal DNS settings. Instead add an entry in the BrowseGate internal servers list of say "DellProxy"

Now ALL PC's on the network (including the server machine itself) can safely use the name of "DellProxy" rather than it's IP address, and it will all work as expected, with the BrowseGate DNS handling all IP address resolution as expected.

The External DNS of BrowseGate is really what is called a DNS forwarding system. What this means is that assuming you have the local DNS enabled, and once BrowseGate has checked it for any matches, it then simply ensures it has a connection to your specified external DNS, and passes the request on to it for final resolution.

The Main BrowseGate Window

The configuration property sheet

Click on the specific topic you want more information on...

The special "BROWSEGATE" DNS entry

This feature has now been removed from BrowseGate 2.70 and later releases.

Things to check when trying to configure applications to use a proxy server

BrowseGate is fully capable of supporting most internet and intranet applications with the exception of Telnet and Ping.

Because of the uneccessary complexity that is involved today in setting up TCP on the Windows platforms, we recognise that some of you just may experience some difficulties when trying to get some networked applications to work correctly via BrowseGate. These problems are usually caused because you have one or more contradictory settings on your PC somewhere, and in our own exprience these are most often connected with how you have setup your exisitng web browser.

Before you go throught this list however - CHECK THE HELP SYSTEM OF YOUR APPLICATION under firewall or Proxy for information you may have missed or that may be important..... ALSO please contact the Help desk for the application itself before asking us how to set up 3rd party applications. We cannot possibly provide support for every network application around !!!

What follows is a wholly unsorted list of potential problem areas you may wish to check out if you are unable to get any particular application to work via BrowseGate.

It may well contain exactly the answer you are looking for....

1. Check your HTTP port settings in your browser.
All browsers have settings for a firewall/proxy server name or ip address and port. Make sure these are set to those configured In BrowseGate.

2. Check that your application uses EXACTLY the same HTTP settings.

3. If your application needs to use SOCKS 4 or 5, make sure you have the SOCKS protocol enabled in BrowseGate, and configured to use the default port.

4. Also for SOCKS, you MUST enable and configure the DNS system in BrowseGate, and make sure it works...

Check or uncheck this to toggle the ability of BrowseGate to support SOCKS 4 or SOCKS 5 on or off.

UDP PORT MAPPING - create/control additional proxy services

For other Configuration tabs - click on tab shown below...

Aliasing	Downloads	Local Web	Blocking	Rules	Blacklist	Password	Cache	SNTP
Connect	Email	News	Map TCP	Map UDP	SOCKS4/5	Realplayer	DNS	Ext.proxy	Options

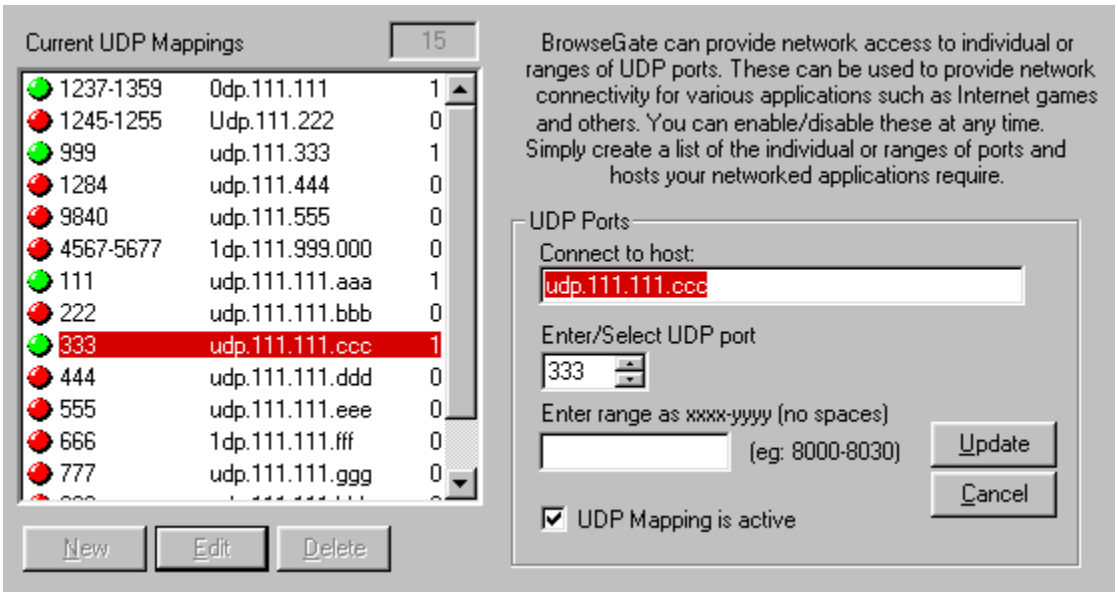
See Also: Setting up internet applications that require UDP ports

BrowseGate gives you the ability for your networked users to use those internet applications that require UDP port mapping as well as the standard TCP mapping.

Please note however that due to limitations in the UDP protocol, and the way ports are mapped and used, you cannot have more than one PC attempting to use the same UDP ports at the same time, as the UDP responses will not be able to identify which machine to respond to.

You can create proxy UDP connections as either single ports or ranges or ports.

All you need do is specify the name of the host to which this proxy is to connect to eg : doom123.games.com and then either specify an individual UDP port number, or whatever range of ports that particular UDP host requires.



Please note that we cannot assist you by providing information on what hosts or UDP ports are needed for the various internet applications that use UDP. This should always be provided by the application concerned. If not please ensure you contact the support staff for the product concerned, and not ourselves.

We cannot think of a single good reason why you might want to do so, but if for whatever reason you find it necessary to fully uninstall your BrowseGate installation, please follow the instructions below.....

Go to the Windows Control Panel
Select Add/Remove programs
Select the entry for "BrowseGate Proxy server"
Click remove

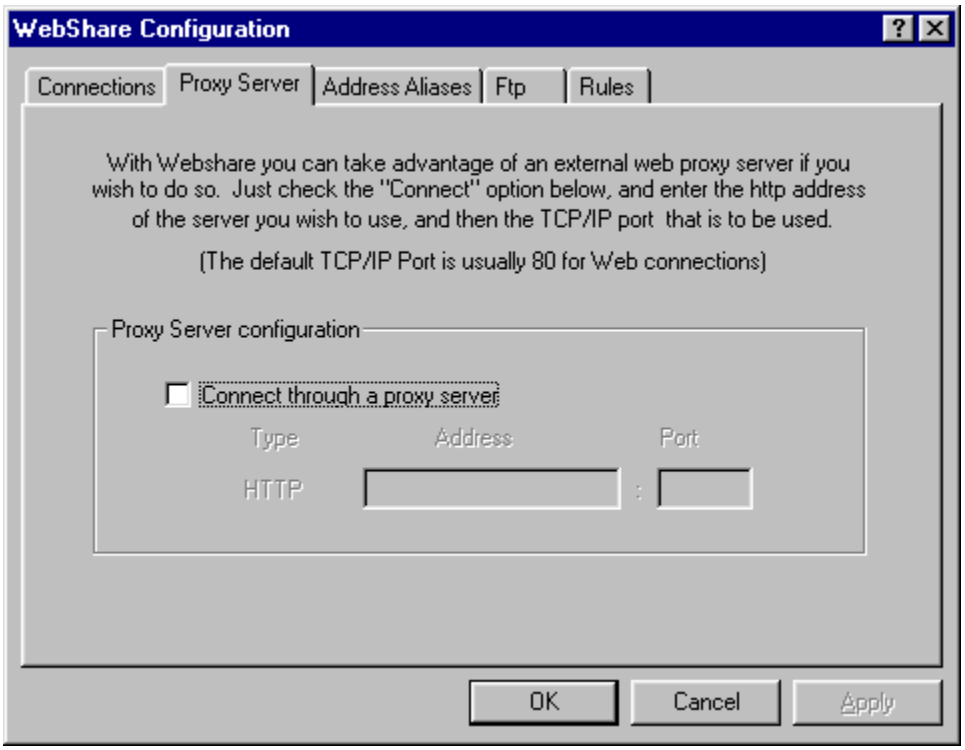
When the uninstall options dialog appears, YOU MUST SELECT the CUSTOM option. Use the SELECT ALL options on each of the following diaologs to mark ALL entries in each of the list boxes presented.

Finally, proceed with the uninstallation. This will remove all relevant files and directories, although you may still be left with a few temporary files or similar in the original installation folder, which you may delete if you wish to do by hand thru Windows Explorer.

Unfortunately, this method of uninstallation is forced on you by a problem in the Wise installer system, whose "standard" uninstall option only removes the basic files....

Using another proxy server

Click wherever the hand icon appears for more information.



Some Windows installations may have what are called a HOSTS or LMHOST file.
If you do not know what these are then you can safely ignore the following information....

However if you have been using either the HOSTS or LMHOSTS files on your network, you can simply copy it to the main BrowseGate installation directory, and then rename it to HOSTS.TXT. BrowseGate is capable of using these files transparently, and handles any comments or commented out entries correctly. eg: a HOSTS file looking like the one below would still be correctly checked

---

```
# HOSTS file for our company network
#created by SysAdmin 12/11/98

192.168.4.1      Dellp200          #temp server name only
#192.168.4.1     MailServer
192.168.4.3      Gateway2200
#192.168.4.4     ASTP90
192.168.4.4      proxy

#EOF
```

All lines that start with "#" in column 0 are ignored, as are any comments following the "#" character on a line after a valid entry

So the line
192.168.4.1 Dellp200 #temp server name only
would return 192.168.4.1 for an enquiry on DellP200, but would ignore the comment - #temp server name only

and the two lines :-
#192.168.4.1 MailServer
#192.168.4.4 ASTP90

would be ignored entirely and these machine names would NOT result in a resolved IP Address

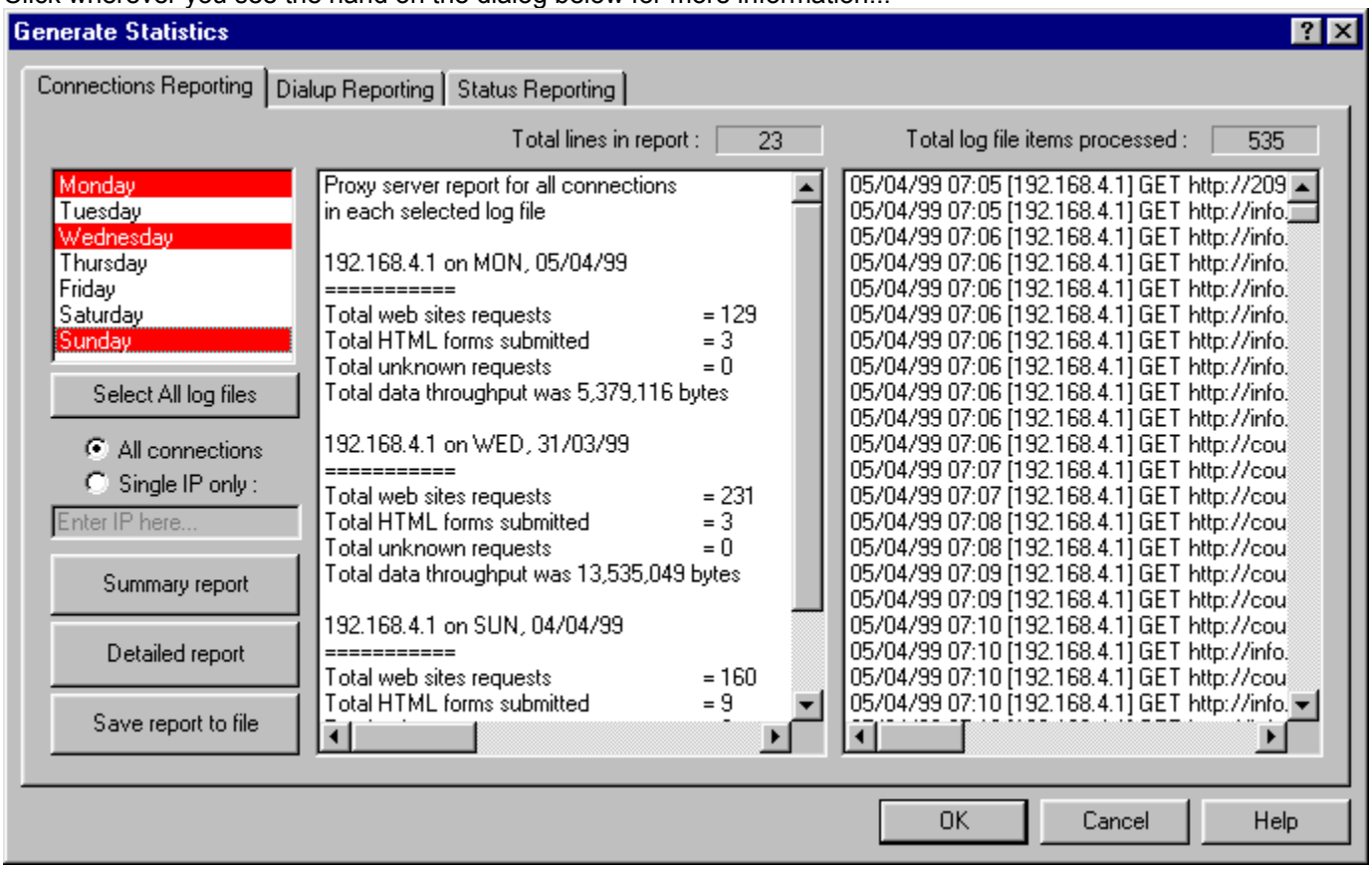
Using the Statistics to control your proxy use

See Also: Monitoring modem usage
Creating status reports

BrowseGate provides a powerful reporting facility that allows you to monitor the throughput of each computer that has used BrowseGate over the last 7 days.

The statistics option takes advantage of the detailed activity log files that are automatically generated for each of the 7 days of the week, and scans these to produce summary information on the activity for each computer (by IP address) that has access the server.

Click wherever you see the hand on the dialog below for more information...



Although you can select one, multiple, or all days, in our example above the three days of Monday, Thursday and Sunday have been selected to be reported on. The middle panel shows the summary report for all of these days. It shows only ONE machine with an IP address of 192.168.4.1 used BrowseGate on various dates, and the total badwidth (data requests + data received for that IP address for each date is summarised below each entry.

If another machine with say, an IP address of 192.168.4.3 had also used BrowseGate on one of these dates, the statistics would have been broken down separately for each machine on that day.

These statistics use the data from the special daily log files that may be found in the \BGLOGS subirectory below the BrowseGate installation directory. BrowseGate maintains a separate set of log files for each day of the week, and overwrites each day's log as the date changes each week. (eg: mon.log dated 13 Mar 99 wouldl be automatically overwritten as soon as any entry dated 20 Mar 99 is received)

When you first run BrowseGate after you have first installed it, you will find that there are only logs for the day(s) that you have had connections. Statistics are always listed in the normal weekly sequence of Mon -> Sun.

Maintaining the "Blacklist" of banned web sites and words

See also: Configuring the use of Blacklists
Editing the contents of Blacklists

Because the web now contains huge numbers of web sites that most business, and of course home users may wish to ensure they do not reach, We have built into BrowseGate a powerful and comprehensive Blacklist system for both web sites themselves and also for specific words that may be contained in an offensive web site URL.

In a very similar way to the that used by **NetNanny** and other similar products, BrowseGate gives you the power to control which web sites may be accessed by any network user by verifying the URL entered against a comprehensive list of web sites that are known to be unacceptable (sex, bombs.drugs etc). You can modify this list at any time to suit your own particular situation.

We provide an initial list (NNSITES.BAN) in it's installation, containing a comprehensive list of approximately 10,000 known pornographic and other unacceptable sites. These are based upon the freely available and well respected "NetNanny" lists. The latest versions of these "blacklists" can be downloaded from our web site at **www.netcplus.com**, but you can modify this list as you wish to suit your own requirements.... (If you download a new list from our web site, don't forget that it will overwrite any existing file including any changes you may have made to it. We recommend that you create your own site additions as a separate ASCII text file, which you can then always add back into any new list you download from us...)

If you have the Blacklist option turned on, BrowseGate will automatically check for any sites listed in this standard ASCII file, and , it will not provide access to any site in the list. BrowseGate also allows you to enforce this list on either of two different basis -

1 - exact match
This means that any URL entered must be found in the list. For example :-
if a networked user enter the URL of say **dutch-wendy.com**
and the blacklist file contained this EXACT entry, then BrowseGate would not allow access to this site, however, if a network user were to enter a URL of :
dutch-wendy.com/home.htm
then this check would FAIL if the blacklist file only contained an entry for dutch-wendy.com...

However..... by using :-

2 - Strict checking
this site would remain banned, because BrowseGate would check to see if just the web site domain address was in the banned list (that is **dutch-wendy.com**), and would therefore continue to ban ANY access whatsoever to any pages on this this site.....

This puts you in control of how strict you wish the checking to be.

You are able to change/remove/add to the list of banned sites at any time via the Configure | Blacklists menu option.

These panels show the version of BrowseGate you are running, plus the TCP port that BrowseGate is monitoring for connections to all of the web browsers on your network.

WS-FTP

WS_FTP (We configured the 95 LE version) does not appear to support totally global configuration of the use of a proxy server/firewall. Therefore the notes below must be applied to each and every FTP connection you use, at least the first time you wish to connect to that site via BrowseGate.....

1. Start WS-FTP32 - The properties dialog for the last session used is displayed....
2. Select the FireWall Tab
3. Check the "Use Firewall" option
4. Check "Save Password" (providing you are the only user of this PC)
5. Enter the host name or ip address of the BrowseGate PC in the "Host Name" field.
6. Optionally - enter your User ID and password for this specific FTP connection.
7. Set the Port to the same value as the local port of any assigned FTP connection in BrowseGate.
8. Ensure you select the "USER with no logon" option for firewall type.
9. Now select the Advanced Tab.
10. Ensure that the "Passive Transfers" option is UNCHECKED.
11. Click the Apply or OK button and close the session properties dialog.

Don't forget that the first time you choose a new or exisitng connection under WS-FTP, you should check the settings on the Firewall tab to make sure it has the "Use Firewall" option checked. This is normally saved between sessions, but typically defaults to OFF initially

You should NOT need to change any other settings, as when you select the "Use Firewall" option, the default settings automatically appear and are used.

Warnings for when you are setting up the Cache for the first time

Because most web browsers tend to be configured to cache web site data themselves, there are a few things you need to remember when first starting to use the BrowseGate cache on your network.

1. You MUST clear any cached data from each and every one of your browsers as they will almost certainly have quite a bit cached away already. Both IE and Netscape provide an option to remove all cached data.

2. We recommend that you configure each browser that is to use BrowseGate to NOT cache data itself. They all do it to a certain extent anyway, but nominally turning this off will make the BrowseGate cache work harder to store ALL the required information, which will hten of course be available to ALL of the browsers on your network overcoming the wasted time and disk space required if each one repeats the same internal caching for the same web sites !!! We suggest that you select whatever the relevant option is on your version of the web browsers that means **"Check for new page every time"** which will force BrowseGate to fetch and store the pages on most occasions.

3. Unless you have a very good reason to do so, do not check the "Ignore proxy for local addresses" option. This MAY stop the BG-HELP commands from working correctly in some installations.

4. Think carefully about the BrowseGate settings you select. In particular when you want it to check for newer versions of web pages etc. If you are likely to use the same web pages very often, and they are not dynamic and subject to rapid change, we recommend you leave the option at the default setting which will tells BrowseGate to automatically check for newer data if any item is older than ONE DAY.

If however, you visit highly dynamic sites regularly, you may want BrowseGate to check for bnewer versions every time a request is received.

5. Make sure you allocate sufficient disk space to handle the amount of cached data you want to access. A fairly good rule of thumb for an average network is to allow 10Mb of disk space per browser that is going to use cached data. eg a 10 user network should allocate 100Mb of cache disk space.

What is the Internal DNS ?

See Also: External DNS
Using any existing HOSTS/LMHOST files

The Internal DNS is actually quite a simple "lookup" system that checks each and every entry in a special file called HOSTS.TXT to see if there is a matching entry for the machine name requested by any application. In the example below you will see that there are actually several different entries in the internal DNS list that are used for exactly the same machine with an IP address of 192.168.4.1.

This is perfectly legal, and can sometimes be very useful if you wish to allocate any specific server PC a different name for use with different applications. BrowseGate will check each and every "human readable" name in an attempt to find a match with the requested one.

So in the example above, when a request is received for a machine with the name of say "devserver", BrowseGate would of course find this in the 3rd entry of the HOSTS.TXT file, and would return the assigned IP address of 192.168.4.1. A different application on the network might be configured to access the same server machine but using a name of just "dev", which would of course, also return the same IP address of 192.168.4.1 (and so of course the same server PC)

However, a more typical list of local (networked) machines would also contain some other machine entries and might look more like :-

192.168.4.1 Dellp200
192.168.4.1 MailServer
192.168.4.3 Gateway2200
192.168.4.4 ASTP90
192.168.4.4 proxy

Which shows that we actually have 3 networked machines, but have chosen to assign 2 names to the machine with the IP address of 192.168.4.1, and also 2 names to the machine with the IP address of 192.168.4.4, but leaving the GateWay2200 with just a single name.

This is known as DNS aliasing.

Of course it is essential that you ensure that no machine names you allocate are duplicated in the DNS List, or the first entry is the only one that will ever be located...

The search and comparison is NOT performed CASE SENSITIVELY, so it is not important that you enter the machine names in any particular case, but you must of course ensure that you spell them totally correctly..

WARNING: If you make changes to the internal DNS list in BrowseGate, you may find it necessary to reboot the BrowseGate PC. This is due to the fact that Windows caches many DNS entries internally, and this can confuse the TCP/IP system and DNS lookups if you happen to remove an entry that is already being cached by Windows itself.

When should or shouldn't I use web site cacheing

When is it best to use the BrowseGate internal cache ?

If your web surfing involves visiting various web sites on a regular basis, it makes a lot of sense to have BrowseGate store the site information locally on your hard disk. If these sites do not change their content too often, then you should definitely use the cache system. If however, they are fairly dynamic and change some of their content quite regularly, you will still see a considerable improvement in performance by using the cache, as typically only a small percentage of the pages or images involved actually need to be re-downloaded.

Reasons why you may NOT want to use the BrowseGate cache

1. If you already connect via a web cache provided by your ISP to reach the Web, you should experiment to see if it is better to turn the BrowseGate cache ON or OFF. This is because BrowseGate needs to check for newer pages first, and then the remote cache has to do so, and finally, it may decide it also has to update itself before passing the data back to BrowseGate. This can result in slower web access rather than the expected faster access a cache will typically provide.

2. If your web surfing involves visiting web sites that you are unlikely to wish to revisit, it is quite clearly a pointless and unnecessary overhead to have BrowseGate store all this information on your hard disk.

3. If you are unable to allocate sufficient disk space to the cacheing system, you will probably find that it will spend rather too much time refreshing and then removing files. We recommend that for maximum efficiency you allow sufficient hard disk space to be able to allocate a maximum disk cache size of at least 10Mb per typical single PC's, which means you need to multiply this by at least the number of users you have accessing the web via BrowseGate to gain the maximum benefit from the cacheing system. eg: a 5 user BrowseGate should have 50Mb of cache space available.

The only time this does not apply is if all the networked users tend to visit the SAME web sites, in which case a small cache of 10Mb or whatever suits your maximum site needs is fine, as of course, BrowseGate will only cache a web site once, NOT once for each user that accesses them.

Why does a service(s) fail to initialize when it is activated?

See Also: A Discussion on ports
Total sockets available in Winsock.

Browsegate always performs a check on startup to ensure that there are no TCP/IP port allocation clashes, and that it is not attempting to open too many sockets.

If it discovers that some other application on the BrowseGate PC is already using the same port as the local port you have assigned to any one of the BrowseGate proxy services, it will automatically terminate it's attempt to provide that particular service.

Where relevant, the activity LED's will show as RED to warn you this has occured, but the status list will always contain an entry similar to the following for any port it has had to disable due to a port clash :-

BrowseGate: xxx proxy service suspended on port xxx

It is a good idea to check the list whenever you have made changes to proxy services or installed other TCP/IP applications on this PC, so that you ensure you have not encountered any suspended services.

To overcome port clashes, you only need to go to the Configure property sheet, select the relevant tab, and select any free port for the local port of any service that has been identifed by BrowseGate as having a port number clash.... or of course, you could also change the port settings of the other application concerned.

If you excedd the total ports available under Windows, you will have to disable one or more of any other proxies you have configured to reduce the total sockets required to some value below 128.

Each address alias entry is made up as follows :

An asterisk (*) that BrowseGate replaces with whatever you type into your browsers URL field.
other possible valid URL combinations that together with the replaced asterisk, will comprise a possible valid web site address.

The examples shown are self explanatory.

Add
Lets you add a new entry to the current banned list.
Edit
Lets you change or "comment out" the selected entry.
Delete
Lets you delete the selected entry from the current banned list.
Delete All
Deletes the ENTIRE LIST - Use with Caution !!!!

If this is checked, the BrowseGate cache system is activated.

If checked, the cache level will be displayed as a numeric percentage only.
If unchecked, the cache level will be displayed as a three colour slider panel.

This button allows you to quickly recalculate the cached data total to ensure that the size of the cached data is correctly indicated

This is the currently selected SNTP server.

By clicking the disconnect button, you can force BrowseGate to drop its active modem connection. Please note that this will only perform the disconnection if either BrowseGate initiated the modem connection, or if another application did so using the same DUN connection.

To illustrate this, if you have more than a single DUN connection configured under Windows on your PC, and another application has used the modem to make a connection via "Demon", and BrowseGate is configured to use a "Virgin" connection and not the "Demon" one, BrowseGate would NOT perform a disconnection of any active "Demon" connection, although it would use it if a request was received for any service provided by BrowseGate.

BrowseGate has been extensively tested to ensure that it will always endeavour to disconnect a modem connection after the specified timeout period. To allow it to do so we strongly recommend that any other applications that may also use this modem on the PC on which BrowseGate is installed should be configured to always use the same DUN connection as BrowseGate. This will avoid the potential for a connection remaining open indefinitely.

Favorites list docked in IE4

The free memory indicator shows you how much free memory Window's reports as being available at any time....

Many FTP sites require you to provide a login and password as parameters. Enter your preferred defaults in these fields,or just accept the defaults provided, which will allow you to access most know public FTP sites.

This is the list of available SNTP servers worldwide.

If you wish to modify this list you can do so by editing the file SNTPSERVERS.DAT that you will find in the BrowseGate installation directory. This is a standard ASCII file, so ensure you save it in TXT format (not DOC or similar WP formats.....

This listbox contains a full list of the banned items (Sites or Words)
you have selected to edit.

You can scroll through the list and Delete, Edit or Add new items.

If you click the Delete button, the item highlighted will be removed.
If you click the Add button, the new item you enter will be inserted
in the list immediately after the currently highlighted item.

If you edit an item, it's position in the list will not be changed.

If you insert a semi colon (;) at the front of an item, this will "comment"
it out, and it will not be included in further match checking.

This allows you to temporarily modify a list if you wish to do so.

This list contains the name of all currently configured access rules. As you click on each one the details of that rule are shown in the fields to the right.

Example of log file entries

27/02/99 7:36 192.168.4.1 Connected to pop3.ps-consultants.co.uk
27/02/99 7:36 192.168.4.1 Connected to pop3.ps-consultants.co.uk
27/02/99 7:36 192.168.4.1 Disconnected from pop3.ps-consultants.co.uk
27/02/99 7:37 192.168.4.1 Connected to pop3.ps-consultants.co.uk
27/02/99 7:37 192.168.4.1 Disconnected from pop3.ps-consultants.co.uk
27/02/99 7:37 192.168.4.1 Connected to pop3.ps-consultants.co.uk
27/02/99 7:38 192.168.4.1 Disconnected from pop3.ps-consultants.co.uk
27/02/99 7:38 192.168.4.1 Connected to pop3.ps-consultants.co.uk
27/02/99 7:38 192.168.4.1 Disconnected from pop3.ps-consultants.co.uk
27/02/99 7:38 192.168.4.1 Disconnected from pop3.ps-consultants.co.uk
27/02/99 7:38 192.168.4.1 Connected to mail.virgin.net
27/02/99 7:38 192.168.4.1 Disconnected from mail.virgin.net
27/02/99 7:38 192.168.4.1 Connected to mailhost.airtime.co.uk
27/02/99 7:38 192.168.4.1 Disconnected from mailhost.airtime.co.uk
27/02/99 7:39 192.168.4.1 Connected to pop3.demon.co.uk
27/02/99 7:39 192.168.4.1 Disconnected from pop3.demon.co.uk
27/02/99 7:39 192.168.4.1 Connected to pop.freeserve.net
27/02/99 7:39 192.168.4.1 Disconnected from pop.freeserve.net
27/02/99 7:41 [192.168.4.1] GET http://bg-help/ HTTP/1.0
27/02/99 7:41 [192.168.4.1] GET http://bg-blacklist/ HTTP/1.0
27/02/99 7:42 [192.168.4.1] GET http://bg-blacklist/ HTTP/1.0
27/02/99 7:42 [192.168.4.1] GET http://bg-help/ HTTP/1.0
27/02/99 7:42 [192.168.4.1] GET http://bg-extra/ HTTP/1.0
27/02/99 7:42 [192.168.4.1] GET http://bg-help/ HTTP/1.0
27/02/99 7:42 [192.168.4.1] GET http://bg-ports/ HTTP/1.0
27/02/99 7:42 [192.168.4.1] GET http://bg-help/ HTTP/1.0
27/02/99 7:42 [192.168.4.1] GET http://bg-about/ HTTP/1.0
27/02/99 7:44 [192.168.4.1] GET http://3438189349/ma/spice747/trip.html HTTP/1.0
27/02/99 7:45 [192.168.4.1] GET http://www.scoot.co.uk/scoot.asp?
&s=SUK&a=&c=F00525&ce=intranet&ae=milton+keynes&a=01048&c=F00525 HTTP/1.0

mIRC is pretty easy to configure for use with BrowseGate.
The following instructions apply to v 5.51(32bit)

1. Start mIRC
2. Open General options dialog from button bar or File | Options menu.
3. Select FireWall in the list of Categories.
4. Check the "Use SOCKS firewall " option
5. Make sure you select Socks5 (Socks 4 wil not work...)
6. Enter in the "Hostname" field the machine name (or IP address) of the PC on which BrowseGate is running.
7. Normally you should leave User ID and Password blank for public IRC servers.
8. Ensure "port" is set to 1080.
9. Check "Ensure DCC's through firewall" option
10. Click OK.
11. Try connecting to an IRC server from the button bar - it should all work !!!

Both the mail and News proxies provide you with the option to have BrowseGate disconnect immediately it has completed a Mail or News connection, or to wait for the defined timeout period as do all other proxies.

This is really only provided for those who are only using BrowseGate as a network gateway for email/news alone. If other proxies are also in use we recommend you leave the default setting to let BrowseGate timeout the dialup connection.

Only If this is checked and you have entered relevant details will the SMTP and POP3 mail proxy(s) will be available to your networked users.

This list box shows in real time what operations are being handled by BrowseGate. It can hold up to 32Kb of information at any one time, which is continually scrolled automatically, but once the list is full, the oldest entries at the top of the list are removed automatically by the system. A complete and detailed list of all connections and operations performed can be created if you check the "Keep log file" option in the configuration.

If you double click on any line in this list that contains "GET http://" this line is automatically copied to the Windows Clipboard) as a fully qualified URL that you can then paste into your browser. All of the other text apart from that required to create a valid URLis removed by BrowseGate. eg:

ORIGINAL LINE : **06:45:37 GET http://www.netcplus.com/xdownlds.htm HTTP/1.0**
Clipboard contents : **http://www.netcplus.com/xdownlds.htm**

On startup, the current configuration of all proxy services is listed here with the internal port numbers used. The green and/or red LED's at the bottom of the window also provide an immediate indicatation of which proxy services BrowseGate is configured to support.

If you wish to provide support for NNTP news access via BrowseGate, you should first check the "Enable NNTP News proxy service" option at the top, which will enable the panel that follows.

Enter the name of your preferred news server in the "News server to collect from" field. This will be an entry such as **news.virgin.net.**
If you are unsure we suggest you check the documentation provided by your ISP or the settings in your existing working news client for the correct values for this field.

The port settings should normally be left set to the default of 119 unless you already have other applications on this PC that are using them.
If this is the case, you will normally only need to select a different port value for the Local Port

The Remote Port should normally be left at the default setting of 119.

You can also choose to have BrowseGate disconnect immediately upon completion of news operations, or to use the same timeout that has been set for web access (on the Connections tab) This allows you to configure the proxy to work the way that suits your own circumstances best. This setting affects both Mail and News proxy operations.

Set Password
Providing you have entered a matching password in BOTH data entry fields BrowseGate will confirm if the password has been accepted. If they do not match, you will be warned.

Clear Password
To clear (remove) and existing password, click this button. BrowseGate will confirm that the password has been removed.

Cancel
Discards any unsaved changes.

NB Immediately you press the "Set Password" button, the new password details are saved immediately.

You should enter the same password you want to use for restricting access to this configration system in both of these text fields

This panel is a warning that any password you enter here is

Most Important !!

Please ensure that you do not forget it or you will be
unable to access the configuration system at all.

If you do forget this for any reason, please send an email to
the support group at NetcPlus addressed to :-

bgpassword@netcplus.com

together with your BrowseGate serial number, and we will then send you
detailed information on how to overcome this problem....

If you wish to enable POP3 and SMTP eMail access via BrowseGate, you should first check the "Enable email proxy services" option at the top, which will give you access to the fields that follow.

Enter the name of your main POP3 mail host mailbox in the "Get incoming mail from" field. This will be an entry such as **mail.virgin.net,** and do the same in the "Send outgoing mail to" field. Typically these are both the same, but you may have a provider that uses **pop3.xxxxx.xxxx** and **smtp.xxxx.xxx** for fetching and sending mail. If you are unsure we suggest you check the documentation provided by your ISP or the settings in your existing working email client(s) for the correct values for these fields.

Both the Local and Remote port settings will usually not need to be changed from the default values of POP3 = 110 and SMTP = 25, unless you already have other network applications on this PC that are using them. If this is the case, you will normally only need to select a different port value for one or both of the the Local Ports

The Remote Port settings shold normally be left at the default settings unless your ISP (host) gives you a different setting.

If you want to configure BrowseGate with the abiilty to connect to multiple mail host machines (typically from different ISP's) then all you need do is click the "Additional POP3 Accounts..." button and complete the require fields on th edialog that will appear.

You can also choose to have BrowseGate disconnect immediately upon completion of email operations, or to use the same timeout that has been set for web access (on the Connections tab) This allows you to configure the proxy to work the way that suits your own circumstances best.

This setting affects both Mail and News proxy operations.

This may be either the name or you can use an IP address of an external proxy server machine. The port number should be set to whatever port is defined for connections by the external proxy server system.

If checked, BrowseGate will connect to the external proxy server specified by the address below.

If you wish to re-enable this email servers tab, you need to edit the configuration file named BRWGATE.INI that you will find in the directory from which you run BrowseGate.
(Ensure you use a standard ASCII editor such as Windows Notepad, not a word processor such as Word....)

Add a new section (if not already present) and add a single entry as shown below :-

[SS]
overide=1

If the value is set to ONE, you will be able to access the email services fields,
if it is set to ZERO, you will not.

Save the changes made and restart the BrowseGate server, and you will be able to access/not access these settings.

This panel can be displayed if you want to monitor the total numbers of socket connections that BrowseGate is using at any point in time. It maintains a real time indication of the number of ports (Sockets) in use at the time. This can be useful if you happen to find yourself experiencing network degradation, as it will show how many ports BrowseGate is using. However BrowseGate is most unlikely to cause any degradation if used with a suitable modem/ISDN/Network connection that can provide the throughput your networked users require.

The slider at the left shows you the percentage of connections (sockets) in use at any point in time. The panel to the right shows the exact number of connections active as a numeric value.

Double clicking on this label will toggle the display of this information ON/OFF as you prefer.

To specify that you want BrowseGate to connect via another proxy server, (which may be on your own network, or on a remote host system available via a dial up connection) you need to check the "Connect through a proxy server" option, and then in the fields provided specify the tcp/ip address and port number that is to be used for the connection between BrowseGate and the other Proxy server.

This address is of course that of the remote proxy server, not the address of the PC on which BrowseGate is running.!!

Use this toggle to activate or deactivate the address aliasing system.

Configuring Real Player (G2)

The following configuration information applies to Real Player G2 release v6.0.5.27 or possibly later releases.

The Real Player product has over time been found to be consistently changing it's configuration options, so you may have to check the options on your version against the ones quoted below a little more carefully if they are different.

Real Player will happily takes advantage of many of the features such as the special PNA support provided by BrowseGate. That said, it is iessential that you go through the configuration process in Real Player very carefully if you want it to work correctly first time with any proxy server.

1. **IMPORTANT - Ensure you have checked the Real Player PNA option on the BrowseGate configuration property sheet and the port is set to 1090.**
2. Start Real Player.
3. Select menu Options | Preferences
4. You now need to work your way through virtually all of

the property sheets provided, following the instructions below :-

The items marked with two asterisks (**) are only important if you do NOT WANT RP to force Internet connections on startup or to perform automatic updates of it's channels, news tickers etc...

General Tab

** We recommend you UNCHECK the "Allow SmartStart to run in System tray" option

Other options on this tab may be set to suit your own preferences.

Display

May be set to suit your own preferences.

Content

** UNCHECK the "Enable automatic headline updating" option
Other options on this tab may be set to suit your own preferences.

Upgrade

All options may be set to suit your own preferences.

Connection

In the Bandwidth selection lists, select 10Mbs LAN if you are running across a LAN, otherwise the most relevant connection to match your PC's configuration. You should almost certainly NOT select and modem type connection type as this will force RP to bypass BrowseGate.

Other options on this tab may be set to suit your own preferences.

Transport

You should use the "automatically select best transport" option to let RP check for, and if required, change the proxy settings on this tab **before** making any changes whatsoever to the proxy tab on this property sheet.

To do this effectively, we recommend that you should have BrowseGate running

and with an active and working connection to the Internet. (use a browser to start a connection)

Now select the "automatically select best transport" option, and click the Auto-configure button. Press OK at the next dialog that appears.
Wait for the auto connection system to complete it's checking.....

RP should report "Autoconfigure completed successfully..."
Click OK at the confirmation dialog
Note that the Auto select option you checked initially has probably been changed by this process to the "Use specified transports" radio button - that's absolutely fine !!!!

You should NOT need to make any further changes to the settings for either the RTSP or PNA settings as these will have been auto sensed by RP.

Do NOT check the "Use specific UDP port" option.

Proxy

If the auto sense system worked correctly when you followed the instructions above, then the "Use PNA" option should be checked, and the port number should be set to 1090.

If the first field is blank (this is the server name field) then you need to enter in this field the NETBIOS name of this computer, or the IP address.

Ensure the RTSP option is UNCHECKED.

The entries you will require in the HTTP Options section on this tab will depend very much on the way your web browser has been configured. If the web browser ON THIS PC is already setup to work via BrowseGate correctly (NB IE5.xx) you can simply check the "use my Web browsers HTTP proxy".

Unless you want RP to connect directly, bypassing BrowseGate, do NOT select the "No HTTP proxy" option

If you want to be absolutely certain that RP will use BrowseGate for all HTTP connectivity the select the "Manually configure HTTP proxy" option, and enter the NETBIOS name of this PC, or the IP address in the first field, and the INTERNAL port number you have set up in BrowseGate for all HTTP connections (typically this is port 80).

You may use the Exception field to "Except" certain local sites if you wish providing always that you are aware of what the restrictions and impact these may have on your network's overall functionality.

Performance

All options may be set to suit your own preferences.

Support

All options may be set to suit your own preferences.

Real Player should now be successfully configured to use BrowseGate for it's connectivity

To confirm this, press OK (not CANCEL!!!!) on the configuration property sheet.

Now go to the RP main window and select any one of the channels under the Presets menu. Watch the LED's on the BrowseGate window, with particular attention to the REAL PLAYER indicator. Once the channel you select starts to load, you should see the Real Player LED start to flash form time to time.

If you do see this LED flash, then BrowseGate is providing PNA support to Real Player.

That's it - RP is now configured to work correctly via BrowseGate :-)

Configuring Netscape AIM v3.xx

BrowseGate full supports SOCKS4/5 connection methods that can be used with the Netscape AOL Messenger v3.0 and later.

It is very easy to get AIM to connect via BrowseGate by following the instructions below.

1. Run AIM.
2. From the sign on screen Select Setup, or the Preferences | User options menu from the main screen
3. Select the "Connection" tab on the property sheet that appears

IF YOU WANT TO USE SOCKS 4/5

4. Check the "Connect using proxy" option
5. Check the "SOCKS5" option in the Protocols frame to the right
6. In the Proxy host field enter either the IP address of the PC on which BrowseGate is installed, or more easily, you can simply use the NETBIOS name of the BrowseGate machine.
7. Set the server port number to whatever local port BrowseGate uses for SOCKS requests across the network (typically this will be port 1080)
8. You do not need to enter anything into the authentication fields.
9. Check the SOCKS version you wish to use. We recommend you use SOCKS 5, but you must have the BrowseGate DNS configured for this to work correctly.
10. If you have the BrowseGate external DNS operating, then also check the "Use proxy to resolve hostnames" option.
11. If you have to pay for telephone calls, we recommend you DO NOT check the "Keep connection alive" option, as this will obviously keep any dial up connection made by BrowseGate open all of the time.
12. Click the OK BUTTON.

IF YOU WANT TO USE HTTP ALONE:

4. Check the "Connect using proxy" option
5. Check the "HTTPS" option in the protocol frame to the right.
6. In the Server name field enter either the IP address of the PC on which BrowseGate is installed, or more easily, you can simply use the NETBIOS name of the BrowseGate machine.
7. Set the server port number to whatever local port BrowseGate uses for HTTPS requests across the network (typically this will be port 80)
8. Perform steps 10 onwards as shown above.

Now test the connection.

NB In our own experience, the "automatic configuration" option in AIM does not appear to locate a network connection to a proxy server correctly

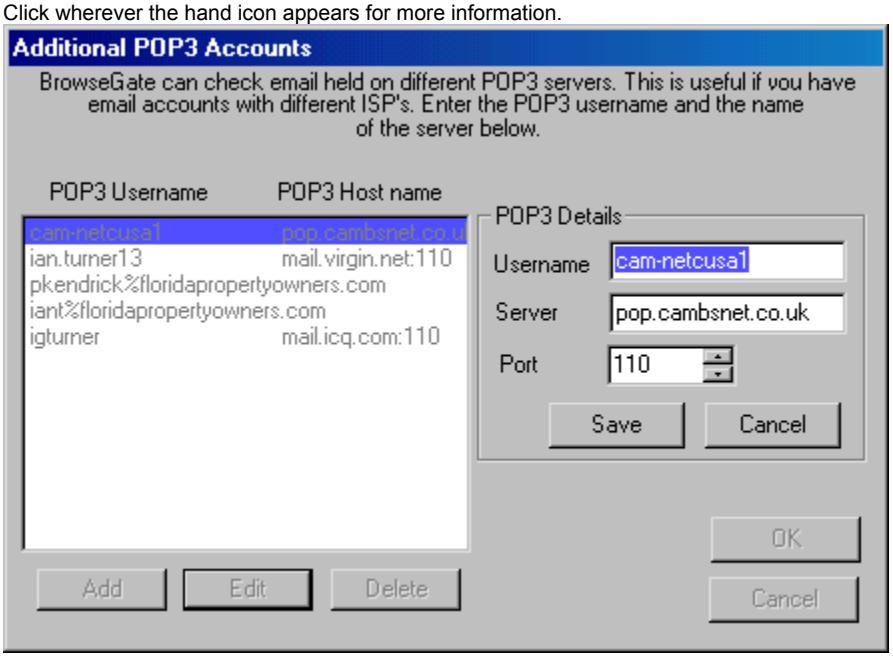
If you still have problems, Please contact Netscape or AOL, or check their web site Help systems for firewalls and proxy information.

Configuring BrowseGate to collect mail from multiple ISP's or multiple mailboxes.

BrowseGate now provides what we have called SmartPOP to allow as many of your networked email clients to take advantage of a proxy server without needing to change their client configurations.

This also provides a very quick and efficient method to allow collection of mail from multiple different POP3 mailboxes without the need to set up different TCP mappings for each individual mailbox. Each of your networked email clients can be setup to use the same internal port.

Click wherever the hand icon appears for more information.



Please note that the port field provided on this dialog is NOT the one to be used by all the email clients on your network to connect to and use this proxy for all entries in the SmartPop system. This is the EXTERNAL port that is used to connect to that particular mailbox. In most cases this will be port 110, but if you do connect to an internal mail server this may be different.

The port for internal connections between BrowseGate and your email client packages is the one you selected or entered on the main email configuration tab

Because we recognize that many of us today have more than one single mail account, and that very often for simplicity we tend to use the same user ID for many of these different accounts, the SmartPOP system allows you to enter two identical POP3 user names but obviously having different Host machine names.

However, you do need to change the user ID setting in your client packages so that SmartPOP is able to identify exactly which mailbox you are asking it to connect to.

This is very simple - all you need to do is enter in the user ID field of your mail client(s) a specially formatted entry that contains BOTH the user name / ID plus the host name, separated by **two** %% characters

So, if we had a second entry in the list shown above for someone with a user ID of ian.turner13, and lets assume the new entry had a host name of mail.netcplus.com. We would need to "identify" both connections as shown below in the USER ID field of the relevant email CLIENT packages :-

iant.turner13%%mail.virgin.net
iant.turner13%%mail.netcplus.com

NB you must use TWO PERCENT SIGNS and no spaces between the user ID and the mail host....

If you do not do this, the SmartPOP system will not be able to identify which specific mailbox you want to connect to, and will therefore default to the first account that matches the user ID received ALONE

This list box contains all of the additional mailboxes that you have configured in BrowseGate.

The list contains the User ID required to access any particular POP3 mailbox, plus the name of the mail host machine.

By selecting any entry you will be able to see the setup of that entry in the data fields to the right.

The Username is the standard User Id that each and every
POP3 mailbox requires to allow access to it's contents.

The Server field contains the name of the mail server machine.
Typically this will be mail.xxxxx.yyyy or pop3.xxx.yyy, but may
of course be any name at all as specified by your ISP.

The Port is the EXTERNAL port that will be used for communications
between BrowseGate and the remote external mail servers.

The default port for this POP3 connection is 110, and you should
ONLY change this if your ISP instructs you to do so, although the
likelyhood of this being asked for is VERY REMOTE INDEED !!!

You can Add, Edit or Delete entries in the SmartPOP list at will.

The limit for SmartPOP entries is approximately 5000. Which really should be sufficient for all environments.

Allow All
By clicking this button you can immediate activate ALL 24 site blocking entries

Allow None
By clicking this button you can immediate disable ALL 24 site blocking entries.

NB If you disable all entries and leave them all disabled, but leave Site blocking activated, then your networked browsers will NOT BE ABLE TO CONNECT TO ANY WEB SITES AT ALL !!!

Menu Bar

File

"Back up Servers configuration" allows you to take a complete copy of all your BrowseGate settings in case of PC or Windows problems. BrowseGate has been designed to use a standard Window's INI configuration file rather than the Window's registry to avoid the problems typical with Window's re-installations or Registry corruption. (Please contact NetCPlus for details of how to use these backup configuration systems.)

"Rerun Setup Wizard" allows you to quickly check and reset the basic proxy settings. NB: If a password has been set this is NOT available without the entry of the password.

"Exit" closes BrowseGate completely.

Options

"Statistics" is a quick way to get to the built-in Statistics system in BrowseGate.

"Register BrowseGate" is only enabled if you are running an evaluation version, otherwise it will always be grayed.

View

The View menu provides you with quick access to most available proxies and other settings in BrowseGate. You can even list all your additional mapped procies if you wish. Clicking any option on this menu will toggle the active status betwen enabled and disabled.

Cache

"Web page cache active" toggles the use (or not) of the built-in web page cache.

"Show cache status window" lets you toggle the visibility of the special Web page cache status window.

"Show status window on startup" lets you tell BrowseGate to automatically display the cache status window each time it is restarted.

Help

"Contents" and "Search Help for..." both Brings you to this Help system....

"How to register your proxy server" shows you exactly how you can register your evaluation copy of BrowseGate quickly and easily. This is only available in Evaluation versions, otherwise it is grayed.

"View/Print Manual (Word 97 format)" provides quick access to a detailed printable manual for BrowseGate. This requires MS Word 97 or later installed on your PC.

"Find out about SmartServer3 email server" takes you to the NetCPlus web site to learn all about our powerful email server. BrowseGate can be used a plug-in to SmartServer.

"Find out about @NetClock Time server" takes you to the NetCPlus web site to learn all about our very useful SNTP TIME server for networks. @NetClock can be installed as a plug-in to BrowseGate.

"Check for latest Upgrade" takes you to the upgrades page of the NetCPlus web site to check for any upgrades that may have been released. It is our policy to only charge customers for MAJOR upgrades, and virtually all of our upgrades over the last 15 months have been free !!!

"About BrowseGate proxy server" provides a standard About Box that contains both your license details plus contact details for both your Reseller and NetcPlus.

The different versions of BrowseGate

BrowseGate is currently released as four entirely separate and different products

This has been done to allow NetCPlus to provide you with the right proxy server for the number of users you need at the most attractive price possible...

BrowseGate (LITE)
This is a TOTALLY free version of our proxy server that is provided for all small Home or small office network users. The LITE version is limited in it's functionality as shown below :-

Only 2 concurrent PC's may use BrowseGate at any one time.
Only the summary statistics reports can be accessed
Only 15 TCP mappings can be configured
Only 15 Rules can be configured.
Only 8 Site blocking entries can be configured.
Only 5 additional POP3/SMTP mailbox entries can be configured
The banned URL's and banned words in the Blacklist system will only load a maximum of 20 entries each,
(all other BrowseGate versions allow unlimited lists and words.)
Access is not allowed to the View menu.

Please Note: Although we provide the Lite version as a totally free proxy server, it still has to be registered with NetcPlus. All you need to do is send an email to BGLITEREGISTER@netcplus.com, with your name, address and the reason you like the Lite version and want to continue using it, and we will send you a special Lite serial number and unlock key that will allow you to continue to use it freely after the maximum 20 days evallautaion period has expired.

BrowseGate (Personal)
The next step up from the Lite version, but still only costing $44.95, the Personal version provides full access to all the features built-in to any of the BrowseGate family of proxy servers, The only limitation is that a maximum of 3 concurrent PC's may use it at any one time.

BrowseGate(Home)
The next step up from the Personal version, but still only costing $99, and provides full access to all the features built-in to any of the BrowseGate family of proxy servers, The only limitation is that a maximum of 4 concurrent PC's may use it at any one time.

BrowseGate(Work)
The flagship version - Starts at only $165, and provides full access to all the features built-in to any of the BrowseGate family of proxy servers. It provides access for 5 (or more if registered) concurrent PC's initially, and this number can be increased in multiples of 5 users at any time for a small incremental license cost..

IMPORTANT - Using IE5 on the same PC as BrowseGate + Internet connection

If you are just setting BrowseGate up, and have noticed that the IE5 Web browser on the same PC as BrowseGate is not using BrowseGate for it's web access, please read on ....

We have spent considerable time discussing the new (and we consider broken) connectivity that MS have built in to IE5.x, which differs considerably from that in all earlier versions of IE.

This problem only appears when you are using a modem connection, and does not (usually) occur if you have a DSL connection or a cable modem connection such as RoadRunner.

What happens is that any PC running IE5 on the same PC as BrowseGate will notice that IE5 will almost certainly NOT use BrowseGate despite it's being configured to use a proxy server. This only seems to apply if the dial-up Internet connection is via a modem and it is on the **same PC as BrowseGate**.

Microsoft insist this behaviour is not a fault, but has been designed into IE5 to allow it to find any existing modem connection, and unfortunately, there is nothing either we or you can do to correct this major problem in IE5. (They did however suggest that if enough users write to Microsoft complaining about it we may get it changed in later releases of IE)

This is NOT A BROWSEGATE SPECIFIC PROBLEM, Microsoft admit that this behaviour will occur using any proxy server whatosever if a dial up connection exists on that PC at the time.

They simply told us that as far as they are concerned you shouldn't be using IE5 on the same PC as a proxy server and the external dial-up connection !!!!!

However - please note that **IE5 will work with BrowseGate totally correctly on any other PC that is connecting across your network, but it will NOT do so on the same PC as BrowseGate and a dial-up connection....**

NB: Netscape v4.xx does NOT have this problem, and works correctly with BrowseGate on the same PC. as well as across your network !!

If you are fortunate enough to have a permanent connection to the Internet via DSL, RoadRunner, a T1/T3 line or other fixed 24/7 connection, then this setting will define how many minutes there should be between BrowseGate's requests to NetClock to reset the server PC's clock.

We recommend a figure of 15 minutes or greater is more than sufficient for this operation, but it can be set to and value from 5 minutes to 1440 minutes (24 hours)

If you have a dial-up connection (Analog, ISDN or similar, this setting is ignored as BrowseGate will always request the time update each time it successfully makes a dial-up connection.

Configuring Netscape Messenger

BrowseGate Setup:

Configure | Email Tab

- Incoming mail tab with remote port set to 110.
- Outgoing mail with remote connection set to port 25.
  Local ports for both set to whatever you wish....

Messenger Setup: **(based on Communicator 4.7)**

1. Start Netscape Messenger
2. Select the menu/dialog options - Edit | Preferences | Mail & Newsgroups | Mail Servers
3. Click Add to create an incoming mail server in the top list

3a. In the Server Name field, enter the NETBIOS name (PC name) or IP address of the PC on which BrowseGate is running.
3b. Select POP3 or IMAP as appropriate in the list box.
3c. Enter the user ID required to access that mailbox in the User Name field.
3d. Set the other options on this tab and the POP tab as preferred.
3e. Click OK to return to the previous dialog.

4. In the Outgoing Mail Server field, enter the NETBIOS name (PC name) or IP address of the PC on which BrowseGate is running.
5. For some reason, you must also enter an Id/name for access to the SMTP server, EVEN IF YOUR SMTP SERVER DOES NOT REQUIRE ONE !!!! It seems to work correctly if you enter your normal POP3 user name/ID.
6. Set other options as required.

Messenger should now connect via BrowseGate !!!

NOTES

We have found that that Messenger may also request your mail box password when trying to send mail

If you have used non standard ports (which are 110 for POP3 and 25 for SMTP) for POP3 and SMTP in BrowseGate, all you need to do is add the port number after a colon at the end of the POP3 or SMTP fields. eg: 192.168.4.10:654 where :654 represents the internal port configured for this protocol in BrowseGate.

This list shows you all of the UDP proxies you have configured at present.

You can enable or disable entries in this list by double clicking them.
The LED will turn GREEN if it is enabled, or RED if it is enabled.

You need to enter the host machine name, or IP addess,
of the remote machine you want this particular proxy to connect to
in this field.

If only a single UDP port is needed, use this field to select or enter the port you want to be used for this connection.

If the proxy you are setting up requires a range of UDP ports enter them in this field in the format xxxx-yyyyy with NO SPACES between them.

This shows you if the proxy is currently available for use. When editing you can check/uncheck this option, but you can also double click the entry in the listbox to toglle the active status of any UDP proxy.

Update
If you wish to save any changes, or a new entry, you MUST click this button BEFORE clicking tghe Apply or OK buttons of the property sheet itself.

Cancel
This button will discard any changes you have made to the current entry.

UDP Port mapping

Because any applications that you may be using with BrowseGate acting as a UDP gateway for outgoing or incoming connections to the external hosts, it is most important that you understand how to "open" these ports in BrowseGate, and how to configure the addressing in the applications concerned.

Setting up the applications

In just the same way as all other proxies are used, you do NOT enter the external host machine names within the networked application, but instead you use either the IP address, or the NETBIOS name of the BrowseGate PC as the host machine to which the application wants to connect. BrowseGate will of course already know the name of the EXTERNAL host to which it needs to connect to provide the required UDP proxy service., so the application itself is configured quite simply to connect to the BrowseGate PC, and NOT THE EXTERNAL HOST MACHINE.

Setting up the proxies in BrowseGate

BrowseGate provides configuration for both incoming and outgoing UDP port mapping. If you wish to open an OUTGOING UDP port, you simply specify the host name that connection is to connect to, and the port (or range of ports) you want to use for it. *Do NOT check the Incoming port option in this case*.

If you wish to open an INCOMING UDP port, you need to enter into the host name field the IP address of the PC that is going to use that inbound connection. Because BrowseGate is (currently at least) a high level proxy server, it is not possible to share these inbound ports amongst multiple networked computers.

You still enter a single port (or range of ports) you want to use for this inbound UDP proxy, but *In this case you MUST ENSURE that you have checked the Incoming port option*.

CAUTION

Due to internal limitations in the Microsoft Windows implementation of the Winsock, there is a limit of approximately 128 sockets that may be used at any one time. If you create AND enable large ranges or UDP sockets (or too many TCP mappings, or any of the other proxies **at one and the same time**, you may exceed this limit, and some of the proxies you expect to have available will almost certainly not work as expected.

This is because the proxies are loaded on a first come first serve basis, and once this Winsock limit is reached, any further requests for a new socket connection will be refused by the Winsock, and will not therefore be made available to your networked applications.

Due to internal limitations in the Microsoft Windows implementation of the Winsock, you may only have approximately 128 sockets open or in use at any one time.

If you create and enable large UDP ranges (or too many TCP mappings or other proxies at one and the same time in BrowseGate, some will almost certainly not work correctly.

This is because the proxies are loaded on an intenally arranged sequence, and once this Winsock limit is reached, all further requests to open a socket will be refused by the Winsock, and will not therefore be made available to your network.

Please note that this is a limit imposed by the Windows operating system, and not a limit caused by BrowseGate.

Configuring AOL v4 to work with BrowseGate

BrowseGate full supports SOCKS4/5 connection methods that can be used with the the AOL v4.0 and later software provided by AOL.

It is very easy to get this to connect via BrowseGate by following the instructions below.

1. Run AOL.
2. From the sign on screen select Setup
3. Select the "Expert Setup" option on the dialog that appears next.
4. Finally select the ISP/LAN connection option on the "Connection setup" window

Now working on the ISP/LAN connection window that will appear

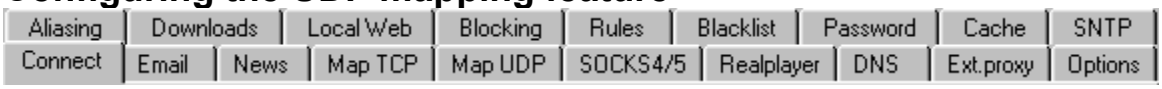
5. Select the TCP/IP Network or other connection option
6. Set the retries to around 10.
7. Click on the Manual Proxy Configuration option
8. Now click the VIEW button.
9. Check the Connect using proxy option
10. Ignore the fields in the Server frame - **these are AOL preset settings**.
11. Check the "SOCKS5" option in the Protocol frame to the right
12. In the Proxy Server host field enter either the IP address of the PC on which BrowseGate is installed, or more easily, you can simply use either the NETBIOS name of the BrowseGate machine.
13. Set the server port number to whatever local port BrowseGate uses for SOCKS requests across the network (typically this will be port 1080)
14. You do not need to enter anything into the authentication fields.
10. Ensure you have the BrowseGate external DNS operating, and **check** the "Use proxy to resolve hostnames" option.
11. If you have to pay for telephone calls, we recommend you DO NOT check the "Keep connection alive" option, as this will obviously keep any dial up connection made by BrowseGate open all of the time.
12. Click the OK BUTTON. and Close buttons all the way back to the login screen to save your changes.

Now test AOL with BrowseGate !!!!

If you still have problems, Please contact Netscape or AOL, or check their web site Help systems for firewalls and proxy information.

Configuring the Netclock plug-in SNTP system (if installed)

Configuring the UDP mapping feature

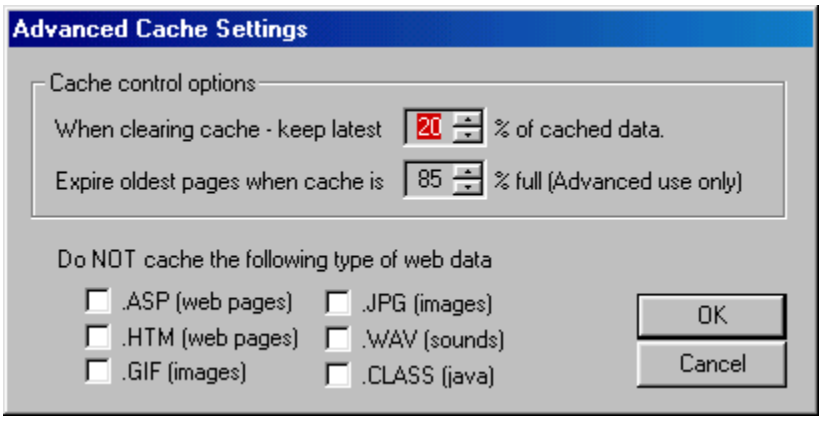


You can configure the new View menu to suit your own preferences.

If the "Show additional mappings" option is checked, the lower section of the menu will list ALL of your additional TCP port mappings.

You can also toggle the display of the port number(s) shown with the second option.

If this option is checked, The BrowseGate log window will exclude all DNS requests received by it.


Advanced Cache Settings
Cache control options
When clearing cache - keep latest
20
% of cached data.
Expire oldest pages when cache is
85
% full (Advanced use only)
Do NOT cache the following type of web data
.ASP (web pages)
.HTM (web pages)
.GIF (images)
.JPG (images)
.WAV (sounds)
.CLASS (java)
OK
Cancel

Setting up your network to use BrowseGate with RoadRunner (& other cable modems)

BACKGROUND

Unless you have purchased more than one IP address to go with your new cable modem or DSL connection, which is what the providers try to get you to do, you may find that when you first have your cable modem connection to the Internet installed, one of the first things you may discover is that only the PC that has the cable modem configured on it is able to access the Internet at all via your nice fast cable modem. This usually applies whether the new connection is plugged into your hub or the back of one PC

There are two solutions to this :-

ONE - Spend more money with your cable suplier buying additional IP addresses for each and every PC on your network. (**Expensive!!**)
TWO - Buy one cheap ($30) network card and use your copy of BrowseGate to provide connectivity to all your networked PC's by following the instructions below. (**Much Cheaper!!**)

Despite what your cable operator may tell you, you do NOT have to purchase additional IP addresses from the cable provider just to let all your PC's connect to the internet. It is totally legal and much cheaper to follow our recommendations which tell you how you can use your BrowseGate proxy server to provide them all with an Internet connection.

Therefore the following information applies only to option **TWO** above for obvious reasons.....

BrowseGate is fully able to provide you with effective and controlled single point internet access through "RoadRunner" or other similar cable modem Internet connection, but there are a few important things you will need to know about and do to set this up to work correctly.

The following instructions may sound complex at first, but actually are really very simple once you have read them through a couple of times

Your cable modem will usually have been plugged into whatever existing network card you already had in the PC that you have decided to designate as being the PC that is to have the cable connection, or they may even have plugged it into your network hub if you have one, but even then, you will still have had to specify which of your networked PC's you wanted to be the "Cable host PC". Either connection type is fine as far as BrowseGate is concerned.

However, although the cable companies will usually tell you that they do not support multiple network cards in a PC, this is purely for their own commercial interest as they are only interested in selling you more IP addresses for each of your other computers!!!.

All you need to get your other PC's connected to the Internet is a second Network Interface card (NIC). This must be installed in the PC you designated as the "Cable host" PC. Once this is installed and configured to be the INTERNAL network connection, all of the PC's on your network will be able to connect to the Internet via BrowseGate through the cable modem on the "Cable host PC". The typical cost of this 2nd NIC is around $30 at most, which is far cheaper than purchasing more fixed IP numbers from your cable supplier.

The reason for needing this second NIC is all down to the way that TCP/IP addresses are

needed on any private network. Your existing network will almost certainly have been set up with what are known as Class "C" addresses, such as 192.168.xxx.xxx or possibly 10.10.xxx.xxx, but because the cable modem makes you a (semi)permanent part of the Internet, it will always assign a dynamic Class "A" address to the relevant NIC in your "Cable host PC" . (NB This dynamically assigned IP address CAN sometimes change, so we recommend you always you always use the machine name of the "Cable Host PC" rather than the ip address as the host in all of your networked applications (see below).

The people that fitted your cable modem will almost certainly have set or reset your network card settings to use a dynamically assigned IP which is essential if the cable modem is to work correctly. This will be an IP address something like 24.92.xx.xx or 207.100.xxx.xxx.

If you already had a network running prior to the cable modem being installed, you have probably noticed that the "Cable host PC" can no longer be seen (under TCP at least) on your internal network due to this change to the dynamically assigned IP address. This is why the 2nd NIC is required. You may have previously had your internal networked PC's connecting to each other using the Microsoft File and Printer sharing alone, and may not have been running TCP, but this is going to be essential now if you want to have all of you networked PC's accessing the internet via BrowseGate and your new cable modem.

So, enough of the background - what do you need to do ?

All you actually need to do is to go to your local computer superstore, purchase and install a new (and 2nd) NIC in any spare slot in your "Cable host PC". Once you have got this working and set up the drivers etc provided, go to the Start -> Control Panel -> Network property sheet, and locate the entry in the list for **TCP/IP** on your **new NIC** card. (Be careful not to change the original one.....)

On the IP address tab, nothing should be selected, so you need to select the "Specify an IP address" option and then in the fields below enter a suitable Class C address that is compatible with the ip addresses on your other network machines. (NB the first 3 sets of digits must be identical, and the last block (the xxx in the following) 192.168.100.xxx must be TOTALLY UNIQUE on your network.) Finally, and don't bother asking why at this stage, the "Net Mask" field should always be set to **255.255.255.0**

So if you networked PC's have been assigned addresses of say 192.168.45.10 and 192.168.45.11 then you might quite reasonably choose 192.168.45.12, or even perhaps 192.168.45.89 if you wish, for the IP address of the new NIC card. Just ensure the LAST number (11, 12, 89 etc) is unique.....

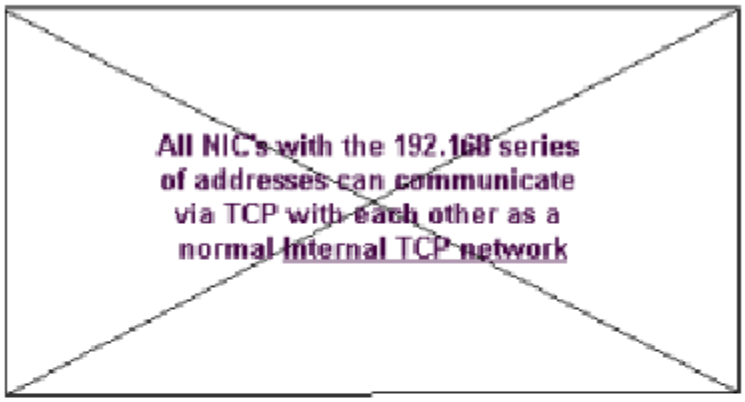
Normally the settings for WINS, Gateway and DNS should all be disabled on most simple networks.

Windows will tell you that you must restart you PC after this process, and once it has rebooted, all of your PC's should now be able to connect to each other under TCP as they (probably) used to (see the diagram below)

BrowseGate will now handle all of the internet connectivity between each of your networked PC's and the cable modem itself as shown in the diagram below..... But you must still configure the Internet applications on each of your networked to use BrowseGate, which is covered in this help system for most commonly used applications.

192.168.100.10

192.168.100.17



192.168.100.15

192.168.100.19

BrowseGate is able to communicate with BOTH sets of IP addresses, thus making the connection between your internal network and the Cable modem totally transparent in day to day use.

The 24.92.xxx.xxx cable modem IP address CANNOT be connected to by any of the other PC's at all.

24.92.175.123

This is the Cable Host PC with TWO IP addresses, 192.168.xx.xx. for internal networking and the other for the dynamically assigned cable modem IP address.

How to use more than the 24 site blocking entries

If you have a need to use more than the 24 site blocking fields provided on the Configure -> "Blocking" tab, you can add further entries manually by following the instructions below CAREFULLY.

BrowseGate uses Window's INI configuration file named BRWGATE.INI to store it's entire configuration information. This are file is a plain ASCII text file that can be edited with Notepad.

Before you make any changes, we recommend you back the file up first.

Open BRWGATE.INI in Notepad or other ASCII text editor.

Find a section heading named [BLOCK] (may be in upper or lower case)

There will always be two sets of 24 entries in this section, numbered from 0 - 23
eg:
al0=www.netcplus.com*
al1=www.microsoft.com*
.....
al23=www.netscape.com*

These are the actual "mask" entries that you want to allow networked users to access.

there are also the same number of entries as shown below
eg:
alinuse0=1
alinuse1=0
.....
alinuse23=1

These are the indicators as to whether a block entry is active (1) or inactive (0).

If you really find that want to add more, you can do so up to a maximum of 999.

All you need to do is to add further entries to this list, ensuring that for each "mask" entry (ALxx) there is also an active status entry (ALINUSExx)

The numbering of these additional entries you add MUST use CONSECUTIVE numbering at all times.
eg :
The first entry you may wish add will always be AL24 and ALINUSE24, etc etc.

If you later choose to remove one or more entries, you MUST renumber the entries so that there are NO GAPS in this numbering scheme.

If you fail to do so, all blocking masks **beyond** the missing number will ALWAYS be ignored by the BrowseGate parser.

NB: You will not of course be able to edit these "additional" entries via the BrowseGate Blocking

property sheet.